

Dell PowerFlex Rack with PowerFlex 4.x

Administration Guide

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Chapter 1: Introduction.....	10
Installing and configuring the jump server.....	10
Install and configure PuTTY.....	10
Install and configure WinSCP.....	11
Chapter 2: Revision history.....	12
Chapter 3: Accessing PowerFlex rack components.....	13
Chapter 4: PowerFlex rack deployment options	14
Chapter 5: Managing components with PowerFlex Manager.....	16
Chapter 6: Add licenses to PowerFlex Manager.....	17
Chapter 7: Enable VMware vCenter high availability.....	18
Chapter 8: Performing maintenance activities in a PowerFlex cluster.....	19
Enter maintenance mode.....	20
Exit maintenance mode.....	21
Enter and exit service mode.....	21
Reboot a PowerFlex node.....	22
Management virtual machines.....	22
Disable the anti-affinity rule for the management virtual machine.....	22
Prepare the management virtual machines for maintenance.....	22
Chapter 9: Monitoring system health.....	23
Monitor system resources.....	23
Manage compliance.....	23
Enabling SupportAssist.....	24
Deploy or configure secure connect gateway.....	24
Configuring the initial setup and generating the access key and pin.....	25
Deploying and configuring policy manager for secure connect gateway.....	25
Configuring SupportAssist on PowerFlex Manager.....	27
Events and alerts.....	29
Managing events and alerts.....	31
Modifying an external source.....	31
Modifying a destination.....	31
Add a notification policy.....	31
Configuring SNMP on the resources for webhook.....	32
Modify a notification policy.....	34
Delete a notification policy.....	34
CloudLink Center.....	35

View CloudLink Center details in PowerFlex Manager.....	35
View CloudLink Center actions.....	35
View CloudLink Center events.....	35
View CloudLink Center security events.....	36
View CloudLink Center alarms.....	36
Chapter 10: Network management.....	37
Networking pre-requisites.....	37
Verify the network configuration.....	41
Add a VLAN to the network.....	41
Add a network to a resource group	43
Registering and configuring Cisco Nexus switches on the Cisco Smart Account portal.....	44
Configure Cisco Smart Account communication using Internet.....	45
Configure Cisco Smart Account communication using the customer proxy server with Internet.....	45
Configure Cisco Smart Account communication using the on-premises Cisco Smart License Utility without Internet.....	46
Configuring networking.....	47
Define a network.....	47
Add a new interface.....	48
Edit a network.....	49
Delete a network.....	49
View port details.....	49
Add the VMware NSX service using PowerFlex Manager.....	50
Chapter 11: Storage management.....	52
Protection domains.....	52
Add protection domains.....	52
Configure network throttling.....	52
Activate a protection domain.....	53
Inactivate a protection domain.....	53
Remove a protection domain.....	53
Fault sets.....	54
Add fault sets.....	54
Place a fault set in maintenance mode.....	54
Exit fault set from maintenance mode.....	55
Cancel protected maintenance mode for fault set.....	55
Delete fault sets.....	55
Storage data servers.....	55
Add storage data servers.....	56
Configure RMcach.....	57
Remove SDSs.....	57
Place storage data server in maintenance mode.....	58
Exit storage data server from maintenance mode.....	58
Cancel entering protected maintenance mode for SDS.....	58
Add storage devices.....	59
Add acceleration devices.....	60
Storage pools.....	60
Add storage pools.....	61
Configure storage pool settings.....	61
Configure RMcach for the storage pool	62

Using the background device scanner.....	62
Set media type for storage pool.....	63
Configuring I/O priorities and bandwidth use.....	64
Acceleration pools.....	64
Add an acceleration pool.....	64
Rename an acceleration pool.....	65
Remove an acceleration pool.....	65
Devices.....	65
Activate devices.....	65
Clear device errors.....	66
Remove devices.....	66
Rename devices.....	66
Set media type.....	67
Set device capacity limits.....	67
Modify device LED settings.....	67
Volumes.....	68
Add volumes.....	68
Delete volumes.....	68
Overwrite volume content.....	69
Create volume snapshots.....	69
Set volume bandwidth and IOPS limits.....	70
Increase volume size.....	70
Map volumes.....	71
Unmap volumes.....	71
Remove a snapshot consistency group	71
Migrating vTrees.....	72
NVMe targets.....	76
Add an NVMe target.....	76
Modify an NVMe target.....	77
Remove an NVMe target.....	77
Understanding NVMe over TCP load balancing.....	77
Hosts.....	81
Add an NVMe host.....	81
Map hosts.....	82
Unmap hosts.....	82
Remove hosts.....	82
Configure or modify approved host IP addresses.....	82
Approve SDCs.....	83
Rename hosts.....	83
Modify an SDC performance profile.....	83
Storage management for PowerFlex controller nodes.....	84
Verify newly added storage data server is reflecting under the appropriate cluster.....	84
Modify the volume capacity.....	84
Increase the datastore size in VMware vCSA.....	84
Configuring replication on PowerFlex nodes.....	85
Clone the storage replication template.....	85
Deploy storage with replication template	86
Clone the hyperconverged replication template.....	86
Deploy PowerFlex hyperconverged nodes with replication template	87
Create and copy certificates.....	88

Create remote consistency groups.....	88
Add peer replication systems.....	89
Redistribute the MDM cluster using PowerFlex Manager.....	90
MDM cluster component layouts.....	90
Redistribute the MDM cluster.....	92
Set rebuild and rebalance settings.....	94
Enabling or disabling SDC authentication.....	94
Log in to PowerFlex using scli.....	95
Prepare for storage data clients authentication.....	95
Configure storage data client to use authentication.....	96
Enable storage data client authentication.....	97
Disable SDC authentication.....	98
Expand an existing PowerFlex cluster with SDC authentication enabled.....	98
Add a Windows or Linux authenticated SDC.....	99

Chapter 12: PowerFlex file storage.....100

NAS server.....	100
Create a NAS server for NFS (UNIX-only) file systems.....	101
Create NAS server for SMB (Windows-only) file systems.....	102
Change NAS server settings.....	103
Configure settings of an existing NAS server.....	103
Manage the network routes between the NAS server and the supported external services.....	103
Modify or configure the NAS server naming services.....	104
NAS server sharing protocols.....	106
NAS server protection and events.....	107
Managing NAS server configuration.....	108
NAS server settings.....	110
NAS server security.....	113
Create a global namespace.....	115
File systems.....	118
Create a file system for NFS exports.....	119
Create a file system for SMB shares.....	120
Change file system settings.....	121
Quotas.....	122
Add file system quotas.....	123
Refresh quotas.....	124
Shares and exports.....	124
Create an NFS export.....	125
Create an SMB share.....	126
File protection.....	128
Create a protection policy.....	128
Create snapshot rules.....	128
Create a snapshot.....	128
Assign a protection policy to a file system.....	129
Unassign a protection policy.....	130
Modify a protection policy.....	130
Delete a protection policy.....	130
Modify a snapshot rule.....	130
Delete a snapshot rule.....	131
Refresh a file system using snapshot.....	131

Restore a file system from a snapshot.....	131
Chapter 13: Reconfiguring MDM roles.....	133
Chapter 14: Set rebuild and rebalance settings.....	134
Chapter 15: Enabling or disabling SDC authentication.....	135
Log in to PowerFlex using scli.....	135
Prepare for storage data clients authentication.....	135
Configure storage data client to use authentication.....	136
Enable storage data client authentication.....	137
Disable SDC authentication.....	138
Expand an existing PowerFlex cluster with SDC authentication enabled.....	139
Add a Windows or Linux authenticated SDC.....	139
Chapter 16: Administering the CloudLink Center.....	141
Add the CloudLink Center license in PowerFlex Manager.....	141
Adding and managing CloudLink Center licenses.....	141
License CloudLink Center.....	141
Delete expired or unused CloudLink Center licenses from PowerFlex Manager.....	142
Configure a custom syslog message format in CloudLink Center.....	142
Manage a self-encrypting drive (SED) from CloudLink Center.....	142
Manage a self-encrypting drive from the command line.....	143
Release a self-encrypting drive.....	143
Release management of a self-encrypting drive from the command line.....	145
Chapter 17: Backup and restore.....	146
VMware vCenter Server.....	146
Back up VMware vCenter Server.....	146
Restore VMware vCenter Server.....	146
PowerFlex Manager.....	147
Edit the backup settings and details.....	148
Back up PowerFlex Manager.....	148
Completing the restore of PowerFlex Manager.....	149
Integrated Dell Remote Access Controller.....	149
Back up iDRAC.....	149
Restore iDRAC.....	150
Network switch configuration back up and restore.....	150
Backing up and restoring CloudLink Center.....	151
View backup information.....	151
Change the schedule for automatic backups.....	151
Generate a backup file manually.....	151
Generate a backup key pair.....	151
Download the current backup file.....	152
Restore the CloudLink backup.....	152
Chapter 18: Powering on and off.....	154
Power on a Technology Extension with PowerScale.....	154
Power on a PowerFlex rack.....	154

Power on the PowerFlex management controller 2.0.....	155
Power on the VMware NSX Edge nodes	157
Power on PowerFlex storage-only nodes.....	158
Power on PowerFlex file nodes.....	158
Power on all PowerFlex hyperconverged nodes.....	158
Power on PowerFlex compute-only nodes.....	159
Complete the powering on of PowerFlex rack.....	159
Power off a PowerFlex rack.....	159
Deactivate protection domain and power off PowerFlex storage-only node using PowerFlex Manager.....	160
Power off PowerFlex compute-only nodes with VMware ESXi.....	161
Power off PowerFlex file nodes.....	161
Power off PowerFlex hyperconverged nodes with VMware ESXi.....	161
Power off the VMware NSX Edge nodes.....	162
Power off the PowerFlex management controller 2.0.....	162
Complete the powering off of PowerFlex rack.....	163
Power off a Technology Extension with PowerScale.....	164

Chapter 19: Usernames and password management..... 165

PowerFlex servers.....	165
Change the Integrated Dell Remote Access Controller 9 (iDRAC9) password.....	165
Change the system and setup passwords.....	165
PowerFlex Manager.....	166
Create credentials for root and non-root users.....	166
Update the PowerFlex Manager password.....	168
Update a credential in PowerFlex Manager.....	168
Updating passwords for nodes.....	169
Updating passwords for system components.....	170
User management.....	170
Virtualization.....	177
Changing a VMware ESXi host root password.....	178
Modify the VMware vCenter Server single sign on default administrator password.....	179
Change the administrator password for VMware vCenter Server Appliance.....	179
Resetting the VMware vCenter Server Appliance root password.....	179
Management VMs.....	180
Change CloudLink passwords.....	180
Unlock secadmin user password.....	180
Manage EmbeddedOS15.3 users credentials for the jump server.....	180
Create users.....	180
Set up desktop icons for a new user.....	181
Delete users.....	181
Enable sudo on a user.....	181
Changing the IPI appliance password.....	181
Changing a user account password on the IPI appliance.....	182
Changing the operating system password.....	182

Chapter 20: System logs and audit logs..... 183

PowerFlex Manager logs.....	183
Generate the troubleshooting bundle.....	183
VMware vCenter logs.....	184

CloudLink logs.....	184
Network logs.....	184
Gather logs from the network switch.....	184
Gathering logs from the Cisco Nexus network for troubleshooting.....	185
Gathering logs from the Dell network for troubleshooting.....	185
Configuring syslogs and audit logs.....	185
Configure syslogs using VMware ESXi.....	186
Configure and forward the syslogs using VMware vCenter.....	186
Configure a custom syslog message format in CloudLink Center.....	186
Configure audit logs in SVMs and PowerFlex storage-only nodes.....	186
Configure iDRAC for audit logging.....	187
Configuring syslogs for Dell PowerSwitch and Cisco Nexus switches.....	188
Enabling audit logging.....	188
Chapter 21: Migrating to NVMe/TCP on ESXi.....	191
Prepare the VMware ESXi node for mapping NVMe/TCP volumes.....	192
Enable the NVMe/TCP VMkernel ports.....	192
Add NVMe /TCP software storage adapter.....	192
Copy the host NQN.....	192
Add a host to PowerFlex.....	193
Create a volume.....	193
Map a volume to the host.....	193
Discover and connect the NVMe/TCP Target.....	193
Perform a rescan of the storage.....	194
Create a VMFS datastore on the NVMe/TCP volume.....	194
Migrate the data with Storage vMotion.....	195

Introduction

This guide provides procedures for administering PowerFlex rack.

It provides the following information:

- Managing components
- Performing maintenance activities in a PowerFlex cluster
- Monitoring
- Network administration
- Storage administration
- Administering the CloudLink Center
- Backup and restore
- Powering on and off
- Usernames and password management
- System logs

The target audience for this document includes system administrators responsible for managing PowerFlex rack, and Dell personnel responsible for remote management.

For additional PowerFlex rack documentation, go to [PowerFlex rack technical documentation](#).

Installing and configuring the jump server

This section covers the configuration and usage of a Windows-based client to access an embedded operating system (embeddedOS 15SPx) jump server. This client allows an administrator to use the jump server more effectively than using the VMware remote console or a virtual desktop. The Windows-based client allows an administrator to run shell commands from a Windows desktop through the jump server and a tool to copy files to and from the jump server from a Windows desktop.

The following table lists the Windows-based tools:

Windows-based tool	Description
SSH (PuTTY)	An open-source and widely used software that allows to connect to a Linux host from a Windows host using SSH.
WinSCP	An open-source and widely used software that allows to transfer files from Windows-based hosts to Linux-based hosts and vice versa.

Install and configure PuTTY

Use this procedure to install and configure PuTTY.

Steps

1. To download PuTTY, do the following:
 - a. Using a web browser of the machine you intend to connect to the jump server with, go to <https://www.putty.org> and click **Download PuTTY**. If troubleshooting is required after following the steps provided, it is recommended to read the documentation that is provided with the software.
 - b. From **Alternative binary files**, download the `putty.exe` for 32-bit x86 to skip installation. If you cannot run or download the binary files, contact your system administrator for assistance.
2. Double-click `putty.exe` to run the binary file.
The **PuTTY Configuration** window opens.
3. Enter the following values:

Field	Do the following
From the Basic options for your PuTTY session	Enter the username and IP address in the Host Name field. For example, admin@10.0.0.5 .
Port	Enter 22 .
Connection Type	Select SSH .
Saved Session	Enter PowerFlex Jump Server and click Save .

4. Click **Open**.

When a warning appears, verify that you are connecting to the appropriate host and click **Accept**.

If you are using the same jump server, the warning does not appear again. If the time taken to accept the connection is too long, a session time out occurs. If you see an empty console, close the session and reconnect.

Install and configure WinSCP

Use this procedure to install and configure WinSCP.

Prerequisites

To download PuTTY, do the following:

1. Using a web browser of the machine you intend to connect to the jump server with, go to <https://winscp.net/eng/downloads.php> and click **Portable Executables**. This allows you to use the software without installing it. This option provides a ZIP file with a WinSCP EXE executable.

Steps

1. Using `winSCP.exe`, log in to configure WinSCP.
2. Enter the following values:

Field	Do the following
File Protocol	Select SCP
Host name	Enter your hostname for the jump server.
Port	Enter 22 .
User name	Enter admin . If you have configured another user on the jump server for this purpose, enter the username.
Password	Enter the password.

3. Optionally, you can save the configuration for ease of usage the next time WinSCP is used.
4. Click **Connect**.
5. When you connect to the jump server for the first time, you must validate the credentials of the jump server. After you confirm the host, click **Yes**.
6. Enter the password when prompted.
After connecting to the jump server, the file structure of the local Windows host appears in the left pane of the window and jump server file structure appears in the right pane.

Revision history

Date	Document revision	Description of changes
January 2024	2.3	Removed references to NFS
November 2023	2.2	Updated support for embedded operating system. Added information on: <ul style="list-style-type: none"> Installing and configuring the jump server Syslogs and audit logs
October 2023	2.1	Updated the powering off procedures for PowerFlex rack and PowerFlex management controller 2.0.
September 2023	2.0	Added support for: <ul style="list-style-type: none"> Multi-VLAN and multi-subnet network Configuring SNMP on the resources for webhook Deploying and configuring policy manager for secure connect gateway Managing NAS server configuration and settings Creating and managing a global namespace Updated the Cisco Smart Account licensing information for Cisco NX-OS 10.2.x
May 2023	1.4	<ul style="list-style-type: none"> Added the hold-down-time configuration for an nve1 interface Updates to backing up PowerFlex Manager
March 2023	1.3	Editorial updates
January 2023	1.2	Updated the following: <ul style="list-style-type: none"> PowerFlex file storage Cisco Smart Account licensing information
September 2022	1.1	Added Cisco Smart Account licensing information.
August 2022	1.0	Initial release

Accessing PowerFlex rack components

Component	Method of access
PowerFlex Manager	https://pxfm_server_ip_address_or_fqdn
Secure connect gateway	https://<hostname(FQDN) or IP address:5700>
Policy manager for secure connect gateway	https://<hostname(FQDN) or IP address:8443>
VMware vCenter	https://vcenter_server_ip_address_or_fqdn
VMware ESXi	https://esxi-ip-address_or_fqdn
iDRAC	https://idrac-ip-address
CloudLink	https://cloudlinkcenterIP
VMware vCenter server appliance management	https://vcenter_server_ip_address_or_fqdn:5480
Jump server	RDP for EmbeddedOS15SPx and VNC for EmbeddedOS 7.x
Network switches	SSH

PowerFlex rack deployment options

PowerFlex rack has several options for deployment.

PowerFlex runs on PowerFlex rack nodes to operate the management and customer storage and tie in workloads. PowerFlex has the following components:

- Storage data client (SDC): Consumes storage from the PowerFlex rack
- Storage data server (SDS): Contributes node storage to PowerFlex rack
- PowerFlex metadata manager (MDM): Manages the storage blocks and tracks data location across the system
- Storage Data Target (SDT): Manages host connections and controllers, process NVMe commands, both IO and Admin and it sends the IO commands forward to SDS through an embedded LibSDC. SDS is unaware to the source of the IO commands: SDC or NVMe hosts.
- Storage data replication (SDR): Enables replication on PowerFlex storage-only nodes

PowerFlex enables flexible deployment options by allowing the separation of SDC and SDS components. PowerFlex Manager allows you to specify a non-root user instead of the root user when you configure a template for a compute-only, storage-only, hyperconverged, or PowerFlex file deployment. It addresses data center workload requirements through the following PowerFlex rack deployment options:

Deployment type	Description
Full hyperconverged	Consists of PowerFlex hyperconverged nodes, which contribute both compute and storage resources to the virtual environment. Front-end (application) and back-end (storage) traffic share the same PowerFlex data networks. This includes PowerFlex hyperconverged nodes and PowerFlex storage-only nodes with NVMe.
Two-layer	Separates compute resources from storage resources, allowing the independent expansion of compute or storage resources. Consists of PowerFlex compute-only nodes (supporting the SDC) and PowerFlex storage-only nodes (connected to and managed by the SDS). PowerFlex compute-only nodes host end-user applications. PowerFlex storage-only nodes contribute storage to the system pool.
Hybrid hyperconverged	Consists of PowerFlex hyperconverged nodes, PowerFlex compute-only nodes, and PowerFlex storage-only nodes. Some PowerFlex nodes contribute both compute resources and storage resources (PowerFlex hyperconverged nodes), some contribute only compute resources (PowerFlex compute-only nodes), and some contribute only storage resources (PowerFlex storage-only nodes).
Storage-only	Consists of nodes that contribute storage resources to the virtual environment. The back-end traffic shares the same PowerFlex data networks. The storage-only PowerFlex rack provide volumes to an external customer compute limited to Dell PowerEdge servers. storage data replication (SDR) is installed to enable native asynchronous replication on the PowerFlex storage-only nodes. No SDC components are installed on these nodes.
Dual network	Consists of a solution integrated into your existing software-defined network (SDN), such as, Cisco application centric infrastructure (ACI). Only PowerFlex hyperconverged nodes and PowerFlex compute-only nodes are affected and have two NICs cabled to a pair of customer access/leaf switches. Aggregation switches by default are tied into the customer SDN border for Layer-2 or Layer-3 access. The solution uses two new customer access switches, two additional network ports on the host, and a new distributed virtual switch to carry traffic seamlessly into the software-defined network.

Two-layer deployments allow rebooting of VMware cluster nodes without PowerFlex ramifications.

When designing initial deployment or specifying later growth, use PowerFlex hyperconverged nodes if both PowerFlex compute-only nodes and PowerFlex storage-only nodes are needed. You can add PowerFlex compute-only nodes or PowerFlex storage-only nodes as needed.

To control the number of processors or cores, consider separating the compute for the application from the PowerFlex nodes that support storage. This deployment is a pure two-layer deployment. Extra workloads are supported or added on:

- PowerFlex hyperconverged nodes
- Two-layer PowerFlex compute-only nodes
- PowerFlex storage-only nodes

This creates a hybrid deployment.

PowerFlex rack is configured with a single VMware vCenter, consisting of separate datacenters for controller and customer nodes. To access controller nodes, use the PowerFlex management controller. To access customer nodes, use the PowerFlex operating system for the customer cluster.

Managing components with PowerFlex Manager

Once PowerFlex Manager is configured, you can use it to perform the ongoing tasks necessary to manage your PowerFlex rack.

The following table describes typical tasks for managing PowerFlex rack components and what steps to take in PowerFlex Manager to initiate each:

If you want to...	Do this in PowerFlex Manager...
View network topology	<ol style="list-style-type: none"> 1. Click Lifecycle > Resource Groups. 2. On the Resource Groups page, select a resource group. 3. On the Resource Group Details page, click the Port View tab.
Run inventory (PowerFlex nodes, switches, and VMware vCenter cluster).	<ol style="list-style-type: none"> 1. Click Resources and click the All Resources tab. 2. Click the check box for the resource you want to update and click Run Inventory. 3. After running the inventory, click Resource Group Details under More Actions on the Resource Groups page for any resource group that requires the updated resource data.
Add an existing resource group	<ol style="list-style-type: none"> 1. Click Lifecycle > Resource Groups. 2. Click +Add Existing Resource Group.
Perform PowerFlex node expansion	<ol style="list-style-type: none"> 1. Click Lifecycle > Resource Groups. 2. On the Resource Groups page, select a resource group. 3. On the Resource Group Details page, under Add Resources and click Add Nodes. <p>The procedure is the same for new resource groups and existing resource groups.</p>
Remove a PowerFlex node	<ol style="list-style-type: none"> 1. Click Lifecycle > Resource Groups. 2. On the Resource Group page, select a resource group. 3. On the Resource Group Details page, under More Actions, click Remove Resource. 4. Select Delete Resource for the Resource removal type.
Enter service mode	<ol style="list-style-type: none"> 1. Click Lifecycle > Resource Groups. 2. On the Resource Group page, select a resource group. 3. On the Resource Group Details page, under More Actions, click Enter Service Mode.
Exit service mode	<ol style="list-style-type: none"> 1. Click Lifecycle > Resource Groups. 2. On the Resource Group page, select a resource group. 3. On the Resource Group Details page, under More Actions, click Exit Service Mode.
Reconfigure MDM roles	<ol style="list-style-type: none"> 1. Click Lifecycle > Resource Groups. 2. On the Resource Group page, select a resource group. 3. On the Resource Group Details tab, click Reconfigure MDM Roles under More Actions. <p>You can also reconfigure MDM roles from the Resources page. Select a PowerFlex gateway and click View Details. Click Reconfigure MDM Roles.</p>
Replace a drive	<ol style="list-style-type: none"> 1. Click Lifecycle > Resource Groups. 2. On the Resource Group page, select a resource group. 3. On the Resource Group Details page, under Physical Nodes, click Drive Replacement.

Add licenses to PowerFlex Manager

PowerFlex Manager comes by default with a trial or evaluation license for first 90 days. There is no requirement to upload an evaluation license. After 90 days, the license should be enforced or it displays an error message and no operation can be performed.

About this task

The license is on a single format which includes both PowerFlex Manager and PowerFlex. The license is based on capacity with no expiry date. If the capacity exceeds the license capacity, a new license with more capacity must be uploaded.

 **NOTE:** New license capacity would be aggregate of old capacity with newly purchased capacity.

Steps

1. To upload the PowerFlex license:
 - a. From PowerFlex Manager, click **Settings > License management**.
 - b. Click **PowerFlex License**. Under **Production license**, click **Choose File** and select the PowerFlex license.
 - c. To upload an MDS license, click **Choose File** in the **Management Data Store (MDS) License** section and select the license file. Click **Save**.
 - d. To upload a production license for PowerFlex, click **Choose File** in the **Production License** section and select the license file. Click **Save**.
2. To upload the CloudLink license:
 - a. Click **Other Software Licenses**.
 - b. Click **Add**.
 - c. From **Upload License**, click **Choose License**.
 - d. Browse and select the license to upload and click **Open**.
 - e. Select the type as **CloudLink** and click **Save**.

Enable VMware vCenter high availability

VMware vCenter high availability (vCenter HA) protects the VMware vCenter Server against host and hardware failures. The active-passive architecture of the solution can also help reduce downtime significantly when you patch the vCenter Server.

After you create a three-node PowerFlex cluster that contains active, passive, and witness nodes. Different configuration paths are available, your selection depends on your existing configuration.

VMware vCenter HA requirements:

- Recommended minimum of three VMware ESXi hosts.
- Validate the flex-vcsa-ha networking and VMware vCenter port groups have been configured.

See the [VMware vSphere Product Documentation](#) for additional requirements and configuration of VMware vCenter HA.

Performing maintenance activities in a PowerFlex cluster

You place a node in maintenance mode to repair, replace, or upgrade hardware components for the customer and management clusters.

When performing maintenance on PowerFlex nodes, the following maintenance options are available:

Mode	Description
Instant maintenance mode	<p>Perform short-term maintenance that lasts less than 30 minutes. It is designed for quick entry to and exit from a maintenance state. The node is immediately and temporarily removed from active participation.</p> <p>Use for scenarios such as non-disruptive, rolling upgrades, where the maintenance window is only a few minutes (for example, a reboot) and there are no known hardware issues.</p>
Protected maintenance mode	<p>Perform maintenance or updates that require longer than 30 minutes in a safe and protected manner. PowerFlex makes a temporary copy of the data, providing data availability without the risk of exposure of an accessible single copy.</p>

Instant maintenance mode

In instant maintenance mode, the data on the node undergoing maintenance is not removed from the cluster. However, this data is not available for use for the duration of the maintenance activity. Instead, extra copies of data residing on the other nodes are used for application reads.

The existing data on the node being maintained is, in effect, frozen on the node. This is a planned operation that does not trigger a rebuild. Instead, the PowerFlex metadata manager instructs the storage data clients (SDC) where to read and write IOs intended to be directed at the node in maintenance.

A disadvantage of instant maintenance mode is that it introduces a risk of having only a single copy of data available during maintenance activity. During instant maintenance mode, there are always two copies of data. However, any copy residing on the node in maintenance is unavailable for the maintenance duration.

When exiting instant maintenance mode, you do not need to rehydrate the node completely. You need to only sync back any relevant changes that have occurred and reuse all the unchanged data on the node. This results in a quick exit from maintenance mode and quick return to full capacity and performance.

Protected maintenance mode

Protected maintenance mode initiates a many-to-many rebalancing process. Data is preserved on the node entering maintenance, and a temporary copy of the data is created on the sustaining nodes. Data on the node in maintenance is frozen and inaccessible. Protected maintenance mode maintains two copies of data at all times, avoiding the risks from the single copy in instant maintenance mode.

During protected maintenance mode, changes are tracked only for writes that affect the SDS under maintenance mode (what does this mean). When exiting the SDS from maintenance mode, only the changes that occurred during maintenance need to be synced to the SDS.

Due to the creation of a temporary third data copy, protected maintenance mode requires more spare capacity than instant maintenance mode. Account for this spare capacity during deployment if you plan to use protected maintenance mode. There

must be enough spare capacity to handle at least one other node failure, as protected maintenance mode cycles might be long and other elements could fail.

Protected maintenance mode makes the best use of all unused, available capacity, as it uses both the allocated spare capacity and any generally free capacity. It does not ignore capacity requirements. Nodes entering protected maintenance mode or in the same fault set may have degraded capacity.

The following equation summarizes the minimum requirements: $\text{Free} + \text{spare} - 5\% \text{ of the storage pool} \geq \text{protected maintenance mode node size}$.

Eject the node from the cluster

When a node is gracefully removed using the UI or CLI, a many-to-many rebalance operation between nodes begins. This ensures that there are two copies of all data on all other nodes before the node being maintained is dropped from the cluster. Data is fully protected as there are always two available copies of the data.

You may need to adjust the spare capacity assigned to the cluster overall, as the data rebalancing uses up free spare capacity on the other nodes. For example, if you start with 10 nodes and 10% spare capacity, running with nine nodes requires 12% spare capacity to avoid an insufficient spare capacity alert. Spare capacity must be equal to or greater than the capacity of the smallest unit (node).

During maintenance, the cluster functions normally, but with one less node and therefore less capacity and lower performance. Data writes are sent to and mirrored on the other nodes. It does not matter how long the maintained node is offline, as it is no longer a part of the cluster. There is no exposure or risk of data unavailability if a problem arises that prohibits the node from being re-added.

General restrictions and limitations

- Do not put two nodes from the same protection domain simultaneously into instant maintenance mode or protected maintenance mode.
- You cannot mix protected maintenance mode and instant maintenance mode on the same protection domain.
- For each protection domain, all SDS concurrently in protected maintenance mode must belong to the same fault set. There are no inter-protection domain dependencies for protected maintenance mode.
- You can take down one SDS or full fault set in protected maintenance mode.

Enter maintenance mode

Use this procedure to enter maintenance mode using PowerFlex Manager.

Steps

1. Log in to PowerFlex Manager.
2. On the menu bar, click **Block > SDSs**.
3. In the list of SDSs, select the relevant SDS and click **More Actions > Enter Maintenance Mode**.
4. In the **Enter SDS into Maintenance Mode** dialog box, select one of the following options:
 - **Instant** - A node is temporarily removed without building a new copy of the data. During maintenance, the system only mirrors new writes. After maintenance is complete, the system applies the new writes to the node that was under maintenance.
 - **Protected** - A third copy is created before entering maintenance mode. This ensures that if there is a node failure where the second copy of SDS is required, there is still a full backup of the SDS. This leaves no room for discrepancy between the copies. More storage capacity from the node is required.
5. Click **Enter Maintenance Mode**.
6. Verify that the operation has finished successfully and click **Dismiss**.
7. Click **Running Jobs** and check the progress of protected maintenance mode.

Exit maintenance mode

Use this procedure to exit maintenance mode using PowerFlex Manager.

Steps

1. Log in to PowerFlex Manager.
2. On the menu, click **Block > SDSs**.
3. In the list of SDSs, select the relevant SDS and click **More Actions > Exit Maintenance Mode**.
4. In the **Exit SDS from Maintenance Mode** dialog box, click **Exit Maintenance Mode**.
5. Verify that the operation has finished successfully and click **Dismiss**.

After the operation has been completed successfully, the SDS returns to normal operation, and data deltas collected on other SDSs during the maintenance period are copied back to the SDS.

Enter and exit service mode

PowerFlex Manager enables you to put a node in service mode when you must perform maintenance operations on the node. When you put a node in service mode, you can specify whether you are performing short-term maintenance or long-term maintenance work. The option that you use for long-term maintenance depends on the PowerFlex version you are using.

About this task

PowerFlex Manager detects when a node is in VMware ESXi or PowerFlex maintenance mode. It automatically places the node in service mode and also ensures that the service itself goes into service mode.

If DAS cache is installed on a node, or if the node has a VMware NSX configuration, PowerFlex Manager does not enable you to enter service mode. PowerFlex Manager also does not enable you to enter service mode if the PowerFlex Gateway used in the service is being updated on the **Resources** page.

Prerequisites

Before evacuating a node for long-term maintenance work, ensure that you have at least four nodes in the cluster. Also, ensure that you have sufficient storage space on the remaining nodes to evacuate the data from the node that is placed in service mode.

Steps

1. From the menu, click **Lifecycle > Resource Groups**.
2. From the **Resource Groups** page, select a resource group and click **View Details**.
3. Under **More Actions**, click **Enter Service Mode**.
4. Select one or more nodes on the **Node Lists** page and click **Next**.
You can only put multiple nodes in service mode simultaneously if all the nodes are in the same fault set.
5. Specify the type of maintenance you want to perform by selecting one of the following options:
 - Instant maintenance mode - Enables you to perform short-term maintenance that lasts less than 30 minutes. PowerFlex Manager does not migrate the data.
 - Protected maintenance mode - Enables you to perform maintenance that requires longer than 30 minutes in a safe and protected manner. When you use protected maintenance mode, PowerFlex makes a temporary copy of the data so that the cluster is fully protected from data loss. Protected maintenance mode applies only to hyperconverged and storage-only resource groups.
6. Click **Finish**.
PowerFlex Manager displays a yellow warning banner at the top of the **Resource Groups** page. The **Service Mode** icon displays for the **Deployment State** and **Overall Resource Group Health**, and **Resource Health** for the selected nodes.
7. To leave service mode, click **More Actions > Exit Service Mode**.

Reboot a PowerFlex node

PowerFlex Manager prevents two nodes from being in service mode simultaneously to protect data.

Prerequisites

Place the PowerFlex node in service mode.

Steps

1. After PowerFlex Manager shows that the node has entered service mode, turn off the PowerFlex node by using the iDRAC interface to run a graceful shutdown.
2. Use the iDRAC interface to power on the PowerFlex node.
3. Exit the node from service mode.

Management virtual machines

This section covers the procedures to disable the anti-affinity rule and prepare the management virtual machines for maintenance.

Disable the anti-affinity rule for the management virtual machine

Move a management virtual machine to another host when performing maintenance activities. You must disable the anti-affinity rule for the management virtual machine.

Steps

1. Log in to the VMware vCenter server.
2. Click **PPMC-MGMT-Cluster**.
3. Click **Configure** and select **VM/Host Rules**.
4. Select the management VM affinity rule, click **Edit** and uncheck **Enable Rule**.
5. Click **OK**.


Prepare the management virtual machines for maintenance

Use this procedure to drain the management virtual machine to safely evict all of your pods before you perform maintenance on the management virtual machine.

Steps

1. Log in to the primary management virtual machine.
2. Type `kubectl get nodes` to list all of the nodes.
3. Identify the node scheduled for maintenance from above, and type `kubectl drain <node> --ignore-daemonsets --delete-emptydir-data` to drain the node.

The node will be cordoned, which will mark the node as unschedulable and prevent the scheduler from placing new pods onto that node.

 **NOTE:** PowerFlex Manager could be inaccessible for five to ten minutes.

4. Perform maintenance procedures.
5. Type `kubectl uncordon <node>` to uncordon the node.

Monitoring system health

Use PowerFlex Manager to monitor the system health.

PowerFlex Manager includes the following features:

- A dashboard that provides system configuration details and communicates health status for PowerFlex rack infrastructure elements and services.
- Release Certification Matrix (RCM) compliance monitoring and reporting
- Release Certification Matrix (RCM) remediation for nodes, switches, PowerFlex, VMware ESXi, and CloudLink.
- Hardware monitoring and alerting through either Secure Remote Services, email, or SNMP and syslog to Dell Technologies Support.
- Aggregated logging for troubleshooting, with the ability to send logs through secure connect gateway to Dell Technologies Support.

Monitor system resources

Use PowerFlex Manager to monitor system health.


The following table describes common tasks for monitoring system health and what steps to take in PowerFlex Manager to initiate each:

If you want to...	Do this in PowerFlex Manager...
Monitor system resources and health	On the Dashboard , look at the Overall Performance , Usable Capacity , and Data Savings sections. For information about which resource groups are healthy and in compliance and which are not, look at the Resource Groups section.
View alerts	On the menu bar, click Monitoring > Alerts .

Manage compliance

Use PowerFlex Manager to manage software and firmware RCM compliance.

The following table describes common tasks and what steps to take in PowerFlex Manager to initiate each:

If you want to...	Do this in PowerFlex Manager...
Monitor software and firmware compliance	<ol style="list-style-type: none"> 1. Click Lifecycle > Resource Groups. 2. On the Resource Groups page, select a resource group. 3. On the Resource Group Details page, click View Compliance Report.
Perform software and firmware remediation	<ol style="list-style-type: none"> 1. From the compliance report, view the firmware or software components. 2. Click Update Resources to update non-compliant resources.
Generate a troubleshooting bundle	<ol style="list-style-type: none"> 1. Click Settings > Serviceability. 2. Click Generate Troubleshooting Bundle. <p> NOTE: You can also generate the troubleshooting bundle from the Resource Group page.</p>
Download a report that lists compliance details for all resources	<ol style="list-style-type: none"> 1. Click Resources. 2. Click Export Report and then click Export Compliance PDF Report or Export Compliance CSV Report.

If you want to...	Do this in PowerFlex Manager...
Download a configuration report	<ol style="list-style-type: none"> 1. Click Resources. 2. Click Export Report > Export Configuration PDF Report.

Enabling SupportAssist

- There are two options to configure events and alerts:
 - Connect directly
 - Connect using secure connect gateway
- If you connect directly, only the call home option is available
- If you connect through secure connect gateway, all options through secure connect gateway are enabled
- You do not need to deploy and configure secure connect gateway if you choose ESE direct

Deploy or configure secure connect gateway


Secure connect gateway is an enterprise monitoring technology that monitors your devices and proactively detects hardware issues that may occur.

Prerequisites


- Download the required version of secure connect gateway from the [PowerFlex rack RCM software](#).
- You must have VMware vCenter Server running on the virtual machine on which you want to deploy secure connect gateway. Deploying secure connect gateway directly on a server running VMware vSphere ESXi is not supported.

Steps


1. Download and extract the OVF file to a location accessible by the VMware vSphere Client.
2. On the right pane, click **Create/Register VM**.
3. On the **Select Creation Type** page, select **Deploy a virtual machine from an OVF or an OVA file** and click **Next**.
4. On the **Select OVF and VMDK files** page, enter a name for the virtual machine, select the OVF and VMDK files, and click **Next**.

 **NOTE:** If there is more than one datastore on the host, the datastores are displayed on the **Select storage** page.

5. Select the location to store the virtual machine files and click **Next**.
6. On the **License agreements** page, read the license agreement, click **I agree**, and click **Next**.
7. On the **Deployment options** page, perform the following steps:
 - a. From the **Network mappings** list, select the network that the deployment template must use.
 - b. Select a disk provisioning type.
 - c. Click **Next**.
8. On the **Customize Settings** page, enter the following details and click **Next**.
 - Domain name server
 - Hostname
 - Default gateway
 - Network IPv4 and IPv6
 - Time zone
 - Root password

 **NOTE:** Ensure that the root password consists of eight characters with at least one uppercase and one lowercase letter, one number, and one special character. Use this root password to log in to secure connect gateway for the first time after the deployment.

9. On the **Ready to complete** page, verify the details that are displayed, and click **Finish**.
A message is displayed after the deployment is complete and the virtual machine is powered on.

 **NOTE:** Wait 15 minutes before you log in to the secure connect gateway user interface.

10. After installation, power on the secure connect gateway.
11. Go to **https://localhost:5700/** and log in using the root credentials to check the user interface access.

Configuring the initial setup and generating the access key and pin

Use the section to generate the access key and pin to register with secure connect gateway and [PowerFlex rack RCM software](#).

Use this link to generate the Dell Support account and access key and pin: <https://www.dell.com/support/kbdoc/en-us/000180688/generate-access-key-and-pin-for-dell-products?lang=en>.

Customers should work with field engineer support to get the SITE ID that is required while generating the access key and pin.

Related information

[Configure SupportAssist using the connect directly mode](#)

Log in to the secure connect gateway user interface

Use this procedure to log in to the secure connect gateway user interface.

Steps

1. Go to **https://<hostname (FQDN) or IP address:5700/>**.
2. Enter the username as root and password created while deploying the VM.
3. Create the admin password:
 - a. Enter a new password.
 - b. Confirm the password.
4. Accept the terms and conditions.
5. Provide the access key and pin generated in *Configuring the initial setup and generating the access key and pin*.
6. Enter the **Primary Support Contacts** information.

Deploying and configuring policy manager for secure connect gateway

Policy manager for secure connect gateway is a device access management technology that is delivered as a virtual appliance. Policy manager for secure connect gateway can be deployed on a hypervisor.

You can configure policy manager for secure connect gateway to perform the following tasks:

- Control remote access to your devices.
- Maintain an audit log of remote connections and file transfers.
- Access administration actions performed on policy manager for secure connect gateway.

Minimum requirements to deploy and use Policy Manager for Secure Connect Gateway

The following sections provide information about:

- Minimum system and network requirements for the local system to deploy policy manager.
- Browsers that can be used to access the policy manager user interface.
- Hypervisors that can be used to deploy policy manager.

System requirements

The system requirements to deploy and use policy manager are:

- Number of processor cores—4
- Installed memory (RAM)—8 GB
- Hard drive space—120 GB—Thin Provisioning

Deploy policy manager for secure connect gateway

Use this procedure to deploy policy manager for secure connect gateway.

About this task

PowerFlex Manager does not manage policies or policy manager for secure connect gateway.

This chapter does not cover procedures to create and manage policies. For information on creating and managing policies, see *Dell Policy Manager for Secure Connect Gateway User's Guide*.

Prerequisites

Before deploying policy manager for secure connect gateway, ensure the following:

- Upgrade secure connect gateway
- Download the latest version of policy manager for secure connect gateway from [Dell Technologies Support site](#).


Steps

1. Download and extract the OVF file to a location accessible by VMware vSphere Client.
2. On the right pane of VMware vSphere Client, click **Create/Register VM**.
The **New virtual machine** window is displayed.
3. On the **Select creation type** page, select **Deploy a virtual machine from an OVF or an OVA file** and click **Next**.
4. On the **Select OVF and VMDK files** page, enter a name for the virtual machine, select the OVF and VMDK files, and click **Next**.
The **Select storage** page is displayed. If there is more than one datastore on the host, the datastores are displayed on the **Select storage** page.
5. Select the location to store the virtual machine files and click **Next**.
6. On the **License agreements** page, read the license agreement, click **I agree**, and click **Next**.
7. On the **Deployment options** page, perform the following steps:
 - a. From the **Network mappings** list, select the network that the deployment template must use.
 - b. Select a disk provisioning type.
 - c. Click **Next**.
8. On the **Additional settings** page, enter the following details and click **Next**:
 - Domain name server
 - Hostname
 - Default gateway
 - Network IPv4 and IPv6
 - Time zone
 - Secure socket layer
 - Root password: Ensure that the root password consists of eight characters with at least one uppercase and one lowercase letter, one number, and one special character.
 - Web administrator username: After deployment, the username is automatically updated to admin.
9. On the **Ready to complete** page, verify the details that are displayed and click **Finish**.
A message is displayed after the deployment is complete and the virtual machine is powered on.
10. Log in to policy manager for secure connect gateway and perform the following steps:
 - a. Go to **https://<hostname(FQDN) or IP address>:8443**
 - b. Enter admin as the user ID.
 - c. If you are logging in for the first time, enter the default password.
 - d. After logging in for the first time, enter the new administrator account password when prompted and click **Save**.
 - e. Enter the new password and click **Log In**.


Configure policy manager settings on secure connect gateway

Use this procedure to ensure connectivity between secure connect gateway and policy manager.

About this task

 **NOTE:** Policy manager is not managed by PowerFlex Manager.

Steps

1. Sign in to secure connect gateway.
2. Go to **Settings > Environment configuration > Connectivity details > Policy Manager**.
3. Click **Enable remote Policy manager**.
4. Enter the hostname or IP address, port number, username, and password of the policy manager server.
 **NOTE:** If the port is SSL secured, the port number must be **8443**. If the port is not SSL secured, the port number must be **8888**.
5. Click **Enable SSL** if policy manager for secure connect gateway is installed on a server that is secured by SSL.
6. If the policy manager server connects to the Internet through a proxy server, perform the following steps in the **Customer proxy server** section:
 - a. Click **Enable proxy server for Policy manager only**.
 - b. Enter the hostname or IP address and port number.
 - c. Click **Proxy requires authentication** and enter the username and password to access the proxy server.
7. Test the connection and click **Apply**.


Configuring SupportAssist on PowerFlex Manager

Depending on the customers requirement, use the following procedures to configure the connect direct or connect using the secure connect gateway.

Configure SupportAssist using the connect directly mode

Use this procedure to enable SupportAssist using the connect directly mode.

Steps

1. Log in to PowerFlex Manager.
2. Click **Settings > Events and alerts**.
3. Click **Notification Policies**.
4. From the policies tab on the grayed out part, click **Configure Now**.
5. On the **Overview** page, click **Next**.
6. Accept the license and telemetry agreement on the connect support assist page and click **Next**.
7. Choose the connection type **Connect Directly**.
 **NOTE:** This helps us directly connect to SupportAssist direct. Call to home feature works on connect direct. The proxy setting is not supported.
8. Click **Connect to cloudIQ**.
It enables PowerFlex Manager to transport telemetry data, alerts and analytics to assist Dell Technologies in providing support.
9. On the **Authentication details** page, provide the following details.
10. Access key and PIN generated in [Configuring the initial setup and generating the access key and pin](#).
You need the software ID for generating the access key and PIN.
11. Choose the **Device type** to be registered like rack, appliance or software.

12. In the **Enterprise License Management Systems** file, enter the software ID used in step 2 while generating the access key and pin.
13. The **Solution serial number** must be provided by customer.
14. In the **Site ID** field, provide the site ID location. If you do not have one, contact Dell Technologies Support to generate one.
15. Click **Next**, provide the contact details for customer, and click **Finish**.
A popup appears on the bottom of the screen configuring SupportAssist and another pop up appears once it is successfully configured.
16. To activate the policy now, click **Configure Now** and enable the policy by making it active.
After the policy is active, it will remove from grayed out mode to available and active mode.

Related information

[Configuring the initial setup and generating the access key and pin](#)


Connect SupportAssist using the secure connect gateway

Use this procedure to enable SupportAssist using the secure connect gateway.

Prerequisites

Configure the secure connect gateway.

Steps

1. Log in to PowerFlex Manager.
2. Click **Settings > Events and alerts**.
3. Click **Notification Policies**.
4. From the **Policies** tab on the grayed out part, click **Configure Now**.
5. Accept the license and telemetry agreement on the **Connect SupportAssist** page and click **Next**.
6. Choose the connection type **connect via gateway**.
 **NOTE:** Connect using the gateway helps register PowerFlex Manager on secure connect gateway and SupportAssist.
From here we can enable the proxy setting.
7. Provide the **SCG IP address and Port** number.
8. Click **Connect to CloudIQ**.
It enables PowerFlex Manager to transport telemetry data, alerts and analytics to assist Dell Technologies in providing support.
9. Enable the **Remote Support** button and click **Next**.
10. On the **Authentication Details** page, provide the following details.
11. Access key and PIN.
12. Choose the **Device** type to register like rack, appliance or software.
13. In the **Enterprise License Management Systems** file, enter the software ID used in step 4 while generating the access key and PIN.
14. The **Solution serial number** must be provided by the customer.
15. In the **Site ID** field, provide the site ID location. If you do not have one, contact Dell Technologies Support to generate one.
16. Click **Connect to CloudIQ**.
It enables PowerFlex Manager to transport telemetry data, alerts and analytics to assist Dell Technologies in providing support.
17. Click **Next**, provide the contact details for the customer, and click **Finish**.
A popup appears on the bottom of the screen configuring SupportAssist and another pop up appears once it is successfully configured.
18. To activate the policy now, click **Configure Now** and enable the policy by making it active.
Once the policy is active, it will remove from grayed out mode to available and active mode.

Events and alerts

A source is used to configure the receiving of external events and syslog content.

A destination is used to configure the ability to send events and alerts information out. A destination is always external.

SupportAssist, email, SNMP, webhooks, remote syslog are considered destinations.

Notification policies define what information is sent to each destination. Events and alerts exist irrespective of whether notification policies are created.

SNMP sources are not automatically discovered and must be configured to receive events about these sources. PowerFlex Manager is preconfigured and events, and alerts are automatically available. Resources in the PowerFlex rack are automatically discovered. Any future resources, for example, switch replacements or additional nodes, are considered external and must be added manually as sources.

PowerFlex Manager enables you to register a notification receiver for pushing alert and event messages through webhooks to a target system, for example, BigPanda.


Configure an external source

You must define a source to enable PowerFlex Manager to receive an external event.

About this task

A syslog source can only go to a syslog destination and does not display in events. An SNMP source, either V2 or V3, displays in events even without a defined notification policy.

For a webhook, the Resources need to be discovered in PowerFlex Manager, and the load balancer IP address need to be configured on the Resources individually. The alerts from individual resources will be sent to Webhooks from the source resource type.

 **NOTE:** For a webhooks destination, SNMPv3 is supported for iDRAC.

SNMPv2c is supported for all Resource types like switch CloudLink, iDRAC.

Steps

1. Go to **Settings > Events and Alerts > Notification Policies**.
2. From the **Sources** pane, click **Add**.
3. Enter a source name and description.
4. Configure either SNMP or syslog forwarding and click **Submit > Dismiss**:
 - For SNMPv2c:
 - a. Enter the community string by which the source forwards traps to destinations.
 - b. Enter the same community string for the configured resource. During discovery, if you selected PowerFlex Manager to automatically configure iDRAC nodes to send alerts to PowerFlex Manager, enter the community string that is used in that credential here.
 - For SNMPv3:
 - a. Enter the username, which identifies the ID where traps are forwarded on the network management system.
 - b. Select a security level from the following:

Security level	Description	authPassword	privPassword
Minimum	noAuthNoPriv	Not required	Not required
Moderate	authNoPriv	Required	Not required
Maximum	authPriv	Required	Required

- If you select Syslog, click **Enable Syslog**.

Configure a destination

Define a location where event and alert data that has been processed by PowerFlex Manager should be sent.

Steps

1. Click **Settings > Events and Alerts > Notification Policies**.
2. From the **Destinations** pane, click **Add**.
3. From the **Destinations** page:
 - a. Enter the destination name and description.
 - b. From **Destination Type** menu, select to configure either SNMP, Syslog, or email (SMTP) forwarding.
 - c. Click **Next**.
 - d. Depending on the destination type, enter the following information:

Destination Type	Protocol settings
SNMP V2c	<ul style="list-style-type: none">• Network name/IP address• Port• Community string
SNMP V3	<ul style="list-style-type: none">• Network name/IP address• Port• Username• Security level:<ul style="list-style-type: none">◦ Minimal - no more information required◦ Moderate - MD5 authentication password required◦ Maximum - MD5 authentication and DES privacy passwords required
Syslog	<ul style="list-style-type: none">• Network name/IP address• Port• Protocol:<ul style="list-style-type: none">◦ UDP◦ TCP• Facility:<ul style="list-style-type: none">◦ All◦ Authentication◦ Security and authentication
Email (SMTP)	<ul style="list-style-type: none">• Destination name• Description• Destination type:<ul style="list-style-type: none">◦ Server type:<ul style="list-style-type: none">▪ SMTP▪ SMTP over SSL▪ SMTPS SMARTTLS◦ Server IP or FQDN◦ Port◦ Sender address and up to five recipient addresses◦ If you choose credentials, enter:<ul style="list-style-type: none">▪ Username, password, sender address, and up to five recipient addresses• Send test email• Test email server connection
Webhook	<ul style="list-style-type: none">• Description<ul style="list-style-type: none">◦ Destination name• Destination Type• Select Webhook (You can have up to three webhook destinations.)• Webhook destination API URL

Destination Type	Protocol settings
	<ul style="list-style-type: none"> For example, if you want to configure a webhook destination for BigPanda, you need to specify the BigPanda endpoint here. You can get this URL from the BigPanda site. Enable Credentials. Credentials <ul style="list-style-type: none"> For example, for BigPanda, the credential you use must have an app key and a token string. You can generate these values on the BigPanda site and then copy them to the app key and token fields. Test Webhook.

- Click **Finish**.

Managing events and alerts

Use this section to manage events and alerts.

Modifying an external source

You can edit the information about how PowerFlex Manager receives an event.

Steps

- Go to **Settings > Events and Alerts > Notification Policies**.
- From the **Sources** pane, click the source that you want to modify.
The **Edit Source** window opens.
- Edit the information and click **Submit**.

Modifying a destination

You can edit the information about where event and alert data that is processed by PowerFlex Manager should be sent.

Steps

- Go to **Settings > Events and Alerts > Notification Policies**.
- From the **pane, click the destination whose information you want to modify.
The **Edit Source** window opens.**
- Edit the information and click **Submit**.

Add a notification policy

When you add a notification policy, you define the rules for processing events or alerts from sources, and to which destinations that information should be sent.

Steps

- Go to **Settings > Events and Alerts > Notification Policies**.
- Click **Create New Policy**.
- Enter a name and a description for the notification policy.
- From the **Source Type** menu, select how you want events and alerts to be received. The source type options are:
 - Snmpv2c**
 - Snmpv3**
 - Syslog**
 - Powerflex**

PowerFlex related alerts are generated and forwarded to a webhook destination when the notification policy is configured with the **Source Type** set to **Powerflex**.

5. From the **Resource Domain** menu, select the resource domain that you want to add a notification policy to. The resource domain options are:
 - **All**
 - **Management**
 - **Block (Storage)**
 - **File (Storage)**
 - **Compute (Servers, Operating Systems, virtualization)**
 - **Network (Switches, connectivity etc.)**
 - **Security (RBAC, certificates, CloudLink etc.)**
6. Select the check box beside the severity levels that you want to associate with this policy. The severity indicates the risk (if any) to the system, in relation to the changes that generated the event message.
7. Select the required destination. You can choose one or more destinations. For a webhook, you can have up to three destinations defined.
8. Click **Submit**.


Next steps

After adding a notification policy, you might need to perform additional configuration steps. For example, If you are setting up a notification policy for a webhook destination that uses BigPanda, you can optionally configure BigPanda to show the severity levels from PowerFlex Manager. To do this, you must configure the status mapping on the BigPanda site. Map the `major` and `minor` severity values from PowerFlex Manager to the `Warning` status for BigPanda.

Configuring SNMP on the resources for webhook

For the SNMP alerts to be forwarded to such a site like BigPanda, the load balancer IP address of the management virtual machine is configured on each of the resources individually.

The resources like CloudLink, iDRAC and the switches should be discovered and managed in PowerFlex Manager.

 **NOTE:** For a webhook destination, SNMPv3 is supported for iDRAC.

SNMPv2c is supported for all resource types like CloudLink, iDRAC, and switches.

Identify the load balancer IP address

Use this procedure to identify the load balancer IP address on the management virtual machines.

Steps

To identify the load balancer IP address on the management virtual machine, type: `kubectl get svc -A | grep snmp`.

Example output:

```
k8-1:~ # kubectl get svc -A | grep snmp
powerflex          snmp-listener
LoadBalancer      10.43.1.151    10.118.146.195
162:32655/UDP,514:31040/UDP,514:31040/TCP
```

Configure SNMP on CloudLink

Use this procedure to configure SNMP on CloudLink.

Prerequisites

Ensure the following:

- CloudLink is discovered in PowerFlex Manager.

- An external source is configured.

Steps

1. Discover CloudLink on **Resources** page.
2. Log in to CloudLink.
3. Click **Server > SNMP** and click **Add**.
4. On the **Add NEW SNMP** configuration window:
 - a. Select the **Target Version** as **SNMPv2**.
 - b. On the **Host** field, add the **Load Balancer IP** to forward SNMP traps from CloudLink to PowerFlex rack.
 - c. The port number to be 162.
 - d. Add the details as description.
 - e. Add the community string, enter the same community string used when creating SNMPv2 source on the PowerFlex management platform appliance, for example: **public**.
 - f. Click **Add**.
5. Click **Send Test Trap**.
A test critical/warning alert is sent to PowerFlex Manager.

Configure SNMP on iDRAC

Use this procedure to configure SNMP on iDRAC.


Prerequisites

Ensure the following:

- iDRAC is discovered in PowerFlex Manager.
- An external source is configured.

Steps

1. Log in to iDRAC.
2. Click **Configuration**.
3. Select **System Settings > Alert Configuration > Alerts** and enable **Alerts**.
4. Expand **Quick alerts Configuration**, select the options as it required to be forwarded to PowerFlex Manager.
 - a. Select **Alert Categories**.
 - b. Select **Issue Severities**.
 - c. Select **SNMP Trap for notification type**.
 - d. Click **Apply**.
5. Under **SNMP Traps Configuration**, complete the following:
 - a. Select the **Alert Destination** and in the Destination Address field, update the **Load Balancer IP**.
 - b. For SNMPv3 traps, choose the user for **SNMP V3 User** under dropdown menu and click **Apply**.

 **NOTE:** SNMPv3 User must be configured on iDRAC before performing SNMPv3 alert forwarding test.
6. Under **SNMP Settings**, complete the following:
 - a. On the **Community String** field, enter the same community string used when creating SNMPv2 source on PowerFlex management platform appliance.
 - b. The port number to be 162.
 - c. Change the **SNMP Trap format** to **SNMP V2** or **SNMP V3**.
 - d. Click **Apply**.

Configure SNMP on a switch

Use this procedure to configure SNMP on a Cisco Nexus or a Dell PowerSwitch switch.

Prerequisites

Ensure the following:


- iDRAC is discovered in PowerFlex Manager.
- An external source is configured.

Steps

Configure SNMP:


- On a Cisco Nexus switch:
 - a. SSH to the Cisco Nexus switch.
 - b. Enable and configure SNMPv2c traps, type the following:


```
# configure terminal
# snmp-server host <Load balancer IP of PFXM> traps version 2c <community string>
```

 **NOTE:** Enter the same community string used when creating SNMPv2 source on PowerFlex management platform, for example: **public**, for example: `# snmp-server host 1.1.1.1 traps version 2c public`
 - c. Save the configuration, type the following:


```
# copy running-config startup-config
```
 - d. Repeat the steps for all of the switches.
- On a Dell PowerSwitch:
 - a. SSH to the Dell OS10 Dell PowerSwitch.
 - b. Enable and configure SNMPv2c traps, type the following:


```
# configure terminal
# snmp-server host <Load balancer IP of PFXM> traps version 2c <community string>
```

 **NOTE:** Enter the same community string used when creating SNMPv2 source on PowerFlex management platform, for example: **public**, for example: `# snmp-server host 1.1.1.1 traps version 2c public`
 - c. Save the configuration, type the following:


```
# copy running-config startup-config
```
 - d. Repeat the steps for all of the switches.

Modify a notification policy

You can modify certain settings that are associated with a notification policy.

About this task

You cannot modify the source type or destination once it is assigned to a notification policy.

Steps

1. Go to **Settings > Events and Alerts > Notification Policies**.
2. Select the notification policy that you want to modify.
3. You can choose to modify the notification policy in the following ways:
 - To activate or deactivate the policy, click **Active**.
 - To modify the policy, click **Modify**. The **Edit Notification Policy** window opens.
4. Click **Submit**.

Delete a notification policy

Use this procedure to delete a notification policy.

About this task

-  **NOTE:** Once a notification policy is deleted, it cannot be recovered.

Steps

1. Go to **Settings > Events and Alerts > Notification Policies**.
2. Select the notification policy that you want to delete.
3. Click **Delete**.
You receive a message to confirm if you want to delete the policy.
4. Click **Submit** and click **Dismiss**.

CloudLink Center

View CloudLink Center details in PowerFlex Manager

View CloudLink Center resource details.

Steps

1. From the menu bar, click **Resources**.
2. From the **Resources** tab, click the row containing CloudLink Center and click **View Details**.
The **Details** page displays detailed information about the CloudLink Center resource on the following tabs:
 - **Summary**: Displays cluster details, system performance, alarms, pending machines, and security events. If CloudLink has clustered CloudLink Centers, PowerFlex Manager shows all CloudLink Centers.
 - **Machines**: Displays machine groups and machines.
 - **Approved networks**: Displays a list of the names and IP addresses for all approved networks going in and out of the CloudLink Center.

The **Details** page displays information that is similar to information provided in the CloudLink application. All the data is based on the last inventory, as indicated by the Last Inventory timestamp shown on the left side of the **Details** page under **Resource Information**. Whenever the inventory is updated, either automatically or manually, any changes that are made in the CloudLink Center are reflected in the **Details** page.
3. To view additional details, click **Launch Console** to launch the CloudLink application.

View CloudLink Center actions

View the actions initiated by users, such as uploading or assigning licenses, accepting a pending machine, or setting the CloudLink Vault mode.

Steps

1. Log in to CloudLink Center.
2. Click **Monitoring > Actions**.
You can view the actions that happened in the last 10 minutes, 30 minutes, 1 hour or more.

View CloudLink Center events

View the internal activity in the system, as well as activity related to actions and alarms.

Steps

1. Log in to CloudLink Center.
2. Click **Monitoring > Events**.
You can view the all the events or events that happened in the last 10 minutes, 30 minutes, or 1 hour.

View CloudLink Center security events

View the CloudLink Center security events that happened in the last 10, 30 minutes, one hour or view all the security events.

Steps

1. Log in to CloudLink Center.
2. Click **Monitoring** > **Security Events**.

View CloudLink Center alarms

An alarm represents a state or condition. When one or more alarm conditions exist, CloudLink Center displays a badge on the Alarms icon in the home page. The badge indicates the number of alarms.

Steps

1. Log in to CloudLink Center.
2. From the Home page, click the bell icon or click **Monitoring** > **Alarms**.

Network management

This section describes common procedures to administer the network in a PowerFlex rack environment using either CLI or PowerFlex Manager.

Networking pre-requisites

Configure the customer network for routing and layer-2 access for the various networks before PowerFlex Manager deploys the PowerFlex rack cluster.

The pre-deployment customer network requirements are as follows:

- Redundant connections to access switches using virtual link trunking (VLT) or virtual port channel (VPC).
- MTU=9216 on all ports or link aggregation interfaces carrying PowerFlex data VLANs.
- MTU=9216 as default on VMware vMotion and PowerFlex data interfaces.

The following table lists customer network pre-deployment VLAN configuration options:

- **Example VLAN:** Lists the VLANs that are used in the PowerFlex rack deployment.
- **Example multi-VLAN:** Lists the multi-VLANs that are used in the PowerFlex rack deployment.
- **Network type:** Type of networks used in the PowerFlex management controller deployment.
- **Descriptor:** Describes each network or VLAN.


NOTE:

- VLAN numbers in the table are an example, they may change depending on customer requirements.
- Configure VLAN 130 on all PowerFlex management controllers connected to access or leaf switches.
- Configure OOB management multi-VLANs on all access or leaf switches.


In a default PowerFlex setup two data networks are standard. Four data networks are only required for specific customer requirements, for example, high performance or use of trunk ports. For more information, contact your Dell Technologies Support.

PowerFlex supports multi-VLAN or a multi-subnet configuration for all network types other than the data, vSAN, and NSX overlay.

For a multi-VLAN, configure the aggregation switches with corresponding SVI interface and trunk allowed VLAN list. For a multi-subnet, an additional IP address configuration is required for each additional subnet used within the VLAN and first hop redundancy configuration as required.

 **CAUTION:** All defined data networks must be accessible from all storage data clients (SDC). If you have implemented a solution with four data networks, all four must be assigned and accessible from each storage data client. Using less than the configured number of networks will result in an error in PowerFlex and can lead to path failures and other challenges if not properly configured.

VLAN network requirements:

- VLAN flex-node-mgmt (105) or pfmc-mgmt (130) and flex-stor-mgmt (150) must be routable to each other
-  **NOTE:** For a multi-subnet or multi-VLAN configuration, configure the PowerFlex management VM and NSX Gateway VM with VLAN 130 instead of the hypervisor management that reside on 105. Standard builds without multi-VLAN or multi-subnet can be available on either hypervisor management (105) or management interface (130) of PowerFlex management VM or NSX Gateway VM.
- VLAN flex-nas-mgmt (250) and flex-stor-mgmt (150) must be routable to each other
- VLAN flex-node-mgmt (105) or pfmc-mgmt (130) and pfmc-sds-mgmt (140) must be routable to each other

Network requirements for PowerFlex management controller 2.0

Example VLAN	Example multi-VLAN	Traffic type	Network type	Description
101	210-224	Hardware Management	General purpose	For connection to PowerFlex management controller node iDRAC interface and PowerFlex Manager (PowerFlex management platform VMs and ingress controller)
103	-	VMware vCenter HA	General purpose	For VMware vCenter high availability (vCenter HA) network interface
105	240-254	Hypervisor management	Hypervisor management	For management interface of VMware ESXi, VMware vCenter
105	-	Hypervisor management recovery	Hypervisor management	PowerFlex management controller management recovery
130	-	PowerFlex management controller for a multi-VLAN or multi-subnet network	Hypervisor management	For VMware vCenter, CloudLink center, jump server, secure connect gateway (SCG) and PowerFlex Manager (PowerFlex management platform VMs and ingress controller)
130	-	PowerFlex management controller recovery	Hypervisor management	PowerFlex management for a multi-VLAN or multi-subnet network recovery
140	300-314	PowerFlex management controller 2.0 PowerFlex management	PowerFlex management	For SVM management interface on management controller PowerFlex cluster
141	-	PowerFlex management controller 2.0 PowerFlex data 1	PowerFlex data	For SDS-to-SDS and SDS-to-SDC data path
142	-	PowerFlex management controller 2.0 PowerFlex data 2	PowerFlex data	
143	330-344	PowerFlex management controller 2.0 Hypervisor migration	VMware vMotion	For VMware vSphere vMotion interface on management controller vSphere cluster
150	360-374	PowerFlex management	Hypervisor management	For SVM and PowerFlex storage-only node Management interface
151	-	PowerFlex data 1	General purpose	For SDS-to-SDS and SDS-to-SDC data path
152	-	PowerFlex data 2	General purpose	For SDS-to-SDS and SDS-to-SDC data path
153	-	PowerFlex data 3 (if required)	General purpose	For SDS-to-SDS and SDS-to-SDC data path
154	-	PowerFlex data 4 (if required)	General purpose	For SDS-to-SDS and SDS-to-SDC data path

Network requirements for PowerFlex production cluster

Example VLAN	Example multi-LAN	Network Name	Description	Properties
101	210-224	Hardware management	For connection to PowerFlex production node iDRAC interface	Layer-2/Layer-3 connectivity, MTU=1500/9216
105	240-254	Hypervisor management	For VMware ESXi management interface on production vSphere cluster	Layer-3 connectivity, MTU=1500/9216
106	270-284	Hypervisor migration	For VMware vSphere vMotion interface on production vSphere cluster	Layer-2 connectivity, MTU=1500/9216 NOTE: Layer-3 if multi-subnet/multi-VLAN is used.
130	-	PowerFlex management for a multi-VLAN network	For VMware vCenter, CloudLink center, jump server, secure connect gateway (SCG) and PowerFlex Manager (PowerFlex management platform VMs and ingress controller)	Layer-3 connectivity, MTU=1500
150	360-374	PowerFlex management	For SVM and PowerFlex storage-only node management interface	Layer-3 connectivity, MTU=1500/9216
151	-	PowerFlex data 1	For SDS-to-SDS and SDS-to-SDC data path	Layer-2 connectivity, MTU=9216
152	-	PowerFlex data 2	For SDS-to-SDS and SDS-to-SDC data path	Layer-2 connectivity, MTU=9216
153	-	PowerFlex data 3 (if required)	For SDS-to-SDS and SDS-to-SDC data path	Layer-2 connectivity, MTU=9216
154	-	PowerFlex data 4 (if required)	For SDS-to-SDS and SDS-to-SDC data path	Layer-2 connectivity, MTU=9216

Network requirements for PowerFlex asynchronous replication (optional)

Example VLAN	Example multi-LAN	Network Name	Description	Properties
161	390-404	PowerFlex replication 1	For SDR-SDR external communication	Layer-3 connectivity, MTU=9216. Routable to replication peer system
162	420-434	PowerFlex replication 2	For SDR-SDR external communication	Layer-3 connectivity, MTU=9216. Routable to replication peer system

Network requirements for PowerFlex file (optional)

Example VLAN	Example multi-VLAN	Network Name	Description	Properties
101	210-224	Hardware management	For connection to PowerFlex file node iDRAC interface	Layer-2/Layer-3 connectivity, MTU=1500/9216
150	360-374	PowerFlex management	For PowerFlex file node operating system management	Layer-3 connectivity, MTU=1500/9216
151	-	PowerFlex data 1	For SDS-to-SDC data path	Layer-2 connectivity, MTU=9216
152	-	PowerFlex data 2	For SDS-to-SDC data path	Layer-2 connectivity, MTU=9216
153	-	PowerFlex data 3 (if required)	For SDS-to-SDC data path	Layer-2 connectivity, MTU=9216
154	-	PowerFlex data 4 (if required)	For SDS-to-SDC data path	Layer-2 connectivity, MTU=9216
250	-	NAS file management	For NAS management traffic	Layer-3 connectivity, MTU=1500/9216
251	-	NAS file data 1	For accessing PowerFlex file data from client	Layer-2/layer-3, MTU=1500/9000
252	-	NAS file data 2	For accessing PowerFlex file data from client	Layer-2/layer-3, MTU=1500/9000

Network requirements for NSX (optional)

Example VLAN	Example multi-VLAN	Network Name	Description	Properties
101	210-224	Hardware management	For connection to NSX node iDRAC interface	Layer-2/Layer-3 connectivity, MTU=1500/9216
105	240-254	Hypervisor management	For VMware ESXi management interface on NSX Edge cluster (Shared with production vSphere cluster)	Layer-3 connectivity, MTU=1500/9216
114	-	nsx-vsan (only if required)	For VMware vSAN interface on NSX Edge cluster (This is optional meaning only if customer chooses to deploy vSAN on NSX Edge cluster)	Layer-2 connectivity, MTU=9216
116	450-464	nsx-vmotion	For NSX vMotion on NSX Edge cluster	Layer-2/Layer-3 connectivity, MTU=1500/9216
121	-	nsx-transport	For NSX Transport interface on NSX Edge cluster (Used for NSX overlay)	Layer-2 connectivity, MTU=9216
122	-	nsx-edge1	For NSX Edge external VLAN1 used for BGP uplink	Layer-3 connectivity, MTU=1500
123	-	nsx-edge2	For NSX Edge external VLAN2 used for BGP uplink	Layer-3 connectivity, MTU=1500

Example VLAN	Example multi-VLAN	Network Name	Description	Properties
130	-	nsx-gateway	For NSX Gateway VM on NSX Edge node	Layer-3 connectivity, MTU=1500/9216

Verify the network configuration

Use this procedure to verify configuration before adding a VLAN to the network.

Steps

1. Verify that the Virtual Port Channel (vPC) / Virtual Link Tunneling (VLT) is available between the access switches:
 - a. For Cisco Nexus switches, type **show vpc brief**.
 - b. For Dell PowerSwitch switches, type **show vlt brief**.
2. To verify the port channel between servers, hosts, and access switches are configured, type **show port-channel summary**.
3. To verify the port channel between customer network switches and access switches are configured, type **show port-channel summary**.
4. To verify that the VLAN is created and enabled on the port channel between the network switches and the access switches, type **show vlan**.
5. To verify that SVI is configured on the network switches, type **show ip int brief**.
6. To verify that you have the VLAN IP address, mask, and gateway to verify the VLAN configuration, type **show vlans**.

Add a VLAN to the network

To enable VLANs on the network backbone, you must manually configure the switches.

About this task

When we add new VLANs to the system, PowerFlex Manager configures the server facing port configurations. You must do the switches manually.

i **NOTE:** If multi-VLAN or multi-subnet is enabled, each network may have multiple VLANs except for data networks. For a multi-VLAN or a multi-subnet configuration, include all the associated VLANs in the **<vlan-list>** variable.

Steps

1. To configure access switches in an access-aggregation configuration:

i **NOTE:** This is applicable for Cisco Nexus and Dell PowerSwitch switches.

- a. Type the following to define the new VLAN on the switch:

```
vlan <VLAN ID> # applicable for a standard configuration
vlan <multi-VLAN ID> # applicable for a multi-vlan configuration
interface vlan <VLAN ID>
no shutdown
```

- b. Type the following to add the VLAN to the uplink connected to the aggregation switch:

```
interface port-channel 1900
Description "Uplink Port Channel from Access Switch to AGG-SWITCH"
switchport trunk allowed vlan add <vlan-list>
```

- c. Type the following to add the VLAN to the peer-link:

```
interface port-channel 100
description "virtual port-channel vpc-peer-link"
switchport trunk allowed vlan add <vlan-list>
```

2. To configure aggregation switches in an access-aggregation configuration:

- a. Type the following to define the new VLAN on the switch:

```
vlan <VLAN ID> # applicable for a standard configuration
vlan <multi-VLAN ID> # applicable for a multi-vlan configuration
name <vlan name>
no shutdown
```

- b. Type the following to add the VLAN to the uplink connected to the aggregation switch:

```
interface port-channel 1900
Description "Downlink from AGG-SWITCH" to Access Switch
switchport trunk allowed vlan add <vlan-list>
```

- c. Type the following to add the VLAN to the peer-link:

```
interface port-channel 100
description "virtual port-channel vpc-peer-link"
switchport trunk allowed vlan add <vlan-list>
```

- d. Type the following to add the new VLAN to the customer connected link (only required if the VLAN is an Layer-2 VLAN):

```
interface port-channel <900>
Description "Connection to Customer Network"
switchport trunk allowed vlan add <vlan-list>
```

- e. Type the following if it is a routed VLAN:

```
interface vlan <x>
ip address <ip address>
ip address <ip address> secondary # repeat for each subnet enabled within a vlan.
Only applicable if multi-subnet is enabled for any network-type
hsrp version 2
hsrp <number> # repeat for each subnet belonging to the same vlan
authentication text <password>
preempt
priority 110
ip <virtual ip>
```

3. To configure leaf/border leaf switches in a leaf-spine configuration:

NOTE: For PowerFlex management controller 2.0, repeat this section for all multi-VLANs configured on leaf switches where the PowerFlex controller nodes are connected.

- a. Type the following to define the new VLAN on the switch:

For...	Do this...
Cisco Nexus switches	<pre>vlan <vlan number> name <vlan name> no shutdown</pre>
Dell PowerSwitch switches	<pre>interface vlan <vlan number> name <vlan name> no shutdown</pre>

- b. Type the following to define VLAN to VXLAN mapping:

```
vlan <vlan number>
name <vlan name>
vn-segment <vxlan number>

interface nve1
source-interface hold-down-time 180
member vni <vxlan number>
suppress-arp
ingress-replication protocol bgp
```

- c. Type the following if it is a routed VLAN:

```
interface Vlan<vlan number>
vrf member <vrf name>
fabric forwarding mode anycast-gateway
carrier-delay msec 100
ip address <distributed gw ip address>
ip address <distributed gw ip address> secondary # repeat for each subnet enabled
within a vlan. Only applicable if multi-subnet is enabled for any network-type
no shutdown
```

- d. Type the following if the VLAN is an Layer-2 VLAN:

```
evpn
vni <vxlan number> 12
rd auto
route-target import auto
route-target export auto
```

Add a network to a resource group

You can add an available network to a resource group or choose to define a new network for a configuration that was initially deployed outside of PowerFlex Manager. You cannot remove an added network using PowerFlex Manager.

About this task

Before you can add a network to a service, define the network.

You can add a static route to allow nodes to communicate across different networks. The static route can also be used to support replication in storage-only and hyperconverged services.

Prerequisites

Ensure that a new VLAN is created on any switches that need access to that VLAN and is added to any management cluster server-facing ports. The VLAN is then added it to any northbound trunks to other switches that it must communicate with.

Steps

1. Log in to PowerFlex Manager.
2. On the menu bar, click **Lifecycle > Resource Group**.
3. From the **Resource Group Details** page, click **Add Resources**, and select **Add Network**.
4. Click **Add Additional Network** to add an additional network and click **Continue** or to add an additional static route, go to the next step.

For a multi-VLAN or multi-subnet configuration, consider additional networks only for the following network traffic:

- Hypervisor management
- Hypervisor migration
- PowerFlex management
- PowerFlex replication
- General purpose VLAN (visible only for PowerFlex storage-only nodes)

5. Click **Add Additional Static Route** and perform the following to add static routes:

- a. Click **Add New Static Route**.
- b. Select a **Source Network (Data)**.

The source network must be a PowerFlex data network or a replication network.

- c. Select a **Destination Network (Rep)**.

The destination network must be a PowerFlex data network or a replication network.

- d. Type the IP address for the **Gateway**.
- e. Repeat steps 5a through 5d for additional static routes required.
- f. Click **Save**.

Registering and configuring Cisco Nexus switches on the Cisco Smart Account portal

Cisco requires customers to register their switches on the Cisco Smart Account portal to monitor the licensing.

The following Cisco Smart Account changes are required:

- Registration - The Cisco Nexus switches must be registered on the Cisco Smart Account portal. The registration must be done by the customer or customer's Smart Account administrator. Customer or customer licensing administrator must register for a Cisco Smart Account if not already registered for an account. See [Cisco Software Licensing Guide](#) and [Cisco Create a new Smart Account](#) for more information.
- Licensing - Switches using routing protocols (Layer-3) require either a term based or perpetual based license. Layer-2 switches do not require a license.

Registering and configuring Cisco Nexus switches on the Cisco Smart Account portal is applicable for all switches except management and access switches.

The following Cisco Smart Account communication methods are supported on Cisco NX-OS 10.x or higher. To upgrade Cisco Nexus switches from NX-OS 9.3.x to NX-OS 10.x, see *PowerFlex Rack with PowerFlex 4.x Upgrade Guide*. These communication methods are available to register the Cisco Nexus switches and configure the Cisco Smart Account communication on the Cisco Smart Account portal:

Cisco Smart Account communication method	Purpose
Offline	<p>Use this method to register the Cisco Nexus switches with no direct connectivity to the Cisco Smart Account portal. Commands are run at the factory to generate a report per switch. The report is manually transferred to the customer.</p> <p>Customer uploads these reports to the Cisco Smart Account portal and receives a corresponding ACK file. Customer provides these ACK files to the Dell Technologies Services to import these ACK files into the switch configuration.</p>
Internet	<p>After Dell Technologies Services completes the offline switch registration with customer Cisco Smart Account, customer can modify the Smart Account communication in the Logical Configuration Survey.</p> <p>Use this method when the customer has no security issues with using Internet for future communication between the switch and Smart Account portal. This type of connectivity can only be configured at the customer location. This method enables communication with the Cisco Smart Account without any type of intervention by Dell Technologies Services.</p>
Internet with proxy server	<p>After Dell Technologies Services completes the offline switch registration with customer Cisco Smart Account, customer can modify the Smart Account communication in the Logical Configuration Survey.</p> <p>Use this method for customer switches to use the customer proxy server to communicate with the Cisco Smart Account portal through the Internet. This type of connectivity can only be configured at the customer location.</p>
On-premises Cisco Smart License Utility	<p>After Dell Technologies Services completes the offline switch registration with customer Cisco Smart Account, customer can modify the Smart Account communication in the Logical Configuration Survey.</p>

Cisco Smart Account communication method	Purpose
	Use this method to configure the Cisco Smart Account using Cisco Smart License Utility. After the customer has deployed the Cisco Smart License Utility, the customer must use the Cisco Smart License Utility to co-ordinate the communication from switch to the Cisco Smart Account. The Cisco Smart License Utility can either be connected to Internet or used offline.

Configure Cisco Smart Account communication using Internet

Use this procedure to configure the Cisco Smart Account communication using Internet.

About this task

Use this method when the customer has no security issues with using Internet for future communication between the switch and Cisco Smart Account portal. The configuration of Cisco Smart Account communication through Internet can only be configured at the customer location. This method enables communication with Cisco Smart Account without any type of intervention by Dell Technologies Services. After Dell Technologies Services completes the offline switch registration with customer Cisco Smart Account, customer can change the Smart Account communication method in the *Logical Configuration Survey* (LCS).


Prerequisites

Verify the Cisco Nexus switches are registered on the Cisco Smart Account portal.

Steps

Use the Cisco NX-OS switch CLI and type the following to change the Smart Account communication method from offline to online:

```
license smart transport smart
exit
copy running-config startup-config
```

 **NOTE:** Switch has access to Internet and DNS server to resolve to `smartreceiver.cisco.com`.

Related information

[Configure Cisco Smart Account communication using the customer proxy server with Internet](#)

Configure Cisco Smart Account communication using the customer proxy server with Internet

Use this procedure to configure the customer switches communicating with Cisco Smart Account portal across the Internet using customer proxy server.

About this task

The configuration of Cisco Smart Account communication through Internet using the customer proxy server can only be configured at the customer location. Future communication with Cisco Smart Account can occur without any type of intervention by Dell Technologies Services. The switches are configured in the factory using the offline method. After the Dell Technologies Services has completed the switch registration with customer Cisco Smart Account, the customer can change the Logical Configuration Survey (LCS) Smart Account communication method from offline to online.

Prerequisites

Verify that Cisco Nexus switches are registered on the Cisco Smart Account portal.

Steps

Use the Cisco NX-OS switch CLI and type the following to change the Smart Account communication method from offline to online:

```
license smart transport smart
license smart proxy <ip address> port <port number>
license smart url smart https://smartreceiver.cisco.com/licservice/license
copy running-config startup-config
```

 **NOTE:** The switch has access to Internet using the customer proxy server IP address or DNS, proxy server port number, and DNS server to resolve to smartreceiver.cisco.com.

Related information

[Configure Cisco Smart Account communication using Internet](#)

Configure Cisco Smart Account communication using the on-premises Cisco Smart License Utility without Internet

Use this procedure to configure the Cisco Smart Account communication using the on-premises Cisco Smart License Utility without Internet.

About this task

Cisco Smart License Utility must be deployed at the customer location. In this case, the customer must use the Cisco Smart License Utility to coordinate the communication between the switch to the Cisco Smart Account. After Dell Technologies Services has completed the switch registration with customer Cisco Smart Account, the customer can use this method to change the Logical Configuration Survey (LCS) Smart Account communication method from offline to online.

Prerequisites

Ensure the following:

- Cisco Smart License Utility must be deployed at the customer location.
- Verify that Cisco Nexus switches are registered on the Cisco Smart Account portal.

Steps

Use the Cisco NX-OS switch CLI and type the following to change the Smart Account communication method from offline to online

```
license smart transport cslu
license smart url cslu http://<cslu ip address>:8182/cslu/v1/pi
exit
copy running-config startup-config
```

 **NOTE:** The switch has access to the Cisco Smart License Utility IP address or DNS and port 8182.

Configuring networking

Adding the details of an existing network enables PowerFlex Manager to automatically configure nodes that are connected to the network.

Define a network

Use this procedure to define a network.

Prerequisites

When defining the PowerFlex management controller management network, ensure the following is met:

- Use PowerFlex Manager to deploy CloudLink and policy manager.
- Deploy a compute service in a multi-VLAN or multi-subnet or customer option in a standard single network build.

Steps

1. On the menu bar, click **Settings > Networking** and click **Networks**.
2. Click **Define**.
3. In the **Name** field, enter the name of the network. Optionally, in the **Description** field, enter a description for the network.
4. From the **Network Type** drop-down, select one of the following network types:
 - General purpose LAN
 - Hypervisor management (supports multi-VLAN or multi-subnet configurations)
 - Hypervisor migration (supports multi-VLAN or multi-subnet configurations)
 - Hardware management
 - PowerFlex data
 - PowerFlex data (client traffic only)
 - PowerFlex data (server traffic only)
 - PowerFlex replication (supports multi-VLAN or multi-subnet configurations)
 - PowerFlex management (supports multi-VLAN or multi-subnet configurations)
 - NAS file management
 - NAS file data

NOTE:

- For a PowerFlex configuration that uses a hyperconverged architecture with two/four data networks, you typically have two or four networks that are defined with the PowerFlex data network type.
- The PowerFlex data network type supports both client and server communications and used with hyperconverged resource groups.
- For a PowerFlex configuration that uses a two-layer architecture with four dedicated data networks, you typically have two PowerFlex (client-traffic only) VLANs and two PowerFlex data (server-traffic only) VLANs. These network types are used with storage-only and compute-only resource groups
- For a multi-VLAN or multi-subnet configuration, include adding additional networks only for the following network traffic:
 - Hypervisor management
 - Hypervisor migration
 - PowerFlex management
 - PowerFlex replication

5. In the VLAN ID field, enter a VLAN ID between 1 and 4094.



NOTE: PowerFlex Manager uses the VLAN ID to configure I/O modules to enable network traffic to flow from the node to configured networks during deployment.

6. Optionally, select the **Configure Static IP Address Ranges** check box, and do the following:
 - a. In the **Subnet** box, enter the IP address for the subnet. The subnet is used to support static routes for data and replication networks.

- b. In the **Subnet Mask** box, enter the subnet mask.
- c. In the **Gateway** box, enter the default gateway IP address for routing network traffic.
- d. Optionally, in the **Primary DNS** and **Secondary DNS** fields, enter the IP addresses of primary DNS and secondary DNS.
- e. Optionally, in the DNS Suffix field, enter the DNS suffix to append for hostname resolution.
- f. To add an IP address range, click **Add IP Address Range**. In the row, indicate the role in PowerFlex nodes for the IP address range and then specify a starting and ending IP address for the range. For the role, select either:
 - **Server or Client**: Default; range is assigned to the server and client roles.
 - **Client Only**: Range is assigned to the client role on PowerFlex hyperconverged nodes and PowerFlex compute-only nodes.
 - **Server Only**: Range is assigned to the server role on PowerFlex hyperconverged nodes and PowerFlex storage-only nodes.

You can add the virtual IP address value to **Server or Client** and **Server Only**.

NOTE: Do not add the PowerFlex replication networks and data networks gateway to this network.

NOTE: The **Configure Static IP Address Ranges** check box is not available for all network types. For example, you cannot configure a static IP address range for the operating system Installation network type. You cannot select or clear this check box to configure static IP address pools after a network is created.

7. Click **Save**.
8. If replicating the network, repeat steps 1 through 7 to add the remote replication networks.

Add a new interface

Use the **Add New Interface** feature to create a network interface to match to a network card on a node when deploying a template.

PowerFlex Manager supports a network layout for hyperconverged, compute-only, and storage-only deployments. This network layout allows you to use trunk ports and port channels for data networks, instead of access ports. In this type of configuration, both data networks are on both NICs, teamed or bonded together in the operating system. For a hyperconverged or compute-only deployment, the first port on both interfaces is for trunk traffic, whereas the second port is for data 1 and data 2. For a storage-only deployment, the first port is for trunk traffic and data 1, whereas the second port is for data 2. PowerFlex Manager still supports the legacy network layout, but the sample templates use the new configuration.

1. On the node component page, under **Network Settings**, click **Add New Interface**.
2. Enter the following information for the new interface:
 - **Port Layout**—Select the NIC type from the list.

For a VMware ESXi deployment with a Mellanox card, you must select the two port, 25-gigabit NIC type.

The second interface ports 1 and 2 are automatically replicated to the first interface. This replication applies to sample templates as well. If you manually create a template from scratch and choose the networks for the interfaces, the second interface's port 1 and 2 are not automatically replicated to the first interface.
3. Enter the network VLANs for each port.
 - a. Click **Choose Networks** for a port.
 - b. To add one or more networks to the port, select **Add Networks to this Port**, then click the check box for each network you want to add from the **Available Networks** list. Alternatively, click the check box in the upper left corner next to the **Name** label to select all the available networks.


If you want to filter the list by network type, select a **Network Type**, then enter a name or VLAN ID to search.

Click **>>** to move the selected items to the **Selected Networks** list on the right.

 - c. To mirror network settings from another port for which you have already chosen the network VLANs, select **Mirror this Port with Another Port**. Then, select the other interface and port from which you want to mirror this port.
 - d. Click **Save**.
4. To view the list of nodes that match the network configuration parameters, click **Validate Settings**.

The list of nodes is filtered according to the target boot device and NIC type settings specified.

When you enable PowerFlex settings for the node, the **Validate Settings** page filters the list of nodes according to the supported storage types (NVMe, All flash, and HDD). Within the section for each storage type, the nodes are also sorted by health, with the healthy (green) nodes displayed first and the critical (red) nodes displayed last.

 **NOTE:** If you select the same network on multiple interface ports or partitions, PowerFlex Manager creates a team or bond on systems with the VMware ESXi operating system. This configuration enables redundancy.

Edit a network

If a network is not associated with a template or resource group, you can edit the network name, the VLAN ID, or the IP address range.

Steps

1. On the menu bar, click **Settings > Networking** and click **Networks**.
2. Select the network that you want to modify, and click **Modify**.
3. Edit the information in any of the following fields: **Name, VLAN ID, IP Address Range**.
For a PowerFlex data or replication network, you can specify a subnet IP address for a static route configuration. The subnet is used to support static routes for data and replication networks.
4. Click **Save**.

Delete a network

You cannot delete a network that is associated with a template or resource group.

Steps

1. On the menu bar, click **Settings > Networking** and click **Networks**.
2. Click the network that you want to delete, and click **Delete**.
3. Click **Yes** when the confirmation message is displayed.

View port details

Use this procedure to view the port details.

About this task

Port View is only available for PowerFlex nodes and is not available for management VMs such as, CloudLink Center, PowerFlex gateway, VMware vCSA, and switches.

Steps

1. Log in to PowerFlex Manager.
2. From the menu, click the **Resources** tab.
3. From the **Resources** tab, select a resource and click **View Details**.
4. Click **Port View**.

Add the VMware NSX service using PowerFlex Manager

Use this procedure only if the PowerFlex nodes are added to the NSX environment.

Prerequisites

- Before adding this service in PowerFlex Manager, verify that the NSX data center is configured on the PowerFlex hyperconverged or compute-only nodes.
- Ensure that the iDRAC of nodes, vCenter, and switches (applicable for full networking) are discovered in PowerFlex Manager.
- After adding an NSX node, if you are using PowerFlex Manager, run **Update Service Details** to represent the appropriate environment. If you are using VMware NSX in a PowerFlex Manager service, the service goes into lifecycle mode.

Steps


1. Log in to PowerFlex Manager.
2. From **Getting Started**, click **Define Networks**.
 - a. Click **Define** and do the following:

NSX information	Values
Name	Type NSX-T Transport
Description	Type Used for east-west traffic
Network Type	Select General Purpose LAN
VLAN ID	Type 121

- b. Click **Save > Close**.
3. Remove the hyperconverged or compute-only service:
 - a. On the menu bar, click **Lifecycle > Resource Groups**.
 - b. Click **HC or CO Service**.
 - c. Click **More Actions > Remove Resource Group**.
 - d. Select **Remove Resource Group** from the drop-down under **Resource Group removal type**.
 - e. On the **Remove Resource Group** page, select **Leave nodes in PowerFlex Manager inventory and set state to Managed**.
 - f. Click **Remove** to remove the service.
 4. From **Getting Started**, click **Add Existing Service** and do the following:
 - a. On the **Welcome** page, click **Next**.
 - b. On the **Service Information** page, enter the following details:

Service information	Details
Name	Type NSX-T Service
Description	Type Transport Nodes
Type	Type Hyperconverged Compute-only
Firmware and software compliance	Select the Release Certification Matrix (RCM) version
Who should have access to the service deployed from this template?	Leave as default

- c. Click **Next**.
- d. On the **Network Information** page, select **Full Network Automation/Partial Network Automation**, and click **Next**.

 **NOTE:** For partial network automation, you must finish the complete network configuration required for NSX. Consider the configuration given in this document as a reference.

- e. On the **Cluster Information** page, enter the following details:

Cluster information	Details
Target virtual machine manager	Select VCSA name
Data center name	Select data center name
Cluster name	Select cluster name
Target PowerFlex gateway	Select PowerFlex gateway name
Target protection domain	Select PD-1
OS image	Select the ESXi image

- f. Click **Next**.
- g. On the **OS Credentials** page, select the OS credentials for each node, and click **Next**.
- h. On the **Inventory Summary** page, review the summary and click **Next**.
- i. On the **Networking Mapping** page, verify that the networks are aligned with the correct dvswitch.
- j. On the **Summary** page, review the summary and click **Finish**.
5. Verify that PowerFlex Manager recognizes that NSX is configured on the nodes:
- Click **Services**.
 - Select the hyperconverged or compute-only service.
 - Verify that a banner appears under the **Service Details** tab, notifying that NSX-T is configured on a node and is preventing some features from being used. If you do not see this banner, check if you have selected the wrong service or NSX is not configured on the PowerFlex hyperconverged or compute-only nodes.

Storage management

Protection domains

A protection domain is a set of SDSs configured in separate logical groups. It may also contain SDTs and SDRs. These logical groups allow you to physically and/or logically isolate specific data sets and performance capabilities within specified protection domains and limit the effect of any specific device failure. You can add, modify, activate, inactivate, or remove a protection domain in the PowerFlex system.

Add protection domains

A protection domain is a set of SDSs, with (optionally) SDTs and SDRs, configured in separate logical groups. You can add protection domains to a PowerFlex system.

Steps

1. On the menu bar, click **Block > Protection Domains**.
2. Click **+Create Protection Domain**.
3. In the **Create Protection Domain** dialog box, enter the name of the protection domain and click **Create**.
4. Verify that the operation has finished successfully, and click **Dismiss**.

Results


You can now add SDSs, fault sets, storage pools, and acceleration pools to the protection domain. Replication can also be set up to ensure the data is protected and saved to a remote cluster.

Configure network throttling

Configure network throttling to control the flow of traffic over the network.

About this task

Network throttling is configured separately for each protection domain. The SDS nodes transfer data between themselves. This data consists of user data being replicated as part of the RAID protection, and data copied for internal rebalancing and recovery from failures. You can modify the balance between these types of data loads by limiting the data copy bandwidth. This change affects all SDSs in the specified protection domain.

 **NOTE:** These features affect system performance, and should only be configured by an advanced user. Contact Dell Technologies Support before you change this configuration.

Steps

1. On the menu bar, click **Block > Protection Domains**.
2. In the list of protection domains, select the relevant protection domain check box, and click **Modify > Network Throttling**.
3. In the **Set Network Throttling for PD** dialog box, enter the bandwidth for the following settings, or select **Unlimited** to allow for unlimited throughput for that setting:
 - **Rebalance throughput limit per SDS**
 - **Rebuild throughput limit per SDS**
 - **vTree migration throughput limit per SDS**
 - **Overall throughput limit per SDS**
4. Click **Apply**.

5. Verify that the operation has finished successfully, and click **Dismiss**.

Activate a protection domain

Activate the protection domain to enable access to data.


Steps

1. On the menu bar, click **Block > Protection Domains**.
2. In the list of protection domains, select the relevant protection domain, and click **More Actions > Activate**.
3. In the **Activate Protection Domain** dialog box, click **Yes** for **Force activate** and then click **Activate** to enable access to the data on the protection domain.
4. Verify that the operation has finished successfully, and click **Dismiss**.

Inactivate a protection domain

Use this procedure for a graceful system shutdown.

About this task

 **NOTE:** When you inactivate a protection domain, the data remains on the SDSs. It is therefore preferable to remove a protection domain if you no longer need it.

While a protection domain is inactivated, the following activities can take place behind the scenes:

- Determine if there are any current rebuild/rebalance activities taking place. If so, the shutdown will be delayed (unless it is forced) until they are finished.
- Block future rebuild/rebalance activities.
- Temporarily disable application I/O and disable access to volumes.
- Move the DRL mode of all SDSs to harden, in preparation for restarting the server.
- Reload of all SDSs before re-enabling data access.

Steps

1. On the menu bar, click **Block > Protection Domains**.
2. In the list of protection domains, select the relevant protection domain, and click **More Actions > Inactivate**.
3. In the **Inactivate Protection Domain**, enter the user password, and click **Inactivate**.
4. Verify that the operation has finished successfully, and click **Dismiss**.

Remove a protection domain

Remove a protection domain from the PowerFlex system.

Prerequisites

Ensure that all SDSs, storage pools, acceleration pools, and fault sets have been removed from the protection domain before removing it from the system.

Steps

1. On the menu bar, click **Block > Protection Domains**.
2. In the list of protection domains, select the relevant protection domain and click **More Actions > Delete**.
3. In the **Delete Protection Domain**, click **Delete**.
4. Verify that the operation has finished successfully, and click **Dismiss**.

Fault sets

Fault sets are logical entities that contain a group of SDSs within a protection domain. A fault set can be defined for a set of servers that are likely to fail together, for example, an entire rack full of servers. PowerFlex maintains mirrors of all chunks within a fault set on SDSs that are outside of this fault set so that data availability is assured even if all the servers within one fault set fail simultaneously.

Add fault sets

Add a fault set to a protection domain to prevent data loss in case of a single failure.

About this task

You must adhere to the following process for creating fault sets:

1. Ensure that a protection domain exists, or add a new one.
2. Ensure that a storage pool and fault sets (with a minimum of three fault units) exist, or add new ones.
3. Add the SDS and designate the protection domain and fault set. At the same time, add the SDS devices into a storage pool.

If you use the automated deployment and installation tools, they follow this order automatically.

You can only create and configure fault sets before adding SDSs to the system. Configuring fault sets incorrectly may prevent the creation of volumes. An SDS can only be added to a fault set during the creation of the SDS.

Steps

1. On the menu bar, click **Block > Fault Sets**.
2. In the right pane, click **+Create Fault Set**.
3. In the **Create Fault Set** dialog box, enter a name and select the protection domain, and click **Create**.
4. Verify that the operation has finished and was successful, and then click **Dismiss**.
The new fault set is a part of the protection domain.

Place a fault set in maintenance mode

Place a fault set into maintenance mode in order to perform non-disruptive maintenance on the group of storage data servers (SDSs).

Steps

1. On the menu bar, click **Block > Fault Sets**.
2. In the list of fault sets, select the relevant fault set check box and click **More Actions > Enter Maintenance Mode**.
3. In the **Enter Fault Set to Maintenance Mode** dialog box, select one of the following maintenance mode options:
 - **Instant** — a node is temporarily removed without building a new copy of the data. During maintenance, the system only mirrors new writes. After maintenance is complete, the system applies the new writes to the node that was under maintenance.
 - **Protected** — a third copy is created before entering maintenance mode. This ensures that if there is a node failure where the second copy of SDS is required, there is still a full backup of the SDS. This leaves no room for discrepancy between the copies. More storage capacity from the node is required.
4. Click **Enter Maintenance Mode**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.
6. Optionally, at the top right side of the toolbar, click the **Running Storage Jobs** icon to check maintenance mode status.

Exit fault set from maintenance mode

Once you have finished performing maintenance tasks, you must manually remove the fault set from maintenance mode.

About this task

Once you have finished performing maintenance tasks on the fault set, you must manually remove maintenance mode to return to normal production.

Steps

1. On the menu bar, click **Block > Fault Sets**.
2. In the list of fault sets, select the relevant fault set check box and click **More Actions > Exit Maintenance Mode**.
3. In the **Exit Fault Set from Maintenance Mode** dialog box, click **Exit Maintenance Mode**.
4. Verify that the operation has finished and was successful, and then click **Dismiss**.

Cancel protected maintenance mode for fault set

When entering protected maintenance mode, a third copy of the SDS is created, which can take a long time. You can back out of this process before entering protected maintenance mode is complete, such as when there is insufficient capacity to create the third copy.

Steps

1. On the menu bar, click **Block > Fault Sets**.
2. In the list of fault sets, select the relevant fault set check box and click **More Actions > Abort Enter Protected Maintenance Mode**.
3. In the **Abort Enter Maintenance Mode** dialog box, click **Abort**.
4. Verify that the operation has finished and was successful, and then click **Dismiss**.

Delete fault sets

Use the following procedure to delete and verify that the desired fault set is deleted.

Prerequisites

Ensure that any configured SDSs have been removed from the fault set that is to be deleted.

Steps

1. On the menu bar, click **Block > Fault Sets**.
2. From the list of fault sets, select the fault set that you want to delete.
3. Select **More Actions > Delete**.
4. In the **Delete Fault Set** dialog box, verify that the desired fault set will be deleted, and click **Delete > Dismiss**.

Storage data servers

The storage data server (SDS) manages the capacity of a single server and acts as a back-end for data access. The SDS is installed on all servers contributing storage devices to PowerFlex. These devices are accessed through the SDS.

SDSs and their devices can be added to a system one by one or in bulk operations. Up to eight IP addresses can be associated with each SDS. You can associate different types of cache with SDSs. SDSs can be entered into maintenance mode to perform maintenance operations on the PowerFlex system.

Add storage data servers

Add storage data servers to the PowerFlex system.

Prerequisites


- Ensure that at least one suitable storage pool is defined in the required protection domain.
- All devices in a storage pool must be the same media type. Ensure that you know the type of devices you are adding to the system.
- Ensure that the storage pool to which you are adding devices is configured to receive that media type.
- If you want to add acceleration devices now, ensure that at least one acceleration pool is defined.

About this task


Device data is erased when devices are added to an SDS. When adding a device to an SDS, PowerFlex checks that the device is clear before adding it. If the device is not clear, an error is returned. A device that has been used in the past can be added to the SDS by using the `Force Device Takeover` option. When this option is used, any data that was previously saved on the device is erased.

You can assign a name to the SDS, as well as to the devices. This name can assist in future object identification. This can be particularly helpful for SDS devices, because the names remain constant, even if the path changes. SDS and device names must meet the following requirements:

- Contains less than 32 characters
- Contains only alphanumeric and punctuation characters
- Is unique within the object type

 **NOTE:** Devices can be tested before going online. Various testing options are available the **Advanced** area of the window (default: **Test and Activate**).

 **NOTE:** Acceleration settings can be configured later from the **Block > Acceleration Pools** page.

 **NOTE:** You cannot enable zero padding after adding the devices.

Steps

1. On the menu bar, click **Block > SDSs**.
2. Click **+ Add SDS**.
3. Configure the following settings:
 - Enter SDS name
 - Select a protection domain
 - Select a fault set
 - Enter SDS port used for communication
 - Enter the IP address for SDC, SDS or both and click **Add IP**.
4. For additional IP addresses, enter the IP address, select the communication role and click **Add IP**.
5. Expand **Advanced** for more options. Configure the following options (for advanced users):
 - To enable RMcache, select **Use Read RAM Cache** and enter the size in MB.
 - Click one of the options for **Performance Profile**: Compact or High.
 - To force clean a node, select **Force Clean SDS**.
6. Click **Add SDS**.

Results

An SDS is added to the system.

Configure RMcachel

RMcache uses RAM that is allocated for caching. Its size is limited to the amount of allocated RAM. By default, RMcachel caching is disabled.

Prerequisites

- Enable RMcachel at the storage pool level for all of the SDSs in the storage pool.
- RMcachel must also be enabled at the SDS level.

About this task

For a read to be stored in the RAM of a specific SDS, the RMcachel feature on that SDS must be enabled, and the relevant storage pool and the relevant volume must both be configured to use RMcachel. Caching only begins after one or more devices are added to the SDS. The amount of RAM that you may allocate for RMcachel is limited and can never be the maximum available RAM.

Enabling RMcachel at the storage pool level allows you to control the cache settings for all SDSs in the storage pool. You can enable RAM caching for a storage pool and then disable caching on one or more SDSs individually.

 **NOTE:** Only I/Os that are multiples of 4k bytes can be cached.

Steps

1. On the menu bar, click **Block > SDSs**.
2. In the list of SDSs, select the relevant SDS, and click **Modify > Cache Settings**.
3. In the **SDS Cache Settings** dialog box, select **Enable Read RMcachel**. Enter the RMcachel cache size.
The minimum RMcachel cache size is 128 MB.
4. Click **Apply**.

Remove SDSs

Remove SDSs and devices gracefully from a system. The removal of some objects in the system can take a long time, because removal may require data to be moved to other storage devices in the system.

About this task

If you plan to replace a device with a device containing less storage capacity, you can configure the device to a smaller capacity than its actual capacity, in preparation for replacement. This will reduce rebuild and rebalance operations in the system later on.

The system has job queues for operations that take a long time to execute. You can view jobs by clicking the **Running Storage Jobs** icon on the right side of the toolbar. Operations that are waiting in the job queue are shown as Pending. If a job in the queue will take a long time, and you do not want to wait, you can cancel the operation using the **Abort** button in the **Remove** command window (if you left it open), or using the `Abort entering Protected Maintenance Mode` command from the **More Actions** menu.

 **CAUTION:** The **Remove** command deletes the specified objects from the system. Use the **Remove** command with caution.

Steps

1. On the menu bar, click **Block > SDSs**.
2. In the right pane, select the relevant SDS check box and click **More Actions > Remove**.
3. In the **Remove SDS** dialog box, click **Remove**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Place storage data server in maintenance mode

Place an storage data server in maintenance mode to perform non-disruptive maintenance on the storage data server.

Steps

1. On the menu bar, click **Block > SDSs**.
2. In the list of storage data servers, select the relevant storage data server and click **More Actions > Enter Maintenance Mode**.
3. In the **Enter SDS into Maintenance Mode** dialog box, select one of the following options:
 - **Instant** — a node is temporarily removed without building a new copy of the data. During maintenance, the system only mirrors new writes. After maintenance is complete, the system applies the new writes to the node that was under maintenance.
 - **Protected** — a third copy is created before entering maintenance mode. This ensures that if there is a node failure where the second copy of storage data server is required, there is still a full backup of the storage data server. This leaves no room for discrepancy between the copies. More storage capacity from the node is required.
4. Click **Enter Maintenance Mode**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.
6. Optionally, at the top right side of the toolbar, click the **Running Storage Jobs** icon to check maintenance mode status.

Exit storage data server from maintenance mode

After completing maintenance tasks, remove the storage data server from maintenance mode.

About this task

Once you have finished performing maintenance tasks on the storage data server, you can manually exit maintenance mode and return the storage data server to normal production.

Steps

1. On the menu bar, click **Block > SDSs**.
2. In the list of storage data servers, select the relevant storage data server and click **More Actions > Exit Maintenance Mode**.
3. In the **Exit SDS from Maintenance Mode** dialog box, click **Exit Maintenance Mode**.
4. Verify that the operation has finished successfully, and click **Dismiss**.

Results

After the operation has been completed successfully, the storage data server returns to normal operation, and data deltas collected on other storage data servers during the maintenance period are copied back to the storage data server.

Cancel entering protected maintenance mode for SDS

When entering protected maintenance mode, a third copy of the SDS is created, which can take a long time. You can back out of this process before entering PMM is complete, such as when there is insufficient capacity to create the third copy.

Steps

1. On the menu bar, click **Block > SDSs**.
2. In the list of SDSs, select the relevant fault set check box and click **More Actions > Abort entering Protected Maintenance Mode**.
3. In the **Abort entering Maintenance Mode** dialog box, click **Abort**.
4. Verify that the operation has finished successfully, and then click **Dismiss**.

Add storage devices

Add storage devices to the PowerFlex system one by one, or in bulk operations. By default, performance tests are performed on the added devices and the results are saved in the system.


Prerequisites

Ensure that at least one suitable storage pool is defined in the required protection domain.

All devices in a storage pool must be the same media type. Ensure that you know the type of devices that you are adding to the system, and that the storage pool to which you are adding devices is configured to receive that media type.

Steps

1. On the menu bar, click **Block > SDSs**.
2. Select the relevant SDS from the SDS list.
3. Click **Add Device > Storage Device**.
4. In the **Add Storage Device to SDS** dialog box, enter the following required parameters for the storage device:
 - a. Device path
The length of the device path must not exceed 63 characters.
For example, this path for an NVMe drive is not supported because it is too long:
`/dev/disk/by-id/Dell_Express_Flash_NVMe_PM1725_1.6TB_SFF_____S2JPNA0J500141`
Alternatively, this equivalent name is supported: `/dev/disk/by-id/nvme-eui.002538957100082e`
 - b. Name of the device
Assigning a name to a storage device can be particularly helpful for identifying devices in the future because the name remains constant, even if the path changes. Device names must meet the following requirements:
 - Contains less than 32 characters
 - Contains only alphanumeric and punctuation characters
 - Is unique within the object type
 - c. Select the storage pool.
 - d. Select the media type of the device: HDD or SSD.
 - e. Click **Add Device**.
The device is added to the Devices list.
5. Repeat the process for each additional storage device you wish to add.
6. Expand **Advanced** for more options; recommended for advanced users only.
7. Under **Device tests**, select the test option:
 - `Test and activate device` — Read and write test will be run on the device before it is capacity is used.
 - `Test only` — Devices will be tested, but not used.
 - `Activate without test` — The device capacity will be used without any device testing.

By default, PowerFlex tests the performance of the device being added before its capacity can be used, and saves the results. Two tests are performed: random writes and random reads. When the tests are complete, the device capacity is added automatically to the storage pool used by the MDM. To modify this behavior, specify one of the test options.
8. Define the device test timeout.
This value is the maximum test run time in seconds. The test stops when it reaches either this limit, or the time it takes to complete 128 MB of data read/write, whichever is first. When `Activate without test` is selected, this timeout is ignored.
9. Select whether to force device takeover.
When devices are added to an SDS, PowerFlex checks that the device is clear before adding it. If the device is not clear, an error message is returned, and the command fails for that device. If you would like to overwrite existing data on the device by forcing the command, set **Force device takeover** to **YES**.
 **CAUTION: Select YES with caution, because all data on the device will be destroyed.**
10. Click **Add Devices**.
11. Verify that the operation has finished and was successful, and click **Dismiss**.

Add acceleration devices


Add acceleration devices to the PowerFlex system one by one or in bulk operations. By default, performance tests are performed on the added devices and the results are saved in the system.

Prerequisites

Ensure that at least one suitable acceleration pool is defined.

All devices in a storage pool must be the same media type. Ensure that you know the type of devices that you are adding to the system and that the storage pool to which you are adding devices is configured to receive that media type.

Steps

1. On the menu bar, click **Block > SDSs**.
2. Select the relevant SDS from the SDS list.
3. Click **Add Device > Acceleration Device**.
4. In the **Add Acceleration Device to SDS** dialog box, enter the following required parameters for the acceleration device:
 - a. Device path
The length of the device path name must not exceed 63 characters.
 - b. Name of the device
Assigning a name to a storage device can be particularly helpful for identifying devices in the future, because the name remains constant, even if the path changes. Device names must meet the following requirements:
 - Contains less than 32 characters
 - Contains only alphanumeric and punctuation characters
 - Is unique within the object type
 - c. Select the acceleration pool.
 - d. Click **Add Device**.
The device is added to the Devices list.
5. Repeat the process for each additional acceleration device you wish to add.
6. Expand **Advanced** for more options; recommended for advanced users only.
7. Under **Device tests**, select the test option:
 - `Test and activate device` — Read and write test will be run on the device before it is capacity is used.
 - `Activate without test` — The device capacity will be used without any device testing.By default, PowerFlex tests the performance of the device being added before its capacity can be used, and saves the results. Two tests are performed: random writes and random reads. When the tests are complete, the device capacity is added automatically to the storage pool used by the MDM. To modify this behavior, specify one of the test options.
8. Define the device test timeout.
This value is the maximum test run time in seconds. The test stops when it reaches either this limit, or the time it takes to complete 128 MB of data read/write, whichever is first. When `Activate without test` is selected, this timeout is ignored.
9. Select whether to force device takeover.
When devices are added to an SDS, PowerFlex checks that the device is clear before adding it. If the device is not clear, an error message is returned, and the command fails for that device. If you would like to overwrite existing data on the device by forcing the command, set **Force device takeover** to `YES`.
 **CAUTION: Select YES with caution, because all data on the device will be destroyed.**
10. Click **Add Devices**.
11. Verify that the operation has finished and was successful, and click **Dismiss**.

Storage pools

A storage pool is a set of physical storage devices in a protection domain. A volume is distributed over all devices residing in the same storage pool. Add, modify, or remove a storage pool in the PowerFlex system.

Add storage pools


A storage pool is a group of storage devices within a protection domain. Each time that you add devices to the system, you must map them to either storage pools or to acceleration pools. Create storage pools before you start adding SDSs and storage devices to the system.


Prerequisites

- Familiarize yourself with the types of storage pools that are available, and ensure that you know the media type of the devices that will be used in the storage pool. Each storage pool must contain devices of only one media type.
- A storage pools with fine granularity data layout, requires an acceleration pool which contains at least one NVDIMM configured as a DAX device is required. Ensure that you have configured an NVDIMM acceleration pool prior to creating a fine granularity storage pool.

Steps

1. On the menu bar, click **Block > Storage Pools**.
2. Click **+ Create Storage Pool**.
3. In the **Create Storage Pool** dialog box, define the following settings:
 - a. Define the storage pool name according to the following rules:
 - Contains less than 32 characters
 - Contains only alphanumeric and punctuation characters
 - Is unique within the object type
 - b. Select the relevant protection domain.
 - c. Select the media type of the devices in the storage pool: HDD or SSD.
All devices for this storage pool must be of the same media type.
 - d. If you select SSD, choose a **Data Layout - Granularity** type: Medium or Fine.
 - e. For a fine granularity storage pool, select the relevant **Acceleration Pool**.
4. To use RMCache for caching, select **Use Read RAM Cache**.
 - a. If you are using RMCache, select the **Write Handling Mode**: Cached or PassThrough.
This defines whether the system stores the data of this storage pool's writes in the SDS RMCache, or not. The default is to store the write data in cache (cached).

 **NOTE:** The RMCache features are advanced features, and it is usually recommended to accept the default values. You can configure these features later, if necessary, by clicking **Modify > Cache**.
5. To enable validation of the checksum value of in-flight data reads and writes, select **Use Inflight Checksum**.
6. By default, the **Use Persistent Checksum** is selected to ensure persistent checksum data validation.

 **NOTE:** This option is enabled only when HDD or SSD with medium granularity is selected.
7. Click **Create Storage Pool**.
8. Verify that the operation has finished successfully, and click **Dismiss**.



Configure storage pool settings

Configure storage pool settings, including checksum, zero padding, and compression.

Steps

1. On the menu bar, click **Block > Storage Pools**.
2. In the list of storage pools, select the relevant storage pool, and click **Modify > General Settings**.
3. In the **Storage Pool Settings** dialog box, configure the following settings for the storage pool:

Option	Description
Enable Rebuild/ Rebalance	By default, the rebuild/rebalance features are enabled in the system because they are essential for system health, optimal performance, and data protection.

Option	Description
	 CAUTION: Rebuilding and rebalancing are essential parts of PowerFlex and should only be disabled temporarily, in special circumstances. If rebuilds are disabled, redundancy will not be restored after failures. Disabling rebalance may cause the system to become unbalanced even if no capacity is added or removed.
Enable Inflight Checksum	Inflight checksum protection mode can be used to validate data reads and writes in storage pools, in order to protect data from data corruption.
Enable Persistent Checksum	Persistent checksum can be used to support the medium granularity layout in protecting the storage device from data corruption. Select validate on read to validate data reads in the storage pool.  NOTE: If you want to enable or disable persistent checksum, you must first disable the background device scanner from the storage pool.
Enable Zero Padding Policy	Use the zero-padded policy when the storage pool data layout is fine granularity. The zero-padded policy ensures that every read from an area previously not written to returns zeros.
Enable Compression	For fine granularity storage pools, inline compression allows you to gain more effective capacity.

- Click **Apply**.

Configure RMcachel for the storage pool


RMcache uses RAM that is allocated for caching. The size is limited to the amount of allocated RAM. By default, RMcachel caching is disabled.

Prerequisites

RMcache must also be enabled for each SDS in the storage pool.

About this task

RMcache caching only begins once storage devices have been added to the SDSs. It is possible to enable RMcachel for a storage pool and then disable caching on one or more SDSs individually.

 **NOTE:** Only I/Os that are multiples of 4K bytes can be cached.

Steps

- On the menu bar, click **Block > Storage Pools**.
- In the list of storage pools, select the check box of the relevant storage pool, and click **Modify > Cache**.
- In the **Storage Pool Cache Settings** dialog box, select **Enable Read RMcachel**.
- Click **Apply**.

Using the background device scanner

The background device scanner scans devices in the system to check for errors.

You can enable and disable the background device scanner, as well as reset the background device scanner counters. Information about errors is provided in event reports.

Reset error counters

Reset the background device scanner error counters for the specified storage pools. There are counters for data comparison errors and fixed read errors.

Steps

- On the menu bar, click **Block > Storage Pools**.


2. In the list of storage pools, select the relevant storage pool check box, and click **More Actions > Reset Error Counters**.
3. In the **Reset Error Counters** dialog box, select the relevant option:
 - **Reset Fixed Read Error Counters** — This counter tracks errors that are automatically fixed.
 - **Reset Compare Error Counters** — This counter tracks read errors.
4. Click **Apply**.
5. Verify that the operation completed successfully and click **Dismiss**.

Enable the background device scanner


Enable the background device scanner to check for errors on the devices in the specified storage pool.

Steps

1. On the menu bar, click **Block > Storage Pools**.
2. In the list of storage pools, select the relevant storage pool check box, and click **More Actions > Background Device Scanner**.
3. In the **Set Background Device Scanner for Storage Pool** dialog box, select the relevant option for the following settings. By default, all options are selected.
 - **Enable Background Device Scanner**
 - **Fix Local Device Errors**— automatically fixes device errors.
 - **Compare Data**— compare between primary and secondary copies of data.

 **NOTE:** Zero padding must be enabled in order to set the background device scanner to data compare mode.

 - If **Compare Data** is selected, select or clear **Fix Local Device Errors**.
 - **Bandwidth Limit** in KB/S. Default=3072 KB/S

 **NOTE:** High bandwidth may create negative impact on system performance and should be used carefully and in extreme cases only—for example, when there is an urgent need to check certain devices. When setting the background device scanner bandwidth, you should take into account the maximum bandwidth of the devices.
4. Click **Apply**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Set media type for storage pool

Update the media type of the storage pool. All devices in the storage pool will be this media type.

Steps

1. On the menu bar, click **Block > Storage Pools**.
2. In the list of storage pools, select the relevant storage pool check box, and click **Modify > Media Type**.
3. In the **Set Media Type for Storage Pool** dialog box, from the **Media Type** list, select the media type for the storage pool.
 - **HDD**
 - **SSD**
 - **Transitional**— The media type is defined per device rather than at the storage pool level, to allow for migration of devices from one storage pool to another.
4. Select the **Overwrite SDS device media type** check box to overwrite the current device media type set for the SDS.
5. Click **Apply**.
6. Verify that the operation has finished and was successful, and click **Dismiss**.


Configuring I/O priorities and bandwidth use

PowerFlex includes advanced settings which control I/O priorities and bandwidth use, which can be used to fine-tune system performance. It is recommended to retain default settings, unless you are an advanced user.

Configure IOPS and bandwidth

PowerFlex includes advanced settings that control I/O priorities and bandwidth use and can be used to fine-tune system performance. This includes bandwidth and concurrent I/Os for rebuild, rebalance, migration and protected maintenance mode.

About this task

 **NOTE:** These features affect system performance, and should only be configured by an advanced user.

Steps

1. On the menu bar, click **Block > Storage Pools**.
2. In the list of storage pools, select the relevant storage pool check box, and click **Modify > IO Priority**.
3. In the **Set IO Priority for Storage Pool** dialog box, for each of the tabs—**Rebuild**, **Rebalance**, **Migration**, and **Maintenance Mode**—select one of the following IO Priority options:
 - **Unlimited** — I/Os are not limited
 - **Limit concurrent IO** — limit the number of allowed concurrent I/Os to the value entered in the **Concurrent I/O limit** field
 - **Favor Application IO** — limit the number of allowed concurrent I/Os to the values entered in the **Concurrent I/O limit** and **Bandwidth I/O limit** fields, regardless of user I/O
4. Click **Apply** and click **Dismiss**.

Acceleration pools

An acceleration pool is a group of acceleration devices within a protection domain. PowerFlex only supports acceleration of fine granularity storage pools.

Fine granularity acceleration uses NVDIMMs devices configured to fine granularity storage pools. Configure NVDIMM acceleration pools for fine granularity acceleration.

Add an acceleration pool

Add an acceleration pool to a protection domain to accelerate fine granularity storage performance.

Prerequisites

Ensure that PowerFlex and acceleration devices are prepared before adding acceleration pools. NVDIMMs must be configured as DAX (acceleration) devices.

Steps

1. On the menu bar, click **Block > Acceleration Pools**.
2. Click **+Create Acceleration Pool**.
3. In the **Create Acceleration Pool** dialog box, specify a name for the acceleration pool.
4. Select the following information from the relevant menus:
 - **Pool type:** Select **NVDIMM** or **SSD** for the acceleration pool type.
 - **Protection Domain:** select the protection domain to be accelerated.
5. In the **Add Devices** area, select the devices that will be used for acceleration:

Option	Description
Add acceleration devices from all SDSs that contribute to the relevant acceleration pool.	Optionally, select the Add Devices To All SDSs check box to add acceleration devices from all SDSs in the protection domain. Otherwise, select acceleration devices one by one.
Add devices one by one.	Enter the path and name of each acceleration device, select the SDS on which the device is installed, and then click Add Devices . Repeat for all desired acceleration devices in the acceleration pool.

- Click **Create**.
- Verify that the operation has finished and was successful, and click **Dismiss**.

Rename an acceleration pool

Rename an acceleration pool.

Steps

- On the menu bar, click **Block > Acceleration Pools**.
- In the acceleration pools list, select the desired acceleration pool.
- Click **Rename**.
- In the **Rename Acceleration Pool** dialog box, enter the new name for the acceleration pool, and click **Apply**.
- Verify that the operation has finished and was successful, and click **Dismiss**.

Remove an acceleration pool

Delete an acceleration pool from PowerFlex.

Prerequisites

Remove all acceleration devices from the acceleration pool before deleting the acceleration pool.

Steps

- On the menu bar, click **Block > Acceleration Pools**.
- In the list of acceleration pools, select the desired acceleration pool.
- Click **Delete**.
- In the **Delete Acceleration Pool** dialog box, click **Delete**.
- Verify that the operation has finished and was successful, and click **Dismiss**.

Devices

Storage devices or acceleration devices are added to an SDS or to all SDSs in the system. There are two types of devices: storage devices and acceleration devices.

Activate devices

Activate one or more devices that were added to a system using the `Test only` option for device tests.

Steps

- On the menu bar, click **Block > Devices**.
- In the list of devices, select the check boxes of the required devices, and click **More Actions > Activate**.
- In the **Activate Device** dialog box, click **Activate**.
- Verify that the operation has finished and was successful, and click **Dismiss**.

Clear device errors

Perform this procedure when device errors have been rectified, but the errors have not been cleared automatically by the system.

Steps

1. On the menu bar, click **Block > Devices**.
2. In the list of devices, select the check boxes of the relevant devices, and click **More Actions > Clear Errors**.
3. In the **Clear device errors** dialog box, click **Clear Errors**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Remove devices

Use this procedure to remove a storage or acceleration device.

Prerequisites

Before removing an NVDIMM acceleration device, remove all storage devices that are being accelerated by the NVDIMM. Then, remove the NVDIMM from its acceleration pool.

Steps

1. On the menu bar, click **Block > Devices**.
2. In the list of devices, find the device that you want to remove, make a note of the SDS in which it is installed, and the storage pool or acceleration pool to which it belongs.
This information will be useful for adding the device back to the system later.
3. Select the required device, and click **More Actions > Remove**.
4. In the **Remove Device** dialog box, verify that you have selected the desired device, and click **Remove**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.
A rebuild/rebalance occurs. For each device that was removed from the SDS, the corresponding cell in the **Used Size** column counts down to zero, and then the device disappears from the **Devices** list.

Rename devices

Use this procedure to change the name of a device.

About this task

You can view the current device name by displaying the **Name** column in the device list. The **Name** column is hidden, by default. When no device name has been defined, the name is set by default to the device's path name.

The device name must adhere to the following rules:

- Contains less than 32 characters
- Contains only alphanumeric and punctuation characters
- Is unique within the object type

Steps

1. On the menu bar, click **Block > Devices**.
2. In the list of devices, select the required device, and click **Modify > Rename**.
3. In the **Rename Device** dialog box, enter the new name, and click **Apply**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Set media type

Set a device media type as SSD or HDD.

Prerequisites

Ensure that you are adding the correct device to the system.

About this task

All devices in a storage pool must be the same media type. Set the media type for a device before adding it to a storage pool.

Steps

1. On the menu bar, click **Block > Devices**.
2. In the list of devices, select the relevant device, and click **Modify > Set Media Type**.
3. Select the media type that corresponds to the device.
4. Click **Apply**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Set device capacity limits

Prior to replacing a storage device with a storage device of a smaller capacity, set the capacity limit of the device being removed to the capacity of the new device. Capacity will be decreased, but the size of the disk remains unchanged.

About this task

 **NOTE:** The capacity assigned to the storage device must be smaller than its actual physical size.

Steps

1. On the menu bar, click **Block > Devices**.
2. In the list of devices, select the relevant device, and click **Modify > Set Capacity Limit**.
3. In the **Set Capacity Limit** dialog box, enter the capacity and select a unit type (MB or GB).
This dialog box displays the maximum capacity available for the device.
4. Click **Apply**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Modify device LED settings

Set a device's LED to blink or turn it off. This feature can help you physically identify a device in the system chassis.

Steps

1. On the menu bar, click **Block > Devices**.
2. In the list of devices, select the relevant device, and click **Modify > LED Settings**.
3. In the **Set device LED settings** dialog box, do one of the following:
 - To turn on the device's LED, select the **On** check box.
 - To turn off the device's LED, clear the **On** check box.
4. Click **Apply**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Volumes

Define, configure and manage volumes in the PowerFlex system.

Add volumes

Use the following procedure to add volumes. Dell Technologies highly recommends giving each volume a meaningful name associated with its operational role.

Prerequisites

There must be at least three SDS nodes in the system and there must be sufficient capacity available for the volumes.

About this task

PowerFlex objects are assigned a unique ID that can be used to identify the object in CLI commands. The default name for each volume object is its ID. The ID is displayed in the Volumes list or can be obtained using a CLI query. Define each volume name according to the following rules:

- Contains less than 32 characters
- Contains only alphanumeric and punctuation characters
- Is unique within the object type

To add one or multiple volumes, perform these steps:

Steps

1. On the menu bar, click **Block > Volumes**.
2. Click **+ Create Volume**.
3. In the **Create Volume** dialog box, configure the following items:
 - a. Enter the number of volumes to be created.
 - If you type **1**, enter a name for the volume.
 - If you type a number greater than 1, enter the **Volume Prefix** and the **Starting Number** of the volume. This number will be the first number in the series that will be appended to the volume prefix. For example, if the volume prefix is **Vol1%i** and the starting number value is **100**, the name of the first volume created will be Vol100, the second volume will be Vol101, and so on.
 - b. Select either **Thin** (default) or **Thick** provisioning options.
 - c. Enter the volume size in GB (basic allocation granularity is 8 GB).
 - d. Select a storage pool.
4. Click **Create**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Next steps

To use the created volume, you must map it to at least one host. If the restricted SDC mode is enabled for the system, you must approve SDCs prior to mapping volumes to them.

Delete volumes

Remove volumes from PowerFlex.

Prerequisites

Ensure that the volume that you are deleting is not mapped to any hosts. If it is, unmap it before deleting it. In addition, ensure that the volume is not the source volume of any snapshot policy. You must remove the volume from the snapshot policy before you can remove the volume.

About this task

To prevent causing a data unavailability scenario, avoid deleting volumes or snapshots while the MDM cluster is being upgraded.

 **CAUTION:** All data is erased from a deleted volume.

Steps

1. On the menu bar, click **Block > Volumes**.
2. In the list of volumes, select the required volume, and click **More Actions > Delete**.
3. In the **Delete Volume** dialog box, verify the volumes to be removed, and click **Delete**.
4. In the warning dialog box, click **Delete**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.


Overwrite volume content


Overwrite the contents of a volume with content from another volume.

Prerequisites

At least two volumes per vTree are required.

About this task

 **NOTE:** Use this command very carefully, since this will overwrite data on the target volume or snapshot.

 **NOTE:** If the destination volume is an auto snapshot, the auto snapshot must be locked before you can continue to overwrite volume content.

Steps

1. On the menu bar, click **Block > Volumes**.
2. In the list of volumes, select the required volume, and click **More Actions > Overwrite Content**.
3. In the **Overwrite Content of Volume** dialog box, in the **Target Volume** tab, the selected volume details are displayed. Click **Next**.
4. In the **Select Source Volume** tab, do the following:
 - a. Select the source volume from which to copy content.
 - b. Click the **Time Frame** button and select the interval from which to copy content. If you choose **Custom**, select the date and time and click **Apply**.
 - c. Click **Next**.
5. In the **Review** tab, review the details and click **Overwrite Content**.
6. Verify that the operation has finished and was successful, and click **Dismiss**.


Create volume snapshots

PowerFlex lets you to create instantaneous snapshots of one or more volumes.

About this task

The **Use secure snapshots** option prohibits deletion of the snapshots until the defined expiration period has elapsed.

When you create a snapshot of more than one volume, PowerFlex generates a consistency group by default. The snapshots under the consistency group are taken simultaneously for all listed volumes, thereby ensuring their consistency. You can view the consistency group by clicking **View Details** in the right pane and then clicking the **Snapshots Consistency Group** tab in the left pane.

 **NOTE:** The consistency group is for convenience purposes only. No protection measures are in place to preserve the consistency group. You can delete members from the group.

Steps

1. On the menu bar, click **Block > Volumes**.
2. In the list of volumes, select the relevant volumes, and then click **More Actions > Create Snapshot**.
3. In the **Create snapshot of volume** dialog box, enter the name of the snapshot. You can accept the default name, or give the new snapshot a name according to the following rules:
 - Contains less than 32 characters
 - Contains only alphanumeric and punctuation characters
 - Is unique within the object type
4. Optionally, configure the following parameters:
 - To set read-only permission for the snapshot, select the **Read Only** check box.
 - To prevent deletion of the snapshot during the expiration period, select the **Use secure snapshot** check box, enter the **Expiration Time**, and select the time unit type.
5. Click **Create**.
6. Verify that the operation has finished and was successful, and click **Dismiss**.

Set volume bandwidth and IOPS limits

Setting bandwidth and IOPS limits for volumes lets you control the quality of service (QoS). Bandwidth and IOPS limits are set on a per-host basis.

Prerequisites

Ensure that the volumes are mapped before you set these limits.

Steps

1. On the menu bar, click **Block > Volumes**.
2. In the list of volumes, select the relevant volume, and then click **More Actions > Set Limits**.
3. In the **Set IO limits for volume** dialog box, enter the required values for **Bandwidth Limits** and **IOPS Limits**, or select the corresponding **Unlimited** check box.
 - The number of IOPS must be larger than 10.
 - The volume network bandwidth is in MB/s.
 - The I/O limits are applied to every mapped SDC.
4. Click **Apply**.
5. Verify that the operation has finished successfully, and click **Dismiss**.

Increase volume size

You can increase (but not decrease) the capacity of one or more volumes at any time, as long as there is enough capacity for the volume size to grow.

Steps

1. On the menu bar, click **Block > Volumes**.
2. In the list of volumes, select the volume, and click **Modify > Resize**.
3. In the **Resize Volume** dialog box, enter the new volume size, and select a unit type. (The basic allocation granularity is 8 GB.)
4. Click **Apply**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Map volumes

Mapping exposes the volume to the specified host, effectively creating a block device on the host. You can map a volume to one or more hosts.

Prerequisites


Volumes can only be mapped to one type of host: either SDC or NVMe. Ensure that you know which type of hosts are being used for each volume, to avoid mixing host types.


About this task

For Linux-based devices, the `scini` device name may change on reboot. Dell recommends that you mount a mapped volume to the PowerFlex unique ID, which is a persistent device name, rather than to the `scini` device name.

To identify the unique ID, run the command `ls -l /dev/disk/by-id/`.

You can also identify the unique ID using VMware. In the VMware management interface, the device is called **EMC Fibre Channel Disk**, followed by an ID number starting with the prefix **eui**.

 **NOTE:** You cannot map a volume if the volume is an auto snapshot that is not locked.

 **NOTE:** You cannot map the volume on the target of a peer system if it is connected to a replication consistency group.

Steps

1. On the menu bar, click **Block > Volumes**.
2. In the list of volumes, select one or more volumes, and click **Mapping > Map**.
3. A list of the hosts that can be mapped to the selected volumes is displayed. If a volume is already mapped to a host, only hosts of the same type, NVMe or SDC, are listed. If the volume is not mapped to a host, click **NVMe** or **SDC** to set the type of hosts to be listed.
4. In the **Map Volume** dialog box, select one or more hosts to which you want to map to the volumes.
5. Click **Map**.
6. Verify that the operation has finished and was successful, and click **Dismiss**.

Unmap volumes

Unmap one or more volumes from hosts.


Steps

1. On the menu bar, click **Block > Volumes**.
2. In the list of volumes, select the relevant volumes, and then click **Mapping > Unmap volumes**.
3. Select the host from which to remove mapping to the volumes.
4. Click **Unmap**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Remove a snapshot consistency group

Remove a consistency group with all its snapshots.

About this task

 **NOTE:** You cannot remove a consistency group that contains auto snapshots.

Steps

1. On the menu bar, click **Block > Volumes**.
2. In the list of volumes, select the relevant volume, and then in the right pane, click **View Details**.

3. In the left pane, click **Snapshots Consistency Group**.
4. Select the required consistency group.
5. Click **Remove SCG**.
6. In the **Remove SCG** dialog box, click **Remove SCG**.
7. Verify that the operation has finished and was successful, and click **Dismiss**.

Migrating vTrees

Migration of a volume tree (vTree) allows you to move a vTree to a different storage pool.

Migration of a vTree frees up capacity in the source storage pool. For example, you can migrate a vTree from an HDD-based storage pool to an SSD-based storage pool, or to a storage pool with different attributes such as *thin* or *thick*.

There are several possible reasons for migrating a vTree to a different storage pool:

- To move the volumes to a different storage pool type
- To move to a different storage pool or protection domain due to multitenancy
- To decrease the capacity of a system by moving out of a specific storage pool
- To change from a thin-provisioned volume to a thick-provisioned volume, or the reverse
- To move the volumes from a medium granularity storage pool to a fine granularity storage pool
- To clear a protection domain for maintenance purposes, and then return the volumes to it

During vTree migration, you can run other tasks such as creating snapshots, deleting snapshots, and entering maintenance mode.

NOTE: You cannot create snapshots when migrating a vTree from a medium granularity storage pool to a fine granularity storage pool.

When a user requests a vTree migration, the MDM begins the process by estimating whether the destination storage pool has enough capacity for a successful migration. The MDM bases the estimation on its information about the current capacity of the vTree. If there is insufficient capacity at the destination based on that estimate, migration does not start. (An advanced option allows you to force the migration even if there is insufficient capacity at the destination, with the intention to increase the capacity as required during the migration.) The MDM does not reserve the estimated capacity at the destination (since the capacity of the source volume can grow during migration and the reserved capacity does not guarantee success). The MDM does not retain source capacity once it has been migrated, but releases it immediately.

Use the following table to understand which vTree migrations are possible, and under what specific conditions:

				Destination SP				
				MG				FG
				Zero Padded		Non Zero Padded		Zero Padded
				Thin	thick	Thin	thick	Thin
Source SP	MG	Non Zero Padded	Thin	*	*			*
			thick	*	*			*
		Zero Padded	Thin			*0	*0	*
			thick			*	*0	*
	FG	Zero Padded	Thin	*	*	*	*0	Compression method cannot be modified

Color Codes:	
Allowed	
Required Force Flag	
Excluded from V3.0	
Zeros Are Sent	0
No Snapshot Support	*
Compression Method may be specified or the default of the destination SP would be used	**

vTree migration can take a long time, depending on the size of the vTree and the system workload. During migration, the vTree is fully available for user I/O. vTree migration is done volume block by volume block. When a single block has completed its migration, the capacity of the block at the source becomes available, and it becomes active in the destination storage pool. During migration, the vTree has some of its blocks active in the source storage pool, and the remaining blocks active in the destination storage pool.

NOTE: You can speed up the migration by adjusting the volume migration I/O priority (QoS). The default favors applications with one concurrent I/O and 10 MB/sec per device. Increasing the 10 MB/sec setting increases the migration

speed in most cases. The maximum value that can be reached 25 MB/sec. The faster the migration, the higher the impact might be on applications. To avoid significant impact, the value of concurrent I/O operations per second should not be increased.

When migrating from a medium granularity storage pool to a fine granularity storage pool, volumes must be zero padded.

You can pause a vTree migration at any time, in the following ways:

- Gracefully—to allow all data blocks currently being migrated to finish before pausing.
- Forcefully—to stop the migration of all blocks currently in progress.

Once paused, you can choose to either resume the vTree migration, or to roll back the migration and have all volume blocks returned to the original storage pool.


vTree migration might also be paused internally by the system. System pauses happen when a rebuild operation begins at either the source or destination storage pool. If the migration is paused due to a rebuild operation, it remains paused until the rebuild ends. If the system encounters a communication error that prevents the migration from proceeding, it pauses the migration and periodically tries to resume it. After a configurable number of attempts to resume the migration, the migration remains paused, and no additional retries will be attempted. You can manually resume migrations that were internally paused by the system.

Concurrent vTree migrations are allowed in the system. These migrations are prioritized by the order in which they were invoked, or by manually assigning the migration to the head or the tail of the migration queue. You can update the priority of a migration while it is being run. The system strives to adhere to the priority set by the user, but it is possible that volume blocks belonging to migrations lower in priority are run before ones that are higher in priority. This can happen when a storage pool that is involved in migrating a higher priority block is busy with other incoming migrations, and the storage pools involved in lower priority migrations are available to run the migration.

Migrate volume trees (vTree)

Migrate a volume and all of its snapshots to a different storage pool. Volumes undergoing migration remain available for I/O.

About this task

 **NOTE:** vTree migration is a long process and can take days or weeks, depending on the size of the vTree.


The following limitations apply:

- Migration between storage pools with different data layouts is only allowed if there is a single volume in the vTree.
- vTrees containing a manually created snapshot cannot be migrated.
- You cannot migrate a volume that is a source volume of a snapshot policy between storage pools with different data layouts.
- Volumes involved in replication cannot be migrated.

Steps

1. On the menu bar, click **Block > Volumes**.
2. In the list of volumes, select the volume that you want to migrate.
3. In the right pane, click **View Details**.
4. In the left pane, click the **VTREE** tab.
5. In the left pane, from the **VTREE** menu on the right, select **Migrate vTree**.
6. In the **Migrate vTree** dialog box, in the **TARGET** area, select the destination storage pool.
Ensure that you select a storage pool with enough capacity for the vTree size.
7. Optionally, expand **Advanced** to select one or several of the following advanced options:

Option	Description
Add migration to the head of the migration queue	Give this vTree migration the highest priority in the migration priority queue.
Ignore destination capacity	Allow the migration to start regardless of whether there is enough capacity at the destination, or not.
Enable compression	Compression is done by applying a compression-algorithm to the data.

Option	Description
Convert vTree from...	Convert a thin-provisioned vTree to thick-provisioned, or vice-versa, at the destination, depending on the provisioning of the source volume.  NOTE: SDCs with a version earlier than v3.0 do not fully support converting a thick-provisioned vTree to a thin-provisioned vTree during migration; after migration, the vTree will be thin-provisioned, but the SDC will not be able to trim it. These volumes can be trimmed by unmapping and then remapping them, or by restarting the SDC. The SDC version will not affect capacity allocation, and a vTree converted from thick to thin provisioning will be reduced in size accordingly in the system.
Save current vTree provisioning state during migration	The provisioning state is returned to its original state before the migration took place.

8. Click **Migrate vTree**.

The vTree migration is initiated. The vTree appears in both the source and the destination storage pools.

9. At the top right of the window, click the **Running Storage Jobs** icon and check the progress of the migration of the vTree.
10. Verify that the operation has finished and was successful, and click **Dismiss**.


Pause vTree migration

You can pause a vTree migration at any time.

About this task

The following methods can be used to pause vTree migration:

- Gracefully—allows all data blocks currently being migrated to finish migration before pausing.
- Forcefully—stops the migration of all blocks currently in progress.

 **CAUTION:** The forceful method carries a potential risk of data loss.

Steps

1. On the menu bar, click **Block > Volumes**.
2. In the list of volumes, select the volume for which you want to pause migration.
3. In the right pane, click **View Details**.
4. In the left pane, click the **VTree** tab.
5. In the left pane, from the **VTree** menu on the right, select **Pause migration**.
6. In the **Pause VTree Migration** dialog box, select the required option:
 - Gracefully
 - Forcefully
7. Click **Pause Migration**.

If you selected to pause the migration gracefully, migration status is displayed. Once paused, you can choose to roll back the vTree migration, or resume the migration using the **VTree** menu.

8. Verify that the operation has finished and was successful, and click **Dismiss**.

Resume a vTree migration

You can resume a vTree migration that was paused at any time.

Steps

1. On the menu bar, click **Block > Volumes**.
2. In the list of volumes, select the volume where migration was paused.
3. In the right pane, click **View Details**.
4. In the left pane, click the **VTree** tab.

5. In the left pane, from the **VTrees** menu on the right, select **Resume migration**.
6. In the **Resume VTree Migration** dialog box, click **Resume Migration**.
7. Verify that the operation has finished and was successful, and click **Dismiss**.

Roll back vTree migration

When a vTree migration is paused, you can roll back the migration so that the volume and all of its snapshots are returned to the source storage pool.

Steps

1. On the menu bar, click **Block > Volumes**.
2. In the list of volumes, select the volume for which you want to roll back migration.
3. In the right pane, click **View Details**.
4. In the left pane, click the **VTrees** tab.
5. In the left pane, from the **VTrees** menu on the right, select **Roll back Migration**.
6. In the **Migrate vTree** dialog box, verify the source and target for the rollback, and click **Roll back Migration**.
7. Verify that the operation has finished and was successful, and click **Dismiss**.


Results

The migration resumes in the reverse direction. Any data already migrated to the destination storage pool is now migrating back to the source storage pool.

Set vTree migration priority

Specify whether a vTree migration will be at the beginning or at the end of the migration queue.

About this task

 **NOTE:** This feature is available only when there is more than one vTree migration currently in the queue.

Steps

1. On the menu bar, click **Block > Volumes**.
2. In the list of volumes, select the relevant volume.
3. In the right pane, click **View Details**.
4. In the left pane, click the **VTrees** tab.
5. In the left pane, from the **VTrees** menu on the right, select **Set Priority**.
6. In the **Set VTree Migration Policy** dialog box, select whether to move the current vTree migration to the head or to the tail of the migration queue, and click **Set Priority**.
7. Verify that the operation has finished and was successful, and click **Dismiss**.

Remove a vTree

You can remove a vTree from PowerFlex, as long as it is unmapped.

Prerequisites

Ensure that the vTree is unmapped.

Steps

1. On the menu bar, click **Block > Volumes**.
2. In the list of volumes, select the volume that you want to remove.
3. In the right pane, click **View Details**.
4. In the left pane, click the **VTrees** tab.

5. In the left pane, from the **VTree** menu on the right, select **Remove**.
6. In the **Remove VTree** dialog box, click **Remove VTree**.
7. Verify that the operation has finished and was successful, and click **Dismiss**.

NVMe targets

NVMe targets (or SDT components) must be configured on the PowerFlex system side, in order to use NVMe over TCP technology.

The NVMe target (or SDT component) is a frontend component that translates NVMe over TCP protocol into internal PowerFlex protocols. The NVMe target provides I/O and discovery services to NVMe hosts configured on the PowerFlex system. A minimum of two NVMe targets must be assigned to a protection domain before it can serve NVMe hosts, to provide minimal path resiliency to hosts.

TCP ports, IP addresses, and IP address roles must be configured for each NVMe target (or SDT component). You can assign both storage and host roles to the same target IP addressess. Alternatively, assign the storage role to one target IP address, and add another target IP address for the host role. Both roles must be configured on each NVMe target.

- The host port listens for incoming connections from hosts, over the NVMe protocol.
- The storage port listens for connections from the MDM.

Once the NVMe targets have been configured, add hosts to PowerFlex, and then map volumes to the hosts. Connect hosts to NVMe targets, preferably using the discovery feature.

On the operating system of the compute nodes, NVMe initiators must be configured. Network connectivity is required between the NVMe targets and the NVMe initiators, and between NVMe targets (or SDT components) and SDSs.

Add an NVMe target

Add an NVMe target (or SDT component) to PowerFlex.

Steps

1. On the menu bar, click **Block > NVMe Targets**.
2. Click **+ Add NVMe Target**.
3. In the **Add NVMe Target** dialog box, configure the following settings:
 - a. For **Target Name**, enter a name for the NVMe target (or SDT component).
 - b. For **Protection Domain**, select a protection domain.
 - c. Accept the default TCP ports, or modify them if necessary.
 - **Storage Port** listens for incoming connections from the MDM, and is only open on an IP address configured with the storage role. Default=12200
 - **I/O Port** listens for incoming connections for I/O, and is only open on an IP address configured with the host role. Default=4420 (which conforms to the NVMe over TCP standard)
 - **Discovery Port** listens for incoming discovery connections, and is only open on an IP address configured with the host role. Default=8009 (which conforms to the NVMe over TCP standard. Use zero to disable the discovery service.)
 - d. For **Target IPs**, enter an IP address, and then select a role for the IP address from the **Target IPs Roles** menu. Click **Add Target IP**, and repeat this step until all IP addresses are configured.
4. Click **Add**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Next steps

The CLI for PowerFlex also provides options for adding an SDT to a fault set.

```
sio@localhost [/home/sio] $ scli --add_sdt --help

Usage: scli --add_sdt --sdt_ip <IP> [--sdt_ip_role <ROLE>] [--storage_port <PORT>] [--nvme_port <PORT>] [--discovery_port <PORT>] [--sdt_name <NAME>] (--protection_domain_id <ID> | --protection_domain_name <NAME>) [--fault_set_id <ID> | --fault_set_name <NAME>] [--profile <PROFILE>] [--force_clean [--i_am_sure]]
Description: Add an SDT
```

Parameters:	
--sdt_ip <IP>	A comma separated list of IP addresses assigned to the SDT
--sdt_ip_role <ROLE>	A comma separated list of roles assigned to each SDT IP address
storage_and_host	Role options: storage_only, host_only, or
--storage_port <PORT>	Port assigned to the SDT (default: 12200)
--nvme_port <PORT>	Port to be used by the NVMe hosts (default: 4420)
--discovery_port <PORT>	Port to be used by the NVMe hosts for discovery
(default: 8009)	
discovery_port	Set to 1 in order to indicate no use of
--sdt_name <NAME>	A name to be assigned to the SDT
--protection_domain_id <ID>	Protection Domain ID
--protection_domain_name <NAME>	Protection Domain name
--fault_set_id <ID>	Fault Set ID
--fault_set_name <NAME>	Fault Set name
--profile <PROFILE>	Set the performance profile from the following options: compact high_performance
--force_clean	The default is high_performance
--i_am_sure	Clean a previous SDT configuration
	Preemptive approval

Modify an NVMe target

Modify the configuration of an NVMe target (or SDT component).

Steps

1. On the menu bar, click **Block > NVMe Targets**.
2. In the list of NVMe targets, select the required NVMe target, and click **Modify**.
3. In the **Modify NVMe Target** dialog box, modify the desired fields.
4. Optionally, add more target IP addresses, by clicking **Add Target IP**.
5. Click **Modify NVMe Target**.
6. Verify that the operation has finished and was successful, and click **Dismiss**.

Remove an NVMe target

Remove an NVMe target (or SDT component) from PowerFlex.

Steps

1. On the menu bar, click **Block > NVMe Targets**.
2. In the list of NVMe targets, select the required NVMe target, and click **Remove**.
3. In the **Remove NVMe Target** dialog box, verify that you are removing the desired NVMe target, and click **Remove**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Understanding NVMe over TCP load balancing

PowerFlex supports load balancing with NVMe over TCP.

Persistent discovery

The persistent discovery controller ensures that the host remains connected to the discovery service after discovery. If at any point there is a change in the discovery information that is provided to the host, the discovery controller returns an asynchronous event notification (AEN) and the host requests the updated **Discovery log** page.

Here are some examples of changes in discovery information:

- A new volume is mapped to the host from a new protection domain.
- A new storage data target (SDT) is added to the system.
- Load balancing wants to move the host connection from one storage data target to another.

When configuring NVMe hosts, ensure that every host is connected for discovery at most once per subnet (data IP address subnet). To use this functionality, ensure that the host operating system supports the Persistent Discovery Controller, and that the Persistent Discovery flag is set in the discovery. (See the respective operating system for the NVMe over TCP host configuration.)

NVMe over TCP hosts network awareness

Hosts are connected to the storage through Layer-2 or Layer-3 network. While the storage does not manage or need to be aware of the network configuration, there are some aspects of the network that impact the storage.

Load balancing takes the data network/subnet into consideration to ensure there is a balance between the host connections on each data network with a specific subnet, hence improved performance.

In Layer-3 networks, the system must have routing tables configured.

Multiple objects need to be defined for load balancing to work:

Object	Description
Host subnet	Networks or subnets used to connect hosts to storage, which can be either layer 2 or layer 3 (routed). You might have to define the data networks before starting the deployment itself. Maximum supported data networks are 4 (in Dell PowerFlex appliance and Dell PowerFlex rack) and 8 in the software-only offering.
System data network	System-wide object that applies to all protection domains. Once a resource group is deployed, configure system data networks/subnets to be used to connect hosts initiator to the storage data target. Maximum allowed system data networks are 8. Configure two or four system data networks for PowerFlex rack and PowerFlex appliance. The number that you need depends on the number of PowerFlex data (SDS-SDS and SDS-SDT communication) networks that are configured for the deployment.

If you have not defined the system data network, by default, a host can reach all system data networks. Ignoring the data networks/subnets may result in unequal load between the host initiator ports and nonoptimized I/O performance with the PowerFlex system. In addition, it may impact the path resiliency if not all the host initiator ports can connect to the system. For Layer-3 networks, the system must have routing tables configured.

Managing system data networks in PowerFlex Manager

The NVMe over TCP load balancer uses the data networks for balancing the host connections. This section summarizes the steps that you must perform in PowerFlex Manager to add, rename, or remove system data networks.

If you want to...	Do this in PowerFlex Manager
Add system data networks	<ol style="list-style-type: none"> 1. On the menu bar, click Settings > Networking. 2. Click System Data networks. 3. Enter the required information and click Save.
Rename system data networks	<ol style="list-style-type: none"> 1. On the menu bar, click Settings > Networking. 2. Click System Data networks. 3. Select the network and click Rename. 4. Rename the network and click Apply.
Remove system data networks	<ol style="list-style-type: none"> 1. On the menu bar, click Settings > Networking. 2. Click System Data networks. 3. Select the network and click Remove.

If you want to...	Do this in PowerFlex Manager
	4. Click Remove to remove the network.

Managing system data networks using SCLI

This section provides the SCLI commands that you need to perform to add, rename, or remove system data networks.

If you want to...	Use this SCLI command
Add system data networks	<pre>scli --add_system_network --network_ip <IP> --network_mask <IP> [--network_name <NAME>] (--host_group_id <ID> --host_group_name <NAME>)</pre>
Rename system data networks	<pre>scli --rename_system_network (--network_id <ID> --network_name <NAME>) --new_name <NAME></pre>
Remove system data networks	<pre>scli --remove_system_network (--network_id <ID> --network_name <NAME>)</pre>

Managing host groups using SCLI

This section provides the SCLI commands that you must perform to add, modify, rename, remove, or query host groups.

This feature is allowed only using SCLI. It is not available in PowerFlex Manager.

The host group holds a subgroup of existing networks that are accessible to a group of hosts. Each host group is associated with a set of system networks. Each host may be associated with multiple host groups. By default, a host is part of the default host group until you create a new host group and associate the host to the new host group. By default, a host supports all data networks and you do not need to configure the host groups. The maximum number of host groups that are allowed per system is 1024.

If you want to...	Use this SCLI command
Add host group	<pre>scli --add_host_group [--host_group_name <NAME>] [--network_id <ID> --network_name <NAME>] [--host_nqn <NQN> --host_id <ID> --host_name <NAME>]</pre>
Modify host group	<pre>scli --modify_host_group (--host_group_id <ID> --host_group_name <NAME>) [--network_id <ID> --network_name <NAME>]</pre>
Rename host group	<pre>scli --rename_host_group (--host_group_id <ID> --host_group_name <NAME>) --new_name <NAME></pre>
Remove host group	<pre>scli --remove_host_group (--host_group_id <ID> --host_group_name <NAME>)</pre>
Assign host to group	<pre>scli --assign_host_to_host_group (--host_nqn <NQN> --host_id <ID> --host_name <NAME>) (--host_group_id <ID> --host_group_name <NAME>)</pre>

If you want to...	Use this SCLI command
Remove host from group	<code>scli --remove_host_from_host_group (--host_nqn <NQN> --host_id <ID> --host_name <NAME>)</code>
Query host group	<code>scli --query_host_group (--host_group_id <ID> --host_group_name <NAME>)</code>
Query all host group	<code>scli --query_all_host_group</code>

Managing network sets using SCLI

This section provides the SCLI commands that you need to perform to add, modify, rename, remove, or query network sets.

This feature is allowed only using SCLI. It is not available in PowerFlex Manager.

A network set is a set of networks that are connected to the same switch. This switch is configured for balancing the I/O traffic between access switches by associating system data networks to network set. The load balancer takes care of the distribution of networks over network sets.

For example, if a system is defined with two system data networks (192.168.150.0 and 192.168.151.0), then you could create two network sets and associate 192.168.150.0 with network set 1 and 192.168.151.0 to network set 2.

Each system data network belongs to exactly one network set. If the network was not assigned to a network set, the network will be considered a network set of its own.

Use the default network set and do not manually create the network set. Creating network sets is applicable for a software-only deployment.

If you want to...	Use this SCLI command
Add network set	<code>scli --add_network_set [--network_set_name <NAME>] [--network_id <ID> --network_name <NAME>]</code>
Modify network set	<code>scli --modify_network_set (--network_set_id <ID> --network_set_name <NAME>) [--network_id <ID> --network_name <NAME>]</code>
Rename network set	<code>scli --rename_network_set (--network_set_id <ID> --network_set_name <NAME>) --new_name <NAME></code>
Remove network set	<code>scli --remove_network_set (--network_set_id <ID> --network_set_name <NAME>)</code>
Query network set	<code>scli --query_network_set (--network_set_id <ID> --network_set_name <NAME>)</code>
Query all network sets	<code>scli --query_all_network_set</code>

Hosts

Hosts are entities that consume PowerFlex storage for application usage. There are two methods of consuming PowerFlex block storage: using the SDC kernel driver, or using NVMe over TCP connectivity. Therefore, a host is either an SDC or an NVMe host.

Once a host is configured, volumes may be mapped to it. In each case, hosts must be mapped to volumes.

Add an NVMe host

Add an NVMe host to PowerFlex.

Prerequisites

- Ensure that you have the host's NVMe Qualified Name (NQN). If you do not know the NQN, see the documentation for the host operating system.
- Ensure that the host is connected to the Ethernet switch.
- Ensure that the host is configured with the correct VLAN ID and routing rules.

Steps

1. On the menu bar, click **Block > Hosts**.
2. Click **+ Add Host**.
3. In the **Add NVMe Host** dialog box, enter a hostname in the **Host Name** field.
4. In the **Host NQN** field, enter the NQN string for the host.
5. In the **Number of Paths Per Volume** field, enter the maximum number of paths to be provided between the host and each volume (default is 4).
6. In the **Number of System Ports per Protection Domain** field, enter the maximum number of ports to be provided between the host and each protection domain (default is 10).
7. Click **Add**.
8. Verify that the operation has finished and was successful, and click **Dismiss**.
9. Configure the host operating system to connect to the cluster's NVMe discovery service on one or more of the NVMe targets.

Next steps

The CLI for PowerFlex also provides options for adding a host group:

```
sio@localhost [/home/sio] $ scli --add_nvme_host --help

Usage: scli --add_nvme_host --nvme_host_nqn <NQN> [--host_name <NAME>] [--
max_number_paths <VALUE>] [--max_number_sys_ports <VALUE>] [--host_os_full_type <OS>] [--
host_group_name <ID> | --host_group_id <NAME>] | --force
Description: Add a NVMe Host to the system
Parameters:
  --nvme_host_nqn <NQN>           NVMe Host NQN
  --host_name <NAME>              Host name
  --max_number_paths <VALUE>      Maximal number of paths allowed per mapped volume
                                  Valid range: 2-8. Default: 4
  --max_number_sys_ports <VALUE>  Maximal number of System Ports allowed per
Protection Domain
  --host_os_full_type <OS>        Valid range: 2-128. Default: 10
                                  NVMe Host OS type
                                  Options: generic (default) or powerflex
  --host_group_id <ID>           Host Group ID
  --host_group_name <NAME>       Host Group name
  --force                        Force NQN, ignore all NQN formating rules.
```

Map hosts

Map hosts to volumes.

Prerequisites

Volumes can only be mapped to one type of host: either SDC or NVMe. Ensure that you know which type of hosts are being used for each volume, to avoid mixing host types.

Steps

1. On the menu bar, click **Block > Hosts**.
2. In the list of hosts, select the relevant host, and click **Mapping > Map**.
3. In the **Map Hosts to Volumes** dialog box, select the volumes to be mapped to the selected hosts, and click **Map**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Unmap hosts

Remove mapping between volumes and hosts.

Steps

1. On the menu bar, click **Block > Hosts**.
2. In the list of hosts, select the relevant host, and click **Mapping > Unmap**.
3. In the **Unmap** dialog box, ensure that the desired host is selected.
4. Click **Unmap**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Remove hosts

Remove hosts from PowerFlex.

Steps

1. On the menu bar, click **Block > Hosts**.
2. In the list of hosts, select the relevant host, and click **Remove**.
3. In the **Remove Host** dialog box, ensure that you have selected the desired host for removal.

 **NOTE:** For SDCs, the host must be disconnected from the PowerFlex cluster before it can be removed.

4. Click **Remove**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Configure or modify approved host IP addresses

When the system's restricted host (SDC) mode is set to approved IP restriction, configure host IP addresses before mapping volumes to the hosts.

Prerequisites

Ensure that the hosts have been approved by GUID.

Steps

1. On the menu bar, click **Block > Hosts**.
2. In the list of hosts, select the relevant host, and click **Modify > Modify Approved IP Addresses**.

3. In the **Modify Approved IP addresses** dialog box, enter the IP address of the hosts, and click **Add IP Address**. Repeat this step for additional addresses.

You can add up to a total of four IP addresses.

4. Click **Apply**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Approve SDCs

When the system's restricted host (SDC) mode is set to GUID restriction, approve SDCs before mapping them to volumes.

Steps

1. On the menu bar, click **Block > Hosts**.
2. In the list of hosts, select one or more hosts and click **Modify > Approve**.
3. In the **Approve host** dialog box, verify that the hosts listed are the ones that you want to approve, and click **Approve**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Rename hosts

About this task

The host name must adhere to the following rules:

- Contains less than 32 characters
- Contains only alphanumeric and punctuation characters
- Is unique within the object type

Steps


1. On the menu bar, click **Block > Hosts**.
2. In the list of hosts, select the relevant host, and click **Modify > Rename**.
3. In the **Rename Host** dialog box, enter the new name, and click **Apply**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Modify an SDC performance profile

SDC performance profiles are set by default to high and can be changed to compact. The compact setting may impact the system performance.

About this task

The default setting configures a predefined set of parameters for very high-performance use cases.

 **NOTE:** Performance tuning is very case-specific. To prevent undesirable effects, Dell Technologies highly recommends that you thoroughly test all changes. For further assistance, contact Dell Technologies Support.

Steps

1. On the menu bar, click **Block > Hosts**.
2. In the list of hosts, select the relevant host, and click **Modify > Modify Performance Profile**.
3. In the **Modify Performance Profile Host** dialog box, select the desired performance profile: **High** or **Compact**.
4. Click **Apply**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Storage management for PowerFlex controller nodes

When PowerFlex management controller 2.0 is expanded with new PowerFlex controller nodes, use the procedures in this section to increase the volume size of the PowerFlex controller nodes.

Verify newly added storage data server is reflecting under the appropriate cluster

Use this procedure to verify that the newly added storage data server is reflecting under the storage data server cluster.

Steps

1. Log in to the primary MDM using the following command:
scli --login --username admin --management_system_ip <PFMP-UI IP> --password <PFMP-UI password> --insecure
2. Run the following command to identify that the newly added PowerFlex node is reflecting under the storage data server
scli --query_all_SDS
3. Execute the following command to capture the protection domain and storage pool name:
scli --query_all_volumes
4. If the storage data server is missing from the storage data server cluster, use the following command to add the storage data server:
scli --add_sds --sds_ip <data1 IPAddress, data2 IPAddress> --protection_domain_name <PD name> --storage_pool_name <spname> --disable_rmcache --sds_name <SDS-name>
5. Add the device for the newly added storage data server:
scli --add_sds_device --sds_name <newly add SDS name> --storage_pool_name <SP-name> --device_path <device path>
6. Using SSH, log in to the PowerFlex node and run the **lsblk** command to identify the device path.

Modify the volume capacity

Use this procedure to modify the volume capacity according to the respective volumes.

Steps

1. Log in to the primary MDM using the following command:
scli --login --username admin --management_system_ip <PFMP-UI IP> --password <PFMP-UI password> --insecure
2. Execute the following command to capture the volume names:
scli --query_all_volumes
3. Extend the volume size using the following command:
scli --modify_volume_capacity --volume_name <volume-name to be modified> --size_gb <volumesize>
4. Execute the following command to identify the extended volume size:
scli --query_all_volumes

Increase the datastore size in VMware vCSA

Use this procedure to increase the datastore size in VMware vCSA.

Steps

1. Log in to VMware vCSA.
2. Click **vSphere Client** > **Storage**.

3. Right-click the respective datastore and click **Increase Datastore Capacity...**
4. Select the diskorlun and verify that the size and volume size are the same.
5. Click **Next > Next > Finish**.
6. Select the datastore with increased capacity, click **Summary**, and verify the capacity.

Configuring replication on PowerFlex nodes

PowerFlex replication provides data protection by mirroring volumes in one system to a remote system asynchronously.

A volume and its remote mirror are called replication consistency groups. A replication consistency group can consist of one or several volumes in a single protection domain that replicate to a remote protection domain. PowerFlex 4.x supports multi-site replication of up to five systems.

Requirements

- PowerFlex Manager must be deployed and configured.
- Replication VLANs must be created on the switches and defined in PowerFlex Manager.

Workflow summary

- Create, publish and deploy storage with replication or hyperconverged template (local and remote)
- Create and copy certificates
- Add peer systems
- Create replication consistency groups

Clone the storage replication template

Use this procedure to clone the storage replication templates.

Steps

1. Log in to PowerFlex Manager.
2. Click **Lifecycle > Templates > Create**.
3. Click **Clone an existing PowerFlex Manager template**.
4. Click **Sample Templates**.
5. From the **Template to be cloned** field, click **Storage - Replication** and click **Next**.
6. Enter a template name.
7. Select or create a new category and enter a description.
8. Select the appropriate compliance version and the appropriate security group and click **Next**.
9. Select the matching customer networks for each category.
10. Under **OS Settings**:
 - a. Select or create (+) the OS credential for the root user.
 - b. Under **Use Compliance File Linux Image**, select **Use Compliance File Linux Image** (or custom if requested).
11. Under **PowerFlex Gateway Settings**, select the appropriate PowerFlex gateway. The default is block-legacy-gateway.
12. Under **Hardware Settings/Node Pool Settings**, select the pool that contains the Replication nodes. The default is Global. Click **Finish**.
13. Under **Node Settings**:
 - a. Click **Node > Modify** and change node count as necessary and select **Continue**.
 - b. Add NTP and time zone information and click **Save**.
14. Under **Network Settings > Static Routes**:
 - a. If routing will be required on the nodes, click **Enabled**.
 - b. Click **Add New Static Route** and select the **Source Network**, **Destination Network**, and enter the gateway to be used for that route.

- c. Click **Finish**.
15. Click **Publish Template**.
16. Click **Yes** on the confirmation dialog.

Deploy storage with replication template

Use this procedure to deploy storage with replication templates.

Steps

1. Click **Lifecycle > Templates**.
2. Select the template created in the previous section.
3. Click **Deploy Resource Group**.
4. Enter the resource group name and a brief description.
5. Select the RCM version.
6. Select the administration group for this resource.
7. Click **Next**.
8. Under Deployment Settings:
 - a. Auto generate or fill out the following fields:
 - Protection domain name
 - Protection domain name template
 - Storage pool name
 - Number of storage pools
 - Storage pool name template
 - b. Let PowerFlex select the IP addresses or manually provide the MDM virtual IP addresses.
 - c. Let PowerFlex select the IP addresses or manually provide the storage-only nodes OS IP addresses.
 - d. Manually select each storage-only node by serial number or iDRAC IP address, or let PowerFlex select the nodes automatically from the selected node pool.
 - e. Click **Next**.
9. Click **Deploy Now > Next**.
10. Review the summary screen and click **Finish**.

Deployment activity can be monitored on right panel under **Recent Activity**.

Clone the hyperconverged replication template

Use this procedure to clone the hyperconverged replication templates.

Steps

1. Log in to PowerFlex Manager.
2. Click **Lifecycle > Templates > Create**.
3. Click **Clone an existing PowerFlex Manager template**.
4. Click **Sample Templates**.
5. From the **Template to be cloned** field, click **Hyperconverged - Replication** and click **Next**.
6. Enter a template name.
7. Select or create a new category and enter a description.
8. Select the appropriate compliance version and the appropriate security group and click **Next**.
9. Select the matching customer networks for each category.
10. Under **OS Settings**:
 - a. Select or create (+) the OS credential for the root user.
 - b. Select or create (+) the SVM OS credential for the root user.
 - c. Under **Use Compliance File ESXi Image**, select **Use Compliance File ESXi Image** (or custom if requested).
11. Under **Cluster Settings**, select the target VMware vCenter.

12. Under **PowerFlex Gateway Settings**, select the appropriate PowerFlex gateway. The default is block-legacy-gateway.
13. Under **Hardware Settings/Node Pool Settings**, select the pool that contains the Replication nodes. The default is Global.
14. Under **Network Settings > Static Routes**:
 - a. If routing will be required on the nodes, click **Enabled**.
 - b. Click **Add New Static Route** and select the **Source Network**, **Destination Network**, and enter the gateway to be used for that route.
 - c. Click **Finish**.
15. Under **Node Settings**:
 - a. Click **Node > Modify** and change node count as necessary and select **Continue**.
 - b. Add NTP and time zone information and click **Save**.
16. Under **VMware Cluster Settings**:
 - a. Select the VMware cluster and click **Modify**.
 - b. Click **Continue**.
 - c. Select or create a new target data center. If it is new, enter a name.
 - d. Select or create a new target cluster. If it is new, enter a name.
 - e. Click **Configure VDS Settings**.
 - f. To create custom port groups, click **User Entered Port Groups** or click **Auto Create All Port Groups** to let PowerFlex Manager provide them.
 - g. Click **Next**.
 - h. Add the VDS name for VDS1, cust_dvswitch.
 - i. Add the VDS name for VDS2, flex_dvswitch.
 - j. Click **Next**.
 - k. Verify network, VLAN ID and portgroup names are as expected and click **Next**.
 - l. Select the MTU size as configured on customer network (or Logical Configuration Survey) and click **Next > Finish**.
 - m. In the confirmation dialogue, click **Yes > Save**.
17. Click **Publish Template** and click **Yes** on the confirmation dialog.

Deploy PowerFlex hyperconverged nodes with replication template

Use this procedure to deploy PowerFlex hyperconverged nodes with replication templates.

Steps

1. Click **Lifecycle > Templates**.
2. Select the template created in the previous section.
3. Click **Deploy Resource Group**.
4. Enter the resource group name and a brief description.
5. Select the RCM version.
6. Select the administration group for this resource.
7. Click **Next**.
8. Under VMware cluster settings, auto generate or fill out the following fields:
 - Data center name
 - Cluster name
 - Storage pool name
 - Number of storage pools
 - Storage pool name template
9. Under **PowerFlex Cluster Settings**:
 - a. Auto generate or fill out the following fields:
 - Protection domain name
 - Protection domain name template
 - Storage pool name
 - Number of storage pools
 - Storage pool name template
 - Set default journal capacity (10%) unless directed differently by Logical Configuration Survey (LCS) or the customer

- b. Let PowerFlex select the IP addresses or manually provide the MDM virtual IP addresses.
 - c. Let PowerFlex select the IP addresses or manually provide the hyperconverged nodes OS IP addresses.
 - d. Let PowerFlex select the IP addresses or manually provide the SVM OS IP addresses.
 - e. Manually select each hyperconverged node by serial number or iDRAC IP address, or let PowerFlex select the nodes automatically from the selected node pool.
 - f. Repeat these steps for each additional node.
 - g. Click **Next**.
10. Click **Deploy Now > Next**.
11. Review the summary screen and click **Finish**.
Deployment activity can be monitored on right panel under **Recent Activity**.

Create and copy certificates

Use this procedure to create and copy certificates.

About this task

You can locate the system ID by logging into the primary MDM by using: `scli --login --username admin --management_system_ip <management_system_ip>`.

Prerequisites

- Deployed storage-only or hyperconverged with replication resource groups at each participating site
- System ID of each participating system

Steps

1. Log in to the primary MDM for each site using SSH to generate, copy and add certificates.
2. Type `scli --login --username admin --management_system_ip <management_system_ip>`, and after the password prompt, enter the PowerFlex Manager password.
3. Extract the certificate for each site, type the following for each site (source and destination): `scli --extract_root_ca --certificate_file /tmp/site-x.crt`.
4. Copy the extracted certificate of the source (primary MDM /tmp folder) to destination (primary MDM /tmp folder) using SCP.
5. Copy the extracted certificate of the destination (primary MDM /tmp folder) to source (primary MDM /tmp folder) using SCP.
6. To add the copied certificate to the source and each destination, type `scli --add_trusted_ca --certificate_file tmp/site-b.crt --comment site-x.crt`.
7. To verify the new certificate, type `scli --list_trusted_ca`.

Create remote consistency groups

Use this procedure to create remove consistency groups.

Prerequisites

- Peer system must be configured
- Source volumes to be replicated

Steps

1. Log in to PowerFlex Manager.
2. Select **Protection > RCGs**.
3. Click **+ Add RCG**.
4. Enter the remove consistency group name.
5. Enter the Recover Point Objective (60 seconds default).
6. Select the source system protection domain.

7. Select the target system and protection domain and click **Next**.
8. Select auto or manual provisioning:

Option	Description
Auto Provisioning (default)	<p>This option is relevant if there are no volumes at the target system.</p> <p>Select the source volumes to protect.</p> <p>The target volumes are automatically created.</p>
Manual Provisioning	<p>This option is relevant if there are volumes at the target system.</p> <p>Select the source volumes to protect.</p> <p>Select the same size volume at the target system to create a pair between the volumes.</p>

9. Click **Next**.
10. Select the source volumes.
11. Select **Target Volume** as thin (default) or thick.
12. Select the target storage pool.
13. Click **Add Pair**.
14. Click **Next**.
15. Optionally, to map a host on the target side:
 - a. Select the target volume.
 - b. Select the target host.
 - c. Click **Map**.
16. Click **Next**.
17. Select **Add and Activate** or **Add** (and activate separately).

i **NOTE:** **Add and Activate** begins replication immediately.

The **Add** function will create the remove consistency group but not start replication. Replication can be deferred until manually activated.

After the volumes begin replication, the final status should be **OK** and the constancy state will be **Consistent** after the initial volume copy completes.

Add peer replication systems

Use this procedure to add peer replication systems.

Prerequisites

- Deployed PowerFlex storage nodes or PowerFlex hyperconverged nodes with replication resource group at each site
- Certificates generated and copied to each participating system

Steps

1. Log in to PowerFlex Manager.
2. Select **Protection > Peer System**.
3. Click **+ Add Peer System**.
4. Enter the following:
 - Peer system name
 - ID
 - IP addresses
5. Click **Add IP for each additional replication IP in the target Replication Group** and click **Add**.
After a few moments the target system should show the state as **Connected**.

Redistribute the MDM cluster using PowerFlex Manager

Redistribute the MDM across clusters to ensure maximum cluster resiliency and availability.

About this task

It is critical that the MDM cluster is distributed across access switches and physical cabinets to ensure maximum resiliency and availability of the cluster. The location of the MDM components should be checked and validated during every engagement and adjusted if found noncompliant with the published guidelines.

When adding new MDM or tiebreaker nodes to a cluster, first place the MDM components on the PowerFlex storage-only nodes (if available). Then, place the components on the PowerFlex hyperconverged nodes.

Use PowerFlex Manager to change the MDM role for a node in a PowerFlex cluster. When adding a node to a cluster, you might want to switch the MDM role from one of the existing nodes to the new node.

You can launch the wizard for reconfiguring MDM roles from the **Lifecycle** page, under the **Resources** tab. The nodes that are listed and the operations available are the same regardless of where you launch the wizard.

Steps

1. Log in to PowerFlex Manager.
2. Click **Lifecycle** > **Resource Groups** and select the resource group to reconfigure the MDM role.
 - a. Click **View Details**.
 - b. Click **More Actions** and click **Reconfigure MDM Roles**.
3. Review the current MDM configuration for the cluster.
4. For each MDM role that you want to reassign, use **Select New Node for MDM Role** to choose the new hostname or IP address. You can reassign multiple roles at a time.
5. Click **Next**. The **Summary** page displays.
6. Type **Change MDM Roles** to confirm the changes.
7. Click **Finish**.

MDM cluster component layouts

This topic provides examples of layouts for MDM components in a PowerFlex rack with two to five cabinets.

The Metadata Manager (MDM) cluster contains the following components:

- Primary MDM 1
- Secondary MDM 2 and 3
- Tiebreaker 1 and 2

When a PowerFlex rack contains multiple cabinets, distribute the MDM components to maximize resiliency.

Distribute the primary MDM, secondary MDMs, and tiebreakers across physical cabinets and access switch pairs to ensure maximum availability of the cluster. When introducing new or standby MDM components into the cluster, make sure you adhere to the MDM redistribution methodology and select your hosts appropriately, so the cluster remains properly distributed across the physical cabinets and access switch pairs.

The following illustrations provide examples of MDM component layouts for two to five cabinets:

- MDM cluster component layout for a two-cabinet PowerFlex rack:

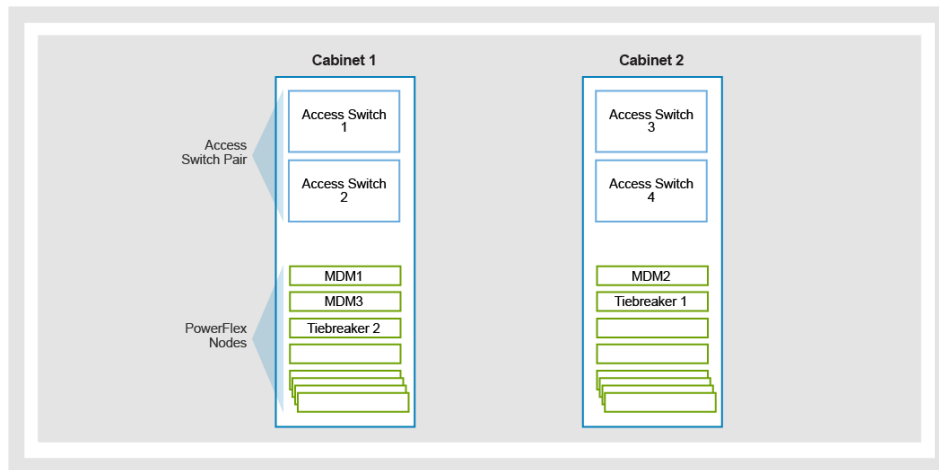


Figure 1.

- MDM cluster component layout for a three-cabinet PowerFlex rack:

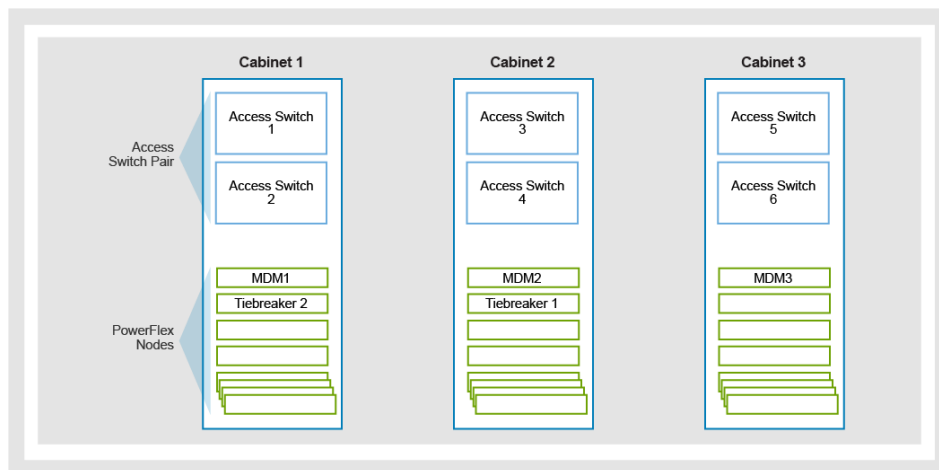


Figure 2.

- MDM cluster component layout for a four-cabinet PowerFlex rack:

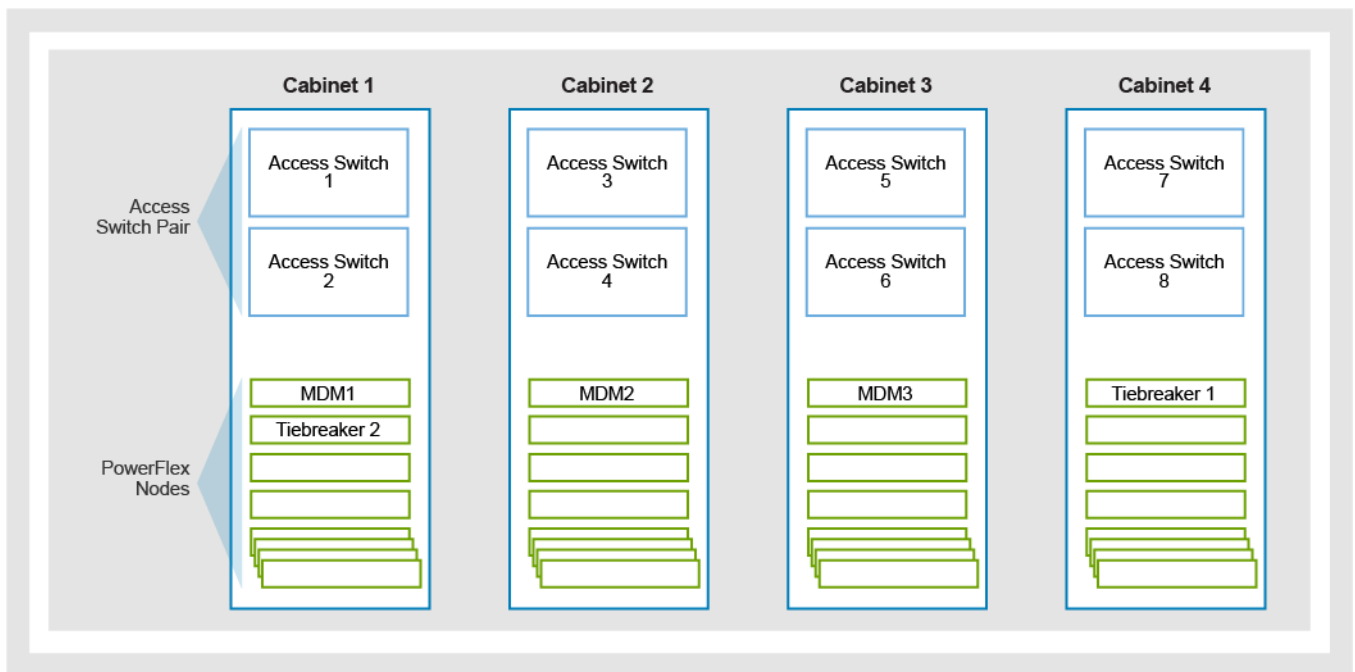


Figure 3.

- MDM cluster component layout for a five-cabinet PowerFlex rack:

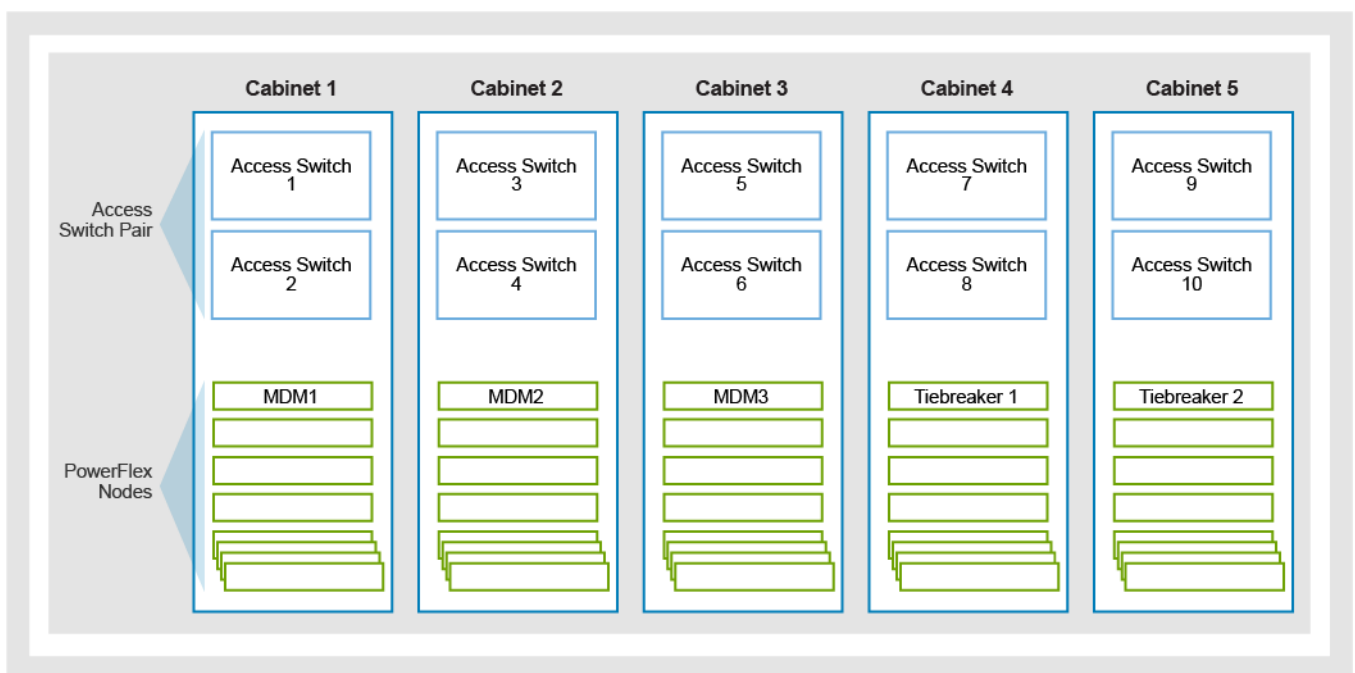


Figure 4.

Redistribute the MDM cluster

Use this procedure to redistribute the MDM cluster manually.

It is critical that the MDM cluster is distributed across access switches and physical cabinets to ensure maximum resiliency and availability of the cluster. The location of the MDM components should be checked and validated during every engagement,

and adjusted if found noncompliant with the published guidelines. If an expansion includes adding physical cabinets and access switches, you should relocate the MDM cluster components.

When adding new MDM or tiebreaker nodes to a cluster, first place the PowerFlex storage-only nodes (if available), followed by the PowerFlex hyperconverged nodes.

Prerequisites

- Identify new nodes to use as MDM or tiebreaker.
- Identify the management IP address, data1 IP address, and data2 IP address (log in to each new node or SVM and enter the `IP addr` command).
- Gather virtual interfaces for the nodes being used for the new MDM or tiebreaker, and note the interface of data1 and data2. For example, for a PowerFlex storage-only node, the interface is bond0.152 and bond1.160. If it is an SVM, it is eth3 and eth4.
- Identify the primary MDM.

Steps

1. SSH to each new node or SVM and assign the proper role (MDM or tiebreaker) to each.
2. Transfer the MDM and LIA packages to the newly identified MDM cluster nodes.

NOTE: The following steps contain sample versions of PowerFlex files as examples only. Use the appropriate PowerFlex files for your deployment.

3. To install the LIA, enter `TOKEN=<flexos password> rpm -ivh EMC-ScaleIO-lia-3.x-x.xxx.el7.x86_64.rpm`.
4. To install the MDM service:
 - For the MDM role, enter `MDM_ROLE_IS_MANAGER=1 rpm -ivh EMC-ScaleIO-mdm-3.x-x.xxx.el7.x86_64.rpm`
 - For the tiebreaker role, enter `MDM_ROLE_IS_MANAGER=0 rpm-ivh EMC-ScaleIO-mdm-3.x-x.xxx.el7.x86_64.rpm`.
5. Open an SSH terminal to the primary MDM and log in to the operating system.
6. Log in to PowerFlex by entering `scli --login --username admin --password <powerflex password>`.
7. Add new standby MDM by entering `scli --add_standby_mdm --mdm_role manager --new_mdm_ip <new_mdm_data1, data2 ip's> --new_mdm_management_ip <mdm management IP> --new_mdm_virtual_ip_interfaces <list both interface, comma seperated> --new_mdm_name <new_mdm name>`.
8. Add a new standby tiebreaker by entering `scli --add_standby_mdm --mdm_role tb --new_mdm_ip <new tb_data1, data2 ip's> --new_mdm_name <new tb name>`.
9. Repeat Steps 7 and 8 for each new MDM and tiebreaker that you are adding to the cluster.
10. Enter `scli --query_cluster` to find the ID for the current MDM and tiebreaker. Note the IDs of the MDM and tiebreaker being replaced.
11. To replace the MDM, enter `scli --replace_cluster_mdm --add_slave_mdm_id <mdm id to add> --remove_slave_mdm_id <mdm id to remove>`.
Repeat this step for each MDM.
12. To replace the tiebreaker, enter `scli --replace_cluster_mdm --add_tb_id <tb id to add> --remove_tb_id <tb id to remove>`.
Repeat this step for each tiebreaker.
13. Enter `scli --query_cluster` to find the IDs for MDMs and tiebreakers being removed.
14. Using IDs to remove the old MDM, enter `scli --remove_standby_mdm --remove_mdm_id <mdm id to remove>`.

NOTE: This step might not be necessary if this MDM remains in service as a standby.

15. To remove the old tiebreaker, enter `scli --remove_standby_mdm --remove_mdm_id <mdm id to remove>`.

NOTE: This step might not be necessary if this tiebreaker remains in service as a standby.

16. Repeat these steps as needed.

Set rebuild and rebalance settings

Define rebuild and rebalance settings before and after RCM upgrades.

Steps

1. On the menu bar, click **Block > Protection Domains**.
2. In the list of protection domains, select the relevant protection domain check box, and click **Modify > Network Throttling**.
3. From the **Set Network Throttling for PD** field, enter the bandwidth for the following settings, or select **Unlimited** to allow for unlimited throughput for that setting:
 - Rebalance throughput limit per SDS
 - Rebuild throughput limit per SDS
 - vTree migration throughput limit per SDS
 - Overall throughput limit per SDS
4. Click **Apply**.
5. Verify that the operation has finished successfully, and click **Dismiss**.
6. Before an RCM upgrade, set the following policies:

Policy settings	Values
Rebuild policy	Unlimited
Rebalance policy	Unlimited
vTree migration policy	Retain the default value
Overall throughput limit per SDS	Limit concurrent I/O=10

7. After an RCM upgrade, set the following policies:


Policy settings	Values
Rebuild policy	Unlimited
Rebalance policy	Unlimited
vTree migration policy	Unlimited
Overall throughput limit per SDS	Unlimited

8. Click **Apply**.

Enabling or disabling SDC authentication

PowerFlex allows authentication and authorization be enabled for all SDCs connected to a cluster. Once authentication and authorization are enabled, older SDC clients and SDCs without a configured password will be disconnected.

The SDC procedures are not applicable for the PowerFlex management cluster.

 **NOTE:** If SDC authentication is enabled in a production environment, data unavailability may occur if clients are not properly configured.

Log in to PowerFlex using scli

The PowerFlex MDM cluster will use mTLS authentication now instead of legacy TLS authentication with username and password.

About this task

Mutual Transport Layer Security (mTLS) is a method for mutual authentication. mTLS ensures that the parties at each end of a network connection are who they claim to be by verifying that they both have the correct private key.

Steps

1. Generate the certificate:
 - a. To copy the management certificate to the root location, type:

```
cp /opt/emc/scaleio/mdm/cfg/mgmt_ca.pem /
```
 - b. To generate the certificate, type `scli --generate_login_certificate --management_system_ip <MNO_IP> --username <USER> --password <PASS> --p12_path <P12_PATH> --p12_password <P12_PASS> --insecure`.
where:
management_system_ip is Ingress IP address and username
username is keycloak username (Ingress UI username)
password is keycloak user password (Ingress UI password). If not provided in the command line then CLI will prompt for it.
--p12_path <P12_PATH> is optional. If not provided then file will be created users home directory
p1_password is the password for p12 bundle. Same password needs to be provided for generation of the certificate and for login operation
2. To add the certificate, type `cd /opt/emc/scaleio/mdm/cfg; scli --add_certificate --certificate_file mgmt_ca.pem`.
3. To log in using the certificate, type `scli --login --p12_path <P12_PATH> --p12_password <P12_PASS>`.

Prepare for storage data clients authentication

Prepare the storage data clients for authentication.

Prerequisites

Ensure that you have the following information:

- Primary and secondary MDM IP address
- PowerFlex cluster credentials

Steps

1. Log in to the primary MDM: `scli --login --username admin --management_system_ip <management_system_ip>`
2. Authenticate with the PowerFlex cluster using the credentials provided.
3. Type `scli --query_all_sdc` and record all the connected SDCs (any of the identifier - NAME, GUID, ID, or IP address):
4. For each SDC in your list, use the identifier recorded to generate and record a CHAP password. Type `scli --generate_sdc_password --sdc_id <id> or --sdc_ip <ip> or --sdc_name <name> or --sdc_guid <guid> --reason "CHAP setup"`.

This password is specific to that SDC and cannot be reused for subsequent SDC entries.

For example:

```
scli --generate_sdc_password --sdc_IP 172.16.151.36 --reason "CHAP setup"
```

Sample output:


```
[root@svml ~]# scli --generate_sdc_password --sdc_ip 172.16.151.36 --reason "CHAP
setup"
Successfully generated SDC with IP 172.16.151.36 password:
AQAAAAAAAAAAAAA8UKVYp0LHCDFD59BrnEXNPVKSlGfLrwAk
```

Configure storage data client to use authentication

Perform this procedure to configure the storage data clients for authentication.

About this task

For each storage data client, populate the generated CHAP password. On a VMware ESXi host, this requires setting a new `scini` parameter through the `esxcli` tool. Use the procedure to perform this configuration change. For Windows and Linux SDC hosts, the included `drv_cfg` utility is used to update the driver and configuration file in real time.

 **NOTE:** Reboot the VMware ESXi hosts for the new parameter to take effect.

Prerequisites

- Generate the pre-shared passwords for all the storage data clients to be configured.
- Ensure that you have the following information:
 - Primary and secondary MDM IP addresses or names
 - Credentials to access all VMware ESXi hosts running storage data clients

Steps


1. Using SSH log in to the VMware ESXi host using the provided credentials.
2. Type **`esxcli system module parameters list -m scini | grep Ioctl`** to list the hosts current `scini` parameters:

```
IoctlIniGuidIdStr          string  d30ff770-b64c-40b5-a341-58d18927e523
                             Ini Guid, for example: 12345678-90AB-CDEF-1234-567890ABCDEF
IoctlMdmIPStr               string
192.168.151.20,192.168.152.20,192.168.153.20,192.168.154.20  Mdms IPs, IPs for MDM in
same cluster should be comma separated. To configure more than one cluster use '+'
to separate between IPs.For Example: 10.20.30.40,50.60.70.80+11.22.33.44. Max 1024
characters
IoctlMdmPasswordStr        string
                             Mdms passwords. Each value
is <ip>-<password>, Multiple passwords separated by ';' signFor example: 10.20.30.40-
AQAAAAAAAAAACSlpIywyOoC5t;11.22.33.44-tppW0eap4cSjsKlCMax 1024 characters
```

 **NOTE:** The third parameter `IoctlMdmPasswordStr` is empty.

3. Using ESXCLI, configure the driver with the existing and new parameters. To specify multiple IP addresses, use a semicolon (;) between the entries, as shown in the following example. Additional data IP addresses, `data3`, and `data4` can be used, if required.

```
esxcli system module parameters set -m
scini -p "IoctlIniGuidIdStr=10cb8ba6-5107-47bc-8373-5bb1dbe6efa3
IoctlMdmIPStr=192.168.151.20,192.168.152.20 IoctlMdmPasswordStr=192.168.151.20-
AQAAAAAAAAA8UKVYp0LHCDFD59BrnExNPvKSlGfLrwAk;192.168.152.20-
AQAAAAAAAAA8UKVYp0LHCDFD59BrnExNPvKSlGfLrwAk bBlkDevIsPdlActive=1
blkDevPdlTimeoutMillis=60000"
```

 **NOTE:** There are spaces between `Ioctl` parameter fields and the opening quotes. The example is entered on a single line.

4. Reboot the VMware ESXi nodes.
The SDC configuration is applied.


If the SDC is a PowerFlex hyperconverged node, go to the next step. For other nodes, continue to Step 8.

5. For PowerFlex hyperconverged nodes, use the presentation manager or scli tool to place the corresponding SDS into maintenance mode.
6. If the SDS is also the cluster primary MDM, switch cluster ownership to a secondary MDM and verify cluster state before proceeding, type **scli --switch_mdm_ownership --mdm_name <secondary MDM name>**.
7. Power off the SVM once the cluster ownership is switched (if needed) and the SDS is in maintenance mode.
8. Manually migrate the workloads to the other hosts if required, and place the VMware ESXi host in maintenance mode.
9. Reboot the VMware ESXi host.
10. Once the host has completed rebooting, remove it from maintenance mode and power on the SVM (if present).
11. Take the SDS out of the maintenance mode (if present).
12. Repeat this procedure for each VMware ESXi SDC host.

Examples - Windows and Linux SDC nodes

Windows and Linux hosts have access to the `drv_cfg` utility, which allows driver modification and configuration in real time.

The `--file` option allows for persistent configuration to be written to the driver's configuration file (so that the SDC remains configured after a reload or reboot).

 **NOTE:** Only one IP address is needed for the command to identify the MDM to modify.

Windows (from within a PowerShell prompt):

```
C:\Program Files\EMC\scaleio\sdsc\bin\drv_cfg --set_mdm_password --ip <MDM IP> --port 6611 --password <secret>
```

Linux:

```
/opt/emc/scaleio/sdc/bin/drv_cfg --set_mdm_password --ip <MDM IP> --port 6611 --password <secret> --file /etc/emc/scaleio/drv_cfg.txt
```

Iterate through the relevant SDCs, using the command examples along with the recorded information.

Enable storage data client authentication

Perform this procedure to enable storage data client authentication.

Prerequisites

- Make sure that all storage data clients are running PowerFlex, and are configured with their appropriate CHAP password. Any older or unconfigured storage data client will be disconnected from the system when authentication is turned on.
- Ensure that you have the following information:
 - Primary MDM IP address
 - Credentials to access the PowerFlex cluster

Steps

1. SSH into the primary MDM.
2. Type **scli --login --username admin --management_system_ip <management_system_ip>** to log in to the PowerFlex cluster using the provided credentials.
3. Type **scli --set_sdc_authentication --enable** to enable storage data client authentication feature.
4. Type **scli --check_sdc_authentication_status** to verify that the storage data client authentication and authorization is on, and that the storage data clients are connected with passwords.

Sample output:

```
[root@svm1 ~]# scli --check_sdc_authentication_status
SDC authentication and authorization is enabled.
Found 4 SDCs.
The number of SDCs with generated password: 4
The number of SDCs with updated password set: 4
```

5. If the number of storage data clients does not match or any storage data clients are disconnected, storage data clients, list any or all of the disconnected storage data clients and then disable the storage data client authentication by typing the following commands:

```
scli --query_all_sdc | grep "State: Disconnected"
```

```
scli --set_sdc_authentication --disable
```
6. Recheck the disconnected storage data clients to make sure that they have the proper configuration applied. If necessary, regenerate their shared password and reconfigure the storage data client. If you are unable to resolve the storage data client disconnection, leave the feature disabled and contact Dell Technologies support as needed.

Disable SDC authentication

Perform this procedure if you need to disable SDC authentication.

Prerequisites

Ensure all SDCs are configured with their appropriate CHAP secret. Any older or unconfigured SDC will be disconnected from the system when authentication is turned on.

You will need the following information:

- Primary MDM IP address
- Credentials to access the PowerFlex cluster

Steps

1. SSH to the primary MDM address.
2. Log in to the PowerFlex cluster using the provided credentials.
3. Disable the SDC authentication, type: `scli --set_sdc_authentication --disable`
Once disabled, SDCs will reconnect automatically unless otherwise configured.

Results

Once disabled, the SDCs reconnect automatically unless otherwise configured.

Expand an existing PowerFlex cluster with SDC authentication enabled

Once a PowerFlex cluster has SDC authentication that is enabled, new SDCs must have the configuration step that is performed after the client is installed. This procedure is not applicable for the PowerFlex management controller 2.0. For Windows PowerFlex compute-only nodes, only firmware upgrades are supported.


Prerequisites

Ensure you have the following information:

- Primary MDM IP address
- Credentials for the PowerFlex cluster
- The IP address of the new cluster members

Ensure you have added the SDC authentication enabled on the PowerFlex cluster.

Steps

1. Install and add the SDCs as per normal procedures (whether using PowerFlex Manager or manual expansion process).
 **NOTE:** New SDCs will show as **Disconnected** at this point, as they cannot authenticate to the system.
2. SSH to the primary MDM.
3. Log in to the PowerFlex cluster using the scli tool.
4. For each of your newly added SDCs, generate and record a new CHAP secret, type: `scli --generate_sdc_password --sdc_IP <IP of SDC> --reason "CHAP setup - expansion."`

5. SSH and log in to the SDC host.
6. If the new SDC is a VMware ESXi host, follow the rest of this procedure.
7. Type **-m scini | grep Ioctl** and **esxcli system module parameters list -m scini** to list the current scini parameters of the host.
8. Using esxcli, type **esxcli system module parameters set -m scini -p** to configure the driver with the existing and new parameters.
For example, **esxcli system module parameters set -m scini -p "IoctlIniGuidStr=09bde878-281a-4c6d-ae4f-d6ddad3c1a8f IoctlMdmIPStr=10.234.134.194,192.168.152.199,192.168"**.
9. At this stage, the SDC's configuration is ready to be applied. On ESXi nodes a reboot is necessary for this to happen. If the SDC is a hyperconverged node, proceed with step 10. Otherwise, go to step 12.
10. For PowerFlex hyperconverged nodes, use the presentation manager or scli tool to place the corresponding SDS into maintenance mode.
11. Once the SDS is in maintenance mode, the SVM may be powered off safely.
12. Place the ESXi host in maintenance mode. No workloads should be running on the node, as we have not yet configured the SDC.
13. Reboot the ESXi host.
14. Once the host has completed rebooting, remove it from maintenance mode and power on the SVM (if present).
15. Take the SDS out of maintenance mode (if present).
16. Repeat steps 5 through 15 for all ESXi SDC hosts.

Add a Windows or Linux authenticated SDC

Use the **drv_cfg** utility on a Windows or Linux machine to modify both a running and persistent configuration. Use the following examples to perform the task on a Windows or Linux based PowerFlex node.

About this task

For Windows PowerFlex compute-only nodes, only firmware upgrades are supported.

Prerequisites

Only one IP address is required for the command to identify the MDM to modify.

Steps

1. Press Windows +R.
2. To open the command line interface, type **cmd**.
3. For Windows, type **drv_cfg --set_mdm_password --ip <MDM IP>** in the drv_cfg utility. For example:
drv_cfg --set_mdm_password --ip <MDM IP> --port 6611 --password <secret>
4. For Linux, type **/opt/emc/scaleio/sdc/bin/drv_cfg --set_mdm_password --ip <MDM IP>**. For example:
/opt/emc/scaleio/sdc/bin/drv_cfg --set_mdm_password --ip <MDM IP> --port 6611 --password <secret> --file /etc/emc/scaleio/drv_cfg.txt
5. Repeat until all new SDCs are connected.

PowerFlex file storage

PowerFlex file uses virtualized file servers that are called NAS servers. A NAS server contains the configuration, interfaces, and environmental information that is used to facilitate access to the file systems.

File storage is managed through NAS servers, which must be created prior to creating file systems. NAS servers can be created to support SMB protocol, NFS protocol, or both. Once NAS servers are created, you can create file systems as containers for your SMB shares for Windows users, or NFS exports for UNIX users.

A file system represents set of storage resources that provide network file storage. The storage system establishes a file system that Windows users or Linux/UNIX hosts can connect to and use for file-based storage. Users access a file system through its shares, which draw from the total storage that is allocated to the file system.

Multitenancy

NAS servers can be used to enforce multitenancy. This is useful when hosting multiple tenants on a single system, such as for service providers. Since each NAS server has its own independent configuration, it can be tailored to the requirements of each tenant without impacting the other NAS servers on the same appliance. Also, each NAS server is logically separated from each other, and clients that have access to one NAS server do not inherently have access to the file systems on the other NAS servers. File systems are assigned to a NAS server upon creation and cannot be moved between NAS servers.

High availability

New NAS servers are automatically assigned on a round-robin basis across the available nodes. The primary node acts as a marker to indicate the node that the NAS server should be running on, based on this algorithm. Once provisioned, the primary node for a NAS server never changes. Backup node, on which the NAS server is backed up for fault tolerance purposes. This means that the NAS server will be moved to this node during any failover event, the node is chosen during NAS server creation by automatic load balancing logic.

PowerFlex file capabilities

NAS server

NAS servers provide access to file systems. Each NAS server supports Windows (SMB) file systems, Linux/UNIX (NFS) exports, or both.

To provide isolated access to a file system, you can configure a NAS server to function as independent file server with server-specific DNS, NIS, and other settings. The IP address of the NAS server provides part of the mount point that users and hosts use to map to the file system storage resource, with the share name providing the rest. Each NAS server exposes its own set of file systems through the file system share, either SMB or NFS.

Once a NAS server is running, you can create and manage file systems and shares on that NAS server.

You can create file system only if there is a NAS server running on the storage system. The types of file systems that you can create are determined by the file sharing protocols (SMB, NFS, or multiprotocol) enabled for the NAS server.

Create a NAS server for NFS (UNIX-only) file systems



Create NAS servers before creating file systems.

Prerequisites

Have the NAS network information available.

Steps

1. Log in to PowerFlex Manager.
2. Click **File > NAS Servers**.
3. Click **Create**, and enter the information in the wizard.

Wizard screen fields	Description
Details	Select NAS Protection Domain from drop down, enter a NAS Server name, description, and network information.  NOTE: You cannot reuse VLANs that are being used for the management and storage networks.
Sharing protocol	Select sharing protocol: Select NFSv3, or NFSv4, or both.  NOTE: If you select SMB and an NFS protocol, you automatically enable the NAS server to support multiprotocol. Unix directory services: (naming services) You can configure the naming services with a combination of Local Files and NIS, or LDAP. You can choose to enable Secure NFS here. Secure NFS requires the following: <ul style="list-style-type: none">• At least one NTP server must be configured to synchronize the date and time. It is recommended that you set up a minimum of two NTP servers per domain to avoid a single point of failure.• A UNIX Directory Service (UDS)• One or more DNS servers• Either an AD or custom realm must be added for Kerberos authentication• A keytab file must be uploaded to your NAS server when using a custom realm in a Kerberos configuration. DNS: DNS information is mandatory when: <ul style="list-style-type: none">• Joining an AD domain, but optional for a stand-alone NAS server.• Configuring Secure NFS.• DNS can also be used to resolve hosts defined on NFS export access lists. User mapping: To enable user mapping, select how Unix users will be mapped to Windows users, and select the Unix Directory Search Order.
Summary	Review the content. Select Back to make corrections.

4. Click **Create NAS Server**.

The **Status** window opens, and you are redirected to the **NAS Servers** page once the server is listed on the page. Once you have created the NAS server for NFS, you can continue to configure the server settings. If you enabled Secure NFS, you must continue to configure Kerberos.



Select the NAS server to continue to configure, or edit the NAS server settings.

Create NAS server for SMB (Windows-only) file systems

Create a NAS server before creating file systems.



Prerequisites

Gather the following information:

- Ethernet port, IP Address, Subnet Mask/Prefix Length, Gateway information for the NAS Server.
 **NOTE:** IP address and subnet mask/prefix length are mandatory.
- VLAN identifier, if the switch port supports VLAN tagging.
 **NOTE:** You cannot reuse VLANs that are being used for the management and storage networks.
- If you are configuring a stand-alone NAS server, obtain the workgroup and NetBIOS name. Then define what to use for the stand-alone local administrator of the SMB server account.
- If you are joining the NAS server to the Active Directory (AD), ensure that NTP is configured on your storage system. Then obtain the SMB system name (used to access SMB shares), Windows domain name, and the username and password of a domain administrator or user who has a sufficient domain access level to join the AD.

Steps

1. Log in to PowerFlex Manager.
2. Click **File > NAS Servers**.
3. Click Create and enter the information in the wizard.

Wizard screen fields	Description
Details	Select NAS Protection Domain from drop-down, enter a NAS Server name, description, and network information.  NOTE: You cannot reuse VLANs that are being used for the management and storage networks.
Sharing protocol	Select sharing protocol: Select SMB .  NOTE: If you select SMB and an NFS protocol, you automatically enable the NAS server to support multiprotocol. Windows server settings: Select Standalone to create a stand-alone SMB server or Join to the Active Directory Domain to create a domain member SMB server. If you join the NAS server to the AD, optionally select Advanced to change the default NetBios name and organizational unit. DNS: If you selected to Join to the Active Directory Domain , it is mandatory to add a DNS server. Optionally, enable DNS if you want to use a DNS server for your stand-alone SMB server. User mapping: The User Mapping page displays if you have selected to join the active directory domain. Keep the default Enable automatic mapping for unmapped Windows accounts/users to support joining the active directory domain. Automatic mapping is required when joining the active directory domain.
Summary	Review the content. Select Back to make corrections.

4. Click **Create NAS Server**.

The **Status** window opens, and you are redirected to the **NAS Servers** page once the server is listed on the page. Once you have created the NAS server for SMB, you can continue to configure the server settings, or create file systems.


Select the NAS server to continue to configure, or edit the NAS server settings.

Change NAS server settings

Change NAS server configuration settings, modify the NAS server properties, delete the NAS server, or move a NAS server from one node to the other in the same appliance.

Steps

1. Log in to PowerFlex Manager.
2. Click **File > NAS Server**.
3. Select a NAS server using the check box, and select one of the following options to make changes to the NAS server configuration settings:
 - a. **Modify:** Modify the NAS server name or description.
 - b. **More Actions:**
 - **Remove:** To remove the NAS server from the system. This option is not available if file systems have been created on the NAS server. You will need to remove all file systems from the NAS server before it can be removed. If the SMB server is joined to the active directory, first unlink the SMB server from the active directory domain.
 - **Move NAS Server:** To move the NAS server from one node to the other node.

 **NOTE:** The new primary node cannot be the current back up node, and the new backup node cannot be current primary node.
 - **Swap Nodes:** Swap NAS primary and backup nodes.

Configure settings of an existing NAS server

Select the NAS server name to get to the details for a specific server. You can add, modify, and delete NAS server settings from the NAS server details page.

The following rules apply to changing NAS server settings:

- You cannot disable multiprotocol file sharing for a NAS server once a file system is created on that NAS server.
- You cannot disable DNS for:
 - NAS servers that support multiprotocol file sharing.
 - NAS servers that support SMB file sharing and that are joined to an Active Directory (AD).
- To reconfigure a NAS server that supports SMB-only or NFS-only file systems so that it supports multiprotocol (both types of file systems simultaneously), first enable a UNIX Directory Service and DNS server for that NAS server.
- If you choose to change from an AD realm to a custom realm after the NAS server is successfully created with Secure NFS you will not be able to create any NFS exports until you perform the following operations:
 1. Create a keytab file.
 2. Remove the AD realm from the NAS server.
 3. Enter the username and password for the AD server.
 4. Enter the custom realm.
 5. Upload the keytab file.

Manage the network routes between the NAS server and the supported external services

Use this procedure to add production and backup file interfaces to a NAS server, and create routes to external services.

About this task

You can add more interfaces and define which will be the preferred interface to use with the NAS server. PowerFlex file assigns a preferred interface by default, but you can set which interface to use first for production and backup. Select **Ping** and enter

an IP address or host name to test the connectivity from the NAS server to an external resource. All properties of the file interface can be modified.

You can add, modify, and delete the network routes between the NAS server and the supported external services. The Destination is the IP address of the external service.

Steps

1. Log in to PowerFlex Manager.
2. For file interfaces, click **File > NAS Servers**. Select the NAS server and click **View Details > Network > File Interface**, and select from the following:

Option	Description
Add	Enter network information.
Modify	Modify file interface IP address, subnet mask/prefix length, gateway and VLAN ID.
Delete	Delete the file interface.
Ping	Ping the IP address or hostname.
Preferred interface	Select the current preferred interface.

3. For routes to external services, **File > NAS Servers**. Select the NAS server and click **View Details > Network > Routes to External Services**, and select from the following:

Option	Description
Add	Enter network information.
Modify	Modify static route values like gateway, destination, and prefix length.
Delete	Delete the route.

Modify or configure the NAS server naming services

Use this procedure to modify or configure naming services.


About this task

Modify or configure the following naming services for the selected NAS server:

- DNS: DNS is required for Secure NFS.
You cannot disable DNS for:
 - NAS servers that support multiprotocol file sharing.
 - NAS servers that support SMB file sharing and that are joined to an Active Directory (AD).
- UDS with NIS: You will need the NIS domain name and the IP addresses of each of the NIS servers.
- UDS with LDAP: LDAP must adhere to the IDMU, RFC2307, or RFC2307bis schemas. Some examples include AD LDAP with IDMU, iPlanet, and OpenLDAP. The LDAP server must be configured properly to provide UIDs for each user. For example, on IDMU, the administrator must go in to the properties of each user and add a UID to the UNIX Attributes tab. You can configure LDAP to use anonymous, simple, and Kerberos authentication.

LDAP authentication types:

Authentication type	Description
Anonymous	Specify the base DN, and the profile DN for the iPlanet/OpenLDAP server.
Simple	Specify the following: <ul style="list-style-type: none">◦ If using AD, LDAP/IDMU:

Authentication type	Description
	<ul style="list-style-type: none"> ▪ Bind DN in LDAP notation format ▪ Base DN ▪ Profile DN ○ If using the iPlanet/OpenLDAP server: <ul style="list-style-type: none"> ▪ Bind DN in LDAP notation format ▪ Password ▪ Base DN ▪ Profile DN for the iPlanet/OpenLDAP server
Kerberos	<p>To use Kerberos authentication, you must perform the following steps before setting LDAP to use Kerberos authentication:</p> <ol style="list-style-type: none"> 1. From the Naming Services card, configure the DNS server used to join and unjoin a Kerberos server to a realm. 2. From the Security card, configure the Kerberos realm. <p>There are two methods for configuring Kerberos:</p> <ul style="list-style-type: none"> ○ Authenticate to the SMB domain. With this option, authenticate using either the SMB server account or authenticate with other credentials. ○ Configure a custom realm to point to any type of Kerberos realm. With this option, the NAS server uses the custom Kerberos realm defined in the Kerberos subsection of the NAS server Security tab. <p> NOTE: If you use NFS secure with a custom realm, you have to upload a keytab file.</p>

- **Local files:** Local files can be used instead of, or in addition to DNS, LDAP, and NIS directory services. To use local files, configuration information must be provided through the files listed in PowerFlex Manager. If you have not created your own files ahead of time, use the download arrows to download the template for the type of file you need to provide, and upload the edited version.

To use local files for NFS, FTP access, the passwd file must include an encrypted password for the users. This password is used for FTP access only. The passwd file uses the same format and syntax as a standard Unix system, so you can leverage this to generate the local passwd file. On a Unix system, use `useradd` to add a new user and `passwd` to set the password for that user. Copy the hashed password from the `/etc/shadow` file, add it to the second field in the `/etc/passwd` file, and upload the `/etc/passwd` file to the NAS server.

- **User mapping:** If you are configuring a NAS server to support both types of protocols, SMB and NFS, you will need to configure the user mapping. When configured for both types of protocol, the user mapping requires that the NAS server is joined with an AD domain. You can configure the SMB server, with AD from the SMB Server card.

If the **Windows Server Type** is set to **Join to the Active Directory Domain**, you must select **Enable automatic mapping for unmapped Windows accounts/users**.

Steps

1. Log in to PowerFlex Manager.
2. For DNS, click **File > NAS Servers**, and select the NAS server. Click **View Details > Naming Services > DNS Server**. Click the **Disabled** button to **Enable** and click **DNS Transport protocol** drop-down menu and select **Protocol**. Enter the domain, the IP address(es), click **Add** and click **Apply**.
3. For UDS with NIS, click **File > NAS Servers**, and select the NAS server. Click **View Details > Naming Services > UDS** and click **Unix Directory Service: NIS**. Enter the domain, the IP address, click **Add**, and click **Apply**.
4. For UDS with LDAP, click **File > NAS Servers**, and select the NAS server. Click **View Details > Naming Services > UDS**, click the **Disabled** button to **Enable**, and click **Unix Directory Service: LDAP**. Enter the port number, IP address, click **Add**, and enter the base DN, select the Authentication from the drop-down menu and click **Apply**.
5. For local files, click **File > NAS Servers**, and select the NAS server. Click **View Details > Naming Services**, and click **Local Files > Upload Local Files**. From the **Upload Local Files** window, select the file type, choose the file to upload and click **Open > Upload**.

6. For user mapping, click **File > NAS Servers**, and select the NAS server. Click **View Details > Naming Services**, and click **User Mapping**. Select **Enable automatic mapping for unmapped Windows accounts/users**, select **Unix Directory Service Search Order** and click **Apply**.

NAS server sharing protocols

SMB Server

Contains options for configuring a Windows server.



If you will be configuring SMB with Kerberos security, you must select to Join to the Active Directory Domain.

If you select to Join to the Active Directory Domain, you must have added a DNS server. You can add a DNS server from the Naming Services card.

If the Windows Server Type is set to Join to the Active Directory Domain, then Enable automatic mapping for unmapped Windows accounts/users must be selected in the User Mapping tab.

NFS Server

Contains options for configuring an NFS, or NFS secure server for Unix support.

Task	Description
Extend the Unix credential to enable the storage system to obtain more than 16 group GIDs	Select or clear Enable extended Unix credentials. <ul style="list-style-type: none">• If this field is selected, the NAS server uses the User ID (UID) to obtain the primary group ID (GID) and all group GIDs to which it belongs. The NAS server obtains the GIDs from the local password file or UDS.• If this field is cleared, the Unix credential of the NFS request is directly extracted from the network information contained in the frame. This method has better performance, but is limited to including up to only 16 group GIDs. <p> NOTE: With secure NFS, the Unix credential is always built by the NAS server, so this option does not apply.</p>
Specify a Unix credential cache retention period	In the Credential cache retention field, enter a time period (in minutes) for which access credentials are retained in the cache. The default value is 15 minutes, the minimum value is 1 minute and the maximum is 1439 minutes. <p> NOTE: This option can lead to better performance, because it reuses the Unix credential from the cache instead of building it for each request.</p>

You can configure Secure NFS when you create or modify a multiprotocol NAS server or one that supports Unix-only shares. Secure NFS provides Kerberos-based user authentication, which can provide network data integrity and network data privacy. There are two methods for configuring Kerberos for secure NFS:

- Use the Kerberos realm (Windows realm) associated with the SMB domain configured on the NAS server, if any. If you configure secure NFS using this method, SMB support cannot be deleted from the NAS server while secure NFS is enabled and configured to use the Windows realm.
- Configure a custom realm to point to any type of Kerberos realm. If you configure secure NFS using this method, you must upload the keytab file to the NAS server being defined.

FTP

FTP or Secure FTP can only be configured after a NAS server has been created.

Passive mode FTP is not supported.

FTP access can be authenticated using the same methods as NFS or SMB. Once authentication is complete, access is the same as SMB or NFS for security and permission purposes. The method of authentication used depends on the format of the username:

- If the format is domain@user or domain\user, SMB authentication is used. SMB authentication uses the Windows Domain Controller.
- For any other single username format, NFS authentication is used. NFS authentication uses local files, LDAP, NIS, or local files with LDAP or NIS.

To use local files for NFS, FTP access, the passwd file must include an encrypted password for the users. This password is used for FTP access only. The passwd file uses the same format and syntax as a standard Unix system, so you can leverage this to generate the local passwd file. On a Unix system, use useradd to add a new user and passwd to set the password for that user. Then, copy the hashed password from the /etc/shadow file, add it to the second field in the /etc/passwd file, and upload the /etc/passwd file to the NAS server.

Configure NAS server sharing protocols

Steps

1. Log in to PowerFlex Manager.
2. To configure SMB:
 - a. Click **File > NAS Servers** and select the NAS server.
 - b. Click **View Details > Sharing Protocols > SMB Server**.
 - c. Click the Disabled button to enable, select Windows Server Type and enter the options per server type:
 - Standalone: Workgroup, Netbios name, Description (optional), Administrator Password
 - Join to the Active Directory Domain: SMB Computer Name, SMB Computer Description (optional), Windows Domain, Domain Username and Password
 - d. Click **Apply**.
3. To configure NFS server:
 - a. Click **File > NAS Servers** and select the NAS server.
 - b. Click **View Details > Sharing Protocols > NFS Server**.
 - c. Click the Disabled button to enable, enter the hostname, click Disabled to enable Extended Credentials, and enter the credential cache retention period.
 - d. Click **Apply**.
4. To configure FTP:
 - a. Click **File > NAS Servers** and select the NAS server.
 - b. Click **View Details > Sharing Protocols > FTP**.
 - c. Click the Disabled button to enable FTP/SFTP, select FTP/SFTP Access, and click **Apply**.

NAS server protection and events

Enable Network Data Management Protocol (NDMP) for the file servers using NDMP.

About this task

The Network Data Management Protocol (NDMP) provides a standard for backing up file servers on a network. Once NDMP is enabled, a third-party Data Management Application (DMA), such as Dell Networker, can detect the PowerFlex NDMP using the NAS server IP address.

The NDMP username is always ndmp.

Steps

1. Log in to PowerFlex Manager.
2. Click **File > NAS Servers** and select the NAS server.
3. Click **View Details > Protection and Events**.
4. Click the Disabled button to enable NDMP backup, enter the username and password, and click **Apply**.

Managing NAS server configuration

Events Publishing allows third-party applications to register to receive event notification and context from the storage system when accessing file systems by using the SMB or NFS protocols. The Common Event Publishing Agent (CEPA) delivers to the application both event notification and associated context in one message. Context may consist of file metadata or directory metadata that is needed for business policy.

You must define at least one event option (pre-, post-, or post-error event) when Events Publishing is enabled.

- Pre-event notifications are sent before processing an SMB or NFS client request.
- Post-event notifications are sent after a successful SMB or NFS client request.
- Post-error event notifications are sent after a failed SMB or NFS client request.

Attributes	Description
NAS server	Identifies the associated NAS server.
Enabled	Identifies whether Events Publishing is enabled on the NAS Server. Valid values are: <ul style="list-style-type: none">• yes• no (default)
Pre-event failure policy	The policy applied when a pre-event notification fails. Valid values are: <ul style="list-style-type: none">• ignore (default)—Indicates that when a pre-event notification fails, it is acknowledged as being successful.• deny—Indicates that when a pre-event notification fails, the request of the SMB or NFS client is not performed by the storage system. The client receives a 'denied' response.
Post-event failure policy	The policy applied when a post-event notification fails. The policy is also applied to post-error events. Valid values are: <ul style="list-style-type: none">• ignore (default)—Continue and tolerate lost events.• accumulate—Continue and use a persistence file as a circular event buffer for lost events.• guarantee—Continue and use a persistence file as a circular event buffer for lost events until the buffer is filled, and then deny access to file systems where Events Publishing is enabled.• deny—On CEPA connectivity failure, deny access to file systems where Events Publishing is enabled.
HTTP port	The HTTP port number used for connectivity to the CEPA server. The default value is 12228. The HTTP protocol is used to connect to CEPA servers. It is not protected by a username or password.
HTTP enabled	Identifies whether connecting to CEPA servers by using the HTTP protocol is enabled. When enabled, a connection by using HTTP is tried first. If HTTP is either disabled or the connection fails, then connection through the MS-RPC protocol is tried if all CEPA servers are defined by a fully qualified domain name (FQDN). When an SMB server is defined in a NAS server in the Active Directory (AD) domain, the NAS server's SMB account is used to make an MS-RPC connection. Valid values are: <ul style="list-style-type: none">• yes(default)• no
Username	When using the MS-RPC protocol, you must provide the name of a Windows user allowed to connect to CEPA servers.
Password	When using the MS-RPC protocol, you must provide the password of the Windows user that is defined by the username.
Heartbeat	Time interval (in seconds) between scanning CEPA servers to detect their online or offline status. The default is 10 seconds. The range is from 1 through 120 seconds.

Attributes	Description
Timeout	Time in milliseconds (millisecond) to determine whether a CEPA server is offline. The default is 1,000 millisecond. The range is from 50 millisecond through 5,000 millisecond.
Health state	Health state of Events Publishing. The health state code appears in parentheses. Valid values are: <ul style="list-style-type: none"> OK (5)—The Events Publishing service is operating normally. OK_BUT (7)—Some CEPA servers configured for the NAS server cannot be reached. Minor failure (15)—The Events Publishing service is not functional. Major failure (20)—All CEPA servers configured for the NAS server cannot be reached.

Managing CEPA pool configuration

Event pools configure the types of events published by the NAS Server, and the addresses of CEPA servers.

Events Publishing must be enabled for both the NAS server and the file system. Certain types of events can be enabled for either the NFS protocol, the SMB protocol, or both NFS and SMB on a file system basis.

Attributes	Description
Pre-events	Lists the selected pre-events. The NAS server sends a request event notification to the CEPA server before an event occurs and processes the response. The valid events are defined in the table that follows.
Post-events	Lists the selected post-events. The NAS server sends a notification after an event occurs. The valid events are defined in the table that follows.
Post-error events	Lists the selected post-error events. The NAS server sends notification after an event generates an error. The valid events are defined in the table that follows.

Attributes	Definition	Protocol
OpenFileNoAccess	Sends a notification when a file is opened for a change other than read or write access (for example, read or write attributes on the file).	<ul style="list-style-type: none"> SMB/CIFS NFS (v4)
OpenFileRead	Sends a notification when a file is opened for read access.	<ul style="list-style-type: none"> SMB/CIFS NFS (v4)
OpenFileReadOffline	Sends a notification when an offline file is opened for read access.	<ul style="list-style-type: none"> SMB/CIFS NFS (v4)
OpenFileWrite	Sends a notification when a file is opened for write access.	<ul style="list-style-type: none"> SMB/CIFS NFS (v4)
OpenFileWriteOffline	Sends a notification when an offline file is opened for write access.	<ul style="list-style-type: none"> SMB/CIFS NFS (v4)
OpenDir	Sends a notification when a directory is opened.	SMB/CIFS
FileRead	Sends a notification when a file read is received over NFS.	NFS (v3/v4)
FileWrite	Sends a notification when a file write is received over NFS.	NFS (v3/v4)
CreateFile	Sends a notification when a file is created.	<ul style="list-style-type: none"> SMB/CIFS NFS (v3/v4)
CreateDir	Sends a notification when a directory is created.	<ul style="list-style-type: none"> SMB/CIFS NFS (v3/v4)
DeleteFile	Sends a notification when a file is deleted.	<ul style="list-style-type: none"> SMB/CIFS

Attributes	Definition	Protocol
		<ul style="list-style-type: none"> NFS (v3/v4)
DeleteDir	Sends a notification when a directory is deleted.	<ul style="list-style-type: none"> SMB/CIFS NFS (v3/v4)
CloseModified	Sends a notification when a file is changed before closing.	<ul style="list-style-type: none"> SMB/CIFS NFS (v3/v4)
CloseUnmodified	Sends a notification when a file is not changed before closing.	<ul style="list-style-type: none"> SMB/CIFS NFS (v3/v4)
CloseDir	Sends a notification when a directory is closed.	SMB/CIFS
RenameFile	Sends a notification when a file is renamed.	<ul style="list-style-type: none"> SMB/CIFS NFS (v3/v4)
RenameDir	Sends a notification when a directory is renamed.	<ul style="list-style-type: none"> SMB/CIFS NFS (v3/v4)
SetAclFile	Sends a notification when the security descriptor (ACL) on a file is changed.	SMB/CIFS
SetAclDir	Sends a notification when the security descriptor (ACL) on a directory is changed.	SMB/CIFS
SetSecFile	Sends a notification when a file security change is received over NFS.	NFS (v3/v4)
SetSecDir	Sends a notification when a directory security change is received over NFS.	NFS (v3/v4)

Limits

- One event pool can have maximum of five CEPA server addresses.
- One event publisher can have a maximum of three event pools.
- One NAS server can have only one event publisher associated with it.

NAS server settings

PowerFlex Manager allows you to configure a Common Event Publishing Agent (CEPA) configuration for NAS servers to receive event notifications. CEPA is a part of the Dell Common Event Enabler (CEE) package, which runs on Windows or Linux servers. The CEE framework is used to provide a working environment for the CEPA facility. It consists of two parts—Common Antivirus Agent (CAVA) and CEPA.

CEPA includes the following subfacilities:

- Auditing**—A mechanism for delivering postevents to registered consumer applications in a synchronous manner. Events are delivered individually in real-time.
- Backup**—A mechanism for delivering postevents in bulk mode to backup applications. A backup-specific delivery cadence is based on either a time period or a number of events.
- Content or quota management (CQM)**—A mechanism for delivering preevents to registered consumer applications in a synchronous manner. Events are delivered individually in real-time, allowing the consumer application to exercise business policy on the event.
- Indexing**—A mechanism for delivering events to Splunk Enterprise or the Splunk Cloud in asynchronous mode. The delivery cadence is based on either a time period or a number of events.
- MessageExchange**—A mechanism for delivering postevents in asynchronous mode, when needed, without consumer use of the CEPA API. Events are published from CEPA to the RabbitMQ CEE_Events exchange. A consumer application creates a queue for itself in the exchange from which it can retrieve events.
- Common Asynchronous Publishing Service (VCAPS)**—A mechanism for delivering postevents in asynchronous mode. The delivery cadence is based on a time period or a number of events.

NOTE: If both CQM events and Auditing events are present, CEPA delivers events to the CQM application first, and then delivers events to the Auditing application.

For more information about CEE CEPA, see *Using the Common Event Enabler* on www.dell.com/support.

CEPA is a mechanism where applications can register to receive event notification and context from the PowerFlex file system. The event publishing agent delivers the event notification and associated context in one message to the consumer application. The context may consist of file metadata or directory metadata that is needed to decide business policy.

You can associate CEPA configurations with NAS servers through event publishers. The event publishers can be grouped in event publisher pools.

Event publishers

The events publisher specifies one to three publishing pools and enables configuration of advanced settings.

- Pre-Events Failure Policy—Determines the pre-event behavior if PowerFlex File cannot reach the CEPA Server.
 - Ignore (default)—Consider preevents acknowledged when CEPA servers are offline.
 - Deny—Deny user access when a corresponding pre-event request to CEPA servers failed.
- Post-Events Failure Policy—Determines the post-event behavior if PowerFlex File cannot reach CEPA Server.
 - Ignore—Continue and tolerate lost events.
 - Accumulate (default)—Continue and persist lost events in an internal buffer.
 - Guarantee—Persist lost events, deny file systems access when the buffer is full.
 - Deny—Deny access to file systems when CEPA servers are offline.
- Connectivity and protocol settings
 - HTTP and Port—HTTP and 12228, by default
 - Microsoft RPC and Accounts—Enabled and SMB, by default
 - Heartbeat and Timeout—10 sec and 1000 millisecond, by default

In the **Event Publishers** tab, you can create, modify, delete, associate, or dissociate CEPA event publishers.

Event publishing pools

The publishing pool specifies which events must trigger notifications and to which servers they must be sent. There can be up to five CEPA servers. These servers can be specified by IPv4 address or FQDN. The available events fall into three categories:

- Pre-Events—When an operation is requested, the NAS server sends a notification and waits for approval before allowing the operation to occur.
- Post-Events—NAS server sends a notification after an operation occurs.
- Post-Error-Events—NAS server sends a notification if an operation generates an error.

Creating event publisher pools

To configure CEPA, you must create a publishing pool and events publisher.

About this task

The publishing pool specifies which events must trigger notifications and the servers to which the notifications must be sent.

Steps

1. Go to **File > NAS Servers > NAS Settings > Publishing Pools**.
2. Click **Create**.
The **Create Events Publishing Pool** window is displayed.
3. Enter a name and an FQDN or IP for the publishing pool.
4. Click **Next** to select the preevents for which you want the notifications.
5. Click **Next** to select the postevents.
6. Click **Next** to select the post-error-events.
7. Click **Finish** to save the publishing pool.

Deleting publishing pools

Prerequisites

Before deleting the CEPA publishing pools, ensure that the event publishers that are associated with the CEPA pool are deleted first.


Steps

1. Go to **File > NAS Servers > NAS Settings > Publishing Pools**
2. Select the check box next to the publishing pool that you want to delete.
3. Click **Delete**.
A message to confirm the deletion is displayed.
4. Click **OK** to confirm.

Creating event publishers

Steps

1. Go to **File > NAS Servers > NAS Settings > Event Publishers**.
2. Click **Create**.
The **Create Events Publisher** window is displayed.
3. Enter a name for the event publisher.
4. In the list of publishing pools displayed below, select the check box next to the publishing pool name you want to add to the event publisher.
You can add only three publishing pools to an event publisher.
5. Click **Next**.
6. In the **Configure Events Publisher** tab, select the required Pre-Events Failure and Post-Events Failure policies.
7. Ensure that the default value for HTTP port is 12228, Heartbeat is 10 seconds, and Timeout is 1000 milliseconds.
8. Select the **Using SMB Server Account** and click **Create Event Publisher**.

 **NOTE:** If Microsoft RPC is selected and the NAS server is a stand-alone SMB server, set the custom user account. Otherwise, the CEPA connectivity fails.

Associating event publishers with NAS servers

Prerequisites


Ensure that the NAS server is SMB enabled to associate an event publisher file with it.

About this task

PowerFlex Manager can apply event publishers to multiple NAS servers. This association, in turn, helps save time in creating CEPA configurations every time you want to associate an event publisher file with a NAS server. To apply the CEPA configuration to a NAS server, provide the file CEPA publisher details—ID and name, while creating the NAS server.

Steps

1. Go to **File > NAS Servers > NAS Settings > Event Publishers**.
2. Select the check box next to the event publisher that you want to associate with the NAS server.
3. Click **Associate**.
The **Associate Event Publisher to NAS Servers** window is displayed.
4. In the **Select NAS Servers** tab, select the NAS servers with which you want to associate the event publisher and click **Next**.
5. In the **Configure File Systems** tab, enable the SMB, NFS, or both options for the NFS servers.

 **NOTE:** Both the SMB and NFS options can be enabled only for multiprotocol NAS servers.

6. Click **Next** to go the **Summary** tab.
The list of NAS servers that you selected for association with the event publisher is displayed.
7. Click **Associate** to complete the process of associating the event publisher with the NAS servers.
You can view the list of NAS servers that are associated with the event publisher in the **Select NAS Servers** tab. The number of NAS servers associated with the event publisher is displayed on the **NAS Settings > Event Publishers** page.

Disassociating event publishers

The disassociate option allows you to disassociate the existing NAS servers or associate new servers with the event publishers.

Steps

1. Go to **File > NAS Servers > NAS Settings > Event Publishers**.
2. Select the check box next to the event publisher that you want to disassociate from the NAS server.
3. Click **Disassociate**.
The **Disassociate Event Publisher to NAS Servers** window is displayed.
4. In the **Select NAS Servers** tab, select the NAS servers with which you want to associate the event publisher. Alternatively, clear the check box next to the NAS server you want to disassociate from the event publisher.
5. Click **Disassociate**.
The updated number of NAS servers disassociated or associated with the event publisher is displayed on the **NAS Settings > Event Publishers** page.

Deleting event publishers

Prerequisites

Before deleting event publishers, ensure that the event publishers are disabled for the NAS server.

Steps

1. Go to **File > NAS Servers > NAS Settings > Event Publishers**.
2. Select the check box next to the event publisher that you want to delete.
3. Click **Delete**.
A message to confirm the deletion is displayed.
4. Click **OK** to confirm.

NAS server security

Kerberos

Kerberos is a distributed authentication service designed to provide strong authentication with secret-key cryptography. It works on the basis of "tickets" that allow nodes communicating over a non-secure network to prove their identity in a secure manner. When configured to act as a secure NFS server, the NAS server uses the RPCSEC_GSS security framework and Kerberos authentication protocol to verify users and services.

- Using Kerberos with NFS requires that DNS and a UDS, are configured for the NAS server and that all members of the Kerberos realm are registered in the DNS server.
- For authentication Kerberos can be configured with either a custom realm, or with Active Directory (AD).
- The storage system must be configured with an NTP server. Kerberos relies on the correct time synchronization between the KDC, servers, and the client network.

Configuring Kerberos for secure NFS

- If configuring the NAS server for NFS only, you must configure the NAS server with a custom realm. If you have configured the NAS server with NFS and SMB, you can use either the AD or custom realm.

- Using LDAPS or LDAP with Kerberos is recommended for increased security.
- A DNS server must be configured at the NAS-server level. All members of the Kerberos realm, including the KDC, NFS server, and NFS clients, must be registered in the DNS server.
- The NFS client's hostname FQDN and NAS server FQDN must be registered in the DNS server. Clients and servers must be able to resolve any member of the Kerberos realm's FQDNs to an IP address.
- The FQDN part of the NFS client's SPN must be registered in the DNS server.
- A keytab file must be uploaded to your NAS server when configuring Secure NFS.
 - Use the Retrieve Keytab File to download a keytab file you have previously uploaded to the NAS server.
 - Use the Upload the Keytab File to upload the keytab file after you have validated the content.

Antivirus (Common AntiVirus Agent (CAVA))

Available for SMB servers only.

Common AntiVirus Agent (CAVA) provides an antivirus solution to clients using a NAS server. It uses an industry-standard SMB protocol in a Microsoft Windows Server environment. CAVA uses third-party antivirus software to identify and eliminate known viruses before they infect files on the storage system.

Antivirus software is important because the storage system is resistant to the invasion of viruses because of its architecture.

The NAS server runs data access in real-time using an embedded operating system. Third parties are unable to run programs containing viruses on this operating system. Although the operating system software is resistant to viruses, Windows clients that access the storage system require virus protection. Virus protection on clients reduces the chance that they will store an infected file on the server and protects them if they open an infected file. This antivirus solution consists of a combination of the operating system software, CAVA agent, and a third-party antivirus engine. The CAVA software and a third-party antivirus engine must be installed on a Windows Server in the domain.

Managing an event publisher configuration

Events Publishing allows third-party applications to register to receive event notification and context from the storage system when accessing file systems with the SMB or NFS protocols. The Common Event Publishing Agent (CEPA) delivers to the application both event notification and associated context in one message. Context may consist of file metadata or directory metadata that is needed for the business policy.

You must define at least one event option (pre-, post-, or post-error event) when Events Publishing is enabled.

- Pre-event notifications are sent before processing an SMB or NFS client request.
- Post-event notifications are sent after a successful SMB or NFS client request.
- Post-error event notifications are sent after a failed SMB or NFS client request.

Enabling event publisher settings

About this task

When an events publisher is created, events publishing on a NAS server can be enabled. Multiple NAS servers can use the same events publisher.

Steps

1. Go to **File > NAS Servers > NAS Servers**
2. Select the check box next to the NAS server name for which you want to enable the event publisher.
3. On the right, click **View Details**.
4. Go to **Security > Events Publishing**.
5. Enable the event publisher and select the required event publisher from the **Event Publisher** drop-down.
6. Select the **Enable for all existing file systems under this NAS server** option.
7. Select the required protocol—SMB, NFS, or both.
8. Click **Apply**.

Configure NAS server security

Steps

1. Log in to PowerFlex Manager.
2. To configure security settings, click **File > NAS Servers**, select the NAS server and click **View Details > Security**.
3. To configure Kerberos, click **File > NAS Servers**, select the NAS server and click **View Details > Security > Kerberos**. Click the Disabled button to enable, enter the realm, enter the IP address, and click **Add**.
4. To enable CAVA, click the Disabled button.
 - a. If you do not have a current CAVA configuration file available, click Retrieve Current Configuration and complete the CAVA configuration file template.
 - b. Upload the current CAVA configuration file.
 - c. Click **Apply** to start antivirus support.

Create a global namespace

You can create a global namespace (GNS) to allow the NAS user to access a single namespace supported by the NAS cluster with a single export.

About this task

A global namespace provides a virtual view of shared folders by grouping shares or exports that are located on different servers into one or more logical namespaces. This virtual view gives you a single entry point to access multiple file systems.

With the global namespace feature enabled, client hosts with correct access permission can access existing and newly added file systems without needing to explicitly map/mount them on each client.

When you create a global namespace, you have the option to set up a single mount point or single export that consists of several file systems that may be SMB or NFS.

PowerFlex file services support a multi-protocol global namespace for both SMB and NFSv4 clients. The GNS infrastructure does not support NFSv3 clients, however they can access the shares directly. Also, NAS server supports creating multiple namespaces.

Prerequisites

Configure at least one NAS server before you attempt to create a global namespace.

Steps

1. Select the **File > Global Name Space** tab.
2. Click **Create Global Name Space** and enter the following information in the wizard:

Option	Description
NameSpace for NFS	For NFS only. The namespace provides access over the NFS(nfsv4) protocol only.
NameSpace for SMB	For SMB only. The namespace provides access over the SMB protocol only.
NameSpace for both NFS and SMB	For SMB and NFS. The namespace provides access over both NFS and SMB protocols.


3. Click **Next**.
4. Choose a NAS server on which to create the GNS and click **Next**.

A NAS server can host multiple namespaces.
5. Select a file system to create the GNS.

Option	Description
Create new Filesystem (Recommended)	Create a dedicated file system to host the GNS.

Option	Description
Select from available General Type Filesystems	Select an existing file system. Do not select the existing NFS file system if the file system root has already been exported.

6. Specify GNS details for the namespace:


Option	Description
Name of the server	The name allows remote hosts to connect to the Global Namespace over the network.
Description	Optional description for the namespace.
Local Path	Local path relative to the NAS server. This path is the local path to the storage resource or any existing subfolder of the storage resource that is shared over the network. The path is relative to the NAS Server and must start with the file system's mountpoint path, which is the file system name. For example, to share the top level of a file system named powerflexfs1, which is mounted on the / powerflexfs1 mountpoint on the NAS Server, use / powerflexfs1 in the path parameter.  NOTE: The Namespace Path is generated based on the interface of the selected NAS server and namespace server name.

7. Review the **Summary** page and choose one of the following options to create the GNS.

- Run in the background
- Add to the Job List to schedule later

Results

The root shares and exports are automatically created on the file system.

 **NOTE:** These shares and exports cannot be deleted without deleting the namespace.

Modify a namespace server

You can modify the configuration of a namespace server after it is created.

Steps

1. Select the **File > Global Name Space** tab.
2. Select the namespace server from the list and click **Modify**.
The **Modify Global Namespace** wizard launches.
3. Modify the **Description**, **Type of Namespace** and **Client Cache Timeout** as needed.

The default client cache timeout is 300 seconds. The client cache timeout is the amount of time that clients cache namespace root referrals. A referral is an ordered list of targets that a client system receives from a namespace server when the user accesses a namespace root or folder with targets in the namespace. You can adjust how long clients cache a referral before requesting a new one.

Remove a namespace server

You can remove a namespace server if it is no longer needed.

Steps

1. Select the **File > Global Name Space** tab.
2. Select the namespace server from the list and click **Remove**.

Create a link for a GNS

You can create a link for a global namespace. The Global Namespace Link object holds information about the related remote locations, which the namespace targets. A link can only have one target.

Steps

1. Select the **File > Global Name Space** tab.
2. Select the namespace server from the list and click **View Details**.
3. Click **Create Link** and enter the following information in the wizard:

Option	Description
Local path	A path name relative to the namespace root (without a forward slash or trailing slash). Remote hosts use this path to connect to the target file system.
Description (Optional)	Description of the link.
Client Cache Timeout (Seconds)	Client cache timeout is the amount of time that clients cache namespace root referrals. A referral is an ordered list of targets that a client system receives from a namespace server when the user accesses a namespace root or folder with targets in the namespace.
Add Target UNC (Universal Naming Convention) Path	Select the target from UNC path from the available exports or shares, or add the target UNC path manually.

Modify a namespace server link

After you create a namespace server, you can modify the link.

Steps

1. Select the **File > Global Name Space** tab.
2. Select the namespace server from the list and click **View Details**.
3. Select the link from the list and click **Modify**.
4. Optionally, modify the description and client cache timeout of the link, as well as the **Target UNC Path**.

Remove a link and target

You can remove the link and target for a namespace server after it is created.

Steps

1. Select the **File > Global Name Space** tab.
2. Select the namespace server from the list and click **View Details**.
3. Select the link and target from the list and click **Remove**.

Restore a Global Name Space

If necessary, you can restore a global namespace.

Restore is needed when you have a namespace that is in an error or inactive state. Ensure that you have a snapshot available for restore.

The namespace will be created automatically after you restore the snapshot.

File systems

PowerFlex file leverages a 64-bit file system that is highly scalable, efficient, and flexible.

A NAS server must be created before you can create a file system.

The NAS server must support the sharing protocol for which you are creating the file system for example, if you are creating a file system with NFS exports, the NAS server must support NFS protocol.

You can choose to create SMB Shares, or NFS Exports the first time you create the file system, or you can create SMB Shares, and NFS Exports on a file system after it has been created. These advanced settings can be configured for a file system which will be used for SMB shares.

Scalability

PowerFlex file systems can accommodate large amounts of data, directories, and files. The following table shows several of the scalability attributes and limits of file system.

File system attribute	Limit
Maximum file system size	256 TB
Subdirectories per directory	~ 10 million
Files per file system	~ 32 billion
Filenames per directory	~ 10 million
ACL IDs	4 million
Timestamp granularity	1 nanosecond

Storage efficiency

All file systems are thinly provisioned and always have compression and deduplication enabled. With thin file systems, only 1.5 GB is allocated upfront for metadata, regardless of how large the file system is. As capacity is consumed on the file system, additional capacity is allocated on demand. This continuously happens until the specified file system size is reached and the file system becomes full.

Compression and deduplication help reduce the total cost of ownership and increase the efficiency of the system by reducing the amount of physical capacity that is needed to store the data. Savings are not only limited to the file system itself, but also to its snapshots and thin clones. Compression and deduplication occur in line between the system cache and the backend drives. The compression task is offloaded to a dedicated chip on the node, which frees up CPU cycles.

Performance

PowerFlex systems are tuned and optimized for high performance across all use cases. In addition, platform components such as Non-Volatile Memory Express (NVMe) drives and dual-socket CPUs enable the system to maintain low response times while servicing large workloads

Shrink and extend

PowerFlex file systems provide increased flexibility by providing the ability to shrink and extend file systems as needed. Shrink and extend operations are used to resize the file system and update the capacity that is seen by the client. Extend operations do not change how much capacity is allocated to the file system. However, shrink operations may be able to reclaim unused space depending on how much capacity is allocated to the file system and the presence of snapshots or thin clones.

If the advertised file system size is too small or full, extending it allows additional data to be written to the file system. If the advertised file system size is too large, shrinking it limits the amount of data that can be written to the file system. For shrink and extend, the minimum value is equal to the used size of the file system and the maximum value is 256 TB. You cannot shrink the file system to less than the used size, as this would cause the client to see the file system as more than 100% full.

Create a file system for NFS exports

Ensure that there is a NAS server that is configured to support the NFS protocol.

Steps

1. Click **File > File Systems**.

2. Click **Create**.

3. Select an NFS enabled NAS server for the file system.

NOTE: Leave the Advanced SMB Settings as is, since this is applicable only for creating file system for SMB shares.

4. Click **Next**.

5. Select the storage pool (where you want to create file system) from drop down list.

6. Specify the file system details, including the file system name and size, minimum size is 3 GB, maximum size is 256 TB.

NOTE: All thin file systems, regardless of size, have 1.5 GB reserved for metadata upon creation. For example, after creating a 100 GB thin file system, PowerFlex file immediately shows 1.5 GB used. When the file system is mounted to a host, it shows 98.5 GB of usable capacity. The metadata space is reserved from the usable file system capacity.

7. Configure the initial export for the file system.

NOTE: You can add NFS exports to the file system at a later time.

8. Click **Next**.

9. Configure security, access permissions, and host access for the system. This option will be enabled only if you created the NFS export.

Option	Description
Minimum security	Select Sys to allow users with non-secure NFS, or Secure NFS to mount and NFS export on the file system. If you are not configuring Secure NFS, you must select this option. If you are creating a file system with Secure NFS, then you can choose from the following options: <ul style="list-style-type: none">• Kerberos to allow any type of Kerberos security for authentication (krb5/krb5i/krb5p).• Kerberos with Integrity to allow both Kerberos with integrity and Kerberos with encryption security or user authentication (krb5i/krb5p).• Kerberos with Encryption to allow only Kerberos with encryption security for user authentication (krb5p).
Default access	The default access that is applied to the hosts unless the hosts are configured with a different access permission.
Add host	Enter hosts individually, or you can add hosts by uploading a properly formatted .CSV file. You can download the CSV file first to obtain a template.

If you are planning to create same file system for both NFS and SMB exports, enter the details, otherwise leave this option as is.

10. Click **Next**.

11. Optionally, add a protection policy to the file system.

If you are adding a protection policy to the file system, the policy must have been created before creating the file system. Only snapshots are supported for protection for file systems. Replication is not supported on file system.

12. Review the summary and click **Create File System**.

The file system is added to the **File System** tab. If you created an export simultaneously, then the export displays in the **NFS export** tab.

Summary NFS Export	Description
Local path	<p>The path to the file system storage resource on the storage system. This path specifies the unique location of the share on the storage system.</p> <ul style="list-style-type: none"> Each NFS share must have a unique local path. PowerFlex file automatically assigns this path to the initial export created within a new file system. The local path name is based on the file system name. Before you create more exports within an NFS file system, create a directory to share from a Linux/UNIX host that is connected to the file system. Then you can create an export from PowerFlex file and set access permissions accordingly.
NFS export path	<p>The path used by the host to connect to the export. PowerFlex file creates the export path that is based on the IP address of the host, and the name of the export. Hosts use either the file name or the export path to mount or map to the export from a network host.</p>

Create a file system for SMB shares

Ensure that there is a NAS server that is configured to support the SMB protocol.

Prerequisites

A file system must be created on the NAS server before you can create an SMB share.

About this task

Sync Writes: Synchronous writes enable the storage system to perform immediate synchronous writes for storage operations, regardless of how the SMB protocol performs write operations. Enabling synchronous writes operations allow you to store and access database files (for example, MySQL) on storage system SMB shares. This option guarantees that any write to the share is done synchronously and reduces the chances of data loss or file corruption in various failure scenarios, for example, loss of power. If SMB3 continuous availability (CA) is enabled, all write operations are automatically synced to satisfy the requirements for continuous availability. This option can have a big impact on performance. It is not recommended unless you intend to use Windows file systems to provide storage for database applications.

Oplocks: Opportunistic file locks (oplocks) allow SMB clients to buffer file data locally before sending it to a server. SMB clients can then work with files locally and periodically communicate changes to the storage system rather than having to communicate every operation over the network to the storage system. Unless your application handles critical data or has specific requirements that make this mode or operation unfeasible, leaving the oplocks enabled is recommended.

The following oplocks implementations are supported:

- Level II oplocks: This informs a client that multiple clients are currently accessing a file, but no client has yet modified it. A level II oplock lets the client perform read operations and file-attribute fetches by using cached or read-ahead local information. All other file access requests must be sent to the server.
- Exclusive oplocks (SMB2 only): This informs a client that it is the only client opening the file. An exclusive oplock lets a client perform all file operations by using cached or read-ahead information until it closes the file, at which time the server must be updated with any changes that are made to the state of the file (contents and attributes).
- Batch oplocks: This informs a client that it is the only client opening the file. A batch oplock lets a client perform all file operations by using cached or read-ahead information (including opens and closes). The server can keep a file opened for a client even though the local process on the client machine has closed the file. This mechanism curtails the amount of network traffic by letting clients skip the extraneous close and open requests.

This option only applies to client access over SMB1 since oplocks are always enabled for client access over SMB2 and SMB3. However, disabling this option also invalidates the SMB2.1 file and directory lease feature. Leasing serves the same purpose as oplocks, but provides greater flexibility and enhancements, increasing performance and reducing network utilization.

- Read-caching lease: This allows caching reads and can be shared by multiple clients.
- Write-caching lease: This allows caching writes and is exclusive to only one client.

- Handle-caching lease: This allows caching handles and can be shared by multiple clients.

Notify on write or access: This option enables notifications when a file system is written to or accessed. Applications that run on Windows platforms, and use the Win32 API, can register with the SMB server to be notified of file and directory content changes, such as file creation, modify, or rename. For example, this feature can indicate when a display must be refreshed (Windows Explorer) or when the cache must be refreshed (Microsoft Internet Information Server), without having to constantly poll the SMB server.

Steps

1. Click **File > File Systems**.
2. Click **Create**.
3. Enter the following information in the **Create File System** wizard:

Option	Description
Select NAS server	Select a NAS server enabled for SMB.
Advanced SMB settings	Optionally choose from the following: <ul style="list-style-type: none"> • Sync Writes Enabled • Oplocks Enabled • Notify on Write Enabled • Notify on Access Enabled • Enable SMB Events Publishing
File system details	Provide the file system name, and the size of the file system. The file system size can be from 3 GB to 256 TB. <i>i</i> NOTE: All thin file systems, regardless of size, have 1.5 GB reserved for metadata upon creation. For example, after creating a 100 GB thin file system, PowerFlex file storage immediately shows 1.5 GB used. When the file system is mounted to a host, it shows 98.5 GB of usable capacity. This is because the metadata space is reserved from the usable file system capacity.
SMB share	Optionally, configure the initial SMB share. You can add shares to the file system after the initial file system configuration.
Protection policy	Optionally, provide a protection policy for the file system. <i>i</i> NOTE: PowerFlex file supports snapshots for file storage protection. Replication protection is not supported for file systems.
Summary	Review the summary. Go back to make necessary updates.

4. Click **Create File System**.

The file system is displayed in the **File System** list, and if you created an SMB Share, it is displayed in the SMB share list.

Change file system settings

Change file system configuration settings, modify the file system properties, delete the file system, and perform additional actions on a file system.

Steps

1. Click **File > File Systems**.
2. Click the checkbox in the file system list to make changes to the file system configuration settings.

Option	Description
Modify	To modify the file system name, description, or size.

Option	Description
Protection	To perform one of the following operations: <ul style="list-style-type: none"> • Assign or unassign a protection policy • Create a snapshot • Restore the file system from a snapshot
More actions	To perform one of the following operations: <ul style="list-style-type: none"> • Remove - To remove the file system from the NAS server. This option is not available if NFS exports or SMB shares have been created on the file system • Refresh quotes

Quotas

PowerFlex includes quota support to allow administrators to place limits on the amount of space that can be consumed to regulate file system storage consumption.

These simple but flexible quotas can easily be configured through any of the available management interfaces. PowerFlex supports user quotas, quota trees, and user quotas on tree quotas. All three types of quotas can co-exist on the same file system and may be used in conjunction to achieve finer grained control over storage usage.

User quotas

User quotas are set at a file system level and limit the amount of space a user may consume on a file system. Quotas are disabled by default, but this can be enabled in the quota properties page dialog box along with the default user quota settings. The default quota limits are applied automatically to all users who access the file system. However, the default limits can be overridden for specific users by creating a new user quota entry in PowerFlex Manager.

Because all unspecified users are subject to the default quota settings, there is no ability to delete a user quota. Instead, a user quota can be set to 0 to allow unlimited access. Alternatively, a user quota can be set to inherit the default limits.

Tree quotas

Quota trees limit the maximum size of a directory on a file system. Unlike user quotas, which are applied and tracked on a user-by-user basis, quota trees are applied to directories within the file system. Quota trees can be applied on new or existing directories.

If an administrator specifies a nonexistent directory when configuring a new quota tree, the directory is automatically created as part of quota configuration. However, an administrator may also specify an existing file system directory with existing data when creating a quota tree, allowing the ability to implement quotas on existing file system and directory structures after they have already been in production. If a tree quota is deleted, the directory itself remains intact and all files continue to be available.

Quota trees may not be nested within a single directory. For example, if a quota tree is created on `/directory1`, another quota tree cannot be created on `/directory1/subdirectory1`. However, it is possible to have quota trees on `/directory2`, `/directory3`, and so on.

In PowerFlex file, the quota grace period setting only applies to user quotas since each tree quota can have its own individual grace period setting. Newly created tree quotas have a default grace period setting of 7 days, and this can be customized during creation or afterwards.

User quotas on tree quotas

Once a quota tree is created, it is also possible to create additional user quotas within that specific directory by choosing to enforce user quotas. When multiple limits apply, users are bound by the limit that they reach first. As an example, a single user may be bound by the following limits on a file system:

- File system user quota: 25 GB
 - This user has a limit of 25 GB across the entire file system
- Tree quota (`/directory1`): 100 GB

- Data from all users in this directory may not exceed 100 GB
- User quota on tree quota (/directory1): 10 GB
 - This user cannot consume more than 10 GB on this directory

Quota limits

All quotas consist of three major parameters which determine the amount of space that can be consumed on a file system and define the behavior when a limit is being approached or exceeded. These parameters are:

- Soft limit (GB)
- Grace period (time)
- Hard limit (GB)

The soft limit is a capacity threshold which triggers the grace period timer to start. For as long as the soft limit is exceeded, the grace period continues to count down. If the soft limit remains exceeded long enough for the grace period to expire, no new data may be added by the user or to the directory. The grace period has a minimum value of 1 minute and maximum value of unlimited. However, if enough data is removed from the file system or directory to reduce the utilization below the soft limit before the grace period expires, data can continue to be written normally. Administrators can also allow users to continue writing data by increasing the value of the soft limit.

A hard limit is also set for each quota configured. Upon reaching a hard limit, no new data can be added to by the user or to the directory. When this happens, the quota must be increased, or data must be removed from the file system before additional data can be written.

Add file system quotas

You can track and limit storage space consumption by configuring quotas for file systems at the file system or directory level.

About this task

You can enable or disable quotas at any time, but it is recommended that you enable or disable them during non-peak production hours to avoid impacting file system operations. You cannot create quotas for read-only file systems. Quotas are supported on SMB, NFS, FTP, NDMP, and multiprotocol file systems.

Steps

1. Click **File > File System**.
2. Select the file system and click **View Details > Quotas**.
3. There are two types of quotas you can put on a file system:

Type	Description
User quotas	Limits the amount of storage that is consumed by an individual user storing data on the file system.
Tree quotas	<p>Tree quotas limit the total amount of storage that is consumed on a specific directory tree. You can use tree quotas to:</p> <ul style="list-style-type: none"> ● Set storage limits on a project basis. For example, you can establish tree quotas for a project directory that has multiple users sharing and creating files in it. ● Track directory usage by setting the tree quota hard and soft limits to 0 (zero). <p>NOTE: If you change the limits for a tree quota, the changes take effect immediately without disrupting file system operations.</p>

4. To track space consumption without setting limits, set Soft Limit and Hard Limit to 0, which indicates no limit.

Type	Description
Hard limit	A hard limit is an absolute limit on storage usage. If a hard limit is reached for a user quota on a file system or quota tree, the user cannot write data to the file system or tree until more space becomes available. If a hard limit is reached for a quota tree, no user can write data to the tree until more space becomes available.
Soft limit	A soft limit is a preferred limit on storage usage. The user is allowed to use space until a grace period has been reached. The user is alerted when the soft limit is reached, until the grace period is over. After that, an out of space condition is reached until the user gets back under the soft limit.
Grace period	The grace period provides the ability to set a specific grace period to each tree quota on a file system. The grace period counts down the time between the soft and hard limit and alerts the user about the time remaining before the hard limit is met. If the grace period expires you cannot write to the file system until more space has been added, even if the hard limit has not been met. You can set an expiration date for the grace period. The default is seven days, alternatively you can set the grace period expiration date to an infinite amount of time and the grace period will never expire, or for specified number of days, hours, or minutes. Once the grace period expiration date is met, the grace period will no longer apply to the file system directory.

Refresh quotas

Refresh the content of tree and user quotas objects.

Steps

1. Click **File > File Systems**.
2. Click on a file system in the list to make changes to the file system configuration settings.
3. Click **More Actions > Refresh Quotas**.
To refresh a user quota, click **Quotas > User Quota > More Actions > Refresh Quotas**.
To refresh a tree quota, click **Quotas > Tree Quota > More Actions > Refresh Quotas**.

Shares and exports

Shares represent mount points through which users or hosts can access file system resources. Each share is associated with a single file system and inherits the file system protocol (SMB or NFS) established for that file system. Shares of a multiprotocol file system can be either SMB or NFS.

Access to shares is determined depending on the type of file system:

- Windows (SMB) shares: Access is controlled by SMB share permissions and the ACLs on the shared directories and files. For example, you can configure share permissions using the Microsoft Computer Management utility.
 - Active directory SMB servers: Configure access for users and groups using Windows directory access controls. User/group authentication is performed through Active Directory.
 - Stand-alone SMB servers: Manage a stand-alone SMB server within a workgroup from a Microsoft Windows host.
- Linux/UNIX (NFS) exports: Hosts access is defined by the NFS access control settings of the NFS export. Use PowerFlex Manager to configure access for individual Linux/UNIX hosts or IP subnets.

All shares within a single file system draw from the total quantity of storage allocated for the file system. Consequently, storage space for shares is managed at the file system level.

SMB and NFS configuration details

The following table provides details you will need when creating file systems, SMB shares or NFS exports.

Option	Description
Name	<p>The name provided for the export or share, along with the NAS server name is the name by which the hosts will access the export or share.</p> <p>NFS export, and SMB share names must be unique at the NAS server level per protocol. However, you can specify the same name for SMB shares and NFS exports.</p>
Local path	<p>The path to the file system storage resource on the storage system. This path specifies the unique location of the share on the storage system.</p> <p>SMB shares:</p> <ul style="list-style-type: none">• An SMB file system allows you to create multiple shares with the same local path. In these cases, you can specify different host-side access controls for different users, but the shares within the file system will all access common content.• A directory must exist before you can create shares on it. Therefore, if you want the SMB shares within the same file system to access different content, you must first create a directory on the Windows host that is mapped to the file system. Then, you can create corresponding shares using PowerFlex Manager. You can also create and manage SMB shares from the Microsoft Management Console. <p>NFS exports:</p> <ul style="list-style-type: none">• Each NFS export must have a unique local path. PowerFlex automatically assigns this path to the initial export created within a new file system. The local path name is based on the file system name.• Before you can create additional exports within an NFS file system, you must create a directory to share from a Linux/UNIX host that is connected to the file system. Then, you can create a share from PowerFlex Manager and set access permissions accordingly.
SMB share path or export path	<p>The path used by the host to connect to the share or export.</p> <p>PowerFlex creates the export path based on the IP address of the file system, and the name of the export or share. Hosts use either the file name or the export path to mount or map to the export or share from a network host.</p>

Create an NFS export

Use this procedure to create an NFS export on a file system that is created with an NFS-enabled NAS server.

Prerequisites

Create snapshots before creating the NFS export.

Steps

1. Click **File > NFS Export**.

2. Click **+ Create NFS Export**.

The **Create NFS Export** wizard appears.

3. Enter the information and note the following:

- **Local Path** must correspond to an existing folder name within the file system that was created from the host-side.
- The value specified in the **NFS Export Details, Name** field, along with the NAS server name, constitutes the name by which hosts access the export.
- NFS export names must be unique at the NAS server level per protocol. However, you can specify the same name for an SMB share, and NFS exports.

4. Approve the settings, and click **Create NFS Export**.

The NFS export displays on the **NFS Export** page.

Create an SMB share

Create an SMB share on a file system that has been created with an SMB-enabled NAS server.

About this task

Continuous availability: Continuous availability is a share-level SMB3 feature. In a client or storage node failure, continuous availability allows persistent access to file systems without loss of the session state. This ability is useful for critical applications such as Microsoft Hyper-V or SQL, where constant availability to files is of the utmost importance. SMB3 uses persistent handles to enable the NAS server to save specific metadata that is associated to an open handle on disk. In a node failure, applications accessing open file content are not affected if the NAS server and file system failover to the peer node completes within the timeout of the application. This action results in clients transparently reconnecting to the peer node after the NAS server failover without affecting client access to files.

Continuous availability is also available on the client side, which is independent from storage continuous availability. Client continuous availability transparently preserves access in a node failure within a client application cluster. When a failure of one node in the cluster occurs, the application is moved to the other node and reopens its content on the share from that node using its originally assigned ApplicationID without an interruption in access. The CA option on the share does not need to be enabled in order to use client continuous availability.

SMB 3.1.1 adds a reliability enhancement for continuous availability for hyper-V cluster client failover by adding an ApplicationInstanceVersion tag in addition to the ApplicationID. The ApplicationInstanceVersion tag is incremented each time that an application is restarted on a new node within the cluster. In situations where network access is lost, but storage access remains available, the application may be restarted on a new node without the cluster knowing due to the lack of network access. The ApplicationInstanceVersion tag enables the storage system to easily identify which node in the cluster is the correct owner of the application. The storage system can safely close any locks that were opened with a lower ApplicationInstanceVersion number, which allows the application to restart without any conflicts.

Protocol encryption: Protocol encryption is a share-level SMB3 feature, which provides in-flight data encryption between SMB3 clients and the NAS server. The client or NAS server encrypts the data before sending it to the destination. It is then decrypted upon reaching its destination, whether that is the NAS server or SMB client. The protocol encryption is enforced at user session level, ensuring the whole SMB traffic is encrypted once the user session is established.

The following setting can be configured in the NAS server registry:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\RejectUnencryptedAccess: Determines if clients that do not support encryption (pre-SMB3.0) have access to the share

- 1 (default): Returns access denied to pre-SMB3.0 clients that do not support encryption
- 0: Allows pre-SMB3.0 clients to access the share without encryption

SMB 3.1.1 also provides improved security and encryption traffic performance for SMB3 by changing the encryption algorithm from AES-CCM-128 to AES-GCM-128. This change improves performance under certain conditions such as large file transfers. In addition, this improves security against man-in-the-middle attacks.

Access-based enumeration: Access-based enumeration is a share-level option that restricts the display of files and folders based on the access privileges of the user attempting to view them. Without access-based enumeration, all users can view all files and folders within a directory. However, users cannot open or view these files and folders without the appropriate access privileges. When access-based enumeration is enabled on a share, users are only able to see files or folders for which they have read access or above.

For example, without access-based enumeration, a user could see all files in a directory, regardless of whether they can open them. However, with access-based enumeration, the inaccessible files are hidden from the user view. Administrator users are always able to see all files and folders, even when access-based enumeration is enabled on a share.

Branch cache: BranchCache is a share-level option that allows users to access data that is stored on a remote NAS server locally over the LAN without being required to traverse the WAN to access the NAS server. This ability is useful in a remote or branch office environment, where branch offices are required to access data stored on PowerFlex at the main office. BranchCache allows this data to be cached locally at the branch, either by a designated Windows BranchCache server or distributed across Windows clients. This ability can reduce WAN bandwidth that is used by many clients constantly and repeatedly traversing the WAN for the same data.

With BranchCache enabled, the client uses the WAN to retrieve the hash of the file from the NAS server at the main office. The client searches the local file cache to look for a file with a matching hash. If all or some of the data is available locally, either on the designated Windows BranchCache server or another Windows client system, the data is retrieved locally. The data is validated using a hash function to ensure that the file is the same. Any data that is not cached locally is retrieved from the NAS server over the WAN, and then cached locally for future requests. BranchCache works best for data that does not change often, allowing files to be cached for longer periods of time at the branch offices.

Steps

1. Click **File > SMB Share**.
2. Click **+ Create SMB Share** and work through the **Create SMB Share** wizard.

Option	Description
Select file system	Select a file system that has been enabled for SMB.
Select a snapshot of the file system	Optionally, select one of the file system snapshots on which to create the share. Only snapshots are supported for file system protection policies. Replication is not supported for file systems.
SMB share details	Enter a name and local path for the share. When entering the location path: <ul style="list-style-type: none"> • You can create multiple shares with the same local path on a single SMB file system. In these cases, you can specify different host-side access controls for different users, but the shares within the file system have access to common content. • A directory must exist before you can create shares on it. If you want the SMB shares within the same file system to access different content, you must first create a directory on the Windows host that is mapped to the file system, then you can create corresponding shares using PowerFlex. PowerFlex also created the SMB share path, which uses the host to connect to the share. The export path is the IP address of the file system, and the name of the share. Hosts use either the file name or the share path to mount or map to the share from the network host.
Advanced SMB properties	Enable one or more of the Advanced SMB settings: <ul style="list-style-type: none"> • Continuous availability • Protocol encryption • Access-based enumeration • Branch cache enabled Decide which objects are available when the share is offline.

3. To modify the share from PowerFlex Manager, select the share from the list on the **SMB Share** page, and click **Modify**.

File protection

PowerFlex uses snapshots to protect file system data.

Create a protection policy

Create a protection policy to provide local protection for your file systems.

About this task

Each protection policy can include up to 16 snapshot rules. A rule can be included in multiple policies.

Steps

1. Click **File > File Protection > Protection Policies**.
2. From the **File Protection** window, click **+ Create**.
3. From the **Create Protection Policy** panel, set the new policy name.
4. Select the snapshot rules you want to include in the policy or create a new snapshot rule.
5. Click **Create Policy**.

Create snapshot rules

Create snapshot rules to control parameters such as the frequency of snapshot creation and snapshots retention period.

About this task

If you want to create a new snapshot rule in addition to the existing rules, it is recommended to review the business requirements with an administrator before proceeding. This can help in achieving and maintaining consistent policies across the system.

Steps

1. Click **File > File Protection**.
2. From the **File Protection** window, click **Snapshot Rules**.
3. Click **+ Create**.
4. From the **Create Snapshot Rules** panel, enter a name for the new rule.
5. Set the following:
 - a. Select the days to create the snapshot.
 - b. Set the frequency:
 - For a snapshot to be taken at a fixed interval, select this option and set the number of hours after which a snapshot will be created.
 - For a snapshot to be taken at a particular time of the selected days, select the **Time of day** option and set the time and time zone.
 - c. Set the retention period.
 - d. For file snapshots, select the file snapshot access type.

The supported file snapshot access types are Protocol (Read-Only) and Snapshot for creating snapshot rules.
6. Click **Create**.

Create a snapshot

Creating a snapshot saves the state of the file system and all files and data within it at a particular point in time. You can use snapshots to restore the entire file system to a previous state.

About this task

Before creating a snapshot, consider:

- Snapshots are not full copies of the original data. Do not rely on snapshots for mirrors, disaster recovery, or high-availability tools. Because snapshots are partially derived from the real-time data of the file systems, they can become inaccessible if the storage resource becomes inaccessible.
- Although snapshots are space efficient, they consume overall system storage capacity. Ensure that the system has enough capacity to accommodate snapshots.
- When configuring snapshots, review the snapshot retention policy that is associated with the storage resource. You may want to change the retention policy in the associated rules or manually set a different retention policy, depending on the purpose of the snapshot.
- Manual snapshots that are created with PowerFlex Manager are retained for one week after creation (unless configured otherwise).
- If the maximum number of snapshots is reached, no more can be created. In this case, to enable creation of new snapshots, you are required to delete existing snapshots.

Steps

1. Click **File > File Systems**.
2. Select the check box of the relevant file system to select it and click **Protection > Create Snapshot**.
3. In the **Create Snapshot of File System** panel, enter a unique name for the snapshot, and set the **Local Retention Policy**.



NOTE: Retention period is set to one week by default. You can set a different retention period or select the **No Automatic Deletion** for indefinite retention.

4. Click the **File Snapshot Access Type**.

For file systems, you can create three access types. The default access type is Protocol (Read-Only) protocol.

- Protocol (read-only): Creates read-only snapshot that can be mounted and accessed later through NFS export or SMB share.
- Snapshot: Creates read-only auto mounted snapshot accessible through the snapshot directory in the file system.
- Protocol (read-write): Creates a read write snapshot that can be mounted and accessed later through NFS export or SMB share.

5. Click **Create Snapshot**.

Assign a protection policy to a file system

Assign a protection policy to one or more file systems to apply the snapshot rules included in the policy to the file systems.

About this task

The protection policy automatically performs snapshot operations based on the specified parameters.

If a protection policy that meets your data protection requirements is available, you can assign it to a file system at any time. You can assign protection policy to a file system during the resource creation or at a later stage.

Steps

1. To assign a protection policy to an existing system:
 - a. Click **File > File Systems**
 - b. Select the check box of the file system to which you want to assign a protection policy.

NOTE: You can select multiple file systems.

 - c. Click **Protection > Assign Protection Policy**.
 - d. From the **Assign Protection Policy** panel, click the protection policy.
 - e. Click **Apply**.
2. To assign a protection policy to multiple file systems:
 - a. Click **File > File Systems > Protection > Assign Protection Policy**.
 - b. From the **Assign Protection Policy** panel, select the file systems and select the relevant objects from the protection policy list.
 - c. Click **Apply**.

Unassign a protection policy

About this task

Removing the protection policy from a file system results in the following:

- Scheduled snapshots, which are based on the rules associated with the policy.
- Existing snapshots are retained in the system, based on the snapshot rule settings when they were created.

Steps

1. Click **File > File Systems**.
2. Select the check box of the storage resource from which you want to unassign a protection policy.
3. Click **Protection > Unassign Protection Policy**.
4. Click **Unassign** to confirm.

Modify a protection policy

Modify a protection policy by adding and removing snapshot rules.

About this task

Changing the settings of a protection policy applies the new settings to all objects to which the protection policy is assigned. If you need to change the protection policy for one resource, it is recommended to create a new protection policy, and assign it to that resource instead.

Steps

1. Click **File > File Protection > Protection Policies**.
2. Select the check box next to the relevant policy and click **Modify**.
3. In the Properties panel, you can modify the following parameters:
 - Policy name
 - Description
 - Selected snapshot rules
4. Click **Apply**.

Delete a protection policy

Detach the protection policy from every file system before you delete.

Steps

1. Click **File > File Protection > Protection Policies**.
2. Select the check box next to the relevant policy and click **Delete**.

Modify a snapshot rule

Steps

1. Click **File > File Protection > Snapshot Rules**.
2. Select the snapshot rule from the list and click **Modify**.
3. Modify the required values and click **Apply**.

Delete a snapshot rule

Detach the snapshot rule from all the policies before you delete.


Steps

1. Click **File > File Protection > Snapshot Rules**.
2. Select the snapshot rule from the list and click **Delete**.
3. From the **Delete Snapshot Rule** page, click **Delete**.

Refresh a file system using snapshot

The content of the snapshot is replaced with the current content of the file system from which the snapshot was taken. You can create a duplicate of the production environment.

About this task

 **NOTE:** Because the refresh operation replaces the contents of a file system, it is recommended to take a snapshot of the file system before refreshing it. Creating a backup allows you to revert to a previous point in time.

Prerequisites

Before refreshing a snapshot, it is mandatory to shut down the application and unmount the file system that is running on the production host, and then flush the host cache to prevent data corruption during the refresh operation.

Steps

1. Click **File > File Systems** and select the check box from the list that you want to restore.
2. Click **View Details > More Actions > Refresh using snapshot**.
3. From the **Refresh Snapshot** panel, click **Refresh**.

Restore a file system from a snapshot

The restore operation is used to reconstruct an environment following an event that may have compromised its data.

About this task


You can use the restore operation to replace the contents of a file system storage resource with data from a snapshot that was taken directly from that storage resource. Restoring resets the data in that storage resource to the point in time at which the snapshot was taken. When restoring a file system, the source for the restore must be a snapshot that was taken directly from the storage resource that you are restoring.

Prerequisites


Before restoring a snapshot, it is mandatory to shut down the application and unmount the file system that is running on the production host, and then flush the host cache to prevent data corruption during the restore operation.

Steps

1. Click **File > File Systems** and select the check box from the list that you want to restore.
2. Click **Protection > Restore from snapshot**.
3. In the **Restore File System from Snapshot** panel, select the snapshot to use for the restore operation.
4. Select whether to create a backup snapshot of the restored object (the option is selected by default).

 **NOTE:** Because the restore operation replaces the contents of a storage resource, it is recommended to create a snapshot prior to restoring. Creating a backup allows you to revert to the original data.

5. Click **Restore**.

 **NOTE:** You can also restore the file system by selecting the file system snapshot from the **Snapshots** view. Click **File** > **File Systems**, and select the file systems from the list, click **View Details**, and click **More Actions** > **Restore from Snapshot**.

Reconfiguring MDM roles

PowerFlex Manager enables you to change the MDM role for a node in a PowerFlex cluster. For example, if you add a node to the cluster, you might want to switch the MDM role from an existing node to the new node.

About this task

You can launch the wizard for reconfiguring MDM roles from the **Resource Groups** page or from the **Resources** page. The nodes that are listed and the operations available are the same regardless of where you launch the wizard.

Each fault set can have a maximum of one MDM role (management or tiebreaker). PowerFlex Manager blocks your role assignments if the reconfigured roles do not conform to PowerFlex best practices.

Steps

1. To access the wizard from the **Resource Groups** page:
 - a. On the menu bar, click **Lifecycle > Resource Groups**.
 - b. Select a resource group that has the PowerFlex gateway for which you want to reconfigure MDM roles.
 - c. In the right pane, click **View Details**.
The **Resource Group Details** page is displayed.
 - d. On the **Resource Group Details** page, click **Reconfigure MDM Roles** under **More Actions**.
The **MDM Reconfiguration** page is displayed.
2. To access the wizard from the **Resources** page:
 - a. On the menu bar, click **Resources**.
 - b. Select the PowerFlex gateway for which you want to reconfigure MDM roles.
 - c. In the right pane, click **View Details**.
The **Details** page is displayed for the selected PowerFlex gateway.
 - d. On the **Details** page, click **Reconfigure MDM Roles**.
The **MDM Reconfiguration** page is displayed.
3. Review the current MDM configuration for the cluster.
4. Find each MDM role that you want to reassign and choose the new Host Name or IP address for the role in the **Select New Node for MDM Role** list.
You can reassign multiple roles at one time.
5. Click **Next**.
The **Summary** page is displayed.
6. Type **CHANGE MDM ROLES** to confirm your changes.
7. Click **Finish**.

Set rebuild and rebalance settings

Define rebuild and rebalance settings before and after RCM upgrades.

Steps

1. On the menu bar, click **Block > Protection Domains**.
2. In the list of protection domains, select the relevant protection domain check box, and click **Modify > Network Throttling**.
3. From the **Set Network Throttling for PD** field, enter the bandwidth for the following settings, or select **Unlimited** to allow for unlimited throughput for that setting:
 - Rebalance throughput limit per SDS
 - Rebuild throughput limit per SDS
 - vTree migration throughput limit per SDS
 - Overall throughput limit per SDS
4. Click **Apply**.
5. Verify that the operation has finished successfully, and click **Dismiss**.
6. Before an RCM upgrade, set the following policies:

Policy settings	Values
Rebuild policy	Unlimited
Rebalance policy	Unlimited
vTree migration policy	Retain the default value
Overall throughput limit per SDS	Limit concurrent I/O=10

7. After an RCM upgrade, set the following policies:


Policy settings	Values
Rebuild policy	Unlimited
Rebalance policy	Unlimited
vTree migration policy	Unlimited
Overall throughput limit per SDS	Unlimited

8. Click **Apply**.

Enabling or disabling SDC authentication

PowerFlex allows authentication and authorization be enabled for all SDCs connected to a cluster. Once authentication and authorization are enabled, older SDC clients and SDCs without a configured password will be disconnected.

The SDC procedures are not applicable for the PowerFlex management cluster.

 **NOTE:** If SDC authentication is enabled in a production environment, data unavailability may occur if clients are not properly configured.

Log in to PowerFlex using scli

The PowerFlex MDM cluster will use mTLS authentication now instead of legacy TLS authentication with username and password.

About this task

Mutual Transport Layer Security (mTLS) is a method for mutual authentication. mTLS ensures that the parties at each end of a network connection are who they claim to be by verifying that they both have the correct private key.

Steps

1. Generate the certificate:
 - a. To copy the management certificate to the root location, type:


```
cp /opt/emc/scaleio/mdm/cfg/mgmt_ca.pem /
```
 - b. To generate the certificate, type `scli --generate_login_certificate --management_system_ip <MNO_IP> --username <USER> --password <PASS> --p12_path <P12_PATH> --p12_password <P12_PASS> --insecure`.
 where:
management_system_ip is Ingress IP address and username
username is keycloak username (Ingress UI username)
password is keycloak user password (Ingress UI password). If not provided in the command line then CLI will prompt for it.
--p12_path <P12_PATH> is optional. If not provided then file will be created users home directory
p12_password is the password for p12 bundle. Same password needs to be provided for generation of the certificate and for login operation
2. To add the certificate, type `cd /opt/emc/scaleio/mdm/cfg; scli --add_certificate --certificate_file mgmt_ca.pem`.
3. To log in using the certificate, type `scli --login --p12_path <P12_PATH> --p12_password <P12_PASS>`.

Prepare for storage data clients authentication

Prepare the storage data clients for authentication.

Prerequisites

Ensure that you have the following information:

- Primary and secondary MDM IP address
- PowerFlex cluster credentials

Steps

1. Log in to the primary MDM: **scli --login --username admin --management_system_ip <management_system_ip>**
2. Authenticate with the PowerFlex cluster using the credentials provided.
3. Type **scli --query_all_sdc** and record all the connected SDCs (any of the identifier - NAME, GUID, ID, or IP address):
4. For each SDC in your list, use the identifier recorded to generate and record a CHAP password. Type **scli --generate_sdc_password --sdc_id <id> or --sdc_ip <ip> or --sdc_name <name> or --sdc_guid <guid> --reason "CHAP setup"**.

This password is specific to that SDC and cannot be reused for subsequent SDC entries.

For example:

```
scli --generate_sdc_password --sdc_IP 172.16.151.36 --reason "CHAP setup"
```

Sample output:


```
[root@svml ~]# scli --generate_sdc_password --sdc_ip 172.16.151.36 --reason "CHAP setup"
Successfully generated SDC with IP 172.16.151.36 password:
AQAAAAAAAAAAAAA8UKVYp0LHCDFD59BrnEXNPVKS1GfLrwAk
```

Configure storage data client to use authentication

Perform this procedure to configure the storage data clients for authentication.

About this task

For each storage data client, populate the generated CHAP password. On a VMware ESXi host, this requires setting a new `scini` parameter through the `esxcli` tool. Use the procedure to perform this configuration change. For Windows and Linux SDC hosts, the included `drv_cfg` utility is used to update the driver and configuration file in real time.

 **NOTE:** Reboot the VMware ESXi hosts for the new parameter to take effect.


Prerequisites

- Generate the pre-shared passwords for all the storage data clients to be configured.
- Ensure that you have the following information:
 - Primary and secondary MDM IP addresses or names
 - Credentials to access all VMware ESXi hosts running storage data clients

Steps

1. Using SSH log in to the VMware ESXi host using the provided credentials.
2. Type **esxcli system module parameters list -m scini | grep Ioctl** to list the hosts current `scini` parameters:

```
IoctlIniGuidStr          string    d30ff770-b64c-40b5-a341-58d18927e523
                          Ini Guid, for example: 12345678-90AB-CDEF-1234-567890ABCDEF
IoctlMdmIPStr            string
192.168.151.20,192.168.152.20,192.168.153.20,192.168.154.20  Mdms IPs, IPs for MDM in
same cluster should be comma separated. To configure more than one cluster use '+'
to separate between IPs.For Example: 10.20.30.40,50.60.70.80+11.22.33.44. Max 1024
characters
IoctlMdmPasswordStr      string
                          Mdms passwords. Each value
is <ip>-<password>, Multiple passwords separated by ';' signFor example: 10.20.30.40-
AQAAAAAAAAACS1pIywyOoC5t;11.22.33.44-tpPW0eap4cSjsKIcMax 1024 characters
```

 **NOTE:** The third parameter `IoctlMdmPasswordStr` is empty.

- Using ESXCLI, configure the driver with the existing and new parameters. To specify multiple IP addresses, use a semicolon (;) between the entries, as shown in the following example. Additional data IP addresses, data3, and data4 can be used, if required.

```
esxcli system module parameters set -m
scini -p "IoctlIniGuidStr=10cb8ba6-5107-47bc-8373-5bb1dbe6efa3
IoctlMdmIPStr=192.168.151.20,192.168.152.20 IoctlMdmPasswordStr=192.168.151.20-
AQAAAAAAAAA8UKVYp0LHCfD59BrnExNPvKSlGfLrwAk;192.168.152.20-
AQAAAAAAAAA8UKVYp0LHCfD59BrnExNPvKSlGfLrwAk bBlkDevIsPdlActive=1
blkDevPdlTimeoutMillis=60000"
```

NOTE: There are spaces between `Ioctl` parameter fields and the opening quotes. The example is entered on a single line.

- Reboot the VMware ESXi nodes.
The SDC configuration is applied.

If the SDC is a PowerFlex hyperconverged node, go to the next step. For other nodes, continue to Step 8.
- For PowerFlex hyperconverged nodes, use the presentation manager or `scli` tool to place the corresponding SDS into maintenance mode.
- If the SDS is also the cluster primary MDM, switch cluster ownership to a secondary MDM and verify cluster state before proceeding, type `scli --switch_mdm_ownership --mdm_name <secondary MDM name>`.
- Power off the SVM once the cluster ownership is switched (if needed) and the SDS is in maintenance mode.
- Manually migrate the workloads to the other hosts if required, and place the VMware ESXi host in maintenance mode.
- Reboot the VMware ESXi host.
- Once the host has completed rebooting, remove it from maintenance mode and power on the SVM (if present).
- Take the SDS out of the maintenance mode (if present).
- Repeat this procedure for each VMware ESXi SDC host.

Examples - Windows and Linux SDC nodes

Windows and Linux hosts have access to the `drv_cfg` utility, which allows driver modification and configuration in real time.

The `--file` option allows for persistent configuration to be written to the driver's configuration file (so that the SDC remains configured after a reload or reboot).

NOTE: Only one IP address is needed for the command to identify the MDM to modify.

Windows (from within a PowerShell prompt):

```
C:\Program Files\EMC\scaleio\sdh\bin\drv_cfg --set_mdm_password --ip <MDM IP> --port
6611 --password <secret>
```

Linux:

```
/opt/emc/scaleio/sdh/bin/drv_cfg --set_mdm_password --ip <MDM IP> --port 6611 --password
<secret> --file /etc/emc/scaleio/drv_cfg.txt
```

Iterate through the relevant SDCs, using the command examples along with the recorded information.

Enable storage data client authentication

Perform this procedure to enable storage data client authentication.

Prerequisites

- Make sure that all storage data clients are running PowerFlex, and are configured with their appropriate CHAP password. Any older or unconfigured storage data client will be disconnected from the system when authentication is turned on.
- Ensure that you have the following information:
 - Primary MDM IP address
 - Credentials to access the PowerFlex cluster

Steps

1. SSH into the primary MDM.
2. Type `scli --login --username admin --management_system_ip <management_system_ip>` to log in to the PowerFlex cluster using the provided credentials.
3. Type `scli --set_sdc_authentication --enable` to enable storage data client authentication feature.
4. Type `scli --check_sdc_authentication_status` to verify that the storage data client authentication and authorization is on, and that the storage data clients are connected with passwords.

Sample output:

```
[root@svml ~]# scli --check_sdc_authentication_status
SDC authentication and authorization is enabled.
Found 4 SDCs.
The number of SDCs with generated password: 4
The number of SDCs with updated password set: 4
```

5. If the number of storage data clients does not match or any storage data clients are disconnected, storage data clients, list any or all of the disconnected storage data clients and then disable the storage data client authentication by typing the following commands:


```
scli --query_all_sdc | grep "State: Disconnected"

scli --set_sdc_authentication --disable
```
6. Recheck the disconnected storage data clients to make sure that they have the proper configuration applied. If necessary, regenerate their shared password and reconfigure the storage data client. If you are unable to resolve the storage data client disconnection, leave the feature disabled and contact Dell Technologies support as needed.

Disable SDC authentication

Perform this procedure if you need to disable SDC authentication.

Prerequisites

Ensure all SDCs are configured with their appropriate CHAP secret. Any older or unconfigured SDC will be disconnected from the system when authentication is turned on.

You will need the following information:

- Primary MDM IP address
- Credentials to access the PowerFlex cluster

Steps

1. SSH to the primary MDM address.
2. Log in to the PowerFlex cluster using the provided credentials.
3. Disable the SDC authentication, type: `scli --set_sdc_authentication --disable`
Once disabled, SDCs will reconnect automatically unless otherwise configured.

Results

Once disabled, the SDCs reconnect automatically unless otherwise configured.

Expand an existing PowerFlex cluster with SDC authentication enabled

Once a PowerFlex cluster has SDC authentication that is enabled, new SDCs must have the configuration step that is performed after the client is installed. This procedure is not applicable for the PowerFlex management controller 2.0. For Windows PowerFlex compute-only nodes, only firmware upgrades are supported.

Prerequisites


Ensure you have the following information:

- Primary MDM IP address
- Credentials for the PowerFlex cluster
- The IP address of the new cluster members

Ensure you have added the SDC authentication enabled on the PowerFlex cluster.

Steps

1. Install and add the SDCs as per normal procedures (whether using PowerFlex Manager or manual expansion process).

 **NOTE:** New SDCs will show as **Disconnected** at this point, as they cannot authenticate to the system.

2. SSH to the primary MDM.
3. Log in to the PowerFlex cluster using the scli tool.
4. For each of your newly added SDCs, generate and record a new CHAP secret, type: `scli --generate_sdc_password --sdc_IP <IP of SDC> --reason "CHAP setup - expansion."`
5. SSH and log in to the SDC host.
6. If the new SDC is a VMware ESXi host, follow the rest of this procedure.
7. Type `-m scini | grep Ioctl` and `esxcli system module parameters list -m scini` to list the current scini parameters of the host.
8. Using esxcli, type `esxcli system module parameters set -m scini -p` to configure the driver with the existing and new parameters.
For example, `esxcli system module parameters set -m scini -p "IoctlIniGuidStr=09bde878-281a-4c6d-ae4f-d6ddad3c1a8f IoctlMdmIPStr=10.234.134.194,192.168.152.199,192.168"`.
9. At this stage, the SDC's configuration is ready to be applied. On ESXi nodes a reboot is necessary for this to happen. If the SDC is a hyperconverged node, proceed with step 10. Otherwise, go to step 12.
10. For PowerFlex hyperconverged nodes, use the presentation manager or scli tool to place the corresponding SDS into maintenance mode.
11. Once the SDS is in maintenance mode, the SVM may be powered off safely.
12. Place the ESXi host in maintenance mode. No workloads should be running on the node, as we have not yet configured the SDC.
13. Reboot the ESXi host.
14. Once the host has completed rebooting, remove it from maintenance mode and power on the SVM (if present).
15. Take the SDS out of maintenance mode (if present).
16. Repeat steps 5 through 15 for all ESXi SDC hosts.

Add a Windows or Linux authenticated SDC

Use the `drv_cfg` utility on a Windows or Linux machine to modify both a running and persistent configuration. Use the following examples to perform the task on a Windows or Linux based PowerFlex node.

About this task

For Windows PowerFlex compute-only nodes, only firmware upgrades are supported.

Prerequisites

Only one IP address is required for the command to identify the MDM to modify.

Steps

1. Press Windows +R.
2. To open the command line interface, type `cmd`.
3. For Windows, type `drv_cfg --set_mdm_password --ip <MDM IP>` in the `drv_cfg` utility. For example:

```
drv_cfg --set_mdm_password --ip <MDM IP> --port 6611 --password <secret>
```
4. For Linux, type `/opt/emc/scaleio/sdc/bin/drv_cfg --set_mdm_password --ip <MDM IP>`. For example:

```
/opt/emc/scaleio/sdc/bin/drv_cfg --set_mdm_password --ip <MDM IP> --port 6611 --password  
<secret> --file /etc/emc/scaleio/drv_cfg.txt
```
5. Repeat until all new SDCs are connected.

Administering the CloudLink Center

Add the CloudLink Center license in PowerFlex Manager

Use this procedure to add CloudLink Center in PowerFlex Manager.

Steps

1. Log in to PowerFlex Manager.
2. Click **Settings** > **License Management**.
3. Click **Other Software Licenses**.
4. Click **Add**.
5. Under **Upload License**, click **Choose License**.
6. Browse and select the license to upload and click **Open**.
7. Select the Type as **CloudLink** and click **Save**.
8. From **Resource**, select the CloudLink VMs, and click **Run inventory**.

Adding and managing CloudLink Center licenses

Perform the following procedures to add CloudLink Center licenses and manage CloudLink Center licenses through PowerFlex Manager.

License CloudLink Center

Use this procedure to add licenses to CloudLink Center.


About this task

CloudLink license files determine the number of machine instances, CPU sockets, encrypted storage capacity, or physical machines with self-encrypting drives (SEDs) that your organization can manage using CloudLink Center. License files also define the CloudLink Center usage duration.

 **NOTE:** CloudLink center can act as a key management interoperability protocol (KMIP) server if you upload a KMIP license to it.

Steps

1. Log in to CloudLink Center.
2. Select **System** > **License**.
3. Click **Upload License**.
4. Browse to select the software or hardware encryption license file and click **Upload**.

 **NOTE:** If the CloudLink environment is managed by PowerFlex Manager, after you update the license, go to the **Resources** page, select the CloudLink Center VMs, and click **Run Inventory**.

Delete expired or unused CloudLink Center licenses from PowerFlex Manager

Use this procedure to delete expired or unused CloudLink Center licenses from PowerFlex Manager.

Steps

1. Log in to PowerFlex Manager.
2. Click **Settings > License Management > Other Software Licenses**.
3. Select the license you want to delete, and click **Delete**.
4. From **Resource**, select the CloudLink VMs, and click **Run inventory**.

Configure a custom syslog message format in CloudLink Center

Use this procedure to configure a custom syslog message format.

Steps

1. Log in to CloudLink Center.
2. Click **Server > Syslog > Change Syslog Format**. The **Change Syslog Format** window appears..
3. From the **Syslog Format** list, select the **Custom** message format.
4. Enter the string for the syslog entry and click **Change**.

Manage a self-encrypting drive (SED) from CloudLink Center

Use this procedure to manage an SED device through CloudLink Center.

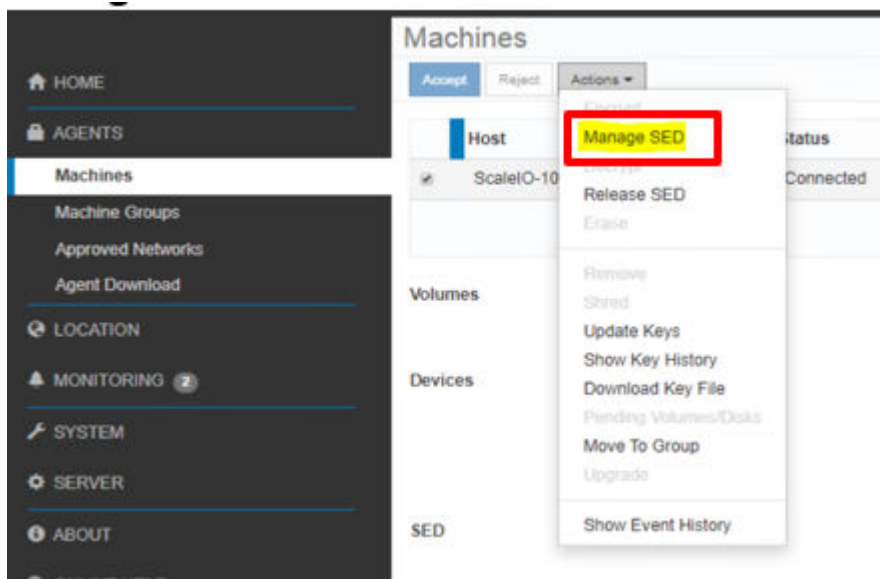
About this task

When managing SEDs from CloudLink Center, be aware of the following:

- CloudLink Center can manage encryption keys for self-encrypting drives (SEDs).
- Managing SEDs with CloudLink Center is functional when the CloudLink agent is installed on machines with SEDs.
- When managed by CloudLink Center, SED encryption keys are stored in the current keystore for the machine group they are in.
- The functionality for managing SEDs requires a separate SED license.
- If the SED cannot retrieve the key from CloudLink Center, the SED remains locked.

Steps

From the CloudLink Center, select **Agent > Machines**, click **Actions** and select **Manage SED**. Ownership of the encryption key is enabled.



NOTE: This option is only available if an SED license is uploaded and an SED is detected in the physical machine managed by CloudLink Center. The **Manage SED** option does not change data on an SED it only takes ownership of the encryption key.

Manage a self-encrypting drive from the command line

As an alternative to CloudLink Center, use the command line to manage an SED.

Steps

1. Log in to the storage data servers (SDS).
2. To manage the SED from the command line, type `svm manage [device name]`.
For example, `svm manage /dev/sdb`.

Release a self-encrypting drive

Use this procedure to release an SED that is managed by CloudLink.

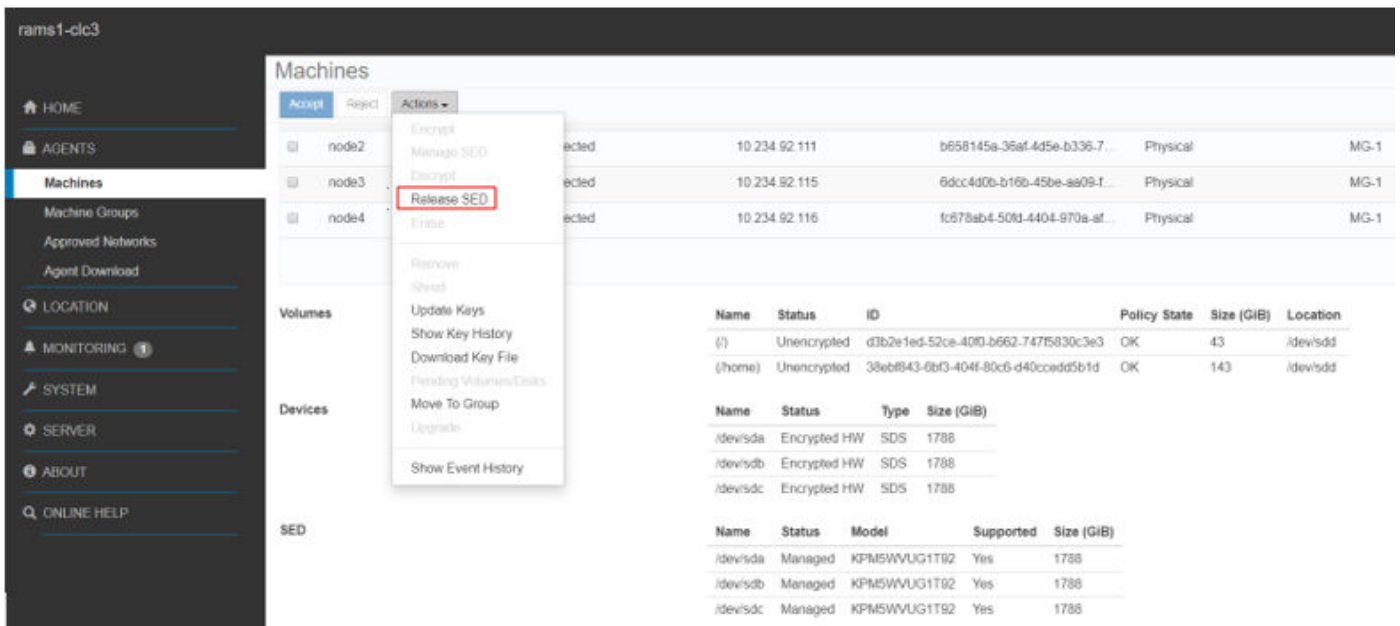
About this task

This option allows you to release ownership of an SED that is managed by CloudLink. This option is only available if an SED license is uploaded and an SED is detected in the physical machine managed by CloudLink Center.

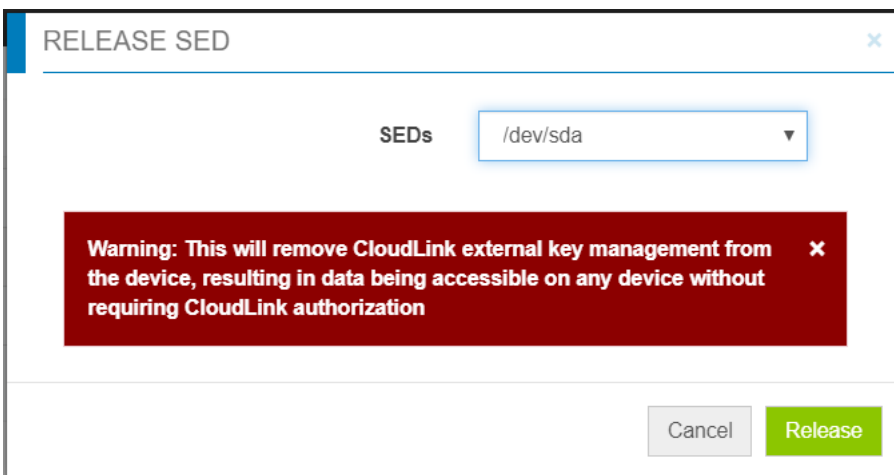
When CloudLink releases an SED, the encryption key is released in CloudLink Center.

Steps

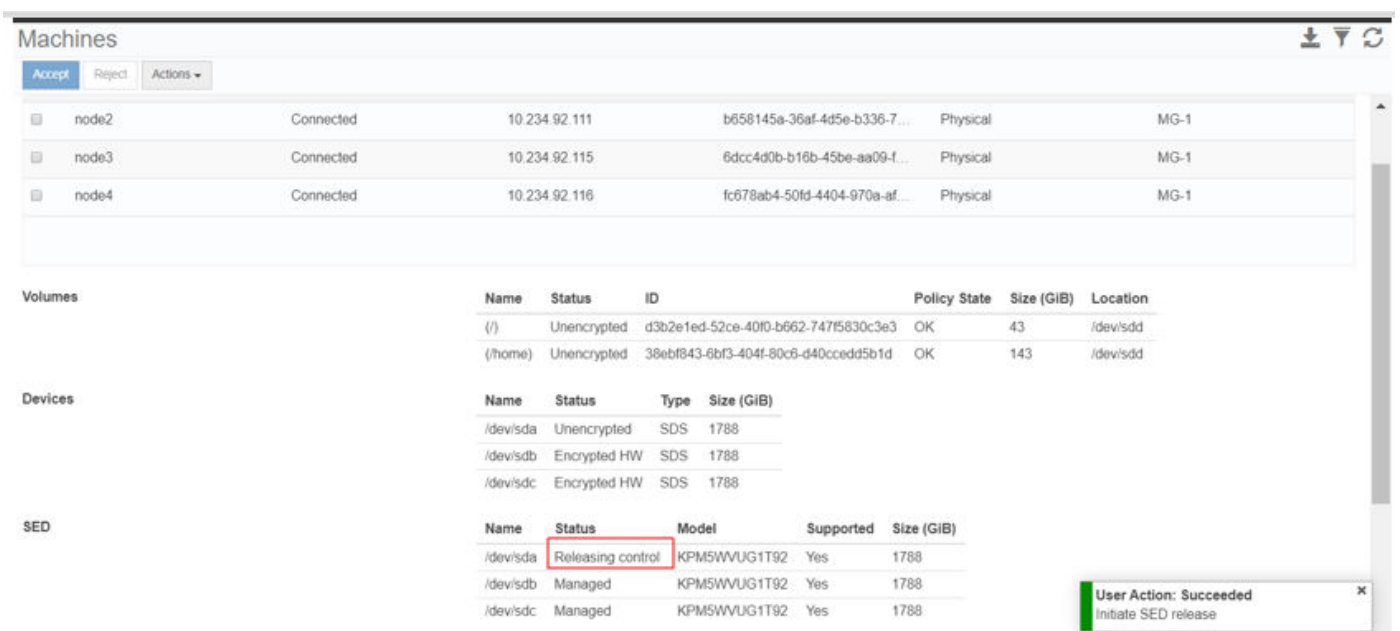
1. From CloudLink Center, go to **Agents > Machines** and select **SDS Machine**. Click **Release SED**.




- From **RELEASE SED**, use the menu to select the SED drive that you want to release and click **Release**.



The status of the SED drive changes to **Releasing Control**.



Once CloudLink releases the control, the SED device status shows as **Unmanaged**.

 **NOTE:** The **Release SED** option does not change any data on the SED.

Release management of a self-encrypting drive from the command line

Use this procedure to release an SED using the command line.

Steps

1. Log in to the storage data server (SDS).
2. To release the SED from the command line, type `svm release [device name]`.

For example, `svm release /dev/sdb`.

Backup and restore

This section contains instructions for backing up and restore for PowerFlex rack components. Backups of collected data is critically important in data management which allows you to restore to a previously known state.

This section also provides instructions for backing up and restoring CloudLink Center.

VMware vCenter Server

Back up VMware vCenter Server

Manually backup the VMware vCenter.

Prerequisites

You must have an FTP, FTPS, HTTP, HTTPS, SFTP, NFS, or SMB server up and running with sufficient disk space to store the backup.

NOTE: If you back up a vCenter Server High Availability cluster, the backup operation only backs up the primary vCenter Server instance. Before restoring a vCenter Server High Availability cluster, you must power off the active, passive, and witness nodes. The restore operation restores the vCenter Server in non-vCenter Server High Availability mode. You must reconstruct the cluster after the restore operation completes successfully.

Steps

1. Go to the vCenter Server Management Interface, <https://appliance-IP-address-or-FQDN:5480> and log in as root.
2. In the vCenter Server Management Interface, click **Backup**.
3. Click **Backup Now**.
4. Enter the backup location details.
5. (Optional) Enter an encryption password if you want to encrypt your backup file.
If you select to encrypt the backup data, you must use the encryption password for the restore procedure.
6. (Optional) Select **Stats**, **Events**, and **Tasks** to back up additional historical data from the database.
7. (Optional) In the Description text box, enter a description of the backup.
8. Click **Start** to begin the backup process.

Restore VMware vCenter Server

Perform this procedure to deploy the VMware vCenter Server Appliance on the PowerFlex R650 controller node planned for vCenter deployment.

About this task

Deploying VMware vCenter Server Appliance (vCSA) is a two-step process:

- Deploy a new appliance to the target VMware vCenter server or ESXi host
- Copy data from the source appliance to the VMware vCenter Server Appliance

Steps

1. Mount the ISO and open the VMware vCSA 7.x installer from `\vcsa-ui-installer\win32\installer.exe`.
2. Select **Restore** from the VMware vCSA 7.x installer.

3. Click **Next** in Stage 1: Deploy vCenter Server wizard.
4. Accept the End User License Agreement and click **Next**.
5. Enter the backup details:
 - Location: The following protocols are supported: FTP, FTPS, HTTP, HTTPS, SFTP, NFS, or SMB
 - ex. ftp://<server_IP_address>/tmp/vCenter/hostname_vcenter.com/<backup_filename>
 - Username: Enter the user name of a user with read privileges on the backup server
 - Password: Enter the password of the user with read privileges on the backup server
6. Click **Next**.
7. Review **Backup Details** and click **Next**.
8. Type the host FQDN of the PowerFlex management controller:
 - a. Provide all the log in credentials.
 - b. Click **Next > Yes**.
9. Accept the certificate warning.
10. Select the deployment size to large and leave storage as default. Click **Next**.
11. In the Select Datastore page, select the Datastore location.
12. Select **Enable Thin Disk Mode**.
13. Click **Next**.
14. Verify the network settings populated from the backup file of the vCenter Server.
15. Click **Next**.
16. Review the summary and click **Finish**.
17. Wait for the OVA deployment to finish.
18. Copy data from the source appliance to the VMware vCenter Server Appliance:
 - a. Click **Continue** and click **Next** on the Introduction page.
 - b. Review the backup details and click **Next**.
 - c. Enter single sign-on username and password and click **Validate and Recover > Next**.
 - d. On the Ready to complete page, review the details, and click **Finish > OK**.
 - e. After the restore finishes, click **Close**.

PowerFlex Manager

Performing a backup saves all user-created data to a remote share from which it can be restored. To restore from a backup, you need to run a script outside of PowerFlex Manager. The user interface does not support the ability to restore from a backup.

Perform frequent backups to guard against data loss and corruption. The best practice is to take a snapshot of PowerFlex Manager every time you perform a restore.

The **Backup** page displays information about the last backup operation that was performed on PowerFlex Manager. The information provided applies to both manual and automatically scheduled backups and includes the following:

- Last backup date
- Last backup status
- Back up directory path to a CIFS share
- Back up directory username

The **Backup** page also displays information about the status of automatically scheduled backups (enabled or disabled).

On this page, you can:

- Manually start an immediate backup
- Edit general backup settings
- Edit automatically scheduled backup settings

After performing a backup operation, you need to run a script outside of PowerFlex Manager to restore from the backup. The user interface does not support the ability to restore from a backup.

Edit the backup settings and details

You can change the location where backup files are saved or the password that is required to access a backup file.

Steps

1. On the menu bar, click **Settings > Serviceability**.
2. Click **Backup**.
The **Backup** page opens.
3. Click **Backup Settings**.
4. Indicate the network share location where the backup file is saved, enter a backup directory path in the **Backup Directory Path** box.
Use the following format:
 - CIFS—\\host\share
5. If the username and password are required to access the network share, enter a username and password in the **Backup Directory User Name** and **Backup Directory Password** boxes.
6. Click **Test Connection** to confirm that the backup settings you provided are correct.
7. To open the backup file, enter a password in the **Encryption Password** box.
8. To verify the encryption password, enter the password in the **Confirm Encryption Password** box.
9. To schedule automatic backups, next to **Scheduled Backups**, select **Enabled**. To discontinue automatically scheduled backups, deselect **Enabled**.
10. To specify the days on which backup must occur, select the days under **Frequency**.
11. From the **Run Time** drop-down list, select the time.
12. Click **Save**.

Back up PowerFlex Manager

In addition to automatically scheduled backups, you can manually run an immediate backup.

Steps

1. Log in to PowerFlex Manager.
2. On the menu bar, click **Settings > Serviceability**.
3. Click **Backup**.
4. Click **Backup Now**.
5. Select one of the following options:
 - To use the general settings that are applied to all backup files, select **Use Backup Directory Path and Encryption Password from Settings and Details**.
 - To use custom settings:
 - a. In the **Backup Directory Path** box, enter a file path where the backup file is saved. Use this format:
CIFS—\\host\share\
 - b. Optionally, enter a username and password in the **Backup Directory User Name** and **Backup Directory Password** boxes, if they are required to access the location you provided.
 - c. Click **Test Connection** to confirm that the backup settings you provided are correct.
 - d. In the **Encryption Password** box, enter a password that is required to open the backup file, and verify the encryption password by entering the password in the **Confirm Encryption Password** box.
6. Click **Backup Now**.


Completing the restore of PowerFlex Manager

Restoring PowerFlex Manager returns user-created data to an earlier configuration that is saved in a backup file. To restore from a backup, you need to run a script outside of PowerFlex Manager. The user interface does not support the ability to restore from a backup.

About this task

 **CAUTION:** Restoring an earlier configuration restarts PowerFlex Manager and deletes data created after the backup file to which you are restoring. Any running jobs could be terminated as well.

Perform frequent backups to prevent data loss and corruption. Perform a back up of PowerFlex Manager after completing a restore.

 **NOTE:** Before removing the PowerFlex management platform installer VM, take a backup of the **PFMP_Config.json** file located at `/opt/dell/pfmp/PFMP_Installer/config`. The **PFMP_Config.json** file is required when restoring PowerFlex Manager.

Restore the **PFMP_Config.json** file to `/opt/dell/pfmp/PFMP_Installer/config` that was backed up before removing installer VM. This is typically backed up to the jump server.

Install the same version or release of the installer that deployed the PowerFlex management platform.

Steps

1. From VMware vCSA, power on the PowerFlex management platform installer VM.
2. Log in to the PowerFlex management platform installer VM.
3. Run the restore script that is included with the installer bundle:

```
./restore-PFMP.sh [BACKUP_LOCATION] [ENCRYPTION_PASSWORD] {CIFS_USERNAME}
[CIFS_PASSWORD]
```

The *BACKUP_LOCATION* path supports CIFS. The *CIFS_USERNAME* and *CIFS_PASSWORD* parameters are optional.

Results

The restore process prints out status information until the restore is complete. Perform a back up of PowerFlex Manager after completing the restore.

Integrated Dell Remote Access Controller

Back up iDRAC

Steps

1. Log in to the iDRAC using root credentials.
2. Click **Configuration > Server Configuration Profile**.
3. Click **Export**.
4. Select one of the following to specify the location type:
 - **Local** to save the configuration file on a local drive.
 - **Network Share** to save the configuration file on a CIFS or NFS share.
 - **HTTP or HTTPS** to save the configuration file to a local file using HTTP/HTTPS file transfer.

Depending on the location type, you must enter the Network Settings or HTTP/HTTPS settings. If proxy is configured for HTTP/HTTPS, proxy settings are also required.

5. Select the components that you need to back up the configuration for.
6. Select the **Export** type:

- Basic
- Replacement Export
- Clone Export

7. Select an **Export file format**.
8. Select **Additional export items**.

Restore iDRAC

Steps

1. Click **Configuration > Server Configuration Profile**.
2. Select one of the following to specify the location type:
 - **Local** to save the configuration file on a local drive.
 - **Network Share** to save the configuration file on a CIFS or NFS share.
 - **HTTP or HTTPS** to save the configuration file to a local file using HTTP/HTTPS file transfer.

Depending on the location type, you must enter the Network Settings or HTTP/HTTPS settings. If proxy is configured for HTTP/HTTPS, proxy settings are also required.


3. Select the components listed in the **Imported Components** option.
4. Select the **Shutdown** type.
5. Select the Maximum wait time to specify the wait time before the system shuts down after the import is complete.
6. Click **Import**.

Network switch configuration back up and restore

Back up and restore running configuration of the Cisco and Dell switches.

About this task

If switches are owned by customer, advise customers to take the switch backup immediate after successful PowerFlex rack deployment.

 **NOTE:** The customer is responsible for providing the backup location and maintaining the backup as well. Dell Technologies recommends to store the backup in separate shared location, for example, not on the jump server.

Steps

1. Connect to the Cisco Nexus or Dell PowerSwitch switch, either via console cable, Telnet or SSH using admin credentials, type **#copy running-config scheme://server/[url/]filename**.
For the scheme argument, you can enter **tftp:**, **ftp:**, **scp:**, or **sftp:**.
The server argument is the address or name of the remote server, and the URL argument is the path to the source file on the remote server. The server, URL, and file name arguments are case sensitive.
For example:

```
switch# copy running-config tftp://10.10.10.1/sw1-run-config.bak
switch# copy running-configuration scp://root:calvin@10.11.10.12/tmp/backup.txt
```
2. Restore the network configuration, connect to the Cisco Nexus or Dell PowerSwitch switch, either via console cable, Telnet or SSH using admin credentials, type **#copy running-config scheme://server/[url/]filename running-config**.
For the scheme argument, you can enter **tftp:**, **ftp:**, **scp:**, or **sftp:**.
The server argument is the address or name of the remote server, and the URL argument is the path to the source file on the remote server. The server, URL, and file name arguments are case sensitive.
For example:

```
switch# copy tftp://10.10.10.1/my-config running-config
switch# copy scp://root:calvin@10.11.10.12/tmp/backup.txt running-configuration
```

Backing up and restoring CloudLink Center

Use this procedure to create a CloudLink Center backup file.

View backup information

You can view the Backup page information.

To view the backup information, log in to the CloudLink Center, and click **System > Backup**. The **Backup** page lists the following information:

- **Backup File Prefix**—Prefix used for the backup files.
- **Current Key ID** —The identifier for the current RSA-2048 key pair.
- **Current Backup File** —The name of the current backup file.
- **Current Backup Time**—The date and time that the current backup file was generated.
- **Backup Schedule**—The schedule for generating automatic backups.
- **Next Backup In** —The time remaining before the next automatic backup is generated.

When a backup file is downloaded, the **Backup** page lists the following additional information:

- **Last Downloaded File** —The name of the backup file that was last downloaded. Only shown when a backup file has been downloaded.
- **Last Downloaded Time** —The date and time of the last backup file download. Only shown when a backup file has been downloaded.
- **Backup Store** —The backup store configuration type. If you have not configured a backup store, the value is Local, which is stored on the local desktop.

You can also use the FTP or SFTP servers as backup stores. To change the backup store, click **Actions > Change Backup Store**.

If you have configured an FTP or SFTP backup store, the following additional information is available:

- **Host** —The remote FTP, SFTP, or FTPS host where you saved the CloudLink Center backups. You can set this value to the host IP address or hostname (if DNS is configured).
- **Port**—The port used to access the backup store.
- **User**—The user with permission to access the backup store.
- **Directory**—The directory in the backup store where backup files are available.

Change the schedule for automatic backups

CloudLink Center automatically generates a backup file each day at midnight (UTC time).

To change the schedule for generating automatic backups, click **System > Backup > Actions > Change Backup Schedule**.

Generate a backup file manually

Use this procedure to generate a backup manually, if you want to preserve CloudLink Center before the next automatic back up. Download the backup file when you generate a backup file manually.

Steps

1. Log in to the CloudLink Center.
2. Click **System > Backup**.
3. Click **Generate New Backup**. A backup file is generated.

Generate a backup key pair

You can generate a new backup key pair. For example, if the private key for a backup key pair is lost, you can generate a new key pair. You cannot access your backup files without the associated private key. When you generate a new key pair, CloudLink

Center automatically generates a new backup file to ensure that the current backup can be opened with the private key of the current key pair.

Dell recommends the following practices when you generate a new backup key pair.

1. Download the private key to the Downloads folder for the current user account. For example, C : \Users\Administrator\Downloads.
NOTE: The previously generated backup key will not open the backup file created, after a new key is generated.
2. Generate the new key pair by clicking **System > Backup > Actions > Generate and Download New Key**.
3. Click **Generate and Download**.

Download the current backup file

You can download the current backup file at any time. The current backup file is either:

- The last backup file that CloudLink Center automatically created.
- The last backup file that you manually generated after the last automatic backup.

To download the backup file:

1. Click **System > Backup > Actions > Download Backup**.
2. In the **Download Current Backup** dialog box, click **Download**.

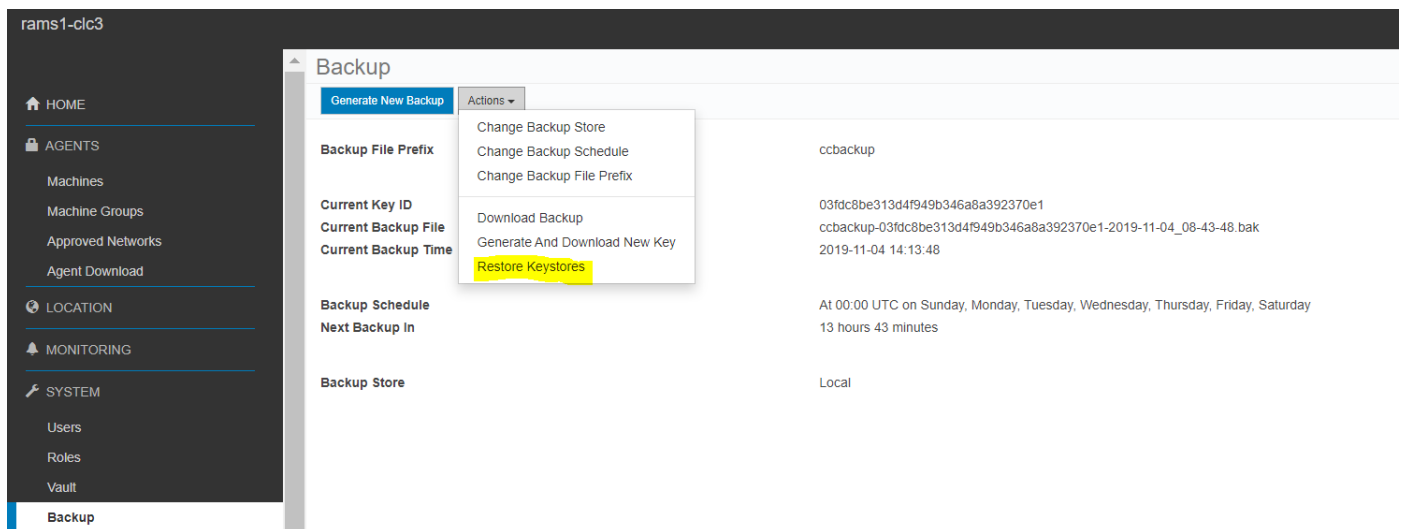
When you download the current backup file, CloudLink Center shows the age of the backup file.

Restore the CloudLink backup

Use this procedure to restore the CloudLink backup.

Steps

1. Log in to the CloudLink Center.
2. Click **System > Backup > Actions > Restore Keystores**.



3. In the **Restore Keystores** dialog box, complete the following steps:
 - a. In the **Key** box, browse to the private key file.
 - b. In the **Backup** box, browse to the backup file.
 - c. In the **Unlock** box, type the passcode that was set during the initial configuration of the CloudLink Center.
 - d. Click **Restore**.

RESTORE KEYSTORES

Key

cckey-03fdc8be313d4i

Backup

ccbackup-03fdc8be31:

Unlock Passcode

.....|

Cancel

Restore


A **Restore Keystores succeeded** message is displayed.

NOTE: If the CloudLink backup is not associated with a key pair, the file is corrupted or key mismatch error message is displayed. In such a scenario, generate a new key pair and download the backup file.

Powering on and off

Power on a Technology Extension with PowerScale

Prerequisites

 **NOTE:** The Technology Extension for PowerScale must be powered on before the PowerFlex rack is powered on.

Steps

1. Power on the switches in the PowerScale cabinet.
2. Power on node 1 first by pressing the **Power** button that is located on the back of the node that is labeled as node 1.
3. Using a serial connection, connect to the console port of node 1 with a laptop and a HyperTerminal or similar connection.
4. Monitor the status of the boot process for node 1. When node 1 has completed booting, it displays the **login** prompt. Note any error codes or amber lights on the node. Resolve any issues before moving to node 2.
5. Move to node 2, power on, and monitor the boot process.
6. Repeat the procedure for each node in the cluster in sequential order.
When all nodes have completed booting, then entire cluster is powered on.

Next steps

See the relevant procedure to power on the PowerFlex rack.


Power on a PowerFlex rack

To safely power on the system, power on one component at a time, in the order specified in this procedure.


About this task

Power on workflow:

- Power on the PDUs
- Power on the network switches
- Power on the PowerFlex management controller 2.0
- Power on the CloudLink Center VMs that are running on management cluster in VMware vCenter (controller data center)
- Power on the UCC Edge VM if Flex on demand is in use
- For PowerFlex file:
 - For PowerFlex file enabled system with hyperconverged:
 - Power on PowerFlex hyperconverged nodes
 - Activate PowerFlex protection domains
 - Power on PowerFlex file nodes
 - For PowerFlex file enabled system with storage-only:
 - Power on PowerFlex storage-only nodes
 - Activate PowerFlex protection domains
 - Power on PowerFlex file nodes
 - Power on the PowerFlex compute-only nodes
- For all other PowerFlex systems:
 - Power on the PowerFlex storage-only nodes
 - Power on the PowerFlex hyperconverged nodes with VMware ESXi
 - Activate protection domains

 **NOTE:** If asynchronous replication is enabled activate the protection domain on both source and destination protection domains.

- Power on the PowerFlex compute-only nodes
- Power on the VMware NSX Edge nodes (if applicable)
- Power on all VMs on or single VMware vCenter (customer cluster VMs)
- Check PowerFlex health and rebuild status

 **NOTE:** Powering on must be completed in this order for the components that you have in your environment. Prioritize and power on the PowerFlex storage-only nodes or PowerFlex hyperconverged nodes with PowerFlex metadata manager (MDM) first.

Prerequisites


- Confirm that the servers are not damaged from the shipment.
- Verify that all connections are seated properly and check the manufacturing handoff notes for any items that must be completed.
- Verify that the following items are available:
 - Customer-provided services such as Active Directory, DNS, NTP
 - Physical infrastructure such as reliable power, adequate cooling, and core network access

See Cisco documentation for information about the LED indicators.

See [Dell PowerSwitch S5200 Series Installation Guide](#) for information about the LED indicators for Dell PowerSwitch switches.

Steps

1. Verify that the PDU breakers are in the OPEN (OFF) positions. If the breakers are not OPEN, use the small enclosed tool to press the small white tab below each switch for the circuit to open. These switches are located below the ON/OFF breaker.
2. Connect the external AC feeds to the PDUs.
3. Verify that power is available to the PDUs and a number is displayed on the LEDs of each PDU.
4. Close the PDU circuit breakers on all PDUs for Zone A by pressing the side of the switch that is labeled **ON**. This action causes the switch to lie flat. Verify all the components that are connected to the PDUs on Zone A light up.
5. Close the PDU circuit breakers on all PDUs for Zone B by pressing the side of the switch that is labeled **ON**. Verify all the components that are connected to the PDUs on Zone B light up.
6. Power on the network components in the following order:

 **NOTE:** Network components take about 10 minutes to power on.

- Management switches - Wait until the PS1 and PS2 LEDs are solid green before proceeding.
- Cisco Nexus aggregation or leaf-spine switches - Wait until the system status LED is green before proceeding.
- Dell PowerSwitch switches - Wait until the system status LED is solid green before proceeding.

Next steps

Power on the PowerFlex management controller.

Power on the PowerFlex management controller 2.0

Use this procedure to power on the PowerFlex management controller 2.0.

Steps

1. Log in to iDRAC and power on all the PowerFlex controller nodes. Monitor the virtual console and wait for some time for the VMware ESXi server to appear.
2. Log in to each VMware ESXi server and verify that all the SVMs have started with the host.
3. Power on all the PowerFlex management platform nodes (management virtual machines from VMware ESXi host client):
 - a. Log in to VMware ESXi using the host client.
 - b. Click **Virtual Machines**, select the management virtual machine, and click **Power on**.
 - c. Repeat step 3b to power on all the management virtual machines.
4. Log in to the nodes running PowerFlex management platform processes (all three management virtual machines):

- a. Run the following command to check the status of the rke2-server:

```
#systemctl status rke2-server
```

Do the following depending on the rke2-server status:

Status of the rke2-server	Do the following
active	Go to the next step.
activating	Repeat the command to check the rke2-server status until active.
failed	Attempt to start the service by running the following command: <pre>#systemctl start rke2-server</pre>

5. Once the rke2-server is running on all the three PowerFlex management platform nodes, ensure that all nodes are in ready state:

- a. Log in to the PowerFlex management platform primary node using SSH and run the following command:

```
#kubectl get nodes
```

If you see an error message, wait for a few minutes and try again. Once the nodes are in ready state, go to the next step.

6. Restore the cluster monitoring operator (CMO) database:

```
#alias k="kubectl -n $(kubectl get pods -A | grep -m 1 -E 'platform|pgo|helmrepo' | cut -d' ' -f1)"

#kubectl config set-context default --namespace=$(kubectl get pods -A | grep -m 1 -E 'platform|pgo|helmrepo|docker' | cut -d' ' -f1)

#k patch $(k get postgrescluster -o name) --type merge --patch '{"spec":{"shutdown":false}}'
```

7. Verify the CMO database:

```
#echo $(kubectl get pods -l="postgres-operator.crunchydata.com/control-plane=pgo" --no-headers -o name && kubectl get pods -l="postgres-operator.crunchydata.com/instance" --no-headers -o name) | xargs kubectl get -o wide
```

8. Monitor the PowerFlex management platform status:

- a. Run the following command to identify the port number for the PowerFlex management platform monitor utility:

```
#kubectl get services monitor-app -n powerflex -o jsonpath="{.spec.ports[0].nodePort}{"\n\"}"
```

Wait for 20-30 minutes and check the overall health status of the PowerFlex management platform.

9. Go to **http://<node IP>:port/**

Where, the node IP address is a management IP address configured on any of the management virtual machines (not the Ingress or PowerFlex management platform UI IP address).

10. Click **PFMP status** and wait for all entries to turn green.

Contact Dell Technical Support if the PowerFlex management platform status persists as red or the main UI is not accessible after 20-30 minutes.

11. Log in to the primary MDM using SSH.

12. Log in to the MDM cluster:

```
#scli --login --management_system_ip <PFxM_IP_Address> --username admin --password <PFxM_Password>
```

13. Verify that the cluster status is Normal:

```
#scli --query_cluster
```

Wait for the rebalance to complete before resuming workload. Contact Dell Technical Support if the cluster status is not in Normal state.

14. To check the rebuild or rebalance status, run the following:

```
#scli --query_all |grep -i reb
```

15. Verify all volumes are available:

```
#scli --query_all_volumes
```

16. Power on the vCenter VM from the VMware ESXi host client, if vCenter high availability is configured, power on active, passive, and witness nodes (nodes can start in any order):
- Log in to VMware ESXi using the host client.
 - Click **Virtual Machines**, select the management virtual machine, and click **Power on**.
17. Modify the startup order of SVMs to manual to enable the vSphere high availability. This is applicable for all SVMs in the management controller PowerFlex cluster:
- In the vSphere Client, select the host where the VM is located.
 - Click the **Configure** tab.
 - Under **Virtual Machines**, select **VM Startup/Shutdown**, and click **Edit**.
The **Edit VM Startup and Shutdown** window opens.
 - To modify the startup order of the virtual machines, select a VM from the **Automatic Startup** category and use the up arrow to move the VM to the **Manual Startup** category.
 - Select the SVM and move back to **Manual Startup** category.
 - Clear the **Automatically start and stop the virtual machines with the system** check box and click **OK**.
 - Repeat the steps for all the SVMs.
18. Enable vSphere high availability:
- Log in to VMware vSphere Client.
 - Click **vSphere Client > Shortcuts > Hosts and Clusters**.
 - Browse to the cluster.
 - Click the **Configure** tab.
 - Select **vSphere Availability** and click **Edit**.
 - Click the toggle button to enable **vSphere HA**.
 - Click **OK**.
19. Power on all other VMs, such as, CloudLink and SCG:
- Log in to VMware vSphere Client.
 - From **vSphere Client > Shortcuts > Hosts and Clusters**.
 - Browse and right-click the VM and click **Power > Power on**.
20. Verify that all the VMs are up and running.

Power on the VMware NSX Edge nodes

Use this procedure to turn on the VMware NSX Edge nodes.


Steps

- Power on the VMware NSX Edge nodes.
- Verify that VMware ESXi has booted and you can ping the management IP address.
- Power on the VMware NSX Edge VMs.

Power on PowerFlex storage-only nodes

Use this procedure to power on PowerFlex storage-only nodes.

Steps

1. From iDRAC, power on all PowerFlex storage-only nodes and allow them time to boot completely.
 **NOTE:** Perform steps 2 to 6 only for a PowerFlex storage-only node cluster, and where the MDM is part of the PowerFlex storage-only node. Do not perform steps 2 to 7 when the PowerFlex storage-only node is part of hyperconverged environment. Activation of PD is included as part of power on PowerFlex hyperconverged node.
2. Log in to the PowerFlex Manager:
 - a. Click **Block > SDSs**. Verify all the SDSs are healthy.
 - b. Click **Block > Devices**. Verify all the SDSs are healthy.
 - c. Click **Block > Protection Domain**, select the protection domain, and click **More actions > Active**.
3. Log in to all host iDRACs as `root` and confirm the NTP, syslog, and SNMP settings.
4. Use SSH to connect to all network switches.
5. To verify that connected interfaces are not in a **not connected** state, type:

```
show interface status
```
6. Do the following:
 - a. Log in to the jump server on the controller stack.
 - b. At the command prompt or the terminal, type **nslookup**, against the correct DNS and verify that the DNS is correct.
For example, `nslookup eagles-r640-f-158.lab.vce.com (node hostname) 10.234.134.100 (dns server ip address)`.

Power on PowerFlex file nodes

Use this procedure to power on PowerFlex file nodes.

Steps

1. From iDRAC, power on all PowerFlex file nodes and allow them time to boot completely.
2. Log in to PowerFlex Manager, verify the **Resource group** is healthy.
3. Ensure back-end PowerFlex storage is up and running before powering on PowerFlex file cluster.
4. Power on PowerFlex file cluster by logging into each PowerFlex file node, type:

```
svc_nas_ctl --enable_ha_monitoring  
svc_nas_ctl --start_nas_container
```

Rarely there can be a requirement for recovery post bring up on NAS volumes which will need service engagement.

Power on all PowerFlex hyperconverged nodes

Use this procedure to power on PowerFlex hyperconverged nodes with VMware ESXi.

Steps

1. From iDRAC, power on all PowerFlex hyperconverged nodes with VMware ESXi and allow them time to boot completely.
2. Log in to the VMware vSphere Client if the PowerFlex rack includes VMware vSphere.
3. Take each PowerFlex hyperconverged node with VMware ESXi out of maintenance mode.
4. If the PowerFlex rack is a full VMware ESXi deployment, power on the MDM cluster PowerFlex VMs, primary, two secondaries, and two tiebreakers.
5. Log in to PowerFlex Manager.
 - a. On the **Block** menu, click **SDSs**. Verify that all the SDSs are healthy.
 - b. On the **Block** menu, click **Devices**, and verify that the devices are online.

- c. Verify that asynchronous replication is enabled:
 - Under the **Protection** menu, click **SDRs**. Verify that the SDRs are healthy.
 - Under the **Protection** menu, click **Journal Capacity**. Ensure that the journal capacity has already been added.
- d. On the **Block** menu, click the protection domain. Select each protection domain, under **More Actions**, select **Activate**.
- e. In the **Active Protection Domain** dialog box, click **Yes** for Force activate and click **Activate** to enable access to the data on the protection domain.
- f. Verify that the operation has successfully completed and click **Dismiss**.
- g. Verify that there are no errors, warnings, or alerts on the Dashboard.

Power on PowerFlex compute-only nodes

Use this procedure to power on PowerFlex compute-only nodes with VMware ESXi.

Steps

1. From iDRAC, power on all PowerFlex compute-only nodes and allow them time to boot completely.
2. For PowerFlex compute-only nodes with VMware ESXi:
 - a. Log in to the VMware vSphere Client if the PowerFlex rack includes VMware vSphere.
 - b. Take each PowerFlex compute-only node with VMware ESXi out of maintenance mode.

Complete the powering on of PowerFlex rack

Complete the power on process for PowerFlex compute-only nodes with VMware ESXi.

Steps

1. From vCenter, power on the remaining VMs of all PowerFlex compute-only nodes with VMware ESXi.
2. From the VMware vSphere Client:
 - a. Rescan to rediscover datastores.
 - b. Mount the previously unmounted datastores, and add any missing VMs to the inventory.
 - c. Power on the remaining VMs.
3. For VMware vSphere, enable HA, DRS, and affinity rules.
4. Delete expired or unused CloudLink Center licenses from PowerFlex Manager using the following commands:
 - a. Log in to PowerFlex Manager.
 - b. Click **Settings > License Management > Other Software Licenses**.
 - c. Select the license to delete and click **Remove**.
 - d. Go to the resource, select the CloudLink VMs, and click **Run inventory** and click **Close**.


Power off a PowerFlex rack


To safely power off the PowerFlex rack, power off one component at a time, in the order specified in this procedure.

About this task

Power off workflow:

- Check PowerFlex health, and rebuild status
- Power off all production cluster VMs on VMware vCenter (except the management virtual machine for controller cluster, SVM on both controller and production cluster, and VMware vCenter VM)
- For PowerFlex file:
 - For PowerFlex file enabled system with storage-only:
 - Power off the PowerFlex compute-only nodes with VMware ESXi
 - Power off PowerFlex file nodes
 - Deactivate PowerFlex protection domains
 - Power off PowerFlex storage-only nodes
 - For PowerFlex file enabled system with hyperconverged:

- Deactivate PowerFlex protection domains
 - Power off PowerFlex hyperconverged nodes
 - Power off PowerFlex file nodes
 - For all other PowerFlex systems:
 - Power off the CloudLink Center VMs that are running on management vCenter
 - Deactivate PowerFlex protection domains and power off PowerFlex storage-only nodes (both source and destination protection domains if asynchronous replication is enabled)
 - Power off PowerFlex compute-only nodes with VMware ESXi
 - Power off VMware NSX Edge nodes
 - Power off PowerFlex storage-only nodes
 - Power off PowerFlex hyperconverged nodes with VMware ESXi
 - Power off the UCC Edge VM if Flex on demand is in use
 - Power off the PowerFlex management controller 2.0
-  **CAUTION:** The power off procedure for PowerFlex management controller 2.0 and the PowerFlex production cluster are different. To power off PowerFlex management controller 2.0, see *Power off the PowerFlex management controller 2.0*.
- Power off PDUs

 **NOTE:** Powering off must be completed in this order for the components that you have in your environment.

Identify node types in the PowerFlex Manager:

- For PowerFlex hyperconverged nodes, click **Block > Host or Block > SDSs**.
- For PowerFlex compute-only nodes with VMware ESXi, click **Block > Hosts**.

Prerequisites

To facilitate powering on the PowerFlex rack later, document the location of the management infrastructure VMs on their respective hosts. Also, verify that all startup configurations for the Cisco and Dell devices are saved.

See the *Dell VxBlock™ System 1000 and PowerFlex Physical Planning Guide* for information about power specifications.

Steps

1. Check PowerFlex health and rebuild status:
 - a. Log in to the PowerFlex Manager and check the dashboard.
 - b. Confirm there is no error and rebuild or rebalance is running.
2. Shut down all the customer VMs on the PowerFlex production cluster other than the SVMs:
 - a. Using the VMware vSphere Client, log in to the customer VMware vCenter or a single VMware vCenter (production cluster).
 - b. Expand the production clusters.
 - c. Shut down all VMs, except for the PowerFlex storage VMs (SVM).

 **CAUTION:** Do not shut down the SVMs. Shutting them down now can result in data loss.

Related information

[Power off the PowerFlex management controller 2.0](#)

Deactivate protection domain and power off PowerFlex storage-only node using PowerFlex Manager

Use this procedure to power off the PowerFlex protection domains and PowerFlex storage-only nodes using PowerFlex Manager. This procedure is applicable only to the PowerFlex production cluster.

Steps

1. Log in to PowerFlex Manager.
2. Select **Block > Protection Domain**.
3. For each protection domain, click **More Actions > Inactivate**.

4. Click **OK** and type the administrator password when prompted. Repeat for each protection domain and verify that each is deactivated.
5. Repeat for each protection domain and verify that each is deactivated.
6. Log in to the iDRAC to power off the PowerFlex storage-only node.

Power off PowerFlex compute-only nodes with VMware ESXi

Use this procedure to power off PowerFlex compute-only nodes with VMware ESXi.

Steps

1. Log in to the VMware vCenter, click **Home**, and click **Inventory**.
2. Disable DRS and HA on the customer cluster.
3. Place the PowerFlex compute-only nodes with VMware ESXi into maintenance mode.
4. Once the node is in maintenance mode, power off the vCLS VM.
5. Power off the PowerFlex compute-only nodes with VMware ESXi.

Power off PowerFlex file nodes

Use this procedure to power off PowerFlex file nodes.

Prerequisites

Shut down all applications that use the NAS filesystem before shutting down the PowerFlex file cluster. If you do not shut them down, there is a chance of DU/DL.

Steps

1. Ensure all the applications which uses NAS filesystems are shut down.
2. Ensure all compute-only or hyperconverged nodes are shut down.
3. Shut down PowerFlex file cluster by logging into each PowerFlex file node and type:

```
svc_nas_ctl --disable_ha_monitoring
```

```
svc_nas_ctl --stop_nas_container
```
4. From iDRAC, shut down on all PowerFlex file nodes and allow them time to power off completely.
5. Log in to PowerFlex Manager and verify the resource group is healthy.

Power off PowerFlex hyperconverged nodes with VMware ESXi

Use this procedure to power off PowerFlex hyperconverged nodes with VMware ESXi.

Steps

1. Log in to the VMware vSphere Client.
2. From VMware vCenter, click **Home > Inventory**.
3. Verify that DRS and HA on the customer cluster are disabled. If they are not disabled, disable them.
4. Shut down all PowerFlex SVMs.
5. Place the PowerFlex hyperconverged nodes into maintenance mode.
6. Power off the PowerFlex hyperconverged nodes with VMware ESXi.

Power off the VMware NSX Edge nodes

Use this procedure to power off the VMware NSX Edge nodes.

Steps

1. In the management VMware vCenter, right-click the NSX Edge VMs and click **Power > Shut Down Guest OS**.
2. In the management VMware vCenter, right-click the NSX Edge nodes and click **Power > Shut Down**.

Power off the PowerFlex management controller 2.0

Power off the PowerFlex management controller 2.0 on each of the PowerFlex management controller VMware ESXi hosts.

Steps

1. Determine the primary MDM IP address:
 - a. Log in to PowerFlex Manager to determine the primary MDM.
 - b. To view the details of a resource group, click **Lifecycle > Resource Groups > PowerFlex management controller 2.0 resource group**. Scroll to the **Service Details** page and make a note of the primary MDM IP address.
2. Log in to the primary MDM using SSH.
3. Log in to the MDM cluster:

```
#scli --login --management_system_ip <PFxM_IP_Address> --username admin --password <PFxM_Password>
```
4. Identify the storage pools for each protection domain and record the protection domain or storage pool mappings:

```
#scli --query_all_volumes --protection_domain_name pfmc | grep "Storage Pool"
```
5. Log in to the PowerFlex management platform master node using SSH and run the following commands to halt the CMO database:

```
# echo alias k="kubectl -n $(kubectl get pods -A | grep -m 1 -E 'platform|pgo|helmrepo' | cut -d' ' -f1)"
# kubectl config set-context default --namespace=$(kubectl get pods -A | grep -m 1 -E 'platform|pgo|helmrepo|docker' | cut -d' ' -f1)
# echo $(kubectl get pods -l="postgres-operator.crunchydata.com/control-plane=pgo" --no-headers -o name && kubectl get pods -l="postgres-operator.crunchydata.com/instance" --no-headers -o name) | xargs kubectl get -o wide
# kubectl -n powerflex patch $(kubectl -n powerflex get postgrescluster -o name) --type merge --patch '{"spec":{"shutdown":true}}'
```
6. Verify the DB shutdown. Only the PostgreSQL operator pod *pgo* must remain the same when running the command:

```
#echo $(kubectl get pods -l="postgres-operator.crunchydata.com/control-plane=pgo" --no-headers -o name && kubectl get pods -l="postgres-operator.crunchydata.com/instance" --no-headers -o name) | xargs kubectl get -o wide
```
7. Disable vSphere high availability and change startup order of SVMs. If the host is part of a vSphere high availability cluster, the automatic startup and shutdown of VMs is disabled.
 - a. Log in to VMware vSphere Client.
 - b. From **vSphere Client > Shortcuts > Hosts and Clusters**.
 - c. Browse to the cluster.
 - d. Click the **Configure** tab.
 - e. Select **vSphere Availability** and click **Edit**.
 - f. Click the toggle button to disable **vSphere HA**.
 - g. Click **OK**.
8. Modify the startup order of SVMs to manual to enable the vSphere high availability. This is applicable for all SVMs in the management controller PowerFlex cluster:
 - a. In the VMware vSphere Client, select the host where the VM is located.
 - b. Click the **Configure** tab.
 - c. Under **Virtual Machines**, select **VM Startup/Shutdown**, and click **Edit**.
The **Edit VM Startup and Shutdown** window opens.

- d. Select the **Automatically start and stop the virtual machines with the system** check box.
 - e. Set shutdown action to **Guest shutdown**.
 - f. To change the startup order of VMs, select a virtual machine from the **Manual Startup** category and use the up arrow to move the VM to the **Automatic** category.
 - g. Select the SVM and move it to **Automatic** category. This ensures that the SVM automatically stops and starts with the VMware ESXi system.
 - h. Repeat the steps for all the SVMs.
 - i. Verify the settings and click **OK**.
9. Gracefully shut down all the VMs except SVMs and vCenter VM:
- a. Log in to VMware vSphere Client.
 - b. From **vSphere Client > Shortcuts > Hosts and Clusters**.
 - c. Browse and right-click the VM and select **Power > Shut Down Guest OS**.
- Since SVMs are set to automatically stop and start, there is no need to manually power off.
10. Identify the host where the vCenter server is running and make a note of the IP address or host name. If vCenter high availability is enabled, make a note of the IP addresses of the hosts where active, passive, and witness nodes are running:
- a. Log in to VMware vSphere Client.
 - b. From **vSphere Client > Shortcuts > Hosts and Clusters**.
 - c. Browse the vCenter VM.
 - d. Make a note of the host IP address from the **Summary** page.
11. Shut down the vCenter server VM gracefully. If you have vCenter high availability configured, shut down the active, passive, and witness nodes:
- a. Log in to the VMware ESXi using the host client.
 - b. Click **Virtual Machines > Select the vCenter VM** and click to open a browser console.
 - c. Press **F12** to shut down the VM.
 - d. Enter the root password and press **OK**.
12. Shut down the VMware ESXi servers gracefully:
- a. Log in to VMware ESXi Host Client.
 - b. Right-click **Host** and select **Shut down**.
 - c. To confirm the shut down of the selected host, click **SHUT DOWN**.
 - d. Repeat the steps for all the remaining nodes.

Related information

[Power off a PowerFlex rack](#)

Complete the powering off of PowerFlex rack

Use this procedure to complete the powering off of your PowerFlex rack.

Prerequisites


 **NOTE:** Ensure that you complete a back-up before powering off.

Steps

1. Connect to all the switches using SSH:
 - For Cisco Nexus switches, type **copy running-config startup-config**
 - For Dell PowerSwitch switches, type **copy running-config tftp://hostip/filepath**.
2. On Zone B (BLUE), turn off all PDU power breakers (OPEN position).
3. On Zone A (RED), turn off all PDU power breakers (OPEN position).
4. To verify that there is no power beyond the PDUs, disconnect the AC feeds to all PDUs.

Power off a Technology Extension with PowerScale

Prerequisites

 **CAUTION:** The Technology Extension for PowerScale must be powered off after the PowerFlex rack is powered off.

- See the relevant procedure in this publication for powering off the attached PowerFlex rack.
- Look at the back panel and confirm that the LEDs on both batteries are green. If either battery is red, it has failed and must be removed from the node. If both batteries are red, replace and verify them before shutting down the node.
- Take a backup switch configuration using below command and store the backup file to a remote server:

```
Copy running-config startup-config
copy startup-config tftp://<server-ip>/<switch_backup_file_name>
```

Steps

1. Open **OneFS** and log in as **root**.
2. Click **CLUSTER MANAGEMENT > Hardware Configuration > Shutdown & Reboot Controls**.
3. Select **Shut Down**.
4. Click **Submit**.
5. **Power off the Switches** in the Technology Extension for PowerScale cabinet.

Results

Verify that all nodes have shut down by looking at the power indicators on each node.

If nodes do not power off:

1. SSH to the node.
2. Log in as **root** and type:

```
Isi config
```

3. In the subsystem, type:


```
shutdown #
```

Where # represents the node number, or type:

```
shutdown all
```

If the node still does not power off, you can force the node to power off by pressing and holding the multifunction/power button on the back of the node.

If the node still does not respond, press **Power** button of the node three times, and wait five minutes. If the node still does not shut down, press and hold **Power** button until the node powers off.

 **NOTE:** Perform a forced shutdown only with a failed and unresponsive node. Never force a shutdown with a healthy node. Do not attempt any hardware operations until the shutdown process is complete. The process is complete when the node LEDs are no longer illuminated.

Username and password management

PowerFlex servers

Change the Integrated Dell Remote Access Controller 9 (iDRAC9) password

Use the iDRAC web console to change the root password.

Steps

1. Open a web browser and type: **http://<ip_address_of_iDRAC>** .
2. Log in as **root**.
3. Expand **iDRAC Settings**.
4. Click **Users > Local Users**.
5. Select **User ID 2** and click **Edit**.
ID 2 is the root user.
6. Under **User Configuration**, in the **User Account Settings** section, change the password.
 - a. In the **Password** box, enter the new password.
 - b. In the **Confirm Password** box, re-enter the new password.
7. Click **Save**.

Change the system and setup passwords

Use this procedure to change the system BIOS password.

Prerequisites

If the password status is set to **locked**, you cannot change or delete the system or setup password.

Steps

1. Enter System Setup by pressing **F2** immediately after turning on or restarting your system.
2. On the System Setup Main Menu, click **System BIOS > System Security**.
3. On the **System Security** screen, ensure that **Password Status** is set to **Unlocked**.
4. In the **System Password** field, change or delete the existing system password and press **Enter**.
5. In the **Setup Password** field, change or delete the existing setup password and press **Enter**.
If you change the system or setup password, a message prompts you to re-enter the password. If you delete a password, a message prompts you to confirm the deletion.
6. Press **Esc** to return to the **System BIOS** screen. Press **Esc** again. A message prompts you to save the changes.

PowerFlex Manager

Create credentials for root and non-root users

Use this procedure to create credentials for root and non-root users in PowerFlex Manager.

Prerequisites

To import and create the SSH keys for a PowerFlex node, switch, OS admin, OS user, ensure you generate SSH key pairs of RSA type without passphrase. See *Related information* for more information.

About this task


You can now use a non-root user instead of the root user for PowerFlex system administration functions. This enhances security by disabling the root user during node discovery, operating system installation, and non-disruptive updates. The default non-root user name is **pflex**.

PowerFlex Manager allows you to specify a non-root user when you configure a template for a compute-only, storage-only, or hyperconverged deployment. SSH key pairs based root or non-root deployments are not supported for PowerFlex file deployments.

Steps


1. On the menu bar, click **Settings > Security**.
2. Click **Resource Credentials**. The Credentials Management page opens.
3. Click **Create**.
4. In the **Create Credentials** dialog box, from the **Credential Type** drop-down list, select one of the following resource types for which you want to create non-root credentials:
 - **Node**
 - **Switch**
 - **OS Admin**
 - **OS User**The **OS Admin** and **OS User** credential types apply to deployed items, not to PowerFlex Manager. If you are creating an OS user credential set for the management virtual machines on a PowerFlex management controller resource group, select **OS User**.
5. In the **Credential Name** field, enter the name to identify the credential.
If you are creating an OS user credential set for the management virtual machines on a PowerFlex management controller resource group, do the following:
 - a. Enter **MVM delladmin** to identify the credential.
 - b. In the **User Name** field, enter **delladmin**.
 - c. Enter the delladmin account password in the **Password** and **Confirm Password** fields.
6. Click **Enable Key Pairs** to enable log in with SSH key pairs and perform the following:

To...	Do this...
Enable key pairs for the Node or Switch credential:	<ol style="list-style-type: none">a. Click Import SSH Key Pair.  NOTE: Manually generate the SSH keys pairs.b. Click Choose File and browse to the file that contains the private key.c. Type a name for the key pair.d. Click Import.
Create keys using PowerFlex Manager for the OS admin or OS user credential and enable key pairs	<ol style="list-style-type: none">a. Click Create a new key.b. Click Create & Download Key Pair.c. On Key Pair Name, type the name for key pair.d. Click Create.e. Click Download Public Key.

To...	Do this...
To manually generate and import an existing key pairs for the OS admin or OS user credential	<ol style="list-style-type: none"> Click Import SSH Key Pair.  NOTE: Manually generate the SSH keys pairs. Click Choose File and browse to the file that contains the public and private key. Type a name for the key pair. Click Import.

If you enable SSH key pairs for a **Node** or **Switch credential** and use that credential for discovery, PowerFlex Manager uses public or private RSA key pairs to SSH into your node or switch securely, instead of using a user name and password.

If you enable SSH key pairs for an OS user or OS admin credential and use that credential for a deployment, PowerFlex Manager uses RSA public or private key pairs for the deployment operations.

 **NOTE:** PowerFlex Manager does not consume SSH keys for all component types. For example, if you enable SSH key pairs for an admin credential, the SSH keys are not used for the deployment of a CloudLink Center VM. Instead, the user name and password are used instead for all communication.

- In the **User Name** field, enter the username for the credential.

For **Nodes** (iDRAC), **root** is the only valid username for root-level credentials. For a non-root user name, enter the default non-root user name.

For the **OS Admin** credential type, the **User Name** field is disabled because the user is assumed to be root. You must use the root user for new deployments.

For the **OS User** credential type, enter the default non-root user name.

For the embedded operating system, this user account must have SSH enabled and have sudo access. For VMware ESXi, the account must be configured with the administrator role on the local server permission setting, which should enable SSH and other tools like esxcli. You can add existing resource groups with a non-root user. The account on the SVM and/or PowerFlex storage-only nodes for the **OS User** credential type must have a /home directory and have the correct group permissions.

- In the **Password** and the **Confirm Password** boxes, enter the password for the credential.

Related information

[Generate SSH key pairs](#)

Generate SSH key pairs

To create the SSH keys for a PowerFlex node, switch, OS, admin OS user, use this procedure to manually generate the SSH keys that is of RSA type and ensure the key is generated without pass phrase.

Steps

- Generate a private key using the following command:

```
ssh-keygen -b 2048 -t rsa
```

- Enter a file path to save the public and private keys or proceed with the default file path without a pass phrase:

Sample output:

```
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase: # do not enter a passphrase
Enter same passphrase again: # do not enter a passphrase
```

Sample output that indicates the public and private keys are saved in the default file path:

```
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:fKILLqp5UXeuEW7xuYeE7PNHpvjAUatNx6I/bisRqRU root@PFMP2-4
The key's randomart image is:
+---[RSA 2048]-----+
|
```

```

|           E           |
|           o.          |
|        .oB..o         |
|       .+*SO=.o        |
|      .o.=BO=oo        |
|     ...o=*.*          |
|    o.   *o*  o         |
|   o.    B*=           |
+----- [SHA256] -----+

```

3. Verify that the public and private keys are saved in the default file path: `/root/.ssh/`.

Sample output:

```
cd /root/.ssh
ls
```

- `id_rsa.pub` indicates a public key.
- `id_rsa` indicates is a private key.

Related information

[Create credentials for root and non-root users](#)

[Update a credential in PowerFlex Manager](#)

Update the PowerFlex Manager password

When you first log in to PowerFlex Manager, you need to set your password. You can also change your password at any time after the first login.

Steps

1. Click the user icon in the upper right corner of PowerFlex Manager.
2. Click **Change Password**.
3. Type the password in the **New Password** field.
4. Type the password again in the **Verify Password** field.
5. Click **Apply**.

Update a credential in PowerFlex Manager

If the password for a resource or component is manually changed outside of PowerFlex Manager, you must update the credential in PowerFlex Manager with the new password.

Prerequisites

To modify the SSH keys of a PowerFlex node, switch, OS, admin OS user, generate SSH keys of RSA type and ensure the key is generated without passphrase. See *Related information* for more information.

About this task

If you change the password for a resource, you must update all similar resources (for example, element manager, node, switches, or VMware vCenter) to have the same password.

Steps

1. Log in to PowerFlex Manager.
2. On the menu bar, click **Settings > Security**. Under **Security**, click **Resource Credentials**.
3. On the **Resource Credentials** page, select the resource whose password you want to edit, and click **Modify**.
4. In the **Edit Resource Credentials** dialog box, perform the following to import new SSH keys:
 - a. Generate the SSH key pairs.
 - b. Click **Import existing key**.

- c. Click **Import SSH Key Pair**.
- d. Click **Choose File** and browse to the file that contains your public and private key.
- e. Type a name for the **Key Pair Name** field.
- f. Click **Import**.
- g. Click **Save**.
5. Click **Save**.
6. On the menu bar, click **Lifecycle > Resource Groups** and select the deployed service that contains the resource whose password is updated.
7. Under **More Actions**, click **Update Resource Group Details**.

Related information

[Generate SSH key pairs](#)

Updating passwords for nodes

You can update the passwords for one or more nodes from PowerFlex Manager.

Steps

1. Log in to PowerFlex Manager.
2. On the menu bar, click **Resources**.
3. On the **All Resources** tab, select one or more nodes for which you want to change the passwords.
4. Click **Update Password**.
PowerFlex Manager displays the **Update Password** wizard.
5. On the **Select Components** page, specify which passwords you want to update for the selected nodes by clicking one or more of the following check boxes.
 - **iDRAC Password**
 - **Node Operating System Password**
 - **SVM Operating System Password**
6. Click **Next**.
7. On the **Select Credentials** page, create a credential with a new password or change to a different credential.
 - a. Open the **iDRAC (n)** object under the **Type** column to see details about each node you selected on the **Resources** page.
 - b. To create a credential that has the new password, click the plus sign (+) under the **Credentials** column.
Specify the **Credential Name** and the **User Name** for which you want to change the password. Enter the new password in the **Password** and **Confirm Password** fields.
 - c. To modify the credential, click the pencil icon for the nodes under the **Credentials** column and select a different credential.
 - d. Click **Save**.

You must perform the same steps for the node operating system and SVM operating system password changes. For a node operating system credential, only the OS Admin credential type is updated.
8. Click **Finish**.
9. Click **Yes** to confirm.

Results

PowerFlex Manager starts a new job for the password update operation, and a separate job for the device inventory. The node operating system and SVM operating components are updated only if PowerFlex Manager is managing a cluster with the operating system and SVM. If PowerFlex Manager is not managing a cluster with these components, these components are not displayed and their credentials are not updated. Credential updates for iDRAC are allowed for managed and reserved nodes only. Unmanaged nodes do not provide the option to update credentials.

Updating passwords for system components

You can update the passwords for some system components from PowerFlex Manager.

Steps

1. Log in to PowerFlex Manager.
2. On the menu bar, click **Resources**.
3. On the **All Resources** tab, select one or more resources of the same type for which you want to change passwords.
For example, you could select one or more iDRAC nodes or you could select one or more PowerFlex gateway components.
4. Click **Update Password**.
PowerFlex Manager displays the **Update Password** wizard.
5. On the **Select Components** page, select one or more components for which you want to update a password and click **Next**.
The component choices vary depending on which resource type you initially selected on the **Resources** page.
6. On the **Select Credentials** page, create a credential or change to a different credential having the same username.
7. Click **Finish** and click **Yes** to confirm the changes.

User management

The **User Management** page allows you to manage local users, LDAP users, and directory services.


Under **Settings > User Management**, you can find three pages:

- Local Users
- LDAP Users
- Directory Services

User roles


User roles control the activities that can be performed by different types of users, depending on the activities that they perform when using PowerFlex Manager.


Ensure that you configure the active directory before assigning roles. The roles that can be assigned to local users and LDAP users are identical. Each user can only be assigned one role. If an LDAP user is assigned directly to a user role and also to a group role, the LDAP user is provided with permissions of both roles.

 **NOTE:** User definitions are not imported from earlier versions of PowerFlex and must be configured again.

The following table summarizes the activities that can be performed for each user role:

Role	Description	Activities
SuperUser	A SuperUser can perform all system operations.	<ul style="list-style-type: none">• Manage storage resources• Manage lifecycle operations, resource groups, templates, deployment, backend operations• Manage replication operations, peer systems, RCGs• Manage snapshots, snapshot policies• Manage users, certificates• Replace drives• Hardware operations• View storage configurations, resource details• View platform configuration, resource details• System monitoring (events, alerts)• Perform serviceability operations• Update system settings

Role	Description	Activities
SystemAdmin	A SystemAdmin can perform all operations, except for user management and security ones.	<ul style="list-style-type: none"> • Manage storage resources • Manage lifecycle operations, resource groups, templates, deployment, backend operations • Manage replication operations, peer systems, RCGs • Manage snapshots, snapshot policies • Replace drives • Hardware operations • View storage configurations, resource details • View platform configuration, resource details • System monitoring (events, alerts) • Perform serviceability operations • Update system settings
StorageAdmin	<p>A StorageAdmin can perform all storage-related front-end operations including element management of already setup NAS and block systems. For example: create volume, create file system, manage file-server user quotas.</p> <p> NOTE: Operations such as create storage pool, create file-server, and add NAS node cannot be performed by Storage Admin, but can be performed by the Lifecycle Admin role.</p>	<ul style="list-style-type: none"> • Manage storage resources • Manage replication operations, peer systems, RCGs • Manage snapshots, snapshot policies • Replace drives • Hardware operations • View storage configurations, resource details • View platform configuration, resource details • System monitoring (events, alerts)
LifecycleAdmin	A LifecycleAdmin can manage the life cycle of hardware and PowerFlex systems.	<ul style="list-style-type: none"> • Manage lifecycle operations, resource groups, templates, deployment, backend operations • Replace drives • Hardware operations • View resource groups and templates • System monitoring (events, alerts)
ReplicationManager	The ReplicationManager is a subset of the Storage Admin role, for work on existing systems for setup and management of replication and snapshots.	<ul style="list-style-type: none"> • Manage replication operations, peer systems, RCGs • Manage snapshots, snapshot policies • View storage configurations, resource details (volume, snapshot, replication views) • System monitoring (events, alerts)
SnapshotManager	SnapshotManager is a subset of StorageAdmin, working only on existing systems. This role includes all operations required to set up and manage snapshots.	<ul style="list-style-type: none"> • Manage snapshots, snapshot policies • View storage configurations, resource details • System monitoring (events, alerts)
SecurityAdmin	The SecurityAdmin manages PowerFlex role-based access control (RBAC), and LDAP user federation. It includes all security aspects of the system.	<ul style="list-style-type: none"> • Manage users, certificates • System monitoring (events, alerts)
DriveReplacer	This is a subset of the Technician role. The DriveReplacer can perform only operations required for a drive replacement.	<ul style="list-style-type: none"> • Replace drives • System monitoring (events, alerts)
Technician	The Technician can perform all hardware FRU operations on the system, including entering a node into maintenance mode.	<ul style="list-style-type: none"> • Replace drives • Hardware operations • System monitoring (events, alerts) • Perform serviceability operations

Role	Description	Activities
Monitor	The Monitor role has read-only access to the system, including topology, alerts, events, and metrics.	<ul style="list-style-type: none"> View storage configurations, resource details View platform configuration, resource details System monitoring (events, alerts)
Support	<p>The Support role is a special kind of SystemAdmin (all activities except for user/security management operations) to be used only by Dell support staff and developers. This user role has access to undocumented, special operations and options for common operations, required only for support purposes.</p> <p> NOTE: This special role should be used only by Dell support. It opens special, often dangerous, commands for advanced trouble shooting.</p>	<ul style="list-style-type: none"> Manage storage resources Manage lifecycle operations, resource groups, templates, deployment, backend operations Manage replication operations, peer systems, RCGs Manage snapshots, snapshot policies Replace drives Hardware operations View storage configurations, resource details View platform configuration, resource details System monitoring (events, alerts) Perform serviceability operations Special Dell Technologies Support operations

Mapping PowerFlex 4.0 or later roles to legacy roles

For reference, the tables below map user and group roles from earlier releases to the roles used in the current release.

Role mapping per legacy user interface

Legacy role (prior to version PowerFlex 4.0)	New role (from PowerFlex 4.0 and later)
PowerFlex Monitor	Monitor
PowerFlex Back-end configurator	LifecycleAdmin
PowerFlex Front-end configurator	StorageAdmin
PowerFlex Configurator	SystemAdmin
PowerFlex Security	SecurityAdmin
PowerFlex Administrator	StorageAdmin
PowerFlex local Super User	SuperUser
PowerFlex technician commands	Support
PowerFlex Manager Administrator	SuperUser
PowerFlex Manager Read only	Monitor
PowerFlex Manager Standard owner	LifecycleAdmin
PowerFlex Manager Standard member	LifecycleAdmin
PowerFlex Manager Operator	DriveReplacer
NAS Storage admin	StorageAdmin
NAS Administrator	StorageAdmin

Legacy LDAP users and groups

LDAP user role permissions were modified in PowerFlex version 4.0. For reference purposes, the following table shows the mapping of legacy users and groups to the roles now supported by PowerFlex.

Prior to PowerFlex version 4.0, PowerFlex mapped LDAP users and groups to actual roles. This mapping allowed assignment of multiple roles to a single group. Assignment of multiple roles to a group is no longer supported.

All legacy roles have a proximate hierarchy. The group's single role will be the highest ranking role.

Ranking	Legacy PowerFlex LDAP role (earlier than v4.0)	PowerFlex v4.0 or later group role without security officer permissions	PowerFlex v4.0 or later group role with security officer permissions
1	Super User	N/A (local user)	N/A (local user)
2	Administrator	Admin	SuperUser
3	Configurator	Admin	SuperUser
4	Front-end config and back-end config	Admin	SuperUser
5	Front-end config or back-end config	StorageAdmin or LifecycleAdmin	SuperUser
6	Monitor	Monitor	SecurityAdmin
Not ranked	Security Officer (SE)	SecurityAdmin	SecurityAdmin

Local users

You can create and manage local users within PowerFlex Manager.

Creating a user

Perform this task to create a local user and assign a role to that user.

Steps

1. On the menu bar, click **Settings** and click **User Management**.
2. Click **Local Users**.
3. On the **Local Users** page, click **Create**.
4. Enter a unique **User Name** to identify the user account.
5. Enter the **First Name** and **Last Name** of the user.
6. Enter the **Email** address.
7. Enter a **New Password** that a user enters to access PowerFlex Manager. Confirm the password in the **Verify Password** field.
The password must be at least 8 characters long and contain one lowercase letter, one uppercase letter, one number, and one special character. Passwords cannot contain a username or email address.
8. In the **User Role** box, select a user role. Options include:
 - SuperUser
 - SystemAdmin
 - StorageAdmin
 - LifecycleAdmin
 - ReplicationManager
 - SnapshotManager
 - SecurityAdmin
 - DriveReplacer
 - Technician
 - Monitor
 - Support
9. Select **Enable User** to create the account with an **Enabled** status, or clear this option to create the account with a **Disabled** status.
10. Click **Submit** and click **Dismiss**.

Results

PowerFlex Manager creates the new user with the specified password. The first time you login with the new user and password, PowerFlex Manager asks you to change the password.

Modifying a user

Perform this task to edit a PowerFlex Manager user profile.

Steps

1. On the menu bar, click **Settings** and click **User Management**.
2. Click **Local Users**.
3. On the **Local Users** page, select the user account that you want to edit.
4. Click **Modify**. For security purpose, confirm your password before editing the user.
5. You can modify the following user account information from this window:
 - **First Name**
 - **Last Name**
 - **User Role**
 - **Email**
 - **Enable User**

If you select the **Enable user** check box, the user can log in to PowerFlex Manager. If you disable the check box, the user cannot log in.

6. Click **Submit** and click **Dismiss**.

Deleting a user

Perform this procedure to remove an existing local user.

Steps

1. On the menu bar, click **Settings** and click **User Management**.
2. Click **Local Users**.
3. On the **Local Users** page, select one or more user accounts to delete.
4. Click **Delete**.
Click **Apply** in the warning message to delete the user. Click **Dismiss**.

Resetting the password for a user

You can reset the password for a local user in PowerFlex Manager.

Steps

1. On the menu bar, click **Settings** and click **User Management**.
2. Click **Local Users**.
3. On the **Local Users** page, select one user account to reset the password.
4. Click **Reset Password**.
5. Enter **New Password** and **Verify Password**.
6. If you wish to set the password as a temporary one, check **Temporary Password**.
7. Click **Apply** and click **Dismiss**.

LDAP users

You can add and modify LDAP users and groups in PowerFlex Manager.

The LDAP realm name must not exceed the 155 character limit defined by Microsoft.

Add LDAP users or groups

Add existing LDAP users or groups to PowerFlex, and assign roles to them.

About this task

These roles control access permissions for the corresponding LDAP user or group. These users and groups must also be configured in the directory service. On the PowerFlex side, these users and groups are mapped to PowerFlex roles.

Steps

1. On the menu bar, click **Settings**.
2. In the left pane, click **User Management**, then in the right pane, click **LDAP Users**.
3. Click **Add**.
4. In the **Add LDAP User/Group** dialog box, select a **Type** option.
 - **User**—a user definition will be configured for an individual user.
 - **Group**—a group definition will be configured for a specific group.
5. In the **User Name** box, enter the user or group name.
6. In the **User Role** box, select the role to be assigned to the user or group. Options include:
 - SuperUser
 - SystemAdmin
 - StorageAdmin
 - LifecycleAdmin
 - ReplicationManager
 - SnapshotManager
 - SecurityAdmin
 - DriveReplacer
 - Technician
 - Monitor
 - Support
7. Click **Apply**.

Modify an LDAP user or group

Modify the user role of an LDAP user or group. User roles control access permissions to the corresponding user or group.

Steps

1. On the menu bar, click **Settings > LDAP Users**.
2. Click **Modify**.
3. In the **Modify LDAP User/Group** dialog box, change the user role by selecting one of the **User Role** options:
 - SuperUser
 - SystemAdmin
 - StorageAdmin
 - LifecycleAdmin
 - ReplicationManager
 - SnapshotManager
 - SecurityAdmin
 - DriveReplacer
 - Technician
 - Monitor
 - Support
4. Click **Apply**.

Directory services

You can create a directory service that PowerFlex Manager can access to authenticate users.

An Active Directory or Open LDAP user is authenticated against the specific directory domain to which a user belongs.

The **Directory Services** page displays the following information about PowerFlex Manager active directories:

- LDAP configuration
- User search settings
- Group search settings

From this page, you can:

- Add a directory service (only available when no service is defined in the system)
- Modify a directory service
- Remove a directory service

Add a directory service

Add a directory service for user authentication.

About this task

Perform the following procedure to add a directory service to PowerFlex:

Steps

1. On the menu bar, click **Settings**.
2. In the left pane, click **User Management**, then in the right pane, click **Directory services**.
3. Click **Add**.
4. For **LDAP Configuration**, configure the following:
 - a. In the **Address** box, enter the address of the authentication server.
The address must be specified in URL-like format:
 - Enter **ldap://HOSTNAME or IP ADDRESS** for a plaintext LDAP connection.
 - Enter **ldaps://HOSTNAME or IP ADDRESS** for a secure LDAP connection.
For example: **ldap://100.68.68.1**
 - b. In the **Bind DN** box, enter the bind distinguished name attributes.
The Bind Distinguished Name (DN) uniquely identifies an entry and its position in the hierarchy of entries contained in a directory server.
For example: **CN= <your AD user account>,CN=Users,DC=asm,DC=delllabs,DC=net.**
 - c. In the **Bind DN Password** box, enter the Bind DN password.
This is the password used to access the LDAP server.
 - d. In the **Timeout** box, enter a value in milliseconds.
For example: **1000**
5. For **User Search Settings**, configure the following:
 - a. In the **Username LDAP Attribute** box, enter the name of an LDAP attribute that is mapped as the username. For many LDAP servers, it can be **uid**. For Active Directory, it can be **sAMAccountName** or **cn**. The attribute should be filled in for all LDAP users you want to import from LDAP to PowerFlex.
For example: **sAMAccountName**
 - b. In the **ID Attribute** box, enter the ID attribute for users.
For example: **sAMAccountName**
 - c. In the **Object Class** box, enter an object class.
For example: **top,person,organizationalPerson,user**
 - d. In the **Search Path** box, enter the search path.
The search path is used to identify and retrieve entries in the directory information tree that match a set of criteria.
For example: **CN=Users,DC=asm,DC=delllabs,DC=net**
6. For **Group Search Settings**, configure the following:
 - a. In the **Group Member Attribute** box, enter a group member name.

For example: **member**

- b. In the **Group ID Attribute** box, enter the group ID.

For example: **cn**

- c. In the **Group Object Class** box, enter the group object class.

For example: **group**

- d. In the **Group Search Path** box, enter the group search path.

The search path is used to identify and retrieve entries in the directory information tree that match a set of criteria for groups.

For example: **CN=Users,DC=asm,DC=delllabs,DC=net**

- 7. Click **Test Connection**.

If the test is successful, the **Submit** button will become active. If the test fails, you will not be able to proceed until you fix the connectivity issue.

- 8. When you have finished making your changes, click **Submit**.

Modify a directory service

The **Modify** option allows you to edit the existing directory service settings.

About this task

Perform the following procedure to edit the settings:

Steps

1. On the menu bar, click **Settings**.
2. In the left pane, click **User Management**, then in the right pane, click **Directory services**.
3. Click **Modify**.
4. In the **LDAP Settings** dialog box, edit the desired fields.
Note that the **Bind DN Password** must be reentered.
5. When you have finished making your changes, click **Test Connection**.
If the test is successful, the **Submit** button becomes active. If the test fails, you will not be able to proceed until you fix the connectivity issue.
6. Click **Submit**.

Remove a directory service

The **Remove** option allows you to remove the directory service configuration from PowerFlex.

About this task

Perform the following procedure to remove a directory service:

Steps

1. On the menu bar, click **Settings**.
2. In the left pane, click **User Management**, then in the right pane, click **Directory services**.
3. Click **Remove**.
4. In the warning dialog box, click **Submit**.

Virtualization

Changing a VMware ESXi host root password

For security reasons it might be necessary to change the password for the root user on a VMware ESXi host after installation.

Use any of the following methods to change the root password for the VMware ESXi host:

- VMware vSphere Client
- VMware ESXi shell command
- VMware ESXi host System Customization menu

Change the password using VMware vSphere Client

Steps

1. Log in to the host UI `https://esxi_IP_address` using root credentials.
2. In the left pane, under **Host**, click **Manage**.
3. Select the **Security & Users** tab, click **Users** and click the **root** user.
4. Click **Edit User**.
5. In the **Edit User** dialog box, enter and confirm a new password.
6. Click **Save**.

Change the password using the VMware ESXi shell command

Prerequisites

Log in to the VMware ESXi host service console as **root user**.

Steps

1. When prompted, enter the current password.
2. To change the root password, enter: **passwd root**.
3. Enter the new root password and press **Enter**.
4. Verify the password by entering it again.

Change the password using the VMware ESXi host system customization menu

Prerequisites

Log in to the VMware ESXi host service console as **root** user.

You can also acquire root privileges by executing the **su** command.

Steps

1. From the **System Customization** menu of the VMware ESXi host, use the keyboard arrows to select **Configure Password** and press **Enter**.
2. In the **Configure Password** dialog box, fill in the required fields to change the password:
 - a. Enter the **Old Password** of the VMware ESXi host.
 - b. Enter the new root password in the **New Password** field. Re-type it in the **Confirm Password** field.
 - c. Press **Enter**.

Modify the VMware vCenter Server single sign on default administrator password

Use this procedure to change the default password for the VMware vCenter single sign on administrator account.

Prerequisites

Log in to the VMware vSphere Client and connect to vCenter.

Steps

1. In the left pane, select **Administration**.
2. Under Single Sign On, select **Users and Groups**.
The **admin** user displays in the right pane.
3. On the **Users** tab, select the domain from the drop-down menu, and select the **administrator** user. Click **Edit**.
4. Set and confirm the password for the admin user account. Be sure to use a strong password as the system validates the password before accepting it.
5. Click **Save**.

Change the administrator password for VMware vCenter Server Appliance

Use this procedure to change the VMware vCenter Server Appliance administrator password.

Steps

1. Log in to the VMware vCenter Server Appliance Web console.
2. On the **Admin** tab, enter your current password in the **Current administrator password** box.
3. Enter the new password in the **New administrator password** and **Retype new administrator password** boxes.
4. Click **Change password**.

Resetting the VMware vCenter Server Appliance root password

Use this procedure to reset a forgotten vCenter Server Appliance root password.

Steps

1. Take a snapshot or backup of the vCenter Server Appliance. Do not skip this step.
2. Reboot the vCenter Server Appliance.
3. After the operating system starts, press the **E** key to access the **GNU GRUB Edit Menu**.
4. Locate the line that starts with the word `linux`. Append the following entries to the end of the line:

`rw init=/bin/bash`
5. Press **F10**.
6. At the command prompt, type the following command: `passwd`
7. Enter a new root password and re-enter the password to confirm it.
8. Unmount the file system by running the following command: `umount /`
9. Reboot the vCenter Server Appliance by running the following command: `reboot -f`
10. Confirm that you can access the vCenter Server Appliance using the new root password.
11. Remove the snapshot taken in step 1 if applicable.

Management VMs

Use this procedure to change users passwords for the management VMs.

About this task

The default username is delladmin.

Steps

1. Log in to the appropriate user account. If changing a password for another user, log in as root.
2. Open a shell prompt and type one of the following commands:
 - To change your own password: `passwd`
 - To change the password of another user: `passwd username`

When prompted ,enter and confirm the new password.


Change CloudLink passwords

CloudLink software is installed on the CloudLink Center VMs.

Unlock secadmin user password

Use this procedure to unlock the secadmin password.

Steps

1. Log in to the controller vCenter web client, and launch the CloudLink Center VM console.
 **NOTE:** For a single vCenter environment, log in to single vCenter with a controller and customer datacenter. Go to the controller datacenter to launch the CloudLink center VM console.
2. Log in using the CloudLink user credentials.
3. In the **Update Menu** dialog box, select **Unlock User**, and click **OK**.
A user unlocked message is displayed.
4. Click **OK**.

Manage EmbeddedOS15.3 users credentials for the jump server

Create users

About this task

useradd allows you to add users and specify certain criteria such as: comments, the users home directory, shell type, and many others account properties for SUSE Linux operating system.

Steps

1. SSH to the jump server using the admin user, and type: `Server1:~# useradd -mU -G trusted <newuser>`.
The following table that explains what each qualifier is used for:

Qualifier	Description
-m	This qualifier makes the useradd command create the users home directory.
-G	This qualifier makes the useradd command to add the user to the group directory

- Set the associated password, type: **server1:~ # passwd <newuser>**.

Once the password is set, the user can successfully log in to the server.

Set up desktop icons for a new user

Steps

- Using SSH, log in as the new user.
- Copy desktop files from admin user home directory to the new user home directory, type:

```
cp /home/admin/Desktop /home/<newuser>/
```

and change the ownership the files to the new user:

```
cd /home/<newuser>/Desktop
sudo chown <newuser> *
```
- Log in as the new user on the user interface.
- Right-click on the desktop, click **Open in Terminal**.
- Type the following commands on the terminal to show the desktop icons:

```
gsettings set org.gnome.shell.extensions.desktop-icons show-home false
gsettings set org.gnome.shell.extensions.desktop-icons show-trash false
gnome-extensions enable desktop-icons@csoriano
```
- Right-click on each .desktop file and click **Allow Launching**.

Delete users

The command to delete users is **userdel** and is specified with the **-r** qualifier which removes the home directory and mail pool.

Steps

SSH to the server and type: **server1:~ # userdel -r <newuser>**

Once you have issued the **userdel** command, you will notice that the **/home/<newuser>** directory is removed. If you only want to delete the user but leave their home directory intact, you can issue the same command but without the **-r** qualifier.

Enable sudo on a user

Steps

- SSH to the server and log in as **root**.
- Type **sudo usermod -a -G wheel <newuser>**.

Changing the IPI appliance password

Use this procedure to change the password for the Intelligent Physical Infrastructure (IPI) appliance.

Steps

- Open a Web browser and access the following URL: **https://< IPI_Appliance_IP_address>**

2. Click the **Setup** tab on the top menu bar.
3. Click **Users** in the left navigation pane.
4. Set the username, password, and/or access level. You can set a unique username for individuals requiring Web management access to the appliance unit. There are three user account levels:
 - Administrator: Full control of IPI appliance configuration settings.
 - Controller: Can view configuration settings.
 - Viewer: Can view configuration settings.User 1/admin is the primary administrator. Do not remove administrator rights from the admin user as it might result in noone having administrator access. If this occurs, a reset to factory defaults is the only solution.
5. Click **Save** to confirm changes.

Changing a user account password on the IPI appliance

Use this procedure to change the password for a user account on the Intelligent Physical Infrastructure (IPI) appliance.

Steps

1. Open a web browser and access the following URL: **https://<IPI_Appliance_IP_address>**
2. From the **Setup** menu, click **Users**.
3. Locate the account for which you are changing the password.
4. Enter the new password in the field.


Do not make any changes to user name or security role.
5. Click **Save**.

Changing the operating system password

If you lose the password on storage VM (SVM), start up in recovery mode to reset it.

Steps

1. Log in to PowerFlex Manager.
2. Select the SVM, and click **Enter Maintenance Mode**.
3. Select **Protected**, and click **Enter Maintenance Mode**.
4. Log in to VMware vCenter. Select the cluster and click **Related Objects > Virtual Machines > Open Console**.
5. Restart the SVM.
6. Enter **ESC** during restart and click **OK** to enter text mode.

 **NOTE:** You might have to hold down the **ESC** key.
7. Type **␣** to edit the password.
8. Select the second line (starts with `kernel /boot...`) and type **␣**.
9. Append **init=/bin/bash** to the end of the line.
10. Select **␣** to restart in recovery mode.
11. After the PowerFlex node restarts, type `passwd`, and enter a new password.
12. Type `reboot`, and allow the SVM to restart using the new password.

System logs and audit logs

PowerFlex Manager logs

Generate the troubleshooting bundle

Use this procedure to generate the troubleshooting bundle.

About this task

PowerFlex Manager collects logs from the Resource Groups page, and includes deployment logs, as well as the resources used in the resource group. A troubleshooting bundle is a compressed file that contains logging information for PowerFlex Manager managed components.

Prerequisites

The following logs are included:

- PowerFlex Manager application
- SupportAssist
- PowerFlex Gateway
- iDRAC lifecycle
- Dell PowerSwitch switch
- Cisco Nexus switch
- VMware ESXi
- CloudLink Center

Steps

1. Log in to PowerFlex Manager.
2. On the **Resource Group Details** page, click **Generate Troubleshooting Bundle**. Alternatively, on the menu bar, click **Settings > Serviceability**. Click **Generate Troubleshooting Bundle**.
3. On **Generate Troubleshooting** window, perform the following:
 - a. If you are using Support Assist, **Send to Configured SupportAssist** is selected by default.
 - b. To download locally, select **Download Locally** and provide a path using the following format with credentials:
For example : For CIFS: \\1.1.1.1\uploadDirectory
 - c. Click **Test Connections** to verify the connection to the CIFS share before generating the bundle.
4. For collecting the PowerFlex File core dump logs, select **Include PowerFlex File Core Dump log**. The SDNAS directory structure, nodes, and files are always collected regardless of whether this box is selected or not. When this option is selected, the additional NAS core dump is collected.
5. For collecting the PowerFlex Block, select one of the PowerFlex log level:
 - Default node logs
 - Default node logs plus additional MDM information
 - Latest logs only (most recent copy of all logs)
6. On **Node selection**, you can select either of the following:
 - Logs from all nodes.
 - To select specific nodes or SVMs, select the **Select specific nodes** and click **View/Select Nodes**. On a **Node Selection** window, select the **Nodes and SVMs listed** check box and click **>>**. Ensure the selected nodes or SVMs appear on the right pane and click **Save**. Verify that you can see the number of nodes selected.

7. Click **Generate**.

VMware vCenter logs

Collect VMware vCenter 7.X log files to a single location.

Steps

1. In the VMware vSphere Client menu, click **Administration > Deployment > System Configuration**.
2. Select a vCenter Server node and click **Export Support Bundle**.
3. Select the support bundle type.
4. Click **Export**.

CloudLink logs

Collect diagnostic log files.

Steps

1. Log in to CloudLink Center.
2. Click **Monitoring > Diagnostics**.
3. Click **View Logs**.
4. In the **Select Logs to View** dialog box, select a log file, and enter the required values for which you want to create a diagnostic file.
5. Click **Show Logs**.
6. Click **Actions > Generate Diagnostics**.

Network logs

Gather logs from the network switch

Generate logs to troubleshoot your network switch.

Steps

1. Open an SSH session with the switch using PuTTY or a similar SSH client.
2. Log in with admin or other credentials with privileges and type **show tech-support**.
3. Enable session logging. If using PuTTY, right-click the menu bar and go to **Change settings > Sessions > Logging**.
4. Select **All session output**.
5. Type a log file name and click **Apply**.
6. In the switch CLI, type the following:

Switch type	Code required
Dell PowerSwitch	<pre>show tech-support show process cpu</pre>
Cisco Nexus	<pre>show tech-support details no-more show tech-support vpc no-more show process cpu history no more</pre>

Gathering logs from the Cisco Nexus network for troubleshooting

It is important to export the technical support file from your Cisco Nexus switch before attempting to troubleshoot the switch or contact Dell Support.

About this task

Use the `show tech-support` command to obtain the technical support file from your Cisco Nexus switch, which contains log output and a snapshot of the switch at the time of failure.

Steps

1. Open an SSH session with the Cisco Nexus switch using PuTTY or a similar SSH client.
2. Log in with admin or other credentials with privileges to run `show tech-support`.
3. Right-click the menu bar and select **Change Settings...** and enter the following information:
 - **Session logging:** select **All session output**
 - **Log file name:** `putty.log`
4. Click **Apply**.
5. In the Cisco NX-OS CLI, type the following:

```
show tech-support details | no-more
show tech-support vpc | no-more
show process cpu history | no-more
```

Gathering logs from the Dell network for troubleshooting

It is important to export the technical support file from your Dell PowerSwitch switch before attempting to troubleshoot the switch or contact Dell Technologies Support.

About this task

Use the `show tech-support` command to obtain the technical support file from your Dell PowerSwitch switch, which contains log output and a snapshot of the switch at the time of failure.

Steps

In the Dell OS CLI, type the following:

```
show tech-support
show processes node-id node-id-number [pid process-id]
```

Configuring syslogs and audit logs

This section covers the procedures to configure system logs/syslogs and audit logs.

The logs can be transmitted through either of the following modes to the remote server:

- Directly
- Using PowerFlex Manager

Consider the following while configuring the syslogs and audit logs:

- TLS is supported if the remote syslog server is configured directly.
- TLS is not supported if PowerFlex Manager is used to configure the remote syslog server.

To configure an external source and a destination, see [Configure an external source](#) and [Configure a destination](#).

Configure syslogs using VMware ESXi

Use this procedure to configure syslogs using VMware ESXi. All system logs are forwarded to a centralized location.

Steps

1. Log in to the VMware ESXi host web interface.
2. Go to **Manage > System > Advanced Settings**.
3. To export logs to a central logging server, search for `Syslog.global.LogHost`.
4. Click **Edit > Syslog.global.logHost** and enter the UDP, IP address or FQDN, and the port number.
For example, `udp://192.168.1.1:514` (or) `tcp://192.168.1.1:514`.
5. Click **Save**.
6. To ensure syslog is started and ports are added, go to **Networking > Firewall rules** and search for **Syslog**.
If syslog is not started, click **Networking > Firewall rules > Action > Enable**.

Configure and forward the syslogs using VMware vCenter

Use this procedure to configure and forward the syslogs using VMware vCenter.

Steps

1. Log in to the vCenter server management interface as root: `<https://vcenterIP:5480>`.
2. In the vCenter server management interface, select **Syslog**.
3. From the **Forwarding Configuration** pane, click **Configure** if you have not configured any remote syslog hosts.
Click **Edit** if you already have configured hosts.
4. In the **Create Forwarding Configuration** pane, enter the server IP address of the destination host. The maximum number of supported destination hosts is three.
5. From **Protocol**, select the protocol to use.
6. In the **Port** text box, enter the port number to use for communication with the destination host.
7. In the **Create Forwarding Configuration** pane, click **Add** to enter another remote syslog server and click **Save**.
8. Verify that the remote syslog server is receiving messages.
9. In the **Forwarding Configuration** section, click **Send Test Message**.

Configure a custom syslog message format in CloudLink Center

Use this procedure to configure a custom syslog message format.

Steps

1. Log in to CloudLink Center.
2. Click **Server > Syslog > Change Syslog Format**. The **Change Syslog Format** window appears..
3. From the **Syslog Format** list, select the **Custom** message format.
4. Enter the string for the syslog entry and click **Change**.

Configure audit logs in SVMs and PowerFlex storage-only nodes

Use this procedure to configure and maintain audit logs of a user in a separate file `commands.log` in SVMs and PowerFlex storage-only nodes and transmit them to the remote servers.

Steps

1. Log in to each SVM or PowerFlex storage-only node using SSH.
2. Run the following commands to record all the commands executed by the users:
 - a. Edit the system-wide BASH runtime configuration file:

- ```
#sudo -e /etc/bash.bashrc
```
- b. Append the following to the end of the file:
 

```
export PROMPT_COMMAND='RETRN_VAL=$?;logger -p local6.debug "$(whoami) [$$]: $(history 1 | sed "s/^[]*[0-9]\+[]*//") [$RETRN_VAL]"'
```
  - c. Press **Esc+:wq** to save the file.
  - d. To setup the audit logging for local6 with a new file as `commands.log`, run the following command to edit the remote syslog BASH runtime configuration file:
 

```
sudo -e /etc/rsyslog.d/bash.conf
```
  - e. Enter the following:
 

```
local6.* /var/log/commands.log
```
  - f. Press **Esc+:wq** to save the file.
3. To forward the audit log file `/var/log/audit/audit.log` to the remote syslog server, edit `/etc/audit/plugins.d/syslog.conf` and do the following::
    - a. Set **active=yes**
    - b. Append **LOG\_LOCAL6** in args:
 For example:

```
#vi /etc/audit/plugins.d/syslog.conf
active = yes # changes made from No to Yes
direction = out
path = /sbin/audisp-syslog
type = always
args = LOG_INFO LOG_LOCAL6 # append LOG_LOCAL6 to write the audit logs to remote
server
format = string
```

4. To transmit the logs to the remote server, do the following:
  - a. Edit the `rsyslog.conf` file:
 

```
vi /etc/rsyslog.conf
```
  - b. Add the following lines to route the logs to the remote server:

```
$ModLoad imfile
$InputFileName /var/log/audit/audit.log
$InputFileTag tag_audit_log:
$InputFileStateFile audit_log
$InputFileSeverity info
$InputFileFacility local6
$InputRunFileMonitor
local6.* @<remoteserverIP>:514 #Remote server IP address to be updated
```

In PowerFlex Manager, both TCP and UDP connections are supported and port number 514 is used for the syslog transfer.

5. Restart the remote syslog service:
 

```
systemctl restart rsyslog.service
```

## Configure iDRAC for audit logging

Use this procedure to manage the alerts, configure bulk alerts, granular alerts, and multiple syslog destinations in iDRAC.

### Prerequisites

Before you configure iDRAC for audit logging, see the following for iDRAC related information:

- iDRAC **Help** in the iDRAC GUI.
- [Event and Error Message Reference Guide](#)
- [Dell EMC iDRAC Service Module Configuration Guide](#)
- [Managing Logs](#)

### About this task

There are 30 audit alerts that can be enabled globally or per alert. Severities can also be configured globally or per alert: critical, warning, and informational. Audit logs cannot be sent to separate destination than the syslog. Separation of iDRAC audit logs can be done by parsing syslog at the syslog destination. For example:

```
Tue Jan 31 14:36:17 2023;10.234.93.12; <174>2023-01-31T22:36:42.113015-06:00 idrac-C0763W2 Severity: Informational, Category: Audit, MessageID: RAC1195, Message: User root via IP 10.234.94.12 requested state / configuration change to Alert Configuration using GUI.
```

### Steps

1. Log in to the iDRAC using the root credentials.
2. To enable or disable alerts, click **Configuration > System Settings > Alert Configuration > Alerts**.
3. To bulk configure alerts by category, severity, and destination type, click **Configuration > System Settings > Alert Configuration > Quick Alert Configuration**.
4. To configure the granular alerts, click **Configuration > System Settings > Alert Configuration > Alert Configuration**.
5. To configure multiple syslog destinations, click **Configuration > System Settings > Alert Configuration > Remote Syslog Settings**.

## Configuring syslogs for Dell PowerSwitch and Cisco Nexus switches

For the Dell PowerSwitch and Cisco Nexus switches, syslog can be transmitted through TLS and audit logs. Ensure TACACS (terminal access controller access-controller system) is used for the audit logs. This section provides links to related information on configuring syslogs for networking components.

| Product                   | Link to the product documentation                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dell PowerSwitch switches | <a href="https://www.dell.com/support/manuals/en-in/smartfabric-os10-emp-partner/smartfabric-os-user-guide-10-5-4/">https://www.dell.com/support/manuals/en-in/smartfabric-os10-emp-partner/smartfabric-os-user-guide-10-5-4/</a>                                                                                                                                                                                                                         |
| Cisco Nexus switches      | <a href="https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/103x/configuration/system-management/cisco-nexus-9000-series-nx-os-system-management-configuration-guide-103x/m-configuring-system-message-logging-10x.html">https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/103x/configuration/system-management/cisco-nexus-9000-series-nx-os-system-management-configuration-guide-103x/m-configuring-system-message-logging-10x.html</a> |
| TACACS logs               | <a href="https://www.cisco.com/c/en/us/td/docs/security/ise/3-2/admin_guide/b_ise_admin_3_2/b_ise_admin_32_maintain_monitor.html#Cisco_Concept.dita_96ba3241-0610-409f-91b2-3331e7a4a947">https://www.cisco.com/c/en/us/td/docs/security/ise/3-2/admin_guide/b_ise_admin_3_2/b_ise_admin_32_maintain_monitor.html#Cisco_Concept.dita_96ba3241-0610-409f-91b2-3331e7a4a947</a>                                                                             |

## Enabling audit logging

This section describes how to enable audit logging in PowerFlex Manager.

The procedures in this section explain how to enable logging for PowerFlex events and Ingress audit messages so this information can be forwarded to an external Security Information and Event Manager (SIEM).

## Define the PowerFlex events notification policy

Use this procedure to define a notification policy to forward events in the PowerFlex system to the rsyslog-forwarder (also known as the syslog-listener). Then, the rsyslog-forwarder forwards the events to the external destinations that are defined in the policy.

### About this task

For this policy, you do not need to define a source, since the required source for PowerFlex events is a built-in feature.

## Steps

### 1. Add a destination:

First, you must add the identified Security Information and Event Manager (SIEM) server as a destination.

#### a. Go to **Settings > Events and Alerts > Notification Policies**.

You can also use the following REST API: `dispatch-destinations/post`

#### b. From the **Destinations** pane, click **Add**.

The **Create New Destination Protocol** window opens.

#### c. Enter the destination name and description.

#### d. From the **Destination Type** menu, select **Syslog**.

#### e. Click **Next** and enter the IP, port, and protocol (TCP) of the target SIEM. Ensure that the SIEM IP, port, and protocol are reachable.

### 2. Create a new policy:

The new policy defines the rules for processing PowerFlex event messages from sources and specifies to which destination that information should be sent.

#### a. Go to **Settings > Events and Alerts > Notification Policies**.

You can also use the following REST API: `dispatch-policies/post`

#### b. Click **Create New Policy**.

#### c. Enter a name and a description for the notification policy. For the policy name, you can enter: **Powerflex events to external Syslog**

#### d. Set the **Source Type** to **Powerflex\_events**.

#### e. From the **Resource Domain** menu, select the resource domain for the notification policy. The resource domain options are:

- All
- Management
- Block (Storage)
- File (Storage)
- Compute (Servers, Operating Systems, virtualization)
- Network (Switches, connectivity etc.)
- Security (RBAC, certificates, CloudLink etc)

#### f. Select the check box beside the severity levels that you want to associate with this policy.

The severity indicates the risk (if any) to the system, in relation to the changes that generated the event message.

#### g. Select the destination that is created in the previous step and click **Submit**.

## Define the Ingress notification policy

Use this procedure to define a notification policy to forward Ingress audit messages. The purpose of this policy is to capture POST, PUT, and DELETE requests of signed-in users passing through the Ingress Controller and send them to the rsyslog-forwarder (also known as the syslog-listener). The rsyslog-forwarder then forwards them to the external destinations.

## Steps

### 1. Add a syslog source, if you do not have one already:

#### a. Go to **Settings > Events and Alerts > Notification Policies**.

You can also use the following REST API: `dispatch-sources/post`

#### b. From the **Sources** pane, click **Add**.

The **Add Source** window opens.

#### c. Enter a source name and description. For the name, you can enter **Ingress**.

#### d. For the type, select **Syslog** and click **Enable Syslog**.

### 2. Create a destination, if you do not have one already.

You can use the destination that you created to define the event to syslog audit notification policy from the previous procedure.

### 3. Create a new policy:

#### a. Go to **Settings > Events and Alerts > Notification Policies**.

You can also use the following REST API: `dispatch-policies/post`

- b. Click **Create New Policy**.
- c. Enter a name and a description for the notification policy. For the policy name, you can enter: **Powerflex Ingress to external Syslog**
- d. Set the **Source Type** to **Syslog**.
- e. Set the **Facility** to **Auditlog**.
- f. Select the check box beside the severity levels that you want to associate with this policy.

The severity indicates the risk (if any) to the system, in relation to the changes that generated the audit messages.

- g. Select the destination that is created in the previous step and click **Submit**.

## Change Ingress setting to emit audit messages

Use this procedure to ensure that requests of signed-in users are sent.

### About this task

This procedure provides the steps that are required to turn the silent flag off (set it to false) in the Ingress audit plug-in. If this flag is not turned off, the audit messages that are related to POST, PUT, and DELETE requests of signed-in users passing through the Ingress Controller will not be sent.

### Steps

1. Log in to one of the management and orchestration cluster nodes with `kubectl` permissions. Then, copy and paste the following script for enabling or disabling the silent flag:

```
kubectl get cm -n kube-system lua-audit-conf -o yaml > ./lua-audit-conf.current.yaml
sed 's/"silent": true/"silent": false/g' ./lua-audit-conf.current.yaml > ./lua-audit-
conf.silent-off.yaml
sed 's/"silent": false/"silent": true/g' ./lua-audit-conf.current.yaml > ./lua-audit-
conf.silent-on.yaml
echo "Copy + Paste either:"
echo "kubectl apply -f ./lua-audit-conf.silent-on.yaml --force"
echo "OR:"
echo "kubectl apply -f ./lua-audit-conf.silent-off.yaml --force"
```

2. Run the following command to start the audit:

```
kubectl apply -f ./lua-audit-conf.silent-off.yaml --force
```

3. Wait one minute.
4. To ensure the configuration changes made are reflected across all nodes, you must now refresh the user interface. To refresh the user interface, quickly press **F5** or **Ctrl+R** on the browser while on the user interface five times. All Ingress audit messages are now forwarded to the configured SIEM servers.

# Migrating to NVMe/TCP on ESXi

This section contains instructions for migrating a VMFS datastore from SDC to NVMe/TCP using Storage vMotion.

PowerFlex offers the following options for migrating from SDC to NVMe/TCP on ESXi:

- Online migration using Storage vMotion (VMFS only), as described in this section  
The standard way of using Storage vMotion to move storage now also supports switching protocols by migrating to a new Datastore.
- Offline conversion (VMFS only)  
Offline conversion is a new option for converting an existing VMFS datastore from SCSI (SDC) to NVMe/TCP without having to copy all the data over the network. This option is covered in this KB: <https://www.dell.com/support/kbdoc/en-us/000213232>

Dell Technologies recommends using VMware Storage vMotion to migrate data from a volume that is presented by SDC to one presented by NVMe/TCP.

This migration is intended for VMDK (noncluster) customers who want to convert their SDC to NVMe/TCP.

Linux environments, ESXi clusters, and RDMS are not included in this section.

## Requirements

See the following VMware product documentation links for information about Storage vMotion requirements and limitations: <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vcenterhost.doc/GUID-A16BA123-403C-4D13-A581-DC4062E11165.html>

See the following VMware product documentation links for information about requirements and limitations of VMware NVMe Storage: <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-9AEE5F4D-0CB8-4355-BF89-BB61C5F30C70.html>

<https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-storage/GUID-9AEE5F4D-0CB8-4355-BF89-BB61C5F30C70.html>

See the following VMware KB article for more details about Storage migration (Storage vMotion), with the virtual machine powered on: <https://kb.vmware.com/s/article/1005241>

Ensure that you satisfy these requirements before you begin the migration:

- Ensure the ESXi version is 7.0u3 or later.
- Ensure the PowerFlex version is 4.5 .x.

## Workflow

The following steps summarize the workflow that you need to follow to migrate from SDC to NVMe/TCP using Storage vMotion:

1. Create and map a new volume of equal or greater size than the current VMFS datastore via NVMe/TCP to the same host.
2. Scan for the newly mapped volume.
3. Create a new datastore on the NVMe/TCP volume.
4. Perform the standard data migration using Storage vMotion by using a non-disruptive process.

# Prepare the VMware ESXi node for mapping NVMe/TCP volumes

Before migrating the data, you must prepare the VMware ESXi node for mapping NVMe/TCP volumes.

Ensure that you satisfy these requirements before you begin:

- You must have an NVMe over TCP target supported PowerFlex system (version 4.5.x or later).
- Deployed VMware ESXi compute-only nodes.
- The host must be at VMware ESXi version 7.0U3 or higher.

## Enable the NVMe/TCP VMkernel ports

Use this procedure to enable the NVMe/TCP VMkernel ports.

### Steps

1. Log in to the VMware vSphere Client.
2. Click **Home/Inventory** and select the host.
3. Select **Configure > VMkernel adapters**.
4. Edit **PowerFlex-Data 1**.
5. Select the **NVMe over TCP** check box and click **OK**.
6. Repeat these steps for the remaining PowerFlex data networks.
7. Repeat the steps for the remaining hosts in the cluster.

## Add NVMe /TCP software storage adapter

Use this procedure to add an NVMe/TCP software storage adapter.

### Steps

1. Log in to the VMware vSphere Client.
2. Click **Home > Inventory > Hosts and Clusters**.
3. In the VMware vSphere console, browse to the customer data center, compute-only cluster, and select the added host.
4. From the right pane, click **Configure > Storage Adapters**.
5. From the right pane, click **Add Software Adapter**.
6. Click **Add NVMe over TCP adapter**.
7. Select the first Virtual switch VMNIC and click **OK**.
8. Click **Add NVMe over TCP adapter**.
9. Select the second Virtual switch VMNIC and click **OK**.

## Copy the host NQN

Use this procedure to copy the host NQN to the copy buffer. The host NQN details are required when you add the host to PowerFlex.

### Steps

1. Log in to VMware vSphere Client.
2. Select the first host.
3. From the right pane, click **Configure > Storage Adapters**.
4. Select the first VMware NVMe over TCP storage adapter. For example, **vmhba6x**.
5. From the pane, select **Controllers/Add Controller**.



The host NQN is listed at the top of the form.

6. Click **COPY** and place the host NQN in the copy buffer.
7. Click **CANCEL**.
8. Repeat the steps for all the hosts.

## Add a host to PowerFlex

Use this procedure to add a host to PowerFlex.

### Steps

1. Log in to PowerFlex Manager.
2. Click **Block > Hosts**.
3. Click **+Add Host**.
4. Enter the hostname and paste the host NQN from the copy buffer.
5. Enter the **Number of Paths Per Volume**. The default number of paths is four per volume, and the maximum number of paths is eight per volume.
6. Enter the **Number of System Ports per Protection Domain**. The default number of system ports is 10 per protection domain, and the maximum number of system ports is 16 per protection domain.
7. Click **Add**.

## Create a volume

Use this procedure to create a volume.

### Steps

1. From PowerFlex Manager, click **Block > Volumes**.
2. Click **+Create Volume**.
3. Enter the number of volumes and the name of the volumes.
4. Select **Thick** or **Thin**. Thin is the default.
5. Enter the required volume size in GB, specifying the size in 8 GB increments.
6. Select the NVMe storage pool and click **Create**.

## Map a volume to the host

Use this procedure to map a volume to the host.

### Steps

1. From PowerFlex Manager, click **Block > Volumes**.
2. Select the volume check box and click **Mapping > Map**.
3. Select the protocol **NVMe**.
4. Select the check box for the host to which you are mapping the volume.
5. Click **Map**.

## Discover and connect the NVMe/TCP Target

Use the procedure to discover and connect the NVMe over TCP Target PowerFlex system. Use the `esxcli` command to perform the operation.

### Steps

1. Log in to the ESXi server using ssh.

2. Run the discovery query on each adapter:

```
#esxcli nvme fabrics discover -a vmhba6x -i 192.168.x.x -p 8009
#esxcli nvme fabrics discover -a vmhba6y -i 192.168.x.y -p 8009
```

In the first example above, 6x is the first NVMe over TCP software adapter and 6y is the second NVMe over TCP software adapter.

In the second example above, 192.168.x.x is first data IP Address and 192.168.x.y is second data IP Address, depends on which VMNIC is enabled for which software NVMe over TCP adapter.

3. Connect to the PowerFlex system by appending “-c” to the discovery query command.

```
#esxcli nvme fabrics discover -a vmhba64 -i 192.168.x.x -p 8009 -c
#esxcli nvme fabrics discover -a vmhba65 -i 192.168.x.y -p 8009 -c
```

4. Get the controller list by verifying the connected controllers.

```
#esxcli nvme controller list
```

## Perform a rescan of the storage

Use this procedure to perform a rescan of the storage.

### Steps

1. In the vSphere Client object navigator, browse to a host, a cluster, a data center, or a folder that contains hosts.
2. From the right-click menu, select **Storage > Rescan Storage**.
3. Specify the extent of the rescan.

| Option                              | Description                                                                                                                                      |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Scan for New Storage Devices</b> | Rescan all adapters to discover new storage devices. If new devices are discovered, they appear in the device list.                              |
| <b>Scan for New VMFS Volumes</b>    | Rescan all storage devices to discover new datastores that have been added since the last scan. Any new datastores appear in the datastore list. |

## Create a VMFS datastore on the NVMe/TCP volume

Use this procedure to create a VMFS datastore on the NVMe/TCP volume.

### Steps

1. Log in to vCenter.
2. Select **Home/Inventory** and select the storage icon.
3. Right-click the CO cluster and select **Storage/New Datastore**.
4. Select VMFS and click **NEXT**.
5. Enter the name of the datastore and select a host from the list.
6. You should see a new disk called NVMe TCP Disk (eui.#####).
7. Select the disk and click **NEXT**.
8. Select VMFS 6 and click **NEXT**.
9. Leave the default configuration unless you have been otherwise instructed and click **NEXT**.
10. Review your selections and click **FINISH**.

# Migrate the data with Storage vMotion

After you prepared the node, you can migrate the data with Storage vMotion.

Follow the standard VMware procedure to migrate the virtual machines from an SDC-based datastore to an NVMe/TCP-based datastore: <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vcenterhost.doc/GUID-A15EE2F6-AAF5-40DC-98B7-0DF72E166888.html>