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

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

Nexenta, NexentaStor, NexentaCloud, NexentaEdge, NexentaFusion, and NexentaCloud are registered trademarks of Nexenta by DDN in the United States and other countries. All other trademarks, service marks, and company names in this document are properties of their respective owners.
| Contents |
|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|
| Preface | 1 Document Overview |
| 1 | 2 |
| About This Document | Accessing Online Help |
| 2 | 3 |
| Supported Web Browsers | Viewing Online Help |
| 3 | 4 |
| Additional Resources | Terminology |
| 4 | 5 |
| What Comes Next? | 2 NexentaFusion Overview |
| 5 | 6 |
| 2 | 7 |
| Introducing NexentaFusion | Initially Logging in to NexentaFusion |
| 6 | 8 |
| TLS/SSL Certificate Warning | Login for the First Time After Installation |
| 7 | 9 |
| Next Steps | 3 Configuring NexentaFusion |
| 8 | 10 |
| Getting Started with NexentaFusion | NexentaFusion Main Menu Bar |
| 9 | 11 |
| Mode Selector: 1 | Appliance List Selector: 2 |
| 10 | 12 |
| Logged-in User: 3 | Fusion Server Health icon: 4 |
| 11 | 13 |
| Main COG: 5 | Availability of Fusion Software Updates: bell icon |
| 12 | 14 |
| 3 | Configuring NexentaFusion |
| 13 | 15 |
| NexentaFusion Icons, Main COG, and Top-Level Tabs | Appliances List Page |
| 14 | 16 |
| NexentaFusion Icons | Main COG |
| 15 | 17 |
| Top-Level Tabs | What Comes Next? |
| 16 | 18 |
| | NexentaFusion Configuration Overview |
Using the NexentaFusion UI to Create and Upload Support Bundles  .......... 48
Using the Console Wizard to Create and Upload Support Bundles .......... 49
Using Docker to Create and Upload Support Bundles  ..................... 50
  Bundle Examples  ..................................................... 50
Fusion Server health .................................................... 51
Elasticsearch Database .................................................. 52
Fusion Services Management ............................................. 52
What Comes Next?  ..................................................... 53

4  Registering NexentaStor Appliances  ..................................... 54
  How to Register a NexentaStor Appliance  ............................. 54
  Confirming Registration ............................................... 57
  Identifying NexentaFusion GUI from NexentaStor ..................... 58
  Rebinding an Appliance .............................................. 59
  Viewing an Appliance Summary ...................................... 59
  Viewing Appliance Licenses .......................................... 60
  Updating the License ................................................. 61
  Removing an Appliance .............................................. 62
    Viewing the Historical Analytics of a Removed Appliance .......... 63
  What Comes Next?  ................................................... 64

5  Managing NexentaStor Appliances  ..................................... 65
  Viewing Server, Enclosure, and Disk Information ...................... 65
    Viewing an Appliance Profile and Version  ........................ 65
    Viewing Server Components ..................................... 66
    Viewing Chassis Enclosures and Devices  .......................... 67
    Viewing Chassis Sensor Values ................................... 68
    Locating Chassis using Blink Feature  ............................. 70
    Viewing and Locating Chassis Devices ................................ 71
  Managing Network Configurations ..................................... 73
    Verifying and Modifying IP Links .................................. 74
    Creating Aggregates .............................................. 75
    Adding a VLAN ..................................................... 77
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Editing System Configuration Settings</td>
<td>103</td>
</tr>
<tr>
<td>Viewing Available Software Updates</td>
<td>106</td>
</tr>
<tr>
<td>Configuring Data Settings</td>
<td>106</td>
</tr>
<tr>
<td>Configuring Logs</td>
<td>106</td>
</tr>
<tr>
<td>Configuring Events Retention</td>
<td>107</td>
</tr>
<tr>
<td>Active Probes</td>
<td>108</td>
</tr>
<tr>
<td>Managing Analytics Aggregation Data</td>
<td>110</td>
</tr>
<tr>
<td>Rebooting or Powering Off a NexentaStor/NexentaCloud Appliance</td>
<td>110</td>
</tr>
<tr>
<td>What Comes Next?</td>
<td>111</td>
</tr>
<tr>
<td><strong>8 Managing Storage</strong></td>
<td>112</td>
</tr>
<tr>
<td>Provisioning Overview</td>
<td>112</td>
</tr>
<tr>
<td>Viewing Available Disks for Pool or Log or Cache</td>
<td>114</td>
</tr>
<tr>
<td>Creating and Removing Pools</td>
<td>114</td>
</tr>
<tr>
<td>Planning for Pools</td>
<td>114</td>
</tr>
<tr>
<td>Viewing Available Disks for a Pool</td>
<td>115</td>
</tr>
<tr>
<td>Creating Pools on Single or Clustered Nodes</td>
<td>116</td>
</tr>
<tr>
<td>Beginning Pool Creation</td>
<td>116</td>
</tr>
<tr>
<td>Selecting Data Devices for Pool Using Auto Method</td>
<td>117</td>
</tr>
<tr>
<td>Selecting Data Devices for the Pool Manually</td>
<td>119</td>
</tr>
<tr>
<td>Guided Configuration</td>
<td>119</td>
</tr>
<tr>
<td>Adding Cache, Log, and Spare Devices to a Pool</td>
<td>122</td>
</tr>
<tr>
<td>Smart Sparing</td>
<td>123</td>
</tr>
<tr>
<td>Finish Pool Creation</td>
<td>124</td>
</tr>
<tr>
<td>Importing and Exporting Pools</td>
<td>125</td>
</tr>
<tr>
<td>Finding an Exported Pool to Import</td>
<td>125</td>
</tr>
<tr>
<td>Exporting a Pool</td>
<td>127</td>
</tr>
<tr>
<td>Destroying a Pool</td>
<td>127</td>
</tr>
<tr>
<td>Maintaining Pools</td>
<td>128</td>
</tr>
<tr>
<td>Scrub</td>
<td>129</td>
</tr>
<tr>
<td>Unmap/Trim</td>
<td>129</td>
</tr>
<tr>
<td>Pool Properties</td>
<td>130</td>
</tr>
<tr>
<td>Editing a Pool - Adding Capacity to an Existing Pool</td>
<td>132</td>
</tr>
</tbody>
</table>
Viewing Pool Status .......................................................... 133
Pool Management Actions for High Availability .................... 133
Managing Pool Data Devices and Faults ............................... 134
Smart Sparing and Device Replacement ............................... 135
Removing a Device from a Pool ........................................ 136
Replacing a Device in a Pool ............................................ 136
Attaching a New Mirror Device ........................................ 137
Detaching a Device from a Mirror .................................... 137
Setting a Device in a Pool to Offline .................................... 137
Setting a Physical Device to Online .................................... 138
Clearing Errors from a Device ........................................... 138
Clearing Errors from all Devices in a Pool .................. 138
What Comes Next? ......................................................... 138

9 Managing Datasets ......................................................... 139
Overview ................................................................. 139
Creating and Managing File Systems ............................... 140
Creating a File System on a Pool ..................................... 140
Note for the Estimated Maximum IOPs ................................ 144
Viewing File Systems ..................................................... 144
Filtering File System Listings .......................................... 147
Sharing File Systems Using NFS ....................................... 148
Configuring and Enabling the NFS Server ....................... 148
Creating an NFS Share .................................................... 149
Open Shares ............................................................. 150
Shares with Security Options ......................................... 150
Creating an NFS Share for a File System ....................... 151
Sharing File Systems Using SMB .................................... 154
Configuring and Enabling the SMB Server ..................... 154
Setting min and max Protocol Version for SMB Client .......... 156
Creating an SMB Share ................................................. 157
Mapping an SMB Share on Windows ........................... 158
Sharing Filesystems Using S3 .......................................... 159
Creating S3 share ...................................................... 160
  Creating an S3 share for a Filesystem ...................... 160
Creating and Managing Volume Groups and Volumes .......... 163
  Creating a Volume Group ...................................... 164
  Creating Volumes .............................................. 166
  Editing Properties for Volume Groups and Volumes ...... 168
  Deleting a Volume Group or Volume ......................... 170
Managing iSCSI Host Groups, Targets, and Groups .......... 171
  Creating, Editing, and Destroying iSCSI Targets and Target Groups ................. 171
    Creating iSCSI Targets .................................... 171
    Creating iSCSI Target Groups ............................... 173
    Viewing iSCSI Target Information and Sessions ............ 174
    Editing or Deleting iSCSI Targets .......................... 175
    Removing iSCSI Targets from a Group and Destroying the Target Group .......... 177
Configuring Secure Authentication ................................ 178
  Unidirectional CHAP Authentication .......................... 178
  Bidirectional CHAP ........................................... 178
Configuring iSCSI Host Groups .................................. 179
Managing FC Host Groups, Targets and Target Groups .... 181
  Configuring FC Host Groups .................................. 181
  Adding FC Targets to a New or Existing FC Target Group .... 182
  Removing FC Targets from a Group ........................... 183
  Viewing Target Group Sessions ................................ 184
  Destroying FC Target Groups .................................. 185
Managing LUNs ........................................................ 185
  Mapping Volumes ................................................ 186
  Viewing LUN Information ...................................... 187
  Editing and Destroying LUN Mappings ......................... 188
Protecting Data ....................................................... 189
  Taking a One-Time Snapshot ................................. 190
  Cloning a Snapshot and Promoting a Clone .................. 191
  Rolling Back or Deleting a Snapshot ......................... 192
Preparing the Appliance for Replication ......................................................... 194
  Setting the Replication Network Interface .............................................. 194
  Setting the Replication Group Password .................................................. 196
Adding a Protection Service ............................................................................ 196
  Working with Protection Services .............................................................. 196
  Adding a Scheduled Replication Service .................................................... 198
  Adding a Scheduled Snapshots Service ..................................................... 201
  Filtering Snapshots and Data Protection Service Data ............................... 203
Configuring Continuous Replication ............................................................... 204
Editing or Deleting a Schedule ....................................................................... 207
Manually Executing a Service ......................................................................... 208
Disabling and Enabling a Protection Service .................................................. 208
Destroying a Protection Service ....................................................................... 209
Viewing the Replication History ................................................................... 211
Flipping the Direction of a Replication Service .............................................. 212
Activating a Destination Dataset ................................................................... 213
Recovering a Faulted Replication Service ..................................................... 214
Verifying and Querying Data Protection Data ............................................... 216
What Comes Next? ....................................................................................... 217

10 Managing High Availability ................................................................. 218
About NexentaStor High Availability .......................................................... 218
  NexentaStor HA on Bare-Metal ................................................................. 218
  NexentaStor VSA on VMware ................................................................. 219
  Additional Information ............................................................................. 219
About NexentaStor High Availability and HA Services ............................... 220
  HA Cluster ................................................................................................. 220
  HA Service ................................................................................................. 220
Editing vCenter Credentials for VSA-based Clusters ................................. 220
Verifying Cluster Status ................................................................................ 221
  Viewing Network Heartbeats ..................................................................... 222
Managing High Availability Storage ............................................................. 222
  Configuring an HA Service for a Pool with Shared Devices ..................... 223
Adding an Unshared Pool to an HA Service .............................................. 224
Viewing Status Details for a Shared Pool .................................................. 226
Moving a Pool under HA Service Control ............................................... 227
Removing a Pool From HA Control ......................................................... 228
Managing HA Services ........................................................................ 229
Verifying Service Status ....................................................................... 230
Viewing VIPs Associated with an HA Service ....................................... 231
Adding a VIP ......................................................................................... 231
Editing and Deleting a VIP .................................................................... 232
Viewing Disk Heartbeats ....................................................................... 232
Viewing SCSI Reservation Details ......................................................... 233
Failing Over Services Manually .............................................................. 233
Moving an HA Service ........................................................................ 234
Setting the HA Service Mode ................................................................. 235
Stopping and Starting an HA Service .................................................... 236
Destroying an HA Service ..................................................................... 236
What Comes Next? ............................................................................... 237

11 Performance Monitoring and Analytics ............................................. 238
Terminology ......................................................................................... 238
Dashboard ........................................................................................... 239
Using the Default Dashboard ................................................................. 240
What Comes Next? ............................................................................... 241
Using the Analytics Workspace ............................................................ 242
Understanding the Analytics Workspace .............................................. 242
Canvas Workspace: 1 ........................................................................... 242
Widget Selection Panel: 2 ..................................................................... 242
Canvas Bar: 3 ....................................................................................... 243
Navigating to the Analytics Workspace ................................................... 243
Using a Canvas .................................................................................... 244
Creating a New Canvas .......................................................................... 244
Adding, Moving, Resizing, and Removing Widgets ................................. 245
Managing Canvases ............................................................................ 246
12 Fault Management ................................................. 264
  About Fusion Alerts, Logs, Audits, and Events .................. 264
  Managing Fusion Alerts ........................................ 265
    Searching for Alerts ......................................... 265
    Acknowledging Alerts ....................................... 266
    Expanding and Exporting Fusion Alerts ....................... 267
    Viewing and Editing an Alert Notification Rule ............... 270
  Managing Logs and Audits ..................................... 270
    Searching for Logs and Audits ................................ 271
    Expanding and Exporting Audits and Logs .................... 272
Creating Rules for Logs and Events ........................................................... 274
Managing Appliance Alert Cases ................................................................. 277
  View Active Cases Detected by the Appliance ........................................... 277
  View Historical Cases .............................................................................. 278
  Using DISK View to View an Active FMA Case ....................................... 279
  Using DISK Case Details to Locate the Problem Device ......................... 280
  Configure SMTP Settings and Alert Settings ............................................ 282
    Set up Warning and Error Alert Threshold Settings ............................... 282
Troubleshooting Data Devices in a Pool ....................................................... 282
  Locating a Failed Disk ............................................................................. 283
  Replacing a Failed Disk ........................................................................... 284
Using NexentaStor Virus Scan Service ........................................................ 285
  About NexentaStor vscan ...................................................................... 285
  Prerequisites ............................................................................................ 285
  Managing Virus Scan Services on a NexentaStor Appliance using NexentaFusion ... 285
Managing Appliance Support Bundles ........................................................ 286
  Create a Support Bundle .......................................................................... 286
  Identify and Include the Core Files to Support Bundle ............................ 287
  Delete Core Files .................................................................................... 287
  Download the Bundle Locally ................................................................... 287
  Default Support Bundle Protocol and Settings ...................................... 288
  Modify Default Settings for Slow Connections ....................................... 288
  Upload Support Bundles to Nexenta's https Server ............................... 288
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.

Product Versions Applicable to this Documentation:

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nf-1.2-userguide-RevB</td>
<td>November, 2018</td>
<td>NexentaFusion 1.2.1 GA version</td>
</tr>
<tr>
<td>nf-1.2-userguide-RevC</td>
<td>May, 2020</td>
<td>NexentaFusion 1.2.2 GA version</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.
Document Overview

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 and NexentaCloud 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 and NexentaCloud appliances in your environment.

- **Chapter 3: Configuring NexentaFusion**
  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 4: Registering NexentaStor Appliances**
  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 5: Managing NexentaStor Appliances**
  This chapter shows how to view appliance nodes, identify disks, and manage network interfaces.

- **Chapter 6: Deploying NexentaCloud Appliances**
  This chapter shows how to prepare for and deploy a NexentaCloud for AWS appliance.

- **Chapter 7: Managing Appliance System and Data settings**
This chapter shows how to manage appliance system services, system configuration settings, data retention settings, and rebooting and powering off the appliance.

- **Chapter 8: Managing Storage**
  This chapter demonstrates how to create and manage pools.

- **Chapter 9: Managing Datasets**
  This chapter demonstrates how to create and share file systems, and create and map volumes to LUNs.

- **Chapter 10: Managing High Availability**
  This chapter explains high availability (HA) and HA services, then demonstrates how to verify cluster status, manage high availability storage and high availability services.

- **Chapter 11: 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 12: 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, 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.x 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. Open a Web browser and enter the following URL: https://<NexentaFusion_IP>:8457
  2. Enter your user login credentials.

  This opens the **Appliance List** view.
3. In the upper right corner, click the Main COG.
4. 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 at [https://nexenta.com/products/nexentastor](https://nexenta.com/products/nexentastor).

**Table 1-1: Documentation Resources**

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>NexentaStor 5.x CLI Configuration Guide</em></td>
<td>This guide demonstrates the basic steps and commands to configure and manage NexentaStor 5.x appliances. Use this document in conjunction with the <em>NexentaStor 5.x Command Line Interface Reference Guide</em>, and the <em>NexentaStor 5.x HA CLI Admin Guide</em>.</td>
</tr>
<tr>
<td><em>NexentaStor 5.x CLI Reference Guide</em></td>
<td>This reference guide provides a summary of the CLI commands. Use it in conjunction with the companion document, <em>NexentaStor 5.x CLI Configuration Guide</em>.</td>
</tr>
<tr>
<td><em>NexentaStor 5.x HA CLI Configuration Guide</em></td>
<td>This guide demonstrates the basic steps and commands to configure and manage the NexentaStor 5.x High Availability (HA) cluster using the NexentaStor 5.x Command Line Interface (CLI).</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>NexentaCloud for AWS Appliance</td>
<td>NexentaCloud is a software based storage solution that is based on the NexentaStor codebase, running in the AWS cloud, using Amazon EBS storage to support file and block services, along with a variety of advanced storage features such as replication, snapshots, and clones.</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).

<table>
<thead>
<tr>
<th>Terms</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<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 12, 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/NexentaCloud appliances. Appliance mode has the necessary UI elements to manage appliances, both single node and clustered.</td>
</tr>
</tbody>
</table>
This chapter introduces the basic functionality of NexentaFusion, and covers the following topics:

- **Introducing NexentaFusion**
- **Initially Logging in to NexentaFusion**
- **Getting Started with NexentaFusion**
- **NexentaFusion Main Menu Bar**
- **NexentaFusion Icons, Main COG, and Top-Level Tabs**
- **What Comes Next?**

### Introducing NexentaFusion

The NexentaFusion user interface (UI) enables you to intuitively manage NexentaStor and NexentaCloud 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=PLlXP6v5WL0ZQRlzhF5ERlq22ReWAmIESW](https://www.youtube.com/watch?v=ryBGX6B0sAA&list=PLlXP6v5WL0ZQRlzhF5ERlq22ReWAmIESW).
Initially Logging in to NexentaFusion

**TLS/SSL Certificate Warning**

After successfully installing NexentaFusion, the End User Licence Agreement (EULA) appears. Scroll to the bottom of the EULA and click **Accept**.

It is possible to receive a warning that a server 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.

Configuring a certificate from a trusted authority is a secure practice for web-based systems that prevents users from encountering browser warnings and other unexpected behavior. Using a trusted certificate authority can also enable important practices, such as certificate revocation.

NexentaFusion is installed with a self-signed certificate. We recommend that after starting Fusion, you install your own custom certificate. While using the self-signed certificate included with NexentaFusion, you can expect to experience the following:

- The first time a browser encounters a certificate that wasn’t issued by a known certificate authority, it will raise an error and refuse to connect to the site.
- You have to sign off on exceptions, which can be done on a one-time basis, or by accepting the certificate indefinitely going forward.
- Many browsers display warning icons or a red color in the address bar as long as you are using the self-signed certificate.
- Even after choosing to accept the certificate, browsers may display warnings to indicate that the certificate remains an exception.

| Note: | The use of a self-signed certificate is not recommended, as it can leave your network open to the vulnerability of attack. See [Managing NexentaFusion SSL Certificates](#) to install a custom certificate. |

In the case of a TLS/SSL certificate warning, do the following:

- 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.

**Login for the First Time After Installation**

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 after installation, do the following:

1. In a Web browser, enter the URL of the system on which NexentaFusion is installed, followed by the default port 8457. For example:
   https://<NexentaFusion_IP_Address>:8457

2. Enter the following NexentaFusion default credentials:
   username: admin
   password: nexenta

3. Change the password for this predefined admin user account.

Note: Passwords should be at least 9 characters long and contain at least 3 of the following classes of characters: lowercase, uppercase, numeric, and special (for example, !, @, #, $, %, ^). Passwords should not be based on English dictionary or slang words, nor English first names or surnames.

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 NexentaFusion Main Menu Bar and NexentaFusion Icons, Main COG, and Top-Level Tabs.

Task 1: Configure NexentaFusion.

Complete the basic configuration to establish the connection between the NexentaFusion and NexentaStor appliances, as described in Chapter 3, Configuring NexentaFusion.

Task 2: Register a NexentaStor appliance or Deploy a NexentaCloud appliance

When you first log in to NexentaFusion you are presented with the Appliances List screen.

To begin managing an on-premise NexentaStor appliance, register it as described in Chapter 4, Registering NexentaStor Appliances.

To deploy and register a NexentaCloud in AWS appliance, follow the directions described in Chapter 6, Deploying and Managing NexentaCloud Appliances.


Start provisioning and managing NexentaStor appliances by clicking the name or icon of the appliance in the list, and following the directions described in Chapter 5, Managing NexentaStor Appliances and Chapter 8, Managing Storage.
NexentaFusion Main Menu Bar

After initially logging in to NexentaFusion, the Main menu bar is set to Appliance mode and the Appliance List view.

**Mode Selector: 1**

- Appliance mode – Used to register, deploy and manage NexentaStor and NexentaCloud appliances. For more information, see Chapter 4, Registering NexentaStor Appliances, Chapter 6, Deploying and Managing NexentaCloud Appliances, and Chapter 5, Managing NexentaStor Appliances.
- Fusion mode—Used to monitor and examine logs and alerts. For more information, see Fault Management.

**Appliance List Selector: 2**

Click on this selector while in appliance mode to select the Appliances List summary page or an individual registered appliance.

- The Appliances List page lets you register a NexentaStor appliance to be managed by Fusion. See Appliances List Page
- Selecting a registered appliance will display the Dashboard page for that appliance, and additional top-level tabs will be displayed in the menu bar for selection. See Top-Level Tabs

**Logged-in User: 3**

The logged-in user name is displayed.

**Fusion Server Health icon: 4**

The health icon will be displayed only if there is information about the Fusion server. A bell will be displayed if a Fusion software update is available. A yellow triangle indicates warning alerts, a red octagon indicates a serious failure condition. Click on the icon to display the health alerts. See Fusion Server health

**Main COG: 5**

The Main COG displays options that apply to NexentaFusion, not a specific appliance. See Main COG and Chapter 3, Configuring NexentaFusion
Availability of Fusion Software Updates: bell icon

The FusionServer health worker monitors various conditions that are critical to the proper functioning of the NexentaFusion application. Detection of a specific error condition will cause the FusionServer Health icon to appear on the Main menu bar. A bell indicates a Fusion software update is available. A yellow triangle indicates warning alerts, a red octagon indicates a serious failure condition. Click on the icon to display the health alerts.

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 NexentaStor or NexentaCloud appliance, the Appliances List page displays with the following information:

- Name—Lists the name of the device with representative icon.
- 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.
NexentaFusion Icons explains the icons that appear on the Appliances List page, and throughout the rest of the NexentaFusion UI.

- 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.

- 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>
<tbody>
<tr>
<td><img src="image" alt="Main COG" /></td>
<td><strong>Main COG</strong>&lt;br&gt;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.</td>
</tr>
<tr>
<td><img src="image" alt="Action COG" /></td>
<td><strong>Action COG</strong>&lt;br&gt;Click an action COG to display a drop-down menu of supported options.</td>
</tr>
<tr>
<td><img src="image" alt="Expand, Collapse" /></td>
<td><strong>Expand, Collapse</strong>&lt;br&gt;Click an arrow to show or hide all of the entries in a table.</td>
</tr>
<tr>
<td><img src="image" alt="Expand (Tree view)" /></td>
<td><strong>Expand (Tree view)</strong>&lt;br&gt;Click the arrow to display a list of hidden items, such as a file system under a pool.</td>
</tr>
<tr>
<td><img src="image" alt="Single node" /></td>
<td><strong>Single node</strong>&lt;br&gt;This icon represents a single node appliance.</td>
</tr>
<tr>
<td><img src="image" alt="Clustered nodes" /></td>
<td><strong>Clustered nodes</strong>&lt;br&gt;This icon represents a two-node clustered appliance.</td>
</tr>
<tr>
<td><img src="image" alt="Metro HA Cluster" /></td>
<td><strong>Metro HA Cluster</strong>&lt;br&gt;This represents a two-node clustered appliance between two geographically remote sites using the licensed Metro HA feature.</td>
</tr>
<tr>
<td><img src="image" alt="NexentaCloud appliance" /></td>
<td><strong>NexentaCloud appliance</strong>&lt;br&gt;This icon represents a NexentaCloud appliance.</td>
</tr>
<tr>
<td><img src="image" alt="Critical — Health state" /></td>
<td><strong>Critical — Health state</strong>&lt;br&gt;This red icon implies there are serious issues.</td>
</tr>
</tbody>
</table>
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 Fusion**—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.

---

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
</table>
| ![Warning icon](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 icon](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 icon](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. |
| ![Shield icon](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. |
| ![Blinking icon](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. |
| ![Blinking icon](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. |
| ![Blinking icon](image) | This icon represents a cluster service that is not running, but should be able to be restarted on a node. |
| ![Blinking icon](image) | This icon represents a cluster service that is not running on either node due to major problems. Intervention is needed. |
• **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 3, Configuring NexentaFusion](#).

• **Support**—Create, Upload, and Remove Fusion support bundles, as described. See [Managing Fusion Support Bundles](#).

• **Help**—Access the NexentaFusion online help, or download the complete help content in a PDF version of the [NexentaFusion 1.2 User Guide](#).

For more information on the Elasticsearch DB, see [Creating Rules for Logs and Events](#) in [Chapter 12, Fault Management](#).

- **To view system and audit logs, do the following:**
  1. Log in to NexentaFusion.
     
     The Appliance List view appears.
  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 12, Fault Management](#).

- **To complete basic configuration tasks in NexentaFusion, do the following:**
  1. Log in to NexentaFusion.
     
     The Appliance List view appears.
  2. Click the **Main COG** and select **Settings** from the drop-down list.
3. Do the following:

- Click **Date/Time** in the left panel to set the date and time for a device. For more information, see *To set the Server timezone, click the pencil icon*.
- Click **Email Setup** in the left panel to configuring an SMTP server for system failure notification. For more information, see *Setting the NexentaFusion SMTP Mail Server (Email Setup)*.
- Click **LDAP Authentication** in the left panel to configure NexentaFusion to access your LDAP server, for user authentication and authorization capabilities. For more information, see *About NexentaFusion as an LDAP-Client*.
- 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 3, 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 and NexentaCloud 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/NexentaCloud 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 *Chapter 5, Managing NexentaStor Appliances; Chapter 8, Managing Storage; Chapter 9, Managing Datasets; Chapter 10, Managing High Availability*.
   - **Analytics**—View performance metrics, configure widgets, create custom canvases, configure the default dashboard. For more information, see *Chapter 11, Performance Monitoring and Analytics*.
• **Administration**—Enable, view, and disable system services. Configure parameters for logs, events, and analytics for the selected NexentaStor appliance. For more information, see [Chapter 5, Managing NexentaStor Appliances; Chapter 6, Deploying and Managing NexentaCloud Appliances; Chapter 7, Managing Appliance System and Data Settings](#) and [Chapter 12, Fault Management](#).

• **Support**—View active appliance Alert cases, and those that are no longer active. View the details for a specific alert, and provide the ability to mark the case as repaired, replaced, or acquitted. Also create and manage appliance support bundle. For more information, see [Managing Appliance Alert Cases, Managing Appliance Support Bundles](#).
### 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><strong>Appliances List</strong></td>
<td>View a list of all registered appliances, or register an appliance. For more information, see Chapter 4, Registering NexentaStor Appliances and Chapter 6, Deploying and Managing NexentaCloud Appliances. Provision registered appliances. For more information, see Chapter 5, Managing NexentaStor Appliances and Chapter 8, Managing Storage.</td>
</tr>
<tr>
<td><strong>Dashboard</strong></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 Chapter 11, Performance Monitoring and Analytics.</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 8, Managing Storage and Chapter 10, Managing High Availability.  
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 Chapter 9, Managing Datasets.  
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 Chapter 9, Managing Datasets.  
Data Protection:  
Verify and query protection service data, as well as create, edit, and delete Protection Services. For more information, see Protecting Data.  
High Availability (HA):  
**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 Chapter 10, Managing High Availability. |
<table>
<thead>
<tr>
<th>Top-Level Tab</th>
<th>Supported Action</th>
</tr>
</thead>
</table>
| Components:  | 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. |
| Networks:    | Manage network interfaces, and aggregate network interfaces.  
|              | Configure VLANs, and create network routes.  
|              | For more information, see Chapter 5, Managing NexentaStor Appliances. |
| Analytics    | 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 11, Performance Monitoring and Analytics. |
Now that you’ve logged in to NexentaFusion and become familiar with the NexentaFusion UI, complete the basic configuration to establish the connection between the NexentaFusion and NexentaStor appliances.

### What Comes Next?

<table>
<thead>
<tr>
<th>Top-Level Tab</th>
<th>Supported Action</th>
</tr>
</thead>
</table>
| Administration | The Administration page allows you to manage appliance services and configuration settings, and data retention settings, as well as rebooting or powering off a NexentaStor appliance, [Chapter 7, Managing Appliance System and Data Settings](#).  
  - Under the **System Settings** tab, you can 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, ndmp, and snmp.  
  - Using the **System Configuration Settings**, you can set up alert emails; enable Swagger documentation, control routing for hosts, modify NexentaStor SMTP settings for the selected NexentaStor appliance.  
  - Under the **Data Settings** tab, you can configure data retention parameters for logs, events, and analytics for NexentaStor appliances. |
| Support       | The Support page allows you to view active appliance Alert cases, and those that are no longer active. This page also provides the ability to mark the case as repaired, replaced, or acquitted and also to create and manage appliance support bundles. See [Chapter 12, Fault Management](#). |
Configuring NexentaFusion

This chapter covers the following topics:

- NexentaFusion Configuration Overview
- Checking and Modifying NexentaFusion Network Settings
- About NexentaFusion as an LDAP-Client
- Setting the Date and Time for NexentaFusion
- Setting the NexentaFusion SMTP Mail Server (Email Setup)
- Creating, Modifying, and Deleting Local UI User Accounts
- Configuring Audit, Log, and Monitor Settings
- Configuring Session Settings
- Setting IRS Warning Message on Fusion Logon Screen
- Managing NexentaFusion SSL Certificates
- Managing Fusion Support Bundles
- Fusion Server health
- Elasticsearch Database
- Fusion Services Management
- What Comes Next?

NexentaFusion Configuration Overview

This section provides an overview of the process to follow for configuring NexentaFusion. The other sections in this chapter provide details on how to perform each of the configuration tasks.

**Note:** NexentaFusion configuration tasks can only be performed by an “Administrator”. For more information, see NexentaFusion User Roles.
To configure NexentaFusion, do the following:

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

2. Verify the NexentaFusion server Network settings, that were set to defaults or configured during the NexentaFusion installation, as described in Checking and Modifying NexentaFusion Network Settings.

3. Configure the date and time for NexentaFusion, as described in Setting the Date and Time for NexentaFusion.

4. Optional: Configure LDAP authentication for NexentaFusion users, as described in About NexentaFusion as an LDAP-Client.

5. Configure the SMTP server, as described in Setting the NexentaFusion SMTP Mail Server (Email Setup).

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

7. Configure NexentaFusion for appliance fault management, as described in Configuring Audit, Log, and Monitor Settings.

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

9. Optional: Install a SSL certificate to replace the Fusion’s default certificate. See Managing NexentaFusion SSL Certificates.


Checking and Modifying NexentaFusion Network Settings

The NexentaFusion network settings are configured during the initial installation process.

If you installed NexentaFusion as a Docker container, use parameters in the Docker run command to change the management IP and the web proxy. They cannot be changed using the Fusion UI. Refer to the NexentaFusion QuickStart Guide for details.
If you installed NexentaFusion as an OVA, the section below demonstrates how to modify select NexentaFusion network settings.

- Network configuration settings—Set and configure the Management address, and change the hostname. The management address is used to bind the NexentaStor appliances to the Fusion database, to allow it to receive analytics, logs, and events from the appliance.
- DNS servers—Explicitly specify custom Nameservers. DHCP configuration can override custom Nameservers, however.
- Search domain—Edit the custom search domain.
- Web Proxy—Edit the proxy settings.

**Note:** You can use a hostname that is resolvable for the Nexenta Management Network interface. Using a hostname is highly-recommended for use with DHCP. You can also use a static IP address.

- **To modify NexentaFusion network settings, do the following:**
  1. Log in to *NexentaFusion*, click the **Main COG** in the right corner of the window and select **Settings** from the drop-down list. The Network page is selected by default.
  2. To modify the NexentaFusion server hostname, do the following in the Network Configuration panel:
     a) Select the server **COG**.
     b) Choose **Edit Hostname** from the drop-down list.
     c) **Enter a Fusion server hostname** in the text field. The hostname must be resolvable.
  3. To reconfigure a network interface, in the Network Configuration panel select the interface **COG**, select **Configure** from the drop down list and modify the following, as necessary:
     a) Choose the **Type** of interface: Static or DHCP.
     b) Choose a network **Family**: IPv4 or IPv6.
     c) Specify the **IP address**.
     d) Specify the **Netmask**.
     e) Optionally, specify the **Gateway**.
     f) Click **Submit**.
  4. To specify the management address in the Network Configuration panel, do one of the following:
     - Select the COG for a hostname, if your network is configured for DHCP, and choose **Set as Management address** from the drop-down list.
     - Select the COG for an interface, if your network is configured for a static IP address, and choose **Set as Management address** from the drop-down list.
The check mark in the Mgmt column changes to indicate that the selected interface is now the Management interface.

<table>
<thead>
<tr>
<th>Note:</th>
<th>Before changing a hostname or reconfiguring a network interface, check with your network administrator. The hostname must be resolvable.</th>
</tr>
</thead>
</table>

5. To add or modify custom DNS Servers, do the following:

<table>
<thead>
<tr>
<th>Warning!</th>
<th>The DHCP configuration can override any custom name servers. You can add up to three custom name servers.</th>
</tr>
</thead>
</table>

   a) Click the Pencil icon.
   b) Enter the name or IP address for up to three custom Nameservers.
   c) Click Save.

6. To modify the Search Domain, do the following:

   a) Click the Pencil icon.
   b) Enter a custom search domain.
   c) Click Save.

7. To edit Web Proxy settings do the following:

   a) Click the Pencil icon.
   b) Enter a web proxy URL.
   c) Click Save.

<table>
<thead>
<tr>
<th>Note:</th>
<th>Fusion support bundles can be uploaded using the proxy.</th>
</tr>
</thead>
</table>

### About NexentaFusion as an LDAP-Client

NexentaFusion can be used as an LDAP-Client to authenticate Fusion users, allowing users to login to Fusion with their LDAP user credentials.

Potential Fusion users should be placed into separate LDAP groups based on their Fusion UI user roles (administrator, user, or viewer). The LDAP configuration screen will then be used to associate the LDAP group with the user role. Delete any local users that are duplicates of the LDAP users, because local user names are checked first for authentication.

### Prerequisites

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

- Ensure that you are logged in to NexentaFusion as an Administrator to configure NexentaFusion with LDAP server.
• If you have a DNS server that is not part of the LDAP, make sure the DNS Server that is used by NexentaFusion has the proper DNS records to locate the LDAP server. This is required only if you are using FQDN and not required when using IP addresses.

**Configuring NexentaFusion for LDAP**

You must be logged in to NexentaFusion as Administrator to perform the following procedure. For an explanation of NexentaFusion user roles, see Table 3-2 *NexentaFusion User Roles*.

- To integrate NexentaFusion with a LDAP server, do the following:
  1. Log in to **NexentaFusion** as an Administrator, 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 **LDAP Authentication**.
  3. In the LDAP window, specify the following:

  **Warning!** Changing the following settings may invalidate active LDAP sessions.

**Basic Configuration**

Enter the following entries to complete the basic configuration.

- **LDAP Server**—Enter the URL of the LDAP server.
  - Specify just the host to connect with the defaults: ldap://host:389. Or specify the protocol or custom port as in this example: ldap://host:port or ldaps://host:port
- **Base DN**—Enter the base distinguished name
  - Specify the entry in the directory from which searches initiated by LDAP clients occur. (For example: dc=mydomain,dc=com)
- **Bind user type**—Select the type of credential you will use for LDAP binding. The bind process authenticates a client as authorized to query the LDAP directory.
  - Logon credentials for binding: select this if the logon user has the rights to search/read the LDAP directory.
  - Custom credentials for binding: select this if the logon user does not have LDAP query rights. If you choose this option, you will be prompted to provide a user and password to use for binding.
  - Anonymous binding: select this if the LDAP directory can be searched without authentication.
- **Bind user**—Bind username with LDAP access rights to read groups and users.
- **Bind user password**—Password for the bind user.
Advanced Options

Fields in the Advanced options display all the default values that are generally used for Active Directory.

- **Group base DN**—Enter the group base distinguished name. The base DN from which to search for groups. This is typically the same value as Base DN. The group search filter (default shown in advanced settings) will begin its search at the directory specified by the Group base DN. Specify a value only if the group base DN is different from the Base DN in your environment.

- **Search filter**—The LDAP search filter is used to find a user by username. The \{{username}\} wildcard is replaced by the username specified in the Fusion Logon screen, to authenticate the user.

- **Group DN property**—Provide the name of the property in the user object that identifies the user, whose value, the user distinguishedName, will replace the \{{userMapping}\} wildcard in the Group search filter.

- **Group search filter**—The Group search filter is used to find the groups to which the logon user belongs. The \{{userMapping}\} wildcard is replaced by the value of the property in the user object, that was configured in the Group DN property entry.

- **Group validate property**—Provide the name of the property in the group object that identifies the common name of the group, to validate the group is a Nexenta user group.

Test User Access

4. Once you entered the above settings, you can validate the settings by clicking on the **Test User Access** button. The username you provide for this test should be a member of one of the Fusion User Accessibility Groups that you have specified.

   This action will:
   - use the provided settings you entered to access the LDAP directory
   - search for the specified user in the LDAP directory
   - check if the user belongs to one of the LDAP user groups specified below

   If the test is successful, you will be presented the option to SAVE all the settings.

Fusion User Accessibility Groups

After authentication, the logon user name will be checked to see if it is a member of one of the specified LDAP groups, to determine the Fusion user type. You can specify more than 1 LDAP group in each category. Click "Enter" after typing the group ID to complete it, then click in the edit box again to enter another group ID.

- **Administrator group**—Enter the unique ID for each administrator group.

  This user group maps to the local NexentaFusion User Role “Administrator” and inherits the privileges assigned to the local NexentaFusion User Role “Administrator”.

- **User groups**—Enter the unique ID for each user group
This user group maps to the local NexentaFusion User Role “User” and inherits the privileges assigned to the local NexentaFusion User Role “User”.

- Viewer groups—Enter the unique ID for each viewer group.

This user group maps to the local NexentaFusion User Role “Viewer” and inherits the privileges assigned to the local NexentaFusion User Role “Viewer”.

See Table 3-2: NexentaFusion User Roles for more information on the available privileges for each group.

5. Once you entered the settings and validated them, click Save.

**Note:** For Active Directory, when adding a user to a Fusion User Accessibility Group, do not set the group as a Primary Group.

### Setting the Date and Time for NexentaFusion

If you installed NexentaFusion as an OVA or as an AWS AMI, you can edit the NTP server.

If you installed NexentaFusion as a Docker container, use the TZ parameter in the Docker run command to change the timezone. It cannot be changed using the Fusion UI. Refer to the NexentaFusion Installation guide for details. The Fusion Settings Date/Time view will display the current settings.

You can edit the NTP server, 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 change the server timezone and synchronize with the NTP server, do the following:**

  1. Log in to **NexentaFusion** as an Administrator, 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 **Server timezone**, click the pencil icon.

**Warning!** Changing the server timezone requires a reboot of the Fusion server.

4. In the Change timezone dialog, **Select server timezone** country and locale from the respective drop-down lists.
5. Enter your login name, and click **Save & Reboot**.
6. Click the **Time synchronization with NTP** check box.
7. Enter the URL for the NTP server of your choice.

8. Click **Save**.

- **To manually configure the date and time, do the following:**
  1. Log in to **NexentaFusion** as an Administrator, 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 **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.

![Date field with calendar](image)

**Note:** Time and Date can be changed only if the synchronization with NTP is not selected.

6. Click **Save**.

**Note:** The time difference between NexentaFusion and NexentaStor appliance may cause various issues while working with analytics in NexentaFusion. In case NexentaFusion notices the time desync with the particular appliance, it displays a modal window with the warning about that. To avoid such situations, it is recommended to use NTP service for both NexentaStor and NexentaFusion and use the same NTP server for both.

### Setting the NexentaFusion 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.

*Table 3-1* lists the parameters you configure for an SMTP server. Have this information ready before you begin to configure the SMTP parameters.
Table 3-1: 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>
</tbody>
</table>
| SMTP Protocol/port  | Secure Socket Layer (SSL) and Transport Layer Security (TSL) are standard security protocols that establish an encrypted link between a web server and a browser. Both cryptographic protocols provide security for communication over a network. The default port is set when the protocol is selected:  
  • SMTP port 25 for PLAIN SMTP  
  • SMTP port 587 for STARTTLS  
  • SMTP port 465 for SSL/TLS  
  You can change the port if needed for your environment. |
| SMTP Authentication method | Method of SMTP authentication used by your mail server:  
  NONE (default value)  
  PLAIN  
  LOGIN  
  CRAM-MD5 |
| SMTP User Name      | Login name for the SMTP server.                                                                |
| SMTP Password       | Password for the SMTP server 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. |
| Check SMTP Settings by sending test email to the address | An email address to which a test message is sent to verify the SMTP setting. |
| Local Administrator email | Email address of the Administrator, required for the recovery of lost passwords. |

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**.
4. Select the protocol.

The default protocol is **Plain SMTP** and the corresponding port is 25. Selecting a different protocol will change the port. The port can be edited, if needed, for your environment.

5. Choose an **Authentication method** (default is None) from the drop-down list as necessary, then specify a **Sender email address**.

6. Enter the **Username** and **Password**, in the respective fields if the authentication method has been changed to not be NONE.

7. Enter the **Recipients** email addresses. Click outside the field after entering a valid email address, then enter another valid address. Recipients will receive emailed alerts when the Enable e-mail notifications checkbox is checked in the rule used to generate the alert. See **Creating Rules for Logs and Events**.

8. To verify the SMTP settings, enter a valid email address in the **Check SMTP Settings by sending test email to the address** field and then click **Check**.
9. Enter a valid Local Administrator email address, and then click Save. This email address is required for the recovery of lost passwords.

Creating, Modifying, and Deleting Local UI User Accounts

Each NexentaFusion user role has specified access privileges that define the tasks a user is allowed to perform. NexentaFusion provides predefined user roles, as described in Table 3-2. This section covers the following topics:

- Creating a New NexentaFusion Local UI User Account
- Changing the Credentials and Role for a NexentaFusion Local UI User
- Deleting a Local NexentaFusion UI User Account

Note: NexentaFusion configuration tasks can only be performed by a “Administrator”. For more information, see NexentaFusion User Roles.

Table 3-2: NexentaFusion 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 the following:</td>
</tr>
<tr>
<td></td>
<td>- Registering an appliance</td>
</tr>
<tr>
<td></td>
<td>- Managing NexentaFusion settings</td>
</tr>
<tr>
<td></td>
<td>- Managing the services of an appliance</td>
</tr>
<tr>
<td></td>
<td>- Rebooting or shutting down an appliance from NexentaFusion</td>
</tr>
<tr>
<td>Administrator</td>
<td>An Administrator account has complete administrative privileges for NexentaFusion and appliance management. An Administrator 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>
Creating a New NexentaFusion 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, password and email address. When you configure LDAP users, you must delete any local users that may be duplicates of the LDAP users. For more information, see About NexentaFusion as an LDAP-Client.

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

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

Note: Passwords should be at least 9 characters long and contain at least 3 of the following classes of characters: lowercase, uppercase, numeric, and special (for example, !, @, #,$, %, ^). Passwords should not be based on English dictionary or slang words, nor English first names or surnames.
8. Click Save.

Changing the Credentials and Role for a NexentaFusion 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 (Administrator) 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 3-2.
To change the login credentials for a local user, do the following:

1. Log in to NexentaFusion as an Administrator 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. For an explanation of NexentaFusion user roles, see Table 3-2.

3. Enter a new Password, 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 this user’s Email address for notification. The Email address cannot be the same as any other local Fusion user’s address.

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 this user will be notified. For information on how to configure the SMTP server, see [Setting the NexentaFusion SMTP Mail Server (Email Setup)].

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

You can delete a local NexentaFusion UI user account at any time from the Local UI User Setup page. For an explanation of NexentaFusion user roles, see Table 3-2.

To change a user role or delete a local NexentaFusion UI User account, do the following:

1. Log in to NexentaFusion as an Administrator, 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.

Note: The default Admin user account cannot be deleted.

Configuring Audit, Log, and Monitor Settings

This section covers how to configure NexentaFusion settings to monitor the NexentaFusion server.

- Configuring NexentaFusion Audit Settings
- Configuring NexentaFusion Server Log Settings
- Configuring NexentaFusion Monitor Settings

Note: NexentaFusion configuration tasks can only be performed by a “Administrator”. For more information, see NexentaFusion User Roles.

Configuring NexentaFusion Audit Settings

This section demonstrates how to configure NexentaFusion audit settings, to collect and manage audit log entries for NexentaStor appliances.

To configure NexentaFusion audit settings, do the following:

1. Log in to NexentaFusion as an Administrator, click the Main COG at the top of the window, and select Settings from the drop-down list.
2. In the left panel, click Auditing.
3. To enable and disable auditing, click the Auditing enabled check box.
4. Select an interval to Store logs for from the drop-down list.
5. Click Save.
To manually delete audit logs and reclaim space, do the following:

1. Click inside the Delete logs older than field.
2. Use the arrows (< >) to navigate to the desired month.
3. Click a date to select it. The date appears in the text field, and the amount of space to recover appears on the Delete Logs button.
4. Click Delete Logs to manually delete these audit logs.

Configuring NexentaFusion Server Log Settings

This section demonstrates how to configure NexentaFusion log settings, to collect and manage log entries created by the NexentaFusion server. See Configuring Data Settings to configure settings for logs generated by the NexentaStor appliance.

To configure NexentaFusion log settings, do the following:

1. Log in to NexentaFusion as an Administrator, click the Main COG at the top of the window, and select Settings from the drop-down list.
2. In the left panel, click Logging.
3. Choose a Log severity level threshold from the drop-down list. Logs of the selected severity level and above will be retained.

4. Select an interval to Store logs for from the drop-down list.
5. Click Save.

To manually delete NexentaFusion server logs and reclaim space, do the following:

1. Click inside the Delete logs older than field.
2. Use the arrows (< >) to navigate to the desired month.
3. Click a date to select it. The date appears in the text field, and the amount of space to recover appears in the Delete Logs button.

4. Click Delete Logs to manually delete server logs.

**Configuring NexentaFusion Monitor Settings**

This section demonstrates how to configure NexentaFusion monitor settings, to manage alerts generated by NexentaFusion.

- To configure NexentaFusion monitor settings, do the following:

  1. Log in to NexentaFusion as an Administrator, click the Main COG at the top of the window, and select Settings from the drop-down list.
  2. In the left panel, click Monitoring.
  3. Specify a Status check interval (in seconds).
     This interval specifies how often (in seconds) the appliance status should be checked. The minimum is five seconds.
  4. Specify a Health check interval (in minutes).
     This interval specifies how often (in minutes) the appliance health should be checked. The minimum is three minutes.
  5. Specify a Free space threshold (in gigabytes).
     The Free space threshold specifies the lowest amount of free space from which to start sending alerts about low storage space.

   ![Appliance monitoring](image)

   - Status check interval (in seconds)
     - 15
   - Health check interval (in minutes)
     - 3
   - Fusion database monitoring
   - Free space threshold (GiB)
     - 5

  6. Click Save.

- To manually delete alerts and health data, do the following:

  1. Click inside the Delete alerts older than field.
  2. Use the arrows (< >) to navigate to the desired month.
3. Click a date to select it. The date appears in the text field, and the amount of space to recover appears in the **Delete Alerts** button.

4. Click **Delete Alerts** to manually delete the alerts.

## Configuring Session Settings

You can configure the inactivity time for NexentaFusion user sessions, between 1 to 60 minutes, after which the user of type “User” or “Administrator” will be required to log in again. The default inactivity time is 30 minutes.

Note: Users of type "Viewer" are read-only and are not bound by the inactivity time, so they can be used to display a dashboard or other analytics in a NOC environment.

- To configure the inactivity time for user sessions, do the following:
  1. Log in to **NexentaFusion** as an Administrator, 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 **System Settings**.
  3. In the **Session inactivity time** field, enter a value between 1 and 60 (minutes).

    | Fusion system settings |
    |------------------------|
    | Session inactivity time | 60 (1-60) minutes |

4. Click **Save**.

The system will require a user to log in again whenever their session is inactive longer than the specified time. The revised inactivity time will take effect after the next login.
Setting IRS Warning Message on Fusion Logon Screen

By default, the Fusion logon screen does not display any messages, however, you can choose to display the IRS Publication 1075 warning banner at initial logon on computers housing federal tax information or display any customized messages by following the steps listed here.

To display the IRS warning message:

1. Log in to NexentaFusion as an Administrator, 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 System Settings.
3. In the Fusion system settings window, toggle the Show warning on logon screen button to YES. This action displays the IRS 1075 warning banner on the logon screen.

Setting Customized Message

4. Use the edit pencil to customize the message and click Save.

Managing NexentaFusion SSL Certificates

NexentaFusion uses a default HTTPS certificate. You can update the SSL certificate if your company security policy requires the use of a specific SSL certificate. You can also add CA certificates based on your requirements.

Note: Currently, NexentaFusion accepts SSL certificates that are RSA encrypted.

Viewing the Installed SSL Certificate

1. Log in to NexentaFusion as an Administrator, 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 **SSL**.
3. Click **Certificate**. This displays the certificate currently installed on the NexentaFusion server.

### Installing a Custom SSL Certificate

4. To install a custom SSL certificate, click **Set New Private and Public Keys**.
5. In the update SSL configuration window, copy and paste the contents of private and public keys.
6. Alternatively import from files.

**Note:** The Fusion server health icon will display a warning when the certificate is within 2 weeks of expiring. See [Fusion Server health](#) for information on viewing the warning.
Installing a CA Certificate(s)

1. To install a CA certificate, log in to NexentaFusion as an Administrator, 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 SSL.

3. Select the CA tab.

   If there is currently a CA(s) installed in the fusion server, clicking the CA tab displays the CA Certificate(s).

4. To view the details of a specific CA, click on the expand button.

   You can delete a CA from this view by clicking on the Delete icon found on the bottom of the CA certificate. By deleting a CA, authorization to some appliances might get denied (example shown below).
5. To add a new CA certificate, click on Add CA Certificates + button.
6. In the Update CA Certificates window, copy and paste the contents of private and public keys.
7. Alternatively import from files.
8. Click Next.

9. Review the Certificate Authority data displayed.

10. Click Add.

11. Enter your password to continue.

This successfully updates the certificate authority.

---

**Note:** The Fusion server health icon will display a warning when the CA is within 30 days of expiring. See Fusion Server health for information on viewing the warning.

---

**Reverting to the Default Self-signed Certificate**

The Fusion UI cannot be accessed if there is any issue with the custom-installed certificate. The following steps let you revert to the default self-signed certificate, so you can use the Fusion UI to install a new certificate.
Using the Console Wizard

1. If installed as an OVA, navigate to the Fusion Server VM’s console with your vSphere Client.
2. If installed as an AWS AMI, ssh to the NexentaFusion console. On the EC2 console, select the NexentaFusion instance, and click Connect for instructions on how to use your access key file to connect. Use the username “fusion” to connect.

   On the console, type fusion-wizard. The Fusion Console Wizard will be displayed.


   ![Configuration Wizard Image]

4. If requested, provide the “admin” user password.
5. Select Create self-signed HTTPS certificate.
6. Select OK.

Using Docker

1. At the Docker command line, enter “fusion-reset-ssl”.
   Enter “y” when asked if you want to continue.

Managing Fusion Support Bundles

A NexentaFusion Server support bundle is a compressed collection of server log files, database logs files, and other system configuration information that can be uploaded to the Nexenta Support server for troubleshooting NexentaFusion problems. The NexentaFusion UI provides an interface for creating, uploading, and managing support bundles.

If the NexentaFusion UI is not operational, a support bundle can also be created and uploaded using Docker or the OVA’s Console Wizard.
Registering the NexentaFusion GUID

To receive technical support for NexentaFusion, you must register the server GUID at the Nexenta support portal.

1. Log in to NexentaFusion as an Administrator, click the Main COG at the top of the window.
2. Select Support from the drop-down list.
3. Copy the hardware GUID displayed for the Fusion server.
4. Login to the Nexenta Support portal, https://portal.nexenta.com, with your account
5. Register the NexentaFusion instance using the copied machine GUID.

This registering feature is available beginning with the NexentaFusion 1.1.0 release.

Modifying Default Support Bundle Protocol and Settings

By default, support bundles are uploaded via S3 protocol to Nexenta servers. By default, S3 uploads use parallel upload for maximum throughput performance, and faster uploads.

❖ To change the default support bundle protocol:
1. Log in to NexentaFusion as an Administrator, click the Main COG at the top of the window.
2. Select Support from the drop-down list.
3. Click on the COG near the FUSION SUPPORT BUNDLES.
4. In the Set bundle upload method window, you will notice that the default upload method is set to “Parallel” upload for fast connections. However, you may change the default upload method to “Sequential S3” upload, If you are experiencing upload failures or have a slow network connection to Nexenta support servers.
5. Or you can upload support bundles to Nexenta's https server. This operation may take a long time depending on the size of the bundle and your internet connection speed.
Sending Periodical NexentaFusion Server Support Bundle

6. To periodically create and automatically send bundles to the Nexenta Support server ensure that the Call Home toggle button is ON.

Using the NexentaFusion UI to Create and Upload Support Bundles

1. Log in to NexentaFusion as an Administrator or User, click the Main COG at the top of the window.
2. Select Support from the drop-down list.
3. Click the Create Support Bundle button.
4. Optionally enter a description for support bundle.
5. Click OK to create the bundle. This may take a few minutes.

6. After the bundle is created, it will be displayed in the table.

7. Click on the COG of the bundle you created.
8. Select **Upload to support server** in the drop down list, to upload the bundle to the Nexenta Support server.

9. Alternatively, you may download the bundle to your local machine and upload it to the Nexenta support team later.

10. To remove the bundle you created, click **Remove bundle**.

**Using the Console Wizard to Create and Upload Support Bundles**

1. If installed as an OVA, navigate to the Fusion Server VM’s console with your vSphere Client.

2. If installed as an AWS AMI, ssh to the NexentaFusion console. On the EC2 console, select the NexentaFusion instance, and click Connect for instructions on how to use your access key file to connect. Use the username “fusion” to connect.

3. On the console, type fusion-wizard. The Fusion Console Wizard will be displayed.

4. Select **Collect Support Bundle**

5. If requested, provide the “admin” user password.

6. Select **Yes** to upload this bundle to the Nexenta Support server after the bundle has been created.

7. Optionally enter a description for the bundle and click **OK**.
8. After the files have been collected into the support bundle, it will be uploaded. Bundles created using the Console Wizard will be visible in the Fusion UI on the Support screen for later removal.

**Using Docker to Create and Upload Support Bundles**

You can use the “bundle” command at the Docker command line to create and upload a support bundle. You must be root to run this tool.

```
$ docker exec <container-name> bundle <args>
```

**usage:** bundle [-q|-v|-d] [-u] [-c path] [-t "description"] [-n name]

**options:**
- `-q` - quiet mode, all warning and diagnostic messages will be suppressed
- `-v` - verbose mode, print all messages to stdout
- `-d` - dialog mode, display messages using dialog boxes

**default mode:** quiet
- `-u` - upload the bundle to the Nexenta Support server
- `-c path` - bundle destination directory, default: `/var/lib/nef/bundles`
- `-t text` - bundle description text, default: ""
- `-n name` - bundle name, default: random UUID

**Bundle Examples**

```
bundle -u  --- Create bundle and upload it to the Nexenta Support server
bundle -t "My bundle" -u  --- Create bundle with description and upload
```

**Note:** Changing the support bundle name may impact uploading the bundle to the Nexenta Support server. Bundles created using the Docker command line will be visible in the Fusion UI on the Support screen for later removal only if they were created in the default destination directory.
Fusion Server health

The FusionServer health worker monitors various conditions that are critical to the proper functioning of the NexentaFusion application. Detection of a specific error condition will cause the FusionServer Health icon to appear on the Main menu bar. A bell indicates a Fusion software update is available. A yellow triangle indicates warning alerts, a red octagon indicates a serious failure condition. Click on the icon to display the health alerts.

The FusionServer health worker will monitor:

- Availability of Fusion software updates
- Database connection and health
- Fusion server CPU usage
- Database storage capacity usage
- Network management address configuration
- Critical Fusion workers health
- Socket.io connection
- OS filesystem writable status
- SSL Certificate expiration within two weeks and CA expiration within 30 days

See Managing NexentaFusion SSL Certificates to upload a new certificate.

Most of these conditions will require contacting support and creating a support bundle. See Managing Fusion Support Bundles.

See Checking and Modifying NexentaFusion Network Settings to resolve network management address configuration issues.

See Configuring Audit, Log, and Monitor Settings to delete data if database capacity is getting low, or contact support to increase database storage capacity.
Elasticsearch Database

NexentaFusion uses the Elasticsearch database to persist metrics for analytics, logs, and alerts. The Elasticsearch database service is placed on the same machine as NexentaFusion and uses port 9200, when NexentaFusion is installed.

Fusion Services Management

A specific error condition may require you to restart “Elasticsearch service” or “NexentaFusion service” or even reboot “NexentaFusion server”.

If you installed NexentaFusion as a Docker container, use Docker commands to restart the container and its services. The Fusion Services Management option is not available.

If you installed NexentaFusion as an OVA, the section below describes how to restart the services or reboot the Fusion server.

**Note:** You must have Administrator privileges to perform this procedure.

1. To reboot “Elasticsearch service” or “NexentaFusion service” or “NexentaFusion server”, do the following:
   1. Log in to NexentaFusion as an Administrator.
   2. Click the Main COG at the top of the window.
   3. Select System Services from the drop-down list.
   4. To restart “Elasticsearch service”, in the System Services window, click on the cog of Elasticsearch service and click Restart.
   5. To restart “NexentaFusion service”, click on the cog of NexentaFusion service and click Restart.
   6. To reboot NexentaFusion server, in the Server Management window, click Reboot NexentaFusion Server button.
What Comes Next?

In the following chapter you learn how to establish the connection between the NexentaFusion and NexentaStor appliances. In the chapter "Deploying NexentaCloud" appliances you learn how to deploy a NexentaCloud in AWS appliance and connect to it using NexentaFusion.
Registering NexentaStor Appliances

This section includes the following topics:

- How to Register a NexentaStor Appliance
- Confirming Registration
- Identifying NexentaFusion GUI from NexentaStor
- Rebinding an Appliance
- Viewing an Appliance Summary
- Viewing Appliance Licenses
- Updating the License
- Removing an Appliance
- What Comes Next?

How to Register a NexentaStor Appliance

Before NexentaFusion can manage NexentaStor storage appliances, the appliances must be registered in NexentaFusion. To register an appliance, it needs to be licensed and the license should be valid. 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.

| Note: | Clustered appliances must be licensed and configured using the CLI before they can be registered with NexentaFusion. 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 an Administrator 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.
Connection to Appliance

Please enter appliance login credentials for:

Enter username: [blank]
Enter password: [blank]

Do you trust the following certificate:

**Serial Number**: A4DB36F8714D80C5

**Fingerprints**

**Subject**
- Common name (CN): nef-cert
- Organization (O): nef
- Country (C): US

**Extensions**
- Basic constraints: CA:TRUE

**Issued By**
- Common name (CN): nef-cert
- Organization (O): nef
- Country (C): US

**Validity Period**
- Issued On: 2017/12/19 09:56:25 -0800
- Expires On: 2019/12/09 09:56:35 -0800

[ ] I trust this certificate

Download certificate
5. For a clustered appliance, after the first node successfully authenticates, a second dialog appears with the pre-filled credentials used 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.

   ![Communication Settings](image)

   7. Configure the SMTP server if it was not already configured on the appliance.

   8. Click **Confirm**.

   Once you have registered the NexentaStor appliance and all the credentials are authenticated, the appliance displays under the Appliances List drop-down list and in the 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.

  3. To start managing an appliance, click on the appliance name or on the appliance icon from the appliance list.
Identifying NexentaFusion GUI from NexentaStor

To identify the NexentaFusion GUI on which a NexentaStor appliance is registered:

1. Note the IP address of the appliance.
2. Point your browser to the NexentaStor appliance URL with no port number, for e.g., <IP address of the NexentaStor appliance>.
   This page provides you the link to access the NexentaFusion interface as well as the link to access the REST API doc for the appliance.

NexentaStor Node Name: 

To access the NexentaFusion Management Interface click the link below:
https://<IP address>:8457/

To access NexentaStor REST API Documentation click the link below:
https://<IP address>:8443/docs
Rebinding an Appliance

If you reinstalled an appliance, after you registered it using NexentaFusion, you must rebind it in order to manage the reinstalled appliance.

To rebind the reinstalled appliance, 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 **Rebind appliance** from the drop-down list.

Viewing an 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.
- **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.
Registering NexentaStor Appliances

Table 4-1: Set of Attributes in a License File

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issued, Expires</td>
<td>Refers to the period of time in which a license remains valid. When the license expires you will be blocked from performing any configuration changes to the NexentaStor Appliances.</td>
</tr>
<tr>
<td>Licensed Capacity</td>
<td>This is the maximum capacity limit for your license. When you reach the limit, you are unable to create or import new pools, or add devices to existing pools. However, IO will continue.</td>
</tr>
<tr>
<td>Subscription ends</td>
<td>Refers to the time period over which you are entitled to software upgrades and hot fixes from Nexenta.</td>
</tr>
<tr>
<td>Licensed Features</td>
<td>Lists the NexentaStor appliance features that you are licensed to use.</td>
</tr>
</tbody>
</table>

Note: When the license is no longer valid for a NexentaStor appliance (time expired or capacity limit exceeded), you will be unable to access any views to manage the appliance from the UI. Appliance I/O continues, and you will be able to use the CLI to get information about the appliance.

See Updating the License for information on how to renew the license.

Updating the License

When the license is no longer valid for a NexentaStor appliance (time expired or capacity limit exceeded) you can update the NexentaStor appliance license using the NexentaFusion UI. To update the NexentaStor license using NexentaFusion, use the activation key you received from Nexenta Systems.

<table>
<thead>
<tr>
<th>Issued to</th>
<th>Nexenta</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Name</td>
<td>NexentaStor Ver 5.0.0</td>
</tr>
<tr>
<td>License Type</td>
<td>Enterprise Trial</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>31-Oct-2016</td>
</tr>
<tr>
<td>Storage Capacity</td>
<td>NA</td>
</tr>
<tr>
<td>Activation Token*</td>
<td>4DEF7BF3-CF8E-41E6-B18A-0704E7105142</td>
</tr>
<tr>
<td>ECCN**</td>
<td>5D992</td>
</tr>
</tbody>
</table>

To update 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.
4. Click the **Update** button to update the license.

5. In the License Activation window, enter the activation token you received from Nexenta and click **OK**.

---

**Note:** To update a clustered appliance, you must update the license on both nodes of the cluster sequentially.

---

### Removing an Appliance

You can remove a registered NexentaStor single or clustered node by doing the following:

1. Log in to NexentaFusion as an Administrator and select **Appliance** from the drop-down list.
2. In the **Appliances List** page, click on the COG next to the appliance you want to remove.
3. Click **Remove** from the action items listed under the COG.
4. If you wish to retain all the data such as analytics or logs in the NexentaFusion database uncheck the check box.

5. **Now click the Remove button.**

   If you removed the appliance but retained the data in the NexentaFusion database, the appliance will be still listed in the appliance list page with the status “removed”.

   This option is provided so that you can view the historical analytics of a decommissioned appliance anytime. See [Viewing the Historical Analytics of a Removed Appliance](#) for more information on viewing the historical analytics.
Viewing the Historical Analytics of a Removed Appliance

When removing the appliance, if you retained all the data such as analytics or logs in the NexentaFusion database, you can view the historical analytics of that decommissioned NexentaStor appliance by clicking on the appliance. A decommissioned appliance will be listed with a Removed status.

To view the historical analytics of a removed appliance:

1. Log in to NexentaFusion as an Administrator and select **Appliance** from the drop-down list.
2. In the **Appliances List** page, click on the appliance that you want to review the historical analytics.
3. This opens the Analytics view. See **Chapter 11, Performance Monitoring and Analytics** for more information on analytics.
What Comes Next?

After successfully registering an appliance, you can view the appliance hardware information, such as CPUs, memory, network adapters, disks, enclosures, and host bus adapters on the Components view as described in Chapter 5, Managing NexentaStor Appliances to start managing the appliance.
Managing NexentaStor Appliances

This section includes the following topics:

- Viewing Server, Enclosure, and Disk Information
- Managing Network Configurations
- What Comes Next?

Viewing Server, Enclosure, and Disk Information

After registering a NexentaStor appliance, you can view the appliance hardware information, such as CPU, memory, network adapters, disks, enclosures, and host bus adapters on the Components view. NexentaFusion provides a graphical or tabular view of the enclosures and disks connected to the appliance for easy management. The ability to view sensor values, blink bay indicators, and view disk details is also accessed on the Components views.

This section covers the following topics:

- Viewing an Appliance Profile and Version
- Viewing Server Components
- Viewing Chassis Enclosures and Devices
- Viewing Chassis Sensor Values
- Locating Chassis using Blink Feature
- Viewing and Locating Chassis Devices

Viewing an 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.x 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.x CLI Configuration 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 click Appliance if not already in the Appliance view.
  2. In the Appliances List, click an appliance and select Management.
3. Click **Components**. If the appliance is clustered, select the node you want to view.

### Viewing Server Components

The Components page displays information about the NexentaStor appliance server as well as enclosures and devices.

- **To view the server components 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**. If the appliance is clustered, select the node you want to view.

4. Under **Server**, click the triangle on the left to expand the view of that component.
5. Click the COG on the far right, and select Display server sensors information. The sensors and their values will be displayed in a tabular form, if available, as in the sample below.

<table>
<thead>
<tr>
<th>Id</th>
<th>Name</th>
<th>Value</th>
<th>Units</th>
<th>Type</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROCESSOR-1-1</td>
<td>CPU1 Temp</td>
<td>29</td>
<td>Degrees-C</td>
<td>temperature</td>
<td>OK</td>
</tr>
<tr>
<td>PROCESSOR-2-2</td>
<td>CPU2 Temp</td>
<td>38</td>
<td>Degrees-C</td>
<td>temperature</td>
<td>OK</td>
</tr>
<tr>
<td>MOTHERBOARD-1-17</td>
<td>System Temp</td>
<td>24</td>
<td>Degrees-C</td>
<td>temperature</td>
<td>OK</td>
</tr>
</tbody>
</table>

6. Click the COG on the far right, and select Rescan inventory to rescan all the devices attached to the node. It can take several minutes to retrieve the new details. Click the Refresh button to retrieve the available updates.

Select the “Cleanup” option when many changes have been made to the device configuration. This will increase the time to complete the rescan.

**Viewing Chassis Enclosures and Devices**

A JBOD chassis may display as having a single enclosure or multiple enclosures. The graphical view of the chassis shows devices in a view that is a representation of the physical layout. The tabular view arranges the devices in a table, and makes it easy to see which active pool is using a device. Filtering by specific enclosures or disk models can simplify the views.

COG actions provide the ability to view enclosure images, change enclosure labels, and view sensors. Depending on the chassis vendor, these capabilities may be available on the enclosure COG or the chassis COG.

Devices that are part of the server enclosure are displayed after the chassis in a section titled “Internal or attached media”.

- To view chassis enclosures and devices, 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**. If the appliance is clustered, select the node you want to view.
  4. To view chassis devices in graphical or tabular mode, select the appropriate icon.

  ![Graphical View](image1) ![Tabular View](image2)

  5. To filter, make selections from the drop-down lists. To clear the filter, click the “x” from the drop-down lists.
In the tabular view only the devices that meet the filtered-condition will be displayed whereas in the graphical view the devices that meet the condition will be displayed in solid colors and those devices that do not meet the filtered-condition will be displayed in muted color.

6. To change the enclosure label, select Edit enclosure label from the COG or double-click on the existing label, and enter the new label in the text field that appears.

7. Select Display enclosure image (for certain chassis models) to see the physical layout.

8. To view the connection details of a JBOD, click View connection Details.

Viewing Chassis Sensor Values

Some JBODs use the IPMI protocol to retrieve sensor data. The chassis or enclosure COG will display the menu item Set IPMI Credential to allow entry of the IP address, user name and password for the chassis. JBODs that retrieve sensors using SES do not require credentials.

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**. If the appliance is clustered, select the node you want to view.

*To configure the chassis for IPMI LAN protocol access*

1. Click the COG on the right side of the chassis, select **Set IPMI Credential**.

2. In the IPMI credentials window, enter the IP address or hostname of the chassis, username, and password.

3. Click **Save**.

*To view the sensors of a chassis or enclosure:*

1. Under Management > Components, click the COG on the right side of the chassis,

2. Select Display enclosure sensors information.
3. The sensors will be displayed in a tabular form, as in the sample below. Refer to the vendor-specific JBOD technical documentation for details on a particular sensor.

<table>
<thead>
<tr>
<th>Id</th>
<th>Name</th>
<th>Value</th>
<th>Units</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SES_CHASSIS-0-32</td>
<td>Temperature</td>
<td>37</td>
<td>Degrees-C</td>
<td>temperature</td>
<td>OK</td>
</tr>
<tr>
<td>SES_CHASSIS-0-34</td>
<td>Fan1</td>
<td>8400</td>
<td>RPM</td>
<td>cooling</td>
<td>OK</td>
</tr>
<tr>
<td>SES_CHASSIS-0-35</td>
<td>Fan2</td>
<td>8220</td>
<td>RPM</td>
<td>cooling</td>
<td>OK</td>
</tr>
</tbody>
</table>

4. If the chassis requires IPMI credentials, and they were not configured prior to selecting Display enclosure sensors information, you will be prompted to configure the credentials as shown below.

**Locating Chassis using Blink Feature**

1. Under **Management > Components**, locate the chassis.
2. To physically locate the chassis using the blink feature, click **Show Indicators**, and then click the **Chassis Ident**.
The Blink feature sets the ident indicator on the Chassis to flash, allowing you to easily locate the chassis in a storage rack.

- Enabling the blink of the led for a slot/drive will enable the blinking of the chassis led.
- Clicking the blink icon for a bay to turn off the ident indicator will not turn off the chassis ident indicator.
- When Show Indicators is clicked, some chassis may not be able to return the current actual physical state of the led, and display it as “off”. Clicking the icon will turn it on, even if it is already physically “on”.

3. To turn off the chassis ident led, if the icon is not displaying it as blinking, click to turn it on, then click again to turn it off.

**Viewing and Locating Chassis Devices**

1. Under Management > Components, locate the desired enclosure.
2. To locate a device using the blink feature, click Show Indicators, and then click the indicator.

The Blink feature sets the ident indicator on the bay to flash, allowing you to easily locate the disk in a storage rack.

Enabling the blink for a bay will also enable the blinking of the chassis led.

If the ident indicator on the bay was previously set to flash, clicking Show Indicators will display the current state of the ident led with the blinking icon for that bay. The chassis ident icon may not be able to display the current state of the ident led. Clicking the chassis ident icon will turn it on, even if it is already physically “on”. Click it again to turn it off.

Clicking the blink icon for a bay to turn off the ident indicator will not turn off the chassis ident indicator.

3. Use the filters to locate devices with particular characteristic. Make selections from the drop-down lists. To clear the filter, click the “x” from the dropdown lists.

Select the tabular view to display only the devices that meet the filtered condition.
In the graphical view, the devices that meet the condition will be displayed in solid colors and those devices that do not meet the filtered condition will be displayed in muted colors.

- Select enclosures – select the enclosures to be displayed. You can make multiple selections. Unselected enclosures will be collapsed.
- Select disk – select the disks of that type to be displayed.
- Select pools – select the pools to display the data devices used in the pool.
- Select attributes – select the type of disks to be displayed from “Unused”, “Encrypted”, and “Faulty” choices.

4. Error icons on a device indicate that FMA (Fault Management) has detected an issue and created an appliance alert case. Click on the error icon to view the details of the alert case. A click on the case ID will navigate the user to the Alert Cases view, with the filter set to that case ID. There, the admin can click on the COG to show additional info.
5. To view the details for a disk, such as model, serial number, and RPM, hover the cursor over the disk label under Chassis.

In the Internal or attached media section, a device may be displayed as an outline and labelled as “RMV”. These are removable devices that cannot be used for pools.

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 IP Address
Verifying and Modifying IP Links

During NexentaStor 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 5-1: 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. 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, MTU, 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 **Add Address** to add a network address, as described in *Adding an IP Address*.
   - Select **Add to...** to add this Link to an existing Aggregate or IPMP group.
   - Select **Assign VLAN** to add a VLAN, as described in *Adding a VLAN*.
   - 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.
   - Optionally, select **Remove <linkname>** to remove a link from an Aggregate.

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

**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**.

7. In the **Add Network Address** dialog, do the following:
   a) Enter a **Name**.
   b) Select an address **Type** from the drop-down list. The remaining fields change depending on the Type of link selected. The information required varies with the type of address.
   c) Specify the information for the remaining fields, and click **Add Address**.

### 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.x 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. Do one of the following:
• Click the COG for a link and choose Assign VLAN from the drop-down list.
• 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 4094

![Assign VLAN Dialog](image)

6. Click Assign, and the VLAN automatically appears in the table.

Adding an IP 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.

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. Do one of the following:
• Click the COG for the link or for the IPMP group and select Add Address from the drop-down menu.
• Click the check box to the left of the Link name, and then click Add Address at the bottom of the window.

5. In the Add Network Address dialog, do the following:
   d) Enter a Name.
   e) Select an address Type from the drop-down list. The information required varies with the type of address being added. The remaining fields change depending on the Type of link selected.
   f) Specify the information for the remaining fields, and click Add Address.

The following example is for a static (IPv4) address.

![Add Network Address dialog](image)

**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 Pool with Shared Devices.

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
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 and Managing an IPMP Group

IP network multipathing (IPMP) provides fault tolerance and load balancing for network interface cards (NICs). This section demonstrates how to create an IPMP group of two or more interfaces for the selected appliance, and then how to delete an IPMP group.

- **To create an IPMP group, 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. In the left column, click two or more check boxes of the links to be included in the IPMP group.

5. Click **Create IPMP Group**.

6. Enter an **IPMP Group Name** in the Create IPMP Group dialog, and click **Create**.

7. In the **Add Network Address** dialog, specify the following:
   - Enter a **Name** that is an alphanumeric string that begins with an alphabet letter and is 32 characters or less.
   - Select a network **Type** from the drop-down list. Static (IPv4) is the default.
   - Enter a valid **IP address**.
   - Enter a Netmask.

8. Click **Add Address**.
   The group appears in the IPMP Group table below.
   
   To add a member to an existing IPMP group, do the following:
   1. In the Links table, click the COG of the link to be added as a member, and select Add to... from the dropdown.
   2. In the resulting dialog, select the IPMP group from the dropdown, and click ADD.
   3. The IPMP Groups table will be updated to display the new member.

   To remove a member from an IPMP group, do the following:
   1. Expand the IPMP group in the IPMP Groups table so the members are visible.
   2. Click the COG on the member to be removed, and select Remove from Group

   To delete an IPMP group, 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**.
   4. In the IPMP Groups table, click the expand arrow to the left of the IPMP Group name.
   5. Click the **COG** of each group member, select **Remove from group** from the drop-down list, and click **Yes** in the confirmation dialog.
      The IPMP must be empty before it can be deleted.
   6. Click the **COG** for the IPMP group, choose **Destroy** from the drop-down list, and click **Yes** in the confirmation dialog to destroy the selected IPMP group.
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.

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. See your network administrator for the appropriate address for your site.
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.

### Routes node-10-170

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3.10.0</td>
<td>10.3.10.122</td>
<td>ipv4</td>
</tr>
<tr>
<td>10.3.10.0</td>
<td>10.3.10.170</td>
<td>ipv4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Route Flags</th>
<th>Gateway</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>indirect</td>
<td>3.10.1</td>
<td>ipv4</td>
</tr>
<tr>
<td>offlink</td>
<td>0:004:0b00f:feef:83b4</td>
<td>ipv6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hostmask</th>
<th>Gateway</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>3.10.175</td>
<td>ipv4</td>
</tr>
<tr>
<td></td>
<td>3.10.1</td>
<td>ipv4</td>
</tr>
<tr>
<td></td>
<td>0:004:0b00f:feef:334c</td>
<td>ipv6</td>
</tr>
</tbody>
</table>

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 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. For more information, see the *NexentaStor 5.x CLI Reference Guide*.

---

**What Comes Next?**

The following chapter covers details to deploy NexentaCloud appliances in AWS using the NexentaFusion management console.
Deploying and Managing NexentaCloud Appliances

This section includes the following topics:

- Introducing NexentaCloud
- About this Chapter
- Deploying NexentaCloud in AWS
- Managing NexentaCloud Appliances
- Viewing NexentaCloud Components
- Additional Resources
- What Comes Next?

Introducing NexentaCloud

NexentaCloud

NexentaCloud for AWS delivers unified file (NFS and SMB) and block (iSCSI) storage services and includes all data management functionality. In combination with NexentaFusion, customers can deploy, run, and scale better than ever before. From getting set up, to daily tasks and checking the health of your storage environment, IT administrators are able to easily manage the needs of their business. Standard day to day tasks including deploying pools and creating a file system are now easy to configure in a matter of minutes.

About this Chapter

This chapter is for storage administrators who would like to deploy and manage NexentaCloud for AWS using the NexentaFusion management console. The NexentaCloud storage appliance will run as an AMI instance in your selected region.

Deploying NexentaCloud in AWS

The following sections will walk you through the configuration and deployment of a NexentaCloud instance in AWS using the NexentaFusion management console.
Preparing the AWS Environment

The following steps must be completed to successfully deploy a NexentaCloud appliance instance using NexentaFusion.

- In the AWS Marketplace, subscribe to NexentaCloud. Review the regions where NexentaCloud will be available and the pricing.
- Using the AWS Services Console VPC feature, configure your Amazon Virtual Private Cloud (VPC) and subnets for the desired region. The recommendation is to configure a private subnet, where you will deploy the NexentaCloud instance, and a public subnet with a NAT Gateway.

Configure your routing tables so NexentaFusion can access the private subnet for appliance management.

Additional interfaces can be added to your NexentaCloud instance for NAS, iSCSI, or replication traffic. Configure additional subnets in the same availability zone for each interface you intend to add.

Configure your routing tables to allow the NexentaCloud appliance to access the internet through the NAT gateway. NexentaCloud accesses the internet to upload support bundles and perform software upgrades.

- Using the AWS Services Console IAM feature, create an access key for your account and download it. The access key must be imported into Fusion, to allow Fusion to execute AWS API’s. See Setting the AWS Access Key.

- The Fusion wizard for deploying a NexentaCloud appliance will give you the option for creating a default security group enumerating the ports used by NexentaCloud, and/or assigning previously configured security groups, for the selected VPC. A security group acts as a virtual firewall that controls traffic to the associated instance. A security group can be modified using the AWS Services Console.

- Review the AWS EC2 Service dashboard EBS limits for your account in your planned region. If you are already utilizing EBS storage in this region, or are expecting to configure a NexentaCloud instance with a lot of EBS storage, you may need to increase your limits prior to deploying a new instance.

- Encrypting a NexentaCloud storage can be done only when deploying the instance, not at later point. To use encrypted storage with a NexentaCloud instance, create a Master key for your account in the AWS service console and download it. The Fusion wizard for deploying a NexentaCloud appliance will give you the option to enable the “storage data encryption” option and to select the Master key you created. When these options are selected, all volumes created at deployment will be encrypted, and any future volumes will also be encrypted. However, the devices in an existing NexentaCloud instance cannot be encrypted or unencrypted at later instance.

NexentaFusion does not support an environment with a mix of encrypted and unencrypted volumes.

Setting the AWS Access Key

NexentaFusion requires an AWS Access Key to sign programmatic requests to AWS to execute AWS API’s, AWS SDKs, REST, or Query API operations. Once you import the access key, Fusion uses the key to sign programmatic requests to AWS.

To set the AWS service access key:

1. Log into NexentaFusion as admin.
2. Click on the main cog and navigate to Settings > Public Cloud.
3. Click on the **Update Access Key** button.

4. Click on the **Import from File** button and navigate to the .csv file containing your access key. The AWS access key ID and secret access key fields will be populated.

   Or

5. Copy and paste your AWS access key ID and secret access key into the fields.

6. Click on the check box next to: "NexentaFusion is authorized to manage capacity requirements for you by purchasing new EBS based volumes as needed to meet operational demands"

7. Click **Save**.

   **To clear the AWS service access key:**

   Clearing the access key will not affect the operation of the NexentaCloud appliance. But, if no valid access key is available to Fusion, you will not be able to use Fusion to upgrade the NexentaCloud license, add capacity, destroy the NexentaCloud instance when it is no longer needed, or deploy a new NexentaCloud instance.

   1. To clear the current access key, navigate back to the main Cog and Settings > Public Cloud.
   2. Click on the **Clear Access Key** button.
   3. Click on the **Yes** button on the confirmation dialog.

### Configuring and Deploying a NexentaCloud Appliance

Ensure that you have completed the steps in Preparing the AWS Environment.

| Note: | You can only configure a single node NexentaCloud appliance in AWS. |

   **Begin to configure and deploy NexentaCloud:**

   1. Log in to NexentaFusion, and click **Appliance** if not already in the Appliance view.
   2. In the **Appliances List** page, click on the **Deploy NexentaCloud Appliance** button. This will launch a wizard to configure and deploy a NexentaCloud appliance.
   3. After reviewing the information on the wizard introduction screen, click **Continue** button.

   | Note: | If the AWS service access key was not setup, the Continue button will be disabled. Click the provided link to navigate to the screen to set the AWS service access key. |

   **Provide the name, region, network settings, and other properties for the NexentaCloud instance:**

   1. Provide the **Appliance name** to be displayed in the NexentaFusion Appliance List view after the instance is launched.
   2. Specify the Appliance password to be used with the user name “admin” to access the NexentaCloud appliance CLI. If you select Use instance ID, the assigned instance id can be viewed on the NexentaCloud Properties view after the deploy completes.
   3. Select the region and city for the desired NexentaCloud **Appliance timezone** or match the browser timezone by clicking on the **Match Browser Timezone** button.
4. The NTP server URL field is pre-populated with the NTP servers used by the NexentaFusion server. Click the “x” to remove an undesired URL. Click in the field and type and hit enter to add a new NTP server URL.

5. In the **AWS region** field, select the AWS region to host your instance. There may be small pricing differences between the regions.

6. Select the **Virtual Private Cloud** (VPC) that will be accessed by this instance. The dropdown will be empty if you have not configured a VPC in the selected region. Use the AWS Services console to configure the VPC and subnets, and then restart the wizard.

7. Select the desired **Subnet**, the segment of the IP address range of the VPC, that this instance can be attached to. The dropdown will be empty if no subnet has been configured. Nexenta recommends that you configure your routing tables so NexentaFusion can access this private subnet for appliance management.

8. Set the **Security group(s)**. Click the **NEW DEFAULT GROUP** button to create a security group enumerating the ports used by NexentaCloud for inbound network connections. You can select additional groups, if needed, to regulate this instance. The security group created using the **NEW DEFAULT GROUP** button can be further modified using the AWS Services Console.

9. Termination protection is set to **YES** by default, to prevent a user from accidentally deleting the NexentaCloud instance using the Amazon EC2 console.

10. Optionally, set the **Override subnet** to disable public IP if desired. The best practice is to launch NexentaCloud in a private subnet, and enable connection to the internet using a NAT gateway.

11. To use encrypted storage with the NexentaCloud instance, set **Enable storage data encryption** option to **YES** and select the **Master key**.

12. Click **Continue**.

   - **Specify the instance workload and EBS storage to allocate:**

   Select the workload category that best fits the intended use of the NexentaCloud appliance. Review the planning considerations for a summary of the EBS storage limits, and the EC2 instance (CPU) that will be assigned. Consider potential future upgrades to support greater capacities, and how this will affect the total # of devices needed. A NexentaCloud instance can support a max of 40 devices, and the instance always requires 1 device for the root pool.

   The POC and High Performance workload categories will allocate high-performance gp2 devices.

   The Backup/DR workload category will allocate high-capacity, lower-performance sc1 devices, and 2 small gp2 devices to use as a mirrored log cache.

   1. Select the **workload category**. The device size and raw capacity selectors will change based on the workload category.
2. Select the **device size**. Drag the capacity balloon to the desired raw capacity.

![Select the workload category](image)

**Planning considerations**
- A NexentaCloud appliance can attach a max of 30
- Review the AWS EC2 Service dashboard EBS Store
- The EC2 instance (CPU) will be selected to support
  - d2.xlarge - up to 50 TIB (46 TIB)
  - r3.2xlarge - up to 150 TIB (136 TIB)
  - r4.4xlarge - up to 360 TIB (334 TIB)

![Select sc1 device size and raw capacity](image)

2 high-performance gp2 devices of 10 GB each will also be allocated as a LOG (cache)

3. Click **Continue**.

   ✷ **Review the configuration selections:**
   
   1. Verify your settings for **NexentaCloud Instance**.
   2. After verifying your Instance summary, click **Deploy Now** to deploy the instance.
   3. Click **Deploy Now** on the confirmation dialog.

   The NexentaCloud deploy will begin, and you will be navigated to the Appliance list page where you can see the ongoing status of the deployment. Deployment can take up to 30 minutes to complete.

![Appliance list](image)

4. You can always cancel the deployment by clicking on the Instance’s COG and choosing **Cancel**.
Verifying NexentaCloud Appliance Creation

1. Log in to NexentaFusion and click Appliance in the drop-down list, if not already in the Appliance view.

2. On the Appliance List page, verify the instance is created. If the instance is successfully deployed, the status shows as Connected.

   Your NexentaCloud appliance will display the same type of information in the Appliances List as an on-premise NexentaStor appliance. Refer to Viewing an Appliance Summary for additional information.

3. Click on the COG and select Properties to review the instance configuration details retrieved from AWS. See Viewing NexentaCloud Properties and Instance ID.

   1. **Unsuccessful deploy:**

      If the instance did not deploy successfully, the status shows as Stopped. Click on the red health icon, for an explanation of the problem.

   ![Unsuccessful deploy](image)

      Note: In most cases, the EC2 instance (CPU) has been created and is being charged, even when the complete deployment is not successful.

      You can

      1. Resolve the issue, if possible. Then click Continue in the Actions COG to continue the deployment process.

         Or
2. Click Cancel in the Actions COG to destroy the EC2 instance, resolve the issue, and start the deployment process again from the beginning.

Managing NexentaCloud Appliances

This chapter will describe the few differences in managing a NexentaCloud appliance.

Review Managing NexentaStor Appliances and subsequent chapters for guidance on configuring email settings for alerts, configuring pools, datasets and shares, data protection, and additional capabilities.

Viewing NexentaCloud Properties and Instance ID

The Properties view will summarize the instance configuration details retrieved from AWS, including the AWS-generated Instance ID.

1. Log in to NexentaFusion and click Appliance in the drop-down list, if not already in the Appliance view.

2. Click on the COG on the right side, and select Properties.

This summarizes the instance configuration details.
Viewing and Upgrading the NexentaCloud License

The NexentaCloud License defines the EC2 (CPU) instance type assigned to this instance, and is used to limit the capacity that can be configured into a pool. The license can be upgraded to support higher capacities. Upgrading the license will temporarily pause NexentaCloud, and move it to a more powerful EC2 instance. Review the costs associated with the EC2 instance types in your region on the AWS website.

1. Log in to NexentaFusion and click **Appliance** in the drop-down list, if not already in the Appliance view.
2. Click on the **COG** on the right side, and select **License**, to view your existing license limits.
3. To upgrade, click the **Upgrade** button, to display the dialog shown below. The Activate capacity value indicates how much of your existing Licensed Capacity limit has been configured into pools.

![Upgrade License Dialog](image)

4. Select from the available upgrade options, and click **Upgrade** to begin.

5. Click **CONTINUE** on the Confirmation dialog to begin the upgrade.

The upgrade will pause your NexentaCloud instance, and may temporarily disrupt I/O. Your instance will be moved to the new EC2 type, and your license will be updated with the new capacity limit.

Monitor the upgrade progress on the Appliance list view.

### Changing the Subscription Pricing Model

When deploying a NexentaCloud instance, the AWS subscription defaults to Monthly. Changing to an Annual subscription must be done on the AWS Marketplace. NexentaFusion provides a link to the AWS Marketplace to convert the subscription on the License dialog.

1. Log in to NexentaFusion and click **Appliance** in the drop-down list, if not already in the Appliance view.

2. Click on the **COG** on the right side, and select **License**, to view your existing license limits.
3. Click **CONVERT TO ANNUAL** button to open a new browser window to NexentaCloud in the AWS Marketplace.

### Viewing NexentaCloud Components

After deploying a NexentaCloud appliance, use the Components view to view virtual server and device information.

To view the NexentaCloud components, 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. Expand the Server entries to view details of the assigned CPU and memory. The Chassis section will display the allocated EBS storage as XEN devices.

---

**Note:** NexentaFusion will allocate gp2 storage in device sizes of 1, 2, or 4 TiB. It will allocate sc1 storage in device sizes of 5 or 10 TiB.

The COG in the upper right will have selections to add additional EBS storage. Refer to [Adding EBS Storage Capacity](#) for details.

### Configuring Pools

Creating and managing pools on a NexentaCloud appliance is largely the same as with a NexentaStor appliance. NexentaCloud allocates highly-reliable EBS storage as virtual devices. Generally, you will create a pool as a stripe, with no additional redundancy.

High-performance pools should be configured using gp2 storage.
High-capacity pools for backup should be configured using sc1 storage, with a log cache configured using gp2 storage.

| Note: | NexentaFusion will allocate gp2 storage in device sizes of 1, 2, or 4 TiB. It will allocate sc1 storage in device sizes of 5 or 10 TiB. Gp2 storage for logs will be allocated in a device size of 16 GiB. |

For information on creating a pool, see Creating Pools on Single or Clustered Nodes and follow the directions of single nodes.

| Note: | You can only configure a single node NexentaCloud appliance. |

### Adding EBS Storage Capacity

Additional EBS Storage capacity can be easily added to your NexentaCloud instance after the initial deployment. Storage capacity can be added beyond what is licensed. The license limits the amount of the capacity that can be configured into storage pools.

Your total capacity is limited to what can be configured in 40 devices. (The root device allocated as part of the AMI deploy is one of the 40 devices.)

Review the AWS EC2 Service dashboard EBS limits. AWS limits the amount of storage your account can allocate in total among all instances in each region. You may need to increase your limits to be successful in adding EBS storage capacity.

To add capacity:

1. Log in to NexentaFusion and click **Appliance** in the drop-down list, if not already in the Appliance view.
2. In the **Appliances List**, click on a NexentaCloud appliance and select **Management**.
3. Click **Components**.
4. Click the **COG**, and select **Add Capacity**. The Installed Capacity table provides a summary of the devices that are already installed and still available for use in pools.
5. Select the desired **Storage type**.

If you have a POC license with a limit of 5 or 10 TB, the only choice is high performance – gp2 EBS storage.
6. Select the desired **Device size**. The device size choices depend on the storage type. If planning to extend an existing pool, select the same size device for the best performance.

![Device size selection](image)

7. The add device for log selector becomes enabled if the high capacity – sc1 storage type has been selected.

Click **YES** to allocate 2 small high-performance gp2 devices to add to an existing or new pool as a mirrored log (cache) device, to improve performance. The # of Devices can be 0 to add only the high-performance devices to use, for example, as an additional mirrored log for an existing pool.

![Add raw capacity](image)

8. Click **ADD**. A confirmation dialog will be displayed. Click **ADD**.

9. After a few minutes, the dialog will close, and the Components view will be updated.

Upon completion, the Components view may display additional device outlines, but without the device size data, as shown below.
Wait another minute or so, click the **COG** in the upper right, and select “**Rescan**” to retrieve the device details.

10. The new devices can now be used to extend an existing pool, or create a new pool.

**Removing and Destroying the NexentaCloud Appliance**

The NexentaCloud appliance can be easily be removed from Fusion management and destroyed, when it is no longer needed.

- **To remove the Instance from Fusion management:**
  1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
  2. Click the **COG** for the NexentaCloud appliance, and select Remove.
  3. In the Remove window, enter the **instance ID** to confirm.
4. Click the **Remove and Destroy** button.

**Note:**
If you choose to remove the appliance from Fusion Management without destroying the instance, you will continue to be charged for the instance. To destroy the instance once it has been removed from Fusion, use the AWS EC2 console.

## Additional Resources

The following NexentaStor documents are applicable for NexentaCloud instances also.

### Table 6-1: Documentation Resources

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>NexentaStor 5.x CLI Configuration Guide</em></td>
<td>This guide demonstrates the basic steps and commands to configure and manage NexentaStor 5.x appliances. Use this document in conjunction with the <em>NexentaStor 5.x Command Line Interface Reference Guide</em>, and the <em>NexentaStor 5.x HA CLI Admin Guide</em>.</td>
</tr>
<tr>
<td><em>NexentaStor 5.x CLI Reference Guide</em></td>
<td>This reference guide provides a summary of the CLI commands. Use it in conjunction with the companion document, <em>NexentaStor 5.x CLI Configuration Guide</em>.</td>
</tr>
<tr>
<td><em>NexentaStor Product Guide</em></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>
</tbody>
</table>
What Comes Next?

The following chapter covers details to manage system and data settings.
Managing Appliance System and Data Settings

This section includes the following topics:

- Managing System and Data Settings
- Rebooting or Powering Off a NexentaStor/NexentaCloud Appliance
- What Comes Next?

Managing System and Data Settings

The Administration page allows you to manage appliance services and configuration settings and data retention settings, as well as Rebooting or Powering Off a NexentaStor/NexentaCloud Appliance.

- Under the System Settings tab, you can enable or disable any system services. You can also configure, edit, and check the status of the services listed in the section Summary of System Services.
- Using the System Configuration Settings, you can set up administrator email, alert emails; alert threshold settings; enable Swagger documentation, control routing for hosts, modify NexentaStor SMTP settings for the selected appliance.
- Using the Node Management settings, you can check the appliance version and time settings, check if there is a software update available and trigger a reboot or power off on the appliance.
- Under the Data Settings tab, you can configure data retention parameters for logs, events, and analytics for appliances.

Note: You must have Administrator privileges to perform this procedure.

This section covers the following topics:

- Summary of System Services
- Enabling and Disabling System Services
- Editing System Services
- Rebooting or Powering Off a NexentaStor/NexentaCloud Appliance
- Viewing Available Software Updates
- Configuring Data Settings

Summary of System Services

- HA cluster service – Enable the ha cluster service to avail of the high availability functionality.
Managing NexentaStor Appliances

• **idmap** – Configure the NexentaStor identity mapping service to concurrently share any file system over NFS and SMB while maintaining tight control on end-user authentication and access permissions.

• **ldapclient** – Configure ldapclient to access and manage directory services.

• **iSCSI target service**—Configure the iSCSI target service and choose the supported authentication services like CHAP and Radius to share the appliance volumes using the iSCSI protocol.

• **NFS server**—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.

• **NTP client**—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 appliance.

• **NDMP service**—Configure Network Data Management Protocol (NDMP) a networking protocol and an open standard for backing up data in a heterogeneous environment.

• **SMB server**—Configure SMB server to provide shared access to files between nodes on a network.

• **SMB client** – Enable and Configure SMB client to connect to Active Directory infrastructure.

• **SNMP service**—Configure Simple Network Management Protocol (SNMP) to monitor devices over an IP network.

• **stmf service** – Configure SCSI Target Mode Framework service to use iSCSI or Fibre Channel target block services.

• **sedctl** – Configure sed service to detect encrypted drives and for NEF to perform pool management correctly even if the pool does not use any encrypted drives)

• **vscan** – Configure vscan to perform virus scanning operation on files

### 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.

5. A service that is in a maintenance state is enabled, but not able to run. The service might be in transition because an administrative action has not yet completed, or administrative action is required to resolve the problem. A service that is in a maintenance state can be disabled. Click the COG, and select Disable from the drop-down list.

### Editing System Services

You can edit the properties for the following services from the Administration > System Settings page: iSCSI target service, NDMP backup service, NFS server, NTP client, SMB server, SMB client, SNMP service, and virus scan 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA Cluster service</td>
<td>online</td>
<td></td>
</tr>
<tr>
<td>idmap service</td>
<td>online</td>
<td></td>
</tr>
<tr>
<td>iSCSI target service</td>
<td>online</td>
<td></td>
</tr>
<tr>
<td>LDAP client</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>NDMP backup service</td>
<td>online</td>
<td></td>
</tr>
<tr>
<td>NFS server</td>
<td>online</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** For a clustered appliance, system setting changes must be made separately on each node.

- **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 with a status of disabled or maintenance. 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 Properties from the drop-down list.

4. Modify the properties for the service as necessary. The properties you can set vary with the type of service.

5. Click Save.

**Editing System Configuration Settings**

Using the System Configuration Settings, you can change common appliance configuration settings for the selected NexentaStor or NexentaCloud appliance.

- **Administrator Email** – Edit the email address of the NexentaStor/NexentaCloud admin user for system failure notifications.

- **Alert Emails** – NexentaStor and NexentaCloud can generate alerts for alert case events. You can specify an email address to receive email notifications directly from the appliance, in addition to displaying the alerts in NexentaFusion. You can also subscribe to be notified by only a subset of all alerts by providing the class prefixes.

  Note: Fusion can generate an email notification for alert case events. See Creating Rules for Logs and Events.

  Example of a class prefix:

  Use dot separated string as shown here: fault.fs.zfs.device. If you want to receive notifications about all faults then you set the Class prefix to fault. If you want to receive notifications only for zfs faults then you set the Class prefix to fault.fs.zfs.

- **Alert threshold settings**

  Using this feature you can specify whether the appliance should generate an alert when CPU utilization thresholds or Network utilization thresholds are exceeded, and set the threshold values. You can also edit the email address to receive the alert notifications directly from the appliance.

  **Defaults for CPU Utilization:**

  The CPU utilization is configured to alert when the default warning threshold exceeds 75% and the error threshold exceeds 90%.

  **Defaults for Network Utilization:**

  The network usage is configured to alert when the warning threshold exceeds 75% and the error threshold exceeds 90%.
• **Network Hostmodel** - This setting controls how outbound IP traffic is routed across multiple interfaces on the NexentaStor node using either the Weak end system model or the Strong end system model as defined in RFC1122. The Weak hostmodel, also known as asymmetric routing, allows the NexentaStor node to select any outbound interface that can reach the destination IP address, independent of the source IP address of the packet. The Strong hostmodel, also known as symmetric routing, should be used for scenarios where outbound traffic must be kept on interfaces that are on the same subnet as the source IP address in the packet. This is particularly useful when strict segregation of IP traffic across different interfaces is required.

• **SMTP** - Many appliance tasks, such as system failure notification, require that you properly configure the SMTP mail server. You may have configured the SMTP server for your appliance when you registered NexentaStor using NexentaFusion. You can modify the SMTP mail server for NexentaStors using the Administration interface. See SMTP Parameters for more details on the various parameters.

• **Enable SWAGGER doc in NexentaStor /NexentaCloud appliance** - The API online documentation is a development tool and access is disabled by default. To access the detailed REST API documentation, you must enable it.

  ❖ *To configure the above settings:*
  1. Log in to NexentaFusion and click Appliance in the drop-down list.
  2. In the Appliances List page, select the appliance for which you must enable access to the REST API documentation.
  4. In the System Configuration Settings panel, find the desired configuration entity and click the COG to Open Settings.
  5. In a clustered appliance, check “Use same settings for all nodes” to send the settings to both nodes of the cluster. If not checked, you will see separate edit fields for each node.
  6. Edit the properties as desired. Click Save.
  7. Click Save to save the changes you made.

Table 7-1: SMTP Parameters

<table>
<thead>
<tr>
<th>SMTP property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Host Name</td>
<td>SMTP server hostname or IP address.</td>
</tr>
<tr>
<td>Port</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. The default port changes to 465 when you select the Use SSL/TLS option.</td>
</tr>
<tr>
<td>User</td>
<td>SMTP User Name that you use to access your e-mail. Login name for this SMTP server.</td>
</tr>
<tr>
<td>Password</td>
<td>SMTP Password that you use to access your e-mail. Password for the SMTP server login.</td>
</tr>
<tr>
<td>Sender email</td>
<td>The mail address displayed in the Sender field for all emails originating from NexentaStor.</td>
</tr>
</tbody>
</table>
Viewing Available Software Updates

- **To check if there is a software update available for the selected registered NexentaStor appliance:**
  1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
  2. In the **Appliances List** page, select the appliance for which you must view if there is a software update available.
  3. Under **Administration**, click **System Settings**.
  4. Under **Node Management**, a bell icon will appear if there is a software update available for the selected registered appliance.
  5. Hover over the bell icon to view the updates available.

<table>
<thead>
<tr>
<th>SMTP property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security mode</strong></td>
<td>Use SSL or STARTTLS to encrypt a communication channel between the SMTP server and your appliance.</td>
</tr>
<tr>
<td><strong>Authentication Method</strong></td>
<td>Method of SMTP authentication mechanism that your mail server uses. The options are: PLAIN LOGIN CRAM-MD5 XOAUTH2</td>
</tr>
<tr>
<td><strong>Reject Unauthorized</strong></td>
<td>Reject any connection which is not authorized with the list of supplied CAs. Set it to <code>NO</code> if SMTP server uses self-signed certificate.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>Timeout interval in milliseconds</td>
</tr>
</tbody>
</table>

**Note:** When you modify the SMTP parameters from what you had initially configured during the registration of the appliance, you will observe that the TEST SETTINGS button changes to SAVE & TEST SETTINGS. This implies that the changes you make will be saved in the NexentaStor appliance before it tests the settings that you had configured.
Configuring Data Settings

You can configure data settings for the retention of system data from the Administration > Data Settings page. This section demonstrates how to configure data settings for logs, events, active probes, as well as how to view and manage analytics aggregation data.

The following topics are covered:

• Configuring Logs
• Configuring Events Retention
• Active Probes
• Managing Analytics Aggregation Data

Configuring 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 click 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 click Save. The default retention period is 3 months.
   c) Make some space by choosing to Delete logs older than the date you select on the pop-up calendar, then click Delete # of Logs, where # is the amount of space to recover.
Configuring Events Retention

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

To configure events 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 policy:
   - Select the length of time to Store events for from the drop-down list and click Save.
4. Make some space on the Elasticsearch database in the following ways:
   - Delete events older than a selected date on the pop-up calendar, then click Delete # of Events.
Active Probes

Active probes utilized by NexentaFusion are enabled/checked by default. The Active probes settings control the types of metric data that is sent to the database from the appliance, for use on the dashboard and analytics chart widgets.

Table 7-2: Active Probe Metrics

<table>
<thead>
<tr>
<th>Active Probe</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFSStat</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>arcStats</td>
<td>Adaptive Replacement Cache hits percentage Probe interval: 15 seconds</td>
</tr>
<tr>
<td>fcLuStats</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>fcTargetStats</td>
<td>FibreChannel Target Port I/O statistics Utilization, bandwidth, and IOPs for read/write operations. Probe interval: 15 seconds</td>
</tr>
<tr>
<td>iscsiLuStats</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>networkIO</td>
<td>IP Link I/O statistics Utilization and bandwidth for read/write operations. Probe interval: 15 seconds</td>
</tr>
<tr>
<td>zpoolStats</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>
</tbody>
</table>
### Active Probe | Description
---|---
SMBStat | Overall host I/O statistics for SMB protocol IOPS, bandwidth and latency for SMB read/write operations. Probe interval: 15 seconds
cpuUtilization | Average CPU utilization percentage Probe interval: 15 seconds
fcSummaryStats | 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
iscsiSummaryStats | Host iSCSI 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
nfsShare | Per NFS share I/O statistics IOPS, bandwidth and latency for read/write operations, including roll-ups (total bytes transferred, total IOPS performed and average latency). Probe interval: 15 seconds
smbShare | Per SMB share I/O statistics IOPS, bandwidth and latency for read/write operations, including roll-ups (total bytes transferred, total IOPS performed and average latency). Probe interval: 15 seconds
zpoolIO | Per pool I/O statistics IOPS, bandwidth and latency for read/write operations, including roll-ups (total bytes transferred, total IOPS performed and average latency). Probe interval: 15 seconds

### Managing Analytics Aggregation Data

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

**Note:** The estimated space will not be a valid estimation until the appliance has been running with representative IO for at least a week.

- 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**
   - **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.

### Rebooting or Powering Off a NexentaStor/NexentaCloud Appliance

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

**Note:**
- You must have Administrator privileges to perform this procedure.
- When you Power off a NexentaCloud appliance, it will be shown as “Stopped” on the AWS Console, and can be started again from the AWS Console. Your account will continue to be charged for the EBS storage assigned to the NexentaCloud appliance while it is in a stopped state.

*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**—When powering off a node that is part of a cluster, HA pools fail-over to the other node.
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**.

**What Comes Next?**

*Chapter 8, Managing Storage* covers details to provision a single node or a clustered NexentaStor appliance.
Managing Storage

This section includes the following topics:

- Provisioning Overview
- Viewing Available Disks for Pool or Log or Cache
- Creating and Removing Pools
- Maintaining Pools
- Managing Pool Data Devices and Faults
- 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.

Once you have created the pool, you can configure a file system, or volume group and volumes and use the NexentaFusion advanced capabilities to share file systems and volumes over the network. See Chapter 9, Managing Datasets for more information.

To provision a single node NexentaStor/NexentaCloud appliance or a clustered NexentaStor appliance using NexentaFusion, complete the tasks in Table 8-1 in the order in which they are presented.

Table 8-1: Provisioning Task Map

<table>
<thead>
<tr>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Identify disks associated with an appliance.</strong></td>
<td>For information, see Viewing Available Disks for Pool or Log or Cache.</td>
</tr>
<tr>
<td>After registering a NexentaStor appliance, and if there are JBOD chassis attached, you may want to review the disks that can be assigned as data, cache, spare, or log devices.</td>
<td></td>
</tr>
<tr>
<td>After deploying a NexentaCloud appliance, the EBS storage devices are visible in a virtual enclosure.</td>
<td></td>
</tr>
<tr>
<td>This section demonstrates how to view all the enclosures and disks enclosed in a chassis.</td>
<td></td>
</tr>
</tbody>
</table>
### Task 2. Update the NexentaStor appliance network, as needed.
This section demonstrates how to do the following:
- Verify the network interface you configured during NexentaStor appliance installation.
- Optional: Configure aggregates and VLANs to maximize the network performance and monitor status.

Instructions: For information, see Managing Network Configurations.

### Task 3. Configure a pool for a single node or clustered appliance.
This section demonstrates how to do the following:
- Identify the disks that can be used in a pool.
- Create a pool with the desired redundancy characteristics.
- Add cache devices and log devices to optimize performance.
- Add spares to improve availability.
- Add unmap support for SSDs to efficiently use the storage.
- Schedule a scrub service to check the pool integrity.

Instructions: For information, see Viewing Available Disks for Pool or Log or Cache.

### Task 4. Configure a shared pool HA service for the failover of HA cluster pools.
A NexentaStor HA Cluster detects system failures and then transfers ownership of shared pools to the alternate node. These sections demonstrate how to do the following:
- Add a shared pool to an HA service.
- Configure a VIP for clients to access.

Instructions: For information, see Chapter 10, Managing High Availability.
Viewing Available Disks for Pool or Log or Cache

Once you register a NexentaStor appliance with a JBOD attached or deploy a NexentaCloud appliance with EBS storage, 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 or log or cache.

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 data vDevs, cache, spares, logs, or used for HA. 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. Devices shown with just an outline are unavailable because they are part of an active or exported pool, or are blacklisted.

---

**Note:** If a device is not available for pool/log/cache, refer to this section [Creating and Removing Pools](#).

---

Creating and Removing Pools

The following tasks demonstrate how to plan for, create, import and remove pools:

- [Planning for Pools](#)
- [Viewing Available Disks for a Pool](#)
- [Creating Pools on Single or Clustered Nodes](#)
- [Importing and Exporting Pools](#)
- [Destroying a Pool](#)

For information on managing pools with high availability, see [Chapter 10, Managing High Availability](#).

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 physical or virtual 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 pool.
- 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, RAID-Z1, RAID-Z2, or RAID-Z3. 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 physical or virtual disks 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.

  ![Available Drives Table](image)

  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

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.

This section demonstrates how to create a pool on a single node or on a clustered appliance using the Automatic data device selection method or manual method.

- **Automatic pool data device selection method:** Nexenta recommends to use Auto pool data device selection method as it will prevent pools being created with different device types or sizes and unbalanced across chassis.
  See [Selecting Data Devices for Pool Using Auto Method](#)

- **Manual pool data device selection method:** Choose the manual data device selection method if you have some requirements to create unique type of pool using different sized drives.
  See [Selecting Data Devices for the Pool Manually](#)

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>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Beginning Pool Creation</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>Selecting Data Devices for Pool Using Auto Method</strong></td>
<td>Select redundancy and add disks to be used as data devices using auto or manual method.</td>
</tr>
<tr>
<td>or <strong>Selecting Data Devices for the Pool Manually</strong></td>
<td></td>
</tr>
<tr>
<td>3. <strong>Adding Cache, Log, and Spare Devices to a Pool</strong></td>
<td>Add disks to be used as cache, log, or spare devices.</td>
</tr>
</tbody>
</table>

**Beginning Pool Creation**

The first step in the pool creation process is to establish a name, specify a High Availability (HA) configuration or not, identify if you want to use inactive devices and specify the build method for the pool.

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 the following:
• If the pool you want to create is part of a clustered appliance and you want to use it in High Availability mode, select Enable from the High Availability drop-down list. This causes the Guided Configuration and Internal and attached media to only show disk devices accessible to both cluster nodes. Otherwise, select the node on which the pool is to reside. Note: The High Availability option only appears when the appliance is a cluster.

• If you want to reuse devices that were previously part of pools that are now inactive or exported, toggle the Allow inactive devices button to Yes.

• Select the build method
  
  Auto: NexentaFusion will auto-select the devices based on specified parameters. You will be able to review and optionally change the selections prior to creating the pool. See Selecting Data Devices for Pool Using Auto Method.
  
  Or
  
  Manual: You will select the devices, optionally in a guided manner. See Selecting Data Devices for the Pool Manually.

Note: Using these inactive devices in the current pool will make the prior pool permanently unavailable.

### Note:

Pool name should be unique.

Selecting Data Devices for Pool Using Auto Method

1. In the Build method, select Auto.
Selecting Auto will open up a Auto-Select Data vDevs for Pool window and will display the enclosures in the appliance and their available drives by capacity.

For a NexentaStor Appliance:

2. Select the Enclosures you would like to use for the pool by clicking on the check boxes.
   The grayed columns show devices that are available in all the selected enclosures. These will populate the Select drive size drop down. When Enclosure level redundancy is selected, the # of enclosures selected will constrain the choices in the Redundancy drop down.

3. By default the Enclosure-level redundancy is set to YES.
   When it is set to YES, the redundancy choices are constrained by the number of selected enclosures and the devices will be spread throughout the enclosures to eliminate data loss during a single enclosure failure.
   When it is set to NO, the system will distribute device selection among the selected enclosures, but an enclosure failure might result in data loss.

For a NexentaCloud appliance:

All storage is in a single virtual enclosure. The Enclosure level redundancy selector is not displayed.

For all appliances:

4. In the Select drive size drop down box, select the drive size available for the selected enclosures.

5. In the Redundancy box, select the type of redundancy you want to use for the devices you selected. For a NexentaCloud appliance, “Stripe” is typically selected as the redundancy type.

6. Select the Number of devices per vDev. Choices available for the number of devices per vDev will be populated based on the number of selected enclosures and the selected redundancy.
7. Enter the **Maximum number of devices to use** for the data vDevs.

8. Once all the above entries are filled in, the following values are computed and displayed as:
   - **Maximum raw size**: sum of the capacity of the devices planned for use in the data vDevs,
   - **Maximum usable size**: maximum usable capacity of the devices for data, prior to compression which does not include parity or mirror copies.

9. Click **Continue**.

10. Review the devices that were selected and make any necessary changes before proceeding with the pool creation. If you selected **Allow inactive devices** to be part of the pool you are creating, hover over the inactive devices, marked with an *, to identify which pool the device previously belonged to that will no longer be usable.

11. Click **Next** and Continue with [Adding Cache, Log, and Spare Devices to a Pool](#).

### Selecting Data Devices for the Pool Manually

1. For the build method, select Manual.

2. In the **Manual Pool Creation** dialog, click **Continue**.

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

### Guided Configuration

This section explains the advantages of using Guided configuration. This feature 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.

The Guided Configuration tool provides greater efficiency in showing the appropriate available disks when creating the data vdevs for the 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 four (4) 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.

3. **Select redundancy** for the pool from the drop-down list:
   - Stripe (Non-redundant, typically selected when using NexentaCloud virtual devices))
   - mirror (two-way or three-way)
   - RAID-Z1 (3 or more disks)
   - RAID-Z2 (4 or more disks)
   - RAID-Z3 (7 or more disks)

4. 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.

5. Bright green devices marked with a plus sign are in a healthy state and can be used for building the pool. Green devices also marked with an asterisk are now inactive devices that were previously part of a pool.

Red indicates a failed, unavailable device. Devices shown with just an outline and a capacity are already part of an active or exported pool, or are blacklisted.

Before adding disks to the pool, verify the details of the available drives by hovering the cursor over the disk label in the table.
If you selected **Allow inactive devices** to be part of the pool you are creating, the inactive devices will appear with an asterisk symbol. For these devices, note the prior pool, which will become permanently unavailable if this device used in the new pool.

6. 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.

The disk outlines in the vDev show the minimum number of disks needed for the selected redundancy. Additional devices can be added by clicking the plus icon (+) for the desired disks.
7. To add another vDev, click **New vDev +**. When Guided Configuration is ON, the vDev is populated with disks similar to those chosen for the previous vDev, if available.

![CREATE POOL: hapool](image)

8. Click **Next** and continue with **Adding Cache, Log, 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, and Spare Devices to a Pool

To improve the performance, you can also add optional devices when creating a pool. 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. For cache, use high performance devices such as SSD.

- **Log**—To improve the performance, use ZFS Intent Log (ZIL) for non-volatile temporary storage for writes not yet stored on the pool. 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. For log, use high performance devices such as SSD.

- **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, and log devices to a pool, do the following:

Now that you have selected the data devices to the pool using Manual or Auto method, proceed with the following steps to add cache, log, and special devices to a pool.

Guided configuration is enabled by default to display only SSD devices for Log, or Cache vDevs. Although not recommended, you can disable guided configuration to use non-SSD devices for Log or Cache.

Note: With NexentaCloud, both gp2 and sc1 devices are reported as HDD. You must disable guided configuration to be able to select the 16 GiB high-performance gp2 devices to configure a mirror log for use with your Data vdevs configured with high-capacity sc1 devices. Also, the option to create a Cache vDev is not provided for a NexentaCloud pool.

1. To add an optional cache device, select Cache and do one of the following:
   - Click Create. Click the plus icon (+) on the desired device(s) to add as cache, and click Save.
   - Click Skip to continue without adding a cache device.

2. 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 the plus icon (+) on the desired device(s) to add as log. If the redundancy type mirror was selected, additional mirror vDevs can be added by clicking New vDev, and adding additional devices.
   - Click Skip to continue without adding a log device.

Smart Sparring

When a device in a pool with raidz or mirror redundancy fails, smart-sparing automatically selects the right spare device to activate by means of an ordered search using media type, size, and locality as criteria. Media types currently supported are HDD and SSD. The size attribute is used to ensure that the spare is at least the same size or bigger than the failed drive. Locality of the device refers to the storage enclosure. For example, for a pool configured with an SSD hot spare (for Log devices) and HDD hot spares (for data devices) in each storage enclosure:

- Smart-sparing will ensure that the SSD spare is only activated in case of a Log SSD failure,
• In case of an HDD failure, smart-sparing will preferentially activate the HDD spare in the storage enclosure where the failure occurred.

❖  **To add spare devices to a pool, do the following:**

1. Choose options from the Select chassis and Select disks drop-down to filter the available disks by enclosure and size, to help locate devices that will be suitable for spares.

2. To add optional spare devices, select Spare and do one of the following:
   - Click **Create**, Click the plus icon (+) on the desired device(s) to add as spares, and click **Save**.
   - Click **Skip** to continue without adding a spare device.

**Finish Pool Creation**

3. 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, if HA mode enable was selected, select the node on which to **Activate pool on**. After the pool is created, you can configure the High Availability service.

4. Click **Create Pool**.

5. If you selected Enable High Availability, see **Configuring an HA Service for a Pool with Shared Devices**. The screen for configuring HA access to the pool appears.
Importing and Exporting Pools

Finding an Exported Pool to Import

The following task demonstrates how to find pools that were previously exported to import.

**Note:** A pool exported by a NexentaStor 4.x appliance cannot be imported by a NexentaStor 5.x appliance. When a pool is destroyed, the data on the pool is not destroyed. If the pool devices have not been reallocated, the pool can be imported and made available for use again using the CLI, but not from Fusion.

❖ **To discover exported pools, 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 information:
   - HA Service State – Shows details of the HA service state, if the pool is being managed by an HA service. This first column on the left only appears for a clustered appliance. Hover the mouse over the shield icon to view the pop-up dialog.
   - Health – (current OK)
   - Node – Shows the node that currently owns the pool, for a clustered appliance.
   - Configured Capacity – Shows the total capacity of the pool after applying the redundancies (RAID/mirror).
   - Allocated/Free – The bar shows how much of the configured capacity is allocated to data and for filesystem and volume reservations.
- Raw % Utilized – This value is reflected in the bubble over the bar as well as in the column. It shows how much of the configured capacity has actually been written with data. Your performance may begin to degrade when more than 75% of the capacity has been utilized.
Exporting a Pool

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.

1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
2. In the **Appliances List** page select the appliance, then select **Management > Pools**.
3. Click the **COG** for the pool and select **Export** from the drop-down list.

Destroying a Pool

Destroying a pool will make the devices used in the pool available for other purposes. If the pool was under HA control, it needs to be removed from HA control before it can be destroyed. (see Chapter 10, Managing High Availability)

The Pool Destroy dialog informs you if you still have shared filesystems or mapped volumes (LUNs) in the pool. LUNs must be destroyed separately, their existence can cause pool destroy to fail. Shared filesystems can be unmounted as part of the pool destroy process if the Force checkbox is checked.

When a pool is destroyed, the data on the pool is not destroyed. If the pool devices have not been reallocated, the pool can be imported and made available for use again, using the CLI.

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 **Destroy** from the drop-down list.
5. If the pool dialog indicates that shared filesystems are detected, and you still want to destroy the pool, click on the check box to force the datasets to be unmounted.
6. Now click **Destroy**.

**Maintaining Pools**

- 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.
  3. Under **Management**, click **Pools**.
  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 [Pool Management Actions for High Availability](#) for detailed descriptions of each of the management actions.
For information on managing pools with high availability, see Chapter 10, Managing High Availability.

**Scrub**

The scrub process traverses the data of the entire pool and checks to make sure that there are no data integrity issues. The scrub process can be scheduled using a cron expression.

Before initiating a scrubbing service, be aware of the following guidelines:

- 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.
- 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.
- 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.

1. Click the COG for the pool and select Scrub from the drop-down list.
   - The dialog that is displayed provides status information about the last scrub/resilver, and gives you the options to
     - Set a schedule for the scrub task
     - Initiate a scrub now

2. Scrub can also be scheduled from the pool Properties dialog.

**Unmap/Trim**

When enabled for pools on SSDs, the Unmap/Trim feature in NexentaStor notifies the underlying storage media about certain sectors that are no longer needed in a volume or a file system enabling the SSD to more efficiently handle garbage collection and wear-leveling management.
The Pool Properties dialog is used to enable Auto unmap, and to schedule the unmap process.

The Pool Unmap dialog can be used to change the unmap schedule, and to trigger an unmap process now.

1. Click the COG for the pool and select Properties from the drop-down list.
   
   The dialog that is displayed provides gives you the options to
   
   - Enable the unmap feature for this pool
   - Schedule the start and stop times for the unmap process
   - Enable Force unmap – if set, it will force ZFS to issue unmap even if it thinks a device does not support it

2. Unmap can also be scheduled or triggered to process now from the pool Unmap dialog.

**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. Click the COG for the pool and select Properties from the drop-down list.
  
  2. On the Edit Pool Properties dialog, modify the option settings as necessary. Table 8-3 explains the available options.

3. Click Close.
### Table 8-3: 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>Scrub-schedule</td>
<td>Runs the auto-scrub service on this schedule. NexentaFusion enables you to run a scrubbing service automatically to periodically examine all the data in the specified pools to verify that it checksums correctly and also to check for consistency errors. If the pool has a redundant configuration, NexentaFusion corrects any errors it finds.</td>
</tr>
<tr>
<td>Comment=TEXT</td>
<td>User-defined pool comment</td>
</tr>
</tbody>
</table>
| Real-time Auto unmap =(on|off) | NexentaFusion supports two modes for UNMAP, for efficient use of the storage. With UNMAP, a storage appliance is able to notify the underlying storage media about certain sectors that are no longer needed in a volume or a file system, enabling the SSD to more efficiently handle garbage collection and wear-leveling management.  
  **Auto Unmap**  
  • At the pool level, you can set the AUTO-UNMAP property to ON for the ZFS to issue UNMAP commands to the underlying vDevs of any blocks as it trims blocks. By default, the AUTO-UNMAP zpool property is set to OFF.                                                                 |
| Real-time Force unmap =(on|off)| Force Unmap  
  • By turning this option ON or OFF, you can control whether device support is taken into consideration when issuing UNMAP commands to the underlying vDevs of the pool. By turning it on, at the pool level, you can invoke the ZFS to force run UNMAP job even if the underlying device does not support it.                                         |
| Scheduled Unmap = (start|stop) | You can invoke ZFS to run UNMAP jobs at a scheduled time, for a set duration. Once invoked, a manual trim runs through all of the empty space on a pool and immediately trims it.  
  Note that trimming may have a considerable performance impact on the pool if the device does not handle trim effectively.                                                                                                                     |
| Delegation                      | Grant a non-privileged user access based on the dataset permissions.                                                                                                                                                                                                                                                                     |
| Failure mode                    | System behavior in the event of catastrophic pool failure.                                                                                                                                                                                                                                                                            |
Editing a Pool - Adding Capacity to 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. Toggle the Show only: pool disks to OFF.
   Disks available for selection are displayed with a white + sign in a bright green background.
4. Select the prompted number of disks from the table on the right and click Save.

To optionally add cache, log, special or spare devices, do the following:

5. To add a cache, special, or spare device, do the following:
   a) Select Cache, Special or Spares.
   b) Click Create and select the prompted number of disks.
   c) Click Save.
6. To add a log device, do the following:
   a) Select Log.
   b) Select log redundancy type from the drop-down list and click Create. Click the plus icon (+) on the desired devices to add as log, and click Save. If the redundancy type mirror was selected, additional mirror vDevs can be added by clicking New vDev, and adding additional devices.

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

Note: You are not allowed to decrease the size of a pool.
7. To add another mirror vDev to an existing mirror log device, do the following:
   a) Select Log.
   b) Click New vDev. Click the plus icon (+) on the desired devices to add, and click Save.

Viewing Pool Status

This section demonstrates how to view pool status, which includes information on the selected pool, the disks in the pool, and the pool properties.

To 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, then select Management > Pools.
3. Click the COG for the pool and select Status from the drop-down list.
   The Info tab is selected by default, showing an Overview of the pool health, status, capacity, and operations.
4. Click the Disks tab to view information on disk health, errors, physical state.
5. To view the chassis ID of the disks and the enclosure location, click on the Expander arrow.
6. Click on Show Indicators to view and optionally blink the Ident LED on the device.
7. Click the Properties tab to view information on configured pool properties.
8. Click Close.

Pool Management Actions for High Availability

For information on managing pools with high availability, adding a pool to an HA service and deleting the pool from an HA service, see Chapter 10, Managing High Availability.
Managing Pool Data Devices and Faults

Editing a Pool - Administering Pool Data Devices

The Edit Pool dialog provides the mechanisms for managing individual devices in a pool, should a device become unreliable or not functioning properly.

This section covers the following topics:

- Smart Sparing and Device Replacement
- 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 Errors from a Device

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.
3. Under **Management**, click **Pools**.
   
   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. The available actions will vary depending upon the redundancy and the type of vDev.

Smart Sparing and Device Replacement

Smart-sparing and auto-replace are NexentaStor features that improve storage availability and simplify maintenance operations. When a device in a pool fails, smart-sparing automatically selects the right spare device to activate by means of an ordered search using media type, size, and locality as criteria.

When a spare has been activated to replace a failed device, it will be displayed in a spare vDev. In the example below, HDD 10 is the failed device. HDD 22 is the spare that has been activated and resilvered to replace it.

With auto-replace, the failed device can be simply removed and physically replaced with a new device. NexentaStor automatically detects the insertion of the new device and triggers re-silvering to the new device. After resilver from the spare to the replacement device is complete, the former spare will revert to being a spare.

An alternative is to make the spare the permanent replacement member of the pool, to eliminate a second resilvering. Using the Edit Pool dialog, click on the image of the failed device, and select “detach” from options on the device COG.
Removing a Device from a Pool

Only non-data devices can be removed from a pool. If the Log or Special vDev are mirrors, the initial device must be "detached". Then the remaining device can be “removed”. After removing a disk from the pool, the disk remains online in the system.

Replacing a Device in a Pool

Replacing a device in a pool with another physical device is equivalent to attaching a new device, resilvering, and then removing the original device from the pool. When resilvering is complete the removed device becomes available 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.

To replace a disk, click on the device COG and select Replace. The enclosure view changes to show the disks that are valid replacement candidates, filtered by the disks that are the same size and media type as the disk to be replaced. (the filter can be changed to expose other disks if needed). Click the “+” on the desired replacement disk.
The left-side panel will show the disk to be replaced and its replacement, until rebuilding completes.

**Attaching a New Mirror Device**

Select **Attach** on the COG of a device in a 2-way mirror to create a 3-way mirror. The enclosure view changes to show the disks that are valid attachment candidates, filtered by the disks that are the same size and media type as the disk to be replaced. Click the “+” on the desired replacement disk.

Select **Attach** on the COG of a device in a non-redundant pool, to create a 2-way mirror with the existing device.

**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 Errors from a Device

When you check the status of a disk and find any transient errors, you can reset the error counters 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.

Clearing Errors from all Devices in a Pool

Use the COG at the upper right of the Edit Pool view to clear the error counters of all the devices in the Pool. Or

On the Pools view, select the COG for a particular pool, and click Clear Errors.

What Comes Next?

Chapter 9, Managing Datasets covers the details to configure a file system, or volume group and volumes. It also covers the details on using the NexentaFusion advanced capabilities to share file systems and volumes over the network.
Managing Datasets

This section includes the following topics:

- Creating and Managing File Systems
- Sharing File Systems Using NFS
- Sharing File Systems Using SMB
- Sharing Filesystems Using S3
- Managing iSCSI Host Groups, Targets, and Groups
- Managing FC Host Groups, Targets and Target Groups
- Managing LUNs
- Protecting Data
- What Comes Next?

Overview

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.

Table 9-1: Provisioning Task Map

<table>
<thead>
<tr>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure a file system, or volume group and volumes.</td>
<td>For information, see: Creating and Managing File Systems, Properties of File System, and Sharing Filesystems Using S3.</td>
</tr>
</tbody>
</table>

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:

- Create and manage file systems.
- Create and manage volume groups and volumes.
Create 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.

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 14 levels of nested file systems below the parent root directory.

See Table 9-3 for a list of tasks you can perform with the filesystem COG options.
To create a file system, do the following:

1. Log in to NexentaFusion and 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.

2. Click the arrows on the left of the heading bar to expand the view of the hierarchy.

3. Click the COG for a pool or file system and select Add New Filesystem from the drop-down list.

4. Set the necessary properties, as described in Table 9-2 and click Create.
Note: When you create a child file system, most unspecified property values are inherited from its parent dataset. Some properties can only be set when the file system is created.
### Table 9-2: Properties of File System

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case sensitivity</td>
<td>Sets the file name matching algorithm used by the file system as casesensitive, caseinsensitive, or a combination of both styles of matching. This parameter is set when the file system is created and cannot be changed afterward.</td>
</tr>
<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>
</tbody>
</table>
### Note for the Estimated Maximum IOPs

The values that will be shown on the Performance Widget (with the IOPs chart) for the share will only be similar to this “Estimated Maximum IOPs” value IFF the xfer size of the client(s) doing IO is the same as the record size used for the estimate.

### 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 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 Properties. A dialog appears showing the editable properties. See Properties of File System for a description of each property.

---

Table 9-3: 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>Activate</td>
<td>The activate action is available for the destination dataset of a replication to mount it for writing. See Activating a Destination Dataset</td>
</tr>
</tbody>
</table>
### Managing Storage and Datasets

#### Task | Description
--- | ---
Data Protection | 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.

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 9-2](#).

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](#), [Sharing File Systems Using SMB](#).

Remove NFS/SMB share | You can unshare a shared file system at any time. When you unshare a file system, you can select to retain or remove the shares for child file systems, if any exist.
Filtering File System Listings

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 system listings, 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, NFS v3, 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 Administrator 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 9-4: NFS Server Tunables

<table>
<thead>
<tr>
<th>NFS Server Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grace Period</td>
<td>Specifies the number of seconds after a server reboots 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 (NFS v4 only), 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.
Creating 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 9-5.

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.

NFS sharing options are explained in Table 9-5.

7. Click **Save**.

<table>
<thead>
<tr>
<th>Anonymous File Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="TBD" /> Set ACE for everyone@ with read/write/modify access</td>
</tr>
<tr>
<td><img src="image" alt="TBD" /> Set ACE for user:nobody with read/write/modify access</td>
</tr>
<tr>
<td><img src="image" alt="TBD" /> Set ACE for specified user with read/write/modify access</td>
</tr>
</tbody>
</table>

These selections will add or replace the following ACE:

- allow everyone@
- rwxpdDARWc--s
- fd----

### Table 9-5: NFS Sharing Options

<table>
<thead>
<tr>
<th>NFS Folder Sharing Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Protocols</td>
<td><img src="image" alt="TBD" /> <strong>AUTH_SYS</strong> — In secure authentication, the user name and password are transferred transparently. <img src="image" alt="TBD" /> <strong>AUTH_NONE</strong> — Null authentication, where NFS clients are mapped by NFS servers as user nobody.</td>
</tr>
<tr>
<td>Open share</td>
<td>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.</td>
</tr>
<tr>
<td>Anonymous File Access Control</td>
<td>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.</td>
</tr>
</tbody>
</table>
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, and 3.02 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 9-6 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 Administrator privileges to perform this procedure.

Table 9-6: SMB Server Tunables

<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 Save to change the workgroup name.</td>
</tr>
<tr>
<td>Join Domain</td>
<td>Enter AD credentials and click Save to join a Windows domain. The default is Workgroup mode.</td>
</tr>
<tr>
<td>Min SMB Protocol level</td>
<td>Sets the minimum version of the SMB protocol to be registered and offered by the SMB server.</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>
</tbody>
</table>

**Note:** Using group ACLs is recommended, as it is more efficient than per-user ACLs.
The following procedure demonstrates how to enable SMB on the appliance, and optionally configure tunables for the SMB server to meet the needs of your IT infrastructure.

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 select **Enable** to activate SMB.
5. To configure SMB, click the COG again and select **Properties** from the drop-down list.
6. Do the following as necessary:
   - Enter a **System comment** to describe the server.
   - To modify the workgroup, click **Edit Workgroup**, enter a **Workgroup name**, and click **Save**.
7. To join the Active Directory Domain, click **Join Domain**, and then in the **Active Directory Domain Settings** dialog do the following:
   a) Enter the **Active Directory domain**, the Primary Domain Controller (PDC) address.
   b) Enter your AD **Login** and **Password**.
   c) Click **Save**.

### SMB Server Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 <a href="#">NexentaStor 5.x CLI Configuration Guide</a>.</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>

Signing Enables SMB signing.

LanMan compatibility level Specifies the LAN Manager (LM) authentication level. The LM compatibility level controls the type of user authentication for workgroup mode or domain mode.

Enable IPv6 Enables IPv6 Internet protocol support within the CIFS Service.

Enable guest access 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.x CLI Configuration Guide.

Enable NetBIOS Enables NetBIOS.

Restrict anonymous Disables anonymous access to IPC.
8. Expand the **Advanced Options** section, and make the necessary selections or changes. Table 9-6 explains the options.

### Table 9-6: Setting min and max Protocol Version for SMB Client

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min SMB protocol level</td>
<td>1</td>
</tr>
<tr>
<td>Max SMB protocol level</td>
<td>3.02</td>
</tr>
<tr>
<td>Active Directory site name</td>
<td>Enter site name</td>
</tr>
<tr>
<td>Preferred domain controller</td>
<td>Enter FQDN</td>
</tr>
<tr>
<td>Signing</td>
<td>required</td>
</tr>
<tr>
<td>LanMan compatibility level</td>
<td>3</td>
</tr>
<tr>
<td>Enable IPv6</td>
<td>ON</td>
</tr>
<tr>
<td>Enable NetBIOS</td>
<td>OFF</td>
</tr>
<tr>
<td>Enable guest access</td>
<td>OFF</td>
</tr>
<tr>
<td>Restrict anonymous</td>
<td>ON</td>
</tr>
</tbody>
</table>

### Setting min and max Protocol Version for SMB Client

NexentaStor supports using the SMB 2.1 client protocol to connect to the Active Directory infrastructure. This is specifically targeted at enabling the appliance to connect to Active Directory servers on which SMB 1 has been disabled.

The SMB client protocol version negotiation can be constrained by setting the min and max protocol versions as appropriate for your environment.

*To configure the SMB client, 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 client and select **Enable** to activate SMB.
5. To configure SMB, click the **COG** again and select **Properties** from the drop-down list.
6. In the SMB client service properties window, do the following as necessary:
   - Validate the current min and max smb client protocol version.
• Set the min, max client protocol version if not set.

Creating an SMB Share

This section demonstrates how to create an SMB share. Table 9-7 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 9-7: 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 $&lt;pool_name/filesystem_name&gt;$ becomes an SMB share named $&lt;pool_name_filesystem_name&gt;$.</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>Encryption</td>
<td>Enables encryption for 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>
<tr>
<td>Continuous availability</td>
<td>This property will be visible and can be set only if the server max protocol version is 3.0 or higher. It enables continuous availability for the smb share.</td>
</tr>
</tbody>
</table>

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

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. Click the COG for the filesystem and select Share using SMB.
5. Enter a **Description** and click **Save**.

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 the 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
  4. Click **Finish**.
Sharing Filesystems Using S3

NexentaStor 5.3 and NexentaFusion 1.2.2 supports sharing filesystems using S3 protocol.

This section covers the following topics:
- Configuring and enabling S3 service
- Creating S3 sharebling and configuring S3 service

By default, S3 service is enabled on NexentaStor 5.3 appliance. You can check the S3 service state on the System Services section of the Administration -> System settings page.

Note: You must have Administrator privileges to be able to control and configure S3 service

To configure S3 service, do the following:
- Log into NexentaFusion and click Appliance in the drop-down list.
- In the Appliances List page, select the appliance that contains the pool.
- Select Administration -> System Settings.
- Under System Services section, click COG for in S3 service and do one of the following:
  - To enable S3 service, select Enable
  - To modify S3 service configuration, select Properties and change the options as necessary

The following table explains the configuration options for the S3 Service:
Creating S3 share

Every S3 share is addressed by protocol, server IP/hostname, port, access and secret keys. While sharing the filesystem using S3 protocol, the system administrator must create an access/secret key pair which should be passed to the client that will be using this share.

The access/secret key pair is associated with the local user on the NexentaStor appliances. The buckets and files that are created by the client that uses the particular access/secret key pair will be created with the UID of the user that is associated with this access/secret key pair. You can create multiple access/secret key pairs for the same S3 share.

Creating an S3 share for a Filesystem

This section demonstrates how to create an S3 share. To do that, follow the steps:

- Log into NexentaFusion and in the Appliances List page, select the appliance.
- Select Management -> Filesystems
- Review the hierarchy of the filesystems and find the filesystem that you would like to share with S3 protocol. Create a new filesystem if needed.
- Click the COG for the filesystem and select Share using S3.
• Click Add key button

• Select the user that will be associated with the key pair
• Opt in generating the access key or in manual access key creation
• Enter the access key in case Generate access key option was unchecked on the previous step
• Press Add
In the opened popup window, copy and save **Access key** and **Secret key**

**Note:** This time is the only time when you can review and copy the secret key. In case this key is lost after the window is closed, there is no way to recover it.

Close the window with the keys. In the **Edit S3 Share** window you are able to review the created key pair.
You may create more key pairs or remove some at this point. When you are done, you may close the Edit S3 Share window.

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. 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. A volume can be accessed remotely by mapping it as an iSCSI or FC LUN.

Table 9-8 is a task map that outlines the process for creating volume groups and volumes.

Table 9-8: Task Map: Managing Volume Groups and Volumes

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

Note: See Managing LUNs for information on Mapping Volumes.
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. Volume groups also serve as consistency groups, simplifying creation of transaction-consistent snapshots of all the volumes they contain. For information on how to create a pool, see Creating Pools on Single or Clustered Nodes.

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.

Note: The properties set for a volume group become the default property values for new volumes that are created in the group.
5. Expand the **Optional Settings** and specify the following properties, 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`.
- **Write-back cache**—Controls if write-back cache is enabled on the dataset. The default is `false`.

6. Click **Create**.
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 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 a unique name for the volume.
   - 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 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 descendents, 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 descendents, 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 properties, or accept the defaults:
   - **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**.
   - **Write-back cache**—Controls if write-back cache (WBC) is enabled for the dataset. The default is **false**.

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.
6. Click Filter to apply the selected filter parameters and view the results, or click Clear to reset the fields.
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 following properties as necessary:
   - **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.
   - **Minimum space reserved for data only**—For thin-provisioned volumes, specify the minimum amount of disk space guaranteed for the volume not including descendents, such as snapshots and clones. 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 descendents, including snapshots and clones. There is no default value. A value of zero means there is no quota.

6. Review the **Usage Data**, expand the **Optional Settings**, and modify the following properties as necessary:
   - **Compression mode**—Enables or disables compression mode for the volume.
   - **Read only**—Controls whether or not the volume can be modified.
   - **Dedupe mode**—Controls whether or not compressed data is removed from the volume.
   - **Sync mode**—Controls synchronous behavior.
   - **Write-back cache**—Controls if write-back cache (WBC) is enabled for the dataset.

7. 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, 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 following properties as necessary:
   - **Volume size**—Specifies the logical size of the volume.
   - **Minimum space reserved for data and protection**—Specify the minimum amount of disk space guaranteed for the volume and its descendents, including snapshots and clones. There is no default value. A value of zero means there is no quota.
7. Review the **Usage Data**, expand the **Optional Settings**, and modify the following properties as necessary:
   - **Compression mode**—Enables or disables compression mode for the volume.
   - **Read only**—Controls whether or not the volume can be modified.
   - **Dedupe mode**—Controls whether or not compressed data is removed from the volume.
   - **Sync mode**—Controls synchronous behavior.
   - **Write-back cache**—Controls if write-back cache (WBC) is enabled for the dataset.
8. 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.

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.

- Creating, Editing, and Destroying iSCSI Targets and Target Groups
- Configuring Secure Authentication
- Configuring iSCSI Host Groups

Note: When making iSCSI changes on a clustered appliance, it may take a few seconds for the screen to refresh and reflect the changes.

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) Optional: Enter a unique name, for the target in the **Alias** field.
   
   b) Optional: Select an **Authentication method** from the drop-down list. The default is None. When you choose CHAP, the CHAP Name and Secret fields appear. For Uni-Directional CHAP, leave the Name and Secret fields empty. For Bi-Directional CHAP, providing a Name is optional, but you must enter a CHAP Secret. If a CHAP name is not provided, the system uses the generated IQN as the CHAP name. For more information, see *Creating, Editing, and Destroying iSCSI Targets and Target Groups*.
   
   c) Optional: Enter an **IQN** address to use, otherwise the system auto-generates one 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.
   
   ![Target portals](image)
   
   e) Select the IP address (es) where the system should listen for the iSCSI traffic. If no port is specified, the system will listen on the default port of 3260.

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*.
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.
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.
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.

**Unidirectional CHAP Authentication**

Unidirectional CHAP assumes that an initiator has its own secret, which you specify on the NexentaStor/NexentaCloud 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 appliance iSCSI target with unidirectional CHAP enabled must have a CHAP secret set. For more information, see Creating, Editing, and Destroying iSCSI Targets and Target 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:

```
  +---+-----+ +---------+ +----------------------------+
  | 1 | 92-01 | example.com | storage:diskarrays-sn-a8675309 |
```

❖ 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.

   **Note:** A LUN can be mapped with iSCSI or Fibre Channel (FC), but not both. iSCSI and FC mappings on the same LUN are not supported.

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 initiator, 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**.

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

When making FC changes on a clustered appliance, it may take a few seconds for the screen to refresh and reflect the changes.

**Note:**

Fibre Channel functionality requires an additional license.

Use the NexentaStor 5.x CLI to set up FC targets, changing ports from initiator to target mode. Currently, Nexenta Fusion does not provide the ability to configure FC targets.

Fibre Channel functionality is not available on a NexentaCloud appliance.

**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.
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.

<table>
<thead>
<tr>
<th>Alias</th>
<th>Creation time</th>
<th>Initiator</th>
</tr>
</thead>
<tbody>
<tr>
<td>QLE2462</td>
<td>Aug 25, 8:05:12</td>
<td>wwn.21000001b32134567</td>
</tr>
</tbody>
</table>

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.

 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. Click the target group COG and select Destroy Target Group in the drop-down list.
   5. In the confirmation dialog, click Yes.

Managing LUNs

NexentaFusion allows you to map volumes to LUNs. 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.

- Mapping Volumes
- Viewing LUN Information
- Editing and Destroying LUN Mappings

Note: When mapping volumes or editing LUN mappings on a clustered appliance, it may take a few seconds for the screen to refresh and reflect the changes.
Managing Storage and Datasets

Mapping Volumes

You can map a volume as an iSCSI LUN or FC LUN. LUN mappings enable you to select the 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.

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.

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. If required in your environment, change the block size to use for this LUN. The block size cannot be changed after the first mapping has been created.
6. 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 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.
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.

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

8. Click Close when the mappings are complete.

### 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.

  4. Mouse over a target group entry to see information on the targets in the group.

  5. In the far right column, click the COG for a LUN and select **Properties** to see additional information like LUN block size.
Editing and Destroying LUN Mappings

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**.

### Protecting Data

Data protection can be used with any dataset, be it a file system, volume group, or volume. Data protection is accomplished through the use of snapshots, clones, and with replication.

- **Snapshots**—A read-only point-in-time copy of a dataset. You can create a one-time snapshot of a dataset, or create a schedule to automatically take snapshots at specified intervals.
- **Clones**—A copy of a snapshot that is a separate, readable and writable dataset. A clone remains linked to the original snapshot from which it was created, until the clone is promoted. The snapshot from which a clone is created cannot be deleted as long as the clone exists. Promoting a clone creates a completely independent dataset.
Managing Storage and Datasets

- Replication—Frequent copying from a database in one location to a database in another location. 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. There are two types of replication: scheduled replication and continuous replication. 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. To perform remote replication to another appliance, the replication group password and data address must be configured.

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

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
- Activating a Destination Dataset
- Recovering a Faulted Replication Service
- Verifying and Querying Data Protection Data

**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 the selected parent data set and 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.

**Note:** Promoting a clone created by a replication service is not supported.

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.
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. To rollback a snapshot for a dataset that has replication services, first select Protection Services and disable the replication services.
5. Select Snapshots, click the COG next to the snapshot you want to roll the dataset back to, and select Rollback.
6. In the confirmation dialog, click **Confirm**.

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**.

### Preparing the Appliance for Replication

This section covers how to specify the dedicated network interface to use for replication, and how to specify the replication group password.

#### Setting the Replication Network Interface

To run high-performance replication (HPR) on an appliance, it is recommended that the interface on each node should be configured with a static IP interface, a 10 Gigabit Ethernet with Jumbo frames. This interface should be dedicated to replication, and not be used for appliance management. HPR uses port 6000 as the default.

> 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 **Data Protection Summary**, hover the cursor over a value on the right to view the service status.
4. Click the pencil icon next to the interface you want to modify. The Data Protection Dedicate Network Interface Address dialog appears.

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

6. Click Save.
Setting the Replication Group Password

Before configuring replication services between NexentaStor/NexentaCloud appliances, you must ensure that they are part of the same replication group. A replication group is defined as a set of appliances that share the same replication password. The replication password provides a simple, non-intrusive level of authentication that protects the appliances from being configured as a replication target of systems that are not in the same replication group.

- **To set or change the replication password:**
  1. Log in to NexentaFusion and in the **Appliances List** page, select the appliance.
  2. Select **Management > Data Protection**.
  3. Click on Change Replication Password to display the dialog where you can type a new password.
     - Note – the password text entry field will not display any indication that a password was previously set.
  4. Click OK.

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 9-9** appear in the Protection column for Filesystems and Volumes as a visual indicators for the type and status of the service.
### Table 9-9: Protection Service Icons

<table>
<thead>
<tr>
<th>Protection Service Icon</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Destination Icon](image) | Indicates the destination location for a replication service.  
**Green** indicates the service is in working order.  
**Red** indicates the service is not working.  
**Gray** indicates the service is disabled.  
**Transparent green** indicates that the child filesystem or volume is protected by a parent data protection policy. |
| ![Source Icon](image) | Indicates the source location for a replication service.  
**Green** indicates the service is in working order.  
**Red** indicates the service is not working.  
**Gray** indicates the service is disabled.  
**Transparent green** indicates that the child filesystem or volume is protected by a parent data protection policy. |
| ![Snapshot Icon](image) | Indicates a scheduled snapshot service.  
**Green** indicates the service is in working order.  
**Red** indicates the service is not working.  
**Gray** indicates the service is disabled.  
**Transparent green** indicates that the child filesystem or volume is protected by a parent data protection policy. |
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. Click the Recursive check box, to take snapshots of the nested datasets under the selected parent dataset. If there are no nested datasets, the Recursive option is grayed out.
6. In the Advanced options window, optionally, for filesystems shared with NFS, click Send NFS settings to replicate nfs share permissions to the destination.
7. In the Throttle field, set a maximum transfer rate for all replication by limiting the total bandwidth used by all transfers at any time.
8. Check the Mount destination filesystem to mount the destination filesystem to the default mountpoint. If unchecked, mountpoint is set to none.
9. To Set destination as read-only, click the check box.
10. Click **Add Schedule**, then in the New Schedule dialog select a Repeat interval (the time interval at which the snapshots should be taken) from the drop-down list:

- **Hourly**— Specify the **hours** interval, then select a **Minutes** value from the drop-down list. The minute intervals appear in the field. Optionally, you can click inside the field and manually enter additional minute interval values.
- **Daily**—Specify the Run every number of days interval, then specify the time of day at which to take the snapshot in the Run at field.

- **Weekly**—Select the Days of Week on which to take the snapshot, then specify the time of day at which to take the snapshot in the Run at field.

- **Monthly**—Specify the Run every number of months interval, type in the Days of Month on which to take the snapshot and press Enter. Then you can type another date. Next, specify the time of day at which to take the snapshot in the Run at field.
11. Select a **Snapshots Keep Policy** from the drop-down list:
   - Specify the number of latest snapshots to be kept locally.
   - Specify the number of latest snapshots to be kept on the secondary dataset or server.

12. 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) Click the **Recursive** check box, to take snapshots of nested (filesystem) datasets under the selected parent dataset. If there are no nested datasets, the Recursive option is grayed out.

5. Click **Add Schedule**, then in the New Schedule dialog select a Repeat interval (the time interval at which the snapshots should be taken) from the drop-down list:
Managing Storage and Datasets

- **Hourly**— Specify the **hours** interval, then select a **Minutes** value from the drop-down list. The minute intervals appear in the field. Optionally, you can click inside the field and manually enter additional minute interval values.

  - **Repeat**
  - **Run every**
  - **Minutes**

- **Daily**— Specify the **Run every** number of **days** interval, then specify the time of day at which to take the snapshot in the **Run at** field.

  - **Repeat**
  - **Run every**
  - **Run at**

- **Weekly**— Select the **Days of Week** on which to take the snapshot, then specify the time of day at which to take the snapshot in the **Run at** field.

  - **Repeat**
  - **Days Of Week**
  - **Run at**

- **Monthly**— Specify the **Run every** number of **months** interval, type in the **Days of Month** on which to take the snapshot and press Enter. Then you can type another date. Next, specify the time of day at which to take the snapshot in the **Run at** field.

  - **Repeat**
  - **Days Of Week**
  - **Run at**
6. Select a Snapshots Keep Policy from the drop-down list, and specify the number of latest snapshots to be kept locally.

7. 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.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous Replication requires an additional license. Scheduled snapshot functionality is included with the base NexentaStor 5.x license. For more information, contact your NexentaStor Sales Engineer.</td>
</tr>
</tbody>
</table>

- 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.

6. Optional: For a file system with nested datasets, click the Recursive check box to take snapshots of all the nested datasets under the selected parent dataset.
   There is no recursive selection for volume groups. All volumes in a selected group are automatically replicated.

7. In the Advanced options window, optionally, for filesystems shared with NFS, click Send NFS settings to replicate nfs share permissions to the destination.

8. In the Throttle field, set a maximum transfer rate for all replication by limiting the total bandwidth used by all transfers at any time.

9. Check the Mount destination filesystem to mount the destination filesystem to the default mountpoint. If unchecked, mountpoint is set to none.

10. To Set destination as read-only, click the check box.
11. In the confirmation dialog, click **Create**.

12. If Continuous Replication has been disabled, you can update the target at any time doing the following:
   
   a) Selecting **Management > Filesystems**.
   
   b) Select the **COG** for the pool and choose **Data Protection** from the drop-down list.
   
   c) Select **Continuous Replication** and then click **Run Once**.
Editing or Deleting a Schedule

This section demonstrates how to edit or delete a schedule.

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 next to the service Name to expand the tree, click the COG for the schedule and select Edit from the drop-down list.
   c) In the Schedules field of the dialog, click the pencil (Edit) icon.
   d) In the Edit Schedule dialog, modify the necessary fields as described in Adding a Scheduled Replication Service or Adding a Scheduled Snapshots Service.
   e) Click Save.
4. To delete the schedule, do the following:
   a) Select Protection Services.
   b) 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 service and select Snap Once or Run Once 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. 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. Find the service to be disabled, and clear the check box in the Service column.
   - If the protection service is a replication service, a confirmation dialog will be displayed. If replication is in progress when DISABLE is clicked, it will complete and then the service will be disabled.

   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.

5. For Continuous Replication, toggle **Service enabled** to OFF. To re-enable the service, toggle **Service enabled** back to ON.

6. 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:

   | 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. |

   - **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**.

**Viewing the Replication History**

The appliance stores the results of the last 10 runs including run-once, scheduled and recovery runs.

- To view the replication history:
  1. Log in to NexentaFusion and in the **Appliances List** page, select the appliance.
  2. Select **Management** 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.
     - Select Data Protection and query for the desired Replication Services.
3. Select Protection Services, click the COG for the service and select Show history from the dropdown list.

<table>
<thead>
<tr>
<th>Run Number</th>
<th>Start Time</th>
<th>End Time</th>
<th>Source Snapshot</th>
<th>Succeed</th>
<th>Send Size</th>
<th>Last Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>5884</td>
<td>Jul 12, 15:25:00</td>
<td>Jul 12, 15:25:02</td>
<td>hpr-2018-07-12-22-25-00-111</td>
<td>yes</td>
<td>1.8 Kib</td>
<td></td>
</tr>
<tr>
<td>5885</td>
<td>Jul 12, 15:55:01</td>
<td>Jul 12, 15:55:02</td>
<td>hpr-2018-07-12-22-55-00-439</td>
<td>yes</td>
<td>1.8 Kib</td>
<td></td>
</tr>
<tr>
<td>5886</td>
<td>Jul 12, 16:00:00</td>
<td>Jul 12, 16:00:01</td>
<td>hpr-2018-07-12-23-00-00-351</td>
<td>yes</td>
<td>1.8 Kib</td>
<td></td>
</tr>
<tr>
<td>5887</td>
<td>Jul 12, 16:05:00</td>
<td>Jul 12, 16:05:01</td>
<td>hpr-2018-07-12-23-05-00-358</td>
<td>yes</td>
<td>1.8 Kib</td>
<td></td>
</tr>
<tr>
<td>5888</td>
<td>Jul 12, 16:10:00</td>
<td>Jul 12, 16:10:01</td>
<td>hpr-2018-07-12-23-10-00-381</td>
<td>yes</td>
<td>1.8 Kib</td>
<td></td>
</tr>
<tr>
<td>5889</td>
<td>Jul 12, 16:15:00</td>
<td>Jul 12, 16:15:01</td>
<td>hpr-2018-07-12-23-15-00-402</td>
<td>yes</td>
<td>1.8 Kib</td>
<td></td>
</tr>
<tr>
<td>5890</td>
<td>Jul 12, 16:20:00</td>
<td>Jul 12, 16:20:01</td>
<td>hpr-2018-07-12-23-20-00-419</td>
<td>yes</td>
<td>1.8 Kib</td>
<td></td>
</tr>
<tr>
<td>5891</td>
<td>Jul 12, 16:25:00</td>
<td>Jul 12, 16:25:01</td>
<td>hpr-2018-07-12-23-25-00-436</td>
<td>yes</td>
<td>1.8 Kib</td>
<td></td>
</tr>
<tr>
<td>5892</td>
<td>Jul 12, 16:30:00</td>
<td>Jul 12, 16:30:02</td>
<td>hpr-2018-07-12-23-30-00-453</td>
<td>yes</td>
<td>1.8 Kib</td>
<td></td>
</tr>
<tr>
<td>5893</td>
<td>Jul 12, 16:35:00</td>
<td>hpr-2018-07-12-23-35-00-468</td>
<td>unknown</td>
<td>653.7 MiB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 the replication direction is flipped, keep policy values are flipped as well.
- Two services cannot replicate to the same destination. It is not allowed.
- Check 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.

**Note:** For details on the advanced configuration options for a HPR service, see the HPR User Guide. Nexenta recommends that you use these advanced functionalities only as disaster recovery solutions.

✈ 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.

Activating a Destination Dataset

In disaster recovery scenarios, following a failure at the source site and once replication is disabled, you will need to explicitly activate the destination dataset (file system or volume) of a replication service before it can be shared to applications. Activating the destination dataset ensures that the dataset is ready to be shared and used by applications on the secondary site.

• if the destination is a file system, it ensures it is mounted to its default mount point. If file system is replicated with sendShareNfs option, file systems will be shared with the same settings as they were shared on the source.
• Activating the dataset sets readonly of any datasets to OFF if it is already ON,
• Activating destroys incompletely received snapshot of any datasets that remains after a replication gets interrupted and may prevent creating new snapshots.

The mount point property is inherited from the parent pool or filesystem.

Note: For details on the advanced configuration options for a HPR service, see the HPR User Guide. Nexenta recommends that you use the advanced functionality only as disaster recovery solutions.

❖ To activate a filesystem, do the following:
   1. In the Appliances List page, select the appliance.
   2. Select Management > Filesystems > Filesystems.
3. Expand the pool, click the COG on the far right of the dataset.
4. Click Activate.

To activate a volume, do the following:
1. In the Appliances List page, select the appliance.
2. Select Management > Volumes > Volumes.
3. Expand the pool, click the COG on the far right of the volume.
4. Click Activate.

Recovering a Faulted Replication Service

Modifying, deleting, or creating snapshots of the destination dataset may cause the replication service to become faulted. Errors include:
- Destination has been modified since the most recent snapshots
- Source and destination snapshots do not match, the replication service should be recovered
- And others

A “Data Protection service faulted” alert will be generated to notify you. Use the Data Protection view to query for services where the State is Faulted. Click on the service COG, to see if the Recover option is available.
Click on Recover, to see the exact steps that will be taken if the RECOVER button is clicked. It will create a new recovery snapshot; then try to find the common snapshot for each replicated dataset separately, and replicate all snapshots created after the common snapshot to the destination. Any changes or snapshots created after the common snapshot will be destroyed. In case the common snapshot does not exist, the dataset will be replicated from scratch.
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.

<table>
<thead>
<tr>
<th>SNAPSHOTS</th>
<th>PROTECTION SERVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Protection Service</td>
</tr>
<tr>
<td>hpr-2016-08-25-21-35-00-236</td>
<td>A1Snap</td>
</tr>
<tr>
<td>hpr-2016-08-25-06-59-56-440</td>
<td>Scheduled Snapshots States enabled</td>
</tr>
<tr>
<td>hpr-2016-08-25-06-59-56-440</td>
<td></td>
</tr>
<tr>
<td>Created</td>
<td></td>
</tr>
<tr>
<td>Aug 10, 2016</td>
<td>12:00:00</td>
</tr>
<tr>
<td>time</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Protection Service</th>
<th>Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>hpr-2016-08-25-21-35-00-236</td>
<td>A1Snap</td>
<td>2016 Aug 25, 14:51</td>
</tr>
<tr>
<td>hpr-2016-08-25-06-59-56-440</td>
<td>Scheduled Snapshots States enabled</td>
<td>2016 Aug 24, 23:51</td>
</tr>
<tr>
<td>hpr-2016-08-25-06-59-56-440</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.
   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.

<table>
<thead>
<tr>
<th>SNAPSHOTS</th>
<th>PROTECTION SERVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Protection Service</td>
</tr>
<tr>
<td>test</td>
<td>pool1/src</td>
</tr>
<tr>
<td></td>
<td>pool2/dst</td>
</tr>
<tr>
<td>Schedule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Snapshots Destroy</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

  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.

What Comes Next?

Chapter 10, Managing High Availability covers verifying cluster status and managing high availability (HA) storage and services.
Managing High Availability

This section includes the following topics:

- About NexentaStor High Availability
- About NexentaStor High Availability and HA Services
- Editing vCenter Credentials for VSA-based Clusters
- Verifying Cluster Status
- Managing High Availability Storage
- Managing HA Services
- What Comes Next?

About NexentaStor High Availability

NexentaStor High Availability (HA) is an enterprise-proven cluster product that manages the availability of critical storage pools. Based on your requirement, the HA cluster can be either configured on bare metal or between NexentaStor Virtual Machines on VMware vSphere.

You initially configure the NexentaStor HA cluster using the NexentaStor Command Line Interface (CLI), and then manage the clustered nodes with NexentaFusion.

Note:

- High Availability functionality is only available when a valid NexentaStor HA license is installed on an appliance. For more information, contact your Nexenta sales engineer or Nexenta Customer Support at support@nexenta.com.
- High Availability functionality is not available for NexentaCloud appliances.

NexentaStor HA on Bare-Metal

NexentaStor HA cluster on bare metal 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 example of a High Availability (HA) cluster configuration would consist of two HA services. Each service is created independently, then assigned to one or more pools. Under normal operation, each node provides services to their designated pools. In the event of either node failure, the high availability of the pools on bare-metal is maintained by the cluster software that uses two functions to provide reliable automated failover services:
1. **Heartbeats**: Each node in the cluster communicates with the other node through different heartbeat mechanisms such as Network and disk heartbeats. These heartbeats are used to monitor the status of the remote node. As long as a remote node responds to network or disk heartbeats, it is deemed operational. If a remote node stops responding to heartbeats for a specific time period, the HA cluster detects system failure and an automatic failover operation is initiated.

2. **SCSI based disk reservations**: SCSI persistent reservations on devices in the pool are used to protect the data in the pool in case of split brain scenarios where two nodes may concurrently attempt to take ownership of a pool, or a node that was temporarily hung attempts to write to a pool it no longer owns.

When a failed node is repaired and restarted, it re-joins the cluster and the administrator controls when the pools are redistributed.

### NexentaStor VSA on VMware

NexentaStor High Availability is also supported between NexentaStor Virtual Machines on VMware vSphere. This configuration is popular for customers looking to add full featured NAS file services to VMware vSphere environments on all-block SANs or Hyper-Converged Infrastructure such as VMware Virtual SAN and Nutanix.

A NexentaStor HA cluster on VMware vSphere relies on two functions to provide reliable automated failover services:

1. **Heartbeats**: Each node in the cluster communicates with the other node through different heartbeat mechanisms such as Network and disk heartbeats. These heartbeats are used to monitor the status of the remote node. As long as a remote node responds to network or disk heartbeats, it is deemed operational. If a remote node stops responding to heartbeats for a specific time period, the HA cluster detects system failure and an automatic failover operation is initiated.

2. **vCenter control point**: vCenter is used to control the power state of NexentaStor virtual machines to protect against split brain scenarios and ensure that a storage pool is only imported on a single node at any time. This is used as an alternative to SCSI persistent reservations used on bare metal clusters.

### Additional Information

For information on the following:

- how to initially configure nodes of an NexentaStor HA cluster,
- how NexentaStor HA is deployed on VMware vSphere functions,
- outline of HA service configuration for NexentaStor VSA on VMware,

see the *NexentaStor HA CLI Configuration Admin Guide*. For information on how to configure an HA service in NexentaFusion, see Configuring an HA Service for a Pool with Shared Devices.
About NexentaStor High Availability and HA Services

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 between the clients and the datasets that can trigger an automatic failover to the other node in the cluster.

Note:

NexentaStor HA Cluster creation must be done in the NexentaStor CLI prior to registering the appliance to NexentaFusion. Configuration settings in NexentaFusion are limited to HA services and the VMware vCenter credential, used when deploying a VSA-based cluster.

For more information, see the NexentaStor 5.x HA QuickStart.

HA Service

- Detects server hardware, software and network failures across the HA Cluster and makes speedy, predictable, and predefined decisions as to what remedial action to take.
- Continually passes HA service state around the HA cluster so that services (and their associated pools) can be automatically started on the alternate node in the cluster if necessary.
- Allows manual movement of services (and their associated pools) in the HA Cluster for load balancing and administrative needs. Provides robust data fencing of pools in the HA Cluster.
- Is configurable using NexentaFusion, NexentaStor CLI or RESTful API.
- Provides notification of significant events across the HA Cluster.
- Exercises unused system components ensuring they are available if required on failover.
- Has no automatic bounce back of HA service after the failed node is repaired.
- Has any number of VIPs that failover with the service.

Editing vCenter Credentials for VSA-based Clusters

In order to deploy a VSA-based cluster, you must establish the connection between the NexentaStor VMs and the vCenter host by setting up the vCenter credentials. This capability is only applicable for NexentaStor appliance 5.2.0 and later.
In order to set up the vCenter credentials, you must meet all prerequisites that are listed under the section “Outline of HA service configuration for NexentaStor VSA on VMware” in NexentaStor HA CLI QuickStart Guide.

To set up the vCenter credentials, 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. To configure VSA-based cluster, click on the COG icon to the right of the Configuration section.
5. In the VSA_based cluster configuration window, enter the vCenter server address or name, port, user, and password and click Save.

   ![VSA-based cluster configuration window]

6. Under Configuration,
   - the VSA-based cluster will display “n/a” if the VSA is not configured yet.
   - The VSA-based cluster will show “offline” in red if configured, but the connection failed. Hover-over the text “offline” to see the details.

Verifying Cluster Status

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

**Viewing Network Heartbeats**

- *To view the network heartbeats, do the following:*
  1. Log in to NexentaFusion and in the **Appliances List** page, select a cluster.
  2. Select **Management > High Availability**.
  3. Select **Cluster Status**.

**Managing High Availability Storage**

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

- **Configuring an HA Service for a Pool with Shared Devices**
- **Adding an Unshared Pool to an HA Service**
- **Viewing Status Details for a Shared Pool**
- **Viewing VIPs Associated with an HA Service**
- **Moving a Pool under HA Service Control**
- **Removing a Pool From HA Control**
Configuring an HA Service for a Pool with Shared Devices

The primary benefit of an HA Service is to provide high availability access to user 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 Creating Pools on Single or Clustered Nodes with HA enabled.
     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 a virtual IP address in the following way:
     a) Enter the VIP Name.
     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 upon which the VIP should be placed, such as an aggregated link, VLAN link, or physical link.
  5. Click Create Service.

Note: If needed, additional VIPs can be configured for the service. See Adding a VIP
After associating a pool with an HA service, the pool table appears with a flashing yellow shield.

### Pools

<table>
<thead>
<tr>
<th>Pool Name</th>
<th>Health</th>
<th>Node</th>
<th>Configured Capacity</th>
<th>Allocated/Free</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alpha</td>
<td>online</td>
<td>node-10-170</td>
<td>3.5 TiB</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Allocated 500.9 GiB</td>
</tr>
<tr>
<td>Delta</td>
<td>online</td>
<td>node-10-175</td>
<td>1.8 TiB</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Allocated 40.2 GiB</td>
</tr>
<tr>
<td>HA_Pool</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Allocated 54.6 GiB</td>
</tr>
</tbody>
</table>

6. After service creation completes, the screen will refresh, and a green shield should be displayed, meaning the pool is ready to handle IOs.

**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.

### Adding an Unshared Pool to an 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**.

   ![ADD TO HA CONTROL: Beta](image)

   ![ADD TO HA CONTROL: Beta](image)

   - 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 Pool with Shared Devices, then click **Create Service**.

   ![ADD TO HA CONTROL: Beta](image)

5. After associating the pool with an HA service, the pool table will redisplay with a flashing yellow shield. After service update or creation completes, the screen will refresh, and a green shield should be displayed, meaning the pool is ready to handle IOs.

   **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.
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 click Appliance in the drop-down list.
2. In the Appliances List page, select the clustered appliance on which the HA service exists.
   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.
Moving a Pool under HA Service Control

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. The service, the pool, and any other pools that are managed by the service, are moved to the other node. You might move a pool that is under an HA service when the active node needs to be taken down for maintenance.

- **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.
  3. Select **Management > Pools**.
      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 a pool or multiple pools, a dialog appears. The text displayed on the dialog is different for just one pool, however.
  5. To move all pools managed by the service to the designated node, click **Yes**.

---

**Note:** Clients using the pool during migration will see a temporary suspension of IO while the failover is in progress.

---

**Warning:** When moving an HA service, all pools managed by the service must move together.

Are you sure you want to move the service Alpha and the following pools to node node-10-175?

- Alpha
- Beta

CANCEL YES
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 the VIP addresses are removed. Removing a pool from HA control has no effect on the service or the other pools the HA service manages, unless you remove the initial pool with which the service was created.

Warning: The HA service is destroyed when the initial pool (with the same name as the HA service) with which the service was created is removed from HA control.

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 HA service is stopped, the pools under its control remain in an exported state, but can be manually imported. 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.

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

![Destroy HA service dialog](image)

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

This section covers the following topics:

- Verifying Service Status
- Viewing VIPs Associated with an HA Service
- Adding a VIP
- Editing and Deleting a VIP
- Viewing Disk Heartbeats
- Viewing SCSI Reservation Details
- Failing Over Services Manually
- Moving an HA Service
- Setting the HA Service Mode
- Stopping and Starting an HA Service
- Destroying an HA Service

For information on how to configure an HA service in NexentaFusion, see Configuring an HA Service for a Pool with Shared Devices.
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. Select a service in the Service summary table.
   - The table entry will display the node that owns the service and the pools. The Unblocked parameter indicates whether or not the HA service is enabled to be started on the node.
5. Additional details for the service are displayed in tables beneath the service details label.

6. To update the data display, click Refresh in the upper right corner.
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 a cluster.
3. Select Management > High Availability.
4. Select Service Management.
5. Select the desired service in the Services summary table.
6. The first table in the Service details section shows the VIPs configured for the selected service.

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.

   After adding the VIP, the VIP information redisplay in the table with a COG on the far right.

**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.

**Viewing Disk Heartbeats**

- To view the disk heartbeats, 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, select the service.

5. To physically locate the device, click on **Show Indicators**.
   Clicking on “Show Indicators” will display a small icon reflecting the ident light led.

6. To locate the disk using the blink feature, click the **Ident LED** icon.

7. The Blink feature enables you to make the indicator for a specific disk bay blink.

**Viewing SCSI Reservation Details**

To view the state and physical location on the physical devices that are configured with SCSI reservations in a cluster, navigate to the following page.

- **To view the SCSI reservation details, do the following:**
  1. Log in to NexentaFusion and in the **Appliances List** page, select the cluster.
  2. Select **Management > High Availability**.
  3. Select **Service Management**.

   ![SCSI Reservation Table](image)

   4. To physically locate the device, click on **Show Indicators**.
      Clicking on the “Show Indicators” will display a small icon reflecting the ident light led.
   5. To locate the disk using the blink feature, click the **Ident LED** icon.
      The Blink feature enables you to make the indicator for a specific disk bay blink.

**Failing Over Services Manually**

This section demonstrates how to manually failover all services running on one node in a cluster to the other node. You would typically failover all services running on a cluster node (to the other cluster node) to perform maintenance on the node.

To move a specific service, and its associated pools, to a different node for load-balancing purposes, see [Moving an HA Service](#).

---

**Warning:** This procedure moves all services from the one node to the other.

- **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**.
  3. Select **Service Management**.
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**.

![Confirm failover dialog](image)

**Warning:** All services will be moved from the source to the destination node.

Select:
- **from node-10-170 to node-10-175**
- **from node-10-175 to node-10-170**

---

**Moving an HA Service**

This section demonstrates how to manually move a selected service to the alternate node in a cluster. You might want to move a specific service, and its associated pools, to a different node for load-balancing purposes.

You would typically failover all services running on a cluster node (to the other cluster node) to perform maintenance on the node. For more information, see [Failing Over Services Manually](#).

| Note: | Clients using the pool during migration will see a temporary suspension of IO while the failover is in progress. |

⚠️ *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**.

3. Select **Service Management**.

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**.

---
The service and the associated pools are 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.

- **Note:** Changing the service mode has no effect on the state of an active service.

- **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**.
  3. Select **Service Management**.
  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**.
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.

What Comes Next?

Chapter 11, 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/NexentaCloud 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 11-1: 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). For more information, see Viewing and Editing the Dashboard Canvas.</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>

Note: When logged in as a “viewer”, the Dashboard view and Analytics views is not subject to the “inactivity timeout”. This allows the dashboard to be displayed in a NOC-type of environment.
4. Continue with Using the Default Dashboard.

**Note:** 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.

![Graph of Pools Configured Capacity](image1)

• 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.

![Graph of NAS IO Performance](image2)

---

**Note:** Changes made from the drop-down menus on the Dashboard tab are temporary. The default values of the drop-down menus can be changed by editing the widget in the Analytics workspace. The Dashboard canvas displays summary information about the operational status of an appliance. For more information, see [Using the Analytics Workspace](#) and [Viewing and Editing the Dashboard Canvas](#).

---

**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 metrics of NexentaStor appliances in real time or historical time. These metrics are 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 11-1.

Figure 11-1: 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.

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

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 WidgetsAnalyzing Data.

Note: All canvases except the dashboard canvas are specific to the selected appliance and are visible to all users.
Managing Canvases

You can customize a canvas in a number of ways. This section demonstrates how to 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, and removing widgets.

- 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). The default Dashboard canvas is used for all appliances.

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—IO widgets provide real-time/historical IO metrics for pools, NFS or SMB shares, iSCSI or FC LUNs, IP Links, FC target ports and the cache hit rate of the appliance. The capacity utilization widget provides historical capacity utilization metrics for pools. You can load and save widgets with specific parameters to fine tune the monitoring of appliance performance. Performance widgets are not available on the dashboard. 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.

### Exporting Widgets to CSV

To use the data in an excel format, you can export widgets in the CSV format. When you export the widgets in the csv format, only the currently filtered data is exported.

- **To export widget data as CSV, 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 export the widget to CSV format, click the **COG** in the upper right corner of the widget and select **Export to CSV** from the drop-down list.

### 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 IO and capacity performance metrics aggregated over a specified period of time. IO Performance Widgets include the following:

- Cache Hit Rate
- CPU Utilization Performance
- FC LUN Performance
- FC Ports Performance
- IP Link Performance
- iSCSI LUN Performance
- NFS Share IO Performance
- Pool IO Performance
- SMB Share IO Performance

Capacity Utilization is a performance widget that charts historic pool capacity utilization.

The following procedure demonstrates how to view IO performance metrics aggregated for a specified time interval.

- To use the Performance widget to view metric data, do the following:
  1. Select one of the following time interval types over which to filter:
     - Real-time—Shows the last 30 minutes, and is updated every 15 seconds.
     - Historical time—Shows the "last N" choices.
     - Custom historical time—Specify a custom time range to view.
  2. Optionally, double-click the title to bring up a dialog to rename the widget.
  3. Select the object to chart (shares, LUNs, pools), and type an entry in the text field to filter the choices for selection.

Objects appear for the selection only after IO has been performed on the object.
4. Hover the cursor over the chart to view details about the IOs for that specific point in time.

5. When a historical time range is selected, 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.
   - Click on the focus timeline outside of the brush area to remove the brush, and display the entire time range in the chart.
   - Click and drag on the focus timeline to re-establish the brush to view a detailed segment of the time range.

Figure 11-2: Using an IO 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
• Graph color for threshold settings, when used space reaches a warning or error level

The capacity utilization performance widget provides historical capacity utilization metrics for pools, at a granularity of 1 day.

To use this widget, do the following:

1. Select the time interval.
   - Historical time – Show the last month, 6 months, or year
   - Custom historical time – Specify a custom time range to view
2. Select the pool to chart.
3. Optionally, double-click the title to bring up a dialog to rename the widget.
4. Hover the cursor over the chart to view the values for the metrics on that day:
   - Capacity: the total configured capacity of the pool.
   - Allocated: the allocated capacity includes the space reserved for data and protection.
   - Usage: this represents the capacity to which data has actually been written
5. Select EDIT from the widget COG drop-down list to change the capacity threshold line. By default, this line is drawn at 80% of the configured capacity.

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
• Top iSCSI LUNs
• Top NFS shares - % of Rate limit
• Top SMB shares - % of Rate limit

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

The Top NFS/SMB shares by % of Rate limit widgets include only shares whose underlying filesystem Rate limit property has been set to a non-zero value. You can edit this widget to further filter the shares to those within a rate limit range.

**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).
- **Data Reduction**—Shows the data reduction ratio for pools, not including dedupe reduction.
- **Installed Capacity**—Shows the sum of the disk sizes installed in the appliance.
- **Licensed Capacity**—Shows how much of the licensed capacity has been activated, and how much is still free.
- **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 allocated 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 each node of the NexentaStor appliance.
- **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.
This chapter covers the following topics:

- About Fusion Alerts, Logs, Audits, and Events
- Managing Fusion Alerts
- Managing Logs and Audits
- Creating Rules for Logs and Events
- Managing Appliance Alert Cases
- Troubleshooting Data Devices in a Pool
- Locating a Failed Disk
- Replacing a Failed Disk
- Using NexentaStor Virus Scan Service
- Managing Appliance Support Bundles

About Fusion Alerts, Logs, Audits, and Events

The Elasticsearch database (ESDB) 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.

Fusion alerts are generated by Fusion when a high-priority event or log meets the conditions specified in a Fusion rule. Fusion alerts can be reviewed on the Fusion Alerts view. 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. NexentaFusion has a set of default rules that generate alerts for high priority events and official logs. You can edit these rules to create email notifications, in addition to displaying the alerts in NexentaFusion.

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 LDAP server
- License compliance violations
- Lost connection between NexentaFusion and NexentaStor appliances

Audits record of NexentaFusion user 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. NexentaFusion has a set of default rules for generating alerts from events that require attention, such as a component has failed or a performance threshold has been reached. Appliance alert cases generate events that can be captured by Fusion to generate a Fusion alert.

Managing Fusion Alerts

The Fusion > Alerts page allows you to search for alerts, view and edit alert notification rules, acknowledge, and export alerts. This section covers the following topics:

- Searching for Alerts
- Acknowledging Alerts
- Expanding and Exporting Fusion Alerts
- Viewing and Editing an Alert Notification Rule

Searching for Alerts

The search fields at the top of the Alerts page allow you to search for alerts by message, query, and time range, with any of the following methods:

- Value—Enter a value from any field, such as: reboot
- Exact phrase or a value with special characters—Enclose an exact phrase, or a value that contains special characters, in double quotes, such as: “kernel panic” “node-10”
- Wildcard—Use the question mark (?) for single character wildcard searches, and an asterisk (*) for zero or more characters wildcard searches, such as: ale?t warn*g
- Field—Specify the fieldname:value, such as: hostname:”node-11”
- Boolean operations—Specify using the key words AND, OR, NOT, or the corresponding symbols &&, ||, !, such as: message: failed AND (severity:critical OR severity error)
- Time range—Select a time interval from the drop-down list, or specify a custom range.

To search for 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.
The **Alerts** page is selected by default.

3. Enter a value or boolean string in the **Search** field and press **Enter**.

4. To further refine the search, do one of the following:
   - Enter another value or boolean string in the **Search** field, and press **Enter**.
   - Select a time interval from the **Time range** drop-down list.

5. To search for alerts over a custom time range, do the following:
   a) From the **Time range** drop-down list, select **Custom Range**.
   b) In the pop-up calendar, use the arrows (< >) to navigate to the desired start and end months.
   c) On the left side of the calendar, click the start date, then select the start time (hour, minutes, seconds, AM/PM) from the drop-down lists.
   d) On the right side of the calendar, click the end date, then select the end time (hour, minutes, seconds, AM/PM) from the drop-down lists.
   e) Click **Apply**.
Acknowledging Alerts

When you acknowledge (ACK) an alert, the row changes to a lighter shade of gray and the ACK icon is replaced by a check mark. The visual changes provide an at-a-glance cue that you have viewed the data.

You can acknowledge (ACK) alerts individually, by select group, by the visible alerts on the screen, or all alerts that have not yet been acknowledged.

To acknowledge alerts, do the following:

1. Log in to NexentaFusion and select Fusion from the main drop-down menu. The Alerts page is selected by default.

2. To acknowledge a single alert, click the ACK icon on the far right. The row changes to a lighter shade of gray and the ACK icon is replaced by a check mark.

3. To find a specific group of alerts to acknowledge, follow the steps in Searching for Alerts.

4. To acknowledge all the alerts that are currently visible on the screen, click ACK visible alerts.

5. In the confirmation dialog, click Yes. The alerts visible on the screen turn a lighter shade of gray, and the ACK icons on the right are replaced with check marks.

6. To acknowledge all the alerts, not just the visible ones, click ACK ALL alerts.
Expanding and Exporting Fusion Alerts

This section demonstrates how to expand alerts to view complete messages, and then export a select group to a comma-separated values (CSV) file. You define the group of alerts to be exported with query and time range parameters.

To expand and export alerts, do the following:

1. Log in to NexentaFusion and select Fusion from the main drop-down menu.
   The Alerts page is selected by default.

2. To view complete alert messages, do the following:
   a) Click Expand all messages.

   ![Expand all messages button]

   b) Click an underlined message to view a dialog with additional information about the alert.

   ![Alert message dialog]

   c) Click the X in the upper right corner to hide the dialog.
3. Define the group of alerts to be exported using query and time range parameters, as described in **Searching for Alerts**.

4. To save the alerts in tabular file format, click **Export as CSV**.

   The alerts data is exported into comma-separated tabular format, such as the following example.

   

   ```
   class: fault#hs#zfs#vdev#not_spared
   location:
   Slot 11
   fru:
   http://product-id=LSI-CORP-SAS2X36:server-id=chassis-id=50030480016c9f3fserial=Z1W321RE0000C516
   GLNT:part=SEAGATE-ST1000NM0023:revision=0004/ses-
   enclosure=0/bay=10/disk=0
   state:
   faulty
   ```

   **d)** To hide the messages, click **Collapse all messages**.
Viewing and Editing an Alert Notification Rule

This section demonstrates how to view and modify the notification rule for a selected alert. For more information on notification rules, see Creating Rules for Logs and Events.

To view and edit an alert notification rule, do the following:

1. Log in to NexentaFusion and select Fusion from the main drop-down menu. The Alerts page is selected by default.
2. On the right, click the View icon for the alert. The Edit Logs or Events Notification Rule dialog appears.
3. View the notification rule for the alert, and make modifications to the options as described in Creating Rules for Logs and Events, and click Save.

Note: Fusion alerts with the name “Appliance error alert generated” or “Appliance warning alert generated” will have a corresponding alert case on the Support view for the appliance identified in the Fusion alert. See Managing Appliance Alert Cases for more information.

Managing Logs and Audits

NexentaFusion displays the logs and audit in a tabular format with messages displayed in reverse chronological order. You can search for a select set of logs or audits, and export the results to a comma-separated values (CSV) file.
You can control what level of logs are persisted for each appliance from the appliance Administration > Data Settings screen.

This section covers the following topics:

- Searching for Logs and Audits
- Expanding and Exporting Audits and Logs

Searching for Logs and Audits

The search fields at the top of the Logs and Audit pages allow you to search by message, query, and time range, with any of the following methods:

- **Value**—Enter a value from any field, such as: reboot
- **Exact phrase or a value with special characters**—Enclose an exact phrase, or a value that contains special characters, in double quotes, such as: “kernel panic” “node-10”
- **Wildcard**—Use the question mark (?) for single character wildcard searches, and an asterisk (*) for zero or more characters wildcard searches, such as: node1? warn*g
- **Field**—Specify the fieldname:value, such as: hostname:“node-11”
- **Boolean operations**—Specify using the key words AND, OR, NOT, or the corresponding symbols &&, ||, !, such as: message: failed AND (severity:critical OR severity error)
- **Time range**—Select a time interval from the drop-down list, or specify a custom range.

To search for logs and audits, do the following:

1. Log in to NexentaFusion.
2. Select FUSION from the drop-down list in the top left corner of the window. The Alerts page is selected by default.
3. 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.
4. Enter a value or boolean string in the Search field and press Enter.
5. To further refine the search, do one of the following:
   • Enter another value or boolean string in the Search field, and press Enter.
   • Select a time interval from the Time range drop-down list.

6. To search for alerts over a custom time range, do the following:
   a) From the Time range drop-down list, select Custom Range.
   b) In the pop-up calendar, use the arrows (< >) to navigate to the desired start and end months.
   c) On the left side of the calendar, click the start date, then select the start time (hour, minutes, seconds, AM/PM) from the drop-down lists.
   d) On the right side of the calendar, click the end date, then select the end time (hour, minutes, seconds, AM/PM) from the drop-down lists.

7. Click Apply.

Expanding and Exporting Audits and Logs

This section demonstrates how to expand alerts to view complete messages, and then export a select group to a comma-separated values (CSV) file. You define the group of alerts to be exported with query and time range parameters.

❖ To expand and export audits and alerts, do the following:
   1. Log in to NexentaFusion and select Fusion from the main drop-down menu.
      The Alerts page is selected by default.
   2. Select FUSION from the drop-down list in the top left corner of the window.
The Alerts page is selected by default.

3. 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.

4. Do one of the following:
   - For Logs, click **Expand all messages**.
   - For Audit, click **Expand all urls**.

   To hide the messages, click **Collapse all**.

5. Define the group of alerts to be exported using query and time range parameters, as described in Searching for Logs and Audits.

6. To save the audits or logs in tabular file format, click **Export as CSV**.
   The data is exported into comma-separated tabular format.
Creating Rules for Logs and Events

NexentaFusion Rules are used to display alerts and generate email notifications. Email notifications are enabled by default. 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 (See note below)</td>
<td>Generates an alert when Fusion receives an event indicating that a specific appliance alert case has been resolved.</td>
<td>Warning</td>
</tr>
<tr>
<td>Appliance error alert generated (See note below)</td>
<td>Generates an alert when Fusion receives an event indicating a case with severity major or critical has been diagnosed on the appliance.</td>
<td>Error</td>
</tr>
<tr>
<td>Appliance reboot needed — firmware change</td>
<td>Generates an alert when there is a 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 (See note below)</td>
<td>Generates an alert when Fusion receives an event indicating a case with severity minor has been diagnosed on the appliance.</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>Data Protection service scheduled start missed</td>
<td>Generates an alert when HPR created a scheduled snapshot but replication of that snapshot was not started because another snapshot is being already replicated.</td>
<td>Warning</td>
</tr>
<tr>
<td>Data Protection scheduled replication service snapshot skipped</td>
<td>Generates an alert when a replication snapshot is skipped. This can occur, for example, during a period of intermittent network congestion, until replication automatically “catches-up”.</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—emergency severity</td>
<td>Generates an alert when an emergency message appears in a log. This rule can be disabled.</td>
<td>Error</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 for events that match rule criteria, and immediately generates an alert with the specified severity of error or warning when one occurs.

Note: You have the option of having the appliance generate an email notification when an alert case is created, or having Fusion generate the email notification. The appliance will generate the email if the appliance’s Alert Emails address is set. See Editing System Configuration Settings.

You can modify default rules to disable email notifications, restrict the email notification to be sent to a specific set of recipients, and disable rules as needed. Disabling rules can be useful during system maintenance, to prevent unnecessary alerts from being generated.

- **To activate/deactivate a rule, or enable/disable e-mail notifications:**
  1. Log in to NexentaFusion and select FUSION from the drop-down list in the upper left corner of the window. Under Notifications, select Rules.
  2. To deactivate a rule, uncheck the Active check box for the rule.
  3. To disable e-mail notifications, uncheck the Email check box for the rule. Email notification is enabled by default for all rules, to email the recipients configured on the NexentaFusion Email Setup view. See Setting the NexentaFusion SMTP Mail Server (Email Setup).

- **To create or edit an event or log 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.

<table>
<thead>
<tr>
<th>Default Rule Name</th>
<th>Description</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<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.</td>
<td>Warning</td>
</tr>
<tr>
<td>Syslog entry—error severity</td>
<td>Generates an alert when an error severity message appears in a log.</td>
<td>Warning</td>
</tr>
</tbody>
</table>
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 Log or Event Message in the text field.
   Search for alerts by message, query, and time range, with any of the following methods:
   - **Value**—Enter a value from any field, such as: reboot
   - **Exact phrase or a value with special characters**—Enclose an exact phrase, or a value that contains special characters, in double quotes, such as: *"kernel panic" "node-10"*
   - **Wildcard**—Use the question mark (?) for single character wildcard searches, and an asterisk (*) for zero or more characters wildcard searches, such as: *"ale?t warn*g*
   - **Field**—Specify the fieldname:value, such as: **hostname:“node-11”**
   - **Boolean operations**—Specify using the key words **AND**, **OR**, **NOT**, or the corresponding symbols &&, ||, !, such as: **message: failed AND (severity:critical OR severity error)**
   - **Time range**—Select a time interval from the drop-down list, or specify a custom range.

5. **Enable e-mail notifications** - by default this feature is enabled
All the recipients you added (under **Recipients**) when configuring the email setup for NexentaFusion will be notified in case of an alert/event. See [Setting the NexentaFusion SMTP Mail Server (Email Setup)](#).

6. Alternatively, if you want to restrict the alert/event emails-notification to be sent to a specific set of recipients, check **Send alerts only to the following recipients** field and enter the email addresses of the recipients.

7. Click **Save**.

### Managing Appliance Alert Cases

The appliance has the ability to detect hardware and software problems, or a transient condition (for example, CPU over-utilization). Each problem is represented by an alert case that is referenced by a unique UUID. These cases can be viewed under the Support tab of the selected appliance. You may view all active alert cases, search the history of all cases, and acquit a case.

In order to receive email notifications of the active detected issues directly from the appliance, you must properly configure the SMTP mail server. You can test and modify the SMTP mail server for the appliance using the **Support** interface.

Using the **Support settings**, you can change common appliance configuration settings for the selected NexentaStor appliance.

**Note:** NexentaFusion rules will generate a Fusion alert when it receives the event that an appliance alert case has been generated, and can optionally generate an email notification. See the rules with the names “Appliance ... alert...” on [Creating Rules for Logs and Events](#).

### View Active Cases Detected by the Appliance

- **To view the list of active cases:**
  1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
  2. In the **Appliances List** menu, select an appliance.
  3. Click **Support**.
By default, this displays all the active cases that are active and have not been repaired, resolved, or acquitted. This view also displays the main COG to configure appliance emails, and individual COGS to acquit alerts.

- To view the details of a specific active case:
  1. Select the active case for which you want to view the details.
  2. Click on its COG.
  3. Click Details from the drop down action items.

- To view the details of a specific active case in a report format:
  4. Click Reports from the drop down action items.

- To acquit:
  5. Click Acquit to acknowledge a failing case and mark it as resolved.

- To mark a case as repaired:
  6. Click Mark as repaired to notify the system that the faulty resource has been repaired.

- To mark as replaced:
  7. Click Mark as replaced to notify the system that the faulty resource has been replaced.

### View Historical Cases

Using the steps below you can view all cases including the ones that are resolved.

1. Log in to NexentaFusion and click Appliance in the drop-down list.
2. In the Appliances List menu, select an appliance.
3. Click Support/Alert Cases.
4. Click **All Cases**.
5. Optionally use the Filter to restrict the cases being displayed.

- **To view the details of a specific historical or non-active case:**
  1. Select the case for which you want to view the details.
  2. Click on its COG.
  3. Click **Details** from the drop down action items.

- **To view the details of a non-active case in a report format:**
  4. Click **Reports** from the drop down action items.

### Using DISK View to View an Active FMA Case

From the components view, you may view the active alert case with a severity of Critical or Major or Minor. An active alert case with a severity of Critical or Major is displayed with the red "stop sign" icon and a case with a severity of Minor is displayed with the triangular "yield" warning icon.

In the case of a cluster, the components view shows separate enclosure views for each node. For the enclosures that are accessible by both nodes, the alert icon is displayed if an FMA alert has been generated on either node for a specific disk. If you have both NodeA and NodeB in a cluster, and an FMA alert is generated for NodeB for device X, you can view the alert icon on the components view on device X when viewing NodeA as well as when viewing NodeB.

If multiple alert cases exist for a device, the icon for the highest severity is displayed.

- **To view the details of the alert cases:**
  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**. If the appliance is clustered, select the node you want to view.
  4. To view chassis devices in graphical or tabular mode, select the appropriate icon.
  5. To filter, make selections from the drop-down lists. To clear the filter, click the “x” from the drop-down lists.
  6. Click on the **Alert** icon to view the details of the alert cases.
  7. Click on the case ID in the Alert cases window for the **All Cases** view.
Using DISK Case Details to Locate the Problem Device

Most alert cases whose Code begins with “DISK” will have additional text in the Details to help identify the device with the issue. Click on the circles under Enclosure and Bay to enable/disable the chassis and bay device ident LEDs. Click on the Show Diagram button to display a graphical representation of the enclosure, with the problem device highlighted.
Fault Management

case ID: e1c0528c-3962-3ee2-c2e5-fac53c86e92e
diagnosed: Wed May 09 2018 17:42:32 GMT-0700 (Pacific Daylight Time)

code: DISK-8000-6R
severity: critical

faulty: true
description: A disk device has experienced too many device errors.
nodeld: 6c0f50c7

node: node-10-175

Suspects

Logical device: cb5000c5008de4f917d0

Location: 5f6b82fe1af3b068

State: RETIRED

Enclosure

Bay: HDD 8

SHOW DIAGRAM  CLOSE

Enclosure

HDD 0  HDD 1  HDD 2  SSD 3
HDD 4  HDD 5  HDD 8  SSD 7
HDD 9  HDD 10  HDD 11

SHOW CONNECTION DETAILS  HIDE INDICATORS  CLOSE
Typically, devices that are flagged with an appliance alert case will also show an error indication on the Components view. See Viewing and Locating Chassis Devices.

**Configure SMTP Settings and Alert Settings**

Dialogs to configure SMTP Settings for generating email alerts directly from the appliance, and Alert Settings for configuring certain alert thresholds, can be accessed from the COG on the upper right. Select SMTP Settings or Alert settings to invoke the same dialogs as are available on the Administration/System Configuration Settings view.

See [Editing System Configuration Settings](#) for details on configuring SMTP settings.

**Set up Warning and Error Alert Threshold Settings**

Using this feature you can enter the desired threshold criteria values for the CPU and Network alerts and also configure the email address to send the notifications to. See [Editing System Configuration Settings](#) for details on configuring the threshold criteria values for the CPU and Network alerts.

**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. To locate the failed disk using the blink feature, click **Show Indicators**.

7. 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.

8. After identifying the type of error in the device, take the required actions, as described in **Replacing a Failed Disk**.

### 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. Blinking the LED for a slot or a drive will implicitly blink the LED of the chassis.

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

**Note:** Using this LED blinking feature, you can also locate the empty slot in a storage enclosure.
Replacing a Failed Disk

With auto-replace, the failed device can be simply removed and physically replaced with a new device. NexentaStor automatically detects the insertion of the new device and triggers re-silvering to the new device.

If a spare was configured for the pool, the spare was activated to replace the failed device. Replacing the failed device will trigger another resilver from the spare to the replacement device. When it is complete, the former spare will revert to being a spare.

An alternative is to make the spare the permanent replacement member of the pool, to eliminate a second resilvering. Using the Edit Pool dialog, click on the image of the failed device, and select “Detach” from options on the device COG.
Using NexentaStor Virus Scan Service

About NexentaStor vsan

To use the NexentaStor vsan service using NexentaFusion, you must set-up a third-party VirusScan engine like McAfee on an external host to perform virus scanning operations on files. You may configure multiple scan engines for use by the NexentaStor vsan service. When you use multiple scan engines the file scan requests are distributed among the configured scan engines to balance the load. NexentaStor will issue a scan request to the virus scan engine every time an open/close operation request is issued from the client to the NAS platform.

This section describes how to use McAfee VirusScan Enterprise as a virus scan engine with the NexentaStor Appliance vsan service.

Prerequisites

To enable virus scanning services with NexentaStor, the following items need to be in place:

- A 3rd-party virus scanning engine that supports ICAP (for example, McAfee) installed on a server.
- A port available in NexentaStor to communicate with the virus scan engine. The vsan service on the NexentaStor appliance uses port 1344 by default.

Managing Virus Scan Services on a NexentaStor Appliance using NexentaFusion

- **Using NexentaFusion, set up the vsan service on the NexentaStor 5.x appliance:**
  1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
  2. In the **Appliances List** page, select the appliance for which you must configure the Virus scan service.
  3. Select **Administration > System Settings**.
  4. Under **System Services**, click the **COG** for the Virus scan service.
  5. Enable the virus scan service by clicking on **Enable** that is listed under the **COG**.
  6. Now query and set virus service attributes by clicking on **Properties** listed under the **COG**.
  7. In the Virus Scan Service Properties window, set the following:
     - **5) In Maximum File Size**, type the maximum size of files that should be virus scanned.
     - **6) In Files Access**, specify whether access will be allowed or denied to files larger than max-size.
7) In **File Types**, list all the file type extension matching rules, using commas as separators.

- **Using NexentaStor CLI, configure vscan on the NexentaStor appliance to point to the McAfee virus scan engines IP address.**

  1. Once you set up the Virus Scan Engine (VSE) in your environment, configure vscan on the NXS 5 node to point to the McAfee scanner through our “vscan” command.

```
CLI@nexenta> vscan set host=10.3.53.119 <vscan engine ID>
```

- **Enable the virus scan option on the filesystem share you want checked for viruses.**

  1. In the **Appliances List** page, select the appliance on which the filesystem exists.
  2. 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.
  3. To only view data for a specific pool, select a Pool from the drop-down list. The default is to show all pools.
  4. To view the entire file system structure, click the arrows on the left of the table header.
  5. To view the list of file systems in a pool, click the expander arrow next to the pool name.
  6. To view file system properties, click the COG for a file system and select **Edit properties**. A dialog appears showing the editable properties.
  7. Click **Optional Settings**.
  8. In the drop down list of **Enable virus scanning**, select **True**.

Now that you have enabled the vscan service on the filesystem, you can mount the NFS/CIFS share and create/access data on that share from a different client machine. This will trigger the McAfee scans.

### Managing Appliance Support Bundles

A support bundle (SB) is an archive containing important system information for Nexenta support service (i.e. core dumps, system configuration files, system logs and so on).

The bundle file name contains the license, hostname and the bundle creation timestamp that helps to easily locate and identify which systems a bundle was generated from.

### Create a Support Bundle

You can create a bundle as a compressed archive on your system. A generated universally unique identifier (UUID) is displayed to reference the created bundle.

1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
2. In the **Appliances List** menu, select the appliance that you want to create a support bundle.
3. Click **Support**.
4. Click on the sub-tab **Support Bundles**.
   The Support Bundle view will display a table that contains the bundle information from both nodes, if the appliance is clustered.

5. Click **Create Support Bundle**.

6. In the case of a clustered appliance, select the appliance on which the support bundle is to be created.

**Identify and Include the Core Files to Support Bundle**

7. With the improved version of Core and crash dump management in NexentaStor, you have the following advantages:
   - You can include the cores in the support bundle (SB), only if you need to, which means the cores are not included in the support bundle by default.
   - You can also identify and select the cores associated with a specific problem to be included in the support bundle. This filtering of cores will speed up the upload of the support bundle. This also implies that the cores will not be removed from the NexentaStor appliance by default.

8. Click **Create**.

**Delete Core Files**

9. You also have an option to remove duplicate cores without having to create a bundle with all of them. Select the bundle you want to remove and click on its **COG**.

10. Click **Remove bundle**.

**Download the Bundle Locally**

In the absence of an internet connection from the NexentaStor node to the Support server or if you are unable to upload bundle to the Support server, you can download the appliance support bundles locally directly from NexentaStor appliance by following these steps. By default the download option is set to false. First you must enable the download option to download the bundle.

- **To enable the download option:**
  1. Under the **Support Bundles** tab, click on the COG next to the Create Support Bundle + button.
  2. Click Edit download enabled.
  3. Toggle the Download enabled button to Yes.

- **To download the bundle:**
  1. Under the **Support Bundles** tab, select the bundle that you want to download.
  2. Click on its **COG**.
  3. From the drop down list, click **Download bundle**.
Default Support Bundle Protocol and Settings

By default, support bundles are uploaded via the S3 protocol to Nexenta servers. By default, S3 uploads use parallel upload for maximum throughput performance, and faster uploads. You can verify bundle upload settings by querying the support config options.

Modify Default Settings for Slow Connections

If you are experiencing upload failures or have a slow network connection to Nexenta support servers, you should enable sequential S3 uploads (implicitly disabling parallel upload).

Upload Support Bundles to Nexenta's https Server

You can upload support bundles to Nexenta's https server. This operation may take a long time depending on size of the bundle and your internet connection speed.

1. Under the Support Bundles tab, select the bundle that you want to upload.
2. Click on its COG.
3. From the drop down list, click Upload bundle.