NexentaStor 5.0 vCenter Plugin
QuickStart Guide

Date: March, 2017
Part Number: 9000-vcenter-5.0-000002-A
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>1</td>
</tr>
<tr>
<td>1 Configuring NexentaStor 5.0 Appliances</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Deploying NexentaStor vCenter Plugin</td>
<td>3</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>4</td>
</tr>
<tr>
<td>Installing the vCenter Plugin</td>
<td>4</td>
</tr>
<tr>
<td>Registering a NexentaStor Appliance</td>
<td>5</td>
</tr>
<tr>
<td>Navigating the vCenter Plugin Interface</td>
<td>6</td>
</tr>
<tr>
<td>Monitoring NexentaStor Appliance Health</td>
<td>8</td>
</tr>
<tr>
<td>Configuring Multi-Tenancy</td>
<td>9</td>
</tr>
<tr>
<td>Upgrading the vCenter Plugin</td>
<td>11</td>
</tr>
<tr>
<td>Uninstalling the vCenter Plugin</td>
<td>11</td>
</tr>
<tr>
<td>2 Managing NexentaStor Appliances with vCenter Plugin</td>
<td>12</td>
</tr>
<tr>
<td>Managing Filesystems</td>
<td>12</td>
</tr>
<tr>
<td>Adding and Configuring Pools</td>
<td>12</td>
</tr>
<tr>
<td>Creating Filesystems</td>
<td>12</td>
</tr>
<tr>
<td>Sharing Filesystems</td>
<td>13</td>
</tr>
<tr>
<td>Prerequisites for Creating Volumes and Datastores</td>
<td>14</td>
</tr>
<tr>
<td>Creating an iSCSI Target</td>
<td>14</td>
</tr>
<tr>
<td>Creating a Target Group</td>
<td>15</td>
</tr>
<tr>
<td>Managing Volumes</td>
<td>15</td>
</tr>
<tr>
<td>Managing Datastores</td>
<td>16</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>16</td>
</tr>
<tr>
<td>Creating and Deleting Datastores</td>
<td>16</td>
</tr>
<tr>
<td>Managing Scheduled and Unscheduled Snapshots</td>
<td>18</td>
</tr>
<tr>
<td>Managing Manual Snapshots Independent of a Protection Service</td>
<td>19</td>
</tr>
<tr>
<td>Managing Scheduled Snapshots Using a Data Protection Service</td>
<td>21</td>
</tr>
</tbody>
</table>
3 Protecting Data .................................................23
  Data Protection Services .....................................23
  Managing Protection Services .................................25
  Viewing Protection Service Status ............................29
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 Network Storage Administrators and assumes that you have experience with virtualization and data storage concepts, such as NAS, SAN, NFS, and ZFS.

Documentation History

The following table lists the released revisions 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>9000-vcenter-5.0-000002-A</td>
<td>March, 2017</td>
<td>GA</td>
</tr>
</tbody>
</table>

Contacting Support

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

Comments

Your comments and suggestions to improve this documentation are greatly appreciated. Send any feedback to doc.comments@nexenta.com and include the documentation title, number, and revision. Refer to specific pages, sections, and paragraphs whenever possible.
Configuring NexentaStor 5.0 Appliances

This chapter covers the following topics:

- **Introduction**
- **Deploying NexentaStor vCenter Plugin**
- **Upgrading the vCenter Plugin**
- **Uninstalling the vCenter Plugin**

**Introduction**

The NexentaStor 5.0 vCenter Web Client Plugin (vCenter Plugin) enables VMware customers to configure and manage storage and virtualization through a single interface. With this plugin, system administrators avail of summary and detailed analytics and real time status monitoring of single and clustered NexentaStor appliances. It simplifies day-to-day operational tasks in a virtual environment by allowing you to:

- Configure and incrementally scale your storage infrastructure by adding datastores using a point and click interface.
- Identify performance bottlenecks and review capacity utilization trends for single or clustered nodes.
- Quickly adapt to changing data protection needs through on-demand and scheduled snapshots and replication services.
- Increase security through integration with vCenter’s role-based authentication mechanism.

**Deploying NexentaStor vCenter Plugin**

This section demonstrates how to deploy the NexentaStor vCenter Plugin, and covers the following topics:

- The prerequisites for a successful plugin deployment.
- Instructions on how to download and install the plugin.
- Registration of the NexentaStor appliances you want to manage in vCenter.
- Verification of your plugin installation.
- Commands to upgrade vCenter plugin versions in the future.
Prerequisites

Before you begin Installing the vCenter Plugin, verify that your environment meets the following requirements:

- Enabled SSH service on the VCSA.
- User credentials of the root account for VCSA.
- Any of the following configured and licensed vCenter Servers—6.0, 6.0U1, 6.0U2, 6.5 or VCSA 6.0 6.0U1, 6.0U2, 6.5.
- NexentaStor 5.0 appliances pre-configured with pools. To manage NexentaStor HA clusters and replication services using this vCenter plugin, these appliances must be activated with the High Availability (HA) and High Performance Replication (HPR) optional feature licenses. For more information, see the NexentaStor 5.0 CLI Reference Guide and NexentaStor 5.0 HA Admin Guide.
- Network connectivity between vmWare vCenter host and the NexentaStor appliances.
- Any of the following supported browsers—Chrome or Firefox browser versions compatible with the vCenter web client.

Note: You must have vSphere administrator privileges to install the NexentaStor 5.0 vCenter plugin.

Installing the vCenter Plugin

This section demonstrates how to perform an initial installation of the vCenter Plugin for Windows and Linux environments. You should have already verified that your system meets the necessary Prerequisites.

Windows Environment

To install the vCenter Plugin on Windows, do the following:

1. Download the NSVP-vCenter-Installer-5.0.xxxx.msi file from the NexentaStor 5.0 download site, and copy the file over to vCenter server.
2. Log in to the vCenter Windows Server, and run the Web Client Plugin installer file.
3. Complete the Windows Installation Wizard:
   a) Verify the environment prerequisites.
   b) Read and accept the End User License Agreement (EULA).
   c) Verify the destination installation folder.
   d) Enter the vCenter credentials.
   e) Click Install, then Finish.
4. After the vCenter plugin is installed, re-log in to the vSphere Web Client.
5. Continue with Registering a NexentaStor Appliance.
Linux Environment

To install the vCenter Plugin on Linux, do the following:

1. Download the nsvp-vcsa-installer-5.0.xxxx.tar file from the NexentaStor 5.0 download site.
2. Log in to the VCSA as root using SSH.
3. Enable BASH access with "shell.set --enabled True" command:
   
   ```shell
   Command> shell.set --enabled True
   ```
4. Run shell:
   
   ```shell
   Command> shell
   ```
5. Create and change directory to upload the installation files:
   
   ```bash
   localhost:~ # mkdir nsvp && cd nsvp
   ```
6. Copy downloaded nsvp-installer-5.0.xxxx.tar from remote host using scp, wget or curl:
   
   ```bash
   localhost:~/vasa # scp remote_host:nsvp-installer-5.0.xxxx.tar .
   ```
7. Extract the contents from the archive by typing the following command:
   
   ```bash
   localhost:~/vasa # tar -xvf nsvp-installer-5.0.xxxx.tar
   ```
8. Optionally, run the help command to view the installation command:
   
   ```bash
   localhost:~/vasa # ./install.sh --help
   ```
9. Run the following command to install:
   
   ```bash
   localhost:~/nsvp # ./install.sh --action install --vcuser administrator@vsphere.local
   ```
10. After the vCenter plugin is installed, re-log in to the vSphere Web Client.
11. Continue with Registering a NexentaStor Appliance.

Registering a NexentaStor Appliance

To establish a connection between the vCenter management framework and the storage appliances that you want to manage, the first post-installation step is to register the NexentaStor 5.0 nodes. You can either register a clustered appliance or a single node.

To register a clustered appliance, you must have already created a VIP address for the cluster using the NexentaStor CLI beforehand. For more information, see the NexentaStor 5.0 HA Admin Guide.

| Note: | The NexentaStor user name used in the following procedure must have (superuser) privileges to execute REST API requests. |

To register a NexentaStor appliance, do the following:

1. Log in to https://<vCenter_ip>:9443/vSphere-client/.
2. Optionally, modify the vCenter server parameters, as follows:
   a) Click Home then click on the Nexenta Storage Systems icon on the right frame.
   b) In the Configuration window, click on the Settings tab.
   c) As needed, edit the protocol and the vCenter IP address with your vSphere credentials.
   d) Modify the Tenancy mode.
   e) Click Save.

3. Before registering a NexentaStor appliance in vCenter, verify the following setting using the NexentaStor CLI.
   
   CLI@host> config list rest.httpsProtocol
   This command should display a value of TLS1.x which is the default value.
   
   NAME   FLAGS    VALUE
   rest.httpsProtocol   --   TLS1.x
   
   If not, reset it to TLS1.x.
   CLI@host> config set rest.httpsProtocol=TLS1.x

4. To register a single (unclustered) node, do the following:
   a) Go to Home > Nexenta Storage Systems icon.
   b) Go to NexentaStorage Systems > Objects.
   c) Click the Register NexentaStor Appliance icon.
   d) Fill in the required fields.
   e) Click Register.
   If you inadvertently register a node as a single node that is actually a member of a cluster, the registration will fail.

5. To register a clustered pair of appliances, do the following:
   a) Go to Home > Nexenta Storage Systems icon.
   b) Go to NexentaStorage Systems > Objects.
   c) Click the Register NexentaStor Appliance icon.
   d) Select the HA Cluster check box, and provide the IP address of both the nodes in the cluster.
   e) Enter the Management IP address or the hostname.
   f) Enter the NexentaStor user and password for both nodes for REST API authentication.
   g) Fill in the required fields.
   h) Click Register.
   If you inadvertently register a single unclustered node as a member of a cluster, the registration will fail.
In both cases, the NexentaStor username you entered must have privileges to execute REST API requests.

6. Continue with Navigating the vCenter Plugin Interface.

Navigating the vCenter Plugin Interface

After deploying the vCenter plugin and registering the appliances, you can perform the following tasks to verify your installation and also orient yourself by navigating through the vCenter user interface (UI):

- Access and view the Nexenta Plugin Manager dashboard.
- Get a list of the registered NexentaStor appliances. Once you have registered a clustered NexentaStor appliance or a single node appliance, the NexentaStor appliance list is immediately populated and is displayed.
- View software license and version for each registered appliance.
- Access the system logs.

To use the vCenter UI to for NexentaStor appliances, do the following:

1. Access the vCenter dashboard, in the following way:
   a) Open a Web browser and enter the following URL: https://<vCenter_ip>:9443/vsphere-client/
   b) Enter your administrator credentials to log in.
   c) On the Home page, click the Nexenta Storage Systems icon.

Once you have registered a clustered NexentaStor appliance or a single node appliance, the NexentaStor appliance list is immediately populated and is displayed.

2. To view the list and status of the registered NexentaStor appliance(s), go to Dashboard > Summary tab. The newly populated list of appliances shows the following information:
   - Status—The health status of the appliance.
• Configured capacity—The sum of the free capacity and the used capacity of the pool after setting the redundancy type (RAID / mirror).
• Installed capacity—The sum of disk sizes installed in the appliance.

3. View the appliance license and version in the following way:
   a) In the left frame click **Nexenta Storage Systems**, and select an appliance from the drop-down list.
   b) Click the **Monitor** tab.
   c) Click the **Hardware** subtab.

4. View the system logs in the following way:
   a) On the Home page, click the **Nexenta Storage Systems** icon.
   b) In the left frame click **Dashboard**.
   c) Click the **System Logs** tab.
   d) Select a log from the list to view the contents.
   e) You can also export the system logs by selecting one from the drop down box and by clicking **Export System Logs** button.

**Monitoring NexentaStor Appliance Health**

Several views are available to monitor the system health of a single node or a clustered appliance.

- To view the health summary, navigate to the following interface:
  1. Click the Nexenta Storage Systems pulldown menu from the left frame.
  2. Select the appliance you want to view.
  3. Click the Monitor tab.
Table 1-1: Health Monitoring Views

<table>
<thead>
<tr>
<th>Role</th>
<th>Access Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Health summary</td>
<td>To get the health summary of all the services for each NexentaStor appliance:</td>
</tr>
<tr>
<td></td>
<td>◆ Click the Service Health subtab.</td>
</tr>
<tr>
<td></td>
<td>You will see the list of pools, appliance services, and HPR replication services running on the appliance.</td>
</tr>
<tr>
<td>Hardware health status</td>
<td>To view the hardware health status of individual NexentaStor appliances:</td>
</tr>
<tr>
<td></td>
<td>◆ Click Hardware subtab.</td>
</tr>
<tr>
<td></td>
<td>The vSphere Web Client display will show hardware information such as the node’s CPUs, network adapters, disks, enclosures, and adapters.</td>
</tr>
<tr>
<td>Performance bottlenecks</td>
<td>To view the performance metrics of individual NexentaStor appliance that can indicate performance bottlenecks:</td>
</tr>
<tr>
<td></td>
<td>◆ Click Performance subtab.</td>
</tr>
<tr>
<td></td>
<td>The chart displays the following metrics. In the case of a clustered appliance, the metrics on both the nodes are displayed.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Aggregated metrics for a single or a clustered pair of appliance</td>
<td>◆ In the case of a clustered appliance, clicking on the Summary tab returns statistics for both member nodes as shown in Figure below.</td>
</tr>
<tr>
<td></td>
<td>The resulting display shows the CPU utilization, network usage, cache hits, data reduction factors, number of volumes and filesystems.</td>
</tr>
</tbody>
</table>

Figure 1-1: Clustered Appliance View
Configuring Multi-Tenancy

A tenant is a group of users who share common access and privileges to the software. The NexentaStor vCenter Plugin uses multitenant architecture, which enables you to:

- Provide multiple tenants with role-based access to the NexentaStor 5.0 appliance.
- Limit access to data, configuration, and user management on a per-tenant basis.

As the vCenter Plugin administrator, you are a superuser with privileges to manage all aspects of storage arrays, tenancy, and access control. Below are instructions on how to enable multi-tenancy and assign the tenant different user roles. Table 1-2, Role-Based Access Controls summarizes the tenant roles and corresponding access rights.

Table 1-2: Role-Based Access Controls

<table>
<thead>
<tr>
<th>Role</th>
<th>Access Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant Administrator</td>
<td>— Rights as a File Systems Administrator</td>
</tr>
<tr>
<td></td>
<td>— Rights as a Backup Administrator</td>
</tr>
<tr>
<td></td>
<td>— Rights as an Administrator for NexentaStor appliances in a given tenant</td>
</tr>
<tr>
<td>File Systems Administrator</td>
<td>— Rights to create, modify, and delete SMB/NFS shares</td>
</tr>
<tr>
<td></td>
<td>— Rights to create, modify, and delete volumes</td>
</tr>
<tr>
<td>Backup Administrator</td>
<td>— Rights to create and schedule snapshots</td>
</tr>
<tr>
<td></td>
<td>— Rights to create and run backups</td>
</tr>
<tr>
<td>Read-Only User</td>
<td>— Read-only access to the NexentaStor appliance</td>
</tr>
</tbody>
</table>

To enable and configure multi-tenancy, do the following:

1. In the left Navigator pane, click **Configuration**.
2. Select the **Setting** tab.
3. From the Tenancy Mode drop-down menu, select **Multi(tenancy)**.
4. Click **Save**.
5. To configure multi-tenancy, do the following:
   a) Select the Access Control tab.
   b) Click the Add Tenancy icon.
   c) Enter a name for the Tenant and click Create.
   d) Click inside the fields to assign the various roles described in **Table 1-2, Role-Based Access Controls**.
   e) Click **Save** to complete each role assignment.

### Upgrading the vCenter Plugin

This section demonstrates how to upgrade a previous version of vCenter Plugin to the latest version. To upgrade the plugin, run the latest version of the NexentaStor vCenter installer and it will automatically upgrade the plugin.

- **To upgrade the vCenter plugin, do the following:**
  1. Download the latest version of the NexentaStor vCenter installer:
     - **For Windows**: Download the NSVP-vCenter-Installer-5.0.xxxx.msi file from the NexentaStor 5.0 download site, and copy the file over to vCenter server.
     - **For Linux**: Download the nsvp-vcsa-installer-5.0.xxxx.tar file from the NeentaStor 5.0 download site.
  2. Log in to the vCenter Windows Server, and run the Web Client Plugin installer file, as described in **Installing the vCenter Plugin**.
  3. Upon completion, re-log in to the vSphere Web Client.
Uninstalling the vCenter Plugin

This section demonstrates how to uninstall the vCenter Plugin, in Windows and Linux environments.

- To uninstall the vCenter Plugin in a Windows environment, do the following:
  2. Follow the prompts.

- To uninstall the vCenter Plugin in a Linux environment, enter the following command:
  #./install.sh -action uninstall -vcuser administrator@vsphere.local
Managing NexentaStor Appliances with vCenter Plugin

This chapter covers the following topics:

- Adding and Configuring Pools
- Managing Filesystems
- Prerequisites for Creating Volumes and DataStores
- Managing Volumes
- Managing Datastores
- Managing Scheduled and Unscheduled Snapshots

Managing Filesystems

This section demonstrates how to create and share file systems.

Adding and Configuring Pools

Before you create and share filesystems in vCenter, you should have already added and configured pools using the NexentaStor CLI or NexentaFusion. For more information, see the NexentaStor 5.0 CLI Reference Guide or NexentaStor 1.0 User Guide.

Creating Filesystems

Once you have created a pool, you can create a file system that you can then share using SMB or NFS.

- To create a filesystem, do the following:
  1. On the Home page, click the Nexenta Storage Systems icon.
  2. Select an appliance, and click the Manage Tab.
  3. Click the NAS button.
4. In the Filesystems window, click Create+, and do the following:
   a) Enter the Filesystem name.
   b) Select a pool.
   c) Select either the NFS or SMB share type.
   d) To set data reduction, record size (up to 1MB), capacity limit, and pool reservation, click the Advanced arrow in the Create Filesystem dialog. Review the Table 2-1, Filesystem Properties for more information.
   e) Click Create.

5. Continue with Sharing Filesystems.

Table 2-1: Filesystem Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The descriptive name of the dataset that cannot be modified after its creation. The name should adhere to the ZFS naming rules.</td>
</tr>
<tr>
<td>Pool</td>
<td>Select the pool under which you want to create the filesystem on.</td>
</tr>
<tr>
<td>Share Type</td>
<td>The options are NFS or SMB.</td>
</tr>
<tr>
<td>Advanced Settings</td>
<td>Advanced setting change depending on the share type that you selected.</td>
</tr>
<tr>
<td>Authentication Type (NFS only)</td>
<td>System Users (AUTH_SYS)—NFS server passes user and group IDs of UNIX users unauthenticated. This method does not require additional administration. Unknown users are recognized as anonymous user nobody.</td>
</tr>
<tr>
<td>Share Access</td>
<td>Enter list of hosts or networks/subnets that will have access to the NFS share. This property is applicable only for NFS shares.</td>
</tr>
<tr>
<td>Data Reduction</td>
<td>The compression algorithm. Select on to enable the data reduction functionality.</td>
</tr>
<tr>
<td>Reservation</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 parent dataset's disk space used, and count against the parent dataset's quotas and reservations.</td>
</tr>
<tr>
<td>Record Size</td>
<td>Size of the filesystem blocks. The default value is 128K.</td>
</tr>
<tr>
<td>Capacity</td>
<td>Optionally, you may select the maximum size of the filesystem.</td>
</tr>
</tbody>
</table>

Sharing Filesystems

This section demonstrates how to share NFS and SMB filesystems.
For SMB filesystems, the Shared Folders Microsoft Management Console (MMC) must be shared with the admin user account if the domain is not configured. This allows the administrator to use the MMC to configure SMB shares. If domain is configured, then the domain administrator can mount the SMB shares. Also see the Enabling Multi-Tenancy section in this document.

- To share NFS or SMB filesystems, do the following:
  1. Click the NAS button.
  2. Select the filesystem you want.
  3. Click Edit.
  4. Select the share type and Save entry.

Prerequisites for Creating Volumes and DataStores

This section covers the necessary steps you need to perform with the CLI on the NexentaStor appliance before creating iSCSI or Fibre Channel (FC) volumes or datastores. For more information, see the NexentaStor 5.0 CLI Reference Guide.

Creating an iSCSI Target

An iSCSI target is a software only service that utilizes the iSCSI protocol to link data storage devices over the network. An iSCSI target is what an initiator connects to. You can create an iSCSI target to associate multiple portal addresses that the target will be bound to. When creating an iSCSI target you can also optionally configure the 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 an iSCSI target on a peer-to-peer model.

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

The CHAP credentials that you specify during the iSCSI Target creation are only relevant for bidirectional CHAP. For non-bidirectional CHAP authentication, specify the CHAP parameters for the initiator when configuring the initiator.

```
CLI@host> iscsitarget create 10.10.10.10
```

where "10.10.10.10" is IP on the NexentaStor appliance you want to use to share iSCSI over
Creating a Target Group

Target groups are necessary to manage LUN mappings. You can create multiple iSCSI targets on the same NexentaStor appliance for a multi-path scenario or unite these iSCSI targets in logical groups to control the access of initiator hosts. LUNs are mapped between a target group and a host group or initiator group.

```
CLI@host> targetgroup create test iqn.2010-08.org.illumos:02:58e0a636-7fac-ed18-d297-a788c0de3edf
```

where "test" is your group name and "iqn.2010-08.org.illumos:02:58e0a636-7fac-ed18-d297-a788c0de3edf" is your target name

Now you can select the iSCSI group you created to create your iSCSI/FC volumes or datastores.

See NexentaStor 5.0 CLI Configuration QuickStart guide for more information on creating a Target and Target group.

Managing Volumes

This section demonstrates how to create and configure iSCSI or Fibre Channel (FC) volumes. Before you create and share filesystems in vCenter, you should have already added and configured pools using the NexentaStor CLI or NexentaFusion. For more information, see the NexentaStor 5.0 CLI Reference Guide or NexentaStor 1.0 User Guide.

- To create and configure volumes, do the following:
  1. Create targets and a target group, as described in Prerequisites for Creating Volumes and Datastores.
  2. Click the SAN button.
  3. In the Volumes window, click Create +, and do the following:
     - For FC and iSCSI volumes you must create a target group using the CLI or API.
     - a) Enter the Volume name and select the pool.
     - b) Select the target group (iSCSI or FC).
     - c) Specify the capacity limit and a reservation value.
     - d) Optionally, you can disable thin provisioning. By default the block is thin provisioned that grows gradually to the maximum size of the volume.
  4. Click Create.

Note: With the Advanced options, you can enable or disable data reduction and set record size (up to 128K) by clicking the down-arrow in the dialog box.
Managing Datastores

Depending on your storage needs, you can create a datastore on the following types: NFS (version 3) or VMFS (iSCSI / FC). You can set up VMFS datastores on any SCSI-based storage devices that the host discovers. Datastores can be created either on a single ESXi host or on an ESXi Cluster.

This section covers the following topics:

- **Prerequisites**
- **Creating and Deleting Datastores**

**Prerequisites**

Prior to **Creating and Deleting Datastores**, verify that the following prerequisites are met:

- You must have at least one pool configured. This was most likely done during the initial configuration of NexentaStor 5.0. For more information, see the [NexentaStor 5.0 CLI Reference Guide](#).
- For VMFS datastore creation, verify that the requirements listed in [Table 2-2, Fiber Channel and iSCSI Requirements](#) are met.

**Table 2-2: Fiber Channel and iSCSI Requirements**

<table>
<thead>
<tr>
<th>Fiber Channel (FC) Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure targets using NexentaStor CLI or API or using the NexentaFusion UI.</td>
</tr>
<tr>
<td>2. Configure target groups in the NexentaStor appliance.</td>
</tr>
<tr>
<td>3. Configure ESXi FC Initiator are configured.</td>
</tr>
<tr>
<td>4. Discover FC targets.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>iSCSI Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure targets on the NexentaStor appliance.</td>
</tr>
<tr>
<td>2. Configure target groups in NexentaStor.</td>
</tr>
<tr>
<td>3. Optional: Configure host groups in NexentaStor.</td>
</tr>
<tr>
<td>4. Configure ESXi iSCSI initiator.</td>
</tr>
<tr>
<td>5. Discover iSCSI targets.</td>
</tr>
</tbody>
</table>

**Creating and Deleting Datastores**

After verifying that the necessary **Prerequisites** have been met, go to the vSphere Web Client Home page to create a datastore.
To create a datastore, do the following:

1. Go to the Home page and click Hosts and Clusters in the right pane.

2. Right-click the host or cluster on which the datastore is to be created, and select All NexentaStor vCenter Plugin Actions from the drop-down list.

3. Click Create Datastore.

4. Select the Location of the datastore, then select NFS Datastore for NFS or VMFS Datastore for NexentaStor zvols provisioned through iSCSI or FC.

5. Select the NexentaStor appliance from which to provision the datastore, then select the pool to be provisioned as a datastore.

6. Select the size for this datastore. For SAN and NAS datastores, select the size of blocks for files in a dataset.

7. Enable or disable Data reduction by toggling it ON or OFF.

8. For an NFS datastore, select the IP address through which to mount the datastore.

   If a pool selected for provisioning as datastore is under HA protection, the VIP is chosen automatically and you are not allowed to edit it.

9. Click Next, move through the menus, filling in the appropriate fields.

10. Click Finish.
When you delete a datastore using the vCenter Plugin, you not only delete the datastore but also take care of other cleanup, such as unsharing datasets and deleting filesystems and volumes.

- **To delete a datastore, do the following:**
  1. Go to the **Home** page and click the **Storage** icon in the right pane.
  2. Right-click the datastore to be deleted, and select **All NexentaStor vCenter Plugin Actions** from the drop-down list.
  3. Click **Delete Nexenta Datastore**, and then click **OK**.

### Managing Scheduled and Unscheduled Snapshots

As with other features, you may have already created and scheduled snapshots when you configured your NexentaStor 5.0 appliance. The NexentaStor vCenter Web Client Plugin also provides the capability to create scheduled or unscheduled snapshots for datastores, filesystems, and volumes. You can create a point-in-time
representation of the NexentaStor datasets to preserve the state of the datasets. You can perform the following actions with a snapshot: clone from a snapshot to a new dataset, rollback a dataset to a snapshot, access the data.

This section covers the following topics:

- Managing Manual Snapshots Independent of a Protection Service
- Managing Scheduled Snapshots Using a Data Protection Service

**Figure 2-1: UI to Manage Manual and Scheduled Snapshots**

```
Managing Manual Snapshots Independent of a Protection Service

This section demonstrates how to manage snapshot creation manually, independent of Data Protection. For information on how to create scheduled snapshots, see Managing Scheduled Snapshots Using a Data Protection Service.

To create manual snapshots for filesystems or volumes, do the following:

1. Go to the Home page and click Nexenta Storage Systems in the right pane.
2. Under the Nexenta Storage Systems from the left panel, select the appliance you want to work with and click the Manage tab.
3. Do one of the following:
   - Click the SAN button to provide snapshot capabilities on the Volumes.
   - Click the NAS button to provide snapshot capabilities on the File Systems.
```

**Note:** You cannot create more than one scheduled snapshot service for a dataset. However, you can always change the schedule for the snapshot service that already exists or add a new schedule to it.
4. Select the Filesystem or Volume for managing snapshots, then select the Snapshots tab to access Snapshots.

5. Click Create + button.

This creates a manual snapshot of the selected filesystem or volume that is independent of the policies of the protection service even if the dataset has replication service.

Once you create the snapshot of the filesystem or volume, it can be managed from the action buttons listed under the Snapshots tab. For more information, see Table 2-3, Snapshot Operations.

To create manual snapshots for datastores, do the following:

1. Go to the Home page and click Storage in the right pane.
2. Select the datastore you want to work with and click the Manage tab.
3. Click the Data Protection tab, then the Snapshots tab.
4. Click Create +.

This creates a snapshot of the selected datastore that is independent of the policies of the protection service even if the dataset has replication service.

Once you create the snapshot of the datastore, it can be managed from the action buttons listed under the Snapshots tab. For more information, see Table 2-3, Snapshot Operations.

To configure a scheduled snapshot, select the Protection Services tab. See Managing scheduled snapshot service for details on how to set up a scheduled snapshot.

After you create a snapshot of a volume, a file system, or a datastore, you can manage them using the action buttons in the Data Protection interface.

Table 2-3: Snapshot Operations

<table>
<thead>
<tr>
<th>Action Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revert</td>
<td>You can revert a file system, volume, or a datastore to the state captured at the moment of snapshot creation. When you revert, select from the following options: —Overwrite existing volume, file systems, or a datastore from the snapshot. —Clone from a snapshot to a new dataset.</td>
</tr>
<tr>
<td>Delete</td>
<td>You can delete any manual snapshots. Use with care when deleting any snapshots because you cannot restore snapshots after deletion. You can only delete snapshots that do not have clones.</td>
</tr>
</tbody>
</table>

Note: Deleting snapshots that belong to a protection service may break the service.
Managing Scheduled Snapshots Using a Data Protection Service

You can create an automatic periodic snapshot service for a filesystem, volume, or a datastore. The service automatically creates a point-in-time representation on a regular frequency (monthly, weekly, daily, hourly), creates snapshots of the datasets and its descendants, and assists in creating a retention policy.

For Volumes and Filesystems

- To create a scheduled snapshot service for volumes and filesystems:
  1. Go to the Home page and click Nexenta Storage Systems in the right pane.
  2. Select the appliance you want to work with and click the Manage tab.
  3. Do one of the following:
     - Click the SAN button to provide snapshot capabilities on the Volumes.
     - Click the NAS button to provide scheduled snapshot capability on the File Systems.
  4. Select the dataset, and then click on the Protection Services tab.
  5. Click Add New Service + button.
  6. In the Create protection service window, select Scheduled Snapshots in the service type dropdown list.
  7. To set a schedule for the snapshot service, click Add Schedule + and fill in the required fields in the Add Schedule window.

Once you create a scheduled snapshot service, you can manage them using the interface shown in the following figure.

For Datastores

- To create a scheduled snapshot service for datastores:
  1. Go to the Home page and click Storage in the right pane.
  2. Select the datastore created with the NexentaStor vCenter plugin to provide snapshot capabilities.
  3. Click the Manage > Data Protection > Snapshots.
  4. Click Create +, then in the Create protection service window select Scheduled Snapshots from the service type drop-down list.
  5. Click Add Schedule + to set a schedule for the snapshot service.

Once you create the snapshot of the datastore, it can be managed from the action buttons listed under the Protection Services tab. For more information, see Table 2-4, Operations on Scheduled Snapshots Belonging to a Protection Service.
Table 2-4: Operations on Scheduled Snapshots Belonging to a Protection Service

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run Now</td>
<td>Irrespective of the schedule set for the snapshot, you can run the service any time manually.</td>
</tr>
<tr>
<td>Enable</td>
<td>When you create a snapshot service, it is enabled by default.</td>
</tr>
<tr>
<td>Disable</td>
<td>You can temporarily disable snapshot services. When you disable a service, it stops creating snapshots for the selected dataset at the scheduled period.</td>
</tr>
<tr>
<td>Delete</td>
<td>You can delete the snapshot services that are no longer in use. When you delete a snapshot service, the information about the service is deleted from VMware vSphere. The snapshots created by this service are not deleted.</td>
</tr>
</tbody>
</table>

Note: You cannot delete or disable a snapshot if the protection service is active.
This chapter covers the following topics:

- Data Protection Services
- Managing Protection Services
- UI to Manage the Continuous Replication Service.

Data Protection Services

Protection service is a high performance replication service that generates snapshots at the source appliance on a set schedule and save them in a destination appliance. The destination can be either local pools on the same NexentaStor appliance or on a remote NexentaStor appliance. Local replication service replicates data from one dataset to another within one host. Remote service replicates data from one host to another.

You can create multiple services from the same source appliance dataset to different destination appliance datasets. Use these snapshots as a backup or an archive, as well as in the disaster recovery use case to handle network failures or sudden power outages.

The following screenshot shows an example of the user interface (UI) for managing scheduled or continuous replication services.

Using the NexentaStor vCenter plugin, you can set up the data protection services for scheduled replication and continuous replication, as described in Table 3-1, Protection Services.
Table 3-1: Protection Services

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Replication</td>
<td>Use this service to set up scheduled replication of your datasets (filesystem, volume, snapshots, datastores) on a regular basis to a local or a remote host(s). Enabled by default with the Enterprise Edition license, with a snapshot schedule of “every 15 minutes” or longer. SR replicates snapshots taken on predefined schedules on the source dataset. If the NexentaStor appliance has the continuous replication license option installed, the snapshot schedule for scheduled replication can be as tight as “every minute”.</td>
</tr>
<tr>
<td>Continuous Replication</td>
<td>Use this service to set up continuous replication of your datasets (filesystem, volume, snapshots, datastores) on a regular basis to a local or a remote host(s). Continuous replication - Requires the continuous replication license option. CR delivers close to-zero Recovery Point Objective (RPO) over any distance without affecting application performance. CR works by asynchronously replicating every write transaction on the source dataset.</td>
</tr>
</tbody>
</table>
Managing Protection Services

This section demonstrates how to create Protection Services for filesystems, volumes, and datastores.

For Filesystems and Volumes

- **To create a protection service for a filesystem or volume, do the following:**
  1. Go to the Home page and click Nexenta Storage Systems in the right pane.
  2. Select the appliance you want to work with, and click the Manage tab.
  3. Do one of the following:
     - Click the SAN button to provide replication service on the Volumes.
     - Click the NAS button to provide replication service on the File Systems.
  4. Select the Filesystems or Volume, and do one of the following:
     - For scheduled replication, click Protection Services > Add New Service +, choose to replicate the datasets to another pool on the same appliance or a remote host, then select Scheduled Replication as the Service Type.
     - For continuous replication, click Continuous Replication tab, then click Configure Continuous Replication.
  5. Select Local Replication to replicate the datasets to another pool on the same appliance, or select the host name in the Remote Appliance field to replicate the datasets to a remote host.
  6. Fill in the Secondary pool and dataset name.
  7. Click Add Schedule.

Once you create the scheduled replication service of the filesystem or volume, it can be managed from the list of actions under the Actions button in the Protection Services tab. For more information, see Table 3-2, Operations of Scheduled Replication Services.

See for information on managing the continuous replication service you created for the filesystem or volume.

For Datastores

- **To create a protection service for a datastore, do the following:**
  1. Go to the Home page and click Storage in the right pane.
  2. Select the datastore you want to work with, and select Manage > Data Protection.
  3. Do one of the following:
     - For scheduled replication, click Protection Services > Add New Service +, choose to replicate the datasets to another pool on the same appliance or a remote host, then select Scheduled Replication as the Service Type.
For continuous replication, click Continuous Replication tab, then click Configure Continuous Replication.

4. Select Local Replication to replicate the datasets to another pool on the same appliance, or select the host name in the Remote Appliance field to replicate the datasets to a remote host.

5. Fill in the Secondary pool and dataset name.

6. Click Add Schedule.

Once you create the scheduled replication service for the datastore, it can be managed from the list of actions under the Actions button in the Protection Services tab. For more information, see Table 3-2, Operations of Scheduled Replication Services.

See for information on managing the continuous replication service you created for the datastore.

**Figure 3-1: UI to Manage the Scheduled Replication Service.**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run Now</td>
<td>Irrespective of the schedule set for the replication service, you can run the service any time manually after its creation.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Flip Direction  | When this action is invoked, the source dataset becomes the destination dataset and vice-versa. This operation can only be performed on a disabled replication services. For a successful flip direction operation, follow these steps:  
1. Stop replication immediately, if running.  
2. Disable service, if not disabled.  
3. Unmap source volumes and unshare source filesystems.  
4. Start replication once and wait until it has finished.  
5. Flip service direction.  
7. Share new source.  
8. Enable service if it was disabled earlier. |
| Clear Replication| This operation clears the state of the service and disables the service.                                                                 |
| Stop Replication | Use this operation to stop the currently running replication service. On the next schedule, the interrupted service will continue to replicate from the point of interruption. |

Figure 3-2: UI to Manage the Continuous Replication Service.
Table 3-3: Operations of Continuous Replication Service.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flip Direction</td>
<td>When this action is invoked, the source dataset becomes the destination dataset and vice-versa. This operation can only be performed on a disabled replication services. For a successful flip direction operation, follow these steps: 1. Stop replication immediately, if running. 2. Disable service, if not disabled. 3. Unmap source volumes and unshare source filesystems. 4. Start replication once and wait until it has finished. 5. Flip service direction. 6. Map volumes. 7. Share new source. 8. Enable service if it was disabled earlier.</td>
</tr>
<tr>
<td>Clear Replication</td>
<td>This operation clears the state of the service and disables the service.</td>
</tr>
<tr>
<td>Remove Service</td>
<td>Using this option you can force the service to be destroyed and also choose to destroy the destination dataset.</td>
</tr>
</tbody>
</table>
Viewing Protection Service Status

This section demonstrates how to view the status of protection services for filesystems, volumes, and datastores.

❖ To view protection service status for filesystems and volumes, do the following:
  1. Go to the Home page and click Nexenta Storage Systems in the right pane.
  2. Select the appliance where the dataset exists, select the Manage tab.
  3. Do one of the following:
     • Click the SAN button to view the replication service on the Volumes.
     • Alternatively, click the NAS button to view the replication service on the File Systems.
  4. Hover the cursor over the icons in the Protection column to view the protection service status.

The following screenshot shows an example of the protection service status for NAS.

❖ To view protection service status for datastores, do the following:
  1. Go to the Home page and click Storage in the right pane.
  2. Select the datastore you want to work with, and select the Manage tab.
  4. Hover the cursor over the icons in the Name column to view the protection service status.

The following screenshot shows an example of protection service status for a datastore.