

NetApp SolidFire Plug-in for VMware vCenter Server Web Client User Guide

Version 3.0

9/20/2017 | 215-12547_A0

Copyright Information

Copyright © 1994-2017 NetApp, Inc. All Rights Reserved.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this document may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

Table of Contents

| | |
|--|-----------|
| Introduction | 1 |
| vCenter Plug-in Overview | 1 |
| Network Ports | 2 |
| VMware vCenter Prerequisites | 4 |
| Getting Started | 5 |
| Deploying a New Management Node | 5 |
| Registering the NetApp SolidFire Plug-in in vCenter | 5 |
| Modifying vCenter Properties for In-House HTTP or HTTPS Server | 8 |
| Successful Installation | 9 |
| How to Use the NetApp SolidFire Plug-in | 10 |
| Discovery | 13 |
| Discovering a Cluster | 13 |
| Viewing Discovered Cluster Details | 14 |
| Cluster Details | 14 |
| Deleting a Cluster Entry from Discovery | 15 |
| Rediscovering a Disconnected Cluster | 16 |
| Enabling Virtual Volumes | 16 |
| Cluster Admin User Credentials Management | 17 |
| Creating User Credentials | 17 |
| Editing User Credentials | 17 |
| Deleting User Credentials | 18 |
| Configuring mNode Settings for QoSSIOC | 19 |
| Configuring SIOC Service Credentials | 19 |
| Viewing QoSSIOC Events | 20 |
| QoSSIOC Event Details | 20 |

| | |
|-------------------------------------|----|
| Reporting | 21 |
| Cluster Details | 21 |
| Viewing Event Logs | 22 |
| Event Log | 22 |
| Event Types | 23 |
| Alerts | 24 |
| Alert Error Codes | 25 |
| Running Tasks | 26 |
| Management | 28 |
| Datastore Management | 28 |
| Creating a Datastore | 28 |
| Viewing the Datastore List | 29 |
| Datastore Details | 30 |
| Extending a Datastore | 30 |
| Cloning a Datastore | 31 |
| Sharing a Datastore | 33 |
| Enabling VAAI UNMAP | 34 |
| Deleting a Datastore | 35 |
| QoSSIOC Automation | 35 |
| Enabling QoSSIOC Automation | 36 |
| Disabling QoSSIOC Integration | 37 |
| Volume Management | 39 |
| Creating a Volume | 39 |
| Viewing Volumes Details | 40 |
| Volume Details | 40 |
| Individual Volume Details | 41 |
| Volume QoS and Stats | 43 |

| | |
|--|----|
| Editing a Volume | 43 |
| Cloning a Volume | 44 |
| Volume Backup and Restore Operations | 45 |
| Volume Backup Operations | 45 |
| Volume Restore Operations | 47 |
| Deleting a Volume | 49 |
| Purging Volumes | 50 |
| Restoring a Deleted Volume | 50 |
| Adding Volumes to an Access Group | 50 |
| Removing Volumes from an Access Group | 51 |
| User Account Management | 51 |
| Account Details | 51 |
| Creating an Account | 52 |
| Editing an Account | 52 |
| Deleting an Account | 53 |
| Volume Access Groups | 53 |
| Volume Access Group Details | 53 |
| Creating Access Groups | 53 |
| Editing Access Groups | 54 |
| Deleting Access Groups | 55 |
| Initiators | 56 |
| Creating an Initiator | 56 |
| Initiator Details | 57 |
| Editing an Initiator | 57 |
| Deleting Initiators | 57 |
| Adding Initiators to a Volume Access Group | 57 |
| Data Protection | 59 |

| | |
|--|----|
| Volume Snapshots | 59 |
| Creating a Volume Snapshot | 60 |
| Volume Snapshot Details | 60 |
| Editing Snapshots | 61 |
| Cloning a Volume from a Snapshot | 61 |
| Rolling Back a Volume to a Snapshot | 62 |
| Volume Snapshot Backup Operations | 62 |
| Backing Up a Volume Snapshot to an Amazon S3 Object Store | 62 |
| Backing Up a Volume Snapshot to an OpenStack® Swift Object Store | 63 |
| Backing Up a Volume Snapshot to a SolidFire Cluster | 63 |
| Deleting a Snapshot | 64 |
| Group Snapshots | 64 |
| Creating a Group Snapshot | 64 |
| Group Snapshot Details | 65 |
| Editing Group Snapshots | 65 |
| Cloning Volumes from a Group Snapshot | 66 |
| Rolling Back Volumes to a Group Snapshot | 66 |
| Deleting a Group Snapshot | 67 |
| Snapshot Schedules | 67 |
| Snapshot Schedule Details | 67 |
| Creating a Snapshot Schedule | 68 |
| Editing a Snapshot Schedule | 69 |
| Deleting a Snapshot Schedule | 69 |
| Copying a Snapshot Schedule | 70 |
| Cluster and Volume Pairing for Real-Time Remote Replication | 70 |
| Cluster | 71 |
| Drives | 71 |

| | |
|---|----|
| Drive Details | 71 |
| Adding Available Drives to a Cluster | 72 |
| Removing a Drive | 73 |
| Removing Failed Drives | 73 |
| Nodes | 74 |
| Storage Nodes | 74 |
| Fibre Channel Nodes | 74 |
| HCI Compute Servers | 74 |
| HCI Storage Nodes | 74 |
| Node Details | 75 |
| Adding a Node to a Cluster | 75 |
| Removing Nodes from a Cluster | 76 |
| VLAN Management | 76 |
| Virtual Network Details | 77 |
| Creating a VLAN | 77 |
| Editing a Virtual Network | 78 |
| Deleting a Virtual Network | 79 |
| Virtual Volumes | 80 |
| Configuring Wols Functionality | 80 |
| Registering the SolidFire VASA Provider | 80 |
| Creating a Wvol Datastore | 81 |
| Viewing Virtual Volumes Details | 82 |
| Virtual Volume Details | 82 |
| Individual Virtual Volume Details | 83 |
| Storage Containers | 85 |
| Creating a Storage Container | 85 |
| Viewing Storage Container Details | 86 |

| | |
|---|------------|
| Storage Container Details | 86 |
| Individual Storage Container Details | 87 |
| Editing a Storage Container | 88 |
| Deleting a Storage Container | 89 |
| Protocol Endpoints | 89 |
| Viewing Protocol Endpoint Details | 89 |
| Protocol Endpoint Details | 90 |
| Individual Protocol Endpoint Details | 90 |
| Unregistering the SolidFire Plug-in | 92 |
| Removing the SolidFire Plug-in | 94 |
| Appendix 1 — Registering the SolidFire Plug-in Using a CLI | 95 |
| Troubleshooting | 97 |
| Related Documentation | 103 |
| Contacting NetApp Support for SolidFire | 105 |

Introduction

The NetApp SolidFire vCenter Plug-in is a web-based tool integrated with the VMware vSphere® Web Client user interface (UI). The Plug-in is an extension and alternative interface for VMware vSphere users who have deployed a NetApp HCI or NetApp SolidFire All-Flash Storage Array cluster environment. The Plug-in provides a scalable and user-friendly interface to manage and monitor NetApp HCI or NetApp SolidFire clusters.

The intended audience for the *NetApp SolidFire Plug-in for VMware vCenter Server Web Client User Guide* is those who install, administer, or troubleshoot storage solutions, and VMware admins who need to allocate storage for virtual machines (VMs). Other IT professionals or software developers may also find this document useful. The following assumptions are made regarding the intended audience:

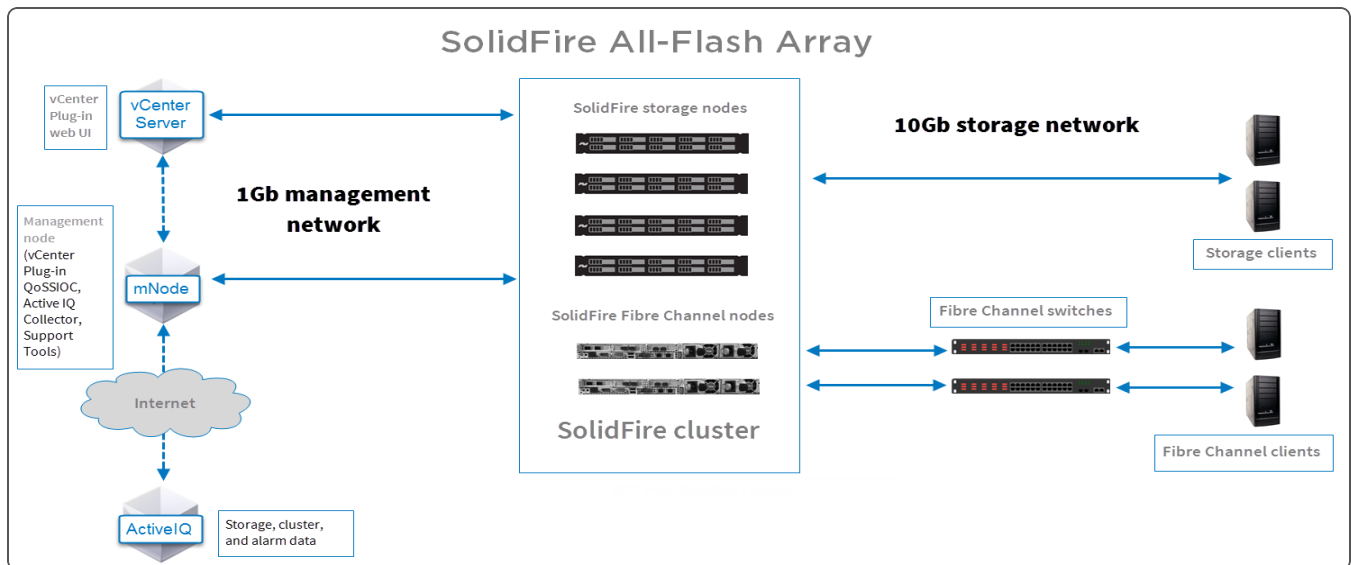
- You have a background or worked as a Linux system administrator.
- You are familiar with working on server networking and network storage, including IP addresses, netmasks, and gateways.

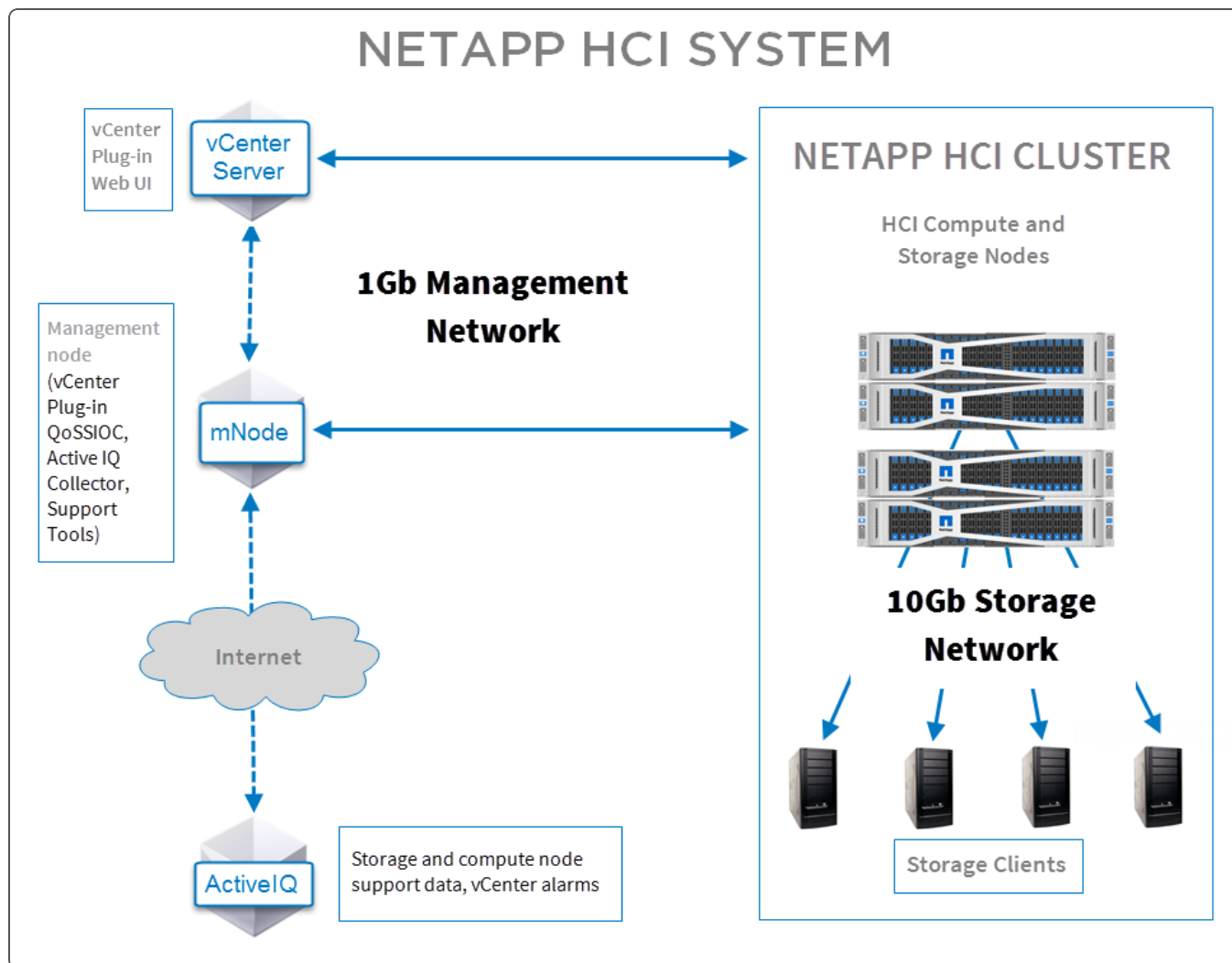
vCenter Plug-in Overview

The NetApp SolidFire vCenter Plug-in is used to discover, configure, and manage NetApp HCI systems or NetApp SolidFire All-Flash Array storage system clusters. You can also monitor cluster activity with real-time reporting, including error and alert messaging for any event that might occur while performing various operations.

You can use the Plug-in user interface to set up, monitor, and allocate storage from cluster capacity to configure datastores and virtual datastores (for Vols). A cluster appears on the network as a single local group that is represented to hosts and administrators by virtual IP addresses.

The following images describe the role of the NetApp SolidFire vCenter Plug-in with a SolidFire All-Flash Array and a NetApp HCI system.





Network Ports

You might need to allow the following network ports through your datacenter's edge firewall so that you can manage the system remotely and allow clients outside of your datacenter to connect to resources. Some ports might not be required, depending on how you use the system.

NOTE: All ports are TCP unless stated otherwise, and should be open bidirectionally.

The following abbreviations are used in the table:

- MIP: Management IP Address
- SIP: Storage IP Address
- MVIP: Management Virtual IP Address
- SVIP: Storage Virtual IP Address

| Source | Destination | Port | Description |
|------------------|-----------------------------|-----------|--|
| iSCSI clients | Storage cluster MVIP | 443 | UI and API access (optional) |
| iSCSI clients | Storage cluster SVIP | 3260 | Client iSCSI communications |
| iSCSI clients | Storage node SIP | 3260 | Client iSCSI communications |
| Management node | sfsupport.solidfire.com | 22 | Reverse SSH tunnel for support access |
| Management node | solidfire.brickftp.com | 22 | SFTP for log bundle uploads |
| Management node | Storage node MIP | 22 | SSH access for support |
| Management node | pubrepo.solidfire.com | 80 | Access to NetApp repository for Element OS and management node updates |
| Management node | Storage cluster MVIP | 161 | SNMP Polling |
| Management node | Storage node MIP | 161 | SNMP Polling |
| Management node | Storage node MIP | 442 | UI and API access to storage node |
| Management node | monitoring.solidfire.com | 443 | Storage cluster reporting to Active IQ |
| Management node | Storage cluster MVIP | 443 | UI and API access to storage cluster |
| SNMP Server | Storage cluster MVIP | 161 | SNMP Polling |
| SNMP Server | Storage node MIP | 161 | SNMP Polling |
| Storage node MIP | Management node | 80 | SolidFire Element OS updates |
| Storage node MIP | S3/Swift endpoint | 80 | HTTP communication to S3/Swift endpoint for backup and recovery |
| Storage node MIP | Management node | 123 | NTP |
| Storage node MIP | NTP server | 123 | NTP |
| Storage node MIP | Management node | 162 | SNMP Traps |
| Storage node MIP | SNMP Server | 162 | SNMP Traps |
| Storage node MIP | Remote storage cluster MVIP | 443 | Remote replication cluster pairing communication |
| Storage node MIP | Remote storage node MIP | 443 | Remote replication cluster pairing communication |
| Storage node MIP | S3/Swift endpoint | 443 | HTTPS communication to S3/Swift endpoint for backup and recovery |
| Storage node MIP | Remote storage node MIP | 2181 | Remote replication intercluster communication |
| Storage node MIP | Management node | 10514/514 | Syslog forwarding. Cluster defaults to port 514 if no port is specified. |
| Storage node MIP | Syslog server | 10514/514 | Syslog forwarding. Cluster defaults to port 514 if no port is specified. |

| Source | Destination | Port | Description |
|-------------------------|-------------------------|-----------|--|
| Storage node SIP | S3/Swift endpoint | 80 | HTTP communication to S3/Swift endpoint for backup and recovery (optional) |
| Storage node SIP | S3/Swift endpoint | 443 | HTTPS communication to S3/Swift endpoint for backup and recovery (optional) |
| Storage node SIP | Remote Storage Node SIP | 2181 | Remote replication intercluster communication |
| Storage node SIP | Storage node SIP | 3260 | Internode iSCSI |
| Storage node SIP | Remote storage node SIP | 4000-4020 | Remote replication node-to-node data transfer |
| System administrator PC | Management node | 442 | HTTPS UI and API access to management node |
| System administrator PC | Storage node MIP | 442 | UI and API access to storage node |
| System administrator PC | Management node | 443 | UI and API access to management node |
| System administrator PC | Storage cluster MVIP | 443 | UI and API access to storage cluster |
| System administrator PC | Storage node MIP | 443 | Storage cluster creation, post-deployment UI access to storage cluster |
| vCenter Server | Storage cluster MVIP | 443 | vCenter Plug-in API access |
| vCenter Server | Management node | 8080/8443 | vCenter Plug-in QoSSIOC service. 8080 redirects to 8443. |
| vCenter Server | Storage cluster MVIP | 8444 | vCenter VASA provider access (Wvols only) |
| vCenter Server | Management node | 9443 | vCenter Plug-in registration. The port can be closed after registration is complete. |

Best Practices: Enable ICMP between the management node, SolidFire nodes, and Cluster MVIP.

NOTE: For vSphere network port requirements, refer to VMware [documentation](#).

VMware vCenter Prerequisites

VMware ESXi Server and vSphere 5.5u3 (earliest version supported), 6.0, or 6.5 are required to use the NetApp SolidFire vCenter Plug-in. It is recommended that all SolidFire clusters under SolidFire vCenter Plug-in management use the same version of vSphere to avoid VMFS compatibility issues.

Getting Started

NOTE: These deployment and registration instructions apply to SolidFire AFA installations only. For information about NetApp HCI installations, see [Related Documentation](#).

You can deploy version 3.0 of the NetApp SolidFire vCenter Plug-in directly in vCenter. Only the quality of service based on storage I/O control (QoSSIOC) portion of the vCenter Plug-in is installed on the management node.

For new and existing installations, review the following topics:

- [Deploying a New Management Node](#)
- [Registering the NetApp SolidFire Plug-in in vCenter](#)

NOTE: Version 3.0 of the vCenter Plug-in requires that you deploy a new management node Open Virtual Appliance (OVA).

Deploying a New Management Node

You can install the QoSSIOC component of the Plug-in by deploying an Element OS Open Virtual Appliance (OVA) to create a new management node (mNode).

Prerequisites

- vCenter Administrator role privileges.
- [BrickFTP](#) download permissions. Contact NetApp SolidFire [support](#) for BrickFTP access.

Procedure

1. Download the OVA for your Element OS that contains the vCenter Plug-in (VCP) QoSSIOC service package (**solidfire-fdva-[element-version]-[vcp-3.x].ova**) from SolidFire [BrickFTP](#).

NOTE: The OVA must be accessible to the vCenter Server.

2. From vCenter Web Client, create a VM by deploying the OVA.

NOTE: Allocate a static IP address or assign a DHCP server.

3. Power on the VM.

NOTE: For Element OS version 8.0, reboot the management node if you are using DHCP.

4. Log out of the vSphere Web Client.

Registering the NetApp SolidFire Plug-in in vCenter

You can deploy the SolidFire plug-in package in the vSphere Web Client by registering the package as an extension on vCenter Server. Once registered, the Plug-in is available to any vSphere Web client that connects to your vSphere environment.

You must register the SolidFire Plug-in on every vCenter Server where you need to use it. When a vSphere Web Client connects to a vCenter Server where your plug-in is not registered, the plug-in is not visible to the client.

NOTE: If you wish to use a command line interface for registration, see [Registering the SolidFire Plug-in Using a CLI](#) to register the Plug-in.

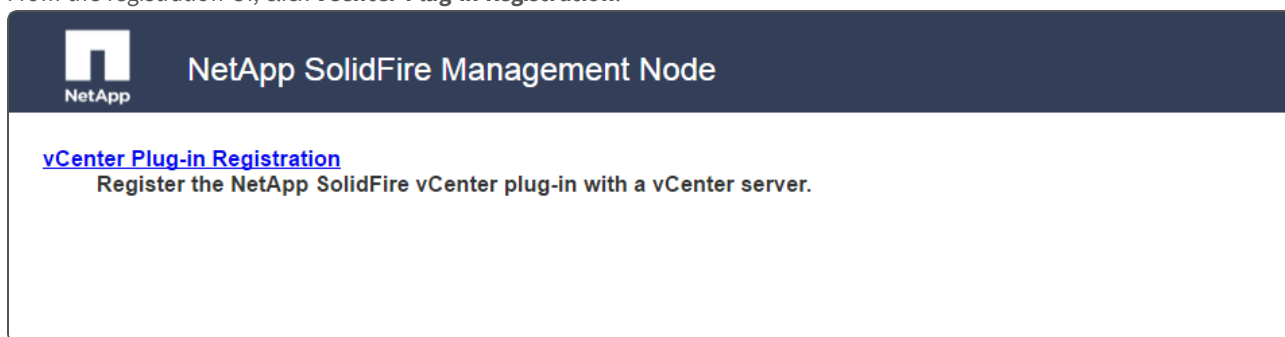
Prerequisites

- vCenter Administrator role privileges to register a plug-in.
- An SSH client or web browser (Chrome 56.0.2924, Mozilla 52.0.2, or Internet Explorer 11 or later) on a Microsoft® Windows® 64-bit system.
- You have deployed a management node with the version 3.0 OVA as described in [Deploying a New Management Node](#). Your management node must be powered on with its IP address configured.
- Firewall rules allow open network communication between the vCenter and the SolidFire Cluster MVIP on TCP ports 443, 8443, and 9443 (9443 is used for registration and can be closed after registration is complete).

NOTE: If you intend to customize a URL for an HTTP or HTTPS server, complete the prerequisite process described in [Modifying vCenter Properties for In-House HTTP or HTTPS Server](#).

Procedure

1. Enter the IP address for your management node in a browser, including the TCP port for registration: **https://[management node IP]:9443**.
2. From the registration UI, click **vCenter Plug-in Registration**.



3. Do one of the following:
 - Click **Register Plug-in** for new installations.
 - Click **Update Plug-in** if you are upgrading.

NOTE: Click **Registration Status**, complete the necessary fields, and click **Check Status** to check if the vCenter Plug-in is already registered and the version number of the current installation.

NetApp vCenter Plug-in Registration

Register Plug-in Update Plug-in Unregister Plug-in Registration Status

Register the vCenter plug-in with your vCenter service.

vCenter Address

vCenter User

vCenter Password

Plug-in Zip URL ☐ Customize URL?

Register

Contact NetApp SolidFire support at <http://solidfire.com/platform/support> or ng-SF-support@solidfire.com

4. Enter the following:

- The IP address of the vCenter on which you will register your Plug-in.
- The vCenter Administrator user name.

NOTE: The user name and password credentials you enter must be for an administrator with vCenter Administrator role privileges.

- The vCenter Administrator password.
- (Optional) A custom URL for the Plug-in ZIP.

NOTE: Most installations will use the default path. You can click **Custom URL** to customize the URL if you are using an in-house HTTP or HTTPS server or have modified the ZIP file name or network settings.

5. Do one of the following:

- Click **Register** for new installations.
- Click **Update** if you are upgrading.

6. Click **Registration Status**.

7. Enter the following:

- The IP address of the vCenter on which you are registering your Plug-in.
- The vCenter Administrator user name.
- The vCenter Administrator password.

8. Click **Check Status** to verify that the new version of the Plug-in is registered on the vCenter.
9. Log into the vSphere Web Client as a vCenter Administrator.

NOTE: If the NetApp SolidFire Plug-in icons are not visible from the vSphere main page, see [Troubleshooting](#).

10. (For upgrades) Verify the version change in the **About** tab in the NetApp SolidFire Configuration extension point. For more details, see [How to Use the NetApp SolidFire Plug-in](#).

NOTE: The NetApp SolidFire vCenter Plug-in contains online help content. To ensure that your online help contains the latest content, clear your browser cache after upgrading your Plug-in.

11. (For upgrades) Update your management node IP in the **mNode Settings** tab in the NetApp SolidFire Configuration extension point. See [Configuring mNode Settings for QoSSIOC](#).

Modifying vCenter Properties for In-House HTTP or HTTPS Server

You must modify the vCenter Web client properties file if you intend to customize a URL for an HTTP or HTTPS server during vCenter Plug-in registration.

Prerequisites

- SolidFire [BrickFTP](#) download access.

Procedure

1. Download the Plug-in ZIP (**solidfire-plugin-[version number]-bin.zip**) from SolidFire [BrickFTP](#) to an HTTP or HTTPS server.

NOTE: If you are deploying a management node, download the OVA for your Element OS that contains the vCenter Plug-in (VCP) QoSSIOC service package. The OVA already contains the vCenter Plug-in ZIP in the web server root directory.

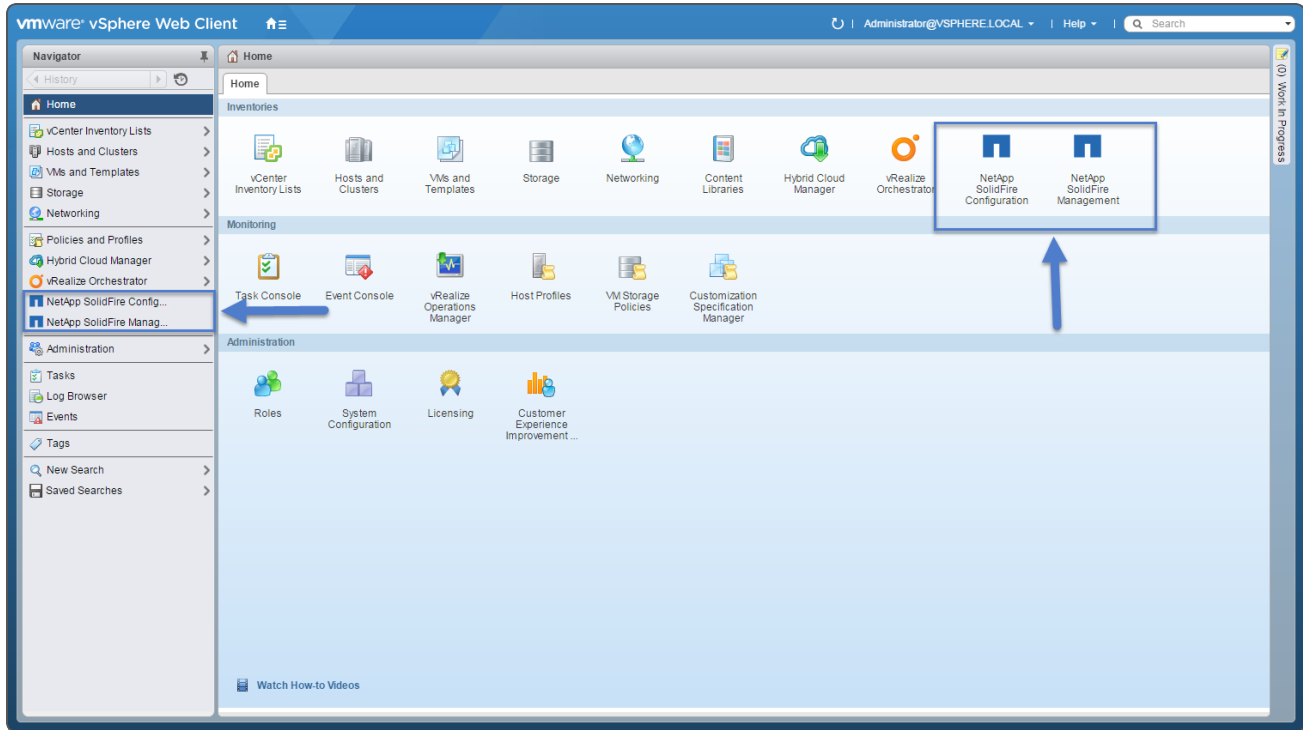
2. (For HTTP server) Modify the vCenter **webclient.properties** file to allow vCenter to download from an HTTP server:
 - Edit the vCenter 5.5 file (either **/var/lib/vmware/vsphere-client/webclient.properties** or **c:\programdata\vmware\vsphere web client\webclient.properties**) and add `allowHttp=true`.
 - Edit the vCenter 6.0 or vCenter 6.5 file (either **/etc/vmware/vsphere-client/webclient.properties** or **c:\programdata\vmware\vcserver\cfg\vsphere-client\webclient.properties**) and add `allowHttp=true`.

NOTE: Once you have completed the registration procedure, you can remove `allowHttp=true`.

3. (For HTTP server) Restart the vCenter web services or reboot the vCenter.

Successful Installation

After successful installation, NetApp configuration and management extension points appear in the Home tab of the vSphere Web Client and in the Navigator side panel.



NOTE: See [Troubleshooting](#) if the Plug-in extension points are not visible in vSphere.

How to Use the NetApp SolidFire Plug-in

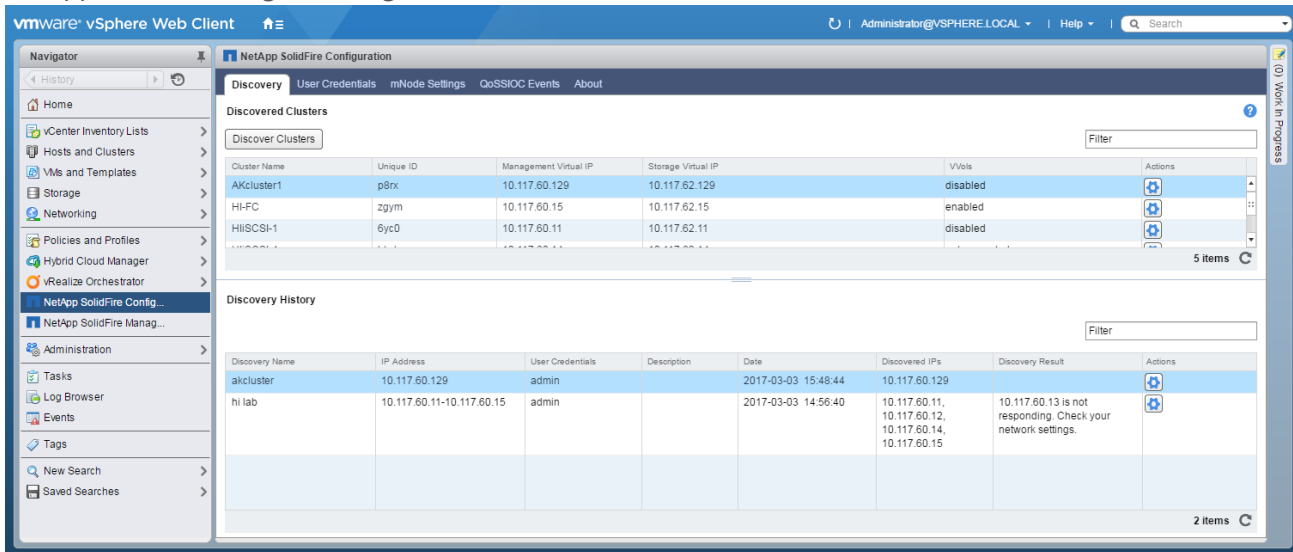
The NetApp SolidFire Plug-in enables you to configure, manage, and monitor SolidFire clusters in the VMware vSphere Web Client.

The Plug-in can be accessed in vSphere either from a global view (vSphere Home page) or contextual view (a host in the vSphere Host and Clusters menu).

Global view allows you to make cluster-wide changes using configuration and management extension points. The **NetApp SolidFire Configuration** extension point allows you to manage cluster discoveries, configure and monitor QoSSIOC events, and control cluster admin user credentials. The **NetApp SolidFire Management** extension point gives you a comparable monitoring and management interface to the Element OS Web UI for central, cluster-wide control of your storage system.

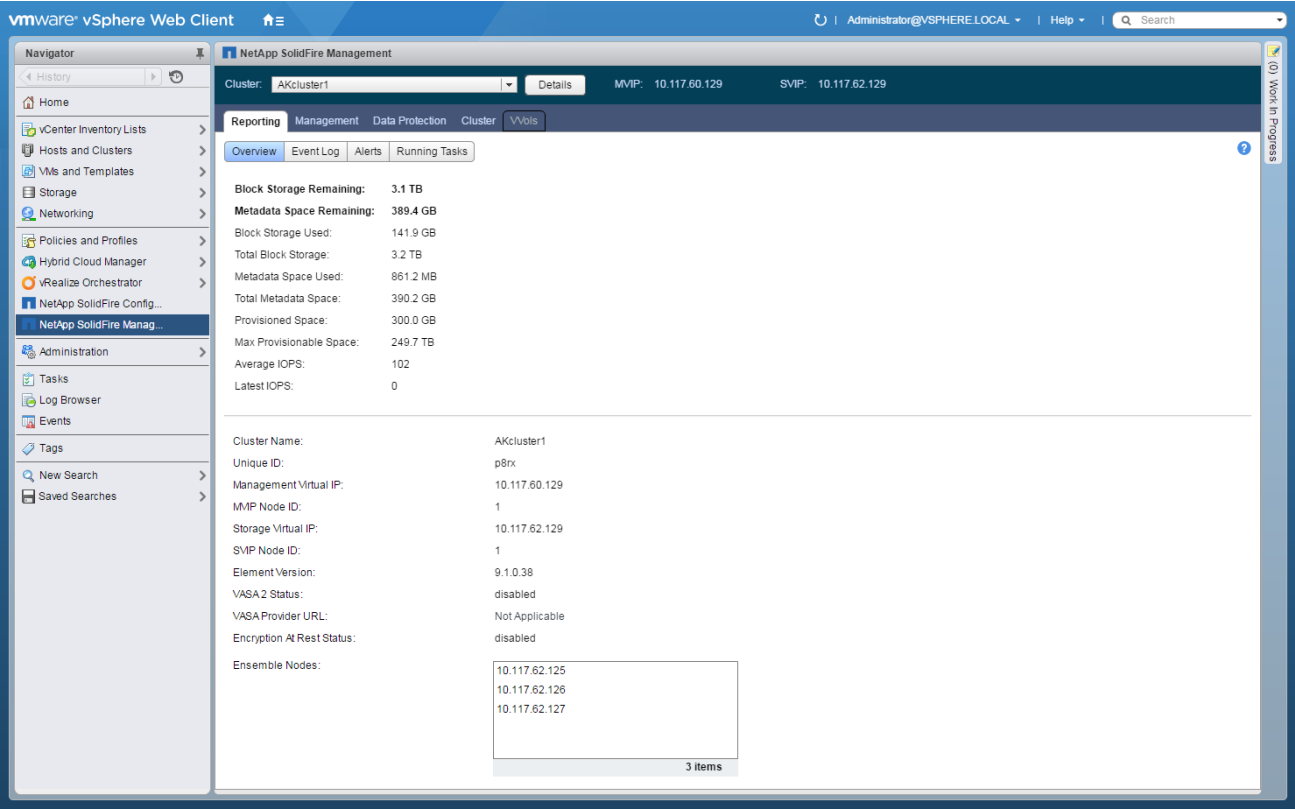
For more granular management of an individual virtual machine or virtual volume, a contextual menu of object-specific management options is available.

NetApp SolidFire Plug-in Configuration Extension Point (Global View)



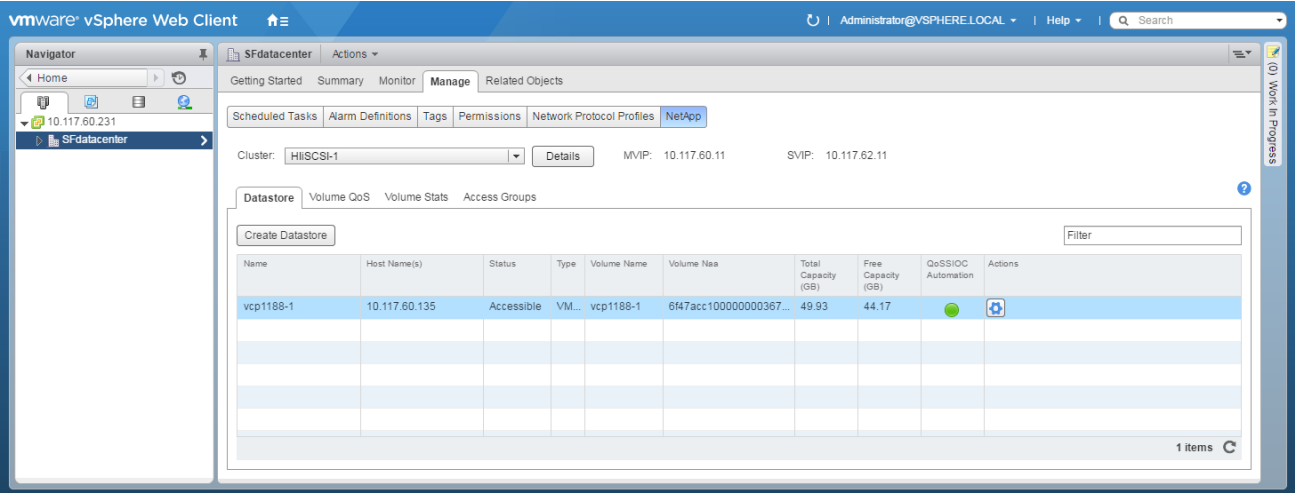
| Tab | Description |
|------------------|---|
| Discovery | Discover clusters and view the history of all discovery requests. |
| User Credentials | Manage Cluster Admin user credentials. |
| mNode Settings | Configure the mNode settings for the QoSSIOC service. |
| QoSSIOC Events | Displays logs for all QoSSIOC errors. |
| About | Displays the NetApp SolidFire Plug-in version number. |

NetApp SolidFire Management Extension Point (Global View)



| Tab | Description |
|-----------------|--|
| Reporting | Displays information about the cluster's components and provides an overview for how the cluster is performing. You can also manage events, cluster faults, and errors from the tab. |
| Management | Create and manage datastores, volumes, user accounts, and access groups. You can also perform backup operations, clones, and snapshots. |
| Data Protection | Manage individual and group snapshots. You can also create schedules for snapshot creation. |
| Cluster | Add and manage drives and nodes. You can also create and manage VLANs. |
| VVols | Manage virtual volumes and their associated storage containers, protocol endpoints, and bindings. |

NetApp SolidFire Plug-in – Hosts and Clusters (Contextual View)



| Tab | Description |
|---------------|--|
| Datastore | Create and manage datastores. |
| Volume QoS | View Quality of Service values that are applied to ensure performance. |
| Volume Stats | View statistics for each volume. |
| Access Groups | Create and manage volume access groups. |

Discovery

The **Discovery** tab allows you to discover clusters that you can then manage from the NetApp SolidFire Management extension point. You can also manage discovery entries and enable Virtual Volumes (VVols) functionality on supported clusters.

See the following topics to learn about or perform discovery-related tasks:

[Discovering a Cluster](#)

[Viewing Discovered Cluster Details](#)

[Cluster Details](#)

[Deleting a Cluster Entry from Discovery](#)

[Rediscovering a Disconnected Cluster](#)

[Enabling Virtual Volumes](#)

Discovering a Cluster

You can specify a cluster to discover and define user credentials for the discovered cluster using the NetApp SolidFire Configuration extension point.

Prerequisites

- At least one cluster must be available for discovery.
- Full cluster admin user credentials for the SolidFire cluster.
- Firewall rules allow open network communication between the vCenter and the SolidFire Cluster MVIP on TCP ports 443 and 8443.

Procedure

1. Go to **NetApp SolidFire Configuration > Discovery**.
2. Click **Discover Clusters**.
3. In the *Discover Clusters* dialog, enter the following:
 - A unique discovery name (required)
 - MVIP address or MVIP address range (required)
 - Description

NOTE: The discovery name and description are recorded in the Discovery History so that clusters can be easily identified and rediscovered.

Best Practices: The SolidFire vCenter Plug-in can discover up to 255 IP addresses per discovery. If your datacenter contains multiple SolidFire clusters, assign MVIP addresses within a 50 IP address range. Use only valid cluster IP addresses to speed up asynchronous discovery.

4. Click **Next**.
5. Select an existing cluster admin user credential or add a new valid cluster admin credential:

NOTE: The credentials must match the current cluster credentials of an existing cluster admin.

| If | Then |
|--|--|
| Cluster admin user credentials have been added: | <ol style="list-style-type: none"> 1. Select a user credential from the list. 2. Proceed with the next step. |
| No cluster admin user credentials have been added: | <ol style="list-style-type: none"> 1. Click Add User Credential. 2. Enter cluster admin credentials: <ul style="list-style-type: none"> • Credential Name: Use any name (can be alphanumeric with special characters) for the credential name. • User ID: Use the existing cluster administrator user name. • Password: Use the existing cluster administrator password. • Description (optional). 3. Click Add. 4. Proceed with the next step. |

6. Click **Next**.

7. Verify the discovery request and click **OK**.

NOTE: To view discovery progress, go to the **Tasks Console** in the vSphere Web Client. You might need to click refresh (C) for both the **Discovered Clusters** and **Discovery History** lists until the discovered cluster appears.

When discovery completes, the discovered cluster appears in the *Discovered Clusters* list and is available to use in the NetApp SolidFire Management extension point.

Viewing Discovered Cluster Details

You can review general and extended details for each discovered cluster using the NetApp SolidFire Configuration extension point.

Procedure

1. Go to **NetApp SolidFire Configuration > Discovery**.

The general information for all cluster discoveries displays in the **Discovered Clusters** or **Discovery History** lists.

2. In the **Discovered Clusters** list, click the **Actions** button (⚙) for the cluster you wish to review.

3. In the resulting menu, select **View Details**.

Cluster Details

Cluster details are available in the NetApp SolidFire Management extension point from either the **Reporting > Overview** page or the **Details** button in the cluster selector. Cluster details are also available from the **Discovery > Discovered Clusters** page of the NetApp SolidFire Configuration extension point.

Cluster Details Available Only in Reporting Overview

| Heading | Description |
|--------------------------|--|
| Block Storage Remaining | The total space remaining on all block drives in the system. |
| Metadata Space Remaining | The space on volume drives remaining to store metadata. |
| Block Storage Used | The space used by all active block drives. |

Cluster Details Available Only in Reporting Overview

| Heading | Description |
|-------------------------|--|
| Total Block Storage | The total space provided by all active block drives. |
| Metadata Space Used | The space on volume drives used to store metadata. |
| Total Metadata Space | The total space on volume drives provided to store metadata. |
| Provisioned Space | Total space provisioned in all volumes on the cluster. |
| Max Provisionable Space | The total amount of provisionable space if all volumes are 100% filled (no thin provisioned metadata). |
| Average IOPs | Average IOPS for the cluster since midnight Coordinated Universal Time (UTC). |
| Latest IOPs | Average IOPS for all volumes in the cluster over the last 5 seconds. |


Cluster Details Available from All Selection Points

| Heading | Description |
|---------------------------|---|
| Cluster Name | The discovery name for the cluster. |
| Unique ID | Unique ID for the cluster. |
| Management Virtual IP | The management virtual IP address (MVIP). |
| MVP Node ID | The node that holds the master MVIP address. |
| Storage Virtual IP | The storage virtual IP address (SVIP). |
| SVIP Node ID | Node holding the master SVIP address. |
| Element Version | The version of the Element OS that the cluster is running. |
| VASA 2 Status | The status of the VASA Provider on SolidFire cluster. |
| VASA Provider URL | The URL of the VASA Provider enabled on the SolidFire cluster, when applicable. |
| Encryption At Rest Status | The status of Encryption at Rest. Possible values: Enabling: Encryption at Rest is being enabled. Enabled: Encryption at Rest is enabled. Disabling: Encryption at Rest is being disabled. Disabled: Encryption at Rest is disabled. |
| Ensemble Nodes | IPs of the nodes that are part of the database ensemble. |

Deleting a Cluster Entry from Discovery

You can use the Discovery History page in the NetApp SolidFire Configuration extension point to remove cluster discoveries that you no longer wish to view.

Procedure



1. Go to **NetApp SolidFire Configuration > Discovery**.
2. Click the **Actions** button () for the cluster entry you want to remove.

3. In the resulting menu, click **Delete**.
4. Confirm the action.

Rediscovering a Disconnected Cluster

You can reconnect to (rediscover) a cluster using the NetApp SolidFire Configuration extension point.

Procedure

1. Go to **NetApp SolidFire Configuration > Discovery**.
2. Under Discovery History, click the **Actions** button () for the cluster entry you want to rediscover.
3. In the resulting menu, click **Rediscover**.
4. Click refresh () , as needed, until a successful reconnection appears in the discovery results.

Enabling Virtual Volumes

You must manually enable vSphere Virtual Volumes (Vvols) functionality through the NetApp SolidFire Configuration extension point. The SolidFire system comes with Vvols functionality disabled by default, and it is not automatically enabled as part of a new installation or upgrade. Enabling the Vvols feature is a one-time configuration task.

Prerequisites

- The SolidFire cluster must be running Element OS version 9.0 or later.
- The SolidFire cluster must be connected to an ESXi 6.0 and later environment that is compatible with Vvols.

Procedure

1. Go to **NetApp SolidFire Configuration > Discovery**.
2. Under **Discovered Clusters**, click the **Actions** () button for the cluster you wish to enable.
3. Click **Enable Vvols**.

CAUTION: Once enabled, Vvols functionality cannot be disabled. Enabling vSphere Virtual Volumes functionality permanently changes Element OS configuration. You should only enable Vvols functionality if your cluster is connected to a VMware ESXi Vvols-compatible environment. You can only disable the Vvols feature and restore the default settings by returning the cluster to the factory image.

4. Click **Yes** to confirm the Virtual Volumes configuration change.

A **VASA Enabled** dialog appears that indicates that the VASA has been enabled on the SolidFire cluster.

NOTE: When Vvols functionality is enabled, the SolidFire cluster starts the VASA Provider, opens port 8444 for VASA traffic, and creates protocol endpoints that can be discovered by vCenter and all ESXi hosts.

5. Copy the VASA Provider URL from the **VASA Enabled** dialog. You will use this URL to register the VASA Provider in vCenter.

NOTE: Additional configuration tasks are required for Vvols. See [Configuring Vvols Functionality](#).

Cluster Admin User Credentials Management

The **User Credentials** tab allows you to create, edit, and delete cluster admin credentials from the NetApp SolidFire Configuration extension point.

See the following topics to learn about or perform discovery-related tasks:

[Creating User Credentials](#)

[Editing User Credentials](#)

[Deleting User Credentials](#)

Creating User Credentials

You can create cluster admin user credentials from the User Credential page in the NetApp SolidFire Configuration extension point or you can create a new cluster admin user credential during cluster discovery. For more details, see [Discovering a Cluster](#).

Prerequisites

The SolidFire cluster administrator user ID and password must be known.

Procedure

1. Go to **NetApp SolidFire Configuration > User Credentials**.
2. Click **Create User Credential**.
3. Enter cluster admin credentials:

NOTE: The credentials must match the current cluster credentials of an existing cluster admin.


- Credential Name: Use any name (can be alphanumeric with special characters) for the credential name.
 - User ID: Use the existing cluster administrator user name.
 - Password: Use the existing cluster administrator password.
 - Description (optional).
4. Click **OK**.

Editing User Credentials

You can edit cluster admin user credentials from the NetApp SolidFire Configuration extension point.

When you change cluster admin user credentials in the Element OS user interface, you must also enter the same cluster admin user credentials in the vCenter Plug-in.

Procedure

1. Go to **NetApp SolidFire Configuration > User Credentials**.
2. From the **User Credentials** list, click the **Actions** button () for the user credentials you want to edit.
3. In the resulting menu, select **Edit**.
4. Change the following as needed:
 - Credential name
 - User ID
 - Password
 - Description

5. Click **OK**.

Deleting User Credentials


You can delete cluster admin user credentials for a specific user from the NetApp SolidFire Configuration extension point.

Prerequisites

The discovery credentials that you are removing are no longer used or the cluster with which they are associated has been removed from the discovery list.

NOTE: Active credentials must be modified or removed from the Element OS user interface.

Procedure

1. Go to **NetApp SolidFire Configuration > User Credentials**.
2. From the **User Credentials** list, click the **Actions** button () for the user credentials you want to remove.
3. In the resulting menu, click **Delete**.
4. Confirm the action.

Configuring mNode Settings for QoSSIOC

You can configure the SolidFire management node (mNode) settings using the NetApp SolidFire Configuration extension point. These configurations are required to be able to enable and use the QoSSIOC service.

Prerequisites

- Change the default user name and password for the SIOC service before using the mNode Settings page for the Plug-in. For instructions, see [Configuring SIOC Service Credentials](#).

Procedure

1. Go to **NetApp SolidFire Configuration > mNode Settings**.
2. Enter the following:

NOTE: User names and passwords can be alphanumeric with special characters except for the following: & () ' ' ` .

- **mNode IP Address:** The IP address of the management node for the cluster that contains the QoSSIOC service.
 - **mNode Port:** The port address for the management node that contains the QoSSIOC service. The default port is 8443.
 - **mNode User Name:** The user name for the SolidFire QoSSIOC service. The default user name is *admin*. See [Configuring SIOC Service Credentials](#) to customize.
 - **mNode Password:** The password for the SolidFire QoSSIOC service. The default password is *solidfire*. See [Configuring SIOC Service Credentials](#) to customize.
 - **Re-enter Password:** Retype the password for the QoSSIOC service.
 - **vCenter User Name:** The user name for the vCenter admin with full Administrator role privileges.
 - **vCenter Password:** The password for the vCenter admin with full Administrator role privileges.
 - **Re-enter Password:** Retype the password for the vCenter admin.
3. Click **OK**.

The QoSSIOC **Status** field displays **UP** when the Plug-in can successfully communicate with the service.

NOTE: The QoSSIOC status does not dynamically update. Click refresh (🔄) to see the current status.

NOTE: Once you have configured a valid mNode, these settings become the default. The mNode settings revert to the last known valid mNode settings until you provide settings for another valid mNode.

Configuring SIOC Service Credentials

It is highly recommended that you change the default user name and password for the SIOC service before using the mNode Settings page for the vCenter Plug-in.

Procedure

1. On the management node, create a properties file in **/opt/solidfire/sioc/** and name it `app.properties`.
2. Add the following lines to the file that include a custom user name and password:
`security.user.name=<User name>`
`security.user.password=<Password>`
3. Change ownership and hide the file from other users:
`chown solidfire:solidfire /opt/solidfire/sioc/app.properties`
`chmod 700 /opt/solidfire/sioc/app.properties`
4. Open the `sioc.conf` file in **/etc/init/**.

5. Locate the following line:

```
sudo -u solidfire java -Xmx1024m -Xms256m -jar /opt/solidfire/sioc/solidfire-sioc-<version number>-boot.jar
```
6. Append user name and password changes:

```
sudo -u solidfire java -Xmx1024m -Xms256m -jar /opt/solidfire/sioc/solidfire-sioc-<version number>-boot.jar --spring.config.location=classpath:/application.properties,/opt/solidfire/sioc/app.properties
```
7. Restart the SIOC service.

```
sudo service sioc restart
```
8. After approximately a minute, open `sioc.log` in `/var/log` to verify that the SIOC service started successfully.

```
2016-06-01 13:02:41,885 46271 [main] INFO com.solidfire.sioc.SiocService - Started SiocService in 44.951 seconds (JVM running for 47.415)
```
9. Enter the user ID and password from the `app.properties` file in **NetApp SolidFire Configuration > mNode Settings**.

Viewing QoSSIOC Events

You can view QoSSIOC events from the NetApp SolidFire Configuration extension point. A QoSSIOC event is reported when a VM is powered on or off that has a datastore with QoS enabled.

Prerequisites

- At least one cluster must be discovered and running.
- The QoSSIOC service must be configured and running using the mNode Settings page for the Plug-in.
- At least one datastore must have QoSSIOC automation enabled.

Procedure

1. Go to **NetApp SolidFire Configuration > QoSSIOC Events**.

The *QoSSIOC Events* page displays a list of events.

QoSSIOC Event Details

On the **QoSSIOC Events** page of the NetApp SolidFire Management extension point, you can view the following information for QoSSIOC events for each cluster.

| Heading | Description |
|----------------|---|
| Date | The date and time of the QoSSIOC event. |
| Datastore Name | The user-defined datastore name. |
| Cluster IP | The IP address of the cluster containing the datastore from which the event originated. |
| Volume ID | The system-generated ID for the associated volume. |
| Min IOPs | The current minimum IOPS QoS setting of the volume. |
| Max IOPs | The current maximum IOPS QoS setting of the volume. |
| Burst IOPs | The current maximum burst QoS setting of the volume. |
| Burst Time | The length of time a burst is allowed. |

Reporting

The **Reporting** tab gives you information about the cluster's components and provides an overview for how the cluster is performing. Reporting opens up into an overview of the cluster components and resources.

See the following topics to learn about or perform reporting tasks:

[Cluster Details](#)

[Viewing Event Logs](#)

[Event Log](#)

[Event Types](#)

[Alerts](#)

[Alert Error Codes](#)

[Running Tasks](#)

Cluster Details

Cluster details are available in the NetApp SolidFire Management extension point from either the **Reporting > Overview** page or the **Details** button in the cluster selector. Cluster details are also available from the **Discovery > Discovered Clusters** page of the NetApp SolidFire Configuration extension point.

Cluster Details Available Only in Reporting Overview

| Heading | Description |
|--------------------------|--|
| Block Storage Remaining | The total space remaining on all block drives in the system. |
| Metadata Space Remaining | The space on volume drives remaining to store metadata. |
| Block Storage Used | The space used by all active block drives. |
| Total Block Storage | The total space provided by all active block drives. |
| Metadata Space Used | The space on volume drives used to store metadata. |
| Total Metadata Space | The total space on volume drives provided to store metadata. |
| Provisioned Space | Total space provisioned in all volumes on the cluster. |
| Max Provisionable Space | The total amount of provisionable space if all volumes are 100% filled (no thin provisioned metadata). |
| Average IOPs | Average IOPS for the cluster since midnight Coordinated Universal Time (UTC). |
| Latest IOPs | Average IOPS for all volumes in the cluster over the last 5 seconds. |

Cluster Details Available from All Selection Points

| Heading | Description |
|-----------------------|---|
| Cluster Name | The discovery name for the cluster. |
| Unique ID | Unique ID for the cluster. |
| Management Virtual IP | The management virtual IP address (MVIP). |

Cluster Details Available from All Selection Points

| Heading | Description |
|---------------------------|---|
| MVP Node ID | The node that holds the master MVIP address. |
| Storage Virtual IP | The storage virtual IP address (SVIP). |
| SVIP Node ID | Node holding the master SVIP address. |
| Element Version | The version of the Element OS that the cluster is running. |
| VASA 2 Status | The status of the VASA Provider on SolidFire cluster. |
| VASA Provider URL | The URL of the VASA Provider enabled on the SolidFire cluster, when applicable. |
| Encryption At Rest Status | The status of Encryption at Rest. Possible values: Enabling: Encryption at Rest is being enabled. Enabled: Encryption at Rest is enabled. Disabling: Encryption at Rest is being disabled. Disabled: Encryption at Rest is disabled. |
| Ensemble Nodes | IPs of the nodes that are part of the database ensemble. |

Viewing Event Logs

You can review event logs for operations performed on the selected cluster along with cluster faults that might occur. Most errors are resolved automatically by the system. Other faults might require manual intervention.

NOTE: The page does not automatically update and must be manually refreshed for new events.

Procedure

1. Go to **NetApp SolidFire Management > Reporting**.
2. Click on the **Event Log** sub-tab.
A list of all events on the cluster displays.
3. Click the **Actions** button (⚙️) for an individual event you wish to review.
4. In the resulting menu, select **View Details**.
The cluster event details message is listed.

Event Log

On the **Reporting > Event Log** page of the NetApp SolidFire Management extension point, you can view information about events detected in the system.

The event log displays key events for the cluster. You can view a detailed Cluster Event message if you click the **Actions** button (⚙️) for an event log and then click **View Details**.

NOTE: The page does not automatically update and must be manually refreshed for new events.

| Heading | Description |
|------------|---|
| Event ID | Unique ID associated with each event. |
| Event Type | The type of event being logged; for example, API events or clone events. |
| Message | Message associated with the event. |
| Service ID | The ID of the service that reported the event (if applicable). The value is "0" (zero) if the fault is not associated with a service. |
| Node | The ID of the node that reported the event (if applicable). |
| Drive ID | The ID of the drive that reported the event (if applicable). |
| Event Time | The date and time the event occurred. |

Event Types

The system reports multiple types of events; each event is an operation that the system has completed. Events can be routine, normal events or events that require administrator attention. The **Event Type** column on the **Event Log** page indicates in which part of the system the event occurred.

NOTE: The system does not log read-only API commands in the event log.

The following table describes the types of events that might appear in the event log.

| Event Type | Description |
|-----------------------|--|
| apiEvent | Events initiated by a user through an API or Web UI that modify settings. |
| binAssignmentsEvent | Events related to the assignment of data bins. Bins are essentially containers that hold data and are mapped across the cluster. |
| BinSyncEvent | System events related to a reassignment of data among block services. |
| BsCheckEvent | System events related to block service checks. |
| bulkOpEvent | Events related to operations performed on an entire volume, such as a backup, restore, snapshot, or clone. |
| cloneEvent | Events related to volume cloning. |
| clusterMasterEvent | Events appearing upon cluster initialization or upon configuration changes to the cluster, such as adding or removing nodes. |
| dataEvent | Events related to reading and writing data. |
| dbEvent | Events related to the global database maintained by ensemble nodes in the cluster. |
| driveEvent | Events related to drive operations. |
| encryptionAtRestEvent | Events related to the process of encryption on a cluster. |
| ensembleEvent | Events related to increasing or decreasing the number of nodes in an ensemble. |
| fibreChannelEvent | Events related to the configuration of and connections to the Fibre Channel nodes. |

| Event Type | Description |
|-----------------------|--|
| gcEvent | Events related to processes run every 60 minutes to reclaim storage on block drives. This process is also known as garbage collection. |
| ieEvent | Internal system error. |
| installEvent | Automatic software installation events. Software is being automatically installed on a pending node. |
| iSCSIEvent | Events related to iSCSI issues in the system. |
| limitEvent | Events related to the number of volumes or virtual volumes in an account or in the cluster nearing the maximum allowed. |
| networkEvent | Events related to the status of virtual networking. |
| platformHardwareEvent | Events related to issues detected on hardware devices. |
| remoteClusterEvent | Events related to remote cluster pairing. |
| serviceEvent | Events related to system service status. |
| statEvent | Events related to system statistics. |
| sliceEvent | Events related to the Slice Server, such as removing a metadata drive or volume. |
| snmpTrapEvent | Events related to SNMP traps. |
| schedulerEvent | Events related to scheduled snapshots. |
| tsEvent | Events related to the system transport service. |
| unexpectedException | Events related to unexpected system exceptions. |
| vasaProviderEvent | Events related to a VASA (vSphere APIs for Storage Awareness) Provider. |

Alerts

Alerts are cluster faults or errors and are reported as they occur on the currently selected cluster. Alerts can be information, warnings, or errors and are a good indicator of how well the cluster is running. Most errors resolve themselves automatically; however, some may require manual intervention.

On the **Reporting > Alerts** page of the NetApp SolidFire Management extension point, you can view information about individual system alerts.

NOTE: The page does not automatically update and must be manually refreshed for new alerts.

After the system resolves an alert, all information about the alert including the date it was resolved is moved to the **Resolved** area.

The following table describes the columns on the page.

| Heading | Description |
|----------|--------------------------------|
| Alert ID | Unique ID for a cluster alert. |

| Heading | Description |
|-----------------|--|
| Severity | <p>warning: A minor issue that may soon require attention. System upgrades are still allowed at this severity level.</p> <p>error: A failure that may cause performance degradation or loss of high availability (HA). Errors generally should not affect service otherwise.</p> <p>critical: A serious failure that affects service. The system is unable to serve API or client I/O requests. Operating in this state could lead to potential loss of data.</p> <p>bestPractice: A recommended system configuration best practice is not being used.</p> |
| Type | <p>node: Fault affecting an entire node.</p> <p>drive: Fault affecting an individual drive.</p> <p>cluster: Fault affecting the entire cluster.</p> <p>service: Fault affecting a service on the cluster.</p> |
| Node | Node ID for the node that this fault refers to. Included for node and drive faults, otherwise set to - (dash). |
| Drive ID | Drive ID for the drive that this fault refers to. Included for drive faults, otherwise set to - (dash). |
| Resolution Date | The date and time the fault was resolved. This information is only available in the Resolved alerts page. |
| Error Code | A descriptive code that indicates what caused the fault. |
| Details | Detailed description of the fault. |
| Alert Time | The date and time the fault was logged. |

Alert Error Codes

The system reports error codes with each alert on the **Alerts** page. Error codes help you determine what component of the system experienced the alert, and you can learn more about why the alert was generated using the information in the **Details** column. The following table outlines the different types of system alerts.

| Alert Type | Description |
|-------------------------------|---|
| BlockServiceTooFull | A block service is using too much space and running low on capacity. |
| BlockServiceUnhealthy | The SolidFire Application cannot communicate with a Block Service. If this condition persists, the system relocates the data to another drive. Once the system relocates the data, you should reboot the unhealthy node to restore communication. |
| ClusterCannotSync | There is an out of space condition and data on the offline block storage drives cannot be synced to drives that are still active. |
| ClusterFull | <p>Stage 3 Cluster Full: Add additional capacity or free up capacity as soon as possible.</p> <p>Stage 4 Cluster Full: Due to high capacity consumption Helix data protection will not recover if a node fails. Creating new Volumes or Snapshots is not permitted until additional capacity is available. Add additional capacity or free up capacity immediately.</p> |
| ClusterIOPSAreOverProvisioned | The sum of all minimum QoS IOPS is greater than the expected IOPS of the cluster. The system cannot maintain minimum QoS in this condition. IOPS may need to be adjusted. |

| Alert Type | Description |
|--|---|
| DisconnectedClusterPair | Paired clusters have become disconnected. Reestablish communication between the clusters. |
| DriveWearFault | A drive may need attention due to wear. |
| EnsembleDegraded | Power or network connectivity has been lost to one or more of the ensemble nodes. Restore network connectivity or power to the affected node. |
| Exception | A non-routine fault has been detected. This fault will not be cleared. Contact NetApp SolidFire Support to resolve the exception fault. |
| FailedSpaceTooFull | A Slice Service is using space reserved for failed writes. Contact NetApp SolidFire Support. |
| FibreChannelAccessDegraded | A Fibre Channel node has stopped responding to the storage nodes in the cluster. |
| FibreChannelAccessUnavailable | All Fibre Channel nodes have become disconnected. |
| InconsistentMtus | Bond1G mismatch: Inconsistent MTUs detected on Bond1G interfaces. MTU to nodeID mapping: <mapping of MTUs to nodes>. Bond10G mismatch: Inconsistent MTUs detected on Bond10G interfaces. MTU to nodeID mapping: <mapping of MTUs to nodes> . |
| InvalidConfiguredFibreChannelNodeCount | There is only one Fibre Channel node configured in a cluster. For proper Fibre Channel operation, at least two Fibre Channel nodes must be configured in a cluster. |
| notUsingLACPBondMode | LACP bonding mode is not configured. NetApp strongly recommends using LACP bonding when deploying SF-Series 19210 and newer nodes; clients may experience timeouts if LACP is not configured. |
| SliceServiceUnhealthy | The SolidFire Application cannot communicate with a metadata service. |
| SliceServiceTooFull | A Slice Service is using too much space and running low on capacity. |
| ProvisionedSpaceTooFull | The overall provisioned capacity of the cluster is too full. |
| VolumeDegraded | Secondary volumes have not finished replicating and syncing. |
| NodeHardwareFault | The system has detected a hardware misconfiguration or a component that is not functioning as expected. |
| Upgrade | The software on one or more nodes is being upgraded. |
| UnbalancedMixedNodes | The storage on the mix of nodes in a cluster has become unbalanced in a way that may degrade performance. |

Running Tasks

On the **Reporting > Running Tasks** page of the NetApp SolidFire Management extension point, you can view information about running tasks in the system that are reported by *ListSyncJobs* and *ListBulkVolumeJobs* API methods.

| Heading | Description |
|------------------|--|
| Task Type | The type of sync job or bulk volume job. Possible values: read write clone remote slice block |
| Node | Specifies the ID of the node onto which the clone is being written. This ID is only present if the task type is clone . |
| Task Description | List of objects describing sync processes or an array of information for each bulk volume job currently running in the system. |
| Current Progress | Number of bytes the clone has processed in the source volume. This information is only present if the task type is clone or slice . |
| Elapsed Time | The time elapsed, in seconds, since the job started. |
| Remaining Time | Estimated time, in seconds, to complete the operation. |

Management

The **Management** tab enables you to create and manage datastores, volumes, accounts, and access groups.

See the following topics to learn about or perform management tasks:

[Datastore Management](#)

[Creating a Datastore](#)

[Viewing the Datastore List](#)

[Datastore Details](#)

[Extending a Datastore](#)

[Cloning a Datastore](#)

[Sharing a Datastore](#)

[Enabling VAAI UNMAP](#)

[Deleting a Datastore](#)

[QoSSIOC Automation](#)

[Enabling QoSSIOC Automation](#)

[Disabling QoSSIOC Integration](#)

Datastore Management

The NetApp SolidFire Plug-in enables you to manage datastores that are created on SolidFire volumes. You can create, extend, clone, share, or delete datastores. You can also use VAAI UNMAP to allow a cluster to reclaim freed block space from thinly provisioned VMFS datastores.

Datastores can be managed on both Global and Contextual Views. The Global View contains all datastores created on SolidFire volumes associated with the cluster, whereas Contextual View is limited by the selected context. Create, extend, clone, share, and delete datastore operations can be monitored using the vSphere Task Console.

Creating a Datastore

You can create a datastore from either the Global View using the NetApp SolidFire Management extension point or Contextual View.

Prerequisites

- At least one cluster must be discovered and running.
- If two or more clusters are discovered, the cluster you intend to use for the task must be selected.
- At least one host must be connected to vCenter server.

Procedure

1. In the vSphere Web Client, do the following:

| If | Then |
|----------------------------|---|
| Using the Global View: | <ol style="list-style-type: none">1. Go to NetApp SolidFire Management > Management.2. Proceed to the next step. |
| Using the Contextual View: | <ol style="list-style-type: none">1. Click Hosts and Clusters.2. In the <i>Hosts and Clusters</i> Contextual View, select the datacenter, cluster, or host. |

| If | Then |
|----|--|
| | <p>3. Click the Manage tab, and then click the NetApp tab.</p> <p>NOTE: For vSphere 6.5, click the Configure tab to find NetApp within the list of options.</p> <p>4. Proceed to the next step.</p> |

2. From the **Datastore** page, click **Create Datastore**.
3. In the *Create Datastore* dialog , enter a name for the datastore.
4. Click **Next**.
5. If you are using the Global View, select the required host for the datastore.
6. Select an existing volume or create a new volume for the new datastore.
7. Click **Next**.
8. Configure host access by selecting one of the following:
 - a. **Use Volume Access Group**
 - OR
 - b. **Use CHAP**

NOTE: Use CHAP for secure secret-based access with no limits on initiators. Use volume access group to explicitly limit which initiators can see volumes.

9. Click **Next**.
10. If you selected **Use Volume Access Group**, configure the volume access group information for the selected host. If no volume access group is found, create a new access group with the available IQN or WWPN.

NOTE: If there is one volume access group, the wizard defaults to this option.

11. Click **Next**.
12. If you want to enable QoSSIOC automation, click the **Enable QoS & SIOC Integration** check box to select it and then configure the QoSSIOC settings.

NOTE: If the QoSSIOC service is not available, you must first configure settings in the **mNode Settings** page in the NetApp Configuration extension point.

13. Click **Next**.
14. Confirm the selections and click **OK**.
15. Click refresh (🔄) if needed until the datastore appears in the list.

Viewing the Datastore List

Available datastores are displayed in the **Datastore** tab from Global or Contextual Views.

Procedure

1. In the vSphere Web Client, do one of the following to view the datastore list:

| If | Then |
|----------------------------|---|
| Using the Global View: | <ol style="list-style-type: none"> Go to NetApp SolidFire Management > Management. <p>The Datastore page appears and shows all current datastores on SolidFire and ESXi (related by discovery).</p> |
| Using the Contextual View: | <ol style="list-style-type: none"> Click Hosts and Clusters. <p>The <i>Hosts and Clusters</i> Contextual View displays.</p> <ol style="list-style-type: none"> Select the datacenter, cluster, or host. Click the Manage tab and then click the NetApp tab. <div> <p>NOTE: For vSphere 6.5, click the Configure tab to find NetApp within the list of options.</p> <p>The Datastore page appears and shows all current datastores filtered based on the context selection. For example, if a cluster is selected, the Plug-in displays the SolidFire datastores for that cluster only.</p> </div> |

NOTE: Datastores spanning multiple volumes (mixed datastores) are not listed.

NOTE: Datastore views will only show datastores that are available on ESXi hosts from the selected SolidFire cluster.

Datastore Details

On the **Management > Datastores** page of the NetApp SolidFire Management extension point or from the **Datastore** tab in Contextual View, you can view the following information for all datastores on the cluster.

| Heading | Description |
|---------------------|---|
| Name | The name assigned to the datastore. |
| Host Name(s) | The address of the host device. |
| Status | Indicates if the datastore is currently connected to vSphere. |
| Type | The VMware files system datastore type. |
| Volume Name | The name assigned to the associated volume. |
| Volume Naa | Globally unique SCSI device identifier for the associated volume in NAA IEEE Registered Extended format. |
| Total Capacity (GB) | Total formatted capacity of the datastore. |
| Free Capacity (GB) | Space that is available for the datastore. |
| QoSSIOC Automation | <p>Button that enables QoSSIOC automation and indicates QoSSIOC status.</p> <p>Grey: QoSSIOC is not enabled.</p> <p>Green: QoSSIOC is enabled.</p> <p>Orange: Volume Max QoS has exceeded the limit value specified.</p> |

Extending a Datastore


You can extend a datastore to increase volume size and extend the VMFS volume related to that datastore.

You can extend datastores from either the Global View using the NetApp SolidFire Management extension point or Contextual View.


Procedure

1. In the vSphere Web Client, do the following:

| If | Then |
|----------------------------|--|
| Using the Global View: | <ol style="list-style-type: none">1. Go to NetApp SolidFire Management > Management.2. Proceed to the next step. |
| Using the Contextual View: | <ol style="list-style-type: none">1. Click Hosts and Clusters.2. In the <i>Hosts and Clusters</i> Contextual View, select the datacenter, cluster, or host.3. Click the Manage tab, and then click the NetApp tab. <div>NOTE: For vSphere 6.5, click the Configure tab to find NetApp within the list of options.</div> <ol style="list-style-type: none">4. Proceed to the next step. |

2. From the **Datastore** page, click the **Actions** button () for the datastore you wish to extend.
3. In the resulting menu, click **Extend**.
4. In the **New Datastore Size** field, type the required size for the new datastore and select GB or GiB.

NOTE: The datastore size cannot exceed the unprovisioned space available on the selected cluster or the maximum volume size the cluster allows.

5. Click **OK**.
6. Click refresh () if needed until the datastore appears in the list.

Cloning a Datastore

The NetApp Plug-in provides the functionality to clone datastores, which includes mounting the new datastore to the desired ESXi server or cluster. You can name the datastore clone and configure its QoS, volume, host, and volume access group settings.

You can clone datastores from either the Global View using the NetApp SolidFire Management extension point or Contextual View.

Prerequisites

- At least one cluster must be discovered and running.
- If two or more clusters are discovered, the cluster you intend to use for the task must be selected.
- Available unprovisioned space must be equal to or more than the source volume size.

Procedure

1. In the vSphere Web Client, do the following:

| If | Then |
|------------------------|---|
| Using the Global View: | <ol style="list-style-type: none">1. Go to NetApp SolidFire Management > Management.2. Proceed to the next step. |

| If | Then |
|----------------------------|--|
| Using the Contextual View: | <ol style="list-style-type: none"> 1. Click Hosts and Clusters. 2. In the <i>Hosts and Clusters</i> Contextual View, select the datacenter, cluster, or host. 3. Click the Manage tab, and then click the NetApp tab. <div data-bbox="704 464 1477 562" data-label="Text"> <p>NOTE: For vSphere 6.5, click the Configure tab to find NetApp within the list of options.</p> </div> 4. Proceed to the next step. |

2. From the **Datastore** page, click the **Actions** button (⚙️) for the datastore you wish to clone.
3. In the resulting menu, click **Clone**.

NOTE: If you attempt to clone a datastore that contains virtual machines with attached disks not located on the selected datastore, copies of the virtual machines on the cloned datastore will not be added to the virtual machine inventory.

4. Enter a datastore name and click **Next**.
5. Enter the volume name and configure the volume by applying QoS settings.

NOTE: You can apply default QoS settings again by clicking **Restore Default QoS**.

6. Click **Next**.
7. Configure host access by selecting one of the following:
 - a. **Use Volume Access Group**
 - OR
 - b. **Use CHAP**

NOTE: Use CHAP for secure secret-based access with no limits on initiators. Use volume access group to explicitly limit which initiators can see volumes.

8. Click **Next**.
9. If you selected **Use Volume Access Group**, configure the volume access group information for the selected host. If no volume access group is found, create a new access group with the available IQN or WWPN.

NOTE: If there is one volume access group, the wizard defaults to this option.

10. Click **Next**.
11. If you want to enable QoSSIOC automation, click the **Enable QoS & SIOC Integration** check box to select it and then configure the QoSSIOC settings.

NOTE: If the QoSSIOC service is not available, you must first configure settings in the **mNode Settings** page in the SolidFire Configuration extension point.

12. Click **Next**.
13. Confirm the selections and click **OK**.

14. Click refresh () if needed if the datastore clone does not appear in the list.

Sharing a Datastore

You can share a selected datastore with one or more hosts.

You can share datastores from either the Global View using the NetApp SolidFire Management extension point or from the cluster or data center level in Contextual View.

NOTE: Datastores can be shared only among hosts within the same data center.


Prerequisites

- At least one cluster must be discovered and running.
- If two or more clusters are discovered, the cluster you intend to use for the task must be selected.
- There must be more than one host under the selected data center.

Procedure

1. In the vSphere Web Client, do the following:

| If | Then |
|----------------------------|---|
| Using the Global View: | <ol style="list-style-type: none">1. Go to NetApp SolidFire Management > Management.2. Proceed to the next step. |
| Using the Contextual View: | <ol style="list-style-type: none">1. Click Hosts and Clusters.2. In the <i>Hosts and Clusters</i> Contextual View, select the datacenter, cluster, or host.3. Click the Manage tab, and then click the NetApp tab.<div>NOTE: For vSphere 6.5, click the Configure tab to find NetApp within the list of options.</div>4. Proceed to the next step. |

2. From the **Datastore** page, click the **Actions** button () for the datastore you wish to share.
3. In the resulting menu, click **Share**.
4. Configure host access by selecting one of the following:
 - a. **Use Volume Access Group**OR
 - b. **Use CHAP**

NOTE: Use CHAP for secure secret-based access with no limits on initiators. Use volume access group to explicitly limit which initiators can see volumes.

5. Click **Next**.

6. Do one of the following:

| If | Then |
|---|---|
| Use Volume Access Group is selected: | <ol style="list-style-type: none"> Configure the Volume Access Group: <ol style="list-style-type: none"> Select one or more volume access groups from the list. If no volume access group is available, select one or more hosts, click Create New VAG, and select the newly created volume access group. If some of the available hosts are not part of any available access groups, select the required access group from the drop-down list and click Add Host(s) to VAG. Click Next. |
| Use CHAP is selected: | <ol style="list-style-type: none"> Select one or more hosts from the list. Click Next. |

7. Confirm the selections and click **OK**.

8. Click  to refresh the datastore list after the share datastore task is complete to verify hosts for the datastore.

Enabling VAAI UNMAP

The VAAI UNMAP feature allows a cluster to reclaim freed block space from thinly provisioned VMFS datastores.

NOTE: For a larger discussion of VAAI and cloning, see this [article](#) from VMware.

Prerequisites

- Ensure that the ESXi host system settings are enabled for VAAI UNMAP (`esxcli system settings advanced list -o /VMFS3/EnableBlockDelete`). The integer value must be set to 1 to enable.
- If the ESXi host system settings are not enabled for VAAI UNMAP, set the integer value to 1 with the command `esxcli system settings advanced set -i 1 -o /VMFS3/EnableBlockDelete`.

Procedure

1. In the vSphere Web Client, do the following:

| If | Then |
|----------------------------|--|
| Using the Global View: | <ol style="list-style-type: none"> Go to NetApp SolidFire Management > Management. Proceed to the next step. |
| Using the Contextual View: | <ol style="list-style-type: none"> Click Hosts and Clusters. In the <i>Hosts and Clusters</i> Contextual View, select the datacenter, cluster, or host. Click the Manage tab, and then click the NetApp tab. <div data-bbox="716 1736 1445 1797" data-label="Text"> <p>NOTE: For vSphere 6.5, click the Configure tab to find NetApp within the list of options.</p> </div> Proceed to the next step. |

2. From the **Datastore** page, click the **Actions** button () for the datastore on which you wish to use VAAI UNMAP.

3. In the resulting menu, click **VAAI Unmap**.
4. Enter a host user name and password for the datastore.
5. Confirm the selections and click **OK**.

Deleting a Datastore

You can delete a datastore using the NetApp SolidFire vCenter Plug-in. This operation permanently deletes all the files associated with the VMs on the datastore that you want to delete.

You can delete datastores from either the Global View using the NetApp SolidFire Management extension point or Contextual View.

Procedure

1. In the vSphere Web Client, do the following:

| If | Then |
|----------------------------|---|
| Using the Global View: | <ol style="list-style-type: none"> 1. Go to NetApp SolidFire Management > Management. 2. Proceed to the next step. |
| Using the Contextual View: | <ol style="list-style-type: none"> 1. Click Hosts and Clusters. 2. In the <i>Hosts and Clusters</i> Contextual View, select the datacenter, cluster, or host. 3. Click the Manage tab, and then click the NetApp tab. <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>NOTE: For vSphere 6.5, click the Configure tab to find NetApp within the list of options.</p> </div> <ol style="list-style-type: none"> 4. Proceed to the next step. |

2. From the **Datastore** page, click the **Actions** button (⚙️) for the datastore you wish to delete.
3. In the resulting menu, click **Delete**.
4. (Optional) If you want to delete the volume that is associated with the datastore, click the **Delete Associated Volume** check box to select it.

NOTE: You can also choose to retain the volume and later associate it with another datastore.

5. Click **OK**.

QoSSIOC Automation

The NetApp SolidFire vCenter Plug-in allows, as an optional setting, automatic quality of service (QoS) based on storage I/O control (SIOC) settings of all VMs on a datastore. This QoS and SIOC integration (QoSSIOC), which can be enabled for datastores in the user interface, runs a scan of all SIOC settings on all associated VMs. The QoSSIOC service uses the sum of all SIOC reservations or shares and the sum of IOPS limits to determine minimum and maximum QoS for the underlying volume of each datastore. A configurable burst factor is also available.

QoSSIOC Automation for dbag

Configure QoSSIOC integration to optimize performance by virtual machines by leveraging NetApp SolidFire QoS and vSphere SIOC.

☒ Enable QoS & SIOC Integration

Burst Factor:

☒ Override Default QoS

Shares:

Limit IOPS:

Refer to your VMware documentation on customizing VM disk shares.

OK

Cancel

| Option | Description |
|-------------------------------|---|
| Enable QoS & SIOC Integration | Enables the automatic monitoring of SIOC values for each VMDK on a datastore and sets QoS values for the underlying volume according to those values. |
| Burst Factor | Multiplier of the sum of SIOC IOPS limit values from each VMDK that determines the burst IOPS contribution for the underlying volume. |
| Override Default QoS | Enables the use of Shares and Limit IOPS values. These values can be used when SIOC settings for each VM are set to default. |
| Shares | The contribution of minimum IOPS from each VMDK if the SIOC settings are set to default. |
| Limit IOPS | The contribution of maximum IOPS from each VMDK if the SIOC settings are set to default. |

When SIOC settings for a VMDK are at the default shares level of Normal and the default IOPS limit of Unlimited, the Shares and Limit IOPS values contribute toward the total QoS for the underlying volume. If the SIOC settings for the VMDK are not at default levels, SIOC shares contribute to Min QoS and SIOC IOPS limit values contribute to Max QoS for the underlying volume.

NOTE: It is possible to set a reservation value through vSphere API. If a reservation value is set for a VMDK, shares are ignored and the reservation value is used instead.

Enabling QoSSIOC Automation

You can enable QoSSIOC automation and customize virtual machine disk (VMDK) performance levels.

You can enable QoSSIOC integration from either the Global View using the NetApp SolidFire Management extension point or Contextual View.

NOTE: If you change versions of vCenter, check your datastore QoSSIOC settings to verify that they are set as desired.

Prerequisites

- You have configured the QoSSIOC service settings in the **mNode Settings** page in the NetApp SolidFire Configuration extension point.

Procedure

- In the vSphere Web Client, do the following:

| If | Then |
|----------------------------|---|
| Using the Global View: | <ol style="list-style-type: none">Go to NetApp SolidFire Management > Management.Proceed to the next step. |
| Using the Contextual View: | <ol style="list-style-type: none">Click Hosts and Clusters.In the <i>Hosts and Clusters</i> Contextual View, select the datacenter, cluster, or host.Click the Manage tab, and then click the NetApp tab.<div>NOTE: For vSphere 6.5, click the Configure tab to find NetApp within the list of options.</div>Proceed to the next step. |

- Click the button in the **QoSSIOC Automation** column for the selected datastore.

TIP: Ensure that the datastore does not have QoSSIOC integration enabled on another vCenter to prevent unexpected changes in QoS.

- Click the **Enable QoS & SIOC Integration** check box.

NOTE: Selecting the **Enable QoS & SIOC Integration** check box automatically enables the **Override Default QoS** setting. If the **Override Default QoS** setting is disabled for the datastore, the **Shares** and **Limit IOPS** values are automatically set based on the default SIOC settings of each VM.

TIP: Do not customize the SIOC share limit without also customizing the SIOC IOPS limit. Retaining **Unlimited** as a value might set **Max QoS** values beyond your desired range in QoSSIOC.

- Configure the **Burst Factor**.

NOTE: The burst factor is a multiple of the IOPS limit (SIOC) setting for the VMDK. If you change the default, make sure to use a burst factor value that will not exceed the maximum burst limit for a SolidFire volume when the burst factor value is multiplied by the IOPS limit for any VMDK.

- (Optional) Click the **Override Default QoS** check box to disable it.
- Click **OK**.

NOTE: When you enable the QoSSIOC Automation for a datastore, the button color changes from grey to green. When the volume Max QoS exceeds the limit value specified, the button color changes to orange.

Disabling QoSSIOC Integration

You can clear the QoSSIOC automation settings to disable QoSSIOC integration.

You can disable QoSSIOC integration from either the Global View using the NetApp SolidFire Management extension point or Contextual View.

Procedure

1. In the vSphere Web Client, do the following:

| If | Then |
|----------------------------|---|
| Using the Global View: | <ol style="list-style-type: none">1. Go to NetApp SolidFire Management > Management.2. Proceed to the next step. |
| Using the Contextual View: | <ol style="list-style-type: none">1. Click Hosts and Clusters.2. In the <i>Hosts and Clusters</i> Contextual View, select the datacenter, cluster, or host.3. Click the Manage tab, and then click the NetApp tab.<div>NOTE: For vSphere 6.5, click the Configure tab to find NetApp within the list of options.</div>4. Proceed to the next step. |

2. Click the button in the **QoSSIOC Automation** column for the selected datastore.
3. Clear the **Enable QoS & SIOC Integration** check box to disable the integration.

NOTE: Clearing the **Enable QoS & SIOC Integration** check box automatically disables the **Override Default QoS** check box.

4. Click **OK**.

Volume Management

Storage is provisioned in the SolidFire system as volumes. Volumes are block devices accessed over the network using iSCSI or Fibre Channel clients.

The NetApp SolidFire vCenter Plug-in enables you to create, view, edit, delete, clone, backup or restore volumes for user accounts. You can also manage each volume on a cluster, and add or remove volumes in volume access groups.

Creating a Volume

You can create a new volume and associate the volume with a given account (every volume must be associated with an account). This association gives the account access to the volume through the iSCSI initiators using the CHAP credentials. You can also specify QoS settings for a volume during creation.

Prerequisites

- At least one cluster must be discovered and running.
- If two or more clusters are discovered, the cluster you intend to use for the task must be selected.
- A user account has been created.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Volumes** sub-tab.
3. From the **Active Volumes** page, click **Create Volume**.
4. Enter a name for the volume.
5. Enter the total size of the volume you want to create.

NOTE: Default volume size selection is in GB. Volumes can be created with GB or GiB:

- 1GB = 1 000 000 000 bytes
- 1GiB = 1 073 741 824 bytes

NOTE: By default, 512 byte emulation is set to ON for all the new volumes.

6. Select a user account from the **Account** drop-down list.

NOTE: You need to create a user account before you can create a new volume.

7. In the **Quality of Service Settings** pane, do one of the following:
 - Select the default QoS.OR
 - Set customized minimum, maximum, and burst values for the IO.

NOTE: Click Reset Default QoS to restore default QoS values.

Caution: Datastore QoS SIOC settings, once enabled, will override any QoS settings at the volume level.

Caution: Volumes that have a Max or Burst IOPS value greater than 20,000 IOPS may require high queue depth or multiple sessions to achieve this level of IOPS on a single volume.


8. Click **OK**.

Viewing Volumes Details

You can review general information for all active volumes on the cluster in the NetApp SolidFire Management extension point in Global View. You can also see details for each active volume, including efficiency, performance, QoS, as well as associated snapshots. Volume QoS and statistics can also be viewed from each host in Contextual View.

Procedure

1. In the vSphere Web Client, do the following:

| If | Then |
|----------------------------|---|
| Using the Global View: | <ol style="list-style-type: none">1. Go to NetApp SolidFire Management > Management.2. From the Volumes tab, click the Actions button () for the volume you wish to review.3. In the resulting menu, select View Details. |
| Using the Contextual View: | <ol style="list-style-type: none">1. Click Hosts and Clusters.2. In the <i>Hosts and Clusters</i> Contextual View, select the datacenter, cluster, or host.3. Click the Manage tab, and then click the NetApp tab.4. Click the Volume QoS and Volume Stats sub-tabs to view volume performance details. |

Volume Details

On the **Management > Volumes** page of the NetApp SolidFire Management extension point, you can view the following information in the list of active volumes.

NOTE: VMware requires 512e for disk resources. If 512e is not enabled, a VMFS cannot be created and volume details are grayed out.

| Heading | Description |
|---------------|--|
| Volume ID | The system-generated ID for the volume. |
| Volume Name | The name given to the volume when it was created. |
| Account | The name of the account assigned to the volume. |
| Access Groups | The name of the volume access group or groups to which the volume belongs. |

| Heading | Description |
|-----------|---|
| Access | <p>The type of access assigned to the volume when it was created.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Read/Write: All reads and writes are accepted. • Read Only: All read activity allowed; no writes allowed. • Locked: Only Administrator access allowed. • ReplicationTarget: Designated as a target volume in a replicated volume pair. |
| Size | The total size (in GB) of the volume. |
| Snapshots | The number of snapshots created for the volume. |
| 512e | Identifies if 512e is enabled on a volume. Can be either Yes or No . |

Individual Volume Details

On the **Management > Volumes** page of the NetApp SolidFire Management extension point, you can view the following active volume information when you select an individual volume and view its details.

| Section | Heading | Description |
|----------------|--------------------|---|
| Volume Details | Volume name | The name assigned to the volume. |
| | Volume ID | The system-generated ID for the volume. |
| | Account ID | The unique account ID of the associated account. |
| | Account | The name of the account assigned to the volume. |
| | Access Groups | The name of the volume access group or groups to which the volume belongs. |
| | Size | The total size (in GB) of the volume. |
| | SCSI EUI Device ID | Globally unique SCSI device identifier for the volume in EUI-64 based 16-byte format. |
| | SCSI NAA Device ID | The globally unique SCSI device identifier for the protocol endpoint in NAA IEEE Registered Extended Format. |
| Efficiency | Compression | The compression efficiency score for the volume. |
| | Deduplication | The de-duplication efficiency score for the volume. |
| | Thin Provisioning | The thin provisioning efficiency score for the volume. |
| | Last Updated | The date and time of the last efficiency score. |
| Performance | Volume Utilization | <p>A floating value that describes how much the client is using the volume.</p> <p>Values:</p> <p>0: Client is not using the volume.</p> <p>1: Client is using their max.</p> <p>>1: Client is using their burst.</p> |

| Section | Heading | Description |
|--------------------|--------------------|---|
| | Actual IOPS | Current actual IOPS to the volume in the last 500 milliseconds. |
| | Average IOP Size | Average size in bytes of recent I/O to the volume in the last 500 milliseconds. |
| | Burst IOPS Credit | The total number of IOP credits available to the user. When volumes are not using up to the Max IOPS, credits are accrued. |
| | Read Operations | The total read operations to the volume since the creation of the volume. |
| | Read Bytes | The total cumulative bytes read from the volume since the creation of the volume. |
| | Read Latency USec | The average time, in microseconds, to complete read operations to the volume in the last 500 milliseconds. |
| | Write Operations | The total cumulative write operations to the volume since the creation of the volume. |
| | Write Bytes | The total cumulative bytes written to the volume since the creation of the volume. |
| | Write Latency USec | The average time, in microseconds, to complete write operations to a volume in the last 500 milliseconds. |
| | Async Delay | The length of time since the volume was last synced with the remote cluster. |
| | Client Queue Depth | The number of outstanding read and write operations to the volume. |
| | Latency USec | The average time, in microseconds, to complete operations to the volume in the last 500 milliseconds. A "0" (zero) value means there is no I/O to the volume. |
| | Throttle | A floating value between 0 and 1 that represents how much the system is throttling clients below their maxIOPS because of re-replication of data, transient errors and snapshots taken. |
| | Zero Blocks | Total number of 4KiB blocks without data after the last round of garbage collection operation has completed. |
| | Non-Zero Blocks | Total number of 4KiB blocks with data after the last garbage collection operation has completed. |
| | Unaligned Reads | For 512e volumes, the number of read operations that were not on a 4k sector boundary. High numbers of unaligned reads may indicate improper partition alignment. |
| | Unaligned Writes | For 512e volumes, the number of write operations that were not on a 4k sector boundary. High numbers of unaligned writes may indicate improper partition alignment. |
| | Last Updated | The date and time of the last performance update. |
| Quality of Service | Min IOPS | The minimum IOPS QoS setting of the volume. |
| | Max IOPS | The maximum IOPS QoS setting of the volume. |
| | Burst IOPS | The maximum burst QoS setting of the volume. |

| Section | Heading | Description |
|-----------|-----------------|--|
| Snapshots | Max Bandwidth | The number of IOPS (based on the QoS curve) multiplied by the IO size. |
| | ID | System generated ID for the snapshot. |
| | Name | User-defined name for the snapshot. |
| | Create Date | The date and time at which the snapshot was created. |
| | Expiration Date | The day and time the snapshot will be deleted. |
| | Size (GB) | User-defined size of the snapshot. |

Volume QoS and Stats

On the **Management > NetApp** tab from a specific host within Contextual View, you can view the following volume information for the host from the **Volume QoS** and **Volume Stats** pages.

NOTE: For Contextual View in vSphere 6.5, click the **Configure** tab to find **NetApp** within the list of options.


| Page | Heading | Description |
|--------------|-------------------------|--|
| Volume QoS | Volume ID | The system-generated ID for the volume. |
| | Volume name | The name assigned to the volume. |
| | Min IOPS | The current minimum IOPS QoS setting of the volume. |
| | Max IOPS | The current maximum IOPS QoS setting of the volume. |
| | Burst IOPS | The current maximum burst QoS setting of the volume. |
| Volume Stats | Volume ID | The system-generated ID for the volume. |
| | Volume name | The name assigned to the volume. |
| | Thin Provisioning | The thin provisioning efficiency score for the volume. |
| | Used Capacity | Used capacity of the volume, in bytes. |
| | Performance Utilization | The percentage of volume capacity being utilized. |

Editing a Volume

You can change volume attributes such as QoS values, volume size, and the unit of measurement in which byte values are calculated. You can also change access levels and which account can access the volume.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Volumes** sub-tab.

3. From the **Active Volumes** page, click the **Actions** button () for the volume you wish to edit.
4. In the resulting menu, click **Edit**.
5. In the **Total Size** field, enter a new volume size in GB or GiB.

NOTE: You can increase, but not decrease, the size of the volume.

6. Modify the account access level to a volume to one of the following:
 - Read/Write
 - Read Only
 - Locked
7. In the **Quality of Service Settings** pane, do one of the following:
 - Select the default QoS.
OR
 - Set customized minimum, maximum, and burst values for the IO.

NOTE: Click Reset Default QoS to restore default QoS values.

Best Practice: When you change IOPS values, NetApp recommends increments in tens or hundreds. Input values require valid whole numbers.

Configure volumes with an extremely high burst value. This allows the system to process occasional large block sequential workloads more quickly, while still constraining the sustained IOPS for a volume.

NOTE: Datastore QoS SIOC settings, once enabled, will override any QoS settings at the volume level.

8. Click **OK**.

Cloning a Volume

You can create a clone of a single volume or multiple volumes to make a point-in-time copy of the data. When you clone a volume, the system creates a snapshot of the volume and then creates a copy of the data referenced by the snapshot. This is an asynchronous process and can take a variable amount of time depending on the size of the volume you are cloning and the current cluster load.

The cluster supports up to two running clone requests per volume at a time and up to 8 active volume clone operations at a time. Requests beyond these limits are queued for later processing.

Caution: Before you truncate a cloned volume by cloning to a smaller size, ensure you prepare the partitions so that they fit into the smaller volume.


NOTE: Cloned volumes do not inherit volume access group membership from the source volume.

Prerequisites

- At least one cluster must be discovered and running.
- If two or more clusters are discovered, the cluster you intend to use for the task must be selected.
- At least one volume must be created.

- Available unprovisioned space must be equal to or more than the volume size.


Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Volumes** sub-tab.
3. To clone a single volume:
 - a. From the **Active Volumes** page, click the **Actions** button () for the volume you wish to clone
 - b. In the resulting menu, click **Clone**.
 - c. In the **Clone Volume** window, enter a **Volume Name** for the newly cloned volume.
 - d. Select a size and measurement for the volume using the **Volume Size** spin box and list.

NOTE: Default volume size selection is in GB. Volumes can be created with GB or GiB:

- 1GB = 1 000 000 000 bytes
- 1GiB = 1 073 741 824 bytes

- e. Select the type of **Access** for the newly cloned volume.
- f. Select an account to associate with the newly cloned volume from the **Account** list.
- g. Click **OK**.

NOTE: The time to complete a cloning operation is affected by volume size and current cluster load. Click refresh () if the cloned volume does not appear in the volume list.

Volume Backup and Restore Operations

You can configure the system to back up and restore the contents of a volume to and from an object store container that is external to SolidFire storage. You can also back up and restore data to and from remote SolidFire storage systems.

NOTE: You can run a maximum of two backup or restore processes at a time on a volume.


Volume Backup Operations

You can back up SolidFire volumes to SolidFire storage, as well as secondary object stores that are compatible with Amazon S3 or OpenStack® Swift.

Backing Up a Volume to an Amazon S3 Object Store

You can back up SolidFire volumes to external object stores that are compatible with Amazon S3.

Procedure


1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Volumes** sub-tab.
3. From the **Active Volumes** page, click the **Actions** button () for the volume you wish to back up.
4. In the resulting menu, click **Backup to**.
5. In the dialog under **Back up volume to**, select **Amazon S3**.

6. Select an option under **with the following data format**:
 - **Native**: A compressed format readable only by SolidFire storage systems.
 - **Uncompressed**: An uncompressed format compatible with other systems.
7. Enter a hostname to use to access the object store in the **Host name** field.
8. Enter an access key ID for the account in the **Access key ID** field.
9. Enter the secret access key for the account in the **Secret Access Key** field.
10. Enter the S3 bucket in which to store the backup in the **Amazon S3 bucket** field.
11. (Optional) Enter a nametag to append to the prefix in the **Nametag** field.
12. Click **OK**.

Backing Up a Volume to an OpenStack® Swift Object Store

You can back up SolidFire volumes to external object stores that are compatible with OpenStack Swift.


Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Volumes** sub-tab.
3. From the **Active Volumes** page, click the **Actions** button () for the volume you wish to back up.
4. In the resulting menu, click **Backup to**.
5. In the dialog under **Back up volume to**, select **OpenStack Swift**.
6. Select an option under **with the following data format**:
 - **Native**: A compressed format readable only by SolidFire storage systems.
 - **Uncompressed**: An uncompressed format compatible with other systems.
7. Enter a URL to use to access the object store in the **URL** field.
8. Enter a user name for the account in the **User name** field.
9. Enter the authentication key for the account in the **Authentication key** field.
10. Enter the container in which to store the backup in the **Container** field.
11. (Optional) Enter a nametag to append to the prefix in the **Nametag** field.
12. Click **OK**.

Backing Up a Volume to a SolidFire Cluster

You can back up volumes residing on a SolidFire cluster to a remote SolidFire cluster. When backing up or restoring from one cluster to another, the system generates a key to be used as authentication between the clusters. This bulk volume write key allows the source cluster to authenticate with the destination cluster, providing a level of security when writing to the destination volume. As part of the backup or restore process, you need to generate a bulk volume write key from the destination volume before starting the operation.

Procedure

1. On the destination cluster, go to **NetApp SolidFire Management > Management**.
2. Click the **Volumes** sub-tab.
3. From the **Active Volumes** page, click the **Actions** button () for the destination volume.
4. In the resulting menu, click **Restore from**.
5. In the dialog under **Restore volume from**, select **NetApp SolidFire**.

6. Select an option under **with the following data format**:
 - **Native**: A compressed format readable only by SolidFire storage systems.
 - **Uncompressed**: An uncompressed format compatible with other systems.
7. Click **Generate Key**.
8. Copy the key from the **Bulk Volume Write Key** box to your clipboard.
9. On the source cluster, go to **NetApp SolidFire Management > Management**.
10. Click the **Volumes** sub-tab.
11. From the **Active Volumes** page, click the **Actions** button (⚙️) for the volume to back up.
12. In the resulting menu, click **Backup to**.
13. In the dialog under **Back up volume to**, select **NetApp SolidFire**.
14. Select the same option as the destination cluster under **with the following data format**:
15. Enter the management virtual IP address of the destination volume's cluster in the **Remote cluster MVIP** field.
16. Enter the remote cluster user name in the **Remote cluster user name** field.
17. Enter the remote cluster password in the **Remote cluster password** field.
18. In the **Bulk volume write key** field, paste the key you generated on the destination cluster earlier.
19. Click **OK**.

Volume Restore Operations

When you restore a volume from a backup on an object store such as OpenStack® Swift or Amazon S3, you need manifest information from the original backup process. If you are restoring a SolidFire volume that was backed up on a SolidFire storage system, the manifest information is not required. You can find the required manifest information for restoring from Swift and S3 in **Reporting > Event Log**.

Restoring a Volume from Backup on an Amazon S3 Object Store

Follow these instructions to restore a volume from a backup on an Amazon S3 object store.

Procedure

1. Go to **NetApp SolidFire Management > Reporting**.
2. Click the **Event Log** sub-tab.
3. Locate the backup event that created the backup you need to restore.
4. Click the **Actions** button (⚙️) for the event.
5. In the resulting menu, click **View Details**.
6. Copy the manifest information to your clipboard.
7. Click **Management > Volumes**.
8. Click the **Actions** button (⚙️) for the volume you wish to restore.
9. In the resulting menu, click **Restore from**.
10. In the dialog under **Restore volume from**, select **Amazon S3**.
11. Select an option under **with the following data format**:
 - **Native**: A compressed format readable only by SolidFire storage systems.
 - **Uncompressed**: An uncompressed format compatible with other systems.
12. Enter a hostname to use to access the object store in the **Hostname** field.

13. Enter an access key ID for the account in the **Access Key ID** field.
14. Enter the secret access key for the account in the **Secret Access Key** field.
15. Enter the S3 bucket in which to store the backup in the **S3 Bucket** field.
16. Paste the manifest information into the **Manifest Information** field.
17. Click **OK**.

Restoring a Volume from Backup on an OpenStack® Swift Object Store

Follow these instructions to restore a volume from a backup on an OpenStack Swift object store.

Procedure

1. Go to **NetApp SolidFire Management > Reporting**.
2. Click the **Event Log** sub-tab.
3. Locate the backup event that created the backup you need to restore.
4. Click the **Actions** button (⚙️) for the event.
5. In the resulting menu, click **View Details**.
6. Copy the manifest information to your clipboard.
7. Click **Management > Volumes**.
8. Click the **Actions** button (⚙️) for the volume you wish to restore.
9. In the resulting menu, click **Restore from**.
10. In the dialog under **Restore volume from**, select **OpenStack Swift**.
11. Select an option under **with the following data format**:
 - **Native**: A compressed format readable only by SolidFire storage systems.
 - **Uncompressed**: An uncompressed format compatible with other systems.
12. Enter a URL to use to access the object store in the **URL** field.
13. Enter a user name for the account in the **Username** field.
14. Enter the authentication key for the account in the **Authentication Key** field.
15. Enter the name of the container in which the backup is stored in the **Container** field.
16. Paste the manifest information into the **Manifest Information** field.
17. Click **OK**.

Restoring a Volume from Backup on a SolidFire Cluster

Follow these instructions to restore a volume from a backup on a SolidFire cluster. When backing up or restoring from one cluster to another, the system generates a key to be used as authentication between the clusters. This bulk volume write key allows the source cluster to authenticate with the destination cluster, providing a level of security when writing to the destination volume. As part of the backup or restore process, you need to generate a bulk volume write key from the destination volume before starting the operation.

Procedure

1. On the destination cluster, go to **NetApp SolidFire Management > Management**.
2. Click the **Volumes** sub-tab.
3. From the **Active Volumes** page, click the **Actions** button (⚙️) for the volume you wish to restore.

4. In the resulting menu, click **Restore from**.
5. In the dialog under **Restore volume from**, select **NetApp SolidFire**.
6. Select an option under **with the following data format**:
 - **Native**: A compressed format readable only by SolidFire storage systems.
 - **Uncompressed**: An uncompressed format compatible with other systems.
7. Click **Generate Key**.
8. Copy the **Bulk Volume Write Key** information to the clipboard.
9. On the source cluster, go to **NetApp SolidFire Management > Management**.
10. Click the **Volumes** sub-tab.
11. From the **Active Volumes** page, click the **Actions** button (⚙️) for the volume you wish to use for the restore.
12. In the resulting menu, click **Backup to**.
13. In the dialog under **Back up volume to**, select **NetApp SolidFire**.
14. Select the option that matches the backup under **Data Format**.
15. Enter the management virtual IP address of the destination volume's cluster in the **Remote Cluster MVIP** field.
16. Enter the remote cluster user name in the **Remote Cluster Username** field.
17. Enter the remote cluster password in the **Remote Cluster Password** field.
18. Paste the key from your clipboard into the **Bulk Volume Write Key** field.
19. Click **Start Read**.
20. Click **OK**.

Deleting a Volume

You can delete one or more volumes from a SolidFire cluster.

The system does not immediately purge a deleted volume. A deleted volume can be restored for approximately eight hours. You can restore a volume before the system purges it or manually purge the volume from the **Deleted** area in **Management > Volumes**. When you restore a volume, it comes back online and iSCSI connections are restored.

Caution: When you delete a volume, any snapshots of that volume are also deleted.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Volumes** sub-tab.
3. To delete a single volume:
 - a. Click the **Actions** button (⚙️) for the volume you wish to delete.
 - b. In the resulting menu, click **Delete**.

NOTE: The Plug-in does not allow a volume with a datastore to be deleted.

- c. Confirm the action.
The system moves the volume to the **Deleted** area in the **Volumes** page.

Purging Volumes

You can manually purge volumes after you have deleted them. The system automatically purges deleted volumes eight hours after deletion. However, if you want to purge a volume before the scheduled purge time, you can perform a manual purge using the following steps.

Caution: When a volume is purged it is permanently removed from the system. All data in the volume is lost.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Volumes** sub-tab.
3. Click the **Deleted** sub-tab.
4. Select the volume or volumes you wish to purge using the mouse pointer + ctrl/command key.
5. Click **Purge**.

Restoring a Deleted Volume

You can restore a volume in the SolidFire system if it has been deleted but not yet purged. The system automatically purges a volume approximately 8 hours after it has been deleted. If the system has purged the volume, you cannot restore it.

NOTE: If a volume is deleted and then restored, ESXi will not detect the restored volume (and datastore if it exists). Remove the static target from the ESXi iSCSI adapter and rescan the adapter.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Volumes** sub-tab.
3. Click the **Deleted** sub-tab to view the list of deleted volumes.
4. To restore a single volume:
 - a. If there are multiple deleted volumes in the list, select the volume you wish to restore using the mouse pointer + ctrl/command key.
 - b. Click **Restore**.
5. To restore multiple volumes:
 - a. Select the volumes you wish to restore using the mouse pointer + ctrl/command key.
 - b. Click **Restore**.
6. Click the **Active** sub-tab and verify that the volume or volumes and all connections are restored.

Adding Volumes to an Access Group

You can add volumes to a volume access group. Each volume can belong to more than one volume access group; you can see the groups that each volume belongs to in the **Active** volumes page.

Prerequisites

- At least one cluster must be discovered and running.
- If two or more clusters are discovered, the cluster you intend to use for the task must be selected.
- At least one access group exists.
- At least one active volume exists.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Volumes** sub-tab.
3. Select one or more volumes you wish to add to the volume access group using the mouse pointer + ctrl/command key.
4. Click **Bulk Actions**.
5. In the resulting menu, select **Add to Access Group**.
6. Confirm the details in the dialog that opens, and select a volume access group from the drop-down list.
7. Click **OK**.

Removing Volumes from an Access Group

You can remove volumes from an access group. When you remove a volume from an access group, the group no longer has access to that volume.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Volumes** sub-tab.
3. Select one or more volumes you wish to remove from the volume access group using the mouse pointer + ctrl/command key.
4. Click **Bulk Actions**.
5. In the resulting menu, select **Remove from Access Group**.
6. Confirm the details in the dialog that opens, and select the volume access group that you wish to no longer have access to the volume.

Caution: Removing a volume from an access group can disrupt host access to the volume.

7. Click **OK**.

User Account Management

User accounts are used to control access to the storage resources on a SolidFire storage network. At least one user account is required before a volume can be created. When you create a volume, it is assigned to an account. If you have created a virtual volume, the account is the storage container. The account contains the CHAP authentication required to access the volumes assigned to it. An account can have up to two thousand volumes assigned to it, but a volume can belong to only one account.

User accounts can be managed from NetApp SolidFire Management extension point in Global View.

Account Details

On the **NetApp SolidFire Management > Accounts** page of the NetApp SolidFire Management extension point, you can view the following information in the list of accounts.

| Heading | Description |
|------------------|--|
| Account ID | System-generated ID for the account. |
| User name | The name given to the account when it was created. |
| Initiator Secret | The unique CHAP secret for the initiator. |
| Target Secret | The unique CHAP secret for the target. |

| Heading | Description |
|-------------------|---|
| Number of Volumes | The number of active volumes assigned to the account. |
| Status | The status of the account. |

Creating an Account

You can create an account to allow access to volumes. After you create an account, you can assign up to 2000 volumes to the account. Each account name in the system must be unique.

Prerequisites

- At least one cluster must be discovered and running.
- If two or more clusters are discovered, the cluster you intend to use for the task must be selected.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Accounts** sub-tab.
3. Click **Create Account**.
4. Enter a **Username**.
5. In the **CHAP Settings** section:
 - a. Enter the **Initiator Secret** for CHAP node session authentication.
 - b. Enter the **Target Secret** for CHAP node session authentication.

NOTE: Initiator and target secrets must differ. If these fields are left blank, the system generates the authentication credentials.

6. Click **OK**.

Editing an Account

You can edit an account to change the status or the CHAP secrets.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Accounts** sub-tab.
3. Click the **Actions** button (⚙️) for the account you wish to edit.
4. In the resulting menu, select **Edit**.
5. (Optional) Click the **Status** drop-down list and select a different status.

Caution: Changing the **Access** to **Locked** terminates all iSCSI connections to the account, and the account is no longer accessible. Volumes associated with the account are maintained; however, the volumes are not iSCSI-discoverable.

6. (Optional) Edit the **Initiator Secret** and **Target Secret** credentials used for node session authentication.

NOTE: If you do not change the **CHAP Settings** credentials, they remain the same. If you make the credentials fields blank, the system generates new passwords.

7. Click **OK**.

Deleting an Account

You can delete accounts when they are no longer needed.

Prerequisites

Delete and purge any volumes associated with the account before you delete the account.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Accounts** sub-tab.
3. Click the **Actions** button (⚙️) for the account you wish to delete.
4. In the resulting menu, select **Delete**.
5. Confirm the action.

Volume Access Groups

A volume access group is a collection of volumes that users can access using either iSCSI initiators or Fibre Channel initiators.

You can create access groups by mapping iSCSI initiator IQNs or Fibre Channel WWPNs in a collection of volumes. Each IQN that you add to an access group can access each volume in the group without requiring CHAP authentication. Each WWPN that you add to an access group enables Fibre Channel network access to the volumes in the access group.

NOTE: Volume access groups have the following system limits:

- A maximum of 64 IQNs or WWPNs are allowed in an access group.
- An access group can be made up of a maximum of 2000 volumes.
- An IQN or WWPN can belong to only one access group.
- A single volume can belong to a maximum of four access groups.

Volume access groups can be managed from the NetApp SolidFire Management extension point in Global View.

Volume Access Group Details

On the **NetApp SolidFire Management > Access Groups** page of the NetApp SolidFire Management extension point, you can view the following information in the list of volume access groups.

| Heading | Description |
|------------------------|---|
| Volume Access Group ID | System-generated ID for the access group. |
| Name | The name given to the access group when it was created. |
| Active Volumes | The number of active volumes in the access group. |
| Initiators | The number of initiators connected to the access group. |

Creating Access Groups

You can create volume access groups with one or multiple initiators. Mapping Fibre Channel or iSCSI client initiators (WWPN) to the volumes in a volume access group enables secure data I/O between a network and a SolidFire volume.

NOTE: You can also create single initiator volume access groups from the Create Datastore wizard.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Access Groups** sub-tab.
3. Click **Create Access Group**.
4. Enter a name for the volume access group.
5. Do one of the following:
 - For clusters running Element OS versions earlier than 9.0, enter an IQN or WWPN in the **Initiators** field.
 - For clusters running Element OS version 9.0, select an unassigned IQN or WWPN from the **Select an Initiator** drop-down list and click **Add Initiator**.

NOTE: Initiators may be added or deleted at a later time. Volume access groups are not visible from Contextual View until an initiator is assigned.

The accepted format of an initiator IQN: `iqn.yyyy-mm` where `y` and `m` are digits, followed by text which must only contain digits, lower-case alphabetic characters, a period (`.`), colon (`:`) or dash (`-`).

Example format:

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

The accepted format of a Fibre Channel initiator WWPN is: `Aa:bB:CC:dd:11:22:33:44`, or `AabBCCdd11223344`.

Example format:

```
5f:47:ac:c0:5c:74:d4:02
```

6. Click **OK**.

Editing Access Groups

You can edit volume access group names or add or remove initiators from Global View or Contextual View.

Procedure

1. In the vSphere Web Client, do the following:

| If | Then |
|----------------------------|---|
| Using the Global View: | <ol style="list-style-type: none">1. Go to NetApp SolidFire Management > Management.2. Proceed to the next step. |
| Using the Contextual View: | <ol style="list-style-type: none">1. Click Hosts and Clusters.2. In the <i>Hosts and Clusters</i> Contextual View, select the datacenter, cluster, or host.3. Click the Manage tab, and then click the NetApp tab. |

| If | Then |
|----|---|
| | <p>NOTE: For vSphere 6.5, click the Configure tab to find NetApp within the list of options.</p> <p>4. Proceed to the next step.</p> |

2. Click the **Access Groups** sub-tab.
3. Click the **Actions** button (⚙️) for the access group you wish to edit.
4. In the resulting menu, select **Edit**.
5. (Optional) Modify the access group name.
6. (Optional) Add or remove initiators.

NOTE: If you are removing an initiator, click the delete button (❌) to remove it. When you remove the initiator, it can no longer access the volumes in that volume access group. Normal account access to the volume is not disrupted.
An initiator, once deleted from an access group, is not shown in the list of available initiators. To recreate the initiator, see [Creating an Initiator](#).

7. Click **OK**.

Deleting Access Groups

You can delete volume access groups from Global View or Contextual View. You do not need to delete Initiator IDs or disassociate volumes from the volume access group prior to deleting the group. After you delete the access group, group access to the volumes is discontinued.

Procedure

1. In the vSphere Web Client, do the following:

| If | Then |
|----------------------------|--|
| Using the Global View: | <ol style="list-style-type: none"> 1. Go to NetApp SolidFire Management > Management. 2. Proceed to the next step. |
| Using the Contextual View: | <ol style="list-style-type: none"> 1. Click Hosts and Clusters. 2. In the <i>Hosts and Clusters</i> Contextual View, select the datacenter, cluster, or host. 3. Click the Manage tab, and then click the NetApp tab. <p>NOTE: For vSphere 6.5, click the Configure tab to find NetApp within the list of options.</p> <ol style="list-style-type: none"> 4. Proceed to the next step. |

2. Click the **Access Groups** sub-tab.
3. Click the **Actions** button (⚙️) for the access group you wish to delete.
4. In the resulting menu, select **Delete**.

5. Confirm the action.

CAUTION: If the access group you are deleting has active volumes associated with it, you are prompted to confirm the deletion. ESXi hosts may lose connectivity to the volumes if you proceed.

Initiators

Initiators enable external clients access to volumes in a cluster, serving as the entry point for communication between clients and volumes. You can create and delete initiators, and give them friendly aliases to simplify administration and volume access. When you add an initiator to a volume access group, that initiator enables access to all volumes in the group.

You can view initiators on the **Management > Initiators** page from the NetApp SolidFire Management extension point in Global View.

Creating an Initiator

You can create iSCSI or Fibre Channel initiators and optionally assign them aliases.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Initiators** sub-tab.
3. Click **Create Initiator**.
4. To create a single initiator:
 - a. Select **Create a Single Initiator**.
 - b. Enter the IQN or WWPN for the initiator in the **IQN/WWPN** field.
 - The accepted format of an initiator IQN: `iqn.yyyy-mm` where `y` and `m` are digits, followed by text which must only contain digits, lower-case alphabetic characters, a period (.), colon (:), or dash (-).

Example format:


```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

- The accepted format of a Fibre Channel initiator WWPN is: `Aa:bB:CC:dd:11:22:33:44`, or `AabBCCdd11223344`.

Example format:

```
5f:47:ac:c0:5c:74:d4:02
```

- c. Enter a friendly name for the initiator in the **Alias** field.
 - d. Click **OK**.
5. To create multiple initiators:
 - a. Select **Create Multiple Initiators**.
 - b. Do one or both of the following:
 - Click **Scan Hosts** to scan vSphere hosts for initiator values not defined in the SolidFire cluster.
 - Enter a list of IQNs or WWPNs in the text box.
 - c. Click **Add Initiators**.
 - d. Under the **Alias (optional)** heading, click the field for each entry to add an alias.

- e. (Optional) To remove an initiator from the list, click  next to the initiator you wish to remove.
- f. Click **OK**.

Initiator Details


On the **Management > Initiators** page of the NetApp SolidFire Management extension point, you can view the following information in the list of initiators.

| Heading | Description |
|--------------|---|
| ID | The system-generated ID for the initiator. |
| Name | The name given to the initiator when it was created. |
| Alias | The friendly name given to the initiator, if any. |
| Access Group | The volume access group to which the initiator is assigned. |

Editing an Initiator

You can change the alias of an existing initiator or add an alias if one does not already exist.


Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Initiators** sub-tab.
3. Click the **Actions** button () for the access group you wish to edit.
4. In the resulting menu, select **Edit**.
5. Enter a new alias for the initiator in the **Alias** field.
6. Click **OK**.

Deleting Initiators

You can delete an initiator once it is no longer needed. When you delete an initiator, the system removes it from any associated volume access group. Any connections using the initiator remain valid until the connection is reset.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Initiators** sub-tab.
3. Do one of the following:
 - Click the **Actions** button () for the initiator you wish to delete.
 - Select one or more initiators you wish to delete using the mouse pointer + ctrl/command key and click **Bulk Actions**.
4. In the resulting menu, select **Delete**.
5. Confirm the action.

Adding Initiators to a Volume Access Group

You can add initiators to an access group to allow access to volumes in the volume access group without requiring CHAP authentication. When you add an initiator to a volume access group, the initiator has access to all volumes in that volume access group.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Initiators** sub-tab.
3. Select one or more initiators to add to an access group using the mouse pointer + ctrl/command key.
4. Click the **Bulk Actions** button.
5. Choose **Add to Volume Access Group** from the resulting list.
6. In the **Add to Volume Access Group** dialog, choose an access group from the **Volume Access Group** list.
7. Click **OK**.

Data Protection

From the **Data Protection** tab you can perform tasks that ensure that copies of your data are created and stored where you need them.

See the following topics to learn about or perform data protection tasks:

Volume Snapshots

[Creating a Volume Snapshot](#)

[Volume Snapshot Details](#)

[Editing Snapshots](#)

[Cloning a Volume from a Snapshot](#)

[Rolling Back a Volume to a Snapshot](#)

[Volume Snapshot Backup Operations](#)

[Backing Up a Volume Snapshot to an Amazon S3 Object Store](#)

[Backing Up a Volume Snapshot to an OpenStack® Swift Object Store](#)

[Backing Up a Volume Snapshot to a SolidFire Cluster](#)

[Deleting a Snapshot](#)

Group Snapshots

[Creating a Group Snapshot](#)

[Group Snapshot Details](#)

[Editing Group Snapshots](#)

[Cloning Volumes from a Group Snapshot](#)

[Rolling Back Volumes to a Group Snapshot](#)

[Deleting a Group Snapshot](#)

Snapshot Schedules

[Snapshot Schedule Details](#)

[Creating a Snapshot Schedule](#)

[Editing a Snapshot Schedule](#)

[Deleting a Snapshot Schedule](#)

[Copying a Snapshot Schedule](#)

Cluster and Volume Pairing for Real-Time Remote Replication

Volume Snapshots

A volume snapshot is a point-in-time copy of a volume. Creating a volume snapshot takes only a small amount of system resources and space; this makes snapshot creation faster than cloning. You can use snapshots to roll a volume back to the state it was in at the time the snapshot was created. However, because snapshots are simply replicas of volume metadata, you cannot mount or write to them.

You can replicate snapshots to a remote SolidFire cluster and use them as a backup copy for the volume. This enables you to roll back a volume to a specific point in time by using the replicated snapshot; you can also create a clone of a volume from a replicated snapshot.

You can create volume snapshots from the **NetApp SolidFire Management > Management > Volumes** page. You can manage these volume snapshots from the **NetApp SolidFire Management > Data Protection > Snapshots** page.

Creating a Volume Snapshot

You can create a snapshot of the active volume to preserve the volume image at any point in time. You can create the snapshot immediately or create a schedule to automate future snapshots of the volume. You can create up to 32 snapshots for a single volume.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Volumes** sub-tab.
3. From the **Active Volumes** page, click the **Actions** button (⚙️) for the volume you wish to use for the snapshot.
4. In the resulting menu, select **Create Snapshot**.
5. In the **Create Snapshot** dialog, enter the snapshot name.
6. (Optional) Select the **Include snapshot in replication when volume is paired** check box to ensure that the snapshot is captured in replication when the parent volume is paired.
7. To choose a **Retention** option for the snapshot, do one of the following:
 - Choose **Keep Forever** to retain the snapshot on the system indefinitely.
 - Choose **Set Retention Period** and use the date spin boxes to choose a length of time for the system to retain the snapshot.
8. To take a single, immediate snapshot:
 - a. Choose **Take Snapshot Now**.
 - b. Click **OK**.
9. To schedule the snapshot to run at a future time:
 - a. Choose **Create Snapshot Schedule**.
 - b. Enter a schedule name.
 - c. Choose a schedule type from the list.
 - d. (Optional) Select the **Recurring Schedule** check box to repeat the scheduled snapshot periodically.
 - e. Click **OK**.

Volume Snapshot Details

On the **Data Protection > Snapshots** page of the NetApp SolidFire Management extension point, you can view the following information in the list of volume snapshots. You can also filter snapshots by using the drop-down option to select individual snapshots that are not associated with a group snapshot, member snapshots that are members of group snapshots, and inactive snapshots.

| Heading | Description |
|---------------|---|
| ID | System generated ID for the snapshot. |
| Snapshot UUID | The unique ID of the snapshot. |
| Name | User-defined name for the snapshot. |
| Size (GB) | User-defined size of the snapshot in GB. |
| Volume ID | ID of the volume from which the snapshot was created. |
| Volume Name | User defined name of the volume. |
| Account | Account the volume is associated with. |

| Heading | Description |
|--------------------|--|
| Volume Size (GB) | Size of the volume from which the snapshot was created in GB. |
| Create Date | The date and time at which the snapshot was created. |
| Expiration Date | The day and time the snapshot will be deleted. |
| Group Snapshot ID | The group ID the snapshot belongs to if grouped together with other volume snapshots. |
| Remote Replication | Identifies whether or not the snapshot is enabled for replication to a remote SolidFire cluster. Possible Values: Enabled: The snapshot is enabled for remote replication. Disabled: The snapshot is not enabled for remote replication. |
| Remote Status | Displays the status of the snapshot on the remote SolidFire cluster. Possible Values: Present: The snapshot exists on a remote cluster. Not Present: The snapshot does not exist on a remote cluster. Syncing: The target cluster is currently replicating the snapshot. Deleted: The target replicated the snapshot and then deleted it. |

Editing Snapshots

You can change replication settings or the retention period for a snapshot. The retention period you specify begins when you enter the new interval. When you set a retention period, you can select a period that begins at the current time (retention is not calculated from the snapshot creation time). You can specify intervals in minutes, hours, and days.

Procedure

1. Go to **NetApp SolidFire Management > Data Protection**.
2. Click the **Actions** button (⚙️) for the snapshot you wish to edit.
3. In the resulting menu, click **Edit**.
4. (Optional) Select the **Include Snapshot in Replication When Paired** check box to ensure that the snapshot is captured in replication when the parent volume is paired.
5. (Optional) Choose a **Snapshot Retention** option for the snapshot:
 - Choose **Keep Forever** to retain the snapshot on the system indefinitely.
 - Choose **Set Retention Period** and use the date spin boxes to choose a length of time for the system to retain the snapshot.

NOTE: When you set a retention period, you select a period that begins at the current time (retention is not calculated from the snapshot creation time).


6. Click **OK**.

Cloning a Volume from a Snapshot

You can create a new volume from a snapshot of a volume. When you do this, the system uses the snapshot information to clone a new volume using the data contained on the volume at the time the snapshot was created. This process also stores information about other snapshots of the volume in the new created volume.

Procedure


1. Go to **NetApp SolidFire Management > Data Protection**.

2. Click the **Actions** button () for the account you wish to edit.
3. In the resulting menu, click **Clone Volume from Snapshot**.
4. In the **Clone Volume from Snapshot** dialog, enter a **Volume Name**.
5. Choose a **Total Size** and size units for the new volume.
6. Select an **Access** type for the volume:
 - **Read Only:** Only read operations are allowed.
 - **Read / Write:** Reads and writes are allowed.
 - **Locked:** No reads or writes are allowed.
 - **Replication Target:** Designated as a target volume in a replicated volume pair.
7. Choose an **Account** from the list to associate with the new volume.
8. Click **OK**.

Rolling Back a Volume to a Snapshot

You can roll back a volume to a snapshot at any time. This reverts any changes made to the volume since the snapshot was created.

Procedure

1. Go to **NetApp SolidFire Management > Data Protection**.
2. Click the **Actions** button () for the snapshot you wish to use for the volume rollback.
3. In the resulting menu, select **Rollback Volume to Snapshot**.
4. (Optional) To save the current state of the volume before rolling back to the snapshot:
 - a. In the **Rollback to Snapshot** dialog, select **Save volume's current state as a snapshot**.
 - b. Enter a name for the new snapshot.
5. Click **OK**.


Volume Snapshot Backup Operations

You can use the integrated backup feature to back up a volume snapshot. You can back up snapshots from a SolidFire cluster to an external object store, or to another SolidFire cluster. When you back up a snapshot to an external object store, you must have a connection to the object store that allows read/write operations.

Backing Up a Volume Snapshot to an Amazon S3 Object Store

You can back up SolidFire snapshots to external object stores that are compatible with Amazon S3.

Procedure


1. Go to **NetApp SolidFire Management > Data Protection**.
2. Click the **Actions** button () for the snapshot you wish to back up.
3. In the resulting menu, click **Backup to**.
4. In the dialog under **Back up volume to**, select **Amazon S3**.
5. Select an option under **with the following data format**:
 - **Native:** A compressed format readable only by SolidFire storage systems.
 - **Uncompressed:** An uncompressed format compatible with other systems.
6. Enter a hostname to use to access the object store in the **Hostname** field.

7. Enter an access key ID for the account in the **Access Key ID** field.
8. Enter the secret access key for the account in the **Secret Access Key** field.
9. Enter the S3 bucket in which to store the backup in the **Amazon S3 Bucket** field.
10. (Optional) Enter a nametag to append to the prefix in the **Nametag** field.
11. Click **OK**.

Backing Up a Volume Snapshot to an OpenStack® Swift Object Store

You can back up SolidFire snapshots to secondary object stores that are compatible with OpenStack Swift.

Procedure

1. Go to **NetApp SolidFire Management > Data Protection**.
2. Click the **Actions** button () for the snapshot you wish to back up.
3. In the resulting menu, click **Backup to**.
4. In the dialog under **Back up volume to**, select **OpenStack Swift**.
5. Select an option under **with the following data format**:
 - **Native**: A compressed format readable only by SolidFire storage systems.
 - **Uncompressed**: An uncompressed format compatible with other systems.
6. Enter a **URL** to use to access the object store.
7. Enter a **Username** for the account.
8. Enter the **Authentication Key** for the account.
9. Enter the **Container** in which to store the backup.
10. (Optional) Enter a **Nametag**.
11. Click **OK**.


Backing Up a Volume Snapshot to a SolidFire Cluster


You can back up a volume snapshot residing on a SolidFire cluster to a remote SolidFire cluster. When backing up or restoring from one cluster to another, the system generates a key to be used as authentication between the clusters. This bulk volume write key allows the source cluster to authenticate with the destination cluster, providing a level of security when writing to the destination volume. As part of the backup or restore process, you need to generate a bulk volume write key from the destination volume before starting the operation.

Prerequisites

- You must create a volume on the destination cluster of equal or greater size to the snapshot you are using for the backup.

Procedure

1. On the destination cluster, go to **NetApp SolidFire Management > Management**.
2. Click the **Actions** button () for the destination volume.
3. In the resulting menu, click **Restore from**.
4. In the dialog under **Restore volume from**, select **NetApp SolidFire**.
5. Select an option under **with the following data format**:
 - **Native**: A compressed format readable only by SolidFire storage systems.
 - **Uncompressed**: An uncompressed format compatible with other systems.
6. Click **Generate Key**.

7. Copy the key from the **Bulk Volume Write Key** box to your clipboard.
8. On the source cluster, go to **NetApp SolidFire Management > Data Protection**.
9. Click the **Actions** button () for the snapshot you are using for the backup.
10. In the resulting menu, click **Backup to**.
11. In the dialog under **Back up volume to**, select **NetApp SolidFire**.
12. Select the same option as the destination cluster under **with the following data format**:
13. Enter the management virtual IP address of the destination volume's cluster in the **Remote Cluster MVIP** field.
14. Enter the remote cluster username in the **Remote Cluster Username** field.
15. Enter the remote cluster password in the **Remote Cluster Password** field.
16. In the **Bulk Volume Write Key** field, paste the key you generated on the destination cluster earlier.
17. Click **OK**.


Deleting a Snapshot

You can delete a volume snapshot from a SolidFire cluster. When you delete a snapshot, the system immediately removes it.

You can delete snapshots that are being replicated from the source cluster. If a snapshot is syncing to the target cluster when you delete it, the sync replication completes and the snapshot is deleted from the source cluster. The snapshot is not deleted from the target cluster.

You can also delete snapshots that have been replicated to the target from the target cluster. The deleted snapshot is kept in a list of deleted snapshots on the target until the system detects that you have deleted the snapshot on the source cluster. Once the target has detected that you have deleted the source snapshot, the target stops replication of the snapshot.

Procedure

1. Go to **NetApp SolidFire Management > Data Protection**.
2. Click the **Actions** button () for the snapshot you wish to use for the volume rollback.
3. In the resulting menu, select **Delete**.
4. Confirm the action.

Group Snapshots

You can create a group snapshot of a related set of volumes to preserve a point-in-time copy of the metadata for each volume. You can use the group snapshot in the future as a backup or rollback to restore the state of the group of volumes to a desired point in time.

Creating a Group Snapshot

You can create a snapshot of a group of volumes immediately or create a schedule to automate future snapshots of the group of volumes. A single group snapshot can consistently snapshot up to 32 volumes at one time.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Volumes** sub-tab.
3. Select one or more volumes to add using the mouse pointer + ctrl/command key.
4. Click **Bulk Actions**.
5. In the resulting menu, select **Create Group Snapshot**.

6. In the **Create Group Snapshot** dialog, enter a name for the group snapshot.
7. (Optional) Select the **Include snapshot member in replication when volumes are paired** check box to ensure that each snapshot is replicated when the parent volume is paired.
8. To choose a **Retention** option for the group snapshot, do one of the following:
 - Choose **Keep Forever** to retain the snapshot on the system indefinitely.
 - Choose **Set Retention Period** and use the date spin boxes to choose a length of time for the system to retain the snapshot.
9. To take a single, immediate snapshot:
 - a. Choose **Take Group Snapshot Now**.
 - b. Click **OK**.
10. To schedule the snapshot to run at a future time:
 - a. Choose **Create Group Snapshot Schedule**.
 - b. Enter a schedule name.
 - c. Choose a schedule type from the list.
 - d. (Optional) Select the **Recurring Schedule** check box to repeat the scheduled snapshot periodically.
 - e. Click **OK**.

Group Snapshot Details

On the **Data Protection > Group Snapshots** page of the NetApp SolidFire Management extension point, you can view the following information in the list of group volume snapshots.

| Heading | Description |
|---------------------|---|
| Snapshot Group ID | System-generated ID for the group snapshot. |
| Unique ID | The unique ID of the group snapshot. |
| Snapshot Group Name | User-defined name for the group snapshot. |
| Create Time | The date and time at which the group snapshot was created. |
| Status | The current status of the snapshot. Possible values: Preparing: The snapshot is being prepared for use and is not yet writable. Done: This snapshot has finished preparation and is now usable. Active: The snapshot is the active branch. |
| Number of Volumes | The number of volumes in the group snapshot. |

Editing Group Snapshots

You can edit the replication and retention settings for existing group snapshots.

Procedure

1. Go to **NetApp SolidFire Management > Data Protection**.
2. Click the **Group Snapshots** sub-tab.
3. Click the **Actions** button (⚙️) for the group snapshot you wish to edit.
4. In the resulting menu, select **Edit**.

5. (Optional) Select the **Include snapshot in replication when paired** check box to ensure that the snapshot is replicated when the parent volume is paired.
6. (Optional) To change the retention setting for the group snapshot, do one of the following:
 - Choose **Keep Forever** to retain the snapshot on the system indefinitely.
 - Choose **Set Retention Period** and use the date spin boxes to choose a length of time for the system to retain the snapshot.
7. Click **OK**.

Cloning Volumes from a Group Snapshot

You can clone a group of volumes from a point-in-time group snapshot. Once you create the volumes, you can use them like any other volume in the system.

Procedure

1. Go to **NetApp SolidFire Management > Data Protection**.
2. Click the **Group Snapshots** sub-tab.
3. Click the **Actions** button (⚙️) for the group snapshot you wish to use for the volume clones.
4. In the resulting menu, select **Clone Volumes From Group Snapshot**.
5. In the **Clone Volumes From Group Snapshot** dialog, enter a new volume name prefix.

NOTE: The prefix distinguishes the new clone volumes from existing volumes. The prefix is applied to all volumes created from the group snapshot.

6. (Optional) Select a different account to which the clone will belong. If you do not select an account, the system assigns the new volumes to the current volume account.
7. (Optional) Select a different access method for the volumes in the clone. If you do not select an access method, the system uses the current volume access.
 - **Read/Write:** All reads and writes are accepted.
 - **Read Only:** All read activity allowed; no writes allowed.
 - **Locked:** Only Administrator access allowed.
 - **Replication Target:** Designated as a target volume in a replicated volume pair.
8. Click **OK**.

NOTE: Volume size and current cluster load affect the time needed to complete a cloning operation.

Rolling Back Volumes to a Group Snapshot

You can roll back a group of volumes at any time to a group snapshot. This restores all the volumes in the group to the state they were in at the time the group snapshot was created. This also restores volume sizes to the size recorded in the original snapshot. If the system has purged a volume, all snapshots of that volume were also deleted at the time of the purge; the system does not restore any deleted volume snapshots.

Procedure

1. Go to **NetApp SolidFire Management > Data Protection**.
2. Click the **Group Snapshots** sub-tab.
3. Click the **Actions** button (⚙️) for the group snapshot you wish to use for the volume rollback.

4. In the resulting menu, select **Rollback Volumes To Group Snapshot**.
5. (Optional) To save the current state of the volumes before rolling back to the snapshot:
 - a. In the **Rollback To Snapshot** dialog, select **Save volumes' current state as a group snapshot**.
 - b. Enter a name for the new snapshot.
6. Click **OK**.

Deleting a Group Snapshot

You can delete a group snapshot from the system. When you delete the group snapshot, you can choose whether all snapshots associated with the group are deleted or retained as individual snapshots.

NOTE: If you delete a volume or snapshot that is a member of a group snapshot, you can no longer roll back to the group snapshot. However, you can roll back each volume individually.

Procedure

1. Go to **NetApp SolidFire Management > Data Protection**.
2. Click the **Group Snapshots** sub-tab.
3. Click the **Actions** button (⚙️) for the group snapshot you wish to delete.
4. In the resulting menu, click **Delete**.
5. Do one of the following in the confirmation dialog:
 - Choose **Delete group snapshot and all group snapshot members** to delete the group snapshot and all member snapshots.
 - Choose **Retain group snapshot members as individual snapshots** to delete the group snapshot but keep all member snapshots.
6. Confirm the action.

Snapshot Schedules

You can schedule a snapshot of a volume to automatically occur at specified date and time intervals. You can schedule either single volume snapshots or group snapshots to run automatically.

NOTE: Schedules are created using UTC+0 time. You may need to adjust the actual time a snapshot will run based on your time zone.

When you create snapshot schedules, you can store the resulting snapshots on a remote SolidFire storage system if the volume is being replicated.

Snapshot Schedule Details

On the **Data Protection > Schedules** page of the NetApp SolidFire Management extension point, you can view the following information in the list of snapshot schedules.

| Heading | Description |
|---------|---|
| ID | System-generated ID for the schedule. |
| Type | Indicates the type of schedule. Snapshot is currently the only type supported. |

| Heading | Description |
|-----------------|--|
| Name | The name given to the schedule when it was created. Snapshot schedule names can be up to 223 characters in length and contain a-z, 0-9, and dash (-) characters. |
| Frequency | The frequency at which the schedule is run. The frequency can be set in hours and minutes, weeks, or months. |
| Recurring | Indicates if the schedule is to run only once or if it is to run at regular intervals. |
| Manually Paused | Identifies whether or not the schedule has been manually paused. |
| Volume IDs | Displays the ID of the volume the schedule will use when the schedule is run. |
| Last Run | Displays the last time the schedule was run. |
| Last Run Status | Displays the outcome of the last schedule execution. Can be either Success or Failure . |

Creating a Snapshot Schedule

You can schedule a snapshot of a volume or volumes to automatically occur at specified intervals. When you configure a snapshot schedule, you can choose from time intervals based on days of the week or days of the month. You can also specify the days, hours, and minutes before the next snapshot occurs.

If you schedule a snapshot to run at a time period that is not divisible by 5 minutes, the snapshot will run at the next time period that is divisible by 5 minutes. For example, if you schedule a snapshot to run at 12:42:00 UTC, it will run at 12:45:00 UTC. You cannot schedule a snapshot to run at intervals of less than 5 minutes.

Procedure


1. Go to **NetApp SolidFire Management > Data Protection**.
2. Click the **Schedules** sub-tab.
3. Click **Create Schedule**.
4. In the **Volume IDs CSV** field, enter a single volume ID or a comma-separated list of volume IDs to include in the snapshot operation.
5. Enter a **New Schedule Name**.
6. To schedule the snapshot to run on certain days of the week:
 - a. Choose **Days of Week** from the **Schedule Type** list.
 - b. Select the days of the week to perform the snapshot using the mouse pointer + ctrl/command key.
 - c. Choose a **Time of Day** for the schedule to run.
7. To schedule the snapshot to run on certain days of the month:
 - a. Choose **Days of Month** from the **Schedule Type** list.
 - b. Select the days of the month to perform the snapshot using the mouse pointer + ctrl/command key.
 - c. Choose a **Time of Day** for the schedule to run.
8. (Optional) Select **Recurring Schedule** to repeat the snapshot schedule indefinitely.
9. (Optional) Enter a name for the new snapshot in the **New Snapshot Name** field.
If you leave the field blank, the system uses the time and date of the snapshot's creation as the name.
10. (Optional) Select the **Include Snapshots in Replication When Paired** check box to ensure that the snapshots are captured in replication when the parent volume is paired.

11. To choose a **Snapshot Retention** option for the snapshot, do one of the following:
 - Select **Keep Forever** to retain the snapshot on the system indefinitely.
 - Select **Set Retention Period** and use the date spin boxes to choose a length of time for the system to retain the snapshot.
12. Click **OK**.

Editing a Snapshot Schedule

You can modify existing snapshot schedules. After modification, the next time the schedule runs it uses the updated attributes. Any snapshots created by the original schedule remain on the storage system.

Procedure

1. Go to **NetApp SolidFire Management > Data Protection**.
2. Click the **Schedules** sub-tab.
3. Click the **Actions** button () for the schedule you wish to edit.
4. In the resulting menu, click **Edit**.
5. In the **Volume IDs CSV** field, modify the single volume ID or comma-separated list of volume IDs currently included in the snapshot operation.
6. Enter a different name for the schedule in the **New Schedule Name** field if desired.
7. To change the schedule to run on different days of the week:
 - a. Choose **Days of Week** from the **Schedule Type** list.
 - b. Select the days of the week to perform the snapshot using the mouse pointer + ctrl/command key.
 - c. Choose a **Time of Day** for the schedule to run.
8. To change the schedule to run on different days of the month:
 - a. Choose **Days of Month** from the **Schedule Type** list.
 - b. Select the days of the month to perform the snapshot using the mouse pointer + ctrl/command key.
 - c. Choose a **Time of Day** for the schedule to run.
9. (Optional) Select **Recurring Schedule** to repeat the snapshot schedule indefinitely.
10. (Optional) Enter or modify the name for the new snapshot in the **New Snapshot Name** field.


If you leave the field blank, the system uses the time and date of the snapshot's creation as the name.
11. (Optional) Select the **Include Snapshots in Replication When Paired** check box to ensure that the snapshots are captured in replication when the parent volume is paired.
12. To choose a different **Snapshot Retention** option for the snapshot, do one of the following:
 - Select **Keep Forever** to retain the snapshot on the system indefinitely.
 - Select **Set Retention Period** and use the date spin boxes to choose a length of time for the system to retain the snapshot.
13. Click **OK**.

Deleting a Snapshot Schedule

You can delete a snapshot schedule. Once you delete the schedule, it does not run any future scheduled snapshots. Any snapshots that were created by the schedule remain on the storage system.

Procedure


1. Go to **NetApp SolidFire Management > Data Protection**.

2. Click the **Schedules** sub-tab.
3. Click the **Actions** button () for the schedule you wish to delete.
4. In the resulting menu, click **Delete**.
5. Confirm the action.

Copying a Snapshot Schedule

You can copy a schedule and maintain its current attributes.

Procedure

1. Go to **NetApp SolidFire Management > Data Protection**.
2. Click the **Schedules** sub-tab.
3. Click the **Actions** button () for the schedule you wish to copy.
4. In the resulting menu, click **Copy**.

The **Create Schedule** dialog appears, populated with the current attributes of the schedule.

5. (Optional) Enter a name and updated attributes for the new schedule.

Cluster and Volume Pairing for Real-Time Remote Replication

From the Element OS Web UI, you can pair two clusters and enable real-time replication functionality. When you pair two clusters, active volumes on one cluster can be continuously replicated to a second cluster to provide continuous data protection (CDP). For more information on establishing a cluster or volume pairing, see the *NetApp SolidFire Element OS User Guide*. While some information regarding remote replication status is available from the **Data Protection** page in the NetApp SolidFire Management extension point, you should use the Element OS Web UI or SolidFire API to manage remote replication relationships.

Cluster

From the **Cluster** tab you can view and change cluster-wide settings and perform cluster-specific tasks.

See the following topics to learn about or perform cluster-related tasks:

Drives

Drive Details

Adding Available Drives to a Cluster

Removing a Drive

Removing Failed Drives

Nodes

Storage Nodes

Fibre Channel Nodes

HCI Compute Servers

HCI Storage Nodes

Node Details

Adding a Node to a Cluster

Removing Nodes from a Cluster

VLAN Management

Virtual Network Details

Creating a VLAN

Editing a Virtual Network

Deleting a Virtual Network

Drives

Each node contains one or more physical drives that are used to store a portion of the data for the cluster. The cluster utilizes the capacity and performance of the drive after the drive has been successfully added to a cluster.

A storage node contains two types of drives:

- **Volume Metadata Drives** store compressed information that defines each volume, clone, or snapshot within a cluster. The total metadata drive capacity in the system determines the maximum amount of storage that can be provisioned as volumes. The maximum amount of storage that can be provisioned is independent from how much data is actually stored on the cluster's block drives. Volume metadata drives store data redundantly across a cluster using SolidFire Double Helix data protection.

NOTE: Some system event log and error messages refer to volume metadata drives as slice drives.

- **Block Drives** store the compressed, de-duplicated data blocks for server application volumes. Block drives make up a majority of the storage capacity of the system. The majority of read requests for data already stored on the SolidFire cluster, as well as requests to write data, occur on the block drives. The total block drive capacity in the system determines the maximum amount of data that can be stored, taking into account the effects of compression, thin provisioning, and de-duplication.

Drive Details

On the **Cluster > Drives** page in the NetApp SolidFire Management extension point, you can view a list of the active drives in the cluster. You can change the list view by selecting **Available**, **Removing**, **Erasing**, **Failed** and **All** options in the drop-down list.

When you first initialize a cluster, the active drives list is empty. You can add drives that are unassigned to a cluster and listed in the **Available** tab after a new cluster is created. The following table describes the elements shown in the list of active drives.

| Heading | Description |
|----------------|---|
| Drive ID | Sequential number assigned to the drive. |
| Drive State | The status of the drive. Possible Values: Active: A drive that is in use by the cluster. Available: An available drive that can be added to the cluster. Removing: A drive is in the process of being removed. Any data previously on the drive is being migrated to other drives in the cluster. Erasing: A drive is in the process of being secure erased. Any data on that drive is permanently removed. Failed: A drive that has failed. Any data that was previously on the drive has been migrated to other drives in the cluster. |
| Node ID | Assigned node number when the node is added to the cluster. |
| Node Name | Name of the node where the drive resides. |
| Slot | Slot number where the drive is physically located. |
| Capacity | GB size of the drive. |
| Serial | Serial number of the SSD. |
| Wear Remaining | Wear-level indicator. |
| Type | Drive type can be block or metadata. |

Adding Available Drives to a Cluster

When you add a node to the cluster or install new drives in an existing node, the drives automatically register as available. You must add the drives to the cluster using either the Web UI or SolidFire API before it can participate in the cluster.

Drives are not displayed in the **Available** Drives list when the following conditions exist:

- Drives are in an **Active**, **Removing**, **Erasing**, or a **Failed** state.
- The node of which the drive is a part of is in a **Pending** state.

NOTE: Drive sizes must be compatible within a node. For example, if a 2405 node drive needs to be replaced, it must be replaced with a drive compatible with a 2405 node system. A drive from a 4805 or 9605 node cannot be used to replace a drive in a 2405 node. This is true for all node models in the SolidFire family of nodes. The SolidFire system does not recognize an incompatible drive, and it is never made available to the system.

Procedure

1. Go to **NetApp SolidFire Management > Cluster**.
2. Select **Available** from the drop-down list to view the list of available drives.
3. To add a single drive:
 - Select the drive you wish to add using the mouse pointer.
 - Click **Add**.

4. To add multiple drives:
 - Select the drives you wish to add using the mouse pointer + ctrl/command key.
 - Click **Add**.
5. Confirm the action.

Removing a Drive

You can remove a drive from the list of active drives or from the failed drives list. This takes the drive offline. Before the system fully removes a drive, it writes the data on the drive to other available drives in the system. The data migration to other active drives in the system can take a few minutes to an hour depending on how much capacity is utilized on the cluster and how much active I/O there is on the cluster.

Procedure

1. Go to **NetApp SolidFire Management > Cluster**.
2. Select **All** from the drop-down list to view the complete list of drives.
3. To remove a single drive:
 - Select the drive you wish to remove using the mouse pointer.
 - Click **Remove**.
4. To remove multiple drives:
 - Select the drives you wish to remove using the mouse pointer + ctrl/command key.
 - Click **Remove**.
5. Confirm the action.

NOTE: If there is not enough capacity to remove active drives prior to removing a node, an error message appears when you confirm the drive removal.

Removing Failed Drives

You can remove a failed drive from the failed drive list. The system puts a drive in a failed state if the self-diagnostics of the drive tells the node it has failed or if communications to the drive stop for 5.5 minutes or longer. The **Failed** drives page displays a list of the failed drives.

Drives in the **Alerts** list show as **blockServiceUnhealthy** when a node is offline. When rebooting the node, if the node and its drives come back online within 5.5 minutes, the drives automatically update and continue as active drives in the cluster.

Procedure

1. Go to **NetApp SolidFire Management > Cluster**.
2. Select **Failed** from the drop-down list to view the list of failed drives.
3. To remove a single drive:
 - Select the drive you wish to remove using the mouse pointer.
 - Click **Remove**.
4. To remove multiple drives:
 - Select the drives you wish to remove using the mouse pointer + ctrl/command key.
 - Click **Remove**.
5. Click **Remove**.
6. Confirm the action.

Nodes

SF-series nodes are the hardware that is grouped into a SolidFire cluster to be accessed as block storage. There are two fundamental types of SF-series node: storage and Fibre Channel.

For H-series nodes, which comprise a NetApp HCI system, there are two types: compute server and storage node. Because each compute server runs VMware ESXi, HCI compute server management is done outside the vCenter Plug-in in vSphere.

Storage Nodes

A SolidFire storage node is a collection of drives that communicate with each other through the CIP1 Bond10G network interface. Drives in the node contain block and metadata space for data storage and data management. You can create a cluster with new storage nodes, or add storage nodes to an existing cluster to increase storage capacity and performance.

Storage nodes have the following characteristics:

- Each node has a unique name. If a node name is not specified by an administrator, it defaults to **SF-XXXX** where **XXXX** is four random characters generated by the system.
- Each node has its own high-performance non-volatile random access memory (NVRAM) write cache to improve overall system performance and reduce write latency.
- Each node is connected to two networks with two independent links for redundancy and performance. Each node requires an IP address on each network.
- You can add or remove nodes from the cluster at any time without interrupting service.

Fibre Channel Nodes

SolidFire Fibre Channel nodes provide connectivity to a Fibre Channel switch, which you can connect to Fibre Channel clients. Fibre Channel nodes act as a protocol converter between the Fibre Channel and iSCSI protocols; this enables you to add Fibre Channel connectivity to any new or existing SolidFire cluster.

Fibre Channel nodes have the following characteristics:

- Fibre Channel switches manage the state of the fabric, providing optimized interconnections.
- The traffic between two ports flows through the switches only; it is not transmitted to any other port.
- Failure of a port is isolated and does not affect operation of other ports.
- Multiple pairs of ports can communicate simultaneously in a fabric.

Fibre Channel nodes are added in pairs, and operate in active-active mode (all Fibre Channel nodes actively process traffic for the cluster). At least two Fibre Channel nodes are required for Fibre Channel connectivity in a SolidFire cluster. Clusters running Element OS version 9.0 and later support up to four Fibre Channel nodes; clusters running previous versions support a maximum of two Fibre Channel nodes.

HCI Compute Servers

NetApp HCI compute servers are node hardware that provide the resources, such as CPU, memory, and networking, that are needed for virtualization in the NetApp HCI system. Because each server runs VMware ESXi, HCI compute server management (adding or removing hosts) must be done within the Hosts and Clusters menu in vSphere.

The NetApp HCI system requires a minimum of two compute servers in the system.

HCI Storage Nodes

NetApp HCI storage nodes are hardware that provide the storage resources for a NetApp HCI system. Drives in the node contain block and metadata space for data storage and data management. Each node contains a factory image of the SolidFire Element OS. NetApp HCI storage nodes can be managed using the NetApp SolidFire Management extension point.

A NetApp HCI system requires a minimum of four storage nodes in the cluster.

Node Details

On the **Cluster > Nodes** page in the NetApp SolidFire Management extension point, you can view a list of the active nodes in the cluster. You can change the list view by selecting from the **Pending**, **PendingActive**, and **All** options in the drop-down list.

| Heading | Description |
|--------------------|---|
| Node ID | System-generated ID for the node. |
| Node Name | The system-generated node name. |
| Node State | The status of the node. Possible Values: Active: The node is an active member of a cluster and may not be added to another cluster. Pending: The node is pending for a specific named cluster and can be added. PendingActive: The node is currently being returned to the factory software image, and is not yet an active member of a cluster. When complete, it will transition to the <i>Active</i> state. |
| Available 4k IOPS | Displays the IOPS configured for the node. |
| Node Role | Identifies what role the node has in the cluster. This can be Cluster Master , Ensemble Node , or Fibre Channel node. |
| Node Type | Displays the model type of the node. |
| Active Drives | Number of active drives in the node. |
| Management IP | Management IP (MIP) address assigned to node for 1GbE or 10GbE network admin tasks. |
| Storage IP | Storage IP (SIP) address assigned to the node used for iSCSI network discovery and all data network traffic. |
| Management VLAN ID | The virtual ID for the management local area network. |
| Storage VLAN ID | The virtual ID for the storage local area network. |
| Version | Version of SolidFire Element OS software running on each node. |

Adding a Node to a Cluster

You can add nodes when a cluster is created, or when more storage is needed.

Nodes require initial configuration when they are first powered on. If you are installing a new storage or Fibre Channel node, you can use the *Getting Started Guide* provided with your new node. When the node has been set up and configured, it registers itself on the cluster identified when the node was configured and appears in the list of pending nodes on the **Cluster > Nodes** page of the NetApp SolidFire Management extension point.

Nodes of smaller or larger capacities can be added to an existing cluster.

SolidFire Fibre Channel nodes are added using the same procedure as a SolidFire storage node. They can be added when a cluster is created or added later.

Prerequisites

- The node you are adding has been set up, powered on, and configured.
- Both the major or minor version numbers of the software on each node in a cluster must match for the software to be compatible. For example, Element OS version 8.0 is not compatible with version 8.1.

NOTE: If the node you are adding has a different major or minor version of Element OS than the version running on the cluster, the cluster asynchronously updates the node to the version of Element OS running on the cluster master. Once the node is updated, it automatically adds itself to the cluster. During this asynchronous process, the node will be in a *pendingActive* state.

Procedure

1. Go to **NetApp SolidFire Management > Cluster**.
2. Click the **Nodes** sub-tab.
3. Select **Pending** from the drop-down list to view the list of available nodes.
4. To add a single node:
 - Select the node you wish to add using the mouse pointer.
 - Click **Add**.
5. To add multiple nodes:
 - Select the nodes you wish to add using the mouse pointer + ctrl/command key.
 - Click **Add**.

Removing Nodes from a Cluster

You can remove nodes from a cluster without service interruption when their storage is no longer needed or they require maintenance.

NOTE: At least two Fibre Channel nodes are required for Fibre Channel connectivity in a SolidFire cluster. If only one Fibre Channel node is connected, the system triggers alerts in the **Event Log** until you add another Fibre Channel node to the cluster, even though all Fibre Channel network traffic continues to operate with only one Fibre Channel node.

Prerequisites

Remove the drives in the node from the cluster before proceeding.

Procedure

1. Go to **NetApp SolidFire Management > Cluster**.
2. Click the **Nodes** sub-tab.
3. To remove a single node:
 - Select the node you wish to remove using the mouse pointer.
 - Click **Remove**.
4. To remove multiple nodes:
 - Select the nodes you wish to remove using the mouse pointer + ctrl/command key.
 - Click **Remove**.
5. Confirm the action.

Any nodes removed from a cluster appear in the list of **Pending** nodes.

VLAN Management

Virtual networking in SolidFire storage allows traffic between multiple clients that are on separate logical networks to be connected to one SolidFire cluster. To implement virtual networking, SolidFire uses VLAN backing technology.

The NetApp SolidFire vCenter Plug-in enables you to manage VLANs for the selected cluster. You can create, view, edit, and delete VLANs. VLAN management options are available only from the NetApp SolidFire Management extension point in Global View.

Virtual Network Details

On the **Cluster > Network** page of the NetApp SolidFire Management extension point, you can view the following information for VLANs.

| Heading | Description |
|-----------|---|
| ID | Unique ID of the VLAN network, which is assigned by the SolidFire system. |
| VLAN Name | Unique user-assigned name for the VLAN network. |
| VLAN Tag | VLAN tag assigned when the virtual network was created. |
| SVIP | Storage virtual IP address assigned to the virtual network. |
| IPs Used | The range of virtual network IP addresses used for the virtual network. |

Creating a VLAN

You can add a new virtual network to a cluster configuration to enable a multi-tenant environment connection to a SolidFire cluster. When a virtual network is added, an interface for each node is created and each will require a virtual network IP address. The number of IP addresses specified when creating a new virtual network must be equal to or greater than the number of nodes in the cluster. Virtual network addresses are bulk provisioned by and assigned to individual nodes automatically. Virtual network addresses do not need to be assigned to nodes manually.

Caution: Using VLANs with Fibre Channel nodes as cluster members is not supported.

Prerequisites

- ESXi hosts have a single iSCSI software adapter.
- Hosts or switches are configured for the VLAN.
- You have identified the block of IP addresses that will be assigned to the virtual networks on the SolidFire nodes.
- You have identified a storage network IP (SVIP) address that will be used as an endpoint for all SolidFire storage traffic.

Procedure

1. Go to **NetApp SolidFire Management > Cluster**.
2. Click the **Network** sub-tab
3. Click **Create VLAN**.
4. In the *Create VLAN* dialog , enter a name for the VLAN.
5. Enter an integer for the VLAN tag.
6. Enter the Storage Virtual IP (SVIP) address for the SolidFire storage cluster.

Caution: The default SVIP does not require initiators to be in the same subnet as the SVIP, and routing is supported.

7. Adjust the netmask, as needed. The default is 255.255.255.0.
8. (Optional) Select the **Enable Virtual Routing and Forwarding** check box.

NOTE: Virtual routing and forwarding (VRF) allows multiple instances of a routing table to exist in a router and work simultaneously. This functionality is available for storage networks only.

Caution: The following criteria should be considered for this configuration:

- VRF can only be enabled at the time of creating a VLAN. If you want to switch back to non-VRF, you must delete and recreate the VLAN.
- VLANs that are not VRF-enabled require initiators to be in the same subnet as the SVIP.
- VLANs that are VRF-enabled do not require initiators to be in the same subnet as the SVIP, and routing is supported.

- a. (Optional) Enter an IP address of a gateway of the virtual network.
9. (Optional) Enter a description for the VLAN.
10. Select the hosts that you want to include in the VLAN.
11. Configure the IP address blocks for the storage nodes:

NOTE: A minimum of one IP address block must be created.

- a. Click **Create Block**.
- b. Enter the starting address for the IP range.
- c. Enter the number of IP addresses to include in the address block.

NOTE: The total number of IP addresses must match the number of nodes in the SolidFire storage cluster.

- d. Click outside the entry to accept the values.
12. Click **OK** to create the VLAN.


NOTE: After the VLAN is created, you can find the SVIP of the VLAN in the entry for the host in the Discovered Clusters list in the NetApp SolidFire Configuration extension point and in the target discovery list of the host's iSCSI software adapter in Contextual View.

Editing a Virtual Network

You can change VLAN attributes, such as VLAN name, netmask, and size of the IP address blocks. The VLAN Tag and SVIP cannot be modified for a VLAN. The gateway attribute can only be modified for VRF VLANs.

NOTE: If any iSCSI, remote replication, or other network sessions exist, the modification might fail.


Procedure

1. Go to **NetApp SolidFire Management > Cluster**.
2. Click the **Network** sub-tab
3. Click the **Actions** button () for the VLAN you wish to edit.
4. Click **Edit**.
5. In the resulting menu, enter the new attributes for the VLAN.
6. Click **Add a Block** to add a non-continuous block of IP addresses for the virtual network.
7. Click **OK**.

Deleting a Virtual Network

You can permanently delete a VLAN object and its block of IPs. Address blocks that were assigned to the VLAN are disassociated with the virtual network and can be reassigned to another virtual network.

Procedure

1. Go to **NetApp SolidFire Management > Cluster**.
2. Click the **Network** sub-tab
3. Click the **Actions** button () for the VLAN you wish to delete.
4. Click **Delete**.
5. Confirm the action.

Virtual Volumes

From the **WVols** tab, you can view information and perform tasks for virtual volumes and their associated storage containers, protocol endpoints, bindings, and hosts. The tab is only visible in the user interface once WVol functionality has been enabled.

See the following topics to learn about or perform Wols-related tasks:

Configuring Wols Functionality

[Registering the SolidFire VASA Provider](#)

[Creating a WVol Datastore](#)

Viewing Virtual Volumes Details

[Virtual Volume Details](#)

[Individual Virtual Volume Details](#)

Storage Containers

[Creating a Storage Container](#)

[Viewing Storage Container Details](#)

[Storage Container Details](#)

[Individual Storage Container Details](#)

[Editing a Storage Container](#)

[Deleting a Storage Container](#)

Protocol Endpoints

[Viewing Protocol Endpoint Details](#)

[Protocol Endpoint Details](#)

[Individual Protocol Endpoint Details](#)

Configuring Wols Functionality

You must perform the following initial configuration steps to use Wols in the NetApp SolidFire Plug-in.

Prerequisites

- The SolidFire cluster must be running Element OS version 9.0 (Fluorine) or later.
- The SolidFire cluster must be connected to an ESXi 6.0 or later environment that is compatible with Wols.

Procedure

1. Enable the WVol feature on the SolidFire cluster using the NetApp Configuration extension point. See [Enabling Virtual Volumes](#).
2. Register the VASA provider with vCenter. See [Registering the SolidFire VASA Provider](#).
3. Create a storage container and associated WVol datastore using the NetApp SolidFire Management extension point. See [Creating a Storage Container](#).
4. Create one or more WVol datastores in vCenter. See [Creating a WVol Datastore](#).

Registering the SolidFire VASA Provider

You must register the SolidFire VASA Provider with vCenter so that vCenter is aware of WVol functionality on the cluster. Registering the VASA provider with vCenter is a one-time configuration task.

Prerequisites

- SolidFire Element OS version 9 (Fluorine) or later.
- vCenter version 6.x.
- ESXi hosts version 6.x.

CAUTION: Do not register a SolidFire VASA provider to more than one vCenter instance. The SolidFire VASA provider can only be registered to a single vCenter due to limitations with how vCenter handles SSL. A single vCenter can have multiple SolidFire clusters, but a SolidFire cluster cannot be shared between two instances of vCenter.

Procedure

1. In vCenter, open the vCenter **Inventory List**.
2. From **Resources**, select **vCenter Servers**.
3. Select a vCenter instance for which you wish to register the SolidFire VASA Provider.
4. Select **Manage > Storage Providers**.
5. From **Storage Providers**, click the **Add** icon.

The **New Storage Provider** dialog appears.

6. Enter the following:
 - a. VASA Provider name.
 - b. VASA Provider URL.

NOTE: The VASA Provider URL is provided to you when you enable Wols in the vCenter Plug-in. It is also available in **NetApp SolidFire Configuration > Discovery** if you click the **Actions** button (⚙️) for the cluster you are enabling and click **View Details**.

- c. Administrative account user name for the SolidFire cluster.
 - d. Administrative account password for the SolidFire cluster.
 - e. Click **OK** to add the VASA provider.
7. Press **Yes** to install the SolidFire SSL cert when prompted.

The SolidFire VASA provider should now be registered with a status of **Connected**.

NOTE: Refresh the storage provider, if necessary, to show the current status of the provider after registering the provider for the first time. You can also verify that the provider is enabled in **NetApp SolidFire Configuration > Discovery**. Click the **Actions** button (⚙️) for the cluster you are enabling and click **View Details**.

Creating a Wol Datastore

You must create a virtual volume datastore that represents the storage container on the SolidFire cluster in vCenter. You can create a Wol datastore using the Create Storage Container wizard or by using this process. You must create at least one Wol datastore to begin provisioning Wol-backed virtual machines.

Prerequisites

- A SolidFire cluster with the Wols functionality enabled.
- An existing storage container in the virtual environment.
- The VASA provider must be registered with vCenter.

NOTE: You might need to rescan SolidFire storage in vCenter to discover storage containers.

Procedure

1. From the Navigator view in vCenter, right-click a storage cluster and select **Storage > New Datastore**.
2. In the **New Datastore** dialog, specify the location of the new datastore and click **Next**.
3. Select **WVol** as the type of datastore to create.
4. Provide a name for the datastore in the **Datastore name** field.
5. Select the SolidFire storage container from the **Backing Storage Container** list.

NOTE: You do not need to manually create protocol endpoint (PE) LUNs. They are automatically mapped to the ESXi hosts when the datastore is created.

6. Click **Next**.
7. Click **Finish** to create the WVol datastore.

Viewing Virtual Volumes Details

You can review general information for all active virtual volumes on the cluster in the NetApp SolidFire Management extension point. You can also view details for each virtual volume, including efficiency, performance, and QoS as well as associated snapshots, parent virtual machine, bindings, and task status.

Prerequisites

- You have completed the steps in [Configuring VVols Functionality](#).
- You have created at least one virtual volume.

Procedure

1. Go to **NetApp SolidFire Management > VVols**.
2. From the **Virtual Volumes** tab, you can search for a specific virtual volume by VM name or WVol ID or click **Display All VVols**.
3. Click the **Actions** button (⚙️) for the virtual volume you wish to review.
4. In the resulting menu, select **View Details**.

Virtual Volume Details

On the **VVols > Virtual Volumes** page of the NetApp SolidFire Management extension point, you can view the following virtual volume information for all active virtual volumes on the cluster.

| Heading | Description |
|--------------------|---|
| Virtual Machine ID | The UUID of the virtual machine. |
| Name | The name assigned to the virtual volume. |
| Type | The virtual volume type: Config, Data, Memory, Swap, or Other. |
| Container | The UUID of the storage container that owns the virtual volume. |
| ID | The ID of the underlying volume. |
| Virtual Volume ID | The UUID of the virtual volume. |

Individual Virtual Volume Details

On the **WVols > Virtual Volumes** page of the NetApp SolidFire Management extension point, you can view the following virtual volume information when you select an individual virtual volume and view its details.

| Section | Heading | Description |
|------------------------|---------------------|---|
| Virtual Volume Details | Volume ID | The ID of the underlying volume. |
| | Virtual Volume ID | The UUID of the virtual volume. |
| | Name | The name assigned to the virtual volume. |
| | Virtual Volume Type | The virtual volume type: Config, Data, Memory, Swap, or Other. |
| | Status | The status of WVol task. |
| | Size | Size of the volume in GB or GiB. |
| | Access | The read/write permissions assigned to the virtual volume. |
| Efficiency | Storage Container | The UUID of the storage container that owns the virtual volume. |
| | Compression | The compression efficiency score for the volume. |
| | Deduplication | The de-duplication efficiency score for the volume. |
| | Thin Provisioning | The thin provisioning efficiency score for the volume. |
| Performance | Last Updated | The date and time of the last efficiency score. |
| | Volume Utilization | A floating value that describes how much the client is using the volume. Values: 0 : Client is not using the volume. 1 : Client is using their max. >1 : Client is using their burst. |
| | Actual IOPS | Current actual IOPS to the volume in the last 500 milliseconds. |
| | Average IOP Size | Average size in bytes of recent I/O to the volume in the last 500 milliseconds. |
| | Burst IOPS Credit | The total number of IOP credits available to the user. When volumes are not using up to the Max IOPS, credits are accrued. |
| | Read Operations | The total read operations to the volume since the creation of the volume. |
| | Read Bytes | The total cumulative bytes read from the volume since the creation of the volume. |
| | Read Latency USec | The average time, in microseconds, to complete read operations to the volume in the last 500 milliseconds. |

| Section | Heading | Description |
|--------------------|--------------------|---|
| | Write Operations | The total cumulative write operations to the volume since the creation of the volume. |
| | Write Bytes | The total cumulative bytes written to the volume since the creation of the volume. |
| | Write Latency USec | The average time, in microseconds, to complete write operations to a volume in the last 500 milliseconds. |
| | Async Delay | The length of time since the volume was last synced with the remote cluster. |
| | Client Queue Depth | The number of outstanding read and write operations to the volume. |
| | Latency USec | The average time, in microseconds, to complete operations to the volume in the last 500 milliseconds. A "0" (zero) value means there is no I/O to the volume. |
| | Throttle | A floating value between 0 and 1 that represents how much the system is throttling clients below their maxIOPS because of re-replication of data, transient errors and snapshots taken. |
| | Zero Blocks | Total number of 4KiB blocks without data after the last round of garbage collection operation has completed. |
| | Non-Zero Blocks | Total number of 4KiB blocks with data after the last garbage collection operation has completed. |
| | Unaligned Reads | For 512e volumes, the number of read operations that were not on a 4k sector boundary. High numbers of unaligned reads may indicate improper partition alignment. |
| | Unaligned Writes | For 512e volumes, the number of write operations that were not on a 4k sector boundary. High numbers of unaligned writes may indicate improper partition alignment. |
| | Last Updated | The date and time of the last performance update. |
| Quality of Service | Min IOPS | The minimum IOPS QoS setting of the virtual volume. |
| | Max IOPS | The maximum IOPS QoS setting of the virtual volume. |
| | Burst IOPS | The maximum burst QoS setting of the virtual volume. |
| | Max Bandwidth | The number of IOPS (based on the QoS curve) multiplied by the IO size. |
| Snapshots | ID | System generated ID for the snapshot. |
| | Name | User-defined name for the snapshot. |
| | Create Date | The date and time at which the snapshot was created. |
| | Expiration Date | The day and time the snapshot will be deleted. |
| | Size (GB) | User-defined size of the snapshot. |
| Virtual Machine | Virtual Machine ID | The UUID of the virtual machine. |

| Section | Heading | Description |
|----------|----------------------|--|
| | Name | The name of the virtual machine. |
| | Guest OS Type | Operating system associated with the virtual volume. |
| | Virtual Volumes | List of virtual volumes UUIDs and VM names. |
| Bindings | Host | The UUID for the ESXi host that hosts virtual volumes and is known to the cluster. |
| | Protocol Endpoint ID | Protocol endpoint IDs that correspond to each node in the SolidFire cluster. |
| | PE Type | Indicates the protocol endpoint type (SCSI is the only available protocol for Element OS version 9.0). |
| Tasks | Operation | <p>The type of operation the task is performing.</p> <p>Values:</p> <p>unknown: The task operation is unknown.</p> <p>prepare: The task is preparing a virtual volume.</p> <p>snapshot: The task is creating a snapshot of a virtual volume.</p> <p>rollback: The task is rolling back a virtual volume to a snapshot.</p> <p>clone: The task is creating a clone of the virtual volume.</p> <p>fastClone: The task is creating a fast clone of a virtual volume.</p> <p>copyDiffs: The task is copying differing blocks to a virtual volume.</p> |
| | Task ID | The unique ID of the task. |
| | Status | <p>The current status of the virtual volume task:</p> <p>Values:</p> <p>Error: The task has failed and returned an error.</p> <p>Queued: The task is waiting to be run.</p> <p>Running: The task is currently running.</p> <p>Success: The task has completed successfully.</p> |

Storage Containers

Storage containers are logical constructs that map to SolidFire accounts and are used for reporting and resource allocation. They pool raw storage capacity or aggregate storage capabilities that the storage system can provide to virtual volumes. A WOL datastore that is created in vSphere is mapped to an individual storage container. A single storage container has all available resources from the SolidFire cluster by default. If more granular governance for multi-tenancy is required, multiple storage containers can be created.

Storage containers function like traditional accounts and can contain both virtual volumes and traditional volumes. A maximum of four storage containers per cluster is supported. A minimum of one storage container is required to enable WOLs functionality.

On the **WOLs > Storage Containers** page of the NetApp SolidFire Management extension point, you can create, delete, and manage storage containers. You can discover storage containers in vCenter during WOLs creation.

Creating a Storage Container

You can create storage containers from the WOLs tab in the NetApp SolidFire Management extension point. You must create at least one storage container to begin provisioning WOL-backed virtual machines.

Prerequisites

- You have enabled Wols functionality for the cluster.

Procedure

1. Go to **NetApp SolidFire Management > VVols**.
2. Click the **Storage Containers** sub-tab.
3. Click the **Create Storage Container** button.
4. Enter storage container information in the **Create a New Storage Container** dialog:
 - a. Enter a name for the storage container.
 - b. Configure initiator and target secrets for CHAP.

Best Practices: Leave the **CHAP Settings** fields blank to automatically generate secrets.

- c. [Optional] Select the **Create datastore** check box.
- d. [Optional] Enter a name for the datastore.

NOTE: A WOL datastore is required to use the storage container in vSphere. If you choose not to create a datastore, you must create one later using the vSphere **New Datastore** wizard.

- e. Click **OK**.
5. Verify that the new storage container appears in the list in the **Storage Containers** sub-tab.

NOTE: Because a SolidFire account ID is created automatically and assigned to the storage container, it is not necessary to manually create an account.

Viewing Storage Container Details

You can review information for all active storage containers on the cluster in the NetApp SolidFire Management extension point. You can also view details for each storage container, including efficiency and performance metrics and associated virtual volumes.

Prerequisites

- You have enabled Wols functionality for the cluster.
- At least one storage container is available to select.

Procedure

1. Go to **VVols > Storage Containers**.
The information for all active storage containers displays.
2. Click the **Actions** button (⚙️) for the storage container you wish to review.
3. In the resulting menu, select **View Details**.

Storage Container Details

On the **VVols > Storage Containers** page of the NetApp SolidFire Management extension point, you can view the following information for all active storage containers on the cluster.

| Heading | Description |
|------------|--|
| Account ID | The ID of the SolidFire account associated with the storage container. |

| Heading | Description |
|-------------------|--|
| Name | The name of the storage container. |
| Status | The status of the storage container. Possible values: Active: The storage container is in use. Locked: The storage container is locked. |
| Number of Volumes | The number of active volumes associated with the storage container account. |

Individual Storage Container Details

On the **VVols > Storage Containers** page of the NetApp SolidFire Management extension point, you can view the following storage container information when you select an individual storage container and view its details.

| Section | Heading | Description |
|---------------------------|------------------------|--|
| Storage Container Details | Account ID | The ID of the cluster account associated with the storage container. |
| | Storage Container ID | The UUID of the virtual volume storage container. |
| | Storage Container Name | The name of the storage container. |
| | Status | The status of the storage container. Possible values: Active: The storage container is in use. Locked: The storage container is locked. |
| | Protocol Endpoint Type | Indicates the protocol endpoint type (SCSI is the only available protocol for Element OS version 9.0). |
| | Initiator Secret | The unique CHAP secret for the initiator. |
| | Target Secret | The unique CHAP secret for the target. |
| Efficiency | Number of Volumes | The number of volumes associated with the storage container account. |
| | Compression | The compression efficiency score for volumes in the account. |
| | Deduplication | The de-duplication efficiency score for volumes in the account. |
| | Thin Provisioning | The thin provisioning efficiency score for volumes in the account. |
| | Missing Volumes | The volumes that could not be queried for efficiency data. |
| | Last Updated | The date and time of the last efficiency score. |
| Performance Metrics | Read Bytes | The total cumulative bytes read from all volumes in the account. |
| | Read Operations | The total read operations to all volumes in the account since the creation of the account. |

| Section | Heading | Description |
|-----------------|-------------------|--|
| | Write Bytes | The total cumulative bytes written to all volumes in the account. |
| | Write Operations | The total cumulative write operations to all volume in the account since the creation of the account. |
| | Unaligned Reads | For all 512e volumes in the account (virtual volumes are 512e by default), the number of read operations that were not on a 4k sector boundary. High numbers of unaligned reads may indicate improper partition alignment. |
| | Unaligned Writes | For all 512e volumes in the account (virtual volumes are 512e by default), the number of write operations that were not on a 4k sector boundary. High numbers of unaligned writes may indicate improper partition alignment. |
| | Non-Zero Blocks | Total number of 4KiB blocks with data after the last garbage collection operation has completed. |
| | Zero Blocks | Total number of 4KiB blocks without data after the last round of garbage collection operation has completed. |
| | Last Updated | The date and time of the last performance update. |
| Virtual Volumes | Volume ID | The ID of the underlying volume. |
| | Virtual Volume ID | The UUID of the virtual volume. |
| | Name | The name of the virtual machine. |
| | Status | Status of the VVol task. |


Editing a Storage Container

You can modify storage container CHAP authentication from the NetApp SolidFire Management extension point.

Prerequisites

- You have enabled Wols functionality for the cluster.
- An existing storage container is available to modify.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Under **Accounts**, click the **Actions** button () for the storage container (account) you wish to modify.
3. In the resulting menu, select **Edit**.
4. [Optional] Under **Modify Account**, edit the **Access** status of the account.

NOTE: If an account is locked, no volume reads or writes are permitted.

5. [Optional] Edit the **Initiator Secret** or **Target Secret** credentials used for authentication.

NOTE: If you do not change the **CHAP Settings** credentials, they remain the same. If you make the credentials fields blank, the system automatically generates new secrets.

6. Click **OK**.


Deleting a Storage Container

You can delete storage containers from the NetApp SolidFire Management extension point.

Prerequisites

- You have enabled Vvols functionality for the cluster.
- An existing storage container is available to delete.
- All volumes have been removed from the storage container.

Procedure

1. Go to **NetApp SolidFire Management > Management**.
2. Click the **Actions** button () for the storage container you wish to delete.
3. In the resulting menu, select **Delete**.
4. Confirm the action.
5. Refresh the list of storage containers in the **Storage Containers** sub-tab to confirm that storage container has been removed.

Protocol Endpoints

VMware ESXi hosts use logical I/O proxies known as protocol endpoints to communicate with virtual volumes. ESXi hosts bind virtual volumes to protocol endpoints to perform I/O operations. When a virtual machine on the host performs an I/O operation, the associated protocol endpoint directs I/O to the virtual volume with which it is paired.

Protocol endpoints in a SolidFire cluster function as SCSI administrative logical units. Each protocol endpoint is created automatically by the SolidFire cluster. For every node in a SolidFire cluster, a corresponding protocol endpoint is created. For example, a four-node cluster will have four protocol endpoints.

For the Element OS version 9.0 release, iSCSI is the only supported protocol. Fibre Channel protocol is not supported.


Protocol endpoints cannot be deleted or modified by a user, are not associated with an account, and cannot be added to a volume access group.

On the **VVols > Protocol Endpoints** page of the NetApp SolidFire Management extension point, you can review protocol endpoint information.

Viewing Protocol Endpoint Details

You can review information for all protocol endpoints on the cluster in the NetApp SolidFire Management extension point.

Procedure

1. Go to **NetApp SolidFire Management > VVols**.
The information for all protocol endpoints on the cluster displays.
2. Click the **Actions** button () for an individual protocol endpoint you wish to review.

3. In the resulting menu, select **View Details**.

Protocol Endpoint Details

On the **VVols > Protocol Endpoint** page of the NetApp SolidFire Management extension point, you can view the following information for all protocol endpoints on the cluster.

| Heading | Description |
|-----------------------|---|
| Primary Provider ID | The ID of the primary protocol endpoint provider. |
| Secondary Provider ID | The ID of the secondary protocol endpoint provider. |
| Protocol Endpoint ID | The UUID of the protocol endpoint. |
| Status | The status of the protocol endpoint. Possible values: Active: The protocol endpoint is in use. Start: The protocol endpoint is starting. Failover: The protocol endpoint has failed over. Reserved: The protocol endpoint is reserved. |
| Provider Type | The type of the protocol endpoint's provider. Possible values: Primary Secondary |
| SCSI NAA Device ID | The globally unique SCSI device identifier for the protocol endpoint in NAA IEEE Registered Extended Format. |

Individual Protocol Endpoint Details

On the **VVols > Protocol Endpoint** page of the NetApp SolidFire Management extension point, you can view the following protocol endpoint information when you select an individual protocol endpoint and view its details.

| Heading | Description |
|-----------------------|---|
| Primary Provider ID | The ID of the primary protocol endpoint provider. |
| Secondary Provider ID | The ID of the secondary protocol endpoint provider. |
| Protocol Endpoint ID | The UUID of the protocol endpoint. |
| Status | The status of the protocol endpoint. Possible values: Active: The protocol endpoint is in use. Start: The protocol endpoint is starting. Failover: The protocol endpoint has failed over. Reserved: The protocol endpoint is reserved. |
| Provider Type | The type of the protocol endpoint's provider. Possible values: Primary Secondary |
| SCSI NAA Device ID | The globally unique SCSI device identifier for the protocol endpoint in NAA IEEE Registered Extended Format. |

| Section | Heading | Description |
|-----------------|------------------------|--|
| Hosts | Host Name | The name of the ESXi host. |
| | Host Address | The IP address or DNS name for the ESXi host. |
| | Initiator | Initiator IQNs for the virtual volume host. |
| | Virtual Volume Host ID | The UUID for the ESXi host that hosts virtual volumes and is known to the cluster. |
| Virtual Volumes | Volume ID | The ID of the underlying volume. |
| | Virtual Volume ID | The UUID of the virtual volume. |
| | Name | The name of the virtual machine. |
| | Status | Status of the WOL task. |

Unregistering the SolidFire Plug-in

You can unregister the NetApp SolidFire vCenter Plug-in using one of the procedures described for your installation. Unregistering the Plug-in has the same effect as disabling it but does not remove all associated files and folders. See [Removing the SolidFire Plug-in](#) for additional information.

Prerequisites

- vCenter Administrator role privileges to unregister a plug-in.
- IP address of the management node.
- URL and credentials for the vCenter from which you are unregistering the Plug-in.

Procedure

1. To unregister the Plug-in, follow the procedure for your installed version:

| If | Then |
|--------------------------|--|
| Version 2.6.1 or earlier | <ol style="list-style-type: none"> 1. In a web browser, enter the URL for the registration utility or locate it in the program directory: <ul style="list-style-type: none"> • https://<FDVA or management node IP>:8443 • /opt/solidfire/vcp/bin/vcp-reg.sh 2. In the vCenter Plugin Register/Unregister window, click Unregister. |
| Version 2.7+ | <ul style="list-style-type: none"> • Use the vCenter Managed Object Browser (MOB) interface in your Web browser to manually unregister. <ol style="list-style-type: none"> 1. Enter the MOB URL: https://[vcenter]/mobcontent. 2. Click Extension Manager > Unregister Extension. 3. Enter com.solidfire. 4. Click Invoke Method. • Unregister using PowerCLI: <pre>Connect-VIServer -Server \$vcenter -User administrator@vsphere.local -PassWord xxxXXx -Force -ErrorAction Stop -SaveCredentials \$em = Get-View ExtensionManager \$em.ExtensionList ft -property Key \$em.UnregisterExtension("com.solidfire") \$em.UpdateViewData() \$em.ExtensionList ft -property Key Disconnect-VIServer * -Confirm:\$false</pre> |
| Version 3.0 or later | <ul style="list-style-type: none"> • Unregister using the NetApp SolidFire vCenter Plug-in registration utility: <ol style="list-style-type: none"> 1. Enter the IP address for your management node in a browser, including the TCP port for registration: https://[management node IP]:9443. 2. From the registration UI, click vCenter Plug-in Registration. 3. Click Unregister Plug-in. 4. Enter the following: <ul style="list-style-type: none"> • The IP address of the vCenter on which you have registered your Plug-in. • The vCenter Administrator user name. |

| If | Then |
|----|---|
| | <div><ul style="list-style-type: none">• The vCenter Administrator password.<div>5. Click Unregister.</div><ul style="list-style-type: none">• Unregister using a CLI:<ol style="list-style-type: none">1. Open an SSH client.2. Log on to the management node as a sudo user. <code>\$ ssh [user id]@[mNode ip]</code><div>NOTE: Use the first user ID that was created for the management node.</div>3. Change the current directory: <code>cd /opt/solidfire</code>4. Enter the following to see usage and sample commands: <code>[mNode admin ID]:/opt/solidfire\$ sudo ./vcp-reg.bash -h</code>5. Execute the vcp-reg.bash script using super-user privileges. Append <code>-z</code> to unregister: <code>sudo ./vcp-reg.bash -v [vCenter IP] -A [vCenter Admin ID] -P [Admin password] -z</code><div>NOTE: Do not use parentheses " " options. Use escape \ before special characters.</div></div> |

NOTE: Unregistering a plug-in package on vCenter Server does not delete the plug-in package files that are installed locally. To remove all Plug-in files, see [Removing the SolidFire Plug-in](#).

Removing the SolidFire Plug-in

For SolidFire vCenter Plug-in versions 2.5 and later, complete the following procedure to manually remove files from vCenter Server.

Prerequisites

- You have unregistered the existing Plug-in. See [Unregistering the SolidFire Plug-in](#).

Procedure

1. Stop the VMware vSphere Web Client service:
 - Windows: See the Services list on vCenter Server.
 - vCenter Server Appliance (VCSA): Use the command `service-control --stop`.
2. Remove SolidFire folders and files from the following locations:
 - Windows: Use Windows Explorer and search for "SolidFire" in C:\Program Data\VMware and C:\Program Files\VMware.
 - VCSA: Use the command `find / -name "*solidfire*"`.
3. Start the VMware vSphere Web Client service:
 - Windows: See the Services list on vCenter Server.
 - VCSA: Use the command `service-control --start`.

Appendix 1 — Registering the SolidFire Plug-in Using a CLI

You can use a CLI on a Windows vCenter or VM to register the SolidFire vCenter Plug-in.

Prerequisites

- vCenter Administrator role privileges to register a plug-in.
- An SSH client or web browser (Chrome 56.0.2924, Mozilla 52.0.2, or Internet Explorer 11 or later) on a Microsoft® Windows® 64-bit system.
- You have deployed or upgraded a management node with the version 3.0 OVA as described in [Deploying a New Management Node](#). Your management node must be powered on with its IP address configured.
- Firewall rules allow open network communication between the vCenter and the SolidFire Cluster MVIP on TCP ports 443, 8443, and 9443 (9443 is used for registration and can be closed after registration is complete).

NOTE: If you intend to customize a URL for an HTTP or HTTPS server, complete the prerequisite process described in [Modifying vCenter Properties for In-House HTTP or HTTPS Server](#).

Procedure

1. Open an SSH client.

NOTE: Do not use parentheses " " options. Use the escape \ before special characters.

2. Log on to the management node as a sudo user.

```
$ ssh [user id]@[mNode ip]
```

NOTE: Use the first user ID that was created for the management node.

3. Change the current directory:

```
cd /opt/solidfire
```

4. Enter the following to see usage and sample commands:

```
[mNode admin ID]:/opt/solidfire$ sudo ./vcp-reg.bash -h
```

5. Execute the **vcp-reg.bash** script using super-user privileges. Append **-r** to register or **-u** to update:

NOTE: Most installations will use the default path. You can customize the URL if you are using an in-house HTTP or HTTPS server or have modified the ZIP file name or network settings. Append **-r** to register and **-Z** to create a custom zip URL.

NOTE: The user name and password credentials you enter must be those for an administrator with vCenter Administrator role privileges.

- `sudo ./vcp-reg.bash -v [vCenter IP] -A [vCenter Admin ID] -P [Admin password] -r`
- `sudo ./vcp-reg.bash -v [vCenter IP] -A [vCenter Admin ID] -P [Admin password] -u`
- `sudo ./vcp-reg.bash -v [vCenter IP] -A [vCenter Admin ID] -P [Admin password] -r -Z [https://[customized path]/[customized name of bin.zip]]`

6. (Optional) Verify registration status:

```
sudo ./vcp-reg.bash -v [vCenter IP] -A [vCenter Admin ID] -P [Admin password] -s
```

7. Log into vSphere Web Client as a vCenter Administrator.

NOTE: If the NetApp SolidFire Plug-in icons are not visible from the vSphere main page, see [Troubleshooting](#).

8. (For upgrades) Verify the version change in the **About** tab in the NetApp SolidFire Configuration extension point. For more details, see [How to Use the NetApp SolidFire Plug-in](#).

NOTE: The NetApp SolidFire vCenter Plug-in contains online help content. To ensure that your online help contains the latest content, clear your browser cache after upgrading your Plug-in.

9. (For upgrades) Update your management node IP in the **mNode Settings** tab in the NetApp SolidFire Configuration extension point. See [Configuring mNode Settings for QoSSIOC](#).

Example

The following is an example of a successful registration:

```
admin@SF-1381:/opt/solidfire$ sudo ./vcp-reg.bash -v 10.117.60.123 -A administrator\@vsphere.local -P lala3F\!re -s
```

```
***** WARNING WARNING WARNING *****
* The integrity of the information stored in your keystore *
* has NOT been verified! In order to verify its integrity, *
* you must provide your keystore password.                *
***** WARNING WARNING WARNING *****
```

Plug-in is Not Registered

```
admin@SF-1381:/opt/solidfire$ sudo ./vcp-reg.bash -v 10.117.60.123 -A administrator\@vsphere.local -P lala3F\!re -r
```

```
***** WARNING WARNING WARNING *****
* The integrity of the information stored in your keystore *
* has NOT been verified! In order to verify its integrity, *
* you must provide your keystore password.                *
***** WARNING WARNING WARNING *****
```

Registered Plugin with using key com.solidfire.

```
admin@SF-1381:/opt/solidfire$ sudo ./vcp-reg.bash -v 10.117.60.123 -A administrator\@vsphere.local -P lala3F\!re -s
```

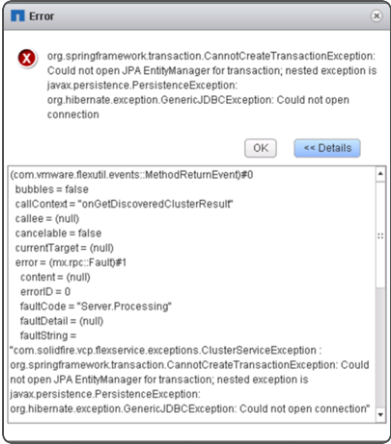
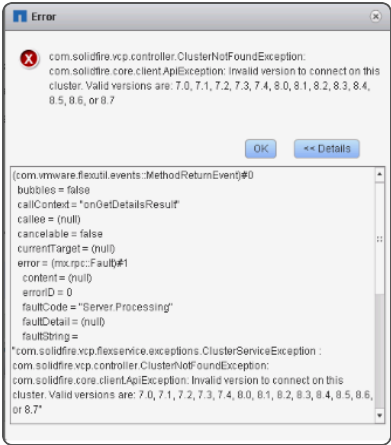
```
***** WARNING WARNING WARNING *****
* The integrity of the information stored in your keystore *
* has NOT been verified! In order to verify its integrity, *
* you must provide your keystore password.                *
***** WARNING WARNING WARNING *****
```

Plug-in with key com.solidfire version 3.0.0 is Registered against 10.117.60.123

Troubleshooting

| Activity | Issue | Resolution/Workaround |
|-------------------------------|---|--|
| Installation and Registration | When using the registration utility, there is an error registering the Plug-in against the vCenter server. A plug-in with the key <code>com.solidfire</code> is already installed. | In the registration utility, use Update Plug-in instead of Register Plug-in . |
| | When using the registration utility, there is an error updating the Plug-in against the vCenter server. A plug-in with the key <code>com.solidfire</code> is not installed for the update. | In the registration utility, use Register Plug-in instead of Update Plug-in . |
| | When using the registration utility, there is an error that indicates the keystore cannot be found at <code>/opt/solidfire/registration/keystore</code> and <code>/var/cache/jetty/tmp/.etc/keystore</code> . | <ol style="list-style-type: none"> 1. Reboot the mNode or execute the following: <code>sudo /opt/solidfire/vcp-reg.bash -F.</code> 2. Refresh the registration utility Web UI. |

| Activity | Issue | Resolution/Workaround |
|-----------|---|---|
| Accessing | Registration shows as successful, but the Plug-in icon is not visible on the Home page. | <ul style="list-style-type: none"> Log out of the vSphere Web Client and log in again. Closing and re-opening your browser may be required. Clear your browser cache. From vCenter, restart the vSphere Web Client Service from the Services menu within Windows Administrative Tools or reboot vCenter. Ensure that you have all required default administrative privileges associated with the vCenter Administrator role. Check that the Plug-in ZIP file successfully downloaded to vCenter: <ol style="list-style-type: none"> Open vsphere_client_virgo.log in the vCenter. <ul style="list-style-type: none"> For vSphere versions 5.x, see the VMware Knowledge Base. For vSphere versions 6.x, see the VMware Knowledge Base. If a failure message indicates that the ZIP download failed, download the ZIP again. <div data-bbox="899 974 1492 1222" data-label="Text"> <p>NOTE: You might need to correct an unreachable or bad URL. Update the Plug-in registration or unregister and register the Plug-in again with a corrected URL. Failure to download the ZIP can also occur if you specified an HTTP URL without changing the <code>allowHTTP</code> setting. See Modifying vCenter Properties for In-House HTTP or HTTPS Server.</p> </div> Verify networking ports. Ensure the management node is reachable from vCenter bidirectionally on the required ports. See Network Ports. Open vsphere_client_virgo.log in the vCenter. If there is no log message about a download, reboot vCenter. |

| Activity | Issue | Resolution/Workaround |
|----------|--|---|
| Upgrades | <p>During a Windows vCenter Server upgrade from version 6.0 to 6.5 , you see a warning that the NetApp SolidFire Extension cannot be upgraded or may not work with the new vCenter Server. After you complete the upgrade and log in to the vSphere Web Client, the following error occurs when you select a vCenter Plug-in extension point:</p>  | <p>The directory that stores the runtime database has changed from version 6.0 to 6.5. The vCenter Plug-in is unable to create the needed files for runtime.</p> <ol style="list-style-type: none">1. Unregister the Plug-in. See Unregistering the SolidFire Plug-in.2. Remove Plug-in files. See Removing the SolidFire Plug-in.3. Reboot the vCenter.4. Register the Plug-in. See Registering the NetApp SolidFire Plug-in in vCenter5. Log into the vSphere Web Client. |
| | <p>After cluster discovery, you update the Element OS version. An error then displays when you try to work with the NetApp SolidFire cluster using the Plug-in:</p>  | <ol style="list-style-type: none">1. Delete the cluster from discovery history. See Deleting a Cluster Entry from Discovery.2. Re-discover the cluster. See Discovering a Cluster. |

| Activity | Issue | Resolution/Workaround |
|-------------|---|---|
| Performance | Cluster status changes to inactive after you change the cluster admin password. | <ol style="list-style-type: none"> 1. Create a new user credential with a new password. 2. Remove the cluster discovery entry. 3. Discover the cluster again and enter new user credentials. 4. Verify the existing datastores. |
| | There is an authentication error after you change the cluster admin password. | <ol style="list-style-type: none"> 1. Create a new user credential with a new password. 2. Remove the cluster discovery entry. 3. Discover the cluster again and enter new user credentials. 4. Verify the existing datastores. |
| | Contextual View has no data. | Contextual View depends on host-to-storage mapping. If no storage from any discovered clusters is attached to a host, nothing will be shown in Contextual View. |

| Activity | Issue | Resolution/Workaround |
|---------------------------|--|---|
| Unregistering the Plug-in | vCenter Plug-in cannot unregister from vCenter after an FDVA or management node IP address change or FDVA or management node reinstallation. | <p>In the vCenter Plug-in version 3.0, use the mNode Settings in the NetApp SolidFire Configuration extension point to make IP address, user ID, or password changes.</p> <p>In the vCenter Plug-in version 2.7, use the QoSSIOC Service settings to make IP address, user ID, or password changes.</p> <p>If you changed the FDVA or management node IP address while using vCenter Plug-in version 2.6.1 and earlier, complete the following procedure to manually unregister the Plug-in:</p> <ol style="list-style-type: none"> 1. Enter the vCenter MOB (<a href="https://<vCenter IP>/mob">https://<vCenter IP>/mob) into your browser. 2. Log in with vCenter Administrator role. 3. Click Content > ExtensionManager > UnregisterExtension. 4. Enter the extension key for your version of the Plug-in. If you have enabled QoSSIOC automation, select the key with <code>qossioc</code> as a suffix: <ul style="list-style-type: none"> • <code>com.calsoft.solidfire</code> (VCP versions earlier than 2.5) • <code>com.calsoft.solidfire.qossioc</code> (VCP versions earlier than 2.5) • <code>com.solidfire</code> (VCP versions 2.5 or later) • <code>com.solidfire.qossioc</code> (VCP versions 2.5 or later) 5. (For vCenter versions 2.6.1 and earlier) Clean up the Plug-in from the FDVA or management node: <ol style="list-style-type: none"> a. Enter the FDVA or management node IP (<a href="https://<FDVA or management node IP>:8443">https://<FDVA or management node IP>:8443) into your browser. b. Click Force Cleanup, and complete the procedure. 6. Register the Plug-in. 7. Restart vCenter services or reboot vCenter. |
| Removal | Removing SolidFire Plug-in package files completed successfully, but NetApp SolidFire icons are still visible on the Home page. | <p>Log out of the vSphere Web Client and log in again. Closing and re-opening your browser may be required.</p> <p>If logging out of vSphere Web Client does not resolve the issue, it might be necessary to restart the vSphere server web services.</p> |

| Activity | Issue | Resolution/Workaround |
|-------------|--|--|
| Credentials | After the admin password for the vCenter that was used to register the Plug-in is changed, the vCenter Plug-in cannot be unregistered or removed. | <p>For Plug-in version 2.6, go to the vCenter Plug-in Register/Unregister page. Click the Update button to change the vCenter IP address, user ID, and password.</p> <p>For Plug-in versions 2.7 and 3.0, update the vCenter Administrator password in the mNode Settings in the NetApp SolidFire Configuration extension point.</p> |
| | A cluster can be discovered once by a SolidFire administrator account with full admin privileges. Once discovered, the cluster discovery credentials used by the admin cannot be removed so that other administrators with limited admin privilege credentials can discover clusters and manage volumes. | Limiting datastore management privileges for any VMware administrator causes the Plug-in icon to disappear and become inaccessible for that administrator. |
| Management | Create, clone, and share datastore tasks fail or volumes are not accessible by the ESXi host. | <ul style="list-style-type: none"> • Check that the software iSCSI HBA is present and enabled on the ESXi host for datastore operations. • Check that the volume is not deleted or assigned to an incorrect volume access group. • Check that the volume access group has the correct host IQN. • Check that the associated account has the correct CHAP settings. • Check that volume status is <code>active</code>, volume access is <code>readWrite</code>, and <code>512e</code> is set to <code>true</code>. |
| | An exception is encountered when viewing datastores or volumes. | Check network connectivity between the FDVA or management node and the SolidFire cluster. |
| | Delete datastore operation fails. | Check that all VMs have been deleted the datastore. You must delete VMs from a datastore before the datastore can be deleted. |
| | The Create Volume Access Group wizard throws an invalid size exception for the initiator name after an IQN is typed into the field. | Remove any additional character after the IQN. If the cursor is returned to the next line, the line is counted as an IQN entry and has no value. |

| Activity | Issue | Resolution/Workaround |
|----------|--|---|
| QoSSIOC | QoSSIOC status in the global settings for the Plug-in displays a warning icon and error message. | <ul style="list-style-type: none"> Unable to reach IP address The IP address is invalid or no responses are received. Verify that the address is correct and that the mNode is online and available. Unable to communicate The IP address can be reached but calls to the address fail. This might indicate that the QoSSIOC service is not running at the specified address or a firewall may be blocking traffic. See Network Ports. Unable to connect to the SIOC service Open sioc.log in /var/log/solidfire/ on the management node to verify that <i>SIOCService</i> started successfully. SIOC service startup can take 50 seconds or more. If the service did not start successfully, try again. You can verify the current status of the SIOC service by opening siocStatus.log in /var/log/solidfire/ on the management node. If you are using a custom user ID or password, see Configuring SIOC Service Credentials. |
| | QoSSIOC service settings displays as UP , but QoSSIOC is unavailable. | From the mNode Settings tab in the NetApp SolidFire Configuration extension point, click the refresh button in the QoSSIOC Service. Update the IP address or user authentication information as needed. |
| | QoSSIOC is enabled for a datastore, but QoSSIOC is unavailable. | <p>Check that the VMware SIOC is enabled on the datastore:</p> <ol style="list-style-type: none"> Open sioc.log in /var/log/solidfire/ on the management node. Search for the text <i>SIOC is not enabled</i>. Use the vSphere Web Client or CLI to enable SIOC on the datastore. |

Related Documentation

The following documents provide additional information about your NetApp system. You can find these documents in [NetApp Documentation: Product Library A-Z](#).

| Document | Focus | Description |
|---|--|--|
| NetApp HCI Prerequisite Checklist | NetApp HCI predeployment | The list of essential steps to complete after purchasing a NetApp HCI system prior to hardware installation and configuring NetApp HCI. The checklist must be completed before you use the NetApp HCI Deployment Engine. |
| NetApp H-Series Installation and Setup Instructions | NetApp HCI hardware installation and setup | A quick start guide for hardware installation provided in the product box. |

| Document | Focus | Description |
|---|--|--|
| NetApp HCI Rail Kit Installation | NetApp HCI hardware installation and setup | A quick start guide for node hardware installation in a rack. |
| NetApp HCI Deployment Engine User Guide | NetApp HCI deployment | A supplementary user guide that is accessible from the NetApp HCI Deployment Engine user interface. The document describes the NetApp HCI deployment process. It also contains descriptions of system features, including Active IQ and alert monitoring management. |
| NetApp HCI Release Notes | NetApp HCI version release information | This document describes HCI features and product improvements for each version. System capabilities and requirements are also described. |
| NetApp SolidFire vCenter Plug-in Release Notes | System management | This document describes the latest features and updates to the tool for managing resources within VMware vCenter. |
| NetApp SolidFire Element OS User Guide | Advanced SolidFire storage operations | This document describes SolidFire storage management using the NetApp SolidFire Element OS Web user interface. Some advanced operations that cannot be performed with Plug-in can be performed from the Element OS Web UI. |
| NetApp SolidFire Element OS API Reference Guide | Advanced SolidFire storage operations | This document describes SolidFire storage management using NetApp SolidFire Element OS APIs. Some advanced operations that cannot be performed with Plug-in can be performed using Element OS APIs. |

Contacting NetApp Support for SolidFire

If you need help or have questions or comments about NetApp SolidFire products, contact NetApp SolidFire Active Support:

- Web: mysupport.netapp.com
- Email: ng-SF-Support@netapp.com
- Phone: 888.4.NETAPP (888.463.8277)



1048 Pearl Street, Suite 250
Boulder, Colorado 80302

Phone: 720.523.3278
Email: info@solidfire.com

Web: netapp.com
Support: mysupport.netapp.com

9/20/2017