Dell PowerFlex 4.5.x

Administration Guide

March 2024
Rev. 3.0

DELL Technologies

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.

Contents

1

Introduction

This document provides procedures for using Dell PowerFlex Manager to administer your Dell PowerFlex system.

It provides the following information:

- Initial configuration and setup
- Performing common tasks
- Displaying system information at a glance
- Managing block storage
- Managing file storage
- Protecting your storage environment
- Performing lifecycle operations for a resource group
- Managing resources
- Monitoring events and alerts
- Configuring system settings
- PowerFlex Manager user interface reference
- Additional administration activities
- Retrieving logs for PowerFlex servers
- Retrieving logs for PowerFlex components
- Additional PowerFlex logs
- Managing storage devices using CloudLink

The target audience for this document includes system administrators responsible for managing PowerFlex systems.

For additional PowerFlex software documentation, go to PowerFlex software technical documentation.

2

Revision history

Table 1. Revisions

Date	Document revision	Description of changes
March 2024	3.0	Updates for release 4.5.2
November 2023	2.0	Updates for release 4.5.1
September 2023	1.0	Initial release

3

Initial configuration and setup

This section includes tasks you need to perform when you first begin using PowerFlex Manager.

Initial configuration

The first time you log in to PowerFlex Manager, you are prompted with an **Initial Configuration Wizard**, which prompts you to configure the basic settings that are required to start using PowerFlex Manager.

Before you begin, have the following information available:

- SupportAssist configuration details

  SupportAssist refers to Secure Connect Gateway, which is used for call home functionality and remote connectivity.

- Information about whether you intend to use a Release Certification Matrix (RCM) or Intelligent Catalog (IC)
- Information about the type of installation you want to perform, including details about your existing PowerFlex instance, if you intend to import from another PowerFlex instance

To configure the basic settings:

1. On the **Welcome** page, read the instructions and click **Next**.
2. On the **SupportAssist** page, optionally enable SupportAssist and specify SupportAssist connection settings, and click **Next**.
3. On the **Installation Type** page, specify whether you want to deploy a new instance of PowerFlex or import an existing instance, and click **Next**.
4. On the **Summary** page, verify all settings for SupportAssist and installation type. Click **Finish** to complete the initial configuration.

After completing the **Initial Configuration Wizard**, you can get started using PowerFlex Manager from the **Getting Started** page.

Enabling SupportAssist

SupportAssist is a secure support technology for the data center. SupportAssist refers to Secure Connect Gateway, which is used for call home functionality and remote connectivity. You can enable SupportAssist, as part of the initial configuration wizard. Alternatively, you can enable it later by adding it as a destination to a notification policy in Events and Alerts.

PowerFlex Manager provides support through integration with the secure connect gateway ensuring better alignment with Dell Technologies services initiatives to enhance the user experience. SupportAssist is the functionality that enables this connection.

When you enable SupportAssist, you can take advantage of the following benefits, depending on the service agreement on your device:

- Automated issue detection - SupportAssist monitors your Dell Technologies devices and automatically detects hardware issues, both proactively and predictively.
- Automated case creation - When an issue is detected, SupportAssist automatically opens a support case with Dell Technologies Support.
- Automated diagnostic collection - SupportAssist automatically collects system state information from your devices and uploads it securely to Dell Technologies. Dell Technologies Support uses this information to troubleshoot the issue.
- Proactive contact - A Dell Technologies Support agent contacts you about the support case and helps you resolve the issue.

The first time that you access the initial configuration wizard, the connection status displays as not configured.

Ensure you have the details about your SupportAssist configuration.

If you do not enable SupportAssist in the initial setup, you can add it later as a destination when adding a notification policy through **Settings** > **Events and Alerts** > **Notification Policies**.

1. Click **Enable SupportAssist**.
2. From the **Connection Type** tab, there are two options:

If you want to:	Do the following:
Connect directly to Dell Technologies.	Click **Connect Directly**.
Connect to a SupportAssist gateway server that connects to Dell Technologies by remote access.	Click **Connect via Gateway Server** and provide the following details: • The IP and port number that is assigned to the primary and secondary gateway servers. The port number is auto populated to **9443**. • Optionally, click **Add Gateway** to include an additional gateway server. The maximum number of gateways is eight. • If your environment has a proxy server, enter the IP address, port number, username, and password for the proxy server. • Enter the access key and PIN for authentication to SupportAssist. • Optionally, click **Test connection** to test the connection status. • Optionally, click **Send Test Alert** to send a test alert.

3. From the **Support Contacts** tab, identify the primary support contact by providing their first name, last name, email, and phone details. Optionally, you can add up to two additional support contacts.
4. From the **Device Registration** tab, register your device by completing the following steps:
   a. Select the type of device registration from the **Type** menu.
   b. Depending on the device registration type, you may have to enter information:

Device registration type	Information required
• PowerFlex rack • PowerFlex appliance	• Enterprise License Management Systems (ELMS) Software Unique ID (eSWUID) • Solution serial number
PowerFlex software	N/a

5. From the **Customize Connection to SupportAssist** tab, you can:
   a. Click **Connect to CloudIQ** to enable Dell Technologies to send telemetry data, alerts, and analytics through SupportAssist.
   b. Click **Enable Remote Support** to enable authorized Dell Technologies support engineers to troubleshoot your system remotely.
6. From the **Re-authenticate SupportAssist** tab, click **request a New Access Key and PIN** to generate an access key and pin. The **AccessKey Portal** opens.
   a. From the menu, select **SERIALNUMBER**.
   b. Enter the serial number of your device or PowerFlex software and click **Submit**.
   c. Click **Generate New Access key**.
7. From the **Re-authenticate SupportAssist** tab, enter the access key and pin.
8. Click **Next**.

After you complete the initial configuration, go to the **Settings** page and verify that SupportAssist has been turned on. You may need to configure the SupportAssist policy explicitly on the **Settings** > **Events and Alerts** > **Notification Policies** page.

Related information

Monitoring events and alerts
License management
Add a notification policy

Specifying the installation type

If you have an existing PowerFlex deployment that you would like to import, you can specify details about this deployment as part of the initial configuration. Alternatively, if you would like to deploy a new instance, you can bypass the import step as part of the initial configuration.

The initial configuration wizard supports three different installation workflows:

- No migration required

You would like to deploy a new instance of PowerFlex.

If you would like to use the legacy PowerFlex Installer to provide an installation topology file, click **Deploy With Installation File** on the **Getting Started** page after you complete the initial configuration. See the topic on deploying a PowerFlex cluster using a CSV topology file in the *Dell PowerFlex 4.5.x Install and Upgrade Guide* for more information.

- Migration from a core PowerFlex (software-only) instance that was not managed with PowerFlex Manager

  In this workflow, you need to provide the IP and credentials for the PowerFlex MDM cluster

- Migration from a full PowerFlex Manager environment that had previously been used to manage a PowerFlex instance

  In this workflow, you need to provide the IP and credentials for the PowerFlex Manager virtual appliance instance

If you are importing an existing PowerFlex deployment that was not managed by PowerFlex Manager, make sure you have the IP address, username, and password for the primary and secondary MDMs. If you are importing an existing PowerFlex deployment that was managed by PowerFlex Manager, make sure you have the IP address, username, and password for the PowerFlex Manager virtual appliance.

1. Click **I want to deploy a new instance of PowerFlex** if you do not have an existing PowerFlex deployment and would like to bypass the import step.
2. Click **I have a PowerFlex instance to import** if you would like to import a an existing PowerFlex instance that was not managed by PowerFlex Manager.

   Specify whether you are currently running **PowerFlex 3.x** or **PowerFlex 4.x**.

   For a PowerFlex 3.x system, provide the following details about the existing PowerFlex instance:

   - IP addresses for the primary and secondary MDMs (separated by a comma with no spaces)
   - Admin username and password for the primary MDM
   - Operating system username and password for the primary MDM
   - LIA password

   For a PowerFlex 4.x system, indicate whether the PowerFlex instance is used for **Production Storage** or a **Management Cluster**. The Management Cluster use case is applicable for PowerFlex appliance and PowerFlex rack install types that have a dedicated management cluster with PowerFlex as a shared storage for the datastore hosting the Management VMs.

   Then, provide the following details about the existing PowerFlex instance:

   - IP addresses for all nodes with a primary and secondary MDM
   - System ID for the cluster
   - LIA password
3. Click **I have a PowerFlex instance managed by PowerFlex Manager to import** if you would like to import a an existing PowerFlex directly from an existing PowerFlex Manager virtual appliance.

   Provide the following details about the existing PowerFlex Manager virtual appliance:

   - IP address or DNS name for the virtual appliance
   - Username and password for the virtual appliance
4. Click **Next** to proceed.

For a full PowerFlex Manager migration, the import process backs up and restores information from the old PowerFlex Manager virtual appliance. The migration process for the full PowerFlex Manager workflow imports all resources, templates, and services from a 3.8 instance of PowerFlex Manager. The migration also connects the legacy PowerFlex gateway to the MDM cluster, which enables the **Block** tab in the user interface to function.

The migrated environment includes the PowerFlex gateway resource. The operating system hostname and asset/service tag are set to **`powerflex`**.

For a software-only PowerFlex system, there is no PowerFlex Manager information available after the migration completes. The migrated environment does not include resources, templates, and services.

Verifying the initial configuration

Before you complete the initial configuration, you can review all the settings you provided for SupportAssist, compliance, and installation type.

1. On the **Summary** page, verify the settings that you configured on the previous pages.
2. To edit any information, click **Back** or click the corresponding page name in the left pane.

3. If you are importing an existing PowerFlex instance from PowerFlex Manager, type **IMPORT POWERFLEX MANAGER**.
4. If the information is correct, click **Finish** to complete the initial configuration.

   If you are importing an existing environment, PowerFlex Manager displays a message indicating that the import operation is in progress. When the import operation is complete, PowerFlex Manager displays the **Getting Started** page.

If you did not migrate an existing PowerFlex environment, you can now deploy a new instance of PowerFlex.

After completing the migration wizard for a full PowerFlex Manager import, you must perform these steps:

1. On the **Settings** page, upload the compatibility matrix file and upload the latest repository catalog (RCM or IC).
2. On the **Resources** page, select the PowerFlex entry, and perform a nondisruptive update.
3. On the **Resource Groups** page, perform an RCM/IC upgrade on any migrated service that must be upgraded.

   The migrated resource groups are initially non-compliant, because PowerFlex Manager is running a later RCM that includes PowerFlex 4.x. These resource groups must be upgraded to the latest RCM before they can be expanded or managed with automation operations.

   CAUTION: Check the Alerts page before performing the upgrade. Look for major and critical alerts that are related to PowerFlex Block and File to be sure the MDM cluster is healthy before proceeding.
4. Power off the old PowerFlex Manager VM, the old PowerFlex gateway VM, and the presentation server VM.

   The upgrade of the cluster causes the old PowerFlex Manager virtual appliances to stop working.
5. After validating the upgrade, decommission the old instances of PowerFlex Manager, the PowerFlex gateway, and the presentation server.

   Do not delete the old instances until you have had a chance to review the initial configuration and confirm that the old environment was migrated successfully.

After completing the migration wizard for a PowerFlex (software-only) import, you must perform these steps:

1. On the **Settings** page, upload the compatibility matrix file and upload the latest software-only catalog.

   The software-only catalog is new in this release. This catalog only includes the components that are required for an upgrade of PowerFlex.
2. On the **Resources** page, select the PowerFlex entry, and perform a nondisruptive update.

   You do not need a resource group (service) to perform an upgrade of the PowerFlex environment. In addition, PowerFlex Manager does not support **Add Existing Resource Group** operations for a software-only migration. If you want to be able to perform any deployments, you need a new resource group. Therefore, you must create a new template (or clone a sample template), and deploy a new resource group from the template.

Getting started

The **Getting Started** page guides you through the common configurations that are required to prepare a new PowerFlex Manager environment. A green check mark on a step indicates that you have completed the step. Only super users have access to the **Getting Started** page.

The following table describes each step:

Step	Description
Upload Compliance File	Provide compliance file location and authentication information for use within PowerFlex Manager. The compliance file defines the specific hardware components and software version combinations that are tested and certified by Dell for hyperconverged infrastructure and other Dell products. This step enables you to choose a default compliance version for compliance or add new compliance versions. You can also click **Settings** > **Repositories** > **Compliance Versions**. **NOTE:** Before you make an RCM or IC the default compliance version, you must first upload a suitable compatibility management file under **Settings** > **Repositories** > **Compatibility Management**.

Step	Description
Define Networks	Enter detailed information about the available networks in the environment. This information is used later during deployments that are based on templates and resource groups. These deployments use the network information to configure nodes and switches to have the right network connectivity. PowerFlex Manager uses the defined networks in templates to specify the networks or VLANs that are configured on nodes and switches for your resource groups. This step is enabled immediately after you perform an initial configuration for PowerFlex Manager. You can also click **Settings** > **Networking** > **Networks**. If you plan to perform an advanced CSV-based deployment, this step can be skipped.
Discover Resources	Grant PowerFlex Manager access to resources (nodes, switches, virtual machine managers) in the environment by providing the management IP and credential for the resources to be discovered. This step is not enabled until you define your networks. You can also click **Resources** > **Discover Resources**. If you plan to perform an advanced CSV-based deployment, this step can be skipped.
Manage Deployed Resources (Optional)	Add an existing resource group for a cluster that is already deployed and manage the resources within PowerFlex Manager. This step is not enabled until you define your networks. You can also click **Lifecycle** > **Resource Groups** > **Add Existing Resource Group**. If you plan to perform an advanced CSV-based deployment, this step can be skipped.
Deploy Resources	Create a template with requirements that must be followed during a deployment. Templates enable you to automate the process of configuring and deploying infrastructure and workloads. For most environments, you can clone one of the sample templates that are provided with PowerFlex Manager and make modifications as needed. Choose the sample template that is most appropriate for your environment. For example, for a hyperconverged deployment, clone one of the hyperconverged templates. For a two-layer deployment, clone the compute-only templates. Then clone one of the storage templates. This step is not enabled until you define your networks. You can also click **Lifecycle** > **Templates**. If you plan to perform an advanced CSV-based deployment, this step can be skipped.
Manage PowerFlex License	Configure licensing for PowerFlex. You can also click **Settings** > **License Management**.

If you would like to use the legacy PowerFlex Installer to provide an installation topology file, click **Deploy With Installation File**. See the topic on deploying a PowerFlex cluster using a CSV topology file in the *Dell PowerFlex 4.5.x Install and Upgrade Guide* for more information.

The topology report sent from PowerFlex Manager to Embedded System Enabler (ESE) must be updated to include SWID and installation ID. These IDs must be sent for all cases- rack, appliance, and software. If the data is missing, fields display empty or null values. Ensure that the file does not break.

To revisit the **Getting Started** page, click **Getting Started** on the help menu.

Related information

Networking
Discover a resource
Adding an existing resource group
Templates
License management

Changing your 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.

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**.

4

Performing common tasks

This section includes tasks that you perform regularly when using PowerFlex Manager.

Deploying and provisioning

The following table describes common tasks for deploying and provisioning the system and what steps to take in PowerFlex Manager to initiate each task:

If you want to...	Do this in PowerFlex Manager...
Perform an advanced PowerFlex CSV deployment	If you would like to use the legacy PowerFlex Installer to provide an installation topology file, click **Deploy With Installation File** on the **Getting Started** page. See the topic on deploying a PowerFlex cluster using a CSV topology file in the *Dell PowerFlex 4.5.x Install and Upgrade Guide* for more information.
Define a resource group and infrastructure requirements	1. If you will be managing and updating components other than PowerFlex, upload the compliance file on the **Settings** > **Repositories** > **Compliance Versions** page. 2. Define the networks you need on the **Settings** > **Networking** > **Networks** page. 3. Discover the resources required for your deployment on the **Resources** > **Discover Resources** page. 4. Clone a sample template and make changes as needed. Click **Lifecycle** > **Templates** and click **Sample templates**. Open a sample template and click **More Actions** > **Clone** on the right side of the screen. For example, for a PowerFlex hyperconverged deployment, clone one of the PowerFlex hyperconverged templates. For a two-layer deployment, clone one of the PowerFlex storage-only templates. Then clone one of the PowerFlex compute-only templates. You can also create a new template. However, for most environments, you can simply clone one of the sample templates that are provided with PowerFlex Manager.
Deploy a new resource group	Click **Lifecycle** > **Resource Groups**. On the **Resource Groups** page, click **Deploy New Resource Group**. You can only deploy a resource group using a published template.

Related information

Repositories
Networking
Resources
Preparing a template for a resource group deployment
Deploying a resource configuration in a resource group

Configuring block storage

The following table describes common tasks for deploying and managing block storage and what steps to take in PowerFlex Manager to initiate each task:

If you want to...	Do this in PowerFlex Manager...
Deploy a new block storage configuration	1. If you will be managing and updating components other than PowerFlex, upload the compliance file on the **Settings** > **Repositories** > **Compliance Versions** page. 2. Define the networks you need on the **Settings** > **Networking** > **Networks** page. 3. Discover the resources required for your deployment on the **Resources** > **Discover Resources** page. 4. Clone a sample template and make changes as needed. Click **Lifecycle** > **Templates** and click **Sample templates**. Open a sample template and click **More Actions** > **Clone** on the right side of the screen. 5. Click **Lifecycle** > **Resource Groups**. On the **Resource Groups** page, click **Deploy New Resource Group**. For example, for a PowerFlex hyperconverged deployment, clone one of the PowerFlex hyperconverged templates. For a two-layer deployment, clone one of the PowerFlex storage-only templates. Then, clone one of the PowerFlex compute-only templates. You can also create a new template. However, for most environments, you can simply clone one of the sample templates that are provided with PowerFlex Manager.
Import an existing block storage configuration	Click **Lifecycle** > **Resource Groups** and click **+Add Existing Resource Group**. Be sure to upload a compliance file (if necessary), define the networks, and discover resources before adding the existing resource group.
Managing block storage	On the menu bar, click **Block**, and choose the type of block storage components you want to manage: • **Protection Domains** • **Fault Sets** • **SDSs** • **Storage Pools** • **Acceleration Pools** • **Devices** • **Volumes** • **NVMe Targets** • **Hosts** If you create new objects on the **Block** tab, you need to update the inventory on the **Resources** page, and then click **Update Resource Group Details** on the **Lifecycle** > **Resource Groups** page for any resource group that requires the updates.

Related information

Repositories
Networking
Discover a resource
Clone a template
Deploying a resource configuration in a resource group
Managing block storage

Configuring file storage

The following table describes common tasks for deploying and managing file storage and what steps to take in PowerFlex Manager to initiate each task:

If you want to...	Do this in PowerFlex Manager...
Deploy a new file storage configuration	1. Deploy a storage-only or hyperconverged resource group that includes a PowerFlex cluster that will be associated with the PowerFlex file cluster. When you deploy the PowerFlex file cluster, the control volumes that are needed for file enablement are added automatically. 2. If you will be managing and updating components other than PowerFlex, upload the compliance file on the **Settings** > **Repositories** > **Compliance Versions** page. 3. Define the networks that you need on the **Settings** > **Networking** > **Networks** page. 4. Discover the resources required for your deployment on the **Resources** > **Discover Resources** page. 5. Clone a sample template and make changes as needed. Click **Lifecycle** > **Templates** and click **Sample templates**. Open a sample template and click **More Actions** > **Clone** on the right side of the screen. For a file storage deployment, clone one of the following sample templates: • **PowerFlex File** • **PowerFlex File - SW Only** 6. Click **Lifecycle** > **Resource Groups**. On the **Resource Groups** page, click **Deploy New Resource Group**. For a PowerFlex file cluster, you must have a minimum of two nodes and a maximum of 16 nodes. For a PowerFlex file cluster, you must choose **Use Compliance File Linux Image** for the **OS Image**, **Compute Only** for the **PowerFlex Role**. Also, select **Enable PowerFlex File**. The sample templates for file storage configuration pull in the PowerFlex management and PowerFlex data networks from the associated PowerFlex gateway. In addition to the PowerFlex management and PowerFlex data networks, you need to include a NAS management network and at least one NAS data network. One NAS data network is enough, but, for redundancy, two networks are recommended. **NOTE:** Check the network settings carefully, as they are different for standard configurations and software-only configurations.
Import an existing file storage configuration	Click **Lifecycle** > **Resource Groups** and click **+Add Existing Resource Group**. Upload a compliance file (if necessary), define the networks, and discover resources before adding the existing resource group. PowerFlex Manager does not support importing existing deployments for software-only NAS environments.
Manage file storage	On the menu bar, click **File**. Then, choose the type of file components you want to manage: • **NAS Servers** • **File Systems** • **SMB Shares** • **NFS Exports** • **File Protection** If you create new objects on the **File** tab, you need to update the inventory on the **Resources** page. Then, you need to click **Update Resource Group Details** on the **Lifecycle** > **Resource Groups** page for any resource group that requires the updates.

Related information

Deploy the PowerFlex file cluster
Managing file storage

Managing components

Once PowerFlex Manager is configured, you can use it to manage the system.

The following table describes common tasks for managing system components and what steps to take in PowerFlex Manager to initiate each task:

If you want to...	Do this in PowerFlex Manager...
View network topology	1. Click **Lifecycle** > **Resource Groups**. 2. On the **Resource Groups** page, select a resource group. 3. On the **Resource Group Details** tab, click the **Port View** tab.
Run inventory (nodes, switches, PowerFlex gateway, and VMware vCenter cluster)	1. Click **Resources** and click the **All Resources** tab. 2. Click the check box for the resource you want to update and then click **Run Inventory**. 3. After running the inventory, click **Update 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	Click **Lifecycle** > **Resource Groups** and click **+Add Existing Resource Group**. Be sure to upload a compliance file (if necessary), define the networks, and discover resources before adding the existing resource group.
Perform node expansion	1. Click **Lifecycle** > **Resource Groups**. On the **Resource Groups** page, select a resource group. 2. On the **Resource Group Details** tab, under **Add Resources**, click **Add Nodes**. The procedure is the same for new resource groups and existing resource groups.
Remove a node	1. Click **Lifecycle** > **Resource Groups**. 2. On the **Resource Groups** page, select a resource group. 3. On the **Resource Group Details** tab, under **More Actions**, click **Remove Resource**. 4. Select **Delete Resource** for the **Resource removal type**.
Enter service mode (applicable for PowerFlex appliance and PowerFlex rack only)	1. Click **Lifecycle** > **Resource Groups**. 2. On the **Resource Groups** page, select a resource group. 3. On the **Resource Group Details** tab, under **More Actions**, click **Enter Service Mode**.
Exit service mode (applicable for PowerFlex appliance and PowerFlex rack only)	1. Click **Lifecycle** > **Resource Groups**. 2. On the **Resource Groups** page, select a resource group. 3. On the **Resource Group Details** tab, under **More Actions**, click **Exit Service Mode**.
Replace a drive	1. Click **Lifecycle** > **Resource Groups**. 2. On the **Resource Groups** page, select a resource group. 3. Under **Physical Nodes**, click **Drive Replacement**.
Reconfigure MDM roles	1. Click **Lifecycle** > **Resource Groups**. 2. On the **Resource Groups** page, select a resource group. 3. On the **Resource Group Details** tab, click **Reconfigure MDM Roles** under **More Actions**. You can also reconfigure MDM roles from the **Resources** page. Select a PowerFlex gateway and click **View Details**. Then, click **Reconfigure MDM Roles**.

Related information

Lifecycle
Resource groups
Templates
Resources

Monitoring system health

Once PowerFlex Manager is configured, you can monitor system health.

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

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.
Monitor software and firmware compliance	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	From the compliance report, view the firmware or software components. Click **Update Resources** to update non-compliant resources.
Generate a troubleshooting bundle	1. Click **Settings** and click **Serviceability**. 2. Click **Generate Troubleshooting Bundle**. You can also generate a troubleshooting bundle from the **Resource Groups** page: 1. Click **Lifecycle** > **Resource Groups**. 2. On the **Resource Groups** page, select a resource group. 3. On the **Resource Group Details** page, click **Generate Troubleshooting Bundle**.
Download a report that lists compliance details for all resources	1. Click **Resources**. 2. Click **Export Report** and download a compliance report (PDF or CSV) or a configuration report (PDF).
View alerts	On the menu bar, click **Monitoring** > **Alerts**.

Related information

Lifecycle
Resources

Managing external changes

If you make manual changes outside of PowerFlex Manager, you might need to perform some steps within PowerFlex Manager to ensure that the external changes are reflected within the user interface and the environment is kept in a healthy state.

The following table describes common tasks for managing external changes and what steps to take in PowerFlex Manager for each task:

If you have...	Do this in PowerFlex Manager...
Manually added VMware NSX to a cluster outside of PowerFlex Manager	Click **Update Resource Group Details** on the resource group, so it will correctly reflect the environment with VMware NSX, which will be in lifecycle mode.

If you have...	Do this in PowerFlex Manager...
Manually replaced a node outside of PowerFlex Manager for a resource group in PowerFlex Manager	1. Remove the node from the resource group. On the **Lifecycle** > **Resource Groups** page, select a resource group. On the **Resource Group Details** page, under **More Actions**, click **Remove Resource**. 2. Remove the node from the list of resources. On the **Resources** page, click the **All Resources** tab. From the list of resources, select the resource, and click **Remove**. 3. Discover the new node. On the **Resources** page, click **Discover** on the **All Resources** tab. 4. Update the resource group details. On the **Lifecycle** > **Resource Groups** page, click **Update Resource Group Details**.
Manually created additional VLANs on the VDS in vCenter outside of PowerFlex Manager	1. Remove the resource group. On the **Resource Group Details** page, click **Remove Resource Group** under **More Actions**. When you click **Remove Resource Group**, do not select **Delete Resource Group** as the **Resource Group Removal Type**. This action completely tears down the resource group and makes configuration changes to the nodes, switch ports, virtual machine managers, and PowerFlex. Instead, select **Remove Resource Group** as the **Resource Group Removal Type**. Then, to keep the nodes in the inventory, select **Leave nodes in PowerFlex Manager inventory and set state to** and choose **Managed**. 2. Rediscover the resource group. On the **Lifecycle** > **Resource Groups** page, click **+Add Existing Resource Group**. If you do not choose the correct options when you remove the resource group, you could tear down the resource group and destroy it, or leave the servers in an unmanaged state, and not be able to add the existing resource group.
Manually created volumes outside of PowerFlex Manager	Click **Run Inventory** on the **Resources** page to update the inventory. Then, click **Update Resource Group Details** on the **Lifecycle** > **Resource Groups** page for any resource group that requires the updated volumes.
Manually deleted volumes outside of PowerFlex Manager	Click **Run Inventory** on the **Resources** page to update the inventory. Then, click **Update Resource Group Details** on the **Lifecycle** > **Resource Groups** page for any resource group that requires updated information about volumes deleted. PowerFlex Manager displays a message indicating that the volumes have been removed from the resource group.
Manually added nodes outside of PowerFlex Manager	Click **Run Inventory** on the **Resources** page to update the inventory. Then, click **Update Resource Group Details** on the **Lifecycle** > **Resource Groups** page for any resource group that requires the updated nodes.
Manually removed nodes outside of PowerFlex Manager	Click **Run Inventory** on the **Resources** page to update the inventory. Then, click **Update Resource Group Details** on the **Resource Groups** page for any resource group that requires updated information about nodes deleted. Then, manually remove the resource on the **Resources** page by clicking the **All Resources** tab, selecting the resource, and clicking **Remove**.
Renamed objects such as VMware ESXi host, volume, datastore, VDS, port group, data center, cluster, and so forth	Click **Run Inventory** on the **Resources** page to update the inventory. Then, click **Update Resource Group Details** on the **Lifecycle** > **Resource Groups** page for any resource group that requires the updates. Note that vCLS datastore names are based on cluster names, so any change to a cluster name renders the vCLS datastore un-recognizable. If you change the cluster name manually for a deployment, the datastore name hosting the vCLS VMs needs

If you have...	Do this in PowerFlex Manager...
	to be updated. You need to change the vCLS datastore name to match the new cluster name and then perform an **Update Resource Group Details** operation. For example: ● Existing cluster name: **`cluster1`** ● vCLS datastore name: **`powerflex-cluster1-ds-1`** ● Updated cluster name: **`cluster1-new`** ● vCLS datastore name: **`powerflex-cluster1-new-ds-1`**
Manually changed the IP address for a switch	1. Remove the switch. On the **Resources** page, click the **All Resources** tab. From the list of resources, select the switch, and click **Remove**. 2. Rediscover the switch. On the **Resources** page, click the **All Resources** tab and click **Discover**. 3. If the IP address is in use, remove the resource group and add it again. On the **Lifecycle** > **Resource Groups** page, click **+Add Existing Resource Group**.
Created new objects on the **Block** or **File** tab	Click **Run Inventory** on the **Resources** page to update the inventory. Then, click **Update Resource Group Details** on the **Lifecycle** > **Resource Groups** page for any resource group that requires the updates.

Related information

Lifecycle
Resource groups

5

Displaying system information at a glance

This section introduces the Dashboard, which displays a graphical view of the overall health of the system.

The **Dashboard** displays at-a-glance information about overall performance, usable capacity, data savings, resources and inventory, resource groups, and alerts.

Overall performance and latency

This section displays graphs that show the overall performance (IOPS and bandwidth) and latency for block and file configurations within the system.

Usable capacity

This section shows the total capacity, along with details about the physical, system, and free capacity.

Data savings

This section provides details about the overall savings and thin provisioning savings.

Resources/inventory

This section shows the number of resources in the current inventory:

- VM managers
- Nodes
- Switches
- Protection domains
- Storage pools
- Volumes
- Hosts
- File systems
- NAS servers

Resource groups

This section displays a graphical representation of the resource groups deployed based on status. The number next to each icon indicates the number of resource groups in a particular state. The resource groups are categorized into the following states:

Tab	Status	Description
Health	**Healthy**	Green band on the graphic indicates that the resource group is successfully deployed.
	Degraded	Yellow band indicates that resources in a resource group require corrective action, but does not affect overall system health. For example, the firmware version that is installed on a resource in the resource group is not compliant.

Tab	Status	Description
	Critical	Red band indicates resource groups that have critical health problems.
	Service Mode	Yellow band indicates that the resource group has been placed in service mode.
Compliance	**Compliant**	Green band indicates that the resource group is compliant with the target compliance version.
	Out of compliance	Yellow band indicates that the resource group is non-compliant with the target compliance version.

You can monitor node health by viewing the status of the resource group on the **Resource Groups** page.

If a resource group is in a yellow (or warning) state, it means that one or more nodes is in a warning or failed state. If a resource group is in a red (or error) state, it indicates that the resource group has fewer than two nodes that are not in a failed state.

To view the status of a failed node component, hover the cursor on the image of the failed component in the resource group.

Alerts

This section lists the current alerts within the system, categorized by severity level:

- Critical
- Major
- Minor

6

Managing block storage

Block storage management involves the configuration of protection domains, fault sets, storage data servers, and storage pools. In addition, block storage management involves configuring acceleration pools, devices, and volumes, as well as NVMe targets and hosts.

Related information

Configuring block storage

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.

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**.

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.

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.

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**.

Inactivate a protection domain

Use this procedure for a graceful system shutdown.

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.

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**.

Activate a protection domain

Activate the protection domain to enable access to data.

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**.

Remove a protection domain

Remove a protection domain from the PowerFlex system.

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

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.

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.

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).

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.

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

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.

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.

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

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.

- 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.

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.

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**.

An SDS is added to the system.

Configure RMcache

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

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

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

Enabling RMcache 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.

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 RMcache**. Enter the RMcache cache size.
   The minimum RMcache 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.

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.

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.

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.

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.

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**.

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.

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.

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.

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.

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.

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.

- 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.

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.

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. **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.

4. Click **Apply**.

Configure RMcache for the storage pool

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

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

RMcache caching only begins once storage devices have been added to the SDSs. It is possible to enable RMcache 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.

1. On the menu bar, click **Block** > **Storage Pools**.
2. In the list of storage pools, select the check box of the relevant storage pool, and click **Modify** > **Cache**.
3. In the **Storage Pool Cache Settings** dialog box, select **Enable Read RMcache**.
4. 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.

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** > **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.

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**.
   - **Bandwith 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.

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.

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

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.

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

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.
     NOTE: NVDIMM also applies to a DAX device with the 16G based options known as SDPM.
   - **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.

6. Click **Create**.

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

Rename an acceleration pool

Rename an acceleration pool.

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

Remove an acceleration pool

Delete an acceleration pool from PowerFlex.

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

1. On the menu bar, click **Block** > **Acceleration Pools**.
2. In the list of acceleration pools, select the desired acceleration pool.
3. Click **Delete**.
4. In the **Delete Acceleration Pool** dialog box, click **Delete**.
5. 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.

1. On the menu bar, click **Block** > **Devices**.
2. In the list of devices, select the check boxes of the required devices, and click **More Actions** > **Activate**.
3. In the **Activate Device** dialog box, click **Activate**.
4. 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.

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.

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.

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.

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

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.

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

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.

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.

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

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.

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.

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

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:

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 `Vol%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**.

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.

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.

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.

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.

At least two volumes per vTree are required.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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

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:

Source SP				Destination SP: MG: Zero Padded: Thin	Destination SP: MG: Zero Padded: thick	Destination SP: MG: Non Zero Padded: Thin	Destination SP: MG: Non Zero Padded: thick	Destination SP: FG: Zero Padded: Thin
	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.

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.

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.
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.

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.

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.

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 **VTree** 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.

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 **VTree** tab.
5. In the left pane, from the **VTree** 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**.

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.

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

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 **VTree** tab.
5. In the left pane, from the **VTree** 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.

Ensure that the vTree is unmapped.

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 **VTree** 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.

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**.

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
                                        Role options: storage_only, host_only,  or
```

```
storage_and_host
    --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)
                                         Set to 1 in order to indicate no use of
discovery port
    --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
                                         The default is high_performance
    --force_clean                        Clean a previous SDT configuration
    --i_am_sure                          Preemptive approval
```

Modify an NVMe target

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

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.

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**.

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.

- 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.

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.

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
                                        Valid range: 2-128. Default: 10
    --host_os_full_type <OS>            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.

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.

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.

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.

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.

Ensure that the hosts have been approved by GUID.

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.

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

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

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.

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.

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**.

7

Managing file storage

File storage management involves creation and configuration of NAS servers, representation of a set of storage resources as network file storage, and the use of snapshots for protection of those file system resources.

Related information

Configuring file storage

Overview of configuring NAS servers

Before you can provision file storage, a NAS server must be running on the system.

A NAS server is a file server that supports the SMB protocol, the NFS protocol, FTP, or a combination of these protocols to share data with host clients. It also catalogs, organizes, and optimizes read and write operations to the associated file systems.

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

You create NAS servers before creating file systems.

Ensure that the NAS network information is available.

1. Select **File** > **NAS Servers**.
2. Select **Create**.
3. Continue to work through the **Create NAS Server** wizard.

Wizard Screen	Description
Details	Select a protection domain, and 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: • 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:

Wizard Screen	Description
	• 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	Select automatic user mapping, or enable the default account for both a Windows and Linux user.
Summary	Review the content and select **Back** to go back and make any corrections.

4. Select **Create NAS Server** to create the 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

You create a NAS server before creating file systems.

Obtain 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 computer 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.

1. Select **File** > **NAS Servers**.
2. Select **Create**.
3. Continue to work through the **Create NAS Server** wizard.

Wizard Screen	Description
Details	Enter a NAS server name, description, and network details.
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. Multiprotocol configuration is not described in this help system. **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**

Wizard Screen	Description
	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 and select **Back** to go back and make any corrections.

4. Select **Create NAS Server**.
   The **Status** window opens, and you are redirected to the **NAS Servers** page once the server is added.

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

You can change NAS server configuration settings or modify the NAS server properties. In addition, you can remove the NAS server, move a NAS server to another node, or swap roles between the primary and the secondary nodes.

1. Go to the **File** > **NAS server** page.
2. Select on a NAS server in the list to make changes to the NAS server configuration settings.
3. Select the checkbox next to the name of the NAS server, and select:

Option	Description
Modify	To modify the NAS server name or description.
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 must remove all file systems from the NAS server before it can be deleted.
Move NAS Server	To move the NAS server from one node to another node (when a cluster contains more than two nodes).
Swap Nodes	To swap roles between the primary and the secondary nodes for the selected NAS Server.

NAS servers

Use the **File** > **NAS Servers** page to create, view, access, and modify NAS servers.

Create a NAS server

Select **Create** to launch the **Create NAS Server** wizard.

NOTE: If you plan to join the NAS server to Active Directory (AD), you must have NTP configured on your system.

You provide the following information the first time you create a NAS server. You can add or modify the settings after you have created the server.

Option	Description
Details	NAS server name and network details
Sharing Protocol	Type of protocol: • For Windows, select SMB. • For UNIX, select NFSv3, or NFSv4, or both. • For multiprotocol, pick SMB and one or more of the UNIX protocols. Enter the **Windows Server Settings**, or **Unix Directory Services** setting, or both for multiprotocol. See the NAS Server Sharing Protocols help for more information. Enable DNS and enter the DNS server details. DNS is required for:

Option	Description
	• Secure NFS • NAS servers that support SMB file sharing and are joined to AD. • NAS servers that support multiprotocol file systems. See the NAS Server Naming Services help for more information.
User Mapping	If you have enabled SMB to join the active directory domain, or enabled the NAS server for both SMB and NFS, then you must provide the user mapping information. See the NAS Server Sharing Protocols help for more information.

Modify the NAS server name and description

Select a NAS server, and select **Modify** to change the name or description of the NAS server.

Move a NAS server

When you create a new NAS server, node placement is automatic. Use this option to move the NAS server to another node.

Swap Nodes

Use this option to swap the roles between the primary and the secondary nodes for the selected NAS Server.

Configure the 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 cannot 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.

NAS server networks

You can add production, and backup file interfaces to a NAS server, and create routes to external services from **File** > **NAS Servers** > **[nas server]** > **Network**.

File interfaces

Presents the NAS server file interfaces.

You can add more interfaces, and define which will be the preferred interface to use with the NAS server. PowerFlex assigns a preferred interface by default, but you can set which interface to use first for production and backup, and IPv4, and IPv6.

Select **Ping** and enter an IP address or host name to test the connectivity from the NAS server to an external resource.

Select the interface to modify or delete it. All properties of the file interface can be modified.

Routes to external services

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.

NAS server naming services

You modify or configure naming services from **File** > **NAS Servers** > **[nas server]** > **Naming Services**.

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 for 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.

Authentication type	About
Anonymous	Specify the Base DN, and the Profile DN for the iPlanet/OpenLDAP server.

Simple	Specify the following:
	• If using AD, LDAP/IDMU:
	  ○ Bind DN in LDAP notation format; for example, cn=administrator,cn=users,dc=svt,dc=lab,dc=com.
	  ○ Base DN, which is the same as the Fully Qualified Domain Name (for example, svt.lab.com).
	  ○ Profile DN.
	• If using the iPlanet/OpenLDAP server:
	  ○ Bind DN in LDAP notation format; for example, cn=administrator,cn=users,dc=svt,dc=lab,dc=com.
	  ○ Password.
	  ○ Base DN. For example, if using svt.lab.com, the Base DN would be DC=svt,DC=lab,DC=com.
	  ○ Profile DN for the iPlanet/OpenLDAP server.

Kerberos	If using Kerberos authentication, you must perform the following steps before setting LDAP to use Kerberos authentication:

Authentication type	About
	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. Use either of the following methods to configure Kerberos: ● Authenticate to the SMB domain. With this option, you can either authenticate using the SMB server account or authenticate with other credentials. ● Configure a custom realm to point to any type of Kerberos realm (Windows, MIT, Heimdal). With this option, the NAS server uses the custom Kerberos realm defined in the Kerberos subsection of the NAS server's **Security** tab. **NOTE:** If you use NFS secure with a custom realm, you must upload a keytab file.

You can also configure LDAP with SSL (LDAP Secure) and can enforce the use of a Certificate Authority certificate for authentication.

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 then 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. 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.

NAS server sharing protocols

You define the NAS server sharing protocols from **File** > **NAS Servers** > **[nas server]** > **Sharing Protocols**.

SMB server

This section contains options for configuring a Windows server.

If you are 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

This section contains options for configuring an NFS, or NFS secure server for Linux or UNIX support.

Task	Description
Extend the Linux or UNIX credential to enable the storage system to obtain more than 16 group GIDs.	Select or clear **Enable extended Unix credentials**. ● 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 that is contained in the frame. This method has better performance, but it is limited to including up to only 16 group GIDs.

Task	Description
	NOTE: With secure NFS, the UNIX credential is always built by the NAS server, so this option does not apply.
Specify a Linux or 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. **NOTE:** This option can lead to better performance, because it reuses the UNIX credential from the cache instead of building it for each request.

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.

  This method of configuring secure NFS requires fewer steps than configuring a custom realm.

- Configure a custom realm to point to any type of Kerberos realm (AD, MIT, Heimdal). 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 that is 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.

User mapping

If you are configuring a NAS server to support both types of protocols, SMB and NFS, you must 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**, then you must select **Enable automatic mapping for unmapped Windows accounts/users**.

NAS server protection and events

You can enable Network Data Management Protocol (NDMP) for the file servers using NDMP from the **File** > **NAS Servers** > **[nas server]** > **Protection** card.

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`.

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.

Creating event publishers

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

Ensure that the NAS server is SMB enabled to associate an event publisher file with it.

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.

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 severs 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.

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

Before deleting event publishers, ensure that the event publishers are disabled for the NAS server.

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.

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.

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

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

Before deleting the CEPA publishing pools, ensure that the event publishers that are associated with the CEPA pool are deleted first.

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.

NAS server security

You can configure the security settings for a NAS server from the **File** > **NAS Servers** > **[nas server]** > **Security** card.

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 you are configuring Kerberos for Secure NFS, be aware of the following:

- 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 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 SPN must be registered in the DNS server.
- A keytab file must be uploaded to your NAS server when configuring Secure NFS.

NOTE:

- Use the **Retrieve Ketyab 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.

Antivirus support for CAVA is disabled by default. To enable CAVA:

1. Click the **Disabled** button and click **Apply**.
2. If you do not have a current CAVA configuration file available:
   a. Click **Retrieve Current Configuration**.
   b. Complete the CAVA configuration file template.
3. **Upload** the CAVA current configuration file.
4. Click **Enabled** to start antivirus support.

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

When an events publisher is created, events publishing on a NAS server can be enabled. Multiple NAS servers can use the same events publisher.

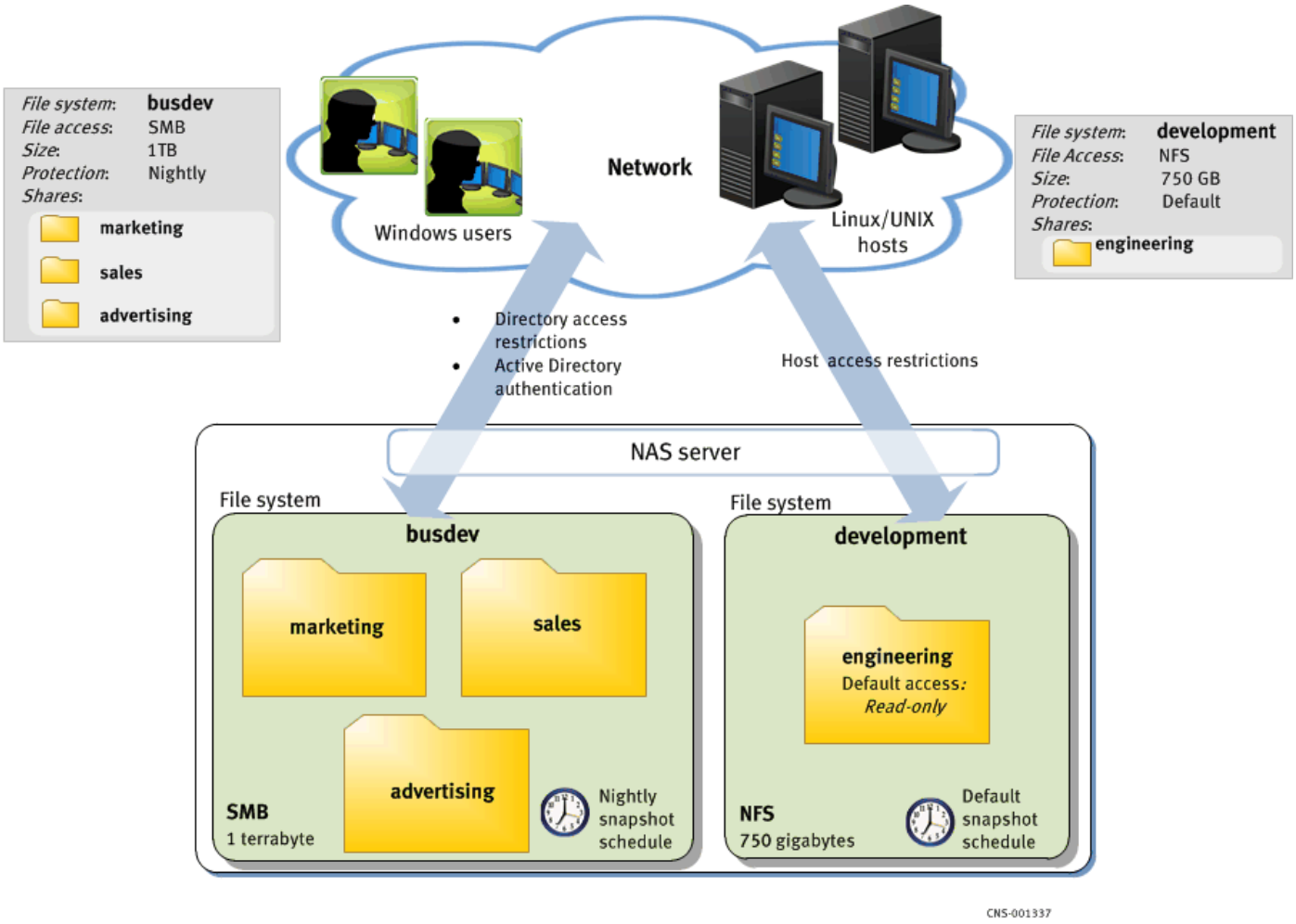
1. Go to **File** > **NAS Servers** > **NAS Servers**
2. Select the check box next to the NAS server name for which you want to enable the event publisher.
3. On the right, click **View Details**.
4. Go to **Security** > **Events Publishing**.
5. Enable the event publisher and select the required event 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**.

About file system storage

A file system represents a 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.



The following table describes the components of file system storage:

Component	Description
NAS server	A file server configured with its network interfaces and other settings exclusively exporting the set of specified file systems through mount points called shares. Client systems connect to a NAS server on the storage system to get access to the file system shares. A NAS server can have more than one file system, but each file system can only be associated with one NAS server.
File system	A manageable container for file-based storage that is associated with the following properties: ● A specific quantity of storage. ● A particular file access protocol (SMB, NFS, or multiprotocol). ● One or more shares (through which network hosts or users can access shared files or folders).
Share or export	A mountable access point to file system storage that network users and hosts can use for file-based storage.
Windows users or Linux/UNIX hosts	A user, host, netgroup, or subnet that has access to the share and can mount or map the resource. For Windows file systems, access to the share is based on share permissions and ACLs that assign privileges

Component	Description
	to objects defined in Active Directory. For Linux/UNIX file systems, access is permitted based on NFS access settings.

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 to configure access for individual Linux/UNIX hosts or IP address 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.

NAS servers

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 files 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.

NOTE: 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 file system for NFS exports

You can create a file system for NFS exports.

Make sure that there is a NAS server that is configured to support the NFS protocol.

1. Select **File** > **File Systems**.
2. Click **Create**.
   The **Create File System** wizard launches.
3. Select an NFS enabled NAS server for the file system.
4. 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 1.5GB reserved for metadata upon creation. For example, after creating a 100GB thin file system, the system immediately shows 1.5GB used. When the file system is mounted to a host, it shows 98.5GB of usable capacity.

   This is because the metadata space is reserved from the usable file system capacity.

5. Configure the initial export for the file system.

   NOTE: You can add NFS exports to the file system at later time.

6. Configure security, access permissions, and host access for the system.

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: • **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 for 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.

Option	Description
Local path	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. • Each NFS share must have a unique local path. PoweFlex 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 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 Manager and set access permissions accordingly.
Export path	The path used by the host to connect to the export. PowerFlex 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.

7. 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.
8. 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.

Create a file system for SMB shares

A file system must be created on the NAS server before you can create an SMB share.

Make sure that there is a NAS server that is configured to support the SMB protocol.

1. Select **File** > **File Systems** and click **Create**.
2. Continue to work through 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: • **Sync Writes Enabled** • **Oplocks Enabled** • **Notify on Write Enabled** • **Notify on Access Enabled**
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.

Option	Description
	NOTE: All thin file systems, regardless of size, have 1.5GB reserved for metadata upon creation. For example, after creating a 100GB thin file system, immediately shows 1.5GB used. When the file system is mounted to a host, it shows 98.5GB 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. **NOTE:** PowerFlex supports snapshots for file storage protection. Replication protection is not supported for file systems. If a protection policy is set for both replication and snapshot protections, PowerFlex implements the snapshot policy on the file system, and ignores the replication policy for the file system.
Summary	Review the summary. Go back to make necessary updates.

3. 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

You can change file system configuration settings, modify the file system properties, delete the file system, and perform additional actions on a file system.

1. Go to the **File** > **File systems** page.
2. Click on a file system in the list to make changes to the file system configuration settings.
3. Click the checkbox next to the name of the file system and click:

Option	Description
Modify	To modify the file system name, description, or size.
More Actions	To perform one of the following operations: • Refresh quotas. • Remove the file system from the NAS server. This option is not available if there are NFS exports or SMB shares on the file system.

Create an SMB share

You can create an SMB share on a file system that has been created with an SMB-enabled NAS server.

1. Select **File** > **SMB Shares**.
2. Click **+ Create SMB Share** and continue to 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 local path: • 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

Option	Description
	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. PowerFlex Manager 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 a network host.
Advanced SMB properties	Enable one or more of the Advanced SMB settings. ● Continuous availability ● Protocol encryption ● Access-based enumeration ● Branch cache enabled Decide which objects are available when the share is offline.

3. Click **Next**.

Once you create a share, you can modify the share from PowerFlex Manager or using the Microsoft Management Console.

To modify the share from PowerFlex Manager, select the share from the list on the **SMB Share** page, and click **Modify**.

Create an NFS export

You can create an NFS export on a file system has been created with an NFS-enabled NAS server.

1. Select the **File** > **NFS Exports** tab.
2. Click **+ Create NFS Export**.
   The **Create NFS Export** wizard launches.
3. Enter the requested information while noting the following:
   - Snapshots must have been created before creating the NFS export.
   - **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. Once you approve the settings, click **Create NFS Export**.
   The NFS Export displays on the **NFS Export** page.

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.

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.

Configure at least one NAS server before you attempt to create a global namespace.

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.
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

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.

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.

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.

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.

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.

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.

More about file systems

You can create, view, access, and manage file systems from the **File** > **File Systems** page.

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. If you are creating a file system with NFS exports, the NAS server must support the NFS protocol. If you are creating a file system with SMB shares, the NAS server must support the SMB 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.

Advanced settings for file systems that support SMB

These advanced settings can be configured for a file system that will be used for SMB shares.

Setting	Description
Sync Writes Enabled	When you enable the synchronous writes option for a Windows (SMB) or multiprotocol file system, the storage system performs immediate synchronous writes for storage operations, regardless of how the SMB protocol performs write operations. Enabling synchronous writes operations enables 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. This option is disabled by default. **NOTE:** The synchronous writes option can have a significant impact on performance. It is not recommended unless you intend to use Windows file systems to provide storage for database applications.
Oplocks Enabled	(Enabled by default) Opportunistic file locks (oplocks, also known as Level 1 opslock) enable 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. This is enabled by default for Windows (SMB) and multiprotocol file systems. 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, which informs a client that multiple clients are 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, which 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, which 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.
Notify on Write Enabled	Enable notification when a file system is written to. This option is disabled by default.
Notify on Access Enabled	Enable notification when a file system is accessed. This option is disabled by default.

Settings for file systems that support NFS

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:

- **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 for user authentication (krb5i/krb5p).
- **Kerberos with Encryption** to allow only Kerberos with encryption security for user authentication (krb5p).

Access setting	Description
No Access	No access permitted to the storage resource or share.
Read-only	Hosts have permission to view the contents of the storage resource or share, but not to write to it.
Read/Write	Hosts have permission to read and write to the NFS datastore or share. **NOTE:** ESXI hosts must have **Read//Write** access in order to mount an NFS datastore using NFSv4 with **Kerberos NFS owner** authentication.
Read/Write, allow Root	Hosts have permission to read and write to the storage resource or share, and to grant revoke access permissions (for example, permission to read, modify and execute specific files and directories) for other login accounts that access the storage. The root of the NFS client has root access to the share. **NOTE:** Unless the hosts are part of a supported cluster configuration, a void granting Read/Write access to more than one host. **NOTE:** VMware ESXi hosts must have **Read/Write, allow Root** access in order to mount an NFS datastore using NFSv4 with NFS Owner:root authentication.
Read-only, allow Root (NFS Exports)	Hosts have permission to view the contents of the share, but not to write to it. The root of the NFS client has root access to the share.

Advanced properties for SMB shares

A file system must be configured to support SMB protocol before you can create a share.

Option	Description
Continuous Availability	Gives host applications transparent, continuous access to a share following a failover of the NAS server on the system (with the NAS server internal state saved or restored during the failover process). **NOTE:** Enable continuous availability for a share only when you want to use Microsoft Server Message Block (SMB) 3.0 protocol clients with the specific share.
Protocol Encryption	Enables SMB encryption of the network traffic through the share. SMB encryption is supported by SMB 3.0 clients and above. By default, access is denied if an SMB 2 client attempts to access a share with protocol encryption enabled. You can control this by configuring the RejectUnencryptedAccess registry key on the NAS Server. 1 (default) rejects non-encrypted access and 0 allows clients that do not support encryption to access the file system without encryption.
Access-Based Enumeration	Filters the list of available files and directories on the share to include only those to which the requesting user has read access. **NOTE:** Administrators can always list all files.
Branch Cache Enabled	Copies content from the share and caches it at branch offices. This allows client computers at branch offices to access the content locally rather than over the WAN. Branch Cache is managed from Microsoft hosts.

Option	Description
Offline Availability	Configures the client-side caching of offline files: • **Manual**: Files are cached and available offline only when caching is explicitly requested. • **Programs and files opened by users**: All files that clients open from the share are automatically cached and available offline. Clients open these files from the share when they are connected to it. This option is recommended for files with shared work. • **Programs and files opened by users, optimize for performance**: All files that clients open from the share are automatically cached and available offline. Clients open these files from the share's local cache, if possible, even when they are connected to the network. This option is recommended for executable programs. • **None**: Client-side caching of offline files is not configured.

SMB and NFS configuration details

The following table provides some details you will need when creating files systems, SMB shares, or NFS exports.

Option	Description
Name	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. 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.
Local path	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. **SMB shares** • 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 Unisphere. You can also create and manage SMB shares from the Microsoft Management Console. **NFS exports** • 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	The path used by the host to connect to the share or export. PowerFlex Manager 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.

File system quotas

You can set quotas on a file system from the **File** > **File System** > **[file system]** > **Quotas** card.

You can track and limit drive space consumption by configuring quotas for file systems at the file system or directory level. 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.

NOTE: You cannot create quotas for read-only file systems.

Quotas are supported on SMB, NFS, FTP, NDMP, and multiprotocol file systems.

You can set the following types of quotas for 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 quota	Tree quotas limit the total amount of storage that is consumed on a specific directory tree. You can use tree quotas to: • 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). **NOTE:** If you change the limits for a tree quota, the changes take effect immediately without disrupting file system operations.
User quota on a quota tree	Limits the amount of storage that is consumed by an individual user storing data on the quota tree.

Quota limits

To track space consumption without setting limits, set **Soft Limit** and **Hard Limit** to 0, which indicates no limit.

Type	Descriptions
Hard	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.

Quota grace period

The quota 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 7 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.

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.

Each protection policy can include up to 16 snapshot rules. A rule can be included in multiple policies.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

1. Click **File** > **File Protection** > **Protection Policies**.
2. Select the check box next to the relevant policy and click **Delete**.

Modify a snapshot rule

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.

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.

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.

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.

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.

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.

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.

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**.

8

Protecting a block storage environment

Use local and remote protection features to protect your block storage.

Snapshots

A snapshot is a copy of a volume at a specific point in time. With snapshots, you can overwrite the contents of the volume, map to a host, and set bandwidth and IOPS limits.

Create snapshots

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

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.

1. On the menu bar, click **Protection** > **Snapshots**.
2. In the list, select the relevant volumes, and click **More** > **Create Snapshot**.
3. In the **Create snapshot of volume** dialog box, enter the name of the snapshot. You can accept the default name, or create a 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 Snapshot**.
6. Verify that the operation has finished and was successful, and click **Dismiss**.

Overwrite volume content from a snapshot

The contents of a volume can be overwritten with the content from another volume, using a snapshot.

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

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.

1. On the menu bar, click **Protection** > **Snapshots**.
2. In the list of snapshots, select the snapshot to be overwritten, and then click **More Actions** > **Overwrite Content**.

The **Target Volume** tab in the **Overwrite Content of Volume** dialog box displays the details of the volume that will be overwritten.

3. Click **Next**.
4. In the **Select Source Volume** tab, do the following:
   a. Select the source volume from which to copy content.
   b. Click **Time Frame**, and then 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 then click **Overwrite Content**.
6. Verify that the operation has finished and was successful, and click **Dismiss**.

Set bandwidth and IOPS limits for snapshots

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

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

1. On the menu bar, click **Protection** > **Snapshots**.
2. In the list of snapshots, select the relevant snapshot, 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 then click **Dismiss**.

Lock and unlock snapshots

You can lock auto snapshots (snapshots created automatically by a snapshot policy) so that they are not removed by the auto removal process. You can unlock the snapshots later, so that they can be automatically removed.

NOTE: If a snapshot policy is displayed for the snapshot in the **Snapshot Policy** column of the snapshots list, it is an auto snapshot.

1. On the menu bar, click **Protection** > **Snapshots**.
2. In the list of snapshots, select the desired snapshot, and then click **More Actions** > **Lock Snapshot/Unlock Snapshot**.
3. In the **Lock/Unlock snapshot** dialog box, click **Apply**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Delete snapshots

Remove snapshots of volumes from PowerFlex.

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

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

CAUTION: Removing a snapshot erases all the data in the corresponding snapshot.

1. On the menu bar, click **Protection** > **Snapshots**.
2. In the list of snapshots, select the desired snapshot, and then click **More Actions** > **Delete**.
3. In the **Delete Volume** dialog box, select an option:
   - Delete volume
   - Delete volume with all its snapshots

4. Click **Delete**.
5. In the next dialog box confirming the snapshots to remove, verify that you are deleting the correct snapshots, and click **Delete**.
6. Verify that the operation has finished and was successful, and click **Dismiss**.

Map snapshots

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

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

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

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, and you cannot map the volume on the target of a peer system if it is connected to an RCG..

1. On the menu bar, click **Protection** > **Snapshots**.
2. In the list of snapshots, select one or more snapshots, and then click **Mapping** > **Map**.
3. In the **Map Volume** dialog box, select one or more hosts to which you want to map the snapshots.
4. Click **Map**, and click **Apply**.
5. Verify that the operation has finished and was successful, and then click **Dismiss**.

Unmap snapshots

Unmap one or more snapshot volumes from hosts.

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

Increase the size of a snapshot

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

1. On the menu bar, click **Protection** > **Snapshots**.
2. In the list of snapshots, select the snapshot, and then 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**.

Migrate a snapshot vTree

You can migrate a volume tree (vTree) for a snapshot to a different storage pool. Volumes undergoing migration remain available for I/O.

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.

1. On the menu bar, click **Protection** > **Snapshots**.
2. In the list of snapshots, select the desired snapshot.
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.
   The storage pool's free capacity is displayed. Ensure that you select a storage pool with enough capacity for the vTree size.
7. Optionally, select one or more 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.
Enable compression	A compression algorithm is applied to the data.
Convert vTree from...	Convert a thin-provisioned vTree to thick-provisioned, or a thick-provisioned vTree to thin-provisioned 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 page, click the **Running Storage Jobs** icon, and check the progress of the migration.
10. Verify that the operation has finished and was successful, and click **Dismiss**.

Pause snapshot vTree migration

PowerFlex allows you to pause a vTree migration at any time.

You can pause vTree migration using the following methods:

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

  CAUTION: This method carries a potential risk of data loss.

1. On the menu bar, click **Protection** > **Snapshots**.
2. In the list of snapshots, select the desired snapshot.
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 desired option, and then click **Pause Migration**.
   If you selected to pause the migration gracefully, the migration state is displayed. Once paused, you can choose to roll back the vTree migration or resume the vTree migration from the **VTree** menu.

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

Roll back snapshot vTree migration

When a snapshot volume tree (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.

1. On the menu bar, click **Protection** > **Snapshots**.
2. In the snapshots list, select the desired snapshot.
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 **Rollback Migration**.
6. In the **Roll back VTree Migration** dialog box, verify the source and target for the rollback, and then click **Rollback Migration**.
7. Verify that the operation has finished and was successful, and click **Dismiss**.

Set snapshot vTree migration priority

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

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

1. On the menu bar, click **Protection** > **Snapshots**.
2. In the list of snapshots, select the desired snapshot.
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 **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 then click **Set Priority**.
7. Verify that the operation has finished and was successful, and click **Dismiss**.

Snapshot policies

Snapshot policies enable you to define policies for the number of snapshots that PowerFlex takes of one or more defined volumes at a given time.

Snapshots are taken according to the defined rules. You can define the time interval between two rounds of snapshots, as well as the number of snapshots to retain, in a multi-level structure. For example, take snapshots every x minutes/hours/days/weeks. You can define a maximum of six levels, with the first level having the most frequent snapshots.

For example:

Rule: Take snapshots every 60 minutes

Retention Levels:

- 24 snapshots
- 7 snapshots
- 4 snapshots

After defining the parameters, select the source volume to add to the snapshot policy. You can add multiple source volumes to a snapshot policy, but only a single policy per source volume is allowed. Only one volume per vTree may be used as a source volume of a policy (any policy).

When you remove the source volume from the policy, you must choose how to handle snapshots. Snapshots created by the policy are referred to as auto snapshots. This is indicated if a snapshot policy is displayed for the snapshot.

- If the source volume has auto snapshots, you cannot unassign the source volume from the snapshot policy. You can remove auto snapshots from **Snapshots**.
- If the source volume has auto snapshots but none of them are locked, you are prompted to confirm that you would like to delete all auto snapshots. If any of the auto snapshots are locked, the locked auto snapshots are just detached from the snapshot policy, but not deleted. You can manually delete auto snapshots. It doesn't matter if the auto snapshot is locked or not, you can still delete.

Create a snapshot policy

Create snapshot policies with a maximum of six retention rules that each specify a retention period and number of snapshots to retain, and then add source volumes to the policy.

1. On the menu bar, click **Protection** > **Snapshot Policies**.
2. Click **Create Snapshot Policy**.
3. In the **Create Snapshot Policy** dialog box, assign the policy a name and the time interval between snapshots.
4. Create retention rules:
   a. In the **Retention** field, add the number of snapshots to retain.
   A retention period is created for the specified number of snapshots times the snapshot interval.
   b. Optionally, to create an additional retention rule, click **Add Retention** and repeat the previous step. Each rule is based on the specified number of snapshots times the previous retention period.

   Up to six retention rules can be created.
5. Optionally, clear the **Read Only** check box to cancel read-only access. This check box is selected by default.
6. Optionally, select the **Secured** check box to prevent the snapshots created by the policy from being modified or deleted before the end of the expiration date.
7. Click **Create** or **Create and Activate** to add the snapshot policy to PowerFlex.

   If created, but not activated, the snapshot policy shall be paused.
8. In the **Snapshot Policy was successfully added** dialog box, click **Assign volume to snapshot policy**.
9. In the **Select volumes you wish to assign to the policy** window, select one or more volumes, and click **Assign Policy**.
10. Verify that the operation has finished successfully, and click **Dismiss**.

Remove snapshot policy

Remove a snapshot policy to stop PowerFlex from automatically creating snapshots for the specified volumes. You cannot remove snapshot policies that are secured.

1. On the menu bar, click **Protection** > **Snapshot Policies**.
2. In the list of snapshot policies, select the relevant policy.
3. Ensure that all source volumes are unassigned from the selected snapshot policy, and click **More Actions** > **Delete**.
4. In the **Remove Snapshot Policy** dialog box, click **Remove**.
5. Verify that the operation has finished successfully, and click **Dismiss**.

Modify snapshot policy

PowerFlex allows you to modify the parameters of snapshot policies, when required.

1. On the menu bar, click **Protection** > **Snapshot Policies**.
2. In the list of snapshot policies, select the relevant policy, and then click **Modify** > **Modify Policy**.
3. In the **Modify Snapshot Policy** dialog box, change the desired parameters:
   a. In the **Retention** field, set the number of snapshots to retain.
   A retention period is created for the specified number of snapshots times the snapshot interval.
   b. Optionally, to create an additional retention rule, click **Add Retention** and repeat the previous step. Each rule is based on the specified number of snapshots times the previous retention period.

   Up to six retention rules can be created.
   c. Optionally, clear the **Read Only** check box to cancel read-only access. This check box is selected by default.
   d. Optionally, select the **Secured** check box to prevent the snapshots created by the policy from being modified or deleted before the end of the expiration date.
4. Click **Modify**.
5. Verify that the operation has finished successfully, and click **Dismiss**.

Rename snapshot policy

1. On the menu bar, click **Protection** > **Snapshot Policies**.
2. In the list of snapshot policies, select the relevant policy, and click **Modify** > **Rename**.
3. In the **Rename Snapshot Policy** dialog box, enter a new name and click **Apply**.
4. Verify that the operation has finished successfully, and click **Dismiss**.

Activate snapshot policy

1. On the menu bar, click **Protection** > **Snapshot Policies**.
2. In the list of snapshot policies, select the relevant policy, and click **More Actions** > **Activate**.
3. In the **Activate Snapshot Policy** dialog box, click **Activate**.
4. Verify in the **State** column that the snapshot policy is active, and click **Dismiss**.

Pause snapshot policy

1. On the menu bar, click **Protection** > **Snapshot Policies**.
2. In the list of snapshot policies, select the relevant policy, and click **More Actions** > **Pause**.
3. In the **Pause Snapshot Policy** dialog box, click **Pause**.
4. Verify in the **State** column that the snapshot policy is in paused state, and click **Dismiss**.

Assign volumes or snapshots to a snapshot policy

1. On the menu bar, click **Protection** > **Snapshot Policies**.
2. In the list of snapshot policies, select the relevant policy, and click **More Actions** > **Assign Volumes**.
3. In the **Assign Voumes to Snapshot Policy** dialog box, select the volumes or snapshots that you want to assign to the policy, and click **Assign Policy**.

Unassign a volume from a snapshot policy

When you unassign volumes from a snapshot policy, the source volume is detached from the snapshot policy and all (unlocked) auto snapshots of the source volume are deleted.

1. On the menu bar, click **Protection** > **Snapshot Policies**.
2. In the list of snapshot policies, select the relevant policy, and click **More Actions** > **Unassign Volumes**.
3. In the **Unassign Volumes from Snapshot Policy** dialog box:
   a. To detach the snapshot policy from a volume, select the check box of the relevant volume.
   b. Optionally, to delete auto snapshots of the selected volume, select the **Delete related snapshots** check box.
4. Click **Unassign Policy**.
5. In the **Unassign Volumes From Snapshot Policy** dialog box, click **Yes**.

   NOTE: If the auto snapshots are locked, they are detached from the snapshot policy, but not deleted. To remove the locked auto snapshots from the system, manually remove the snapshots by navigating to **Protection** > **Snapshots**. Select the desired snapshots, and click **Delete**.

Remote protection

PowerFlex enables native asynchronous replication for PowerFlex storage-only and hyperconvered configurations. Remote protection is an optional feature which ensures data protection of the PowerFlex environment. It creates a remote copy of one volume from one cluster to another.

Replication is used to quickly and easily recover from a physical or logical disaster, to migrate data, to test data at a remote site, or to offload backup. The PowerFlex implementation is designed to allow a sub-minute RPO reducing the data-loss to minimal if there is disaster recovery. As with all other PowerFlex data services, replication is elastic, can scale online by adding or removing nodes, is flexible, and easy to manage. It enables instant test and failover operations.

When replicating between systems it is recommended to have the same storage pool type, disk capacity and type, and performance capabilities between the local and remote sites. While replication between medium granularity (MG) to fine granularity (FG) storage pools is fully supported, account for the performance characteristics of each storage pool. PowerFlex does not support replication of volumes mapped to NVMe hosts.

The following workflow summarizes setup of remote replication. See specific procedures for detailed steps.

1. Install the remote (target) PowerFlex system.
2. Extract a certificate on each PowerFlex system and copy it to its peer system.
3. Configure journal capacity. Journal capacity is a percentage of the total storage capacity. There are several factors that should be considered when defining it:
   - Journal capacity must be allocated to be able to add SDRs to the system.
   - Before configuring journal capacity, ensure that there is enough space in the storage pool.
   - The journal capacity depends on the change rate and Recovery Point Objective (RPO). Data writes are accumulated in the journal until half the RPO time has been reached, to ensure that data is not lost and a consistent copy is maintained between the volumes.
   - When the total storage capacity in the system increases, a small percentage is needed for the journal capacity.
   - As application workload increases, more journal capacity must be added, accordingly.
4. Ensure that SDRs are installed and added to the source and peer systems.
   - The SDR component is typically installed during installation of PowerFlex. It manages replication activity within the system, and between the source and target. Dell recommends installation of at least three SDRs per system, for failure or backup purposes. Within the system, the SDR channels the I/O writes from the host to the source journal. Simultaneously, it also sends the data to the SDS to be logged. As data accumulates in the source journal, the system decides when to close the journal (this is usually at half the RPO time) in order to be ready to transfer the data to the target journal. At the target site, the SDR is also responsible for applying the data from the target journal to the target volume.
5. Define peer (target) systems from the source side.
6. Create and activate replication consistency groups (RCGs).
   - An RCG is a set of volumes which must maintain a consistent copy on the remote (target) site where write order is maintained between volumes. This pair shares the same attributes.
   - The volumes to be replicated must be the same size on source and target systems. If the network is up, the systems should be connected.

Extract and upload certificates

On both source and target replication systems, extract the root certificate and copy it to the peer system. This procedure is required to allow communication and data transfer between the systems.

Ensure that you have admin user credentials for command line access to both PowerFlex systems.

1. In command line, log in to the source system:

   ```
   scli --login --username <M&O UI user> --password <M&O UI password> --
   management_system_ip <M&O UI IP>
   ```

2. Extract the root certificate:

   ```
   scli --extract_root_ca --certificate_file <FILE_PATH>
   ```

   where *<FILE_PATH>* is the location where the certificate will be saved, and the file name. For example: `/opt/source_sys.crt`

3. Copy the certificate file to the target system.

4. On the target system, perform steps 1 and 2.
5. Copy the target system's certificate file to the source system.
6. On the source system, add the certificate for the target system:

   ```
   scli --add_trusted_ca <PATH_TO_LOCAL_COPY_OF_TARGET_CERT>
   ```

   where *<PATH_TO_LOCAL_COPY_OF_TARGET_CERT>* is the copy of the target system's certificate that you copied to the source system.
7. On the target system, add the source system's certificate:

   ```
   scli --add_trusted_ca <PATH_TO_LOCAL_COPY_OF_SOURCE_CERT>
   ```

   where *<PATH_TO_LOCAL_COPY_OF_SOURCE_CERT>* is the copy of the source system's certificate that you copied to the target system.

Journal capacity

You should consider several factors when allocating journal capacity.

Journal capacity is defined as a percentage of the total storage capacity in the storage pool and must equal at least 28 GB per SDR. In general, journal capacity should be at least 5% of replicated usable capacity in the protection domain, including volumes used as source and targets. It is important to assign enough storage capacity for the replication journal.

The amount of capacity needed for the journal is based on the following factors:

- Minimal requirements—108 GB multiplied by the number of SDR sessions. The number of SDR sessions is equal to the number of SDRs plus one. The extra SDR session is to ensure that a new session can be allocated for an SDR during a system upgrade.
- The capacity needed to sustain an outage—application WAN bandwidth multiplied by the planned WAN outage. In general, journal capacity in the protection domain should be at least 5% of the application pool. If the application has a heavy I/O load, larger capacity should be used. Similarly, if a long outage is expected, a larger capacity should be allocated. If there are replicated volumes in more than one storage pool in the protection domain, this calculation should be repeated for each storage pool, and the allocated journal capacity in the protection domain must at least equal the sum of the size per application pool.

Use the following steps to calculate exactly how much journal capacity to allocate:

1. Select the storage pools from which to allocate the journal capacity. The journal is shared between all of the replicated RCGs in the protection domain. Journal capacity should be allocated from storage pools as fast as (or faster than) the storage pool of the fastest replicated application in the protection domain. It should use the same drive technology and about the same drive count and distribution in nodes.
2. Consider the minimal requirements needed (28 GB multiplied by the number of SDR sessions) and the capacity needed to sustain an outage. Journal capacity will be at least the maximum of these two factors.
3. Take into account the expected outage time. The minimal outage allowance is one hour, but at least three hours are recommended.
4. Calculate the journal capacity needed per application: maximal application throughput x maximum outage interval.
5. Since journal capacity is defined as a percentage of storage pool capacity, calculate the percentage of capacity based on the previously calculated needs.

For example:

- An application generates 1 GB/s of writes.
- The maximal supported outage is 3 hours (3 hours x 3600 seconds = 10800 seconds).
- The journal capacity needed for this application is 1 GB/s x 10800 s = ~10.547 TB.
- Since the journal capacity is expressed as a percentage of the storage pool capacity, divide the 10.547 TB by the size of the storage pool, which is 200 TB: 100 x 10.547 TB/200 TB = 5.27%. Round this up to 6%.
- Repeat this for each application being replicated.

When a protection domain has several storage pools and several replicated applications, the journal capacity should be calculated as in the example above, and the capacity can be divided among all the storage pools (provided they are fast enough). For higher availability, the journal capacity should be allocated from multiple storage pools.

NOTE: When storage pool capacity is critical, capacity cannot be allocated for new volumes or for expanding existing volumes. This behavior must be taken into account when planning the capacity available for journal usage. The volume

usage must leave enough capacity available in the storage pool to allow provisioning of journal volumes. The plan should account for the storage pool staying below critical capacity even when the journal capacity is almost fully utilized.

It is important to note that since journal capacity is defined as a percentage of the total storage capacity in the storage pool, increasing the total storage capacity by adding devices will increase the journal capacity. Similarly, if you decrease the total storage capacity by removing devices from the storage pool, the journal capacity will automatically decrease.

Add journal capacity

Set the percentage of storage pool capacity that is allocated for journal capacity.

1. On the menu bar, click **Protection** > **Journal Capacity**.
2. Click **Add Journal Capacity**.
3. In the **Add Journal Capacity** dialog box, search for, and select the required storage pool.
4. Enter a percentage for the journal capacity.
5. Click **Add**.
6. Verify that the operation has finished and was successful, and click **Dismiss**.

Modify journal capacity

Reset the journal capacity according to the updated storage device size.

1. On the menu bar, click **Protection** > **Journal Capacity**.
2. In the list of storage pools, select the required storage pool and click **Modify**.
3. In the **Storage Pool** dialog box, enter the updated percentage for journal capacity.
4. Click **Modify** to update the journal capacity.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Delete journal capacity

Delete journal capacity from a storage pool.

1. On the menu bar, click **Protection** > **Journal Capacity**.
2. Select the required storage pool from the list, and click **Delete**.
3. In the **Delete Journal Capacity** dialog box, click **Delete**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Add a peer system

On the source system, add the connection information of the target system (remote site) to enable replication between the peer systems.

Obtain the system ID of both source and target systems, using command line. The system ID is displayed immediately after login. You can also obtain it by running the command `scli --query_all`.

1. On the source system, on the menu bar, click **Protection** > **Peer Systems**.
2. Click **Add Peer System**.
3. In the **Add Peer System** dialog box, enter the connection information of the peer system:
   a. Enter the peer system's name.
   b. Enter the system ID of the remote site.
   c. Accept the default, or enter the port number that will be used to connect the systems.
   d. Enter the MDM IP address of the remote site.

      Either enter the remote system's virtual IP address, or enter both primary and secondary MDM IP addresses, using the **Add IP** option.
   e. Click **Add Peer** to initiate a connection with the peer system.

   After adding peer system at source and before adding peer system at the target, the peer state is **Not Authorized**.
4. Repeat steps 1–3 on the target system.

After the peer system has been set up on both systems, the state of the peers should show that they are connected.

NOTE: If connection is not successful, verify that both source and target systems have a copy of their peer's certificate.

Restart the replication cluster

This task describes how to restart the nodes in the replication cluster.

Inactivate the protection domain first on the source and then on the target system.

In case of 2-way replication, inactivate the protection domains in any order. Ignore error messages that appear in the active protection domain. To avoid lengthy synchronization times or running out of journal capacity, it is advisable to activate the replication cluster quickly.

1. Shut down all nodes within the replication cluster.
2. Power on all nodes within the replication cluster.
3. Activate the protection domain first on the target and then on the source system.
4. Validate that the RCG in the replication cluster returns to a working state.

SDRs

Storage Data Replicators (SDRs) are responsible for processing all I/Os of replication volumes.

All application I/Os of replicated volumes are processed by the source SDRs. At the source, application I/Os are sent by the SDC to the SDR. The I/Os are sent to the target SDRs and stored in their journals. The target SDRs' journals apply the I/Os to the target volumes. A minimum of two SDRs are deployed at both the source and target systems to maintain high availability. If one SDR fails, the MDM directs the SDC to send the I/Os to an available SDR.

Add SDR

Add an additional SDR to an existing PowerFlex system, or add back a new SDR if a previously existing SDR was removed. A minimum of two SDRs are required on each replication system. Each SDR must be configured with one or more IP addresses and roles.

The SDR communicates with several components, including: SDC (application), SDS (storage) and remote SDR (external). When an IP address is added to an SDR, the role or roles of the IP address must be defined. The IP address role determines the component with which that IP address communicates. For example, the application role means that the associated IP address is used for SDR-SDC communication. By default, all the roles are selected for an IP address.

SDR components must be deployed as resources before you can add them using this procedure.

1. On the menu bar, click **Protection** > **SDRs**.
2. Click **Add SDR**.
3. In the **Add SDR** dialog box, enter the connection information of the SDR:
   a. Enter the SDR name.
   b. If necessary, modify the SDR port number.
   c. Select the relevant protection domain.
   d. Enter the IP address of the SDR.
   e. Select one or more roles, for example, default: all roles are selected.
   f. If the SDR has more than one IP address, click **Add IP** to add more IP addresses and their roles.
   g. Click **Add SDR** to initiate a connection with the peer system.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Modify IP address role

Update the role of an IP address configured on the SDR.

The SDR communicates with several components, including: SDC (application), SDS (storage) and remote SDR (external). When an IP address is added to an SDR, the role or roles of the IP address must be defined. The IP address role determines the component with which that IP address communicates. For example, the application role means that the associated IP address is used for SDR-SDC communication. The default setting is all roles.

1. On the menu bar, click **Protection** > **SDRs**.
2. In the list of SDRs, select the relevant SDR, and click **Modify** > **Modify IP Role**
3. In the **Modify IPs Role** dialog box, select or clear the desired roles for the IP address.
4. Click **Apply**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Modify an SDR performance profile

The SDR performance profile is set to high by default, but can be modified. Ensure that your system's architecture is equipped to handle enhanced system performance of SDR activities.

1. On the menu bar, click **Protection** > **SDRs**.
2. In the list of SDRs, select the relevant SDR, and click **Modify** > **Modify Performance Profile**.
3. In the **Modify Performance Profile SDR** dialog box, click either **High** or **Compact**.
4. Click **Apply**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Enter SDR into maintenance mode

Place the SDR in maintenance mode prior to performing maintenance on the SDR.

There must be at least two SDRs installed on each system.

When maintenance mode is activated, the MDM changes the mapping and distributes the I/Os to the remaining SDRs.

1. On the menu bar, click **Protection** > **SDRs**.
2. In the list of SDRs, select the desired SDR, and click **More Actions** > **Enter Maintenance Mode**.
3. In the **Enter SDR to Maintenance Mode** dialog box, click **Enter Maintenance Mode**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Exit SDR from maintenance mode

Remove the SDR from maintenance mode. This returns the SDR to regular operation.

When maintenance mode is deactivated, the MDM changes the mapping and resumes distribution of the I/Os to the SDR.

1. On the menu bar, click **Protection** > **SDRs**.
2. In the list of SDRs, select the relevant SDR check box, and click **More Actions** > **Exit Maintenance Mode**.
3. In the **Exit SDR from Maintenance Mode** dialog box, click **Exit Maintenance Mode**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Replication consistency group

Replication Consistency Group (RCG) is an entity that includes a set of consistent volume pairs. The volume on the source from a single protection domain is replicated to a remote volume from a single protection domain on the target. This creates a consistent pair of volumes.

When replication is first activated for an RCG, the target volumes need to be synchronized with the source volumes. For each volume pair, the entire contents of each source volume are copied to the corresponding target volume. When there is more than one volume pair in the RCG, the order in which the volumes are synchronized is determined by the order in which the volume pairs were created. The initial synchronization occurs while all applications are running and performing I/O. Any writes to an area of the volume that has already been synchronized will be sent to the journal. Writes to an area of the volume that has not already been synchronized will be ignored, as the updated content will be copied over eventually as part of the synchronization.

The initial synchronization can also take place while the system is offline, however the application I/O must first be paused.

You can add and manage RCGs on both the source and target systems.

Replication direction and mapping

Use this table as a reference for replication direction and default access to volumes according to a subsequent RCG operation and action of the PowerFlex system.

The replication involves two peers, system A and system B. When the replication is set up, system A is set as source and system B is set as target. The following replication direction refers to the initial direction A->B and to changes to that direction.

Subsequent RCG operations	Possible actions	Replication direction/access	Access to volumes
Normal	Switchover/test failover/ failover Remove	A to B	Access to the volumes is allowed only through the source (system A)
After failover	Reverse/restore Remove	N/A - data is not replicated	By default access to the volume is allowed through the original target (system B). It is possible to enable access through the original source (system A).
After failover + reverse **NOTE:** Switchover and test failover are only possible after the peers are synchronized.	Switchover/test failover/ failover Remove	B to A	Access to the volumes is allowed only through the original target (system B)
After failover + restore **NOTE:** Switchover and test failover are only possible after the peers are synchronized.	Switchover/test failover/ failover Remove	A to B	Access to the volumes is allowed only through the source (system A)
After switchover	Switchover/test failover stop/failover Remove	B to A	Access to the volumes is allowed only through the original target (system B)
After test failover	Switchover/test failover/ failover Remove	A to B	Access to the volumes is allowed through both systems (system A and system B)

Create an RCG

Create a replication consistency group (RCG) and add it to the system. Replication occurs between volumes, and RCGs maintain consistency between volume pairs in an RCG.

- Volumes in an RCG pair must be exactly the same size.
- Protection domains must be configured on both source and target systems.

The recovery point objective (RPO) configured in RCGs defines the maximum amount of time during which data is lost. Dell recommends setting a low RPO to ensure that not much data is lost during a possible compromise of data transfer from source to target. If for example, if one minute is set as the RPO, you will not lose more than 30 seconds of data. Dell highly recommends that the RPO be low, because this ensures that minimal data is lost. There is no replication unless the source volume is consistent with the data from the target volume.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click **Add RCG**.
3. In the **Add RCG** wizard, enter the information for the RCG:

a. On the **Properties** page:
   - Enter the **RCG Name**.
   - Enter the number of **RPO** (recovery point objective) seconds or minutes. This is the amount of time of data loss is tolerated if replication between the systems is compromised.

     NOTE: It is recommended to enter the minimum amount of time the feature allows, which is 15 seconds.
   - Select the **Source Protection Domain**.
   - Select the **Target System**.
   - Select the **Target Protection Domain**.
   - Click **Next** .

b. On the **Provisioning Type** page:
   - If you have not defined volumes to receive replicated data in the target system, select **Auto Provisioning**.
   - If you have already defined volumes to receive replicated data in the target system, select **Manual Provisioning**.

c. For auto provisioning only, on the **Replication Pairs** page, perform the following:
   - Click the desired volume in the **Source** column.
   - Select a type: **Thick** or **Thin**.
   - Select a storage pool from the target system.
   - Click **Add Pair**. The volume pair is added.
   - Click **Next**.
   - On the **Map Volumes** page, select a volume on the target side.
   - Select a host to which to map the volume.
   - Click **Next**, and go to step 3(e).
   - Click **Next**.

d. For manual provisioning only, on the **Replication Pairs** page, perform the following:
   - Select the desired volume in the **Source** column, and then in the **Target** column, select the target volume (only volumes of the same size are displayed).
   - Click **Add Pair**. The volume pair is added.
   - Click **Next**.

e. On the **Summary** page, ensure that the correct source and volume pair are defined, and then click **Create and Activate** or **Create**.

   The **Create and Activate** option creates the RCG and starts replication. The **Create** option creates the RCG but does not activate it. You can activate it later from **Protection** > **RCGs** > **More Actions** > **Activate**.

4. Optionally, at the top right of the window, click the **Running Jobs** icon, and check the progress of the initial copy state.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Map RCG target volumes to hosts

Designate which hosts can access the RCG from the target volumes.

This option is only enabled from the target RCG.

1. On the menu bar, click **Protection** > **RCGs**.
2. In the **Map RCG Target Volume** dialog box, click the relevant RCG check box, and click **Mapping** > **Map**.
3. Select one or more volumes on the left and click **>>** to add them to the selection list on the right.

   Optionally, filter the list of the volumes by entering a search string in the **Filter** box.
4. Click **Next**.
5. Select the host(s) that you want to map to the selected volumes.

   Optionally, filter the list of the hosts by entering a search string in the **Filter** box.
6. Click **Next**.
7. Assign the **Access Mode** to the hosts that will be mapped to the target volumes.
   a. To assign the Read Only mode to a set of mappings, select the mappings and click **Read Access** at the top of the page.
   b. To assign the No Access mode to a set of mappings, select the mappings and click **No Access** at the top of the page.

   NOTE: **Read Access** mode applies to all platforms, except Windows clusters, which require the **No Access** mode.
8. Click **Finish**.

Unmap a host from RCG target volumes

Unmap a host from RCG target volumes.

This option is only enabled from the target RCG.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and click **Mapping** > **Unmap**.
3. In the **Unmap RCG** dialog box, select the relevant host check boxes to unmap them from the RCG volumes, and click **Unmap**.

Set the target to inconsistent mode

Set the target to inconsistent mode to pause the apply process from target journal to target volume until the source journal has completed sending data to the target journal. If there is no consistent image on the target journal, the system does not apply it.

NOTE: Dell recommends taking a snapshot of the target before setting the target to inconsistent mode. The snapshot can later be used for recovery purposes, using a consistent snapshot.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and click **Modify** > **Set Target to Inconsistent Mode**.
3. In the **Set Target to Inconsistent Mode RCG** dialog box, click **Apply**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Set the target to consistent mode

If the target is set to inconsistent mode, set it back to consistent mode. As data is transferred from source to target, the SDR verifies that the data in the journal is consistent with the data from the source. The SDR then sends an apply command to the journal to prompt the SDR to send data to the volume.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and click **Modify** > **Set Target to Consistent Mode**.
3. In the **Set Target to Consistent Mode RCG** dialog box, click **Apply**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Modify RPO

Update recovery point objective (RPO) time as required.

The Recovery Point Objective (RPO) defines the maximum amount of time during which data is lost. Dell recommends setting a low RPO to ensure that not much data is lost during a possible compromise of data transfer from source to target. If for example, if one minute is set as the RPO, you will not lose more than 30 seconds of data. Dell highly recommends that the RPO be low, because this ensures that minimal data is lost.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and click **Modify** > **Modify RPO**.
3. In the **Modify RPO for RCG** dialog box, modify the RPO time, and click **Apply**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Add a replication pair to an RCG

Add a replication pair to an existing replication consistency group (RCG).

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and then click **Modify** > **Add Pair**.
3. In the **Add Pairs** wizard, perform the following:
   a. On the **Provisioning Type** page:
      - If you have not defined volumes to receive replicated data in the target system, select **Auto Provisioning**.
      - If you have already defined volumes to receive replicated data in the target system, select **Manual Provisioning**.

b. For auto provisioning only, on the **Replication Pairs** page, perform the following:
   - Click the desired volume in the **Source** column.
   - Select a type: **Thick** or **Thin**.
   - Select a storage pool from the target system.
   - Click **Add Pair**. The volume pair is added.
   - Click **Next**.
   - On the **Map Volumes** page, select a volume on the target side.
   - Select a host to which to map the volume.
   - Click **Next**, and go to step 3d.
   - Click **Next**.

c. For manual provisioning only, on the **Replication Pairs** page, perform the following:
   - Select the desired volume in the **Source** column, and then in the **Target** column, select the target volume (only volumes of the same size are displayed).
   - Click **Add Pair**. The volume pair is added.
   - Click **Next**.

d. On the **Summary** page, ensure that the correct source and volume pair are defined, and click **Add Pairs**.

4. Optionally, at the top right of the window, click the **Running Jobs** icon, and check the progress of the initial copy state.
5. Verify that the operation has finished and was successful, and then click **Dismiss**.

Pause replication for an RCG

Pause replication for a replication consistency group (RCG). The pause command stops the transfer of data from the source to the target.

1. On the menu bar, click **Protection**.
2. Click the relevant RCG check box, and click **More Actions** > **Pause**.
3. In the **Pause RCG** dialog box, click one of the following options:
   - **Stop Data Transfer**—this option saves all the data in the source journal volume until there is no longer any available capacity
   - **Track Changes**—this option enables manual slim mode where only metadata in the source journal volumes is saved
4. Click **Pause**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Resume replication for an RCG

Resume replication for a replication consistency group (RCG). The resume command resumes the transfer of data from the source to the target.

1. On the menu bar, click **Protection**.
2. Click the relevant RCG check box, and click **More Actions** > **Resume**.
3. In the **Resume RCG** dialog box, click **Resume**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Create a snapshot of an RCG volume

Create a local snapshot of a volume that is in a replication consistency group (RCG). The latest image of the volume is used for the snapshot. When creating a snapshot, the RCG enters freeze mode.

1. On the menu bar, click **Protection** > **RCGs**.
2. In the right pane, select the relevant RCG check box, and click **More Actions** > **Create Snapshots**.
3. In the **Create Snapshots RCG** dialog box, click **Create Snapshots**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Add an RCG snapshot policy

Create snapshot policies with a maximum of six retention rules that each specify a retention period and number of snapshots to retain, and then add source volumes from the replication consistency group (RCG) to the policy.

1. On the menu bar, click **Protection** > **RCGs**.
2. From the RCGs list, select the desired RCG, and click **More Actions** > **Add Snapshot Policy**.
3. In the **Create Snapshot Policy** dialog box, assign the policy a name and the time interval between snapshots.
4. Create retention rules:
   a. In the **Retention Rules** area, add the number of snapshots to retain.
   A retention period is created for the specified number of snapshots times the snapshot interval.
   b. Optionally, to create an additional retention rule, click **Add Retention** and repeat the previous step. Each rule is based on the specified number of snapshots times the previous retention period.

   Up to six retention rules can be created.
5. Optionally, clear the **Read Only** check box to cancel read-only access. This check box is selected by default.
6. Optionally, select the **Secured** check box to prevent the snapshots created by the policy from being modified or deleted before the end of the expiration date.
7. Click **Create** or **Create and Activate** to add the snapshot policy to PowerFlex.
8. In the **Snapshot Policy was successfully added** dialog box, click **Assign volume to snapshot policy**.
9. In the **Select volumes you wish to assign to the policy** window, select the desired volumes, and then click **Assign Policy**.
10. Verify that the operation has finished successfully, and click **Dismiss**.

Perform a failover

If the system is not healthy, you can fail over the source role to the target system. When the source is compromised, data from the host stops sending I/Os to the source volume, replication is then stopped and the target system takes on the source role. The host on the target starts sending I/Os to the volume. The target takes on the role of source, and the source takes on the role of target.

Before performing a failover, stop the application and unmount the file systems at the source (if the source is available). Target volumes can only be mapped after performing a failover.

There are two options when choosing to fail over an RCG:

- Switchover—This option is a complete synchronization and failover between the source and the target. Application I/Os are stopped at the source, and then source and target volumes are synchronized. Access mode is changed of the target volumes to the target host, roles are switched, and finally, the access mode of the new source volumes is changed to read/write.
- Latest PIT—The system prevents any writes to the source volumes.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and then click **More Actions** > **Failover**.
3. In the **Failover RCG** dialog box, select one of the following options: **Switchover (Sync & Failover)** or **Latest PIT: (date & time)**.
4. Click **Apply Failover**.
5. In the **RCG Sync & Failover** dialog box, click **Proceed**.
6. Verify that the operation has finished and was successful, and click **Dismiss**.
7. From the upper right, click the **Running Jobs** icon and check the progress of the failover.

Reverse replication

When the RCG is in failover or switchover mode, you can reverse or restore the replication. Reversing replication changes the direction, so that the original target becomes the source. All data at the original source is overwritten by the data at the target side. This option may be selected from either source or target systems.

This option is available when RCG is in failover mode, or when the target system is not available. It is recommended to take a snapshot of the original source before reversing the replication for backup purposes.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and click **More Actions** > **Reverse**.

3. In the **Reverse Replication RCG** dialog box, click **Apply**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Restore replication

When the replication consistency group is in failover or switchover mode, you can reverse or restore the replication. Restoring replication maintains the replication direction from the original source and overwrites all data at the target side. This option may be selected from either source or target systems.

This option is available when an RCG is in failover mode, or when the target system is not available. Dell recommends taking a snapshot of the original destination for backup purposes, before restoring replication.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and click **More Actions** > **Restore**.
3. In the **Restore Replication RCG** dialog box, click **Apply**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Test Failover

Test failover of the latest copy of snapshots of source and target systems before performing a failover.

Replication is still running and is in a healthy state.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and then click **More Actions** > **Test Failover**.
3. In the **RCG Test Failover** dialog box, click **Start Test Failover**.
4. In the **RCG Test Failover using target volumes** dialog box, click **Proceed**.
5. Verify that the operation has finished and was successful, and click **Dismiss**.

Stop a failover test

Stop a failover test that is currently in progress.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and click **More** > **Test Failover Stop**.
3. Click **Approve**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Freeze an RCG

The freeze command stops the writing of data from the target journal to the target volume. This option is used while creating a snapshot or copy of the replicated volume.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and click **More Actions** > **Freeze Apply**.
3. Click **Freeze Apply**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Unfreeze an RCG

The unfreeze apply command resumes data transfer from the target journal to the target volume.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and click **More Actions** > **Unfreeze Apply**.
3. Click **Unfreeze Apply**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Activate an RCG

The activate command starts the initial copy process of replication for the replication consistency group (RCG), and activates replication of the RCG.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and click **More Actions** > **Activate**.
3. In the **Activate RCG** dialog box, click **Apply**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.
5. Click **View Details**. On the **Topology** tab, check that the replication status is Active.

Click **View Details**. On the **Topology** tab, the replication status should be **Active**.

Terminate replication in an RCG

The terminate command stops replication in the replication consistency group (RCG). The configuration of the RCG is maintained.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and click **More Actions** > **Terminate**.
3. In the **Terminate RCG** dialog box, click **Apply**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.
5. Click **View Details**. On the **Topology** tab, check that the replication status is **Inactive**.

Delete an RCG

Delete an RCG.

If you no longer require replication of the pairs in an RCG, you can delete it.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and click **More Actions** > **Delete**.
3. In the **Delete RCG** dialog box, verify that you have selected the desired RCG, and click **Delete**.
4. Verify that the operation has finished and was successful, and click **Dismiss**.

Pause creation of an initial copy

Pause replication of an initial copy from source to target.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and click **View Details**.
3. Click the **Volume Pairs** tab.
4. Select the volume pair for which you want to pause copying.
5. Click **Initial Copy** > **Pause Initial Copy**.
6. In the **Pause Initial Copy** dialog box, click **Pause Initial Copy**.
7. Verify that the operation has finished and was successful, and click **Dismiss**.

Resume creation of initial copy

Resume replication of an initial copy from source to target.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and click **View Details**.
3. Click the **Volume Pairs** tab.
4. Select the volume pair for which you want to resume copying.
5. Click **Initial Copy** > **Resume Initial Copy**.
6. In the **Resume Initial Copy** dialog box, click **Resume Initial Copy**.

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

Set copying priority

Set the priority order for copying volume pairs. Set the highest priority for pairs to be copied first, or set the lowest priority for pairs to be copied last.

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and click **View Details**.
3. Click the **Volume Pairs** tab.
4. Select the relevant volume pair.
5. Click **Initial Copy** > **Set Priority**.
6. In the **Set Priority for Pair** dialog box, select **Default** or **High** and click **Save**.
7. Verify that the operation has finished and was successful, and click **Dismiss**.

Unpair from RCG

Remove a pair from a replication consistency group (RCG).

1. On the menu bar, click **Protection** > **RCGs**.
2. Click the relevant RCG check box, and click **View Details**.
3. Click the **Volume Pairs** tab.
4. Select the volume pair that you want to remove from the RCG.
5. Click **Unpair**.
6. In the **Remove Pair from RCG** dialog box, click **Remove Pair**.
7. Verify that the operation has finished and was successful, and click **Dismiss**.

9

Performing lifecycle operations for a resource group

This section provides tasks for deploying resource groups and building templates.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

Deploying a resource configuration in a resource group

This section includes tasks for deploying and managing system resources in a resource group.

A resource group is a PowerFlex Manager object representing the infrastructure that is configured during a deployment. This object persists in PowerFlex Manager if the infrastructure is required. A resource group is viewed and interacted with to perform compliance, health, and life cycle management on the deployed infrastructure. PowerFlex Manager supports the deployment of three types of PowerFlex resource groups:

- Hyperconverged resource groups
- Storage-only resource groups
- Compute-only resource groups

NOTE: Standard users see only the details of the resource groups that they created or for which they have permission.

The **Resource Groups** page displays the resource groups that are in the following states in both **Tile** and **List** view.

State	Description
Healthy	The resource group is successfully deployed and is healthy.
Warning	One or more resources in the resource group requires corrective action.
Critical	The resource group is in a severely degraded or nonfunctional state and requires attention.
Pending	The deployment is scheduled for a later time or date.
In Progress	The resource group deployment is in progress, or has other actions currently in process, such as a node expansion or removal.
Cancelled	The resource group deployment has been stopped. You can update the resources or retry the deployment, if necessary.
Incomplete	The resource group is not fully functional because it has no volumes that are associated with it. Click **Add Resources** to add volumes.
Service Mode	The resource group is in service mode.
Lifecycle Mode	The resource group is in life-cycle mode. Resource groups in life cycle mode are enabled with health and compliance monitoring, and non-disruptive upgrade features only.
Managed Mode	The resource group is in managed mode. Resource groups in managed mode are enabled with health and compliance monitoring, non-disruptive update, automated resource addition, and automated resource replacement features.

On the **Resource Groups** page, you can:

- Click **Deploy New Resource Group** to deploy a new resource group.

NOTE: Standard users are allowed to deploy only those resource groups they have created or for which they have permissions.

- Click **Add Existing Resource Group** to add an existing resource group.

To switch views, click the **Tile View** icon or **List View** icon .

To view the resource groups based on a particular resource group state, select an option from the **Filter By** drop-down list. Alternately, in the **Graphical** view, click the graphic in a particular state.

In the **Tile** view, each square tile represents a resource group and has the status of the resource group at the bottom of the graphic. The state icon on the graphic indicates the state of the resource group. The components in blue indicate the component types that are in the deployment. The components that are in gray indicate the component types that are not in the resource group.

In the **List** view, the following information displays:

- **Status**—Status of the resource group.
- **Name**—Name of the resource group.
- **Deployed By**—Name of the user who deployed the resource group.
- **Deployed On**—Date and time when the resource group is deployed.
- **Components**—Components used in the resource group.

Click the resource group in the **List** view or **Tile** view to view the following information about the resource group in the right pane:

- Resource group name and description to identify the resource group.
- Name of the user who deployed the resource group.
- Date and time when the resource group is deployed.
- Name of the reference template that is used in the resource group.
- Number of resources that are in the resource group for deployment, based on component type (cluster or node).

Click **View Details** to view more details about the resource group. You can also generate troubleshooting bundles from the resource group details page.

Click the resource group name in the **List** view to open the **Resource Group Details** page.

Click **Update Resources** to update the firmware of all nodes in the resource group that are not compliant.

Related information

Configuring block storage
Deploying and provisioning

Basic tasks

This section provides basic tasks for resource group management.

Deploying a resource group

Deployment is the automated process of selecting and configuring specific resource requirements that are outlined in a template using the integrated automation workflows provided with PowerFlex Manager. You cannot use a template that is in a draft state to deploy a resource group. Publish the template before using it to deploy a resource group.

Before you begin, enable LLDP on the switches, and update the inventory in PowerFlex Manager.

1. On the menu bar, click one of the following:
   - **Lifecycle** > **Resource Groups**. Then, click **Deploy New Resource Group**.
   - **Lifecycle** > **Templates**. Then, click **Deploy**.

   The **Deploy Resource Group** wizard opens.
2. On the **Deploy Resource Group** page, perform the following steps:
   a. From the **Select Published Template** list, select the template to deploy a resource group.
   b. Enter the **Resource Group Name** (required) and **Resource Group Description** (optional) that identifies the resource group.
   c. To specify the version to use for compliance, select the version from the **Firmware and Software Compliance** list or choose **Use PowerFlex Manager appliance default catalog**.

You cannot select a minimal compliance version when you deploy a new resource group, since it only includes server firmware updates. The compliance version for a new resource group must include the full set of compliance update capabilities. PowerFlex Manager does not show any minimal compliance versions in the **Firmware and Software Compliance** list.

PowerFlex Manager checks the VMware vCenter version to determine if it matches the VMware ESXi version for the selected compliance version. If the ESXi version is greater than the vCenter version, PowerFlex Manager blocks the resource group deployment and displays an error. PowerFlex Manager instructs you to upgrade vCenter first, or use a different compliance version that is compatible with the installed vCenter version.

NOTE: Changing the firmware repository might update the firmware level on nodes for this resource group. The global default firmware repository maintains the firmware on the shared devices.

d. Indicate **Who should have access to the resource group deployed from this template** by selecting one of the following options:
   - To restrict access to super users, select **Only PowerFlex SuperUser**.
   - To grant access to super users and some specific lifecycle administrators and drive replacers, select the **PowerFlex SuperUser and specific LifecycleAdmin and DriveReplacer** option, and perform the following steps:
     i. Click **Add User(s)** to add one or more LifecycleAdmin or DriveReplacer users to the list displayed.
     ii. Select which users will have access to this resource group.
     iii. To delete a user from the list, select the user and click **Remove User(s)**.
     iv. After adding the users, select or clear the check box next to the users to grant or block access.
   - To grant access to super users and all lifecycle administrators and drive replacers, select **PowerFlex SuperUser and all LifecycleAdmin and DriveReplacer**.

3. Click **Next**.
4. On the screens that follow the **Deployment Settings** page, configure the settings, as needed for your deployment.
5. Click **Next**.
6. On the **Schedule Deployment** page, select one of the following options and click **Next**:
   - **Deploy Now**—Select this option to deploy the resource group immediately.
   - **Deploy Later**—Select this option and enter the date and time to deploy the resource group.
7. Review the **Summary** page.
   The **Summary** page gives you a preview of what the resource group will look like after the deployment.
8. Click **Finish** when you are ready to begin the deployment. If you want to edit the resource group, click **Back**.

Related information

Lifecycle
Viewing resource group details
Adding components to a resource group
Build and publish a template
Component types
Removing a resource group

Adding an existing resource group

You can add an existing resource group to discover and import hardware resources that were not originally deployed with PowerFlex Manager.

Ensure that the following conditions are met before you add an existing resource group:

- The vCenter, PowerFlex gateway, CloudLink Center, and hosts must be discovered in the resource list.
- You must have a resource group that includes the manager MDMs prior to importing other resource groups. The first resource group that you import must include the manager MDMs so that PowerFlex Manager has the manager MDM credentials.
- The PowerFlex File gateway must be deployed on the same PowerFlex Manager appliance before you add an existing resource group for NAS. You must have a protection domain that maps to a PowerFlex gateway with PowerFlex file nodes in the current resource inventory.

1. On the menu bar, click **Lifecycle** > **Resource Groups** and then click **+ Add Existing Resource Group**.
2. On the **Add Existing Resource Group** page, enter a resource group name in the **Name** field.
3. Enter a description in the **Description** field.

4. Select the **Type** for the resource group.

   The choices are **Hyperconverged**, **Compute Only**, **Storage Only**, and **PowerFlex File**.

   PowerFlex Manager checks to see whether there are any vCLS VMs on local storage. If it finds any, it puts the resource group in life cycle mode and lets you migrate these VMs to shared storage.

5. To specify the compliance version to use for compliance, select the version from the **Firmware and Software Compliance** list or select **Use PowerFlex Manager appliance default catalog**.

   You cannot specify a minimal compliance version when you add an existing resource group, since it only includes server firmware updates. The compliance version for an existing resource group must include the full set of compliance update capabilities. PowerFlex Manager does not show any minimal compliance versions in the **Firmware and Software Compliance** list.

   NOTE: Changing the compliance version might update the firmware level on nodes for this resource group. Firmware on shared devices is maintained by the global default firmware repository.

6. Specify the resource group permissions under **Who should have access to the resource group deployed from this template?** by performing one of the following actions:
   - To restrict access to super users, select **Only PowerFlex SuperUser**.
   - To grant access to super users and some specific lifecycle administrators and drive replacers, select the **PowerFlex SuperUser and specific LifecycleAdmin and DriveReplacer** option, and perform the following steps:
     a. Click **Add User(s)** to add one or more LifecycleAdmin or DriveReplacer users to the list.
     b. Select which users will have access to this resource group.
     c. To delete a user from the list, select the user and click **Remove User(s)**.
     d. After adding the users, select or clear the check box next to the users to grant or block access.
   - To grant access to super users and all lifecycle administrators and drive replacers, select **PowerFlex SuperUser and all LifecycleAdmin and DriveReplacer**.
7. Click **Next**.
8. Choose one of the following network automation types:
   - **Full Network Automation**
   - **Partial Network Automation**

   When you choose **Partial Network Automation**, PowerFlex Manager skips the switch configuration step, which is normally performed for a resource group with **Full Network Automation**. Partial network automation allows you to work with unsupported switches. However, it also requires more manual configuration before a deployment can proceed successfully. If you choose to use partial network automation, you give up the error handling and network automation features that are available with a full network configuration that includes supported switches.

   In the **Number of Instances** box, provide the number of component instances that you want to include in the template.

9. On the **Cluster Information** page, enter a name for the cluster component in the **Component Name** field.
10. Select values for the cluster settings:

    For a hyperconverged or compute-only resource group, select values for these cluster settings:

    a. **Target Virtual Machine Manager**—Select the vCenter name where the cluster is available.
    b. **Data Center Name**—Select the data center name where the cluster is available.
       NOTE: Ensure that selected vCenter has unique names for clusters in case there are multiple clusters in the vCenter.
    c. **Cluster Name**—Select the name of the cluster you want to discover.
    d. **OS Image**—Select the image or choose **Use Compliance File ESXi image** if you want to use the image provided with the target compliance version. PowerFlex Manager filters the operating system image choices to show only ESXi images for a hyperconverged or compute-only resource group.

    For a storage-only resource group, select values for these cluster settings:

    a. **Target PowerFlex Gateway**—Select the gateway where the cluster is available.
    b. **Protection Domain**—Select the name of the protection domain in PowerFlex.
    c. **OS Image**—Select the image or choose **Use Compliance File Linux image** if you want to use the image provided with the target compliance version. PowerFlex Manager filters the operating system image choices to show only Linux images for a storage-only resource group.

    For a PowerFlex file resource group, select values for these cluster settings:

a. **Target PowerFlex Gateway**—Select the gateway where the cluster is available.
b. **OS Image**—Choose **Use Compliance File Linux image** for a PowerFlex file resource group.

11. Click **Next**.
12. On **OS Credentials** page, select the OS credential that you want to use for each node, SVM, and MVM.

    You can select one credential for all nodes, SVMs or MVMs, or choose credentials for each item separately. You can create the operating system credentials on the **Credentials Management** page under **Settings**.

    PowerFlex Manager validates the credentials before it creates the resource group. This validation makes it possible for PowerFlex Manager to run a full inventory on all nodes, SVMs, and MVMs before creating the resource group.

    PowerFlex Manager runs the inventory on all nodes, SVMs, and MVMs for which the credentials are valid. The resource group uses any nodes, SVMs, and MVMs for which it has a successful inventory. For example, if you have four nodes, and one node has an invalid operating system password, PowerFlex Manager adds the three nodes for which the credentials are valid and ignores the one with an invalid password.

13. Click **Next**.

    The list of resources available in the cluster is displayed on the **Inventory Summary** page.
14. Review the inventory on the **Inventory Summary** page.

    The summary shows all nodes that are available. If a node is not available, it might be because this node does not match the **Type** you selected for the resource group (**Hyper-converged**, **Compute only**, **Storage only**, or **PowerFlex File**).

    Depending on how the node is configured, the summary might show additional inventory information. For example, for a node that has NVDIMM compression, the summary shows additional information about the acceleration pool and compression settings.

    If the resources are discovered and in an available state, the **Available Inventory** displays the components as **Yes**. An unavailable PowerFlex gateway is shown as **No**.

    If the credentials are invalid for a node or SVM, or if you have a network connectivity problem, PowerFlex Manager displays **No** in the **Available Inventory** column for the node, and displays an error message to notify you about the problem.

    PowerFlex Manager cannot update firmware and software versions for PowerFlex clusters that do not have available PowerFlex Gateways. If expected PowerFlex Gateways are not shown as available, you can discover the gateways and run the wizard again.

    NOTE: PowerFlex Manager retrieves the hostname value from iDRAC and not the operating system. If the hostname field is not updated in iDRAC, an incorrect value can be displayed in PowerFlex Manager. Certain operating systems require extra packages that are installed for iDRAC to update the correct hostname.
15. Click **Next**.
16. On the **Network Mapping** page, review the networks that are mapped to port groups and make any required edits.

    PowerFlex Manager attempts to select the correct network based on the VLAN ID, subnet, or IP ranges entered in PowerFlex Manager. If PowerFlex Manager finds only one network for a given network type, it selects the network automatically. If it finds more than one, you must select the network from the **Network** drop-down list. The OS Installation network does not get a VLAN ID.

    NOTE: If the OS install VLAN is not already configured in your environment, add it. This network is required to perform node expansions. This network is typically added during PowerFlex Manager configuration.

    If there are any port groups for which you do not want PowerFlex Manager to manage access, leave those port groups cleared. If no network is selected for a particular port group, PowerFlex Manager leaves it out of the deployment data and does not add it to the nodes.

17. To import many general-purpose VLANs from vCenter, perform these steps:
    a. Click **Import Networks** on the **Network Mapping** page.
    PowerFlex Manager displays the **Import Networks** wizard. In the **Import Networks** wizard, PowerFlex Manager lists the port groups that are defined on the vCenter as **Available Networks**. You can see the port groups and the VLAN IDs.
    b. Optionally, search for a VLAN name or VLAN ID.
    PowerFlex Manager filters the list of available networks to include only those networks that match your search.
    c. Click each network that you want to add under **Available Networks**. If you want to add all the available networks, click the check box to the left of the **Name** column.
    d. Click the double arrow (>>) to move the networks you chose to **Selected Networks**.
    PowerFlex Manager updates the **Selected Networks** to show the ones that you have chosen.
    e. Click **Save**.

18. Click **Next**.
19. Review the **Summary** page and click **Finish** when you are ready to add the resource group.

    The process of adding an existing resource group causes no disruption to the underlying hardware resources. It does not shut down any of the nodes or the vCenter.

    For an existing resource group, the **Reference Template** field shows **Generated Existing Resource Group Template** on the **Resource Group Details** page. You can distinguish existing resource groups from new resource groups that were deployed with PowerFlex Manager.

    When PowerFlex Manager must put a resource group in lifecycle mode, the **Summary** page for the **Add Existing Resource Group** wizard displays a warning message indicating the reason.

    In some situations, an imported configuration might not meet the minimal requirements for lifecycle mode. In this case, PowerFlex Manager does not allow you to add the resource group.

When you add an existing resource group, PowerFlex Manager matches the hosts, vCenter, and other items it finds with discovered resources in the resource list. If you missed a component initially, you can change your resource inventory, and update the resource group to reflect these changes. Go back to the resources list, select the component, and mark it as **Managed** by selecting **Change resource state to Managed**. Then, perform an **Update Resource Group Details** operation on the resource group to pull in the missing component.

When you deploy an existing resource group, PowerFlex Manager reserves any IP addresses from vCenter or the PowerFlex gateway that it needs. If you later tear down the resource group, it releases those IP addresses so that they can be reused.

If you add an existing resource group that supports NSX-T or NSX-V, PowerFlex Manager displays a banner indicating that the resource group supports a limited set of actions. Most resource group actions are disabled for an NSX-T or NSX-V configuration, except the ability to update the firmware and software components, remove resources (or the resource group as a whole), and update resource group details.

When you add an existing resource group, PowerFlex Manager checks to see whether there are any vCLS VMs on local storage. If it finds any, it displays a banner on the **Resource Group Details** page indicating that it has put the resource group in lifecycle mode and gives you the opportunity to migrate the VMs to shared storage.

Related information

Getting started
Lifecycle
Support for full and partial network automation
Migrating vCLS VMs to shared storage

Updating a resource group with new firmware and software

You can update resource group components with new firmware and software versions.

If you are updating the CloudLink Agent, it must be the same version as the CloudLink Center.

CAUTION: Check the Alerts page before performing the upgrade. Look for major and critical alerts related to PowerFlex Block and File to be sure the MDM cluster is healthy before proceeding.

If the new firmware and software catalog causes the PowerFlex gateway or CloudLink Agent to become non-compliant, you must upgrade the PowerFlex gateway or CloudLink Center first from the **Resources** page with the target RCM or IC. PowerFlex Manager blocks some of the resource group actions in this situation. For example, PowerFlex Manager disables scale up or scale down, firmware upgrade, the ability to delete the resource group, network scale up, and node actions.

1. On the **Resource Groups** page, click the **Non-Compliant** link, or click **View Compliance Report**.
2. On the **Node Compliance Report** page, click the **Change** button.
3. On the **Change Compliance File** page, choose the **Preferred Compliance File**.
4. Review the **Compatibility** setting. If it shows **Recommended** or **Supported**, you can proceed with the change. If it shows **Not Allowed**, PowerFlex Manager blocks the change. Review the alert for details about recommended or supported paths.
5. Type `CHANGE COMPLIANCE FILE` in the confirmation box and click **Save**.
6. On the **Node Compliance Report** page, choose the components to be upgraded.
7. Click **Update Resources**.

Related information

Upgrading a PowerFlex gateway

Viewing a compliance report

PowerFlex Manager enables you to view a compliance report and perform firmware and software updates as needed. You can update software and firmware components for a new resource group that PowerFlex Manager deploys or an existing resource group that was not originally deployed by PowerFlex Manager.

If you want to update only the firmware on the nodes, select a minimal compliance version with firmware only as the target version for the resource group before you proceed.

The update process handles node, BIOS, firmware, ESXi driver updates, and ESXi upgrades automatically.

PowerFlex Manager does not upgrade vCenter itself. However, it checks the vCenter version to determine if it matches the ESXi version. If the ESXi version is greater than the vCenter version, PowerFlex Manager blocks the ESXi host upgrade and displays an error.

1. On the menu bar, click **Lifecycle** > **Resource Groups**.
2. Select a resource group to view the compliance report.
3. In the right pane, click **View Details**.
   The **Resource Group Details** page is displayed.
4. On the **Resource Group Details** page, click **View Compliance Report**.
   The **Node Compliance Report** page is displayed.

   You can also view the compliance status on this page.

   When you view a compliance report, PowerFlex Manager checks to see whether there are any vCLS VMs on local storage. If it finds any, it displays a banner at the top of the report and gives you the opportunity to migrate the VMs to shared storage.
5. Click **Change** to modify the target compliance version.
   a. Select the **Preferred Compliance File**.
   b. Review the **Compatibility** setting. If it shows **Recommended** or **Supported**, you can proceed with the change. If it shows **Not Allowed**, PowerFlex Manager blocks the change. Review the alert for details about recommended or supported paths.
   c. If the change is either recommended or supported, type **`CHANGE COMPLIANCE FILE`** if you are ready to proceed.
   d. Click **Save**.
6. Click **Firmware Components** to view the firmware components.
7. Click **Software Components** to view the software components.

   For compute-only and storage-only resource groups, PowerFlex Manager lists the software components that are available for update under the **Components** drop-down list. For hyperconverged resource groups, PowerFlex Manager displays the following subcategories of software components that are available for update:

   - **Node Software** lists the ESXi drivers that are installed if you choose to update.
   - **SVM Software** lists the embedded operating system packages that are installed if you choose to update.
   - **MVM Software** lists the embedded operating system packages that are installed if you choose to update.
8. Select one or more noncompliant nodes, and click **Update Resources**.

   The PowerFlex gateway must first be compliant before you update the PowerFlex components for a node. If a node is already compliant, it is disabled and cannot be selected.

   If you are planning to perform an upgrade on all the nodes in a PowerFlex rack or PowerFlex appliance, click the box in the upper left corner of the **Firmware Components** tab to select all the nodes in the resource group.

9. Specify when to apply the resource updates and click **Apply**:
   - To perform a non-disruptive update right away, choose **Allow PowerFlex Manager to perform firmware and software updates now**.

     Specify the type of update you want to perform by selecting one of the following options:

     - **Instant Maintenance Mode** enables you to perform updates quickly. PowerFlex Manager does not migrate the data.
     - **Protected Maintenance Mode** enables you to perform updates that require 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.

For a non-disruptive update, PowerFlex Manager performs updates for PowerFlex nodes within a single resource group in a serialized workflow. The workflow updates one node at a time.

- To perform a non-disruptive update later, choose **Schedule firmware and software updates**.

  Specify the type of update you want to perform by selecting one of the following options:

  - **Instant Maintenance Mode** enables you to perform updates quickly. PowerFlex Manager does not migrate the data.
  - **Protected Maintenance Mode** enables you to perform updates that require 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.
- To perform a disruptive update right away for a full PowerFlex rack or PowerFlex appliance upgrade, choose **Allow PowerFlex Manager to perform disruptive updates now**.

  PowerFlex Manager does not support disruptive updates for the PowerFlex management platform (PFMP).

  The full system upgrade process is faster. This process should take a matter of hours. However, the nodes and all of the data are unavailable while the upgrade is in process.

  If you are certain that you want to proceed, type **`REBOOT ALL NODES AT ONCE`**.

  For a full system upgrade, PowerFlex Manager ensures that the PowerFlex gateway is used only by this resource group, and checks to see whether any other VMs are running in the cluster. PowerFlex Manager stops the process if these conditions are not met.

10. If you encounter any errors while performing firmware or software updates, you can view the PowerFlex Manager logs for the resource group. On the **Resource Group Details** page, click **Generate Troubleshooting Bundle**.

    This action creates a compressed file that contains:

    - PowerFlex Manager application logs
    - SupportAssist logs
    - PowerFlex gateway logs
    - iDRAC life-cycle logs
    - Dell PowerSwitch switch logs
    - Cisco Nexus switch logs
    - VMware ESXi logs
    - CloudLink Center logs

    The logs are for the current resource group only.

    Alternatively, you can access the logs from a VMware console, or by using SSH to log in to PowerFlex Manager.

Related information

Lifecycle

Entering and exiting service mode

PowerFlex Manager enables you to put a node in service mode when you must perform maintenance operations on the node.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

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.

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 resource group itself goes into service mode.

If the node has a VMware NSX-T or NSX-V 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 resource group is being updated on the **Resources** page.

1. On the menu bar, click **Lifecycle** > **Resource Groups**.
2. On the **Resource Groups** page, select a resource group and click **View Details** in the right pane.
3. Click **Enter Service Mode** under **More Actions**.
4. Select one or more nodes on the **Node Lists** page and click **Next**.

You can only place multiple nodes in service mode simultaneously if all the nodes are in the same fault set.

In a PowerFlex file resource group, only one node at a time can be put in service mode.

5. Specify the type of maintenance that 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 for the **Resource Health** for the selected nodes.
7. When you are ready to leave service mode, click **More Actions** > **Exit Service Mode**.

Replacing a drive

You can replace a failed drive in a deployed node. PowerFlex Manager supports the replacement of SSD and NVMe drives for PowerFlex storage-only nodes and hyperconverged nodes.

Ensure that you have a replacement drive and can access the node.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

PowerFlex Manager supports drive replacement for:

- Nodes that have NVDIMM compression enabled.
- SSD for HBA330 controllers.

  NOTE: RAID controllers are not supported.
- CloudLink-enabled PowerFlex nodes with self-encrypting drives (SEDs) or software encryption.

If either DAS Cache is installed on a node, or if the node has an NSX-T or NSX-V configuration, PowerFlex Manager does not enable you to replace a drive.

1. On the menu bar, click **Lifecycle** > **Resource Groups**.
2. On the **Resource Groups** page, select a resource group and click **View Details** in the right pane.
3. Scroll down to the **Physical Nodes** section of the page.
4. Under **Physical Nodes**, click **Drive Replacement**.
   PowerFlex Manager displays the **Node List** panel in the **Drive Replacement** wizard.
5. Click the node for which you want to perform a drive replacement.
6. Click **Next**.
   PowerFlex Manager displays the **Select Drive** panel. Any empty slots are shown in gray. The slots that have drives are shown in black.
7. Select the drive that you want to replace by clicking the drive slot in the hardware image, or select the drive from the table.

   Be sure to click the correct drive, because the drive replacement process is irreversible.

   The color for the selected drive changes to blue and the table below the hardware image is selected. The table shows details about the selected drive. To help you pick the correct drive, PowerFlex Manager provides the iDRAC name for the drive, the PowerFlex drive name, and the serial number.
8. Optionally, click **Launch iDRAC GUI** to see iDRAC details about the selected drive before proceeding.

   When you launch iDRAC, the iDRAC GUI opens in a different tab. Log in and go to the drive details.
9. Optionally, click **Blink LED** to cause the selected drive to blink.
   PowerFlex Manager turns on the blinking LED on the selected drive and keeps it blinking until you pull the disk out. A new disk is not in a blinking state. PowerFlex Manager is not able to determine whether the drive is blinking. If the drive is already blinking, you can click **Unblink LED** to turn off the blinking LED.
10. Click **Next** when you are ready to delete the drive.
    PowerFlex Manager displays the **Confirmation** page. PowerFlex Manager provides details about the drive and shows a hardware image again with the drive that is selected in blue.

11. Review the information carefully under **Confirm Drive Replacement** to be sure that you have selected the correct drive. If you are certain that you want to proceed, type **REMOVE DRIVE**.
12. Click **Confirm**.
    PowerFlex Manager puts the resource group into the **In Progress** state and updates the **Recent Activity** to show that a drive removal operation is started. After several minutes, if the node ejection is successful, PowerFlex Manager places the resource group and the node in service mode and deletes the drive from the storage pool. The resource group and the node remain in service mode until the drive is replaced in the node, and the drive replacement process has completed. During this period, PowerFlex Manager does not enable you to enter service mode for the node, or perform another drive replacement within the same resource group.

    PowerFlex Manager displays a banner at the top of the **Resource Group Details** page to notify you that a drive replacement is in process for the selected drive.

    For NVMe disks, PowerFlex Manager initiates a job to instruct iDRAC to delete the NVMe disk safely from the operating system.

    If the drive ejection process fails, PowerFlex Manager displays a banner at the top of the **Resource Group Details** page to notify you that the initial step to eject the drive failed. When the delete drive step fails in the drive replacement process, the banner displays a **Retry Drive Replacement** option to help you to restart the drive replacement process.

    If there is a failure, the resource group and the node do not remain in service mode. Instead, they return to the previous state that the resource group was in before you attempted the drive replacement.
13. Pull the disk out of the slot, and insert the new disk.
14. On the disk replacement banner at the top of the **Resource Group Details** page, click **Actions**>**Complete Drive Replacement**.

    PowerFlex Manager opens the **Complete Drive Replacement** wizard and runs inventory on the node. It takes a couple of minutes to get the updated inventory for the node.

    After getting the updated inventory, PowerFlex Manager displays the **Found New Drive** page or the **Continue Without Drive** page. If PowerFlex Manager finds the new drive, it displays the drive that is selected in green on the **Found New Drive** page.

    If PowerFlex Manager does not find the new drive, it displays the **Continue Without Drive** page. If you are certain that you want to proceed without a new drive, type **CONTINUE WITHOUT DRIVE**. If you proceed, the node is taken out of service mode with fewer drives, which might impact the capacity and performance of the resource group. Click **Confirm** to finish the process without adding a drive.
15. Click **Complete** to finish the disk replacement process.
    PowerFlex Manager puts the resource group into the **In Progress** state and updates the **Recent Activity** to show that a complete drive replacement operation is started. Then, PowerFlex Manager replaces the drive in the resource group, and takes the resource group and the node out of service mode.

    When the drive addition is complete, PowerFlex Manager displays a banner at the top of the resource group to notify you that the drive replacement is complete. PowerFlex Manager enables the **Reconfigure MDM Roles** and **Drive Replacement** options again. The resource group returns to the previous state after the drive replacement successfully completes.

Replacing NVDIMM node or battery

PowerFlex Manager supports replacement of faulty NVDIMM node and NVDIMM batteries.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

1. On the menu bar, click **Lifecycle** > **Resource Groups**.
2. On the **Resource Groups** page, select a resource group and click **View Details** in the right pane.
3. Scroll down to the **Physical Nodes** section of the page.
4. Under **Physical Nodes**, click **NVDIMM Replacement**.
   PowerFlex Manager displays the **Node List** panel in the **NVDIMM Replacement** wizard.
5. Select the node for which you want to perform a drive replacement.
6. Click **Next**.
   PowerFlex Manager displays the **Select Component** panel. All the available NVDIMM nodes are displayed under the **NVDIMM** header while the available NVDIMM batteries are displayed under **NVDIMM Battery**.
7. Select the NVDIMM node or battery that you want to replace.
8. Click **Next**.

A message stating the removal or addition of the NVDIMM node or battery, with the node and slot numbers, is displayed on the **Resource Groups** page. The status of the resource group and the individual node is "In Progress". The log details are also displayed in the **Recent Activity** section on the right side of the page.

After the node is replaced, the host and SVM are turned off. After the physical replacement of the node and the battery, the status of the host and node on the **Resource Groups** page display service mode. Also, the option **Discover Replacement NVDIMM** is displayed on the page. The **Discover Replacement NVDIMM** turns on the node and does a system erase of the NVDIMMs. On completion of the discovery, the option, **Complete NVDIMM Replacement** is displayed. After the NVDIMM is replaced, you can create virtual hardware for the NVDIMM device, remove the SDS from maintenance or service mode, and turn on the SVM.

Completing NVDIMM replacement

On the **Complete NVDIMM Replacement** page, you can view details of the node at the top. The details are—the compliance status, inventory update, name, and size of the NVDIMM node. When you add a node, the **Inventory Update** column displays "Adding" next to the node that is added. A firmware update is initiated only if the NVDIMM device is noncompliant.

You also see the list of NVDIMM batteries that are replaced, at the bottom of the page. The battery details are—name of the battery, device ID, enabled state, health, and operational status of the battery.

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.

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.

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**.

Related information

Viewing PowerFlex system details

Migrating vCLS VMs to shared storage

When you add an existing resource group, PowerFlex Manager checks to see whether there are any vSphere Cluster Services (vCLS) VMs on local storage. If it finds any, it puts the resource group in lifecycle mode and lets you migrate the VMs to shared storage.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

After you add an existing resource group, PowerFlex Manager displays a warning banner to notify you that the resource group is in lifecycle mode. You can then migrate the vCLS VMs to shared storage by launching the **Migrate vCLS VMs** wizard.

You can launch the wizard for migrating vCLS VMs to shared storage from the **More Actions** section of the **Resource Group Details** page. You can also launch the wizard from the warning banner at the top of the **Resource Group Details** page or from the warning banner at the top of the **Node Compliance Report**. The operations available are the same regardless of where you launch the wizard.

When you migrate vCLS VMs, PowerFlex Manager automatically creates two resource group volumes and maps these volumes to datastores. The resource group volume names follow the convention of `powerflex-resource group-vol-<NUMBER>`, where *<NUMBER>* is the next available digit that has not been taken. The datastore names follow the convention of `powerflex-<CLUSTER_NAME>-ds-<NUMBER>`, where *<CLUSTER_NAME>* is the name of the vCenter cluster and the *<NUMBER>* is the next available digit. Examples of generated resource group volumes are: powerflex-resource group-vol-1 and powerflex-resource group-vol-2. Examples of generated resource group datastores are: powerflex-Hyperconverged-DKIM-ds-1 and powerflex-Hyperconverged-DKIM-ds-2.

CAUTION: Do not rename the automatically generated resource group volumes and datastores. If for some reason, the names have been changed, PowerFlex Manager creates new resource group volumes and datastores, as needed, that use the correct naming conventions. Also, be sure not to migrate vCLS VMs manually to a nonheartbeat datastore. This action activates lifecycle mode and requires a migration. In this case, volumes and datastores may be created with new names and digits (for example, powerflex-resource group-vol-3, powerflex-resource group-vol-4, and so forth).

1. To access the wizard from the **More Actions** section of the **Resource Group Details** page:
   a. On the menu bar, click **Lifecycle** > **Resource Groups**.
   b. Select a resource group that is in lifecycle mode because it includes vCLS VMs that are on local storage.
   c. In the right pane, click **View Details**.
      The **Resource Group Details** page is displayed.
   d. In the right pane, click **Migrate vCLS VMs** under **More Actions**.
      The **Migrate vCLS VMs** wizard is displayed.
2. For a compute-only resource group, select a protection domain from the **Protection Domain** field.

   The **Protection Domain** field is not displayed for a hyperconverged resource group, since it is already defined by the resource group.
3. For a hyperconverged or compute-only resource group, select a storage pool in the **Storage Pool** drop-down.

   The list of storage pools available for selection is filtered to list the storage pools in the selected protection domain.
4. Review the **Destination Datastores**. The destination datastores are the two heartbeat datastores that PowerFlex Manager creates automatically when you migrate the vCLS VMs to shared storage.

   PowerFlex Manager also creates two resource group volumes and maps these volumes to the destination datastores.

   Only two datastores and resource group volumes are created. If you already have existing datastores, PowerFlex Manager adds the new datastores to the list. If you already have datastores with the same names in the same cluster, PowerFlex Manager does not create new ones, but simply uses the ones that exist already.
5. Type **`MIGRATE VCLS VIRTUAL MACHINES`** to confirm.
6. Click **Confirm**.

After the migration, PowerFlex Manager takes the resource group out of lifecycle mode, and the full set of resource group actions are available.

Related information

Adding an existing resource group
Viewing PowerFlex system details

Adding components to a resource group

You can add one or more node, volume, or network components to a new resource group that PowerFlex Manager deploys, or to an existing resource group not deployed by PowerFlex Manager.

You can add components to a resource group for which deployment was successful or to a failed resource group deployment. You do not need to go back to the original template from which the resource group was originally deployed. Standard users can add components only to a resource group for which they have permission.

1. On the menu bar, click **Lifecycle** > **Resource Groups**.
2. On the **Resource Groups** page, select a resource group and click **View Details** in the right pane.
3. On the **Resource Group Details** page, in the right pane, click one of the following options from the **Add Resources** menu:
   - **Add Nodes** —Add one or more nodes to the resource group
   - **Add Volumes**—Add one or more volumes to the resource group
   - **Add Network**—Add one or more networks to the resource group

   If a node has an NSX-T or NSX-V configuration, PowerFlex Manager removes the **Add Resources** button under **Resource Actions**.

   If the PowerFlex gateway used in the resource group is being updated on the **Resources** page, PowerFlex Manager also removes the **Add Resources** button.

   If the PowerFlex gateway used in the resource group is being updated on the **Resources** page, PowerFlex Manager does not allow you to add a node.

Related information

Component types
Deploying a resource group

Adding nodes to a resource group

To add a node to a resource group:

1. On the **Resource Groups** page, click **Add Resources** and choose **Add Nodes**.
2. In the **Duplicate Node** wizard:
   a. From the **Resource to Duplicate** list, select a node.

      Select a node that is of the same type as the other nodes within the resource group.

   b. In the **Number of Instances** box, enter the number of node instances that you want to add to the resource group.

      PowerFlex Manager requires a minimum of two nodes in a NAS cluster. You can expand the cluster up to a maximum of 16 nodes.

   c. Click **Next**.

   d. Under **PowerFlex Settings**, specify the **PowerFlex Storage Pool Spare Capacity** setting by choosing one of the following options:

      - **Recommended Spare Capacity <n>%** sets the spare capacity to 1 divided by the current number of Storage Data Servers (SDSs) in the protection domain, plus the number of nodes that you want to duplicate. For example, if you have three SDSs and you want to add one more node instance, the recommended spare capacity is set to 25 percent based on the formula 1/4.
      - **Current Spare Capacity <n>%** sets the spare capacity to 1 divided by the current number of SDSs in the protection domain. For example, if you have three SDSs in the protection domain, the current spare capacity is set to 34 percent, based on the formula 1/3, rounded up.

   e. Under **OS Settings**, set the **Host Name Selection** to **Auto-Generate**, **Specify at Deployment Time**, or **Reverse DNS Lookup**.

   f. If you choose **Specify at Deployment**, provide a name for the host in the **Host Name** field. If you choose **Auto-Generate**, specify a template for the name in the **Host Name Template** field.

      For an existing resource group that was not deployed by PowerFlex Manager, the **Host Name Selection** option is automatically set to **Specify at Deployment Time** and you must type the hostname.

g. If you are adding a node to a hyperconverged resource group, specify the **Host Name Selection** under **SVM OS Settings** and provide details about the hostname, as you did for the **OS Settings**.

h. In the **IP Source** box, provide an IP address. For an existing resource group that was not deployed with PowerFlex Manager, the default choice is **User Entered IP** and the IP settings for each network default to **Manual Entry**. However, you can change the setting to **PowerFlex Manager Selected IP**.

   If the **Multi-Network Selection** option is selected and the IP source is **PowerFlex Manager Selected IP**, the IPs are assigned sequentially from all the networks of that type. If an IP cannot be assigned from any of the multiple networks of the selected type, an error is displayed. If the IP source is **User Entered IP**, a generic name is displayed for the IP Source setting. For example: "PowerFlex Management IP Source".

   If multi networking is not enabled and the IP source is **User Entered IP**, the name of the network is displayed as on the **Network Settings** page. If the selected IP Source setting is of **Manual Entry** type, the IP you entered is validated against all the networks of the selected type. An error is displayed when the IP is not validated in one of the networks.

   Under **Hardware Settings**, the **Target Boot Device** option is automatically set to **Use Local Flash Storage for Dell PowerFlex** for an existing hyperconverged or compute-only resource group that was not deployed by PowerFlex Manager.

i. Under **Hardware Settings**, in the **Node Source** box, select **Node Pool** or **Manual Entry**.

   For an existing resource group that was not deployed by PowerFlex Manager, the node source defaults to **Manual Entry**, but you can change it to **Node Pool**.

j. In the **Node Pool** box, select the node pool. Alternatively, if you chose **Manual Entry**, select the specific node in the **Choose Node** box.

   You can view all user-defined node pools and the global pool. Standard users can see only the pools for which they have permission.

   For an existing resource group that was not deployed by PowerFlex Manager, the **Node Pool** defaults to **Global**.

k. Under **PowerFlex Settings**, specify the **Fault Set** for a node:
   - Select **PowerFlex Manager Selected Fault Set** to have PowerFlex Manager choose the fault set name based on the template settings.
   - Select ***fault-set-name*** to choose one of the fault sets in the resource group.

   You can add nodes within a fault set, but PowerFlex Manager does not allow you to add a new fault set within the same resource group. To add a new fault set, you must deploy a separate resource group with settings for the fault set you want to create.

l. Click **Next**.

m. Review the **Summary** page and click **Finish**.

   If the node you are adding has a different type of disk than the base deployment, PowerFlex Manager displays a banner at the top of the **Summary** page to inform you of the different disk types. You can still complete the node expansion. However, your resource group may have suboptimal performance.

   Based on the component type, the required settings and properties are displayed automatically and can be edited as permitted for a node expansion.

3. Click **Save**.

Adding volumes to a resource group

Use this procedure to create new volumes or add existing volumes to a resource group.

You can create new volumes for a storage-only or hyperconverged resource group. Alternatively, you can add existing volumes to a compute-only resource group or hyperconverged resource group. PowerFlex Manager allows you to create up to 50 new volumes at a time for a storage-only or hyperconverged resource group.

A compute-only resource group consumes volumes that are provided by a storage-only or hyperconverged resource group. Initially, there are no volumes for a new resource group. The resource group is in an incomplete state until you add volumes. Add at least one volume to a resource group to get it out of the incomplete state. If the resource group is a VMware ESXi cluster that has VMware High Availability (HA) enabled, you need at least two volumes.

NOTE: For a hyperconverged resource group, PowerFlex Manager does not put the resource group in an incomplete state, because it automatically creates two resource group volumes that are mapped to two heartbeat datastores.

After you create the volumes in a storage-only resource group, they are added to PowerFlex, but not mapped. When you add the volumes to a compute-only resource group, PowerFlex maps the volumes and creates the datastores.

For a hyperconverged resource group, the added volumes are mapped to the datastore. PowerFlex Manager requires you to enter the datastore name for each new volume that must be added. This is because PowerFlex Manager also creates an ESXi cluster and vCenter datastore for a hyperconverged resource group.

PowerFlex Manager allows you to enable compression when adding volumes to a storage-only or hyperconverged resource group.

PowerFlex Manager does not allow you to add volumes to a PowerFlex file (NAS) resource group.

To add volumes to a resource group:

1. On the **Resource Groups** page, click **Add Resources** and choose **Add Volumes**.
2. To add existing volumes to a compute-only or hyperconverged resource group, select **Add Existing Volumes** and follow these steps:
   a. Click **Select Volumes** to choose the volumes you want to add.
   b. Enter a volume or datastore name search string in the **Search Text** box.
   c. Optionally, apply additional search criteria by specifying values for the **Size**, **Type**, **Compression**, and **Storage** filters.
   d. Click **Search**.
   PowerFlex Manager updates the results to show only those volumes that satisfy the search criteria. If the search returns more than 50 volumes, refine the search criteria to return only 50 volumes.
   e. Click the checkbox for each volume you want to add.
   f. Click the **>>** button to select the volumes.

      To remove a selected volume, click the checkbox for the volume to remove and click the **<<** button.

   g. When you are ready to add the selected volumes, click **Add**.
   h. After you have selected the volumes that you want to add, define a template for datastore names in the **Datastore Name Template** field and click **Next**.

      The template must include a variable that allows PowerFlex Manager to produce a unique datastore name.
3. To create new volumes for a storage-only or hyperconverged resource group, select **Create New Volumes** and follow these steps:

   If you want to create a single volume with a specified name:

   a. Click **+ Add Volume** to add a new volume section.

      PowerFlex Manager adds a new volume section to the **Add Volume** wizard.

   b. In the **Volume Name** field, select **Specify Name**.
   c. In the **New Volume Name** field, type the volume name.
   d. In the **Datastore Name** field, select **Create New Datastore** to create a new datastore, or select a datastore.
   e. In the **New Datastore Name** field, type the name for the datastore.
   f. In the **Storage Pool** drop-down, choose the storage pool where the volume will reside.
   g. Select the **Enable Compression** check box to take advantage of the PowerFlex NVDIMM compression feature.
   h. In the **Volume Size (GB)** field, select the size in GB. The minimum size is 8 GB and the value you specify must be divisible by eight.
   i. In the **Volume Type** field, select thick or thin.

      A thick volume provides a larger amount of storage in advance, whereas a thin volume provides on-demand storage and faster setup and startup times.

      If you enable compression on a hyperconverged or storage-only resource group with the granularity of the storage pool set to fine, the only option for **Volume Type** is thin. This is the case regardless of whether you deploy a compressed or non-compressed volume.

   If you want to create multiple volumes that share a common naming pattern:

   a. Click **+ Add Volume** to add a new volume section.

      PowerFlex Manager adds a new volume section to the **Add Volume** wizard.

   b. In the **Volume Name** field, select **Auto Generate Name**.
   c. In the **Volume Name Template** field, define the template for volume names.

      The template must include a variable that allows PowerFlex Manager to produce a unique volume name.

d. In the **How Many Volumes** field, select the number of volumes you want to create.

   The number must not be greater than 50.

e. In the **Datastore Name Template** field, define a template for datastore names.

   The template must include a variable that allows PowerFlex Manager to produce a unique datastore name.

f. In the **Storage Pool** drop-down, choose the storage pool where the volume will reside.

g. Select the **Enable Compression** check box to take advantage of the PowerFlex NVDIMM compression feature.

h. In the **Volume Size (GB)** field, select the size in GB. The minimum size is 8 GB and the value you specify must be divisible by eight.

i. In the **Volume Type** field, select thick or thin.

   A thick volume provides a larger amount of storage in advance, whereas a thin volume provides on-demand storage and faster setup and startup times.

   If you enable compression on a hyperconverged or storage-only resource group with the granularity of the storage pool set to fine, the only option for **Volume Type** is thin. This is the case regardless of whether you deploy a compressed or non-compressed volume.

4. Optionally, click **Add volume** again to add another volume section. Then, provide the required information for that section.
5. Click **Next** once you have included information about all of the volumes you want to add.
6. On the **Summary** screen, review the volume details to be sure that everything looks correct.

   If you added existing volumes, you can click **View Volumes** to review the list of volumes previously selected.

7. Click **Finish**.

   The resource group moves to the **In Progress** state and the new volume icons appear on the **Resource Group Details** page. You may see multiple volume components while the add operation is still in progress. One the operation is complete, you will see just one volume component with the count updated.

   After the deployment completes successfully, you can click **View Volumes** in the **Storage** list on the **Resource Group Details** page to search for volumes that are part of the resource group.

   The PowerFlex user interface shows the new volumes under the storage pool. For a storage-only resource group, the volumes are created, but not mapped. For a compute-only or hyperconverged resource group, the volumes are mapped to SDCs. In the vSphere client, you can see the volumes in the storage section and also see the hosts that are mapped to the volumes, once the mappings are in place.

Related information

Resize a volume
Viewing and selecting volumes

Adding a network to a resource group

You can update the workload network by adding a network to a resource group. Alternatively, 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 resource groups.

1. On the **Resource Group Details** page, click **Add Resources** and choose **Add Network**.
   The **Add Network** window is displayed. All used resources and networks are displayed under **Resource Name** and **Networks**.
2. Click **Add Additional Network** to add an additional network:
   a. From the **Available Networks** list, select the network, and click **Add**.
      The selected network is displayed under **Network Name**. You can define a new network by clicking **Define a New Network**. For more information, see Defining a network.
   b. Select **Port Group** from the **Select Port Group** list.
   c. Click **Save**.

      NOTE: You cannot remove an added network using PowerFlex Manager.

3. Click **Add Additional Static Route** to add an additional static route:
   a. Click **Add New Static Route**.
   b. Select a **Source Network**.

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

c. Select a **Destination Network**.

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

d. Type the IP address for the **Gateway**.
e. Click **Save**.

Resize a volume

After adding volumes to a resource group, you can resize the volumes.

For a storage-only resource group, you can increase the volume size. For a VMware ESXi compute-only resource group, you can increase the size of the datastore that is associated with the volume. For a hyperconverged resource group, you can increase the size of both the volume and the datastore.

If you resize a volume in a storage-only resource group, you must update the datastore size in the corresponding VMware ESXi compute-only resource group. The datastore size cannot exceed the size of the volume.

1. On the **Resource Groups** page, click the volume component and choose **Volume Actions** > **Resize**.
2. Choose the volume that you want to resize:
   a. Click **Select Volume**.
   b. Enter a volume or datastore name search string in the **Search Text** box.
   c. Optionally, apply additional search criteria by specifying values for the **Size**, **Type**, **Compression**, and **Storage** filters.
   d. Click **Search**.
   PowerFlex Manager updates the results to show only those volumes that satisfy the search criteria. If the search returns more than 50 volumes, you must refine the search criteria to return only 50 volumes.
   e. Select the row for the volume you want to resize.
   f. Click **Apply**.
3. Update the sizing information:

   If you are resizing a volume for a hyperconverged resource group, perform these steps:

   a. In the **New Volume Size (GB)** field, specify a value that is greater than the current volume size.
   b. Optionally, select **Resize Datastore** to increase the size of the datastore.

   If you are resizing a volume for a storage-only resource group, enter a value in the **New Volume Size (GB)** field. Specify a value that is greater than the current volume size. Values must be in multiples of eight, or an error occurs.

   If you are resizing a volume for a compute-only resource group, review the **Volume Size (GB)** field to see if the volume size is greater than **Current Datastore Size (GB)**. If it is, PowerFlex Manager expands the datastore size.

4. Click **Save**.

Related information

Adding volumes to a resource group

Removing resources from a resource group

You can remove resources that were previously added to a resource group.

If you are removing a node that is fulfilling a Meta Data Manager (MDM) role, verify that you will have at least two MDMs and one tiebreaker in the cluster after the removal of the node. When you remove a node, PowerFlex Manager puts a standby node in place of the one that you removed. For a storage-only resource group, the platform minimum is four nodes in the cluster. This enables you to scale down to three nodes for a component replacement.

If the node has an NSX-T or NSX-V configuration, you can remove the node information that PowerFlex Manager displays for the resource group, but not delete the node from the resource group entirely. If the PowerFlex gateway used in the resource group is being updated on the **Resources** page, PowerFlex Manager does not enable you to remove resources from the resource group.

1. On the menu bar, click **Lifecycle** > **Resource Groups**.
2. Select a resource group from which you want to delete resources.

3. In the right pane, click **View Details**.
4. On the **Resource Group Details** page, in the right pane, under **More Actions**, click **Remove Resource**.
5. In the **Remove Resource** dialog box, select the node that you want to remove and click **Next**.
6. Select the **Resource removal type**:
   - **Delete Resource** makes configuration changes to the nodes, switch ports, virtual machine managers, and PowerFlex to unconfigure those components, and returns the components to the available inventory.
   - **Remove Resource** removes deployment information, but does not make any configuration changes to the nodes, switch ports, virtual machine managers, and PowerFlex, and returns the components to the available inventory.
7. If you choose **Remove Resource**, perform the following steps:
   a. To keep the node in the inventory, select **Leave resource in PowerFlex Manager inventory and set state to** and select the state:
      - **Managed**
      - **Unmanaged**
      - **Reserved**
   b. To remove the node, select **Remove resource from the PowerFlex Manager inventory**.
   c. Click **Remove**.
8. If you choose **Delete Resource**, perform the following steps:
   a. If you are certain that you want to proceed, type **`DELETE RESOURCE`**.
   b. Click **Delete**.

When you delete a node from a resource group, PowerFlex Manager performs the following steps to clean up the underlying components associated with the node:

1. Reconfigures the MDM cluster to ensure that the cluster is in good, working order. This step is necessary only if the node is part of an MDM cluster.

   If necessary, PowerFlex Manager reconfigures the MDM role for each node to be a manager or tiebreaker when you perform a scale down operation. PowerFlex Manager rebalances the roles as needed for a new resource group or for an existing resource group. PowerFlex Manager applies the required role changes for nodes that are within the same resource group or in a different resource group.
2. If the node is on the list of SDSs, it removes the node from the list of SDSs within PowerFlex, The node might only be removed from the SDS list if the spare capacity is sufficient, and the environment provides enough space.
3. Deletes the SVM for the node
4. Deletes the virtual networking configuration
5. Removes the host from vCenter (hyperconverged resource groups only)
6. Removes the operating system on the node
7. Removes the node from the SDC list within PowerFlex

When deleting a node for a hyperconverged resource group that has compression, PowerFlex Manager removes the DAX from the acceleration pool.

If you remove a node that is CloudLink enabled from a hyperconverged or storage-only resource group, PowerFlex Manager also performs these cleanup tasks:

- Unencrypts the drives on the server.
- Removes the machine from the machine group.
- Removes IP addresses from approved networks.

PowerFlex Manager does not remove the machine groups or keystores. The machine groups and keystores can be reused for subsequent deployments.

After a node is deleted from a resource group, the **Resource Group Details** page shows the cluster without the removed node, and updates the MDM roles to reflect the new configuration.

Adding NVMe/TCP storage access

PowerFlex Manager enables you to add NVMe/TCP storage access to nodes in a resource group. When you add storage access, it installs the SDT (Storage Data Target) package on all nodes in the resource group.

NVMe storage access is only supported for a resource group that is on PowerFlex 4.0. In addition, the option to add NVMe storage access is only available if the resource group was deployed with the **SDC Only** option selected for **Client Storage Access** in the template.

1. On the menu bar, click **Lifecycle** > **Resource Groups**.
2. Select the resource group.
3. On the **Resource Group Details** page, under **More Actions**, click **Add NVMe Storage Access**.
4. Review the list of nodes.
5. Type **`ADD SDT TO NODES`** to confirm your changes.
6. Click **Confirm**.

Additional resource group management tasks

This section provides additional tasks for resource group management.

Redeploying a resource group

You can redeploy a resource group that failed to deploy because of errors. Standard users can redeploy only a failed resource group that they have deployed.

1. On the menu bar, click **Lifecycle** > **Resource Groups**.
2. On the **Resource Groups** page, select a resource group in an error state and click **View Details** in the right pane.
3. On the **Resource Group Details** page, in the right pane, under **More Actions**, click **Retry**.
4. Click **Yes** when a confirmation message appears.

   If necessary, PowerFlex Manager reconfigures the MDM role for each node to be a manager or tiebreaker when you perform a retry operation. PowerFlex Manager rebalances the roles as needed for a new resource group or for an existing resource group. PowerFlex Manager applies the required role changes for nodes that are within the same resource group or in a different resource group.

Edit resource group information

You can edit information about a resource group such as the resource group name, description, and who has access to the resource group information.

1. On the menu bar, click **Lifecycle** > **Resource Groups**.
2. On the **Resource Groups** page, click the resource group.
3. On the **Resource Group Details** page, in the right pane click **Modify**.
4. In the **Modify Resource Group Information** dialog box, modify the **Resource Group Name** and **Resource Group Description** that identifies the resource group.
   - To update the firmware and software running on the nodes when you deploy a resource group that uses this template, select **Firmware and Software Compliance**.

     If you select a minimal compliance version for a resource group, PowerFlex Manager puts the resource group in lifecycle mode and restricts the actions that can be performed. In lifecycle mode, the resource group supports monitoring, service mode, and compliance upgrade operations only. All other resource group operations are blocked.

     NOTE: Changing the firmware repository might update the firmware level on nodes for this resource group. The global default firmware repository maintains firmware on shared devices.
5. Set the **OS Image** for the resource group.

   You can optionally select a custom operating system image that will be used for future add node operations on the resource group. The custom image must be added to the **OS Image Repositories** tab on the **Settings** > **Compliance and OS Repositories** page.

   PowerFlex Manager filters the list of images available for selection to include only those images that are suitable for the current resource group. For example, if you are editing a hyperconverged resource group, PowerFlex Manager only allows you to choose ESXi images.
6. Specify the permissions for this resource group under **Who should have access to the resource group deployed from this template?** by performing one of the following actions:
   - To restrict access to super users, select **Only PowerFlex SuperUser**.
   - To grant access to super users and some specific lifecycle administrators and drive replacers, select the **PowerFlex SuperUser and specific LifecycleAdmin and DriveReplacer** option, and perform the following steps:

a. Click **Add User(s)** to add one or more LifecycleAdmin or DriverReplacer users to the list displayed.
b. Select which users will have access to this resource group.
c. To delete a user from the list, select the user and click **Remove User(s)**.
d. After adding the users, select or clear the check box next to the users to grant or block access.

- To grant access to super users and all lifecycle administrators and drive replacers, select **PowerFlex SuperUser and all LifecycleAdmin and DriveReplacer**.

7. Click **Save**.

Viewing resource group details

You can view the state of a resource group at the component level. You can view the component topology and connections in a selected resource group template. You can view component logs, display the port view, place a component in service mode, and replace a disk.

If the resource group state is incomplete, a banner at the top of the page indicates that you must add volumes to make it fully functional. In some cases, you may only need to run **Update Resource Group Details** to ensure that the resource group is complete.

To view the details of a resource group component, scroll down on the **Resource Group Details** page. The following information is displayed based on the resource types in the resource group:

Resource type	Description
Clusters	View the following information about the clusters in the VMware vCenter environment: • **Health** • **Data Center Name** • **Cluster Name** • **Asset/Service Tag** • **Management IP**
PowerFlex Gateways	View the following information about the gateways that are part of the resource group: • **Health** • **System Name** • **Primary MDM IP** • **Management IP** • **Virtual IP** • **Total Storage Pools** Provides the number of storage pools in the resource group. If the resource group has storage pools, PowerFlex Manager also lists the granularity setting and acceleration pool for each storage pool. In PowerFlex, the storage pools enable the generation of different storage tiers. A storage pool is a physical storage device in a protection domain. Each storage device belongs to one (and only one) storage pool. The resource group deployment results in the creation of a separate storage pool for each type of disk (SSD/NVMe or hard drive) found in the nodes. The deployment process adds the disks from the nodes to the appropriate storage pools based on the expected types for each pool. • **Protection Domain** In PowerFlex, a protection domain is a logical entity that contains a group of Storage Data Servers (SDSs) that provide backup to each other. Each SDS belongs to one (and only one) protection domain. Each protection domain is a unique set of SDSs. It may also contain SDTs and SDRs.
CloudLink	View the following information about the CloudLink Centers participating in the resource group: • **Health** • **Hostname** • **Management IP**

Resource type	Description
	• **Machine Group** • **Keystore** When a resource group is deployed, if CloudLink has clustered CloudLink Centers, PowerFlex Manager shows all CloudLink Centers on the **Resource Group Details** page. PowerFlex Manager ensures that the resource group deployment succeeds as long as at least one CloudLink Center in the cluster is working.
Storage	View details about the storage volumes added for the resource group. Click **View Volumes** to search for volumes and see the following information about the volumes: • **Name** • **Size** • **Type** • **Compression** • **Storage Pool** • **Datastore**
Physical Nodes	View the following information about the nodes that are part of the resource group: • **Health** • **Asset/Service Tag** • **iDRAC IP/Hostname** • **PowerFlex Mode** The mode for each node is one of the following: ○ **Hyper-converged** includes both SDS and SDC components. ○ **Storage Only** includes only the SDS component. ○ **Compute Only** includes only the SDC component. • **MVM Hostname** For a hyperconverged resource group, PowerFlex Manager adds IP addresses for the MVM to the node IP list. PowerFlex Manager appends `(MVM)` to all network names for the MVM. If there are no MVM hostnames, the MVM Hostname column is not shown. • **Associated IPs** • **MDM Role** The MDM role is the metadata manager role. The MDM role applies only to those nodes that are part of a PowerFlex cluster. The MDM role is one of the following: ○ **Primary**: The MDM in the cluster that controls the SDSs and SDCs. The primary MDM contains and updates the MDM repository, the database that stores the SDS configuration, and how data is distributed between the SDSs. This repository is constantly replicated to the secondary MDMs, so they can take over with no delay. Every PowerFlex cluster has one primary MDM. ○ **Secondary**: An MDM in the cluster that is ready to take over the primary MDM role if necessary. ○ **Tie Breaker**: An MDM whose sole role is to help determine which MDM is the primary. ○ **Standby MDM**: A standby MDM can be called on to assume the position of a manager MDM when it is promoted to be a cluster member. ○ **Standby Tie Breaker**: A standby node that is prepared to take over as a tiebreaker. • **Fault Set**: A logical group of SDSs within a protection domain that defines by the way it is grouped where the copies of data exist. If there is no fault set, this column is not shown.

View all settings

View All Settings allows you to view the settings configured on the resources in a resource group for deployment.

When you click **View All Settings**, the **Resource Group Deployment Settings** page shows each top-level component on a separate tab. Click on a tab for a component to see the details for the component. By displaying the details on separate tabs, PowerFlex Manager greatly improves the performance when you are working with a resource group that includes a large number of nodes.

For a PowerFlex resource group, the **VMware Cluster** section of the **Settings** page shows the **PowerFlex Settings** section, and the **Target PowerFlex Gateway** should specify the gateway that is included with the resource group.

For a PowerFlex resource group, the **Use Local Storage For Dell PowerFlex** property is set to **true** within the **OS Settings** section for any node in an existing PowerFlex resource group deployment, and for the nodes in a new PowerFlex resource group deployment.

Generate troubleshooting bundle

Generate Troubleshooting Bundle allows you to generate a compressed file of logs to use for troubleshooting. The following logs are included:

- ASM deployer
- iDRAC life cycle
- Dell PowerSwitch switch
- Cisco Nexus switch
- VMware ESXi
- CloudLink Center
- NAS
- Standard output logs from all pods
- Kubernetes logs about pods, services, deployments, secrets, drivers, and volumes

View compliance report

View Compliance Report allows you to view the software or firmware compliance report.

Add resources

Add Resources allows you to add nodes, volumes, and networks to a resource group.

More actions

Under **More Actions**, you can perform the following tasks:

Click...	To...
Update Resource Group Details	Update resource group definition.
Enter Service Mode	Put nodes in service mode so that maintenance operations can be performed.
Exit Service Mode	Take nodes out of service mode.
Reconfigure MDM Roles	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.
Remove Resource Group	Remove a resource group that is no longer required. PowerFlex Manager supports two types of removal: • Delete the entire resource group, which deletes the deployment information and makes any required configuration changes for components that are associated with the resource group. This includes making destructive changes such as unconfiguring the nodes in the resource group and powering them down. • Delete the deployment information for the resource group without making any configuration changes to the deployed components.

Click...	To...
Remove Resource	Removes resources from a resource group.
Retry	Redeploy a failed or canceled resource group. This button is only visible when a resource group is in a critical state. If you see a resource group fail for any reason, try clicking **Retry** to correct the problem. For example, a server deployment might fail with a `ChangeBootOrderByInstanceID failed` message. You can correct this failure by retrying the resource group.
Cancel	Cancel the resource group.

Resource actions

Under **Resource Actions**, you can perform the following tasks:

Click...	To...
Add Resources	Select the type of the resources that you want to add to the resource group. If you must input data for the template that is used to create the running resource group, click **Confirm Resource Group Settings**. In the **Update Resource Group Component** window, enter values for all displayed fields. Click **Save**.
Remove Resource	Remove resources from a resource group.

Resource group information

In the **Resource Group Information** box on the right, you can view the following information:

- **Overall Resource Group Health**—Displays the health of the resource group. The following information determines the overall resource group health:
  - **Resource Health** —Displays the health monitoring of resources.
  - **Compliance**—Displays if the resources are firmware or software-compliant. This option is applicable only if you have enabled firmware or software update on the resource group.
  - **Deployment State**—Indicates if the deployment of the resource group completed successfully.
- **Deployed By**—Displays the name of the user who deployed the resource group.
- **Deployed On**—Displays the date and time when the resource group is deployed.
- **Reference Template**—Displays the name of the reference template that is used in the resource group.

  NOTE: For existing resource groups, the name displays as **User Generated Template** and not a template name from the inventory.
- **User Permissions**—Displays one of the following:
  - **Enabled**—Indicates that the permission is granted for one or more standard users to deploy this resource group.
  - **Disabled**—Indicates that the permission is not granted for the standard users to deploy this resource group.

Recent activity

Recent Activity displays component deployment status and information about the current deployed resource group.

You can also click the **Port View** tab to display port view details.

If you want to see the current firmware or software repository that is in use, look at **Target Version**. To change the compliance version, click **Change Target**.

If you select a minimal compliance version for a resource group, PowerFlex Manager puts the resource group in lifecycle mode and restricts the actions that can be performed. In lifecycle mode, the resource group supports monitoring, service mode, and compliance upgrade operations only. All other resource group operations are blocked.

Related information

Deploying a resource group
Updating firmware and software

Viewing all settings

The **View All Settings** option lets you display the settings that are used to configure the resources in the deployment of a resource group.

When you click **View All Settings**, the **Resource Group Deployment Settings** page shows each top-level component on a separate tab. Click on a tab for a component to see the details for the component. By displaying the details on separate tabs, PowerFlex Manager greatly improves the performance when you are working with a resource group that includes a large number of nodes.

You can see all settings that are defined for the clusters and nodes, as well as storage. To search for volumes within the resource group, you can click **View Volumes** under **Storage**.

During volume operations, the **Resource Group Deployment Settings** page displays additional information about the volume operations that are in progress. If you create a new volume or add an existing volume, or resize a volume, the page provides details that can be helpful for troubleshooting. For example, if you specified an invalid name template string variable, the **Resource Group Deployment Settings** page indicates that this is the cause of a volume not being added.

Viewing and selecting volumes

Use this procedure to search for volumes in a resource group, and optionally select volumes for an add or resize operation.

You can use the volume search dialog to search for volumes using various types of search criteria. You can search by volume name or datastore name, as well as by volume type, compression setting, and storage pool name.

You can launch the volume search dialog from various places with the PowerFlex Manager user interface. You can launch the dialog from the following locations:

- **Storage** section of the **Resource Group Details** page
- **View All Settings** page
- **Add Volumes** wizard
- **Resize Volume** wizard

When you perform a search, PowerFlex Manager updates the results to show only those volumes that satisfy the search criteria. If the results would include more than 50 volumes, you must refine the search criteria to return only 50 volumes.

After performing a search in the **Add Volumes** wizard, you can select one or more existing volumes to add to a resource group. In the **Resize Volume** wizard, you can select the volume that you want to resize.

Identify the naming patterns that are used for the volumes and datastores within the resource group, so you can easily enter a search pattern.

1. To access the **Volumes** dialog from the **Storage** section of the **Resource Group Details** page:
   a. On the menu bar, click **Lifecycle** > **Resource Groups**.
   b. Select a resource group.
   c. On the **Resource Group Details** page, click **View Volumes** in the Storage section.

      You can also click **View Volumes** in the Storage section of the **View All Settings** page, which is also available from the **Resource Group Details** page.

      The **Volumes** dialog is displayed.
2. To access the **Volumes** dialog from the **Add Volumes** wizard:
   a. On the menu bar, click **Lifecycle** > **Resource Groups**.
   b. Select a resource group.
   c. On the **Resource Groups** page, click the **Add Resources** button and choose **Add Volumes**.
   d. When PowerFlex Manager displays the **Add Volume** wizard, click **Add Existing volumes**.
   e. Click **Select Volumes**.
      The **Select Existing Volumes** dialog is displayed.
3. To access the **Volumes** dialog from the **Resize Volume** wizard:
   a. On the menu bar, click **Lifecycle** > **Resource Groups**.
   b. Select a resource group.

c. On the **Resource Groups** page, click the volume component and choose **Volume Actions** > **Resize**.
d. Click **Select Volume**.
The **Select Volume** dialog is displayed.

4. Provide the search criteria needed to filter the results to show 50 volumes or fewer:
a. Enter a volume or datastore name search string in the **Search Text** box.
b. Optionally, select a **Size** range.
c. Optionally, **Thick** or **Thin** for the **Type**.
d. Optionally, select **Enabled** or **Disabled** for the **Compression** setting.
e. Optionally, select a specific **Storage Pool**.
f. Click **Search**.
PowerFlex Manager updates the results to show only those volumes that satisfy the search criteria. If the search returns more than 50 volumes, you must refine the search criteria to return only 50 volumes.
g. If you are viewing volumes, click **Close** when you are done looking at the search results.
5. If you are adding existing volumes, you can select one or more volumes to add:
a. Select each volume you want to add.
b. Click **>>** to add the volumes.

To remove a selected volume, click the checkbox for the volume to remove and click **<<**.

c. When you are ready to add the selected volumes, click **Add**.
6. If you are selecting a volume for a resize operation, you can select the volume that you want to resize and click **Apply**.

Related information

Adding volumes to a resource group

Updating the details for a resource group

When new resources are added or removed outside of PowerFlex Manager, you can update the resource group details to pull in those changes. If nodes are removed externally, updating the resource group details does not pull in the changes.

You can update the details for a new resource group that was deployed with PowerFlex Manager, or for an existing resource group that includes resources that were not originally deployed with PowerFlex Manager.

If the PowerFlex gateway used in the resource group is currently being updated on the **Resources** page, PowerFlex Manager does not enable you to update the resource group details.

Whenever you update the resource group details, PowerFlex Manager pulls in a representation of the components from the vCenter cluster, PowerFlex gateway, or CloudLink Center that was specified for the resource group. These components might include new nodes, volumes, SVMs, or MVMs. When a new component is added to the definition of a resource group, PowerFlex Manager does not modify the component.

If the CloudLink Center for the resource group shuts down, PowerFlex Manager loses communication with the CloudLink Center. If the CloudLink Center is part of a cluster, PowerFlex Manager moves to another CloudLink Center when you update the resource group details.

Before you update the details for a resource group, ensure that you run inventory for the vCenter and the PowerFlex gateway.

1. On the menu bar, click **Lifecycle** > **Resource Groups**.
2. Select the resource group.
3. On the **Resource Group Details** page, under **More Actions**, click **Update Resource Group Details**.
4. Review the **OS Credentials** page, and click **Next**.

PowerFlex Manager shows all nodes, SVMs, and MVMs, along with their credentials. This enables you to update the username and password if it has changed for any of these items.

5. Review the **Inventory Summary** page, and click **Next**.

PowerFlex Manager does a rediscovery of the resource group, and tracks whether items are new to the resource group.

In the **Inventory Update** column, PowerFlex Manager shows which items are added, removed, or kept as is within the resource group:

- **Adding** indicates that an item was added externally and will now be added to the resource group.
- **Removing** indicates that an item was removed externally and will now be removed from the resource group.
- **No Change** indicates that an item was not modified externally and will be kept in the resource group.

6. Review the **Summary** page, and click **Finish**.
   PowerFlex Manager checks the configuration and inventory of selected resources to ensure that everything is configured properly. The resource group is moved to the **In Progress** state, and any new component types are displayed on the **Resource Group Details** page. **Recent Activity** shows that a new deployment started.

Confirming resource group settings

If a PowerFlex Manager upgrade added new required fields to components within the template from which a resource group was deployed, the **Confirm Resource Group Settings** button is displayed on the **Resource Groups** page. Although confirming resource group settings is not mandatory, certain resource group or resource functions are not available until this step is complete.

Click **Confirm Resource Group Settings** to launch the **Upgrade Resource Group Components** window. Fields in this window vary depending on which components contain newly required settings. Complete all the displayed fields, and click **Save**.

Removing a resource group

You can remove a resource group that is no longer required. PowerFlex Manager supports two types of removal:

- Delete the entire resource group, which deletes the deployment information and also makes any required configuration changes for components that are associated with the resource group.
- Remove just the deployment information for the resource group without making any configuration changes to the deployed components.

If the node has an NSX-T or NSX-V configuration, you can remove the deployment information for a resource group, but not delete the resource group entirely. PowerFlex Manager also does not allow you to delete a resource group if the PowerFlex gateway used in the resource group is currently being updated on the **Resources** page.

Standard users can delete only the resource groups that they have deployed.

To remove a resource group, perform the following steps:

1. On the menu bar, click **Lifecycle** > **Resource Groups**.
2. Select the resource group.
3. On the **Resource Group Details** page, under **More Actions**, click **Remove Resource Group**.
4. In the **Remove Resource Group** dialog box, select the **Resource group removal type**:
   - **Delete Resource Group** makes configuration changes to the nodes, switch ports, virtual machine managers, and PowerFlex to unconfigure those components. Also, it returns the components to the available inventory.
   - **Remove Resource Group** removes deployment information, but does not make any configuration changes to the nodes, switch ports, virtual machine managers, and PowerFlex. Also, it returns the components to the available inventory.
5. If you choose **Remove Resource Group**, perform the following steps:
   a. To keep the nodes in the inventory, select **Leave nodes in PowerFlex Manager inventory and set state to** and select the state:
      - **Managed**
      - **Unmanaged**
      - **Reserved**
   b. To remove the nodes, select **Remove nodes from the PowerFlex Manager inventory**.
   c. Click **Remove**.
6. If you choose **Delete Resource Group**, perform the following steps:
   a. Select **Delete Clusters(s) and Remove from vCenter** to delete and remove the clusters from vCenter.
   b. Select **Remove Protection Domain and Storage Pools from PowerFlex** to remove the protection domain and storage pools that are created during the resource group deployment.

      If you select this option, you must select the target PowerFlex gateway. The PowerFlex gateway is not removed. PowerFlex Manager removes only the protection domain and storage pools that are part of the resource group. If multiple resource groups are sharing a protection domain, you might not want to delete the protection domain.

      For a compression enabled resource group, PowerFlex Manager deletes the acceleration pool and the DAX devices when you delete the resource group.

   c. Select **Delete Machine Group and remove from CloudLink Center** to clean up the related components in CloudLink Center.

CloudLink Center cleanup includes the deletion of the machine group, keystore, and approved network that is related to the resource group being deleted. These components are removed from CloudLink Center only if all the machines that are associated to the machine group are deleted first. If all the machines that are related to this machine group are not removed, the cleanup does not succeed as there are machines associated with the machine group.

d. If you are certain that you want to proceed, type **DELETE RESOURCE GROUP**.
e. Click **Delete**.

Related information

Deploying a resource group

Canceling a resource group

Canceling a resource group stops a scheduled/pending, or in-process resource group deployment. After canceling a resource group, you can update the content and retry the deployment later.

1. On the menu bar, click **Lifecycle** > **Resource Groups**.
2. Select a resource group that is in **In Progress** or **Pending state**.
3. On the **Resource Group Details** page, click **Cancel** under **More Actions**.
4. On the **Cancel Deployment** page, click **Cancel Deployment**.

   You cannot cancel existing resource groups or resource groups that are used for managing the firmware.

   When you cancel a deployment, a banner displays at the top of the screen that displays a warning.

Preparing a template for a resource group deployment

This section includes tasks for preparing a template that will be used to deploy a set of infrastructure resources in a resource group.

A template is an object in PowerFlex Manager that represents resource types and their required configuration and topology. A template specifies requirements for the deployment of a set of infrastructure resources through PowerFlex Manager's automation workflows.

On the **Templates** page, you can access the default sample templates or create templates that meet your specific requirements. For most environments, you can clone one of the sample templates that are provided with PowerFlex Manager and edit as needed. Choose the sample template that is most appropriate for your environment.

PowerFlex Manager allows you to create templates that support hyperconverged, storage-only, and compute-only resource group deployments.

After you create a template, PowerFlex Manager saves the template in a draft state. You must publish the template before deploying it.

Lifecycle administrators can view and use only those templates for which they have been granted permission by a super user.

Related information

Deploying and provisioning

Basic tasks

This section provides basic tasks for template management.

Clone a template

The **Clone** feature allows you to copy an existing template into a new template. A cloned template contains the components that existed in the original template. You can edit it to add additional components or modify the cloned components.

For most environments, you can simply clone one of the sample templates that are provided with PowerFlex Manager and edit as needed. Choose the sample template that is most appropriate for your environment.

To clone an existing template:

1. On the menu bar, click **Templates**.
2. Open a template, and then click **More Actions** > **Clone** in the right pane.

   You can also click **Clone** on the **My Templates** page if you want to clone one of your own templates, rather than one of the sample templates.

3. In the **Clone Template** dialog box, enter a template name in the **Template Name** box.
4. Select a template category from the **Template Category** list. To create a template category, select **Create New Category**.
5. In the **Template Description** box, enter a description for the template.
6. To specify the version to use for compliance, select the version from the **Firmware and Software Compliance** list or choose **Use PowerFlex Manager appliance default catalog**.

   You cannot select a minimal compliance version for a template, since it only includes server firmware updates. The compliance version for a template must include the full set of compliance update capabilities. PowerFlex Manager does not show any minimal compliance versions in the **Firmware and Software Compliance** list.

7. Indicate **Who should have access to the resource group deployed from this template** by selecting one of the following options:
   - To restrict access to super users, select **Only PowerFlex SuperUser**.
   - To grant access to super users and some specific lifecycle administrators and drive replacers, select the **PowerFlex SuperUser and specific LifecycleAdmin and DriveReplacer** option, and perform the following steps:
     a. Click **Add User(s)** to add one or more LifecycleAdmin or DriveReplacer users to the list displayed.
     b. Select which users will have access to this resource group.
     c. To delete a user from the list, select the user and click **Remove User(s)**.
     d. After adding the users, select or clear the check box next to the users to grant or block access.
   - To grant access to super users and all lifecycle administrators and drive replacers, select **PowerFlex SuperUser and all LifecycleAdmin and DriveReplacer**.
8. Click **Next**.
9. On the **Additional Settings** page, provide new values for the **Network Settings**, **OS Settings**, **Cluster Settings**, **PowerFlex Gateway Settings**, and **Node Pool Settings**.

   If you clone a template that has a **Target CloudLink Center** setting, the cloned template shows this setting in the **Original Target CloudLink Center** field. Change this setting by selecting a new target for the cloned template in the **Select New Target CloudLink Center** setting.

   When defining a template, you choose a single CloudLink Center as the target for the deployed resource group. If the CloudLink Center for the resource group shuts down, PowerFlex Manager loses communication with the CloudLink Center. If the CloudLink Center is part of a cluster, PowerFlex Manager moves to another CloudLink Center when you update the resource group details.

10. Click **Finish**.

Related information

Configuring block storage

Add a template

The **Create** feature allows you to create a template, clone the components of an existing template into a new template, or import a pre-existing template.

For most environments, you can simply clone one of the sample templates that are provided with PowerFlex Manager and edit as needed. Choose the sample template that is most appropriate for your environment.

1. On the menu bar, click **Templates**.
2. On the **Templates** page, click **Create**.
3. In the **Create** dialog box, select one of the following options:
   - **Clone an existing PowerFlex Manager template**
   - **Upload External Template**
   - **Create a new template**

If you select **Clone an existing PowerFlex Manager template**, select the **Category** and the **Template to be Cloned**. The components of the selected template are in the new template.

- For software-only block storage, ensure that you select a template that includes **`SW Only`** in its name.
- For software-only file storage, ensure that you select a template that includes **`File-SW Only`** in its name.

4. Enter a **Template Name**.
5. From the **Template Category** list, select a template category. To create a category, select **Create New Category** from the list.
6. Enter a **Template Description** (optional).
7. To specify the version to use for compliance, select the version from the **Firmware and Software Compliance** list or choose **Use PowerFlex Manager appliance default catalog**.

   You cannot select a minimal compliance version for a template, since it only includes server firmware updates. The compliance version for a template must include the full set of compliance update capabilities. PowerFlex Manager does not show any minimal compliance versions in the **Firmware and Software Compliance** list.

   NOTE: Changing the compliance version might update the firmware level on nodes for this resource group. Firmware on shared devices will still be maintained by the global default firmware repository.

8. Specify the resource group permissions for this template under **Who should have access to the resource group deployed from this template?** by performing one of the following actions:
   - To restrict access to super users, select **Only PowerFlex SuperUser**.
   - To grant access to super users and some specific lifecycle administrators and drive replacers, select the **PowerFlex SuperUser and specific LifecycleAdmin and DriveReplacer** option, and perform the following steps:
     a. Click **Add User(s)** to add one or more LifecycleAdmin or DriveReplacer users to the list displayed.
     b. Select which users will have access to this resource group.
     c. To delete a user from the list, select the user and click **Remove User(s)**.
     d. After adding the users, select or clear the check box next to the users to grant or block access.
   - To grant access to super users and all lifecycle administrators and drive replacers, select **PowerFlex SuperUser and all LifecycleAdmin and DriveReplacer**.
9. Click **Next** to select the remaining options to complete the wizard.

Build and publish a template

After creating a template using the **Create** feature, you use the template builder page to build and publish the customized template. Publishing a template indicates that a template is ready for deployment.

1. Click **Modify Template**.
2. To add a component type to the template, click **Add Node**, **Add Cluster**, or **Add VM** at the top of the template builder.

   The corresponding **<component type> component** dialog box appears.
3. If you are adding a node, choose one of the following network automation types:
   - **Full Network Automation**
   - **Partial Network Automation**

   When you choose **Partial Network Automation**, PowerFlex Manager skips the switch configuration step, which is normally performed for a resource group with **Full Network Automation**. Partial network automation allows you to work with unsupported switches. However, it also requires more manual configuration before deployments can proceed successfully. If you choose to use partial network automation, you give up the error handling and network automation features that are available with a full network configuration that includes supported switches.

   In the **Number of Instances** box, provide the number of component instances that you want to include in the template.
4. If you are adding a cluster, in the **Select a Component** box, choose one of the following cluster types:
   - **PowerFlex Cluster**
   - **VMware Cluster**
   - **PowerFlex File Cluster**
5. If you are adding a VM, in the **Select a Component** box, choose one of the following cluster types:
   - **CloudLink Center**
   - **PowerFlex Gateway**
6. Under **Related Components**, perform one of the following actions:

- To associate the component with all existing components, click **Associate All**.
- To associate the component with only selected components, click **Associate Selected** and then select the components to associate.

Based on the component type, specific settings and properties appear automatically that are required and can be edited.

7. Click **Save** to add the component to the template builder.
8. Repeat steps 1 through 6 to add additional components.
9. After you finish adding components to your template, click **Publish Template**.

   A template must be published to be deployed. It remains in draft state until published.

   After publishing a template, you can use the template to deploy a resource group on the **Resource Groups** page.

Related information

Support for full and partial network automation
Deploying a resource group

Edit a template

You can edit an existing template to change its draft state to "published" for deployment or to modify its components and their properties.

1. On the menu bar, click **Templates**.
2. Open a template, and click **Modify Template**.
3. Make changes as required to the settings for components within the template.

   Based on the component type, required settings and properties are displayed automatically. You can edit these settings by performing these steps:

   PowerFlex Manager facilitates sending the active RCM version to the Data Items portal. The compliance file includes the RCM and intelligent catalog (IC). When multiple resource groups run on different compliance files besides the default PowerFlex Manager compliance file, all the active and default RCM and IC versions are sent to the Data Items portal. If PowerFlex Manager is not managing any resource groups, then the default RCM of PowerFlex Manager is sent to the data items section of the Embedded SupportAssist Enabler. By default, this information is sent every Saturday at 02:00 AM UTC.

   NOTE: If an RCM associated with the template is modified, a wrench icon with the text, Modified, is displayed. However, if the update file is moved or deleted, the wrench icon with the text, Needs Attention, is displayed.

   a. To edit PowerFlex cluster settings, select the **PowerFlex Cluster** component and click **Modify**. Make the necessary changes and click **Save**.
   b. To edit the VMware cluster settings, select the **VMware Cluster** component and click **Modify**. Make the necessary changes, and click **Save**.
   c. To edit node settings, select the **Node** component and click **Modify**. Make the necessary changes, and click **Save**.
4. Optionally, click **Publish Template** to make the template ready for deployment.

Related information

Component types

Edit template information

To edit information for a template, perform the following steps:

1. On the menu bar, click **Templates**.
2. On the **Templates** page, click the template that you want to edit and click **Modify Template** in the right pane.
3. On the template builder page, in the right pane, click **Modify**.
4. In the **Modify Template Information** dialog box, enter a template name in the **Template Name** field.
5. Select a template category from the **Template Category** list. To create a template category, select **Create New Category**.
6. In the **Template Description** box, enter a description for the template.
7. To specify the version to use for compliance, select the version from the **Firmware and Software Compliance** list or choose **Use PowerFlex Manager appliance default catalog**.

8. Indicate **Who should have access to the resource group deployed from this template** by selecting one of the following options:
   - To restrict access to super users, select **Only PowerFlex SuperUser**.
   - To grant access to super users and some specific lifecycle administrators and drive replacers, select the **PowerFlex SuperUser and specific LifecycleAdmin and DriveReplacer** option, and perform the following steps:
     a. Click **Add User(s)** to add one or more LifecycleAdmin or DriverReplacer users to the list displayed.
     b. Select which users will have access to this resource group.
     c. To delete a user from the list, select the user and click **Remove User(s)**.
     d. After adding the users, select or clear the check box next to the users to grant or block access.
   - To grant access to super users and all lifecycle administrators and drive replacers, select **PowerFlex SuperUser and all LifecycleAdmin and DriveReplacer**.
9. Click **Save**.

Deploying a resource group

Deployment is the automated process of selecting and configuring specific resource requirements that are outlined in a template using the integrated automation workflows provided with PowerFlex Manager. You cannot use a template that is in a draft state to deploy a resource group. Publish the template before using it to deploy a resource group.

Before you begin, enable LLDP on the switches, and update the inventory in PowerFlex Manager.

1. On the menu bar, click one of the following:
   - **Lifecycle** > **Resource Groups**. Then, click **Deploy New Resource Group**.
   - **Lifecycle** > **Templates**. Then, click **Deploy**.

   The **Deploy Resource Group** wizard opens.
2. On the **Deploy Resource Group** page, perform the following steps:
   a. From the **Select Published Template** list, select the template to deploy a resource group.
   b. Enter the **Resource Group Name** (required) and **Resource Group Description** (optional) that identifies the resource group.
   c. To specify the version to use for compliance, select the version from the **Firmware and Software Compliance** list or choose **Use PowerFlex Manager appliance default catalog**.

      You cannot select a minimal compliance version when you deploy a new resource group, since it only includes server firmware updates. The compliance version for a new resource group must include the full set of compliance update capabilities. PowerFlex Manager does not show any minimal compliance versions in the **Firmware and Software Compliance** list.

      PowerFlex Manager checks the VMware vCenter version to determine if it matches the VMware ESXi version for the selected compliance version. If the ESXi version is greater than the vCenter version, PowerFlex Manager blocks the resource group deployment and displays an error. PowerFlex Manager instructs you to upgrade vCenter first, or use a different compliance version that is compatible with the installed vCenter version.

      NOTE: Changing the firmware repository might update the firmware level on nodes for this resource group. The global default firmware repository maintains the firmware on the shared devices.

   d. Indicate **Who should have access to the resource group deployed from this template** by selecting one of the following options:
      - To restrict access to super users, select **Only PowerFlex SuperUser**.
      - To grant access to super users and some specific lifecycle administrators and drive replacers, select the **PowerFlex SuperUser and specific LifecycleAdmin and DriveReplacer** option, and perform the following steps:
        i. Click **Add User(s)** to add one or more LifecycleAdmin or DriveReplacer users to the list displayed.
        ii. Select which users will have access to this resource group.
        iii. To delete a user from the list, select the user and click **Remove User(s)**.
        iv. After adding the users, select or clear the check box next to the users to grant or block access.
      - To grant access to super users and all lifecycle administrators and drive replacers, select **PowerFlex SuperUser and all LifecycleAdmin and DriveReplacer**.
3. Click **Next**.
4. On the screens that follow the **Deployment Settings** page, configure the settings, as needed for your deployment.
5. Click **Next**.
6. On the **Schedule Deployment** page, select one of the following options and click **Next**:

- **Deploy Now**—Select this option to deploy the resource group immediately.
- **Deploy Later**—Select this option and enter the date and time to deploy the resource group.

7. Review the **Summary** page.
   The **Summary** page gives you a preview of what the resource group will look like after the deployment.
8. Click **Finish** when you are ready to begin the deployment. If you want to edit the resource group, click **Back**.

Related information

Lifecycle
Viewing resource group details
Adding components to a resource group
Build and publish a template
Component types
Removing a resource group

Additional template management tasks

This section provides additional tasks for template management.

Add cluster component settings to a template

To deploy a PowerFlex compute-only node or a PowerFlex hyperconverged node, you must add VMware and PowerFlex cluster components settings to a template. For a PowerFlex storage-only node deployment, you must add cluster settings for the PowerFlex cluster component only. For a PowerFlex file deployment, you must add cluster settings for the PowerFlex file cluster component.

1. On the template builder page, click **Add Cluster**.
2. In the **Cluster Component** dialog box, from the **Select a Component** list, select **VMware cluster**, **PowerFlex Cluster**, or **PowerFlex File Cluster**.
3. Under **Related Components**, select the components that you want to map to the selected cluster instance.
4. Click **Continue**.
5. Under **Cluster Settings**, specify the settings that you want to configure on the cluster components and click **Add**.

Related information

Cluster component settings

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.

Add a new static route

Use the **Add New Static Route** feature to create a static route in a template.

A static route allows nodes to communicate across different networks. The static route can also be used to support replication in storage-only and hyperconverged resource groups.

1. On the node component page, under **Network Settings**, click **Enabled** under **Static Routes**.
2. Click **Add New Static Route**.
3. Enter the following information for the static route:
   - **Source Network**—Select the PowerFlex data network or replication network that is the source.

     If you add or remove a network for a port, the **Source Network** list still shows the old networks. In order to see the changes, you must save the node settings and edit the node again.
   - **Destination Network**—Select the PowerFlex data network or replication network that is the destination for the static route.
   - **Gateway**—Enter the IP address for the gateway.

Configure VDS settings

Use the **Configure VDS Settings** feature to create the virtual distributed switch (VDS) settings for the VMware cluster component in a template.

You can specify the port group names or have PowerFlex Manager specify them for you.

1. On the VMware cluster component page, under **vSphere VDS Settings**, click **Configure VDS Settings**.
2. To specify the port group names, click **User Entered Port Groups** and click **Next**:
   a. Provide the name for each VDS under **VDS Naming**.
      For each VDS, click **Create VDS...** and type the VDS name.
   b. Click **Next**.
   c. On the **Port Group Select** page, for each VDS, click **Create Port Group...** and type the port group name. Initially, the port group name defaults to the name of the network, but you can type over the default to suit for your requirements.
      Alternatively, you can click **Select** and choose an existing port group.
   d. Click **Next**.
3. To have PowerFlex Manager assign the port group names for you, click **Auto Create All Port Groups** and click **Next**:

   PowerFlex Manager determines the VDS order based on the following criteria:
   a. PowerFlex Manager first considers the number of port groups on each VDS.
   b. PowerFlex Manager considers whether a management port group is present on a particular VDS.
   c. PowerFlex Manager considers the network type for port groups on a VDS.

d. PowerFlex Manager considers the network name for port groups on a VDS.

a. Provide the name for each VDS under **VDS Naming**.

   For each VDS, click **Create VDS...** and type the VDS name.

b. Click **Next**.

c. On the **Port Group Select** page, review the port group names automatically assigned for the networks.

d. Click **Next**.

4. On the **Advanced Networking** page, optionally change the **MTU Size** for the Hypervisor Management and vMotion networks.

   PowerFlex Manager allows you to select 1500 or 9000 as the setting for either network. The default setting for the Hypervisor Management network is 1500. The default setting for the vMotion network is 9000.

5. Review the settings on the **Summary** page and click **Finish**.

View template details

View more details about the topology of the components in the template builder.

1. On the **Templates** page, select a template.
2. In the right pane, click **View Details**.
3. To view all the component settings, click **More Actions** > **View All Settings** in the right pane.

   The **Template Settings** page shows each top-level component on a separate tab. Click a tab for a component to see the details for the component.

   NOTE: If an RCM is mapped to the template and is modified, a wrench icon with the text, "Modified", is displayed. However, if the update file is moved or deleted, the wrench icon with the text, "Needs Attention", is displayed.

Related information

Component types

Export a template

To export a template:

1. On the menu bar, click **Templates**.
2. Select the template that you want to export.
3. Click **Export**.
4. In the **Export Template to ZIP File** window, enter values as follows:
   a. Enter a name for the template file in the **File Name**.
   b. If you have set an encryption password, select **Use Encryption Password from Backup Setting** to use that password. To set an encryption password, clear this option.
   c. If you clear **Use Encryption Password from Backup Setting**, two additional fields display. Enter a new password in the **Set File Encryption Password** field and enter the password again to confirm it.
5. Click **Export** to download the file. Select a location to save the file and click **OK**.

Import a template

The **Import Template** feature allows you to import the components of an existing template and its component configurations into a template. For example, you can create a template that defines a specific cluster and node topology and import this template definition into another template. After importing, you can modify the component properties of the imported components.

Editing an imported template does not affect the original template.

As an alternative to this procedure, you can also start from a new template and import an existing template as you create it. This is a better approach to use. To do this, you select **Create**, then choose **Clone an existing VxFlex Manager template** in the wizard.

To import a template, perform the following steps:

1. On the menu bar, click **Templates**.
2. On the **Templates** page, select the template into you want to import an existing template and click **Edit** in the right pane.
3. On the **Template Builder** page, in the right pane, click **Import Template**.
4. In the **Import Template** dialog box, select a specific template from the **Select a template** list and click **Import**.

Upload an external template

To upload a template, perform the following steps:

1. On the **Templates** page, click **Create**.
2. In the **Create** dialog box, select **Upload External Template**.
   The **Upload External Template** page appears.
3. Click **Browse** to select the exported file from your directory.
4. Select the **Use Encryption Password from Backup Settings** check box, if you have set the encryption password in **Backup and Restore**.

   Clear the **Use Encryption Password from Backup Settings** check box if you have not set the encryption password in **Backup and Restore**.

   If you clear the **Use Encryption Password from Backup Settings**, you must enter the encryption password in the **Encryption Password** field.
5. Enter the template name in the **Template Name** field.
6. Select a template category from the **Template Category** list.

   If you want to create a template category, select **Create New Category**.
7. In the **Template Description** box, enter a description for the template.
8. To specify the version to use for compliance, select the version from the **Firmware and Software Compliance** list or choose **Use PowerFlex Manager appliance default catalog**.

   NOTE: Changing the firmware repository might update the firmware level on nodes for this resource group. Firmware on shared devices is maintained by the global default firmware repository.
9. Indicate **Who should have access to the resource group deployed from this template** by selecting one of the following options:
   - To restrict access to super users, select **Only PowerFlex SuperUser**.
   - To grant access to super users and some specific lifecycle administrators and drive replacers, select the **PowerFlex SuperUser and specific LifecycleAdmin and DriveReplacer** option, and perform the following steps:
     a. Click **Add User(s)** to add one or more LifecycleAdmin or DriverReplacer users to the list displayed.
     b. Select which users will have access to this resource group.
     c. To delete a user from the list, select the user and click **Remove User(s)**.
     d. After adding the users, select or clear the check box next to the users to grant or block access.
   - To grant access to super users and all lifecycle administrators and drive replacers, select **PowerFlex SuperUser and all LifecycleAdmin and DriveReplacer**.
10. Click **Upload and Continue**.
    The **Additional Settings** page appears.
11. On the **Additional Settings** page, provide new values for the **Network Settings**, **OS Settings**, **Cluster Settings**, **PowerFlex Gateway Settings**, and **Node Pool Settings**.
12. Click **Finish**.

Deploy a CloudLink Center

Use this task to deploy a CloudLink Center. Although PowerFlex Manager supports up to three instances of CloudLink Center, two are recommended.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

Ensure the following:

- Hypervisor management or PowerFlex management networks are added to PowerFlex Manager.
- A VMware vCenter with a valid data center, cluster, network, and datastore is discovered.
- The system has the following resources:

Compliance file version	vCPU	VRAM (GB)	Disk space (GB)
3.5.1	4	6	64

1. On the menu bar, click **Templates** > **Sample Templates**.
2. On the **Sample Templates** page, click **Management - CloudLink Center**.
3. Click **More Actions** > **Clone**.
4. In the **Clone Template** wizard, do the following:
   a. Enter a template name.
   b. From the **Template Category** list, select a template category. To create a category, select **Create New Category** from the list.
   c. Enter a **Template Description** (optional).
   d. To specify the version to use for compliance, select the version from the **Firmware and Software Compliance** list or choose **Use PowerFlex Manager appliance default catalog**.
   e. Specify the resource group permissions for this template under **Who should have access to the resource group deployed from this template?**:
      - To restrict access to super users, select **Only PowerFlex SuperUser**.
      - To grant access to super users and some specific lifecycle administrators and drive replacers, select the **PowerFlex SuperUser and specific LifecycleAdmin and DriveReplacer** option, and perform the following steps:
        i. Click **Add User(s)** to add one or more LifecycleAdmin or DriverReplacer users to the list displayed.
        ii. Select which users will have access to this resource group.
        iii. To delete a user from the list, select the user and click **Remove User(s)**.
        iv. After adding the users, select or clear the check box next to the users to grant or block access.
      - To grant access to super users and all lifecycle administrators and drive replacers, select **PowerFlex SuperUser and all LifecycleAdmin and DriveReplacer**.
   f. Click **Next**.
5. On the **Additional Settings** page, do the following:
   a. Under **Network Settings**, select **Hypervisor Network** (PowerFlex management network).
   b. Under **OS Settings**, select **CLC** credential or click **+** to create a credential with root or CloudLink user.
   c. Under **Cloudlink Settings**, do the following:
      i. Select the secadmin credential from the list or click **+** to create a secadmin credential and do the following:
         i. Enter **Credential Name**.
         ii. Enter **User Name** as **`secadmin`**.
         iii. Leave the **Domain** empty.
         iv. Enter the password for **`secadmin`** in **Password** and **Confirm Password**.
         v. Select **V2** in **SNMP Type**.
         vi. Click **Save**.
      ii. Select a license file from the list based on the types of drives or click **+** to upload a license through the **Add Software License** page.
      NOTE: For SSD/NVMe drives, upload a capacity-based license. For SED drives, upload an SED-based license.
   d. Under **Cluster Settings**, select **Management vCenter**.
   e. Click **Finish**.
6. Select the **VMware Cluster** and click **Edit** > **Continue**.
   a. Under **Cluster Settings**, select **Datacenter Name**, and then select **Cluster Name** from the drop-down list.
   b. Under **vSphere Network Settings**, select the hypervisor management port group or PowerFlex management port group.
   c. Click **Save**.

   NOTE: To deploy a CloudLink Center from PowerFlex Manager, you need a Management vCenter, Datacenter, and Cluster along with DvSwitch port groups for PowerFlex management or hypervisor management.

7. Select the **VM** and click **Edit** > **Continue** (by default, the number of CloudLink instances is two and PowerFlex Manager supports up to three instances).
   a. Under **VM Settings** select the **Datastore** and **Network** from the drop-down list.
   b. Under **Cloudlink Settings** select the following:
      i. For **Host Name Selection**, either select **Specify At Deployment Time** to manually enter at deployment time or **Auto Generate** to have PowerFlex Manager generate the name.

ii. Enter the vault passwords.

NOTE: Other details such as OS credentials, NTP, and secadmin credentials are auto populated.

8. Under **Additional Cloudlink Settings**, you can choose either or both of the following settings:
   - **Configure Syslog Forwarding**
     a. Select the check box to configure syslog forwarding.
     b. For **Syslog Facility**, select the **syslog** remote server from the list.
   - **Configure Email Notifications**
     a. Select the check box to configure email alerts.
     b. Specify the IP address of the email server.
     c. Specify the port number for the email server. The default port is 25. Enter the port numbers in a comma-separated list, with values between 1-65535.
     d. Specify the email address for the sender.
     e. Optionally, specify the username and password.
9. Click **Save**.
10. Click **Publish Template** and click **Yes** to confirm.
11. In the **Deploy Resource Group** wizard, do the following:
    a. Select the published template from the drop-down list, and enter **Resource Group Name** and description.
    b. Select who should have the access to the resource group and click **Next**.
    c. Provide **Hostname** and click **Next**.
    d. Select **Deploy Now** or **Schedule deployment** and click **Next**.
    e. Review the details in **Summary** page and click **Finish**.

Deploy the PowerFlex file cluster

Perform this task to deploy the PowerFlex file cluster.

Deploy a storage-only or hyperconverged resource group that includes a PowerFlex cluster that will be associated with the PowerFlex file cluster. When you deploy the PowerFlex file cluster, the control volumes that are needed for file enablement will be added automatically.

1. On the menu bar, click **Templates**.
2. On the **Templates** page, click **Create**.
3. In the **Add a Template** wizard, click **Clone an existing PowerFlex Manager template**.
4. For **Category**, select **Sample Templates**. For **Template to be Cloned**, select **PowerFlex File** or **PowerFlex File - SW Only**. Click **Next**.
5. On the **Template Information** page, provide the template name, template category, template description, firmware and software compliance, and who should have access to the resource group deployed from this template. Click **Next**.
6. On the **Additional Settings** page, enter new values for the **Network Settings**, **PowerFlex Gateway Settings**, **OS Settings**, and **Node Pool Settings**.

   For the **Network Settings** in a PowerFlex file cluster template, you must provide a **NAS Management** network and two **NAS Data** networks.

   For the **OS Settings**, you must choose **Use Compliance File Linux Image**.

   For the **PowerFlex Gateway Settings**, select **block-legacy-gateway**.

7. Click **Finish**.
8. After creating the template, click **Templates**, select the cloned template, and click **Modify Template**.
9. Edit the PowerFlex cluster, PowerFlex file cluster, and node components as needed and click **Save**.
10. Publish the template and deploy the resource group.

NAS volumes are shown during the deployment, and then compressed to one icon with a number based on the number of nodes. For example, you might see the number **4** for a two-node NAS compute-only deployment. Each time you expand the deployment by adding another node, the number is incremented to show that another volume is added.

Related information

Configuring file storage

Cluster settings for the PowerFlex cluster

This table describes the most important cluster settings for the PowerFlex cluster in a NAS deployment.

Setting	Description
Target PowerFlex Gateway	Choose the block-legacy-gateway.

Cluster settings for the PowerFlex file cluster

This table describes the most important cluster settings for the PowerFlex file cluster.

Setting	Description
PowerFlex File Gateway	Name of the PowerFlex file gateway.
Number of Protection Domains	Number of protection domains you want to use in this template.
Protection Domain <n>	One or more protection domains provided by the PowerFlex cluster deployed as part of the storage-only or hyperconverged resource group. This setting will be empty if you have not yet deployed the storage-only or hyperconverged resource group.
Storage Pool <n>	One or more storage pools provided by the PowerFlex cluster deployed as part of the storage-only or hyperconverged resource group. This setting will be empty if you have not yet deployed the storage-only or hyperconverged resource group.

Node settings (PowerFlex file template)

This table describes the most important node settings for the **PowerFlex File** template.

Setting	Description
Number of Instances	For a PowerFlex file cluster, you must have a minimum of two nodes and a maximum of 16 nodes. When you deploy a NAS template, PowerFlex Manager automatically creates control volumes for the deployment. Two of the volumes are common and are mapped to every node (one for the NAS cluster and the other for the Postgres cluster). The other volumes (SVDM volumes) are mapped separately to each of the nodes added. The control volumes are special NAS cluster volumes that cannot be deleted or modified. These control volumes are hidden from view in the management software appliance.
Related Components	Choose **All Components**.
OS Settings: OS Image	For a PowerFlex file cluster, you must choose **Use Compliance File Linux Image**.
OS Settings: PowerFlex Role	Choose **Compute Only**.
OS Settings: Enable PowerFlex File	This option must be selected for NAS.
OS Settings: Switch Port Configuration	Choose **Port Channel (LACP Enabled)** or **Trunk Port**. **Port Channel (LACP Enabled)** is the preferred option. **Port Channel** is not supported with this template.

Setting	Description
OS Settings: Teaming and Bonding Configuration	Choose **Mode 4 (IEEE 802.3ad policy)** for **Port Channel (LACP Enabled)**.
Hardware Settings: Target Boot Device	Choose **Local Hard Drive**.
Network Settings	The PowerFlex file template pulls in the PowerFlex management and PowerFlex data networks from the associated PowerFlex gateway. To ensure that the PowerFlex file resource group works properly, you need to deploy a storage-only or hyperconverged resource group first that includes the target gateway. In addition to the PowerFlex management and PowerFlex data networks, you need to include a NAS management network and at least one NAS data network. One NAS data network is enough, but, for redundancy, two networks are recommended. By default, the template includes two interfaces with two ports on each interface. The second interface mirrors the first interface.

Node settings (PowerFlex File-SW Only template)

This table describes the most important node settings for the **PowerFlex File-SW Only** template.

Setting	Description
Number of Instances	For a PowerFlex file cluster, you must have a minimum of 2 nodes and a maximum of 16 nodes. Software-only NAS nodes also need to be discovered with a resource type of **Node (Software Management)**. The operating system has to be installed and configured manually for each software-only node. The software-only nodes must also have base networking configured. PowerFlex Manager takes care of provisioning the NAS application-level components on top of the operating system. When you deploy a PowerFlex File-SW Only template, PowerFlex Manager automatically creates control volumes for the deployment. Two of the volumes are common and are mapped to every node (one for the NAS cluster and the other for the Postgres cluster). The other volumes (SVDM volumes) are mapped separately to each of the nodes added. The control volumes are special NAS cluster volumes that cannot be deleted or modified. These control volumes are hidden from view in the management software appliance.
Related Components	Choose **All Components**.
OS Settings: OS Image	For a PowerFlex file cluster, you must choose **Use Compliance File Linux Image**.
OS Settings: PowerFlex Role	Choose **Compute Only**.
OS Settings: Enable PowerFlex File	This option must be selected for NAS.
OS Settings: Switch Port Configuration	Choose **Port Channel (LACP Enabled)** or **Trunk Port**. **Port Channel (LACP Enabled)** is the preferred option. **Port Channel** (standard port channel with LACP disabled) is not supported with this template.

Setting	Description
OS Settings: Teaming and Bonding Configuration	Choose **Mode 4 (IEEE 802.3ad policy)** for **Port Channel (LACP Enabled)**.
Network Settings	The PowerFlex File-SW Only template pulls in the PowerFlex management and PowerFlex data networks from the associated PowerFlex gateway. To ensure that the PowerFlex file resource group works properly, you need to deploy a storage-only or hyperconverged resource group first that includes the target gateway. In addition to the PowerFlex management and PowerFlex data networks, you need to include a NAS management network and at least one NAS data network. One NAS data network is enough, but, for redundancy, two networks are recommended. By default, the software-only template includes six interfaces with a single network VLAN on each interface. These interfaces could be for six physical NICs, or for a single physical NIC. For a software-only deployment, the interfaces do not have a one-to-one relationship with the physical NIC ports. In the case of a software-only deployment, PowerFlex Manager does not know about the physical NICs. It only knows about the networks in the operating system.

Deploy software management

You can deploy software management on an existing node through PowerFlex Manager. First, PowerFlex Manager discovers the node with the operating system installed and the networking that is configured. Then, PowerFlex Manager installs PowerFlex on the node and configures the protection domain and the storage pool. The SDS and SDS devices are added to the storage pool.

Software management supports the following features:

- Deployment, expansion, and removal of PowerFlex storage-only nodes (storage data server (SDS)/Storage Data Target (SDT) Only) (includes installation of the MDM cluster)
- Deployment, expansion, and removal of PowerFlex hyperconverged nodes (SDS and SDC) (includes installation of the MDM cluster)
- Deployment, expansion, and removal of PowerFlex compute-only node (SDC Only)
- Update of PowerFlex packages on the PowerFlex nodes
- Hard Disk Drives (HDD)
- Solid State Drives (SDD)
- NVMe
- Replication
- Compression
- Ability to configure the MDM cluster
- Ability to reconfigure the MDM roles

Before you deploy a software management node, complete the list of prerequisites which are detailed in the deployment checklist for software management.

You can choose to build a software management template or clone an existing template. Once the template is published, you can deploy the software management resource group.

Related information

Deployment checklist for software management
Building a software management template
Node settings (software management)
Sample templates
Discover a software management node

Deployment checklist for software management

There are compute, storage, and networking deployment requirements that must be met to deploy a software management node.

<table>
<tr><th></th><th colspan="3">Item</th><th>Checked</th></tr>
<tr><td>1</td><td colspan="3">There is a supported operating system that is installed on any hardware, for example, a VM or a server.</td><td></td></tr>
<tr><td>2</td><td colspan="3">There is at least one free 100 GB drive with no partitions (required for PowerFlex storage-only nodes and PowerFlex hyperconverged nodes only).</td><td></td></tr>
<tr><td>3</td><td colspan="3">There are no PowerFlex packages preinstalled.</td><td></td></tr>
<tr><td>4</td><td colspan="3">The networks are configured including any static routes.</td><td></td></tr>
<tr><td>5</td><td colspan="3">Any repository that is configured should be functional.</td><td></td></tr>
<tr><td>6</td><td colspan="3">The firewall is enabled and the SSH port is open.</td><td></td></tr>
<tr><td>7</td><td colspan="3">The root user is configured in the software management node operating system, and the OS Admin user with root credentials are configured in PowerFlex Manager.</td><td></td></tr>
<tr><td>8</td><td colspan="3">There must be at least one network that is configured in the software management node operating system that PowerFlex Manager can reach. In addition, there is a minimum of one PowerFlex data type network that must be configured in PowerFlex Manager, and added to a software management template.

ⓘ NOTE: When creating a PowerFlex data network to be used with a software management node and resource group, the VLAN is optional, but is still a required parameter to create the network. If no VLAN is configured on the network, then enter 1 for this value.</td><td></td></tr>
<tr><td>9</td><td colspan="3">The software management node requires access to the PowerFlex Manager HTTP share:

<code>https://[external_loadbalancer_ip_address]/httpshare/download/</code></td><td></td></tr>
<tr><td rowspan="4">10</td><td colspan="3">The following operating system dependent packages are already installed:</td><td rowspan="4"></td></tr>
<tr><td>Operating system</td><td>Package type</td><td>Package name</td></tr>
<tr><td rowspan="2">Centos
Oracle Enterprise Linux (OEL)
Red Hat Enterprise Linux</td><td>Normal</td><td>numactl
libaio1
wget
apr
java-11-openjdk-headless
python2-rpm or python3-rpm
yum-utils</td></tr>
<tr><td>With compression</td><td>ndctl</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">SUSE Linux Enterprise Server (SLES)</td><td>Normal</td><td>numactl
libaio1
wget
libapr1
java-11-openjdk-headless
python2-rpm or python3-rpm</td><td rowspan="2"></td></tr>
<tr><td>With compression</td><td>ndctl</td></tr>
<tr><td></td><td>Ubuntu</td><td>Normal</td><td>numactl
libaio1
wget
libapr1</td><td></td></tr>
</table>

	Item			Checked
			• *java-11-openjdk-headless*	
		With compression	*ndctl*	

Related information

Deploy software management
Deploy a software management node

Building a software management template

You can choose to build a software management template instead of cloning one of the existing templates. The template builder allows you to build a customized template by configuring both physical and virtual components.

As a PowerFlex Manager superuser, you can deploy software management on four PowerFlex hyperconverged nodes with compression and replication that is enabled on the nodes. Each node has one management and one data network. You can restrict access to only PowerFlex super users.

1. From the PowerFlex Manager menu, go to **Lifecycle** > **Templates**.
2. On the **Templates** page, go to **My Templates** > **Create**.
3. Select **Create a new template** and enter a **Template Name**.
   For example, `Deployment 8201`.
4. From the **Template Category** list, select a template category. To create a category, select **Create New Category** from the list.
5. Enter a **Template Description** (optional).
   For example, `Software management hyperconverged four node deployment`.
6. Select **Use PowerFlex Manager appliance default catalog**.
7. To restrict access to super users, select **Only PowerFlex SuperUser** under **Who should have access to the resource group deployed from this template?**.
8. Click **Save**.
9. Click **Add Node**.
10. From the **Select a Component** menu, select **Node (Software only)**.
11. From the **Number of instances**, enter `4` and click **Continue**.
12. From the **OS Settings** pane, complete the following:
    a. From the **Operating System** menu, select the **Suse Enterprise Linux** option.
    b. Select the check box for **Use Node For Dell PowerFlex**.
    c. From **PowerFlex Role**, select **Hyperconverged**.
    d. Select the check box for **Enable Compression**.
    e. Select the check box for **Enable Replication**.
13. From the **Node Settings** pane, select **Global** from the **Node Pool** menu.
14. From the **Network Settings** pane, complete the following steps:
    a. Click **Add New Interface**.
    b. Click **Choose Networks**. The **Interface 1 Port 1 Network Configuration** page opens.
    c. Select **Add Networks to this Port**.
    d. From the **Available Networks** list, select the check box for the management network that you want to add to the **Selected Networks** list.
    e. From the **Available Networks** list, select the check box for the data network that you want to add to the **Selected Networks** list.
    f. Click **Save**.
15. Click **Validate Settings**.

Related information

Deploy software management

Discover a software management node

PowerFlex Manager must discover a software management node in order to manage it.

Ensure the following:

- The root user credentials must be configured in PowerFlex Manager. You must create an **OS Admin** user credential in order to discover a node with the root user credentials.
- The networking must include one PowerFlex data network and at least one management network, or the data network must be reachable through PowerFlex Manager.

1. From the PowerFlex Manager menu, click **Resources** > **Discover Resources**.
   The **Discover Wizard** opens.
2. Click **Next**.
3. Click **Add Resource Type** and complete the following:
   a. From the **Resource Type** menu, select **Node (Software Management)**.
   b. Enter the IP address in the **IP/Hostname Range** field.
   c. Select **Managed** from the **Resource State** menu.
   d. Select **Global** from the **Discover into Node Pool** menu.
4. Select the **OS Admin** credential from the **Credentials** menu or create the **OS Admin** credential. To create a credential, click the **+** sign to the right of the **Credentials** box.
5. Click **Next.**

Related information

Deploy software management

Deploy a software management node

Deploying a software management resource group enables you to install and configure PowerFlex components on a set of nodes where an existing operating system is already installed.

Ensure the following:

- A software catalog is installed in PowerFlex Manager.
- A compatibility file is installed in PowerFlex Manager.
- For the initial deployment of PowerFlex storage, a minimum of three nodes is required.
- The deployment checklist for software management is complete, because these prerequisites are the basis upon which filtering is carried out.

IP addresses are already configured on software management nodes. When a resource group is deployed, the IP addresses that are found on the software management nodes are reserved within the appropriate PowerFlex networks that were created and added to the template.

If you are deploying a PowerFlex storage-only node or a PowerFlex hyperconverged node where an MDM cluster is created, an IP address is reserved from your networks as a virtual IP address.

1. On the menu bar, click **Templates**.
2. On the **Templates** page, click **Create**.
3. In the **Add a Template** wizard, click **Clone an existing PowerFlex Manager template**.
4. For **Category**, select **Sample Templates**. For **Template to be Cloned**, select the template and click **Next**.
5. On the **Additional Settings** page, enter new values for the **Network Settings**, **PowerFlex Gateway Settings**, **OS Settings**, and **Node Pool Settings**.
6. Click **Finish**.
7. After creating the template, click **Templates**, select the cloned template, and click **Modify Template**.
8. Edit the node components as needed and click **Save**.
9. Publish the template and deploy the resource group.

Related information

Deployment checklist for software management
Node settings (software management)

Node settings (software management)

This table describes the operating system, node, and network settings for the deployment of a software management node.

Setting	Description	Software management setting option
OS Setting		
Operating System	Specifies the operating system.	Specify one of the following operating systems: • Red Hat Enterprise Linux/CentOS • SUSE Linux Enterprise Server (SLES) • Oracle Enterprise Linux • Ubuntu Linux The server is deployed based on this selection.
Use Node For Dell PowerFlex	Indicates that this node component is used for a PowerFlex deployment.	Select the check box for software only (software management).
PowerFlex Role	Specifies a deployment type	Select one of the following: • **Hyperconverged** • **Compute Only** • **Storage Only**
Enable PowerFlex File	Enables NAS capabilities on the node.	Select or clear the check box.
Client Storage Access	Determines how clients access storage.	For a storage-only role, select one of the following options: • **Storage Data Client (SDC) Only** • **SDC and NVMe/TCP Initiator** For a compute-only role, the **Client Storage Access** control is not displayed, and the client access is set to SDC automatically. For a hyperconverged role, the **Client Storage Access** control is not displayed, and the client access is set to SDC/SDS automatically.
Enable Compression	Enables compression on the protection domain.	Select or clear the check box.
Enable Replication	Enables replication for a storage-only or hyperconverged resource group.	Select or clear the check box.
Node Settings		
Component Name	Indicates the node component name.	Select **Node (Software Only)**.
Number of Instances	Selects the number of instances that you want to add.	If you select more than one instance, a single component representing multiple instances of an identically configured component are created. Edit the component to add extra instances. If you require different configuration settings, you can create multiple components. The limit on the number of instances for software only is 128.
Related Components	Associates all or specific components to the new component.	Select: • **Associate All** • **Associate Selected**

Setting	Description	Software management setting option
Node Pool	Specifies the pool from which nodes are selected for the deployment.	You can select the default **Global** setting from the menu or create one.
Network Settings		
Add New Interface	Creates a network interface where network settings are specified for a node.	Click **Add New Interface**. A minimum of one PowerFlex data network that PowerFlex Manager can reach is required. PowerFlex Manager requires a VLAN to create a network. If there is no VLAN configured on the network, enter **1**. Each network has one interface. The recommendation is to create one interface per IP address that you want PowerFlex Manager to reach.
Validate Settings	Determines what can be chosen for deployment.	Click **Validate Settings** to determine what can be chosen for a deployment with this template component. The **Validate Settings** wizard displays a banner when one or more resources in the template do not match the configuration settings that are specified in the template. The wizard displays the following tabs: • **Valid (*number*)** lists the resources that match the configuration settings. • **Invalid (*number*)** lists the resources that do not match the configuration settings. The reason for the mismatch is shown at the bottom of the wizard. For example, you might see `Network Configuration Mismatch` as the reason for the mismatch if you set the port layout to use a 100-GB network architecture, but one of the nodes is using a 25 GB architecture.

Related information

Deploy a software management node
Deploy software management

Removing a software management resource group

You can remove a software management node that is no longer required. PowerFlex Manager supports both the deletion and removal of a software management resource group.

You can choose to perform either of the following actions:

- Delete the software management resource group, which deletes deployment information and also makes required configuration changes to remove the PowerFlex storage. If you choose the delete option, the PowerFlex packages that are installed during deployment, the PowerFlex repositories that are created during the deployment, and the http share certificates are removed. The operating system and networking are left intact.
- Remove the software management resource group, which removes the deployment information for the software management resource group without making any configuration changes to the deployed components.

If the PowerFlex gateway used in the resource group is being updated on the **Resources** page. PowerFlex Manager also does not allow you to delete a resource group.

If the role you were assigned to at deployment time enables you to deploy resource groups, you can delete the resource groups that you deployed.

1. From the PowerFlex Manager menu, click **Lifecycle** > **Resource Groups**.
2. Select the software management resource group.
3. On the **Resource Group Details** page, under **More Actions**, click **Remove Resource Group**.
4. In the **Remove Resource Group** dialog box, select the **Resource group removal type**.
5. If you choose **Remove Resource Group**, perform the following steps:
   a. To keep the nodes in the inventory, select **Leave nodes in PowerFlex Manager inventory and set state to** and select the state:
      - **Managed**
      - **Unmanaged**
      - **Reserved**
   b. To remove the nodes, select **Remove nodes from the PowerFlex Manager inventory**.
   c. Click **Remove**.

Upgrading a software management node

You can perform a non-disruptive update to a software management node through the PowerFlex gateway on the **Resources** page.

Any packages that are associated with PowerFlex must be installed.

You can only view compliance through the resource group. You cannot make updates through the resource group. Compliance is reflective of compliance with PowerFlex packages only.

1. From the PowerFlex Manager menu, select the **Resources** page.
2. Select the PowerFlex gateway that is non-complaint.
   A **Compliance Report** window opens.
3. Click **Update Resources**.

Delete a template

The **Delete Template** option allows you to delete a template from PowerFlex Manager.

1. On the menu bar, click **Templates**.
2. Select the template that you want to delete. Click **More Actions** > **Delete Template** in the right pane.
3. Click **Yes** to confirm the deletion.

10

Managing resources

This section includes tasks for discovering and managing resources in the PowerFlex Manager inventory.

A resource is a physical and virtual data center object that PowerFlex Manager interacts with, including but not limited to nodes, network switches, VM managers (for example, VMware vCenter), and element managers (for example, CloudLink Center).

The **Resources** page displays detailed information about all the resources and node pools that PowerFlex Manager has discovered and inventoried. You can perform various operations from the **All Resources** and **Node Pools** tabs.

NOTE: Depending upon the number of resources, it might take few minutes to display the discovered resources every time you run the inventory.

The **All Resources** tab displays the following information about the resources that are discovered and managed in PowerFlex Manager:

Field name	Description
Health	Indicates the resource health.
Compliance	Indicates if the resource firmware and software compliance state is **Compliant**, **Non-compliant**, **Update required**, or **Update failed**. Compliance is determined by the firmware/software version for the selected resource, based on the default compliance version. Click the compliance status to view the compliance report.
OS Hostname	Indicates the resource hostname. This capability is available on the PowerFlex appliance and PowerFlex rack offerings only. **NOTE:** PowerFlex Manager retrieves the hostname value from iDRAC and not the operating system. If the hostname field is not updated in iDRAC, an incorrect value might display in PowerFlex Manager. Certain operating systems require additional packages to be installed for iDRAC to update the correct hostname.
Resource Name	Indicates the name of the resource.
Management IP	Indicates the resource IP address. Click the IP address to open the **Element Manager**.
Asset/Service Tag	Indicates the resource service tag. This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.
Deployment Status	Indicates if the resource deployment status is **In Use**, **Not in use**, **Available**, **Updating resource**, or **Pending Updates**. Click the deployment status to view resource group details.
Managed State	Indicates the resource state. If you did not upload a license file in the **Initial Configuration Wizard**, PowerFlex Manager is configured for monitoring and alerting only. All resources are restricted to the **Unmanaged** resource state, and you cannot change the state to **Managed** or **Reserved**.
Model	Indicates the resource manufacturer name and model number.

Field name	Description
	This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

To filter the resources that display, click the toggle filters icon on the **Resource** page.

To filter based on...	Select a value...
Resource Type	• **Element Manager** • **Node (Hardware/Software Management)** • **Switches** • **VM Manager** • **PowerFlex Gateway** • **Node (Software Management)**
Health	• **Healthy** • **Warning** • **Critical** • **Unknown** • **Service Mode**
Resource Groups	Allows you to choose one or more resource groups.
Resource State	**Managed**, **Unmanaged**, or **Reserved**
Node Pool	Lets you choose **Global** or one or more node pools.

On the **Resources** page, you can also perform the following tasks:

Task	How to perform
Discover new resources	Click **Discover Resources**.
Manually run an inventory operation on a resource and update PowerFlex Manager with the latest resource details	Select a resource and click **Run Inventory**. After running the inventory, you can perform an **Update Resource Group Details** operation on any resource group that requires the updated resource data.
Remove a resource from PowerFlex Manager	Click **Remove**.
Update the firmware or software of a resource	Select one or more resources and click **Update Resources**.
Export a compliance details report for all resources to a CSV or PDF file	Click **Export Report** and select a report format.
Modify the current state of a resource	Select a resource and click **Change resource state to**. You can change the state to **Managed**, **Unmanaged** or **Reserved**.
View detailed information about a resource	Select the resource. In the right pane, click **View Details**.
View a firmware and software compliance report for a resource	Select the resource. In the right pane, click the link corresponding to **Compliance** field.
Update password for a resource	Select the resource and click **Update Password**.

Basic tasks

This section provides basic tasks for resource management.

Discover a resource

A resource must be discovered in PowerFlex Manager in order for PowerFlex Manager to manage it.

Before you start discovering a resource, complete the following:

- Gather the IP addresses and credentials that are associated with the resources.
- Ensure that both the resources and PowerFlex Manager are connected to the network.

A resource in PowerFlex Manager is categorized into one of the following groups: Element Manager, Node (Hardware/Software Management), Switch, VM manager, PowerFlex gateway, Node (Software Management) or PowerFlex System.

1. Access the **Discovery Wizard** by performing either of the following actions:
   - On the **Getting Started** page, click **Discover Resources**.
   - On the menu bar, click **Resources**. On the **Resources** page, click **Discover Resources** on the **All Resources** tab.
2. On the **Welcome** page of the **Discovery Wizard**, read the instructions, and click **Next**.
3. On the **Identify Resources** page, click **Add Resource Type**, and perform the following steps:
   a. From the **Resource Type** list, select a resource that you want to discover.
      - **Element Manager**, for example, CloudLink Center.
      - **Node (Hardware / Software Management)**
      - **Switch**
      - **VM Manager**
      - **PowerFlex Gateway**
      - **Node (Software Management)**
      - **PowerFlex System**

      If you want to discover a software-only node or management VM (MVM) node with a credential that uses SSH key pairs, you must add the public keys to the nodes manually before performing the discovery. If you do not add the public keys first, the discovery fails.

      The **PowerFlex System** resource type is used to discover an MDS gateway.

      For a PowerFlex 4.x system, indicate whether the PowerFlex instance will be used for **Production Storage** or a **Management Cluster**.

   b. Enter the management IP address (or hostname) of the resources that you want to discover in the **IP/Hostname Range** field.

      To discover one or more nodes by IP address, select **IP Address** and provide a starting and ending IP address.

      To discover one or more nodes by hostname, select **Hostname** and identify the nodes to discover in one of the following ways:

      - Enter the fully qualified domain name (FQDN) with a domain suffix.
      - Enter the FQDN without a domain suffix.
      - Enter a hostname search string that includes one of the following variables:

Variable	Description
${num}	Produces an automatically generated unique number.
${num_2d}	Produces an automatically generated unique number that has two digits.
${num_3d}	Produces an automatically generated unique number that has three digits.

      If you use a variable, you must provide a start number and end number for the hostname search.

   c. Select one of the following options from the **Resource State** list:

Option	Description
Managed	Select this option to monitor the firmware version compliance, upgrade firmware, and deploy resource groups on the discovered resources. A managed state is the default option for the switch, vCenter, element manager, and PowerFlex gateway resource types. Resource state must be set to **Managed** for PowerFlex Manager to send alerts to SupportAssist.
Unmanaged	Select this option to monitor the health status of a device and the firmware version compliance only. The discovered resources are not available for a

Option	Description
	firmware upgrade or deploying resource groups by PowerFlex Manager. This option is the default for the node resource type. If you have yet not uploaded a license, PowerFlex Manager is configured for monitoring and alerting only. In this case, **Unmanaged** is the only option available.
Reserved	Select this option to monitor firmware version compliance and upgrade firmware. The discovered resources are not available for deploying resource groups by PowerFlex Manager.

d. To discover resources into a selected node pool instead of the global pool (default), select an existing or create a node pool from the **Discover into Node Pool** list. To create a node pool, click the **+** sign to the right of the **Discover into Node Pool** box.
e. Select an existing or create a credential from the **Credentials** list to discover resource types. To create a credential, click the **+** sign to the right of the **Credentials** box. PowerFlex Manager maps the credential type to the type of resource that you are discovering. The credential types are as follows:
   - Element Manager
   - Node (Hardware/Software Management)
   - Switch
   - VM Manager
   - PowerFlex Gateway
   - Node (Software Management)
   - PowerFlex System

   The default node (Hardware/Software Management) credential type is **Dell PowerEdge iDRAC Default**.
f. If you want PowerFlex Manager to automatically reconfigure the iDRAC nodes it finds, select the **Reconfigure discovered nodes with new management IP and credentials** check box. This option is not selected by default, because it is faster to discover the nodes if you bypass the reconfiguration.
g. To have PowerFlex Manager automatically configure iDRAC nodes to send alerts to PowerFlex Manager, select the **Auto configure nodes to send alerts to PowerFlex Manager** check box.

4. Click **Next**.

   You might have to wait while PowerFlex Manager locates and displays all the resources that are connected to the managed networks.

   To discover multiple resources with different IP address ranges, repeat steps 2 and 3.

5. On the **Discovered Resources** page, select the resources from which you want to collect inventory data and click **Finish**. The discovered resources are listed on the **Resources** page.

Related information

Getting started
Configuring block storage
Resource health status
Compliance status

Discover a PowerFlex system

Perform this task to discover a PowerFlex system.

The Management Data Store (MDS) and cluster for a PowerFlex system are not automatically discovered when you perform a migration on the **Initial Configuration** wizard. Therefore, you must bring in these resources after migration.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

Before you start discovering a PowerFlex system, complete the following:
- Gather the IP addresses and credentials that are associated with the resource.
- Ensure that both the resource and PowerFlex Manager are connected to the network.

- The MDS cluster must be installed manually before you attempt to do the discovery of the PowerFlex system on the **Resources** page.

1. Access the **Discovery Wizard** by performing either of the following actions:
   - On the **Getting Started** page, click **Discover Resources**.
   - On the menu bar, click **Resources**. On the **Resources** page, click **Discover Resources** on the **All Resources** tab.
2. On the **Welcome** page of the **Discovery Wizard**, read the instructions, and click **Next**.
3. On the **Identify Resources** page, click **Add Resource Type**, and perform the following steps:
   a. From the **Resource Type** list, select **PowerFlex System**.

      For a PowerFlex 4.x system, indicate whether the PowerFlex instance will be used for **Production Storage** or a **Management Cluster**.

   b. Enter the management IP addresses of the LIA nodes in the **MDM Cluster IP Address** field. You must provide the IP addresses for all the nodes in a comma-separated list. The list should include a minimum of three nodes and a maximum of five nodes.

      If you forget to add a node, the node will not be reachable after discovery. To fix this problem, you can rerun the discovery later to provide the missing node. You can enter just the one missing node, or all the nodes again. If you enter IP addresses for any nodes that were previously discovered, these nodes are ignored on the second run.

   c. For the **System ID**, specify the same System ID provided when you created the MDS cluster.
   d. Select an existing credential or create a new one from the **Credentials** list. The credential must be a **PowerFlex Management System** credential. Be sure to provide the LIA password that was used for the original setup. The LIA password is required for the mTLS configuration.
4. Click **Next**.
5. On the **Summary** page, click **Finish**.
   After you complete the discovery, you should see a **PowerFlex System** resource on the **Resources** page. The OS Hostname and Asset/Service tag are set to **`powerflex-mds`**. The discovery process also performs a bootstrap process that generates the required certificates and places them on the MDS nodes. Once you have completed the steps to discover a PowerFlex system, you must use the login certificate (not a username and password) to log in to the MDMs.
6. SSH to the two SVMs associated with the **`powerflex-mds`** system. Run `scli --add_certificate --certificate_file /opt/emc/scaleio/mdm/cfg/mgmt_CA.pem`.

Viewing resource details

Standard users can view details only for resources that are part of node pools for which they have permissions.

1. On the menu bar, click **Resources**.
2. On the **All Resources** tab, click a resource for which you want to view details.
3. In the right pane, click **View Details**. The **Details** page displays detailed information about the resource and associated components.

   For the PowerFlex rack Intelligent Physical Infrastructure (IPI) cabinet, you can view information including system name and location, model number, IP address, cabinet temperature, and humidity details.

   For PowerEdge servers, you can also see performance details, including system usage, CPU usage, memory usage, and I/O usage. Performance usage values are updated every five minutes.

   For a PowerFlex gateway, you can view MDM cluster, storage, and node details.

   For supported switches, you can view packet count by port for all ports or a specific port. The packet count for all ports shows the average packet count for all the ports in that switch.

Viewing node details

From the **Node Details** page, you can:

- Open the remote console of the node's Integrated Dell Remote Access Controller (iDRAC).
- View recent activities performed on the node.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

1. On the menu bar, click **Resources**.
2. On the **All Resources** tab, select a node from the resources list to view its details.

3. In the **Details** pane, click **View Details**.
   The **View Details** page displays the detailed information about the node on the following tabs:
   - **Network Interfaces**
   - **Port View**
   - **Firmware/Software Revisions**
   - **CPUs**
   - **Memory**
   - **Local Storage**

     NOTE: You can select one of the following options from the **Filter By** list.

     - **Logical Disks**
     - **Physical Disks**

       To see which disks are self-encrypting drives (SED), look at the **Security Status**. The value **Encryption Capable** indicates that the disk is an SED. The value **Not Capable** indicates that the disk is not an SED.

Viewing VMware vCenter details

You can view details for VMware vCenter.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

1. On the menu bar, click **Resources**.
2. On the **All Resources** tab, click VMware vCenter from the resource list to view the details.
   In the right pane, you can see the basic information about the VMware vCenter, such as power state, management IP address, data centers, clusters, hosts, and virtual machines.
3. In the **Details** pane, under **vCenter Details**, expand **vCenter** > **Datacenter** > **Cluster** to view the lists of nodes and applications.

Opening the iDRAC remote console

To simplify routine node maintenance, you can open a remote console to the node's Integrated Dell Remote Access Controller (iDRAC) directly from PowerFlex Manager.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

1. On the menu bar, click **Resources**.
2. On the **All Resources** tab, click a node.
3. In the **Details** pane, click **View Details**.
4. Click **Launch iDRAC GUI**.

Viewing PowerFlex system details

You can view performance metrics and storage details for a PowerFlex system.

PowerFlex Manager stores up to 15 GB of PowerFlex gateway PowerFlex system metrics. Once this threshold is exceeded, PowerFlex Manager automatically purges the oldest data to free up space.

1. On the menu bar, click **Resources**.
2. On the **All Resources** tab, click a PowerFlex system resource from the list to view its details.
   The right pane displays basic information about the resource, such as the unused and spare space for PowerFlex. It also shows the number of protection domains, volumes, storage data clients (SDC), and storage data servers (SDS).
3. In the right pane, click **View Details**.
   The **Details** page displays detailed information about the PowerFlex System resource on the following tabs:
   - **MDM Cluster**: Displays details about the MDM roles within the cluster.
   - **Storage**: Displays the protection domain, storage pools, volumes, and mapped storage data clients.
   - **Nodes**: Displays the protection domain, type (SDS or SDC), connection, name, IP address for the SDS or SDC, and fault set.

   The **Details** page also allows you to launch a wizard to see the status of a recent upgrade or reconfigure the MDM roles in the PowerFlex cluster.

4. Click the **MDM Cluster** tab to see information about the MDM roles within the cluster.
5. Click the **Storage** tab. For each storage pool within a protection domain, PowerFlex Manager shows the granularity setting and acceleration pool. For each volume within a storage pool, PowerFlex Manager shows the **Compression** and **Type** settings.

   For a storage pool that has compression disabled, the granularity is set to medium. For a storage pool that has compression enabled, the granularity is set to fine.

   For volumes, you may see a different number in the **Volumes** column on the **Resources** tab than you see for the total number of reported volumes on the **Volumes** page on the **Block** tab. The count of volumes that are listed on the PowerFlex system details view is the "vTree" count (volume + snapshots). The count of volumes that are listed on the **Block** tab is just the count of volumes.

   To search for volumes associated with the gateway:

   a. Enter a volume or datastore name search string in the **Search Text** box.
   b. Optionally, select a **Size** range.
   c. Optionally, select **Thick** or **Thin** for the **Type**.
   d. Optionally, select **Enabled** or **Disabled** for the **Compression** setting.
   e. Optionally, select a specific **Storage Pool**.
   f. Click **Search**.
   PowerFlex Manager updates the results to show only those volumes that satisfy the search criteria. If the search returns more than 50 volumes, you must refine the search criteria to return only 50 volumes.

Related information

Reconfiguring MDM roles
Migrating vCLS VMs to shared storage

Viewing PowerFlex file gateway details

You can view details for the PowerFlex file gateway.

1. On the menu bar, click **Resources**.
2. On the **All Resources** tab, click a PowerFlex file gateway resource from the list to view its details.
   The right pane displays basic information about the resource, such as the cluster IP address, node count, and the number of protection domains for which the file capability has been enabled.
3. In the right pane, click **View Details**.
   The **Details** page displays detailed information about the PowerFlex file gateway resource. **Nodes** displays the cluster name and IP address. In addition, it shows the name, management IP, protection domain, and storage pool for each node in the cluster.

Viewing PowerFlex rack IPI cabinet details

The IPI cabinet contains an appliance that is configured to provide information about power, thermals, alerts, and all components in the cabinet's physical infrastructure. PowerFlex Manager uses SNMPv2 to poll the IPI appliance status and send results about temperature and humidity to be viewed in PowerFlex Manager.

This capability is available on the PowerFlex rack offering only.

- If your cluster is running on several nodes, you must add the IP address of each node to the SNMP network management system (NMS) section in the Panduit Appliance UI.
- Ensure that PowerFlex Manager discovers the IPI cabinet. You can verify by clicking the list of resources and checking that the IPI cabinet is present.

You can view additional cabinet details in the IPI appliance management application.

To view the details for the IPI cabinet, perform the following steps:

1. On the menu bar, click **Resources**.
2. On the **All Resources** tab, click the row containing the IPI cabinet.
3. In the right pane, click **View Details**. The **Details** page displays detailed information about the IPI cabinet, including system name and location, model number, and IP address. It also displays cabinet temperature and humidity details.
4. To view additional details, click **Launch IPI Cabinet Manager** to launch the IPI appliance management application.

Viewing CloudLink Center details

You can view details for CloudLink Center.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

To view the details for CloudLink Center, perform the following steps:

1. On the menu bar, click **Resources**.
2. On the **All Resources** tab, click the row containing the CloudLink Center.
3. In the right pane, 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 **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.
4. To view additional details, click **Launch Console** to launch the CloudLink application.

Viewing NVDIMM details

To view NVDIMM details for a node, perform the following steps:

1. On the menu bar, click **Resources**.
2. On the **All Resources** tab, click the row containing a node that has NVDIMM compression.
3. In the right pane, click **View Details**.

   The **Details** page displays detailed information about the node.
4. Click the **Memory** tab.

   The **Memory** tab shows the NVDIMM modules and all DIMMs in the server. The DIMMs with rank 1 are the NVDIMM devices. The NVDIMMs shown in the top section of the **Memory** tab provide the name of each **NVDIMM Module**, as well as the **Battery Enabled State**, **Battery Health State**, **Battery Operational Status**, **Remaining Rated Read Write Endurance**, and **Size** for the module.

   All of the data is based on the last inventory.

Update resource inventory

You can run inventory to incorporate changes that are made to resource data outside of PowerFlex Manager. After running the inventory to incorporate these changes into the **Resources** page, you can update the details on any resource group that needs to include the new resource data.

Super users can run the inventory on any resources. Lifecycle administrators can run the inventory only on resources that are part of a node pool for which they have permission.

1. On the menu bar, click **Resources**.
2. On the **Resources** page, click the **All Resources** tab.
3. From the list of resources, click a resource, and in the **Details** pane, click **Run Inventory**.

   The resource state changes to **Pending**. When the inventory is complete, the resource state changes to **Available**. See PowerFlex Manager logs to view the start time and end time of the resource inventory operation.

   When you run the inventory, PowerFlex Manager checks to see whether DAS Cache is installed on any of the SVMs. If DAS Cache is installed, PowerFlex Manager disables some resource group features. PowerFlex Manager does not enable you to expand or remove resources within a resource group. Also, you cannot enter service mode, perform a drive replacement, perform firmware updates, delete a resource group, or retry a resource group deployment.

Viewing a compliance report for a resource

Perform the following steps to view a compliance report for a single resource:

1. On the menu bar, click **Resources**.
2. Select the resource for which you want to view the compliance report.
3. In the right pane, click the link corresponding to the **Compliance** option.
   The **Compliance Report** page displays.
   NOTE: If an RCM is mapped to the resource group and is modified, a wrench icon with the text, "Modified", is displayed. However, if the update file is moved or deleted, the wrench icon with the text, "Needs Attention", is displayed.
4. Select the **Firmware Components** option to view the details of the firmware available on the selected resource. For example, a switch.
5. Select the **Software Components** option to view the software components in the compliance report or to update the software components for a resource. If the resource is in the **In Use** state, it redirects you to the **Resource Groups** page.
6. To update the non-compliant resources, click **Update Resource**.
   NOTE: If there is no compliance version attached to the resource, you cannot perform the firmware update or software update.

Related information

Updating firmware and software
Exporting a compliance report for all resources

Updating firmware and software

You can update the firmware and software of shared resources from the **Resources** page.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

A firmware or software update on a node that is part of a cluster is successful only if the node is set to maintenance mode. PowerFlex Manager sets nodes in a cluster to maintenance mode before performing an update. To ensure that the node remains in maintenance mode, ensure that there are other nodes available in the cluster to host the virtual machines of the node being updated.

A firmware update on a VMware cluster is successful only if the cluster is properly configured for HA. For example, the host system can be set in maintenance mode and the virtual machines can be moved from one host to another in the cluster.

CAUTION: Check the Alerts page before performing the upgrade. Look for major and critical alerts before proceeding.

If any resources are not compliant with the default compliance catalog, you can update the firmware or software to the minimum recommended level.

1. On the menu bar, click **Resources**.
2. Select the check box for one or more resources and click **Update Resources**.
3. On the **Update Details** page, confirm that all the information is correct. For a PowerFlex gateway, you must reconfigure one or more nodes before proceeding with the upgrade.
4. Click **Next**.
5. On the **Summary** page, select one of the following options:
   - **Allow PowerFlex Manager to perform firmware and software updates now**—Select this option to update the firmware and software immediately.

     PowerFlex Manager applies the firmware updates and reboots the selected resources immediately. If the resource is in use, this update could be disruptive.

   - **Schedule firmware and software updates**—Select this option and then select the date and time to update the firmware and software.

     PowerFlex Manager applies the firmware updates at the selected date and time and reboots the selected resources. If the resource is in use, this update could be disruptive.

6. If you are updating a PowerFlex gateway, type **`UPDATE POWERFLEX`** to confirm that you are ready to proceed with the update.

7. Click **Finish**.

Related information

Viewing resource group details
Viewing a compliance report for a resource
Upgrading a PowerFlex gateway
Upgrading CloudLink Center

Upgrading a PowerFlex gateway

You can update the firmware and software of a PowerFlex gateway from the **Resources** page.

Upgrading the PowerFlex gateway is a two-step process. When you upgrade the PowerFlex gateway for a deployed resource group from the **Resources** page, PowerFlex Manager upgrades the PowerFlex gateway version. Then it automatically upgrades all the SDSs for all the resource groups that are tied to the Gateway.

Any nodes that require reconfiguration prior to an upgrade are shown in the **Needs Attention** section of the wizard. If you choose to reconfigure all the nodes, you can proceed with the upgrade process. If you select only a few of the nodes, PowerFlex Manager reconfigures these nodes, but does not proceed with the upgrade process until you have reconfigured the remaining nodes. You must reconfigure all the nodes before you can complete the upgrade process.

PowerFlex Manager does not allow you to downgrade the PowerFlex gateway.

NOTE: PowerFlex Manager requires the LIA password to be the same as the MDM cluster or PowerFlex gateway admin password. If it is different, during the upgrade of PowerFlex storage-only components using PowerFlex Manager, PowerFlex Manager will reset the LIA password to be the same as the MDM cluster or PowerFlex gateway admin password.

CAUTION: Check the Alerts page before performing the upgrade. Look for major and critical alerts related to PowerFlex Block and File to be sure the MDM cluster is healthy before proceeding.

1. Choose the PowerFlex gateway from the **Resources** page.

   You cannot upgrade more than one PowerFlex gateway at a time.
2. Click **Update Resources**.
3. On the **Update Details** page, check the **Needs Attention** section to see whether any of the nodes must be reconfigured before upgrade. Select any nodes that you want to reconfigure. To select all nodes, click the box to the left of **SDS Name**.
4. Click **Next**.
5. On the **Summary** page, choose **Allow PowerFlex Manager to perform non-disruptive updates now** or **Schedule non-disruptive updates to run later**.

   Specify the type of update you want to perform by selecting one of the following options:

   - **Instant Maintenance Mode** enables you to perform updates quickly. PowerFlex Manager does not migrate the data.
   - **Protected Maintenance Mode** enables you to perform updates that require longer than 30 minutes in a safe and protected manner.
6. If you only selected a subset of the nodes for reconfiguration, confirm the reconfiguration by typing **`RECONFIGURE NODES`**. Otherwise, confirm the update action by typing **`UPDATE POWERFLEX`**.

   If you reconfigured only a subset of the nodes, you must restart the wizard later to reconfigure the remaining nodes before you can complete the upgrade process.
7. Click **Finish**.
8. Go to the **Resource Groups** page to update any resource groups that are not in compliance with the new version of PowerFlex.

The PowerFlex gateway upgrade process performs some health prechecks to confirm that the resource group is healthy before the upgrade. If the resource group is not healthy, the PowerFlex gateway upgrade is not successful.

After a successful upgrade, the PowerFlex gateway should be in compliance with the new target version. However, the nodes in the resource group may require additional maintenance. In this case, you must update any resource groups that are noncompliant from the **Resource Groups** page.

When you initiate a PowerFlex gateway update, PowerFlex Manager upgrades both the Gateway RPM and the software components that are non-compliant.

Related information

Updating a resource group with new firmware and software
Updating firmware and software

Upgrading CloudLink Center

Upgrading CloudLink is a two-step process. First, PowerFlex Manager upgrades the CloudLink Center version of the deployed resource group. Then, you must upgrade any CloudLink Agent that is not running the same version as the CloudLink Center to the same version as the CloudLink Center.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

You must be running CloudLink version 6.8.1 to upgrade to CloudLink version 6.9. You must be running CloudLink version 6.9 to upgrade to CloudLink version 7.0. You must be running CloudLink version 7.0 to upgrade to CloudLink version 7.1.

After the CloudLink Center upgrade completes successfully, the PowerFlex nodes require additional maintenance because the CloudLink Agent is not in compliance with the new version for the resource group. In this case, you must update any resource groups that are noncompliant from the **Resource Groups** page. Firmware or software update of nodes will be blocked until CloudLink Center is updated and compliant.

PowerFlex Manager does not allow you to downgrade the CloudLink Center.

1. Choose the CloudLink Center from the **Resources** page.
2. Click **Update Resources**.
3. Choose **Allow PowerFlex Manager to perform firmware and software updates now** or **Schedule firmware and software updates**.
4. Click **Apply**.
5. Go to the **Resource Groups** page to update any resource groups that are not in compliance with the new version of the CloudLink Center.

Related information

Updating a resource group with new firmware and software
Updating firmware and software

Removing resources

Only super users can remove resources from PowerFlex Manager.

To remove a resource from PowerFlex Manager, perform the following steps:

1. On the menu bar, click **Resources**.
2. On the **Resources** page, click the **All Resources** tab.
3. From the list of resources, select one or more resources, and click **Remove**.
4. Click **OK** when the confirmation message appears.

If you remove a node, the node state changes to **Pending** and it powers off.

NOTE: Before you add new nodes using an existing iDRAC IP address in inventory, ensure that you remove the old nodes from PowerFlex Manager before discovering the new nodes.

Related information

Resource health status
Compliance status

Additional resource management tasks

This section provides additional tasks for resource management.

Creating a node pool

You can create a node pool on the **Resources** page.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

1. On the menu bar, click **Resources**. Click the **Node Pools** tab.
2. On the **Node Pools** page, click **Create**.
   The **Create Node Pool** wizard starts.
3. On the **Welcome** page, read the instructions, and click **Next**.
4. On the **Node Pool Information** page, enter a name and description for the node pool. Click **Next**.
5. On the **Add Nodes** page, select the nodes that you want to add to the node pool. Click **Next**.
6. On the **Assign Users** page, select the users that you want to grant access rights to the node pool. Click **Next**.
7. On the **Summary** page, review the node pool configuration and click **Finish**.

Modifying a node pool

You can modify the details for a node pool on the **Resources** page.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

1. On the menu bar, click **Resources**. Click the **Node Pools** tab.
2. On the **Node Pools** page, click **Modify**.
   The **Modify Node Pool** wizard starts.
3. To change the name and description of the node pool, in the left pane, click **Node Pool Information**. Make the updates and click **Save**.
4. To add or remove nodes from the node pool, in the left pane, click **Add Nodes**. Make the updates and click **Save**.
5. To add or remove the access rights to the node pool, in the left pane, click **Assign Users**. Make the updates and click **Save**.

Removing a node pool

You can remove a node pool on the **Resources** page.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

1. On the menu bar, click **Resources**. Click the **Node Pools** tab.
2. On the **Node Pools** page, select one or more node pools to delete. Click **Remove**.
3. Click **OK** when the confirmation message appears.

Viewing the port view details

Port view is a PowerFlex Manager feature that is associated with a resource group deployment. It enables you to view the physical network configuration characteristics and topology from the network interface cards to upstream switches, highlighting such details as switch ports, VLANs, and network identifiers such as MAC addresses.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

You can access port view from both the **Resources** and **Resource Groups** pages. Port view provides connectivity information for both new and existing resource groups.

The **Port View** page displays the following information:

- Topology information for all networks and VLANs deployed in a resource group
- Network connections between the devices
- Health of the resources
- Connection details section with information about the network devices

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

PowerFlex Manager does not show switch connectivity for deployments with partial network automation.

To view the port view details:

1. On the **Resource Groups** page, view the details for a resource group and click **Port View**. If you are accessing the port view from the **Resources** page, select a node that is in a **Deployed** state and click **View Details** on the right pane first.

   If you select a node that is not in a deployed state, only the interface card information is displayed.

2. To view device details such as hostname, model name, and management IP address, or information about associated devices, click the specific ports or devices.
3. To view information about intermediate devices in port view, ensure that the devices are discovered and available in the inventory. Sometimes, connectivity cannot be determined for an existing resource group because the switches have not yet been discovered. In this case, you see only the node in port view, but you do not see connectivity information. You can correct this by going back and discovering the switches, and updating the resource group again.

   PowerFlex Manager cannot discover interface cards that do not have integrated LLDP support (such as Intel X520).

4. To filter information based on the connectivity, select an option from the **Display Connections** list. **Show All Connections** is the default option.

Exporting a compliance report for all resources

You can download a CSV or PDF report that lists compliance details for all resources.

The CSV report includes all information and can be imported into a database for querying.

The PDF format contains a subset of information to make it easier to read. It measures each resource against a specified compliance file version. For each resource, it lists the components, the current and expected software or firmware version, and whether the component is compliant.

To download a compliance report for all resources:

1. On the menu bar, click **Resources**.
2. Click **Export Report**.
3. Select either **Export Compliance PDF Report** or **Export Compliance CSV Report** from the drop-down list.
   The selected report downloads.

Related information

Viewing a compliance report for a resource
Resource health status
Compliance status

Exporting a configuration report for all resources and resource groups

You can download a PDF report that lists configuration details for all resources and resource groups.

The configuration report shows the result of various configuration checks that PowerFlex Manager performs against the system. You can use the report to troubleshoot your resources and resource groups.

The report shows the following kinds of information:

Column name	Description
Resource Name	Provides the name of the resource for which the checks have been run. This column corresponds to the **Resource Name** shown on the **Resources** page.
Asset/Service Tag	Provides the asset or service tag of the resource for which the checks have been run. This column corresponds to the **Asset/Service Tag** shown on the **Resources** page.
Management IP	Specifies the **Management IP** of the resource for which the check is run. For a PowerFlex cluster, the management IP address is the MDM cluster IP address. For a PowerFlex gateway, the management IP address is the PowerFlex gateway IP address.
Result	Shows the result of the check (`PASS` or `FAIL`).

Column name	Description
Severity	Indicates the severity of the check. The severity is based on the result. The severity levels are INFO, WARNING, HIGH, or CRITICAL. If the result is PASS, the severity is INFO. If the result is FAIL, the severity depends on the type of check. PowerFlex Manager supports only CRITICAL checks.
Details	Provides a description of the check that was run.
Affected Resources	Gives a list of the IP addresses or unique identifiers of resources that are impacted by the check. The list of affected resources helps with troubleshooting.

1. On the menu bar, click **Resources**.
2. Click **Export Report**.
3. Select **Export Configuration PDF Report** from the drop-down list.

   The selected report downloads.

Related information

Configuration checks

Importing networks

You can import a large number of general-purpose VLANs from vCenter.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

After importing networks, you can add them to templates or resource groups. You can also import networks when you add an existing resource group.

1. On the menu bar, click **Resources**.
2. On the **All Resources** tab, click the VMware vCenter from which you want to import networks.
3. In the right pane, click **Import Networks**.
   PowerFlex Manager displays the **Import Networks** wizard. In the **Import Networks** wizard, PowerFlex Manager lists the port groups that are defined on the vCenter as **Available Networks**. You can see the port groups and the VLAN IDs.
4. Optionally, search for a VLAN name or VLAN ID.
   PowerFlex Manager filters the list of available networks to include only those networks that match your search.
5. Click each network you want to add under **Available Networks**. If you want to add all the available networks, click the check box to the left of the **Name** column.
6. Click the double arrow (>>) to move the networks you chose to **Selected Networks**.
   PowerFlex Manager updates the **Selected Networks** to show the ones you have chosen.
7. Click **Save**.

PowerFlex Manager creates a job to add the networks. The job may finish quickly, so you may not see on the **Jobs** page.

Go to **Settings** > **Networks** to see the imported networks.

Updating passwords for system components

You can update the passwords for some system components from PowerFlex Manager.

1. On the menu bar, click **Resources**.
2. 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.
3. Click **Update Password**.

   PowerFlex Manager displays the **Update Password** wizard.
4. 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.
5. On the **Select Credentials** page, create a credential or change to a different credential having the same username.
6. Click **Finish** and click **Yes** to confirm the changes.

Updating passwords for nodes

You can update the passwords for one or more nodes from PowerFlex Manager.

1. On the menu bar, click **Resources**.
2. On the **All Resources** tab, select one or more nodes for which you want to change the passwords.
3. Click **Update Password**.

   PowerFlex Manager displays the **Update Password** wizard.
4. 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**
   - **MVM Operating System Password**

   The option to update passwords for SVMs and MVMs will only appear if a node is in a resource group.
5. Click **Next**.
6. On the **Select Credentials** page, create a credential with a new password or change to a different credential.
   a. Open the **iDRAC**, **OS Password**, **SVM Password**, or **MVM Password** object under the **Type** column to see credential details for each node you selected on the **Resources** page.

      The **SVM Password** and **MVM Password** sections do not appear if there is nothing to show for SVMs or MVMs.

   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.
7. Click **Finish**.
8. Click **Yes** to confirm.

PowerFlex Manager starts a new job for the password update operation, and a separate job for the device inventory. The node operating system, SVM, and MVM operating components are updated only if PowerFlex Manager is managing a cluster with these components. 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 PowerFlex gateway components

You can update the passwords for one or more PowerFlex gateway components from PowerFlex Manager.

1. On the menu bar, click **Resources**.
2. On the **All Resources** tab, select one or more PowerFlex gateway components for which you want to change the passwords.
3. Click **Update Password**.

   PowerFlex Manager displays the **Update Password** wizard.
4. On the **Select Components** page, select **PowerFlex Password**.
5. Click **Next**.
6. On the **Select Credentials** page, create a credential with a new password or change to a different credential.
   a. Open the **PowerFlex** object under the **Type** column to see details about each gateway 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**, as well as the **Gateway Admin User Name** and **Gateway OS User Name** for which you want to change passwords. Enter the new passwords for both users and confirm these passwords.

c. To modify the credential, click the pencil icon for one of the nodes under the **Credentials** column and select a different credential.
d. Click **Save**.

7. Click **Finish**.
8. Click **Yes** to confirm.

PowerFlex Manager starts a new job for the password update operation, and a separate job for the device inventory. If PowerFlex Manager is managing a cluster for any of the selected PowerFlex gateway components, it updates the credentials for the **Gateway Admin User** and **Gateway OS User**, as well as any related credentials, such as the LIA and lockbox credentials. If PowerFlex Manager is not managing the cluster, it only updates the credentials for the **Gateway Admin User** and **Gateway OS User**.

11

Monitoring events and alerts

This section includes tasks for monitoring events and alerts from resources that are installed or automatically discovered.

Event and alert monitoring provides information regarding occurrences in your system.

An event is a notification that something happened in the system. Events monitor configuration changes, activities of the system, faults, and errors in the system and send notifications accordingly to inform the administrator.

An event that requires attention generates an alert as well. Other events can update or clear an alert when the system detects a change in the condition that needs attention.

An alert is a state in the system which is usually on or off. Alerts monitor serious events that require user attention or action.

Although the events may be interesting for troubleshooting purposes, it is not necessary to monitor events. Whereas an alert is a summation of one or more events that need or needed attention.

The **Monitoring** menu displays the events, alerts, and jobs on your system.

Related information

Enabling SupportAssist

Events

An event is a notification that something happened in the system. An event happens at a single point in time and has a single timestamp. An event may be unique or be part of a series.

Each event message is associated with a severity level. The severity indicates the risk (if any) to the system, in relation to the changes that generated the event message.

PowerFlex Manager stores up to 3 million events or events that are up to 13 months old. Once this threshold is exceeded, PowerFlex Manager automatically purges the events to free up space. The threshold is reviewed daily.

NOTE: An event is published each day that lists the events which have been removed that day.

Events severity level

The severity levels are as follows:

Severity level	Explanation	Example
Information	Informs you of events that you should be aware of, but that do not put the system at risk (no urgency).	`The volume is created.`
Minor	Indicates a failure that may result from an acceptable condition (for example user error), but can also indicate a possible failure.	`The Device media type is mismatched.`
Major	An error alarm raised by the system. This error requires your attention. The system is stable but could be degraded.	`The device failed.`
Critical	A major error alarm raised by system. The system requires immediate attention. Some data may be unavailable.	`The storage pool is running out of capacity.`

Event default and advanced fields

The default and advanced fields are as follows:

Field	Description	Example
Timestamp	The time the event occurred in the following format: `YYYY-MM-DD hh:mm:ss.sss`	`2022-04-03T13:49:18.709Z`
Severity	A predefined severity level that is associated with an event.	`INFORMATION`
Event ID	A unique identifier specific to the event instance that is always 16 digits.	`B46b66c8c79e4a2a`
Code	A unique event code that is always eight digits and identifies a specific event.	`80120001`
Event Name	An alphanumeric descriptive name for the event that is unique.	`MISCELLANEOUS`
Description	A free text description of the event.	`Successfully initialized the Discovery Manager`
Sub system	A resource domain that identifies the area that the alert relates to. The resource domains are: • Management • Block • File • Compute • Network • Security	`MANAGEMENT`
Resource Type	The type of resource that is involved in the event.	`basic-system-config`
Resource Name	The name of the resource that is involved in the event.	`asm manager`
Resource ID	The system specific ID of the resource involved in the event.	`asmcore`
Category	There are six categories of events that help you to filter: • Security • Audit • Software • Hardware • Maintenance • State changed	`STATE_CHANGED`
Service Name	The name of the service that generated the event.	`mdm_gw`
Details	Extra details that are relevant to the operation, for example, user command URL or a list of command parameters.	`[cmd: login, user: admin]`
Originator Application Name	The name of the application that generated the event. This field can be null.	`REST`
Message	A message that describes the event.	`Successfully initialized the Discovery Manager`

Viewing an event

You can view an event in PowerFlex Manager.

1. Go to **Monitoring** > **Events**.
   The **Events** page opens which displays a list of system events. You can add one or more filters to control the list of events displayed.
2. Select the event that you want to view.

   NOTE: You can reset the default and advanced field columns by clicking the **Reset Columns** icon.

Alerts

An alert is a state in the system which is usually on or off. Alerts monitor serious events that require user attention or action.

When an alert is no longer relevant or is resolved, the system automatically clears the alerts with no user intervention. This action ensures that cleared alerts are hidden from the default view so that only relevant issues are displayed to administrators. Cleared alerts can be optionally displayed through table filtering options. Alerts can also be acknowledged which removes the alert from default view. Acknowledging an alert does not indicate that the issue is resolved. You can view acknowledged alerts through the table-filtering options.

Alert severity level

The severity levels are as follows:

Severity level	Explanation	Example
Information	An information level informs you of things that happen in the system that do not require action.	NDU
Minor	A minor level informs you that action is required but is not urgent.	This Storage Pool contains devices that are not being accelerated.
Major	A major level informs you that action is required soon.	The MDM certificate is about to expire.
Critical	A critical level informs you that the system requires immediate attention.	The MDM certificate has expired.

Alert default and advanced fields

The default and advanced fields are as follows:

Field	Description	Example
Description	A message that describes the alert.	The MDM cluster is degraded, and data is not protected.
System impact	A free text, description of the system impact of the alert.	Risk of cluster unavailability
Repair Flow	Free text, actions that you can take in order to repair the issue.	Check that all MDM cluster nodes are functioning correctly, and fix and replace faulty nodes, if necessary, to return to full protection
Alert Details	Any extra details that are relevant to the object and or incident involved.	Percentage of SP capacity usage
Associated Events	A list of events that modified the life cycle of the alert.	[object Object]

Field	Description	Example
Resource ID	The ID of the resource that is associated with the alert.	86fb0000000000
Resource Name	The name of the resource that is associated with the alert. This is usually the resource that is involved with raising the event.	sds212
Resource Type	The type of resource that is associated with the alert. this is usually the resource that is involved with raising the event.	sdses
Last Updated	The UTC date and time that the alert was last updated.	2022-04-28T07:58:46.16Z
Timestamp	The UTC date and time that the alert was initially raised.	2022-04-28T07:58:46.16Z
Acknowledged status	The acknowledged status indicates whether the alert is acknowledged or unacknowledged.	Y

The total number of alerts that can be sent to Secure Remote Services gateway from the PowerFlex Manager dispatcher service is restricted to 200 per day. The threshold for the number of alerts for a particular event is set to three per hour. After the first three alerts are sent, if fourth alert is generated for the same event, it is not sent to the Secure Remote Services. However, if the alerts are sent from two different systems running iDRAC, the alerts are sent to the Secure Remote Services gateway.

A new threshold alert is triggered from PowerFlex Manager when the threshold of 200 alerts per 24 hrs is crossed per day and is automatically sent to Secure Remote Services gateway. Similarly, a new alert is triggered from PowerFlex Manager and sent to Secure Remote Services gateway when threshold of three alerts per hour for same alert type, symptom code, or resource is reached.

Viewing and acknowledging an alert

You can view and acknowledge an alert in PowerFlex Manager. When you acknowledge an alert, PowerFlex Manager removes the alert from the default view. Acknowledging an alert simply indicates that you have seen the alert. It does not indicate that the issue is resolved. You can view acknowledged alerts through the table filtering options.

1. Go to **Monitoring** > **Alerts**.
   The **Alerts** page opens and displays a list of system alerts. You can add one or more filters to control the list of alerts displayed.
2. Select the alert that you want to view or acknowledge.

   NOTE: You can reset the default and advanced field columns by clicking the **Reset Columns** icon.

3. You can:
   - Click **Acknowledge** to acknowledge an alert.
   - Click **Unacknowledge** to remove an alert acknowledgment.

Jobs

In PowerFlex Manager, you can view the details of discovery, firmware update, inventory, and resource group deployment jobs. Only a user with an administrator role can view jobs.

The **Jobs** page displays the following information about the jobs that are scheduled or running in PowerFlex Manager:

- **State** — Displays one of the following states that is based on the job status:
  - **Error** —Job has completed with errors (job is complete but failed on one or more resources).
  - **Scheduled**—Job is scheduled to run at a specific time. It can be scheduled to run at a single time or at several times as a recurring job.
  - **In progress**—Job is running.
- **Job Name**—Identifies the name of the job.

- **Started By**—Displays the name of the user who started the job.
- **Start Time**—Displays the date and time when the job is scheduled to run.
- **Time Elapsed**—Displays the time that has elapsed from the start time to the end time of a job instance.
- **Details**—Displays the detail of a job instance.

If a job scheduled is a one-time job, after execution, it is not listed in the **Jobs** page.

To cancel the job, select the job that you want to cancel, and click **Cancel**.

To filter for a job, click the filter icon.

12

Configuring system settings

This section provides information about configuring settings for PowerFlex Manager.

Only a user with the administrator role can configure certain settings.

Go to **Settings** to complete the following tasks:

- Manage local users, LDAP users, and directory services
- Manage compliance versions, OS images, and compliance management versions
- Define networks and specify the port numbers that PowerFlex Manager should use to verify IP addresses
- Configure settings for events and alerts, including notification policies, inputs, destinations, and alert severities
- Upload a production license for PowerFlex, as well as other software licenses
- Configure security settings, including SSL trusted certificates, appliance SSL certificates, and resource credentials
- Perform serviceability operations, such as generating a trouble-shooting bundle and performing a backup
- Upgrade the management software

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.	• 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.	• 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	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. **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.	• 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.	• 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.	• 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.	• 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.	• 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.	• 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.	• 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.	• View storage configurations, resource details • View platform configuration, resource details • System monitoring (events, alerts)
Support	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. **NOTE:** This special role should be used only by Dell support. It opens special, often dangerous, commands for advanced trouble shooting.	• 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.

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**.

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.

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.

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.

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**.

Remote users and groups

You can add and modify remote users and groups in PowerFlex Manager. Remote users are users tied to an LDAP directory service or to an SSO identity provider.

For LDAP configurations, the LDAP realm name must not exceed the 155 character limit defined by Microsoft.

Add remote users or groups

Add remote users or groups to PowerFlex, and assign roles to them. Remote users are users tied to an LDAP directory service or to an SSO identity provider.

When you add users and groups, you can also assign roles to the users and groups. The roles control access permissions for the corresponding LDAP user or group. The users and groups must also be configured in the LDAP directory service or SSO identity provider. On the PowerFlex side, these users and groups are mapped to PowerFlex roles.

1. On the menu bar, click **Settings**.

2. In the left pane, click **User Management**, then in the right pane, click **Remote Users/Groups**.
3. Click **Add**.
4. In the **Add Remote 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. Select the LDAP directory service or SSO identity provider in the **Provider** drop-down.
6. In the **User Name** box, enter the user or group name.
7. 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
8. Click **Apply**.

Modify a remote user or group

You can modify the user role of a user or group tied to an LDAP directory service or an SSO identity provider. User roles control access permissions to the corresponding user or group.

1. On the menu bar, click **Settings** > **Remote Users**.
2. Click **Modify**.
3. In the **Modify Remote 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.

Perform the following procedure to add a directory service to PowerFlex:

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.

Perform the following procedure to edit the settings:

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.

Perform the following procedure to remove a directory service:

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**.

SSO Identity Provider (IdP) Configuration

You can configure Single Sign-on (SSO) authentication through an Identity Provider (IdP) using the SAML 2.0 protocol. This configuration makes it possible for users to take advantage of SSO capabilities.

PowerFlex Manager allows you to add up to three identity providers for SSO authentication. For each identity provider that you add, you must download the service provider metadata for PowerFlex and configure the service provider within the identity provider.

PowerFlex Manager configures a single SSO service provider for each PowerFlex management platform (PFMP).

From this page, you can:

- Add an SSO identity provider configuration
- Modify an SSO identity provider configuration
- Enable or disable an SSO identity provider configuration
- Delete an SSO identity provider configuration

Add an identity provider

Add an SSO Identity Provider (IdP) for PowerFlex Manager to allow users to take advantage of single sign-on (SSO) capabilities through other applications.

Perform the following procedure to add an identity provider:

Before adding an identify provider, you must log on with an account that has the SecurityAdmin role. You also must upload the identity provider root CA certificate for Active Directory Federation Service (ADFS). Ensure that you have access to the ADFS before you begin this procedure.

1. On the menu bar, click **Settings**.
2. In the left pane, click **User Management**, then in the right pane, click **SSO Identity Provider (IdP) Configuration**.
3. Click **Add**.
4. On the **Name** page, provide a name for the identity provider and click **Next**.
5. On the **Service Provider** page, download the service provider metadata for PowerFlex and configure the PowerFlex service provider within your identity provider.
   a. To download the metadata as a file, select **Download File** and click **Download SP Metadata (XML)**.
   b. To copy the metadata, click **Manual Copy** and click **Copy** for each piece of metadata.
   c. Configure PowerFlex as a service provider within your identity provider.

      In the ADFS user interface, perform these steps:

i. Log in to ADFS.
ii. Go to the **Relying Party Trusts** folder under **ADFS**.
iii. Click **Add Relying Party Trust...** under **Actions**.
iv. On the **Welcome** screen, select **Claims aware** and click **Start**.
v. On the **Select Data Source** screen, select **Import data about the relying party from a file**.
vi. In the **Federation metadata file location** field, specify the location of the downloaded service provider metadata file and click **Next**.

NOTE: If you copied the metadata instead of downloading the file, select **Enter data about the relying party manually** and input the copied metadata.

vii. On the **Specify Display Name** screen, enter the name that you would like to use for the service provider and click **Next**.
viii. On the **Choose Access Control Policy** screen, choose a policy and click **Next**.
ix. On the **Ready to Add Trust** screen, click **Next**.
x. On the **Finish** screen, select **Configure claims insure policy for this application** and click **Close**.
xi. On the **Relying Party Trusts** screen, select the display name for the newly created service provider, and click **Edit Claim Insurance Policy...** under **Actions**.
xii. Click **Add Rule...** to add the following LDAP attribute rule:

- For the **Claim rule template**, select **Send LDAP Attributes as Claims**.
- For the **Claim rule name**, type **`LDAP attributes`**.
- For the **Attribute store**, select **Active Directory**.
- For the Mapping of **LDAP attributes to outgoing claim types**, select the following attributes:

LDAP attribute	Outgoing claim type
E-Mail-Addresses	E-Mail Address
SAM-Account-Name	Name ID
Surname	Surname
Given-Name	Given Name

- Click **Finish**.

xiii. Click **Add Rule...** to add the following custom rule:

- For the **Claim rule template**, select **Send Claims Using a Custom Rule**.
- For the **Claim rule name**, type **`Get groups`**.
- For the **Custom rule**, paste in the following string:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/
windowsaccountname", Issuer == "AD AUTHORITY"]  => add(store = "Active
Directory", types = ("http://schemas.xmlsoap.org/claims/Group"), query =
";tokenGroups;{0}", param = c.Value);
```

- Click **Finish**.

xiv. Click **Add Rule...** to add another custom rule:

- For the **Claim rule template**, select **Send Claims Using a Custom Rule**.
- For the **Claim rule name**, type **`Claim of groups membership`**.
- For the **Custom rule**, paste in the following string:

```
c:[Type == "http://schemas.xmlsoap.org/claims/Group"]  => issue(Type =
"Group", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value =
c.Value, ValueType = c.ValueType);
```

- Click **Finish**.

xv. Click **OK**.

d. Return to PowerFlex Manager and click **I have configured PowerFlex as a SP in my IdP using the metadata above** on the **Service Provider** page of the **Add Identity Provider (IdP)** wizard.
e. Click **Next**.

6. On the **IdP Setup** page, upload the identity provider metadata so that PowerFlex can establish a connection to the identity provider.
   a. To upload the metadata as a file, select **Upload File** and specify the file location.
   b. To retrieve the metadata from a URL, select **URL** and specify the following URL:`https://hostname/FederationMetadata/2007-06/FederationMetadata.xml`

The URL is always the same, except for the hostname, which you must specify for your environment.

c. Click **Next**.

7. On the **Settings** page, review the attribute mappings that are imported from the identity provider.
   a. Check the attribute mappings to be sure they are correct.
   b. Click **Next**.
8. Review the **Summary** page and click **Finish**.

After you add a new identity provider, PowerFlex Manager adds it to the list of identity providers on the **SSO Identity Provider (IdP) Configuration** page. In addition, PowerFlex Manager updates the login page to show a login button with the new identity provider. You can see this button the next time you log in PowerFlex Manager.

Modify an identity provider

The **Modify** option allows you to edit the existing identity provider settings.

Perform the following procedure to edit the settings:

1. On the menu bar, click **Settings**.
2. In the left pane, click **User Management**, then in the right pane, click **SSO Identity Provider (IdP) Configuration**.
3. Select an identity provider.
4. Optionally, change the name for the identity provider.
5. Optionally, enable or disable the identity provider.
6. Click **Apply**.

Enable or disable an identity provider

You can disable an identity provider after the initial configuration. If needed, you can also reenable the provider after it has been disabled.

Perform the following procedure to enable or disable an identity provider:

1. On the menu bar, click **Settings**.
2. In the left pane, click **User Management**, then in the right pane, click **SSO Identity Provider (IdP) Configuration**.
3. Click **Enable** or **Disable**.

Delete an identity provider

You can delete an identity provider if you no longer need it.

Perform the following procedure to delete an existing identity provider:

1. On the menu bar, click **Settings**.
2. In the left pane, click **User Management**, then in the right pane, click **SSO Identity Provider (IdP) Configuration**.
3. Click **Delete**.

Update the certificate for an identity provider

You can update the certificate for an identity provider if it is about to expire.

1. On the menu bar, click **Settings**.
2. In the left pane, click **User Management**, then in the right pane, click **SSO Identity Provider (IdP) Configuration**.
3. Check the **Status** column to see if any of the identity providers are about to expire.
4. If an identity provider is about to expire, select the identity provider and click **Update Certificate** in the details pane to the right of the list of providers.

Repositories

On the **Repositories** page, you can load compliance files, operating system images, and compatibility management files.

You can load compliance files and specify a default version for compliance checking on the **Compliance Versions** tab. You can load multiple compliance files into PowerFlex Manager with different operating system images included. The compliance file includes operating system images for ESXi and PowerFlex. When you add a compliance file, these images are automatically added to the **OS Images** tab. If necessary, you can also create your own operating system image repositories. You can also load the compatibility management file on the **Compatibility Management** tab to allow PowerFlex Manager to determine which upgrade paths are valid and which are not.

On the **Compliance Versions** tab, click **Add** to load a compliance version. Click **Change** to change the default compliance version to a new file.

You cannot make a minimal compliance version the default version for compliance checking, since it includes only server firmware updates. The default version must include the full set of compliance update capabilities. PowerFlex Manager does not show any minimal compliance versions in the **Default Version** drop-down list.

The **Compliance Versions** tab displays the following information:

Field	Description
State	Displays an icon indicating one of the following states: ● Pending—The compliance file download process is in progress. ● Downloading—The compliance file is being downloaded and PowerFlex Manager provides the percentage complete for the download operation. ● Unpacking—The compliance file is being unpacked and provides the percentage complete for the unpacking operation. ● Synchronizing—The compliance file is being synchronized with the management software after unpacking. ● Available—The compliance file is downloaded and copied successfully. ● Error—There is an issue downloading the compliance file. ● Needs Approval—The compliance file is unsigned and needs approval for use.
Version	Displays the compliance version.
Source	Displays the share path of the compliance version in a file share.
Signature	Displays whether the digital signature on the compliance file is signed or unsigned.
File Size	Displays the size of the compliance file in GB.
Type	Displays **Minimal** if the compliance file only contains firmware updates, or **Full** if it contains firmware and software updates.
View bundles	Displays details about any bundles added for the compliance version.
Available Actions	Select an option for a compliance file that is in an **Error** state: ● Delete the compliance version ● Resynchronize a compliance version
	Select an option for a compliance file that is in a **Needs Approval** state: ● Allow unsigned file ● Delete

Use the **OS Image Repositories** tab to create operating system image repositories and view the following information:

Field	Description
State	Displays the following states: ● Available—The operating system image repository is downloaded and copied successfully. ● Pending—The operating system image repository download process is in progress. ● Error—There is an issue downloading the operating system image repository.
Repository	Displays the repository name.

Field	Description
Image Type	Displays the operating system type.
Source Path	Displays the share path of the repository in a file share.
In Use	Displays **True** (the operating system image repository is in use) or **False** (the operating system image repository is not in use).
Available Actions	Select an option to delete or resynchronize.

You cannot perform any actions on repositories that are in use. However, you can delete repositories that are in an **Available** state, but not in use and not set as a default version.

All the options are available only for repositories in an **Error** state. The **Resynchronize** option appears only when you must perform a backup and restore of a previous image.

Use the **Compatibility Management** tab to load the compatibility management file. To facilitate upgrades, PowerFlex Manager uses information that is provided in the compatibility matrix file to determine which upgrade paths are valid and which are not. When you attempt an upgrade, PowerFlex Manager warns you if the current version of the software is incompatible with the target version, or if any of the RCM or IC versions that are currently loaded are incompatible with the target compliance versions.

Related information

Configuring block storage
Deploying and provisioning

Compliance versions

PowerFlex Manager displays the following information about the compliance versions:

Field	Description
State	Displays an icon indicating one of the following states: ● Pending—The compliance file download process is in progress. ● Downloading—The compliance file is being downloaded and PowerFlex Manager provides the percentage complete for the download operation. ● Unpacking—The compliance file is being unpacked and provides the percentage complete for the unpacking operation. ● Synchronizing—The compliance file is being synchronized with the management software after unpacking. ● Available—The compliance file is downloaded and copied successfully. ● Error—There is an issue downloading the compliance file. ● Needs Approval—The compliance file is unsigned and needs approval for use.
Version	Displays the compliance version. If one or many components in the RCM are modified, a wrench icon and the text, "Modified" is displayed next to the name of the RCM. But, if the file is deleted from the file share after a component is updated, the wrench ion with the text, "Modified | Needs Attention", is displayed.
Source	Displays the share path of the compliance version in a file share.
Signature	Displays whether the digital signature on the compliance file is signed or unsigned.
File Size	Displays the size of the compliance file in GB.
Type	Displays Minimal if the compliance file only contains firmware updates, or Full if it contains firmware and software updates.
View bundles	Displays details about any bundles added for the compliance version.
Available Actions	Select an option if the compliance file is in an **Error** or **Needs Approval** state: ● Delete the compliance version ● Resynchronize a compliance version ● Allow unsigned file

Select the compliance version to view the following information about the firmware package:

- **Bundles**—Displays the number of bundles available in the firmware package.
- **Components**—Displays the number of software components available in the firmware package.
- **Created On**—Displays the date when the compliance version was created.
- **Last Updated**—Displays the date when the compliance version was last updated.
- **Resource Groups Affected**—Displays the resource groups in which the firmware is used.

From this page, you can:

- Add a compliance file.

  A compliance file can be large and take some time to download and unpack. To help you monitor the progress of the downloading and unpacking operations, PowerFlex Manager provides percentage complete information for these operations in the **State** column on the **Compliance Versions** tab.

- Select **Default Version** and choose a version from the drop-down list to set it as the default for compliance.
- Select a compliance version from the list, and click the delete icon in the same row to remove the version.

  If you remove a compliance version, the version is deleted from the appliance not from the file share.

- Select a version from the list, and, in the right pane, click **View Bundles** to view the firmware and software bundles available in the compliance version.

Add a compliance file

A compliance file must be in an available state for PowerFlex Manager to add the file.

1. From the **Getting Started** page, click **Upload Compliance File**.

   Alternatively, click **Settings** > **Repositories**. On the **Repositories** page, select the **Compliance Versions** tab, and click **Add**.

2. In the **Add Compliance File** dialog, select one of the following options:
   - **Download from SupportAssist (Recommended)**—Select this option to import the compliance file that contains the firmware bundles you need.
     - **Download from local network path**—Select this option to download the compliance file from a CIFS file share. This option is intended for sites that do not have Internet accessibility to SupportAssist.
3. If you selected **Download from SupportAssist (Recommended)**, click the **Available Compliance Files** drop-down list, and select the file.

   Before downloading a compliance file from SupportAssist, you must configure SupportAssist. To configure the SupportAssist, you must enable SupportAssist in the **Initial Configuration** wizard.

   If you are downloading a compliance file from SupportAssist, the file type is a ZIP or TAR.GZ file.

   NOTE: The XML file type is not supported as a download option.

4. If you selected **Download from local network path**, perform the following:
   - In the **File Path** box, enter the location of the compliance file. Use the following format:
     - CIFS share for ZIP file: **`\\host\share\filename.zip`**
     - CIFS share for TAR.GZ file: **`\\host\share\filename.tar.gz`**
   - If you are using a CIFS share, enter the **User Name** and **Password**.
   - Mark the target upgrade catalog as the default version for compliance checking.

   Download the 3.6.x and the 4.5.x software catalogs. PowerFlex requires the catalog for the version that the system is on and the target version.

5. Click **Save**.

   PowerFlex Manager unpacks the compliance file as a repository that includes the firmware and software bundles that are required to perform any updates.

   If the compliance file contains an embedded ISO file for an operating system image (such as for an VMware ESXi or PowerFlex image), the download process unpacks the file and adds it to the operating system image repository.

A compliance file can be large and take some time to download and unpack. To help you monitor the progress of the downloading and unpacking operations, PowerFlex Manager provides percentage complete information for these operations in the **State** column on the **Compliance Versions** tab.

Changing the compliance file

To perform upgrades against a different compliance version, you can change the compliance file.

1. To change the default compliance version, click **Change** on the **Compliance and OS Repositories** page.

   To change the target version for a resource group, click **Change Target** on the **Resource Group Details** page or click **Change** on the **Node Compliance Report**.
2. Choose the **Preferred Compliance File**.
3. Review the **Compatibility** setting. If it shows **Recommended** or **Supported**, you can proceed with the change. If it shows **Not Allowed**, PowerFlex Manager blocks the change. Review the alert for details about recommended or supported paths.
4. If the change is either recommended or supported, type **`CHANGE COMPLIANCE FILE`** if you are to proceed.
5. Click **Save**.

Firmware repository types

The **Resources** page displays devices that are validated against the default repository.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

There are two types of firmware repositories:

Repository	Description
Default	The default firmware repository is applied to all devices that are not in a resource group. To set a default firmware repository, you must download a compliance file from either SupportAssist or an internal share through PowerFlex Manager. If you set a default compliance version, you can view compliance with this repository on the Resources page. Devices with firmware levels below the minimum firmware that is listed in the default compliance version are viewed as non-compliant (out of compliance).
Service level	This repository is applied only to nodes that are in service and assigned the service level firmware repository. Devices with firmware levels below the minimum firmware level that is listed in the service level repository are marked as non-compliant. When a service level firmware repository is assigned to a resource group, the firmware validation is checked only against the service level firmware repository and the default firmware repository checks are no longer applied to the devices associated with this resource group.

Viewing firmware and software bundles details

To view the firmware and software bundles details:

1. On the menu bar, click **Settings** and click **Compliance and OS Repositories**.
2. Click the **Compliance Versions** tab, select a repository, and then click **View Bundles**.

   A list of system and software bundles is displayed.
3. Click **Firmware Bundles** to view the firmware or system bundles.
4. Click **Software Bundles** to view the software bundles.

You can see the following information regarding bundles:

- Name—Name of the firmware or software update package.
- Version—Version of the firmware or software update package.
- Date and Time—Date and time when the firmware or software update package was downloaded.

OS images

To add an OS image repository:

1. On the **Repositories** page, click **OS Images**, and then click **Add**.
2. In the **Add OS Image Repository** dialog box, enter the following:
   a. In the **Repository Name** box, enter the name of the repository. The repository name must be unique.
   b. In the **Image Type** box, enter the image type.
   c. In the **Source Path and Filename** box, enter the path of the OS image file name in a file share.

      To enter the CIFS share, see the format that is used in the following example: `\\host\lab\isos\filename.iso`

   d. If you are using the CIFS share, enter the **User Name** and **Password** to access the share.
3. Click **Add**.

After adding an OS image, you can modify it or remove it by selecting the image, then clicking **Modify** or **Remove**.

Resynchronizing an OS image repository

Use the resynchronize option to restore the OS image from the database after a backup and restore.

If an operating system image was uploaded as a part of an ISO file, you must resynchronize the OS image repository from the **OS Image Repositories** tab. However, if the operating system image was uploaded as a part of a compliance ZIP file, go to the **Compliance Versions** tab and resynchronize the ZIP file. The following procedure provides steps for performing the resynchronization from the **OS Image Repositories** tab.

To resynchronize the OS image repository for an operating system image that was uploaded as part of an ISO file:

1. On the **Repositories** page, click **OS Images**.
2. Click **Resynchronize** for a repository in an **Error** state.
   The **Resynchronize OS Repository** page is displayed.
3. Enter the user credentials and click **Test Connection** to test the network connection.

   NOTE: You cannot edit the **Source Path** and **Filename**.

4. Click **Resynchronize**.
   The repository state changes to `Copying state`.

Compatibility management

To facilitate upgrades, PowerFlex Manager uses information that is provided in the compatibility matrix file to determine which upgrade paths are valid and which are not.

When you attempt an upgrade, PowerFlex Manager warns you if the current version of the software is incompatible with the target version, or if any of the RCM or IC versions that are currently loaded are incompatible with the target compliance versions. To determine which paths are valid and which are not, PowerFlex Manager uses information that is provided in the compatibility matrix file. The compatibility matrix file maps all the known valid and invalid paths for all previous releases of the software.

When you first install PowerFlex Manager, the software does not have the compatibility matrix file, so you must upload the file before performing any updates. You must upload the latest compatibility matrix file to ensure that PowerFlex Manager has access to the latest upgrade information.

You can download the file from SupportAssist or upload it from a local directory path. The file has a GPG extension and an associated compatibility version number.

If you are uploading from a local directory path, ensure that you have access to a valid compatibility matrix file that has the GPG extension. If you are using SupportAssist, ensure that SupportAssist has been properly configured.

1. On the menu bar, click **Settings** and then click **Compatibility Management**.
2. Click **Edit Settings**.
3. Click **Download from Dell Technologies SupportAssist** if you are using SupportAssist.
4. Click **Upload from Local** to use a local file. Then, click **Choose File** to select the GPG file.

Getting started

If you want to return to the **Getting Started** page, you can launch it from the **Settings** page.

The **Getting Started** page guides you through the common configurations that are required to prepare a new PowerFlex Manager environment. A green check mark on a step indicates that you have completed the step. Only super users have access to the **Getting Started** page.

Networking

On the **Networking** page, you can define, edit, or delete a network. You can also verify which IP addresses are in use before deployment.

Related information

Getting started
Configuring block storage
Deploying and provisioning

Networks

The **Networks** page displays information about networks that are defined in PowerFlex Manager, including:

- **Name**
- **Network Type**
- **VLAN ID**
- **IP Address Setting**
- **Starting IP Address**
- **Ending IP Address**
- **Role**
- **IP Address in Use**

On the **Networks** page, you can:

- Define or modify an existing network.
- Delete an existing network.
- Click **Export All** to export all the network details to a CSV file.
- Export network details for a specific network. To export the specific network details, select a network, and then click **Export Network Details**.
- Click a network to see the following details in the **Summary** tab:
  - Name of the user who created and modified the network.
  - Date and time that the network was created and last modified.
- Sort the column by network names, click the arrow next to the column header. You can also refresh the information about the page.

If you select a network from **Networks** list, the network details are displayed.

For a static network, the following information is displayed:

- **Subnet Mask**
- **Gateway**
- **Primary DNS**
- **Secondary DNS**
- **DNS Suffix**
- **Last Updated By**
- **Date Last Updated**
- **Created By**
- **Date Created**
- **Static IP Details**

For a DHCP network, the following information is displayed:

- **Last Updated By**
- **Date Last Updated**
- **Created By**
- **Date Created**

You can filter the IPs by selecting any of the following options from the **View** drop-down list, under the **Static IP Address Details** section:

- **All IP Addresses**
- **IP Addresses in Use**
- **Available IP Addresses**

You can also select the links under the **IP Address in Use** column. The IPs are automatically filtered based on the **IP addresses In Use** criteria.

Defining a network

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

Ensure that the following conditions are met before you define the network:

- PowerFlex Manager can communicate with the out-of-band management network.
- PowerFlex Manager can communicate with the operating system installation network in which the appliance is deployed.
- PowerFlex Manager can communicate with the hypervisor management network.
- The DHCP node is fully functional with appropriate PXE settings to PXE boot images from PowerFlex Manager in your deployment network.

To define a network, complete the following steps:

1. On the menu bar, click **Settings** and then click **Networking**.
2. Click **Networks**.
   The **Networks** page opens.
3. Click **Define**. The **Define Network** page opens.
4. In the **Name** field, enter the name of the network. Optionally, in the **Description** field, enter a description for the network.
5. From the **Network Type** drop-down list, select one of the following network types:
   - **General Purpose LAN**
   - **Hypervisor Management**
   - **Hypervisor Migration**
   - **Hardware Management**
   - **PowerFlex Data**
   - **PowerFlex Data (Client Traffic Only)**
   - **PowerFlex Data (Server Traffic Only)**
   - **PowerFlex Replication**
   - **NAS File Management**
   - **NAS File Data**
   - **PowerFlex Management**

   For a PowerFlex configuration that uses a hyperconverged architecture with two data networks, you typically have two networks that are defined with the PowerFlex data network type. The PowerFlex data network type supports both client and server communications. The PowerFlex data network type is 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.
6. 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 that enable network traffic to flow from the node to configured networks during deployment.
7. Optionally, select the **Configure Static IP Address Ranges** check box, and then do the following:

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.

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**: 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.

   Repeat this step to add IP address ranges based on the requirement. For example, you can use one range for SDC and another for SDS.

   NOTE: IP address ranges cannot overlap. For example, you cannot create an IP address range of 10.10.10.1–10.10.10.100 and another range of 10.10.10.50–10.10.10.150.

8. Click **Save**.

Modifying 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.

1. On the menu bar, click **Settings** and then click **Networking**.
2. Click **Networks**.
   The **Networks** page opens.
3. Select the network that you want to edit and click **Modify**. The **Modify Network** page opens.
4. 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.

5. Click **Save**.

You can also view details for a network or export the network details by selecting the network, then clicking **View Details** or **Export Network Details**.

Deleting a network

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

1. On the menu bar, click **Settings** and then click **Networking**.
2. Click **Networks**.
   The **Networks** page opens.
3. Click the network that you want to delete, and then click **Delete**.
4. Click **OK** when the confirmation message is displayed.

Adding an IP verification port number

You must verify what IP addresses are in use before they are deployed. PowerFlex Manager uses default ports 22, 80, and 135 for verification.

1. On the menu bar, click **Settings** and click **Networking**.

2. Under **IP Verification Port Number**, click **Edit**.
3. In the **Port Numbers Used for IP Verification** box, add or remove the port numbers used by PowerFlex Manager to verify the IP addresses.

   Port numbers must be entered in comma-separated list, and must be between 1 and 65535.
4. Click **Save**.

To remove a port number, click **X** to the right of the port number.

System data networks

The **System Data Networks** page displays information about system data networks for use with NVMe/TCP. This information includes:

- **Name**
- **Network**
- **Network Mask**

On the **System Data Networks** page, you can:

- Add a system data network.
- Rename a system data network.
- Remove a system data network.

Adding a system data network

Use this procedure to add a new data network for NVM/TCP host connectivity.

To add a system data network, complete the following steps:

1. On the menu bar, click **Settings** and then click **Networking**.
2. Click **System Data Networks**.
   The **System Data Networks** page opens.
3. Click **Add**. The **Create System Data Network** page opens.
4. In the **Name** field, enter the name of the network.
5. In the **Network** field, enter the IP address of the network.
6. In the **Network Mask** field, enter the network mask.
7. Click **Create**.

Renaming a network

After you have added a system data network, you can edit the network name.

1. On the menu bar, click **Settings** and then click **Networking**.
2. Click **System Data Networks**.
   The **System Data Networks** page opens.
3. Select the network that you want to edit and click **Rename**. The **Rename System Data Network** page opens.
4. Edit the information in the **System Data Network Name**.
5. Click **Apply**.

Removing a system data network

After you have added a system data network, you can delete it, if necessary.

1. On the menu bar, click **Settings** and then click **Networking**.
2. Click **System Data Networks**.
   The **System Data Networks** page opens.
3. Click the network that you want to delete, and then click **Remove**.
4. Click **OK** when the confirmation message is displayed.

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, and 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, PowerFlex appliance, and VxFlex Ready Node are automatically discovered. Any future resources, for example, switch replacements or additional nodes, are considered external and must be added manually as sources.

Related information

Enabling SupportAssist

Configuring an external source

You must define a source to enable PowerFlex Manager to receive an external event. You do not need to create a source to receive PowerFlex events.

External resources such as iDRAC, CloudLink, and Dell or Cisco Switches have to be discovered on the **Resources** page either in managed or unmanaged state.

Alerts received from external resources like iDRAC, CloudLink, and Dell or Cisco Switches are seen only on **Events** Page.

PowerFlex related alerts can be seen on both the **Alerts** and **Events** pages.

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.

1. Go to **Settings** > **Events and Alerts** > **Notification Policies**.
2. From the **Sources** pane, click **Add**.
   The **Add Source** window opens.
3. Enter a source name and description.
4. Configure either SNMP or syslog forwarding:
   - If you select **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.
   - If you select **SNMP V3**:
     a. Enter the username, which identifies the ID where traps are forwarded on the network management system.
     NOTE: The username must be at most 16 characters.
     b. Select a security level from the following:

Security Level	Details	Description	authPassword	privPassword
Minimal	noAuthNoPriv	No authentication and no encryption	Not required	Not required
Moderate	authNoPriv	Messages are authenticated but not encrypted (Password-based encryption with message digest (MD5) with at least eight characters)	Required	Not required

Security Level	Details	Description	authPassword	privPassword
Maximum	authPriv	Messages are authenticated and encrypted (MD5 and Data Encryption Standard (DES) both with at least eight characters)	Required	Required

Currently, SNMP v3 alerts are supported by PowerFlex only for iDRAC.

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

5. Click **Submit**.

Related tasks

Modifying an external source
Configuring a destination
Modifying a destination
Add a notification policy
Modify a notification policy
Delete a notification policy

Modifying an external source

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

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

Related tasks

Configuring an external source
Configuring a destination
Modifying a destination
Add a notification policy
Modify a notification policy
Delete a notification policy

Configuring a destination

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

1. Go to **Settings** > **Events and Alerts** > **Notification Policies**.
2. From the **Destinations** pane, click **Add**.
   The **Create New Destination Protocol** window opens.
3. From the **Destination Properties** window:
   a. Enter the destination name and description.
   b. From the **Destination Type** menu, select either **SNMP V2c**, **SNMP V3**, **Syslog**, **Email (SMTP)**, or **Webhook**.
4. Click **Next**.
   The **Protocol Settings** window opens.
5. Depending on the destination type, enter the following information:

Destination type	Protocol settings
SNMP V2c	• Network Name/IP Address • Port • Community string

SNMP V3	• Network Name/IP Address
	• Port
	• Username
	• Security level:
	  ○ Minimal - no more information required
	  ○ Moderate - MD5 authentication password required
	  ○ Maximum - MD5 authentication and DES privacy passwords required

Syslog	• Network Name/IP Address
	• Port
	• Protocol
	  ○ UDP
	  ○ TCP
	• Facility
	  ○ All
	  ○ Authentication
	  ○ Security and authentication

Email (SMTP)	• Destination name
	• Description
	• Destination Type
	  ○ Server Type:
	  ▪ SMTP
	  ▪ SMTP over SSL
	  ▪ SMTPS SMARTTLS
	  ○ Server IP or FQDN
	  ○ Port
	  ○ Sender address and up to five recipient addresses
	  ○ If you choose to use credentials enter:
	  ▪ Username, password, sender address and up to five recipient addresses
	• Send Test Email
	• Test Email Server Connection

Webhook	• Destination name
	• Description
	• Destination Type
	  ○ Select Webhook.
	  ○ You can have up to three webhook destinations.
	• Webhook Destination API URL
	  ○ For example, if you want to configure a webhook destination for BigPanda, you must specify the BigPanda endpoint here.
	  ○ You can get this URL from the BigPanda site.
	• Enable Credentials
	• Credentials
	  ○ 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

6. Click **Finish**.

Related tasks

Configuring an external source

Modifying an external source
Modifying a destination
Add a notification policy
Modify a notification policy
Delete a notification policy

Modifying a destination

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

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

Related tasks

Configuring an external source
Modifying an external source
Configuring a destination
Add a notification policy
Modify a notification policy
Delete a notification policy

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.

1. Go to **Settings** > **Events and Alerts** > **Notification Policies**.
2. Click **Create New Policy**.
3. Enter a name and a description for the notification policy.
4. 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**.

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.

Related tasks

Configuring an external source
Modifying an external source
Configuring a destination
Modifying a destination
Modify a notification policy
Delete a notification policy

Related information

Enabling SupportAssist

Modify a notification policy

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

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

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**.

Related tasks

Configuring an external source
Modifying an external source
Configuring a destination
Modifying a destination
Add a notification policy
Delete a notification policy

Delete a notification policy

Use this procedure to delete a notification policy.

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

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**.

Related tasks

Configuring an external source
Modifying an external source
Configuring a destination
Modifying a destination
Add a notification policy
Modify a notification policy

License management

You can upload a Management Data Store (MDS) license and a single production license for the whole PowerFlex system. You can also upload other software licenses (for example, for CloudLink).

No license is required for the first 90 days of use. During this period, you are running PowerFlex in trial mode.

You can only upload an MDS license if an MDS Gateway has been discovered.

When you deploy a PowerFlex cloud-based cluster, you are provided with a free evaluation license. This license gives you 90 days to use the cloud-based storage cluster. After 90 days, the storage is preserved. However, you are not allowed to make configuration changes to the deployment. Once the evaluation license has expired, you must purchase a subscription or permanent license to continue using the cluster with the full range of capabilities.

PowerFlex Manager shows the start date and end date for both evaluation and subscription licenses on the **License Management** page. This allows you to see when your license will expire. Evaluation licenses apply only to cloud deployments, whereas subscription licenses apply to both cloud and on-premises deployments.

Related information

Getting started
Enabling SupportAssist

Uploading a PowerFlex license

You can upload PowerFlex licenses in PowerFlex Manager.

You can upload a PowerFlex license file for two use cases:

- Production License for a single system and if you have an PowerFlex appliance or PowerFlex rack system
- Management Data Store (MDS) license for the internal PowerFlex management controller

In either case, the license is a single file.

No license is required for the first 90 days of use. During this period, you are running PowerFlex in trial mode, and all features are enabled. PowerFlex Manager shows an alert on the **Monitoring** > **Alerts** page when you are running in trial mode.

You need to deploy the MDM cluster before uploading a PowerFlex license. You need to discover an MDS Gateway before uploading an MDS license.

1. On the menu bar, click **Settings** and then click **License Management**.
2. Click **PowerFlex License**.
3. To upload an MDS license, click **Choose File to Browse** in the **Management Data Store (MDS) License** section, select the license file, and click **Open**.
4. Click **Save**.
5. To upload a production license for PowerFlex, click **Choose File to Browse** in the **Production License** section, select the license file, and click **Open**.
6. Click **Save**.

When you upload a license file, PowerFlex Manager checks the license file to ensure that it is valid.

After the upload is complete, PowerFlex Manager stores the license details and displays them on the **PowerFlex Manager License** page. You can see the installation ID, system name, and SWID for PowerFlex. In addition, you can see the total licensed capacity, as well as the license capacity left. You can upload a second license, as long as the license is equal to or more than the total system capacity.

Uploading other software licenses

You can also upload other software licenses, in addition to the licenses required for PowerFlex. For example, you might want to upload a license for CloudLink.

1. On the menu bar, click **Settings** and then click **License Management**.
2. Click **Other Software Licenses**.
3. Click **Add**.
4. Click **Choose File** and select the license file.

5. Choose the **Type** of license you want to upload.
6. Click **Save**.

To remove a license, select it and click **Remove**.

Security

On the **Security** page, you can upload SSL trusted certificates for connecting to Active Directory, as well as appliance SSL certificates that ensure data secure transmission for PowerFlex Manager. You can also define credentials for the resources that PowerFlex Manager accesses and manages.

Adding SSL trusted certificates

You can upload a trusted SSL certificate from a certificate authority (CA). You can use a trusted SSL certificate to establish a secure LDAP connection to Active Directory.

Before you upload a trusted SSL certificate, you must obtain the certificate file. The file must contain an X.509 certificate in PEM format. It must start with **`---BEGIN CERTIFICATE---`** and end with **`---END CERTIFICATE---`**.

1. On the menu bar, click **Settings** and then click **Security**.
2. Click **SSL Trusted Certificates**.
   The **SSL Trusted Certificates** page opens.
3. Click **Add**.
4. Click **Choose File** and select the SSL certificate.
5. Provide a **Name** for the certificate. The name must be a single word.
6. To upload the certificate, click **Save**.

To delete an SSL trusted certificate, select the certificate and click **Delete**.

Adding appliance SSL certificates

Uploading an SSL certificate for the appliance ensures secure transmission by encrypting data that PowerFlex Manager sends over the web. It also provides authentication and ensures that data is routed to its intended endpoint and prevents users from receiving browser security errors.

To upload an SSL certificate, you typically perform the steps in the process:

1. Generate a certificate signing request (CSR) from the PowerFlex Manager user interface. Generating a CSR using a third party certificate tool is unsupported.
2. Download the CSR.
3. Submit the CSR to a certificate authority (CA). The CA provides a valid SSL certificate.
4. Upload the SSL certificate to PowerFlex Manager.

Generating a certificate signing request

A certificate signing request (CSR) includes information (such as domain name, locale) that certificate authorities require to provide a valid SSL certificate. After generating the CSR, download the encrypted text, and then submit it to a certificate authority. The certificate authority provides a valid SSL certificate for you to upload.

1. On the menu bar, click **Settings** and then click **Security**.
2. Click **Appliance SSL Certificates**.
   The **Appliance SSL Certificates** page opens.
3. Click **Generate Certificate Signing Request**.
   a. In the **Distinguished Name (www.domain.com)** box, enter a distinguished name in the format **`www.domain.com`** (for example, dellpowerflex.com).
   b. In the **Business Name** box, enter a business name where the certificate is recorded.
   c. In the **Department Name** box, enter a department name of the organizational unit (for example, IT, HR, or Sales) for which the certificate is generated.

d. In the **Locality (Town/City)** box, enter a locality name in which the organization is located.
e. In the **State (Province/Region)** box, enter a state name in which the organization is located (do not abbreviate).
f. From the **Country** list, select a country in which the organization is located.
g. In the **Email** box, enter a valid email address.
h. Click **Generate**.

4. Click **Download Certificate Signing Request**, and then copy the text that is displayed. To receive a valid SSL certificate, submit this text to a certificate authority.

Downloading the certificate signing request

After generating the certificate signing request (CSR), download the resulting text and submit it to a certificate authority. The certificate authority provides an SSL certificate for you to upload to PowerFlex Manager.

1. On the menu bar, click **Settings** and then **Security**.
2. Click **Appliance SSL Certificates**.
   The **Appliance SSL Certificates** page opens.
3. Click **Download Certificate Signing Request**.
4. To receive a valid SSL certificate, copy the displayed text and then submit it to a certificate authority.

After the certificate authority provides the SSL certificate, upload it to PowerFlex Manager.

Uploading an SSL certificate

Before you upload an SSL certificate, generate and download a certificate signing request (CSR). To receive a valid SSL certificate, submit the CSR to a certificate authority. Save the certificate to a local network share. The file must contain an X.509 certificate in PEM format. The file must start with **`---BEGIN CERTIFICATE---`** and end with **`---END CERTIFICATE---`**.

1. On the menu bar, click **Settings** and then click **Security**.
2. Click **Appliance SSL Certificates**.
   The **Appliance SSL Certificates** page opens.
3. Click **Choose File** under **SSL Certificate** and select an SSL certificate.
4. Click **Choose File** under **Trusted CA Certificate** and select an SSL certificate.
5. To upload the certificate, click **Save**.

Adding resource credentials

PowerFlex Manager requires a root-level username and password to access and manage nodes, switches, VMware vCenter, element managers, PowerFlex gateway, and operating system resources.

The **Credentials Management** page displays the following information about the credentials:

- **Name**—A user-defined name that identifies the credentials.
- **Type**—A type of resource that uses the credential.
- **Resources**—The total number of resources to which the credential is assigned.

From the credential list, click a credential to view its details in the **Summary** tab:

- Name of the user who created and modified the credential.
- Date and time that the credential was created and last modified.

On the **Credentials Management** page, you can:

- Create credentials
- Edit existing credentials
- Delete existing credentials

Create credentials

Perform this procedure to create credentials:

1. On the menu bar, click **Settings** and click **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 the credentials:
   - **Node**
   - **Switch**
   - **vCenter**
   - **Element Manager**
   - **PowerFlex Gateway**
   - **OS Admin**
   - **OS User**
   - **PowerFlex Management System**

   The **OS Admin** and **OS User** credential types apply to deployed items, not to PowerFlex Manager itself.
5. In the **Credential Name** field, enter the name to identify the credential.
6. Click **Enable Key Pairs** to enable login with SSH key pairs:

   To enable key pairs for the **Node** or **Switch** credential type:
   a. Import an existing key:
      i. Click **Import SSH Key Pair**.
      ii. Click **Choose File** and browse to the file that contains your public and private key, and select the private key.
      iii. Type a name for the key pair.
      iv. Click **Import**.

   To enable key pairs for the **OS Admin** or **OS User** credential type:
   a. To create a new key:
      i. Click **Create a new key**.
      ii. Click **Create & Download Key Pair.**.
      iii. Type a name for the key pair.
      iv. Click **Create**.

      The private key file (id_rsa) will be downloaded on your downloads folder. Click the **Download Public Key** button to download the public key file (id_rsa.pub).

   b. To import an existing key:
      i. Click **Import existing key**.
      ii. Click **Import SSH Key Pair**.
      iii. Click **Choose File** and browse to the file that contains your public and private key.
      iv. Type a name for the **Key Pair Name field**.
      v. 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 username 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/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. In this case, the username and password would be used instead for all communication.
7. In the **Domain** box, optionally specify an LDAP domain for the user.
8. In the **User Name** field, enter the username for the credential.

   `root` is the only valid username for root-level credentials on nodes (iDRAC). You can add iDRAC users with a username other than **`root`**.

   For the **OS User** credential type, you can enter a user other than root. For the embedded operating system, this user account must have SSH enabled and have sudo access. For 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 nonroot user.

The account on the SVM and/or storage-only nodes for the **OS User** credential type must have a `/home` directory and have the correct group permissions. For example, if the account were pfxm_admin, the home directory would be: `/home/pfxm_admin`

Here is an example showing the requirements for a pxflex user in the pxflex-grp group on an SVM:

```
[root@svm-dkim-hc-node1 home]# ls -alhtr
        total 0
        drwxr-xr-x.  3 root   root        20 Feb 26 16:03 .
        drwxr-xr-x   3 pxflex pxflex-grp  22 Feb 26 16:10 pxflex
        dr-xr-xr-x. 17 root   root       224 Feb 26 16:37 ..
        [root@svm-dkim-hc-node1 home]# cd pxflex/
        [root@svm-dkim-hc-node1 pxflex]#
        [root@svm-dkim-hc-node1 pxflex]#
        [root@svm-dkim-hc-node1 pxflex]# pwd
        /home/pxflex
```

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.

Provide two usernames for the PowerFlex gateway credential type:

- **Gateway Admin User Name**
- **Gateway OS User Name**

The Gateway admin user is the REST API administrator. The Gateway OS user is the SSH login user. The Gateway admin user must be the **`admin`** user, and the Gateway OS user must be **`root`**.

9. In the **Password** and the **Confirm Password** boxes, enter the password for the credential.

   NOTE: When the SSH key pair feature is enabled, the switch credential does not require the **Password** option.

   For the PowerFlex gateway credential type, provide two passwords:

   - **Gateway Admin Password**
   - **Gateway OS Password**

   PowerFlex Manager allows you to supply different passwords for the Gateway admin and Gateway OS users. The passwords are validated when you discover the PowerFlex gateway on the **Resources** page. The discovery fails if the passwords were not specified correctly on the **Credentials Management** page. PowerFlex Manager does not update the Gateway Admin and Gateway OS passwords on the node itself. However, if you change the password manually for either of these users, you can update the password on the **Credentials Management** page, and PowerFlex Manager ensures that subsequent operations on the resource group use the new password.

   Optionally, provide additional settings for VMware vCenter and element manager, and for switch credentials:

   - For VMware vCenter and element manager, in the **Domain** box, optionally enter the domain ID.
   - For switch credentials, under **Protocol**, optionally click one of the following connection protocols that are used to access the resource from remote:
     - **Telnet**
     - **SSH**

       NOTE: SSH is enabled on supported switches by default.

10. To configure trap receiving for SNMPv2:
    a. Under **SNMP Configuration**, select **V2** as the SNMP type.
    b. Click **+** beside the **SNMP v2 Community String** box.
    The **SNMP v2 Community String** page opens.
    c. Enter the community string by which PowerFlex Manager receives traps from devices and by which it forwards traps to destinations.
    d. Click **Save**.

    NOTE: You can add more than one community string. For example, add more than one if the community string by which PowerFlex Manager receives traps differs from the community string by which it forwards traps to a remote destination.

11. To configure trap receiving for SNMPv3:
    a. Under **SNMP Configuration**, select **V3** as the SNMP type.
    b. Click **+** beside the **SNMP V3 User** box.
    The **SNMP V3 User** page opens.
    c. Enter the **Username**, which identifies the ID where traps are forwarded on the network management system.

NOTE: The username must be at least 16 characters.

d. Select a **Security Level** from the following:

- **Minimal** - No additional information is required.
- **Moderate** - Provide an **MD5 Authentication Password** which is at least eight characters.
- **Maximum** - Provide an **MD5 Authentication Password** and a **DES Privacy Password** which is at least eight characters.

You can add more than one user.

NOTE: You can only select SNMPv3 for nodes. Select the **Auto configure nodes to send alerts to PowerFlex Manager** check box to discover iDRACs.

12. Click **Save**.

Modify credentials

Perform this procedure to modify credentials:

1. On the menu bar, click **Settings** and click **Security**.
2. Click **Resource Credentials**.
   The **Credentials Management** page opens.
3. Select a credential that you want to edit, and click **Modify**.
4. Modify the credential information in the **Modify Credentials** dialog box.
5. Click **Save**.

Remove credentials

Perform this procedure to remove credentials:

1. On the menu bar, click **Settings** and then click **Security**.
2. Click **Resource Credentials**.
   The **Credentials Management** page opens.
3. On the **Credentials Management** page, select the credential that you want to delete, and click **Remove**.
4. Click **OK** when the confirmation message appears.

Converting a private key from PuTTY format to OpenSSH format

Perform this procedure to convert a private key from PuTTY to OpenSSH format.

1. Navigate to the folder where PuTTY was installed.
2. Double-click `puttygen.exe` to open the **PuTTY Key Generator**.
3. Click **File** > **Load private key** on the menu bar.
4. Select the private key that you want to convert to OpenSSH format and click **Open**.
5. Click **Conversions** > **Export open SSH key** on the menu bar.
6. Click **Save** to save the key.
   The key should now be in OpenSSH format.
7. Copy the public key content that is displayed on the **Key** tab in the **PuTTY Key Generator**.
   You need this content so you can copy it to the nodes.

Configuring SSH key pairs

Perform this procedure to configure SSH key pairs for nodes and switches.

1. To configure an SSH key pair for a software-only node, run these commands:

```
# below command will generate SSH Key pair in /tmp directory
ssh-keygen -m PEM -b 2048 -t rsa -f /tmp/sshkey-key1 -q -N ""
```

```
# To copy public key to software only node
ssh-copy-id -i /tmp/sshkey-key1.pub root@100.68.105.233

# Keys can be copied for both root and non-root users
```

2. To configure an SSH key pair for a Cisco Nexus switch, run these commands to add the public key:

```
username pfxmsvc password <password> role priv-15

username pfxmsvc sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDWxvVQ9PgfFI3NMsg3TsR9G89ykZ3UEyciz47hcXH/
YXNakva5PV5l7ubHY4nUxKj3zpVHXg/Bq9zRK5lQFs4KGC5eaYB9nm2xEwhuhpvsCvROo8SzjjTNRcpok2EMD/
3VhuZAWdaXITSukq2D1Ek5W7qeE0LiLSC+2s0u6iPTU5KHs3mrELbRlxpVxnHQtrgUZnsLvkxwzuEnBKWNIEZ0
6HoDLP1vBCaYJslE5iDseUCZstWvFbvkaeE4FOrqohllAhVGVH19B6Q38ijVjLAwjXX03a6IQqeWj+JkpHpB61
vMsAqqje4pm9VFzAY2NAcvoBo7Oab+52qA1vJTCbG7

username pfxmsvc passphrase  lifetime 99999 warntime 14 gracetime 3
```

3. To configure an SSH key pair for an OS10 switch, run these commands to add the public key:

```
username pfxmsvc password <password> role sysadmin priv-lvl 15

username pfxmsvc sshkey "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDWxvVQ9PgfFI3NMsg3TsR9G89ykZ3UEyciz47hcXH/
YXNakva5PV5l7ubHY4nUxKj3zpVHXg/Bq9zRK5lQFs4KGC5eaYB9nm2xEwhuhpvsCvROo8SzjjTNRcpok2EMD/
3VhuZAWdaXITSukq2D1Ek5W7qeE0LiLSC+2s0u6iPTU5KHs3mrELbRlxpVxnHQtrgUZnsLvkxwzuEnBKWNIEZ0
6HoDLP1vBCaYJslE5iDseUCZstWvFbvkaeE4FOrqohllAhVGVH19B6Q38ijVjLAwjXX03a6IQqeWj+JkpHpB61
vMsAqqje4pm9VFzAY2NAcvoBo7Oab+52qA1vJTCbG7"
```

Note that the quotes must be used as shown in the command line above.

4. To configure an SSH key pair for iDRAC, perform these steps:
   a. Connect to iDRAC.
   b. Choose **iDRAC Settings** > **Users** > **Edit/Add User** > **SSH Key Configuration** > **SSH Key (Edit)**.
   c. Add the public key.

Serviceability

On the **Serviceability** page, you can generate a troubleshooting bundle and also perform a backup of the appliance. 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.

Generating a troubleshooting bundle

A troubleshooting bundle is a compressed file that contains logging information for PowerFlex Manager managed components. If necessary, download the bundle and send it to Dell Technologies Support for issue debugging.

The troubleshooting bundle includes the following logs:

- ASM deployer
- iDRAC life cycle
- Dell PowerSwitch switch
- Cisco Nexus switch
- VMware ESXi
- CloudLink Center
- NAS
- Standard output logs from all pods
- Kubernetes logs about pods, services, deployments, secrets, drivers, and volumes
- PowerFlex Block logs

NOTE: You can generate troubleshooting bundles from the **Resource Groups** page too.

1. On the menu bar, click **Settings** > **Serviceability**.
2. Click **Generate Troubleshooting Bundle**.
3. If you are using SupportAssist, **Send to Configured SupportAssist** is selected by default. Leave this default setting. If SupportAssist is not configured, this option is disabled.

   If you are not using SupportAssist, select **Download Locally** to download the troubleshooting bundle to a local file. Provide a path using the following format:

For...	Use this path...
CIFS	`\\IP Address\Any folder`

   For example:

   CIFS: `\\192.168.1.1\uploadDirectory`

   Also, provide a username and password.

4. Click **Test Connection** to verify the connection to the CIFS share before generating the bundle.
5. Optionally, select **Include PowerFlex File Core Dump logs**, if you want to include core dump logs for NAS.

   The NAS directory structure, nodes, and files are always collected regardless of whether this box is checked. When it is checked, the additional NAS core dump is collected.

6. To collect PowerFlex logs, select one of the following log level options:
   - Default Node Logs
   - Default Node Logs plus additional MDM information
   - Latest Logs only (Most recent copy of all logs)
7. To collect PowerFlex node logs, select one of the following options:
   - Logs from all nodes
   - Select Specific Nodes

   If you select the **Select Specific Nodes** option and select the number of nodes for which you want to generate the log, the **View/Select Nodes** button is displayed. Click the button to view the list of nodes in the **Node Selection** window. Select the required nodes from the **Available Nodes** list and click >> to view them in the **Selected Nodes** list. Click **Save** to return to the **Generate Troubleshooting bundle** page.

   For the **Select Specific Nodes** option, **Generate** is enabled only if a node is selected in the **Node Selection** window.

8. Click **Generate**.

Sometimes, the troubleshooting bundle does not include log information for all the nodes. The log collection may appear to succeed, but the log for one or more of the nodes may be missing. You may see an error message in the scaleio.trace.log file that says `Could not run get_info script`. If you see this message, you may need to generate the troubleshooting bundle again to include information for all the logs.

Selecting PowerFlex nodes for generating a troubleshooting bundle

1. From the **Available Nodes** list, select the check box next to the nodes you want to include in the troubleshooting bundle.
2. Click the right double arrow (>>) to move the selected nodes to the **Selected Nodes** list.
3. Click **Save** to save your selection.

Back up and restore

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.

Editing 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.

1. On the menu bar, click **Settings** and then click **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**.

Backing up

In addition to automatically scheduled backups, you can manually run an immediate backup.

1. On the menu bar, click **Settings** > **Serviceability**.
2. Click **Backup**.
   The **Backup** page opens.
3. Click **Backup Now**.
4. 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.

5. Click **Backup Now**.

Restoring

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.

Before you begin the restore procedure, you need to satisfy these prerequisites:

- The restore cluster must be exactly the same PowerFlex version and Kubernetes version.
- The restore cluster must have exactly the same IP addresses and configuration.

  The cluster configuration must be the same as the cluster configuration where the backup was taken.

  - All Kubernetes nodes must have the same IP addresses.
  - All Kubernetes nodes must have the same names.
  - All LoadBalancer IP addresses must be the same.

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.

1. Login to the node where the PowerFlex Manager platform (PFMP) installer was initially run.
2. Run the restore script that is included with the installer bundle:

```
./restore_backup.sh
```

3. Provide details as needed to complete the execution of the script.

   You will be prompted to provide the SSH username and password. In addition, you will be asked to specify whether the passwords are the same for all nodes, and also provide the location of the backup file and the encrypted password for the file. You may also be asked to provide the CIFS username and password. The CIFS credentials may not be required for a CIFS share that allows for anonymous access.

   NOTE: The passwords must be in base64 encoded format.

   To complete the execution of the restore script, you must specify whether the restore operation will be performed on an existing cluster or a new cluster.

   Here is a snippet that shows a sample run of the restore script:

```
[root@sheetal-installer scripts]# ./restore_backup.sh

/usr/local/lib/python3.8/site-packages/paramiko/transport.py:236:
CryptographyDeprecationWarning: Blowfish has been deprecated "class":
algorithms.Blowfish, Installation logs are available at <Bundle root>/PFMP_Installer/
logs/ directory. More detailed logs are available at <Bundle root>/atlantic/logs/
directory. PFMP Installer is about to reset a PFMP cluster based on the configuration
specified in the PFMP_Config.json.

Please enter the ssh username for the nodes specified in the
PFMP_Config.json[root]:root

Are passwords the same for all the cluster nodes[Y]?:Y

Please enter the ssh password for the nodes specified in the PFMP_Config.json.
Password:

Please enter backup file location - Example CIFS: \\1.2.3.4\Lab\backup\file.tgz

Please enter CIFS username. Press enter to skip if username is not
required:administrator

Please enter CIFS password(base64 encoded). Press enter to skip if username is not
required: UmFpZDR1cyE=
```

```
Please enter encryption password for backup file (base64 encoded): UmFpZDR1cyE=

Perform restore on existing cluster? Please enter yes/y or no/n :
```

The restore process prints out status information until the restore is complete.

Backup and restore using VM snapshots

If the PowerFlex management platform (PFMP) is running on VMs, you can backup and restore using VMware VM snapshots, as long as you perform some steps to shut down the database and VMs.

If the cluster is deployed on VMWare VMs, you can simply take the snapshots from the vSphere Client user interface, or you can use a CLI command on the ESX system that is hosting the VMs.

For VM snapshots, the database and VMs need to be shut down first before reliable snapshot(s) can be taken.

CAUTION: When you shut down the database and VMs, you effectively shut down the PFMP. The user interface will not be accessible and any running jobs will fail when the system comes back on. The VMs should be shut down and snapshots taken once the database is shut down.

Follow the steps below to shut down the database and VMs. For every command listed below, you first need to set the k alias and namespace.

1. Set the k alias and default namespace:

```
# Run this to make it easier to run the rest of the code and set the default
namespace.
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)
```

2. Verify the pgo controller pod and all database pods are up and running with no errors in the logs:

```
# Get the PostgreSQL operator pod and PostgreSQL cluster pods to verify.
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
```

3. Gracefully shut down the database cluster:

```
# Trigger a shutdown
k patch $(k get postgrescluster -o name) --type merge --patch '{"spec":{"shutdown":
true}}'
```

4. At this point, you can shut down the VMs to take snapshots and adjust resources, as needed. Follow the next steps after the VMs are powered back on.
5. Verify the shutdown occurred:

```
# Verify the shutdown
# Only the PostgreSQL operator pod "pgo" should remain when running this 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
```

6. Run this command to start the cluster back up:

```
# Trigger a shutdown
k patch $(k get postgrescluster -o name) --type merge --patch '{"spec":{"shutdown":
false}}'
```

7. Verify the startup occurred:

```
# Verify the database pods started and are in a running state
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
```

To restore to the previous point in time, you can revert the VMs from the snapshots in the vSphere Client user interface.

Software upgrade

When a new version of the management software becomes available, you can upgrade to that version from the **Software Upgrade** page.

Upgrading PowerFlex Manager using Dell SupportAssist

Upgrading the management software using SupportAssist is the recommended method of upgrading. SupportAssist refers to Secure Connect Gateway, which is used for call home functionality and remote connectivity.

Before you begin, ensure that you:

- Take a backup of PowerFlex Manager settings.
- Configure SupportAssist.
- Upload the latest compatibility matrix file to ensure that PowerFlex Manager has access to the latest upgrade information.

When you attempt an upgrade, PowerFlex Manager warns you if the current version of the software is incompatible with the target version, or if any of the RCM or IC versions that are currently loaded on the management software are incompatible with the target compliance versions. To determine which paths are valid and which are not, PowerFlex Manager uses information that is provided in the compatibility matrix file. The compatibility matrix file maps all the known valid and invalid paths for all previous releases of the software. Before proceeding with an upgrade, PowerFlex Manager notifies you if any of the following situations is detected:

- No upgrade is required. This situation occurs when the current and target versions are the same. You can still force an upgrade, if needed.
- The upgrade path that you are attempting to perform is a valid path. The source version of PowerFlex Manager is compatible with the target version and the source version of the RCM or IC is also compatible with the target version.
- The source version of PowerFlex Manager is compatible with the target version. However, the source version of the RCM or IC is not compatible with the target version. Your resource groups may go into lifecycle mode until you perform an RCM or IC upgrade. PowerFlex Manager puts a resource group in lifecycle mode if the RCM or IC for a resource group is not within a year of the target PowerFlex Manager launch. You can mitigate a resource group that is in lifecycle mode by upgrading to a compliance version that is within a year of the current PowerFlex Manager launch.
- The upgrade path that you are attempting to perform is not supported.

The compatibility matrix file is required for all upgrades. When you first install PowerFlex Manager, the software does not have the compatibility matrix file, so you must upload the file before performing any upgrades.

Whenever a new version of the management software is available, PowerFlex Manager displays a banner at the top of all pages to notify you of the new release. The banner appears only if you have registered with SupportAssist.

1. On the menu bar, click **Settings**, and click **Software Upgrade**.

   Alternatively, click **View Details** on the notification banner at the top of the page.

2. Click **Management Software Upgrade**.
3. On the **Management Software Upgrade** page, you can see the **Current Management Software Version** and check the **Available Management Software Version** field to see if a newer version of PowerFlex Manager is available.
4. Click **Edit Settings**.

   Select **Update Software from configured Dell SupportAssist (Recommended)** and click **Save**.

   The **Repository Path** field on the **Management Software Upgrade** page shows your saved changes.

5. At the top of the **Management Software Upgrade** page, click **Upgrade Now**.
   After you click **Upgrade Now**, a dialog box displays with a warning message indicating whether the upgrade path is valid.
6. Under **Management Credentials**, optionally override the default username and password for the nodes hosting PowerFlex Manager. The upgrade requires access to the nodes that are hosting PowerFlex Manager. Provide a single user that has superuser privileges for all nodes. You can enter the username for the first row in the table, and the changes you make will be applied to all the nodes. Enter the password for each of the nodes.
7. Type **`UPDATE POWERFLEX MANAGER`** if you want to proceed with the update. If you want to perform an update even if none is required, type **`FORCE UPDATE`**.
8. Click **Yes** to update PowerFlex Manager.
   The update process displays messages indicating the progress of the update. Depending on which services were upgraded, you may be required to log in once again, after the upgrade process is complete.

After upgrading to PowerFlex Manager, you may notice that resource groups that are tied to the PowerFlex gateway are no longer in compliance. To bring the resource groups into compliance, you may need to upgrade them. In this case, you must change to a later RCM or IC and upgrade the resource groups.

If you do not want to upgrade the resource groups, you do not need to perform the upgrade.

Upgrading PowerFlex Manager from a local repository path

You can upgrade the management software from a .TGZ file on a local repository path.

Before you begin, ensure that you:

- Take a backup of PowerFlex Manager settings.
- Upload the latest compatibility matrix file to ensure that PowerFlex Manager has access to the latest upgrade information.

When you attempt an upgrade, PowerFlex Manager warns you if the current version of the software is incompatible with the target version, or if any of the RCM or IC versions that are currently loaded on the management software are incompatible with the target compliance versions. To determine which paths are valid and which are not, PowerFlex Manager uses information that is provided in the compatibility matrix file. The compatibility matrix file maps all the known valid and invalid paths for all previous releases of the software. Before proceeding with an upgrade, PowerFlex Manager notifies you if any of the following situations is detected:

- No upgrade is required. This situation occurs when the current and target versions are the same. You still can force an upgrade, if needed.
- The upgrade path that you are attempting to perform is a valid path. The source version of PowerFlex Manager is compatible with the target version and the source version of the RCM or IC is also compatible with the target version.
- The source version of PowerFlex Manager is compatible with the target version. However, the source version of the RCM or IC is not compatible with the target version. Your resource groups may go into lifecycle mode until you perform an RCM or IC upgrade. PowerFlex Manager puts a resource group in lifecycle mode if the resource group's RCM or IC is not within a year of the target PowerFlex Manager launch. You can mitigate a resource group that is in lifecycle mode by upgrading to a compliance version that is within a year of the current PowerFlex Manager launch.
- The upgrade path that you are attempting to perform is not supported.

The compatibility matrix file is required for all upgrades. When you first install PowerFlex Manager, the software does not have the compatibility matrix file, so you must upload the file before performing any upgrades.

1. If you are using PowerFlex rack, log in to Dell Technologies Download Center. Then, go to the section for PowerFlex Manager.
2. If you are using PowerFlex appliance, log in to Dell Technologies Support. Then, enter your service tag to be taken to available downloads.
3. Download the PowerFlex management platform .TGZ file.
4. Copy the PowerFlex management platform .TGZ file to a share drive location.
5. On the menu bar, click **Settings**, and then click **Software Upgrade**.
6. Click **Management Software Upgrade**.
7. On the **Management Software Upgrade** page, you can see the **Current Management Software Version** and check the **Available Management Software Version** field to see if a newer version of PowerFlex Manager is available.
8. Click **Edit Settings**.
   a. To upgrade from a specific version on a local repository path, select **Update Software from local repository path**, and enter the path in the **Repository Path** box.
   b. Enter the username and password.
   c. Click **Save**.
9. At the top of the **Management Software Upgrade** page, click **Upgrade Now**.
   After you click **Upgrade Now**, a dialog box displays with a warning message indicating whether the upgrade path is valid.
10. Under **Management Credentials**, optionally override the default username and password for the nodes hosting PowerFlex Manager. The upgrade requires access to the nodes hosting PowerFlex Manager. Provide a single user that has superuser privileges for all nodes. You can enter the username for the first row in the table, and the changes you make will be applied to all the nodes. Enter the password for each of the nodes.
11. Type **`UPDATE POWERFLEX MANAGER`** if you want to proceed with the update. If you want to perform an update even if none is required, type **`FORCE UPDATE`**.
12. Click **Yes** to update PowerFlex Manager.
    The update process displays messages indicating the progress of the update. Depending on which services were upgraded, you may be required to login once again, after the upgrade process is complete.

After upgrading to PowerFlex Manager, you may notice that resource groups that are tied to the PowerFlex gateway are no longer in compliance. To bring the resource groups into compliance, you may need to upgrade them. In this case, you will need to change to a later RCM or IC and upgrade the resource groups.

If you do not want to upgrade the resource groups, you do not need to perform the upgrade.

Editing the upgrade settings

To edit the upgrade settings:

1. On the menu bar, click **Settings** and then click **Software Upgrade**.
2. Click **Management Software Upgrade**.
3. Click **Edit Settings**.
   a. To update to the latest version using SupportAssist, select **Update Software from configured Dell SupportAssist**.
   b. To upgrade from a specific version on a local repository path, select **Update Software from local repository path**, and enter the path in the **Repository Path** box.

      You can upgrade from a .tgz file on a network share. This option provides an easy way to update the software in a dark site. Provide a path using one of the following formats:

For...	Use this path...
CIFS	`\\IP Address\Any folder\file-name.tgz`
FTP	`ftp://IP Address/Any folder/file-name.tgz`
HTTP	`http://IP Address/Any folder/file-name.tgz`
HTTPS	`http://IP Address/Any folder/file-name.tgz`

   c. Optionally, provide a **User Name** and **Password**.

      The username and password are only used with CIFS. All other local repository paths must specify public share locations.

   d. Click **Save**.
4. On the **Management Software Upgrade** page, you can view the updated settings for **Current Management Software Version**, **Available Management Software Version**, and **Repository Path**.
5. To perform the upgrade, click **Upgrade Now**. A message displays confirming that you want to update the software.
6. Click **Upgrade Software**.
7. Click **Yes**.
8. Depending on which services were upgraded, you may be required to login again once the upgrade process is complete.

13

PowerFlex Manager user interface reference

This section provides reference details for various parts of the user interface for PowerFlex Manager.

The topics in this section are organized according to the main tabs within the user interface.

Lifecycle

This section provides reference information for the **Resource Groups** and **Templates** pages.

Related information

Managing components
Monitoring system health
Managing external changes
Deploying a resource group
Adding an existing resource group
Viewing a compliance report

Resource groups

This section provides reference information for the **Resource Groups** page.

Related information

Managing components
Managing external changes

Resource group states

Icon	Resource group state	Description
	**Healthy**	The resource group was deployed successfully, and the resources are firmware compliant and healthy.
	**Warning**	One or more resources in the resource group require corrective action. This state does not affect overall system health. For example, the firmware running on the resource is not at the required level or not compliant.
	**Critical**	Resource group deployment has failed due to some issues.
	**Pending**	Resource group deployment is scheduled for a later time or date.
	**In Progress**	Resource group deployment is in progress.
	**Canceled**	Resource group deployment was canceled.
	**Incomplete**	The resource group is not fully functional because it has no associated volumes. Click **Add Resources** to add volumes.

Icon	Resource group state	Description
	**Service Mode**	The resource group has been placed in service mode because one of the nodes within the resource group was put into service mode. If a node is in ESXi maintenance mode or PowerFlex maintenance mode, PowerFlex Manager detects this situation and automatically places the node in service mode and also ensures that the resource group itself goes into service mode. If a node is in PowerFlex maintenance mode for more than 30 minutes, PowerFlex Manager sends a critical alert to SupportAssist.
	**Lifecycle Mode**	The resource group supports health and compliance monitoring, service mode, and non-disruptive updates. All other resource group operations are blocked. Lifecycle mode controls the operations that can be performed for configurations that have limited support.
	**Managed Mode**	The resource group supports health and compliance monitoring, non-disruptive updates, automated resource addition, and automated resource replacement features.

Existing resource groups

If you already have a cluster deployed that includes Dell-based hardware, you can discover and import these hardware resources as an existing resource group. Even though these resources were not originally deployed with PowerFlex Manager, you can take advantage of the health monitoring, compliance, and update features.

When you add an existing resource group for a PowerFlex cluster, PowerFlex Manager matches up the hosts, vCenter, and other items it finds with discovered resources in the resource list.

Only managed or reserved resources are included in the resource group. Any resource discovered as **Unmanaged** is missing from the resource group. If a component is missing, you can change your resource inventory, and update the resource group to reflect these changes. Go to the resources list, select the component, and mark it as **Managed** by selecting **Change resource state to Managed**. Then perform an **Update Resource Group Details** operation on the resource group to pull in the missing component.

Each node is identified as a PowerFlex host if the inventory for the node shows that it is present in a gateway, and it is properly configured as a Storage Data Client (SDC) and Storage Data Server (SDS) node. A PowerFlex host has the **Use Node for Dell PowerFlex** check box set to **True** in the operating system settings for the node within the resource group deployment settings.

You can perform most of the actions on an existing resource group that are available within PowerFlex Manager for a new resource group. For some configurations, PowerFlex Manager displays a yellow banner for the resource group to indicate that some features are not available.

PowerFlex Manager enables you to add an existing resource group for an environment using VMware NSX-T or NSX-V. Most resource group actions are disabled for an NSX-T or NSX-V configuration, except the ability to update the firmware and software components, remove resources (or the resource group as a whole), and update resource group details.

When you add an existing resource group for a CloudLink configuration, you choose a single CloudLink Center as the target for the resource group. If the CloudLink Center for the resource group shuts down, PowerFlex Manager loses communication with the CloudLink Center. If the CloudLink Center is part of a cluster, PowerFlex Manager moves to another CloudLink Center when you update the resource group details.

Lifecycle mode

If you add an existing resource group that includes an unsupported configuration, PowerFlex Manager might put the resource group in lifecycle mode. This mode limits the actions that you can perform within the resource group.

Lifecycle mode allows the resource group to perform only monitoring, service mode, and compliance upgrade operations. All other resource group operations are blocked when the resource group is in lifecycle mode. Lifecycle mode is used to control the operations that can be performed for configurations that have limited support.

When you add an existing resource group, PowerFlex Manager puts the resource group in lifecycle mode if the configuration you want to import includes any of the following:

- Invalid server inventory

- Missing network settings

  The minimum required IP addresses are one data IP and one PowerFlex IP for a storage-only resource group, and one data IP, one PowerFlex IP, and one ESXi IP for a hyperconverged resource group.
- Unsupported NIC (a 1 GB QLogic NIC, for example)
- Unsupported server configurations (an unsupported SD Boot device, for example)
- Unsupported NIC teaming policies, an unsupported switch port configuration, or an unsupported access facing port configuration
- Network configuration without a PXE VLAN setting
- No switch configuration
- PowerFlex MDM cluster without virtual IPs
- DAS cache
- vSphere Cluster Services (vCLS) VMs on local storage

When you add an existing resource group, PowerFlex Manager checks to see whether there are any vSphere Cluster Services (vCLS) VMs on local storage. If it finds any, it puts the resource group in lifecycle mode and lets you migrate the VMs to shared storage.

PowerFlex Manager also puts a resource group in lifecycle mode if you select a minimal compliance version that includes firmware only for the resource group.

When PowerFlex Manager must put a resource group in lifecycle mode, the **Summary** page for the **Add Existing Resource Group** wizard displays a warning message indicating the reason.

In some situations, an imported configuration might not meet the minimal requirements for lifecycle mode. In this case, PowerFlex Manager does not allow you to add the resource group.

For missing virtual IPs or no switch connectivity, you can correct the error and use **Update Resource Group Details** to take the resource group out of lifecycle mode.

If you have manually added NSX to a cluster outside of PowerFlex Manager, click **Update Resource Group Details** on the resource group, so it will correctly reflect the environment with NSX, which will be lifecycle mode.

Templates

This section provides reference information for the **Templates** page.

Related information

Getting started
Managing components

Managing templates

On the **Templates** page, you can view information about templates in a list or tile view. To switch between views, click the tile icon or list icon at the top of the **Templates** page. When in tile view, you can view the templates under a category by clicking the graphic that represents the category.

Users with standard permissions can view details of only those templates for which the administrator has granted permission.

Templates - My Templates List View

The **My Templates** page displays the details of the templates that you have created.

Field	Description
+ Add a Template	Allows you to add a template. After you add a template, you can add node, cluster, and VM components on the template builder page.
Export All	Allows you to export all templates to a CSV file.
Filter By	Allows you to filter and view templates based on the template category.

Field	Description
State	Displays the state of the template - **Draft** or **Published**.
Category	Displays the template category.
Name	Displays the template name.
Last Deployed On	Displays the date when the template was last deployed.
Components	Displays the components in the template.

Templates - Sample Templates

The **Sample Templates** page displays the default templates that you can use in your environment.

Field	Description
Name	Displays the template name.
Components	Displays the components in the template.

Templates

On the **Templates** page, the right pane displays the name of the template, icons of components in the template, and the following details for a selected template:

Field	Description
Edit	Click to edit the template.
Delete	Click to delete the template.
View Details	Click to view the details of the template, such as components in the template.
Clone	Click to clone the template.
Export Template	Click to export the template to a GPG file. You can use the exported template to duplicate the settings.
Created On	Displays the date and time when the template was created.
Created By	Displays the name of the user who created the template.
Updated On	Displays the date and time when the template was updated.
Updated By	Displays the name of the user who updated the template.

Sample templates

This topic lists the sample templates that are provided with PowerFlex Manager.

Template name	Description	Minimum number of nodes required	Minimum number of VMs required	Minimum number of data networks required
Compute - Linux - SW Only	A Linux compute-only, software-only node deployment. This template requires that hyperconverged or storage-only nodes be deployed first.	1	0	1
Compute - ESXi	A standard ESXi compute-only node deployment. This template requires that hyperconverged or storage-only nodes be deployed first.	3	0	2

Template name	Description	Minimum number of nodes required	Minimum number of VMs required	Minimum number of data networks required
Compute - ESXi 100 Gb	An ESXi compute-only node deployment. 100 GB networking deployment. This template requires that hyperconverged or storage-only nodes be deployed first.	3	0	2
Compute - ESXi - Partial Network	A standard ESXi compute-only node deployment with partial network automation. The partial network feature allows you to work with unsupported switches. If you choose to use the partial network feature, you give up the error handling and network automation features that are available with a full network configuration that includes supported switches. This template requires that hyperconverged or storage-only nodes be deployed first.	3	0	2
Compute - Linux	A Linux compute-only node deployment. This template requires that hyperconverged or storage-only nodes be deployed first.	4	0	2
Compute - Linux - Partial Network	A standard Linux compute-only node deployment with partial network automation. The partial network feature allows you to work with unsupported switches. If you choose to use the partial network feature, you give up the error handling and network automation features that are available with a full network configuration that includes supported switches. This template requires that hyperconverged or storage-only nodes to be deployed first.	3	0	2
Hyperconverged	An ESXi standard hyperconverged node deployment.	4	0	2
Hyperconverged - SW only	A Linux hyperconverged, software-only node deployment.	4	0	2
Hyperconverged - 100 Gb	An ESXi hyperconverged node deployment with 100 GB networking. Nodes require Mellanox CX5 or CX6 interface cards.	4	0	2
Hyperconverged - Compression	A standard ESXi hyperconverged node deployment with compression-enabled. Requires NVDIMM in nodes.	4	0	2
Hyperconverged - Encryption	A standard ESXi hyperconverged node deployment with CloudLink encryption. Requires CloudLink Center in environment.	4	0	2
Hyperconverged - Leaf-Spine	An ESXi hyperconverged node deployment with networking without a vPC.	4	0	2

Template name	Description	Minimum number of nodes required	Minimum number of VMs required	Minimum number of data networks required
	This is the most common leaf-spine configuration.			
Hyperconverged - Partial Network	A standard ESXi hyperconverged node deployment with partial network automation. The partial network feature allows you to work with unsupported switches. If you choose to use the partial network feature, you give up the error handling and network automation features that are available with a full network configuration that includes supported switches.	4	0	2
Hyperconverged - Replication	A standard ESXi hyperconverged node deployment with replication enabled.	4	0	3 Two networks for data. One network for replication.
Hyperconverged - Comp - SW Only	A Linux hyperconverged, software-only node deployment with compression enabled. Requires NVDIMM in nodes.	3	0	1
Hyperconverged - Repl - SW Only	A Linux hyperconverged, software-only node deployment with replication enabled.	3	0	1
Management - CloudLink Center	A two node CloudLink Center cluster deployment, for use in encryption templates.	0	2	N/a
PowerFlex File	A PowerFlex file cluster deployment.	2	0	Four PowerFlex Data networks One NAS File Data network **NOTE:** Two NAS File Data networks are recommended for redundancy.
PowerFlex File - SW Only	A PowerFlex file cluster deployment in a software-only environment.	2	0	1
Storage	A standard storage-only node deployment.	4	0	2
Storage - Perf, No HA Management	A storage-only non-HA management node deployment.	4	0	2
Storage - SW Only	A storage-only, software-only node deployment.	3	0	1
Storage - Compression - SW Only	A storage-only, software-only node deployment with compression enabled.	3	0	1

Template name	Description	Minimum number of nodes required	Minimum number of VMs required	Minimum number of data networks required
	Requires NVDIMM in nodes.			
Storage - Replication - SW Only	A storage-only, software-only node deployment with replication enabled. Configures storage data replicator (SDR) and journal capacity.	3	0	2 One network for data. One network for replication.
Storage with NVMe/TCP	A storage-only node deployment with NVMe/TCP.	4	0	2
Storage with NVMe/TCP - SW Only	A storage-only, software-only node deployment with NVMe/TCP.	3	0	1
Storage - 100 Gb	A storage-only node deployment with 100 GB networking. Nodes require Mellanox CX5 or CX6 interface cards.	4	0	2
Storage - Compression	A storage-only node deployment with compression enabled. Requires NVDIMM in nodes.	4	0	2
Storage - Encryption	A storage-only node deployment with encryption enabled.	4	0	2
Storage - Partial Network	A storage-only node deployment with partial network deployment. The partial network feature allows you to work with unsupported switches. If you choose to use the partial network feature, you give up the error handling and network automation features that are available with a full network configuration that includes supported switches.	4	0	2
Storage - Replication	A storage-only node deployment with replication enabled. Configures storage data replicator (SDR) and journal capacity.	4	0	2

Related information

Deploy software management

Building a template overview

The template builder allows you to build a customized template by configuring both physical and virtual components. On the template builder page, you can set the component properties. For example, you can create a template that provisions only physical nodes with operating systems on them.

NOTE: A newly created or a cloned template appears in a draft state on the **Template** page and remains in the same state until published.

You can configure node, cluster, and VM components in a template.

The template builder page displays a graphical representation of the topology that is created within a particular template. From this page, you can:

- Add node, cluster, and VM components to a template
- Build and publish a template
- Delete a template
- Import a template
- Deploy a resource group (this feature is available only on published templates)

Component types

Components (physical or virtual or applications) are the main building blocks of a template.

PowerFlex Manager has the following component types:

- Node (Software/hardware and software only)
- Cluster
- VM

Related information

Adding components to a resource group
Edit a template
Deploying a resource group
View template details

Node settings

This table describes the following node settings: hardware, BIOS, operating system, and network.

Setting	Description
Full network automation	Allows you to perform deployments with full network automation. This feature allows you to work with supported switches, and requires less manual configuration. Full network automation also provides better error handling since PowerFlex Manager can communicate with the switches and identify any problems that may exist with the switch configurations.
Partial network automation	Allows you to perform switchless deployments with partial network automation. This feature allows you to work with unsupported switches, but requires more manual configuration before a deployment can proceed successfully. If you choose to use partial network automation, you give up the error handling and network automation features that are available with a full network configuration that includes supported switches. For a partial network deployment, the switches are not discovered, so PowerFlex Manager does not have access to switch configuration information. You must ensure that the switches are configured correctly, since PowerFlex Manager does not have the ability to configure the switches for you. If your switch is not configured correctly, the deployment may fail and PowerFlex Manager is not able to provide information about why the deployment failed. For a partial network deployment, you must add all the interfaces and ports, as you would when deploying with full network automation. However, you do not need to add the operating system installation network, since PXE is not required for partial network automation. PowerFlex Manager uses virtual media instead for deployments with partial network automation. The **Switch Port Configuration** must be set to **Port Channel (LACP enabled)**. In addition, the LACP fallback or LACP ungroup option must be configured on the port channels.
Component Name	Indicates the node component name

Setting	Description
Drive Encryption Type	Specifies the type of encryption to use when encryption is enabled. The encryption options are: • Software encryption • Self-encrypting drive (SED)
Number of Instances	Enter the number of instances that you want to add. If you select more than one instance, a single component representing multiple instances of an identically configured component is created. Edit the component to add extra instances. If you require different configuration settings, you can create multiple components.
Related Components	Select **Associate All** or **Associate Selected** to associate all or specific components to the new component.
Import Configuration from Reference Node	Click this option to import an existing node configuration and use it for the node component settings. On the **Select Reference Node** page, select the node from which you want to import the settings and click **Select**.
OS Settings	
Host Name Selection	If you choose **Specify At Deployment Time**, you must type the name for the host at deployment time. If you choose **Auto Generate**, PowerFlex Manager displays the **Host Name Template** field to enable you to specify a macro that includes variables that produce a unique hostname. For details on which variables are supported, see the context-sensitive help for the field. If you choose **Reverse DNS Lookup**, PowerFlex Manager assigns the hostname by performing a reverse DNS lookup of the host IP address at deployment time.
OS Image	Specifies the location of the operating system image install files. You can use the image that is provided with the target compliance file, or specify your own location, if you created additional repositories. To deploy a compute-only or storage-only resource group with the Linux image that is provided with a compliance file, choose **Use Compliance File Linux image**. If you want to deploy a NAS cluster, you must also choose **Use Compliance File Linux image**. To deploy a storage-only resource group with Red Hat Enterprise Linux, you must create a repository on the **Settings** page and specify the path to the Red Hat Enterprise Linux image on a file share. Dell Technologies recommends that you use one of your own images that are published from the customer portal at Red Hat Enterprise Linux. For Linux, you may include one node within a resource group. For ESXi, you must include at least two nodes. **NOTE:** If you select an operating system from the **OS Image** drop-down menu, the field **NTP Server** displays. This field is optional, but it is highly recommended that you enter an NTP server IP to ensure proper time synchronization with your environment and PowerFlex Manager. Sometimes when time is not properly synchronized, resource group deployment failure can occur.
OS Credential	Select an **OS Admin** or **OS User** credential that you created on the **Credentials Management** page. Alternatively, you can create a credential while you are editing a template. If you select a credential that was created on the **Credentials Management** page, you do not need to type the username and password, since they are part of the credential definition.

Setting	Description
	PowerFlex Manager allows to specify a non-root user instead of the root user when you configure a template for a compute-only, storage-only, or hyperconverged deployment.
NTP Server	Specifies the IP address of the NTP server for time synchronization. If adding more than one NTP server in the operating system section of a node component, be sure to separate the IP addresses with commas.
Use Node For Dell PowerFlex	Indicates that this node component is used for a PowerFlex deployment. When this option is selected, the deployment installs the MDM, SDS, and SDC components, as required for a PowerFlex deployment in a VMware environment. The MDM and SDS components are installed on a dedicated PowerFlex VM (SVM), and the SDC is installed directly on the ESXi host. To deploy a PowerFlex cluster successfully, include at least three nodes in the template. The deployment process adds an SVM for each hyperconverged node. PowerFlex Manager uses the following logic to determine the MDM roles for the nodes: 1. Checks the PowerFlex gateway inventory to see how many primary MDMs, secondary MDMs, and tiebreakers are present, and the total number of SDS components. 2. Adds the number of components being deployed to determine the overall PowerFlex cluster size. For example, if there are three SDS components in the PowerFlex gateway inventory, and you are deploying two more, you will have a five node cluster after the deployment. 3. Adds a single primary MDM and determines how many secondary MDMs and tiebreakers should be in the cluster by looking at the overall cluster size. The configuration varies depending on the size of the cluster: ● A three-node cluster has one primary, one secondary, and one tiebreaker. ● A five-node cluster has one primary, two secondaries, and two tiebreakers. 4. Determines the roles for each of the new components being added, based on the configuration that is outlined above, and the number of primary, secondary, and tiebreakers that are already in the PowerFlex cluster. At deployment time, PowerFlex Manager automatically sets up the DirectPath I/O configuration on each hyperconverged node. This setup makes the devices available for direct access by the virtual machines on the host and also sets up the devices to run in PCI passthrough mode. For each SDS in the cluster, the deployment adds all the available disks from the nodes to the storage pools created. For each compute-only or hyperconverged node, the deployment installs the SDC VIB. When you select this option, the teaming and failover policy for the cluster are automatically set to **Route based on IP hash**. Also, the uplinks are configured as active and active, instead of active and standby. Teaming is configured for all port groups, except for the PowerFlex data 1 and PowerFlex data 2 port groups. If you select the option to **Use Node For Dell PowerFlex**, the **Local Flash storage for Dell PowerFlex** option is automatically selected as the **Target Boot Device** under **Hardware Settings**.
PowerFlex Role	Specifies one of the following deployment types for PowerFlex: ● **Compute Only** indicates that the node is only used for compute resources. ● **Storage Only** indicates that the node is only used for storage resources.

Setting	Description
	• **Hyperconverged** indicates that the node is used for both compute and storage resources. If you select an ESXi image type in the **OS Image** field, the **PowerFlex Role** must be set to **Compute Only** or **Hyperconverged**. If you add a compute-only node, only the SDC is added. If you add a hyperconverged node, both the SDC and SDS are added. If you select a Red Hat Enterprise Linux image type in the **OS Image** field, the **PowerFlex Role** must be set to **Storage Only**. If you add a storage-only node, only the SDS is added. The only prerequisites for a storage-only node are that the iDRAC must have an IP address and a credential. PowerFlex Manager takes care of all other configuration steps that are required for the node. For each node, PowerFlex Manager configures the MDM roles as needed and configures the SDS RPMs. Once the cluster is set up, PowerFlex Manager adds every node as an SDS. Then, it adds all available disks for the SDS device, adds a storage pool, and adds all disks to the storage pool. If you are creating a compute-only or hyperconverged template, be sure to include both the **VMware Cluster** and **PowerFlex Cluster** components in the template builder. If you are creating a storage-only template, do not include a **VMware Cluster** component in the template builder. Only the **PowerFlex Cluster** component is required for a storage-only template. For a NAS template, be sure to select **Compute Only** as the role and add both the **PowerFlex Cluster** and **PowerFlex File Cluster** components to the template.
Enable PowerFlex File	Enables NAS capabilities on the node. If you want to enable NAS on the nodes in a template, you need to add both the **PowerFlex Cluster** and **PowerFlex File Cluster** components to the template. This option is only available if you choose **Use Compliance File Linux Image** as the **OS Image** and then choose **Compute Only** as the **PowerFlex Role.** If **Enable PowerFlex File** is selected, in the **Hardware Settings** section, the only available choice for **Target Boot Device** is **Local Hard Drive**. If **Enable PowerFlex File** is selected, you must ensure that the template includes the necessary **NAS File Management** and **NAS File Data** networks. If you do not configure these networks on the template, the template validation fails.
Client Storage Access	Determines how clients access storage. For a storage-only role, select one of the following options: • Storage Data Client (SDC) Only • SDC and NVMe/TCP Initiator For a compute-only role the Client Storage Access control is not displayed, and the client access is set to SDC automatically. For a hyperconverged role, the Client Storage Access control is not displayed, and the client access is set to SDC/SDS automatically.
Enable Compression	Enables compression on the protection domain. This option allows you to take advantage of PowerFlex NVDIMM (non-volatile inline memory module) compression. You can enable compression on a storage-only or hyperconverged resource group. Compression is supported for new resource group deployments, and existing resource groups. You can also enable compression for storage-only and hyperconverged nodes when performing a scale up of a resource group. If you select this option, PowerFlex Manager looks for nodes that have at least two NVDIMMs installed, and SSD or NVMe, and have persistent memory. Fine granularity is not supported on HDDs.

Setting	Description
	If compression is enabled, the template adds fields to the **PowerFlex Cluster Settings** to allow you to specify an acceleration pool name and granularity setting for the storage pool. The storage pool must be set to fine granularity. The compression method at the storage pool level is overridden by the setting at the volume level. PowerFlex Manager creates the acceleration pool and sets the granularity according to **PowerFlex Cluster Settings** when you deploy the resource group.
Enable Encryption	Enables disk encryption on the node. This option allows you to take advantage of CloudLink encryption. You can enable CloudLink encryption on a storage-only or hyperconverged resource group. Encryption is supported for new resource group deployments, and existing resource groups. You can also enable encryption for storage-only and hyperconverged nodes when performing a scale up of a resource group. A resource group cannot mix encrypted and unencrypted nodes. Scale up of a storage-only or hyperconverged resource group is supported, with the new nodes using the same encryption settings as the nodes already in the resource group. If you select this option, PowerFlex Manager looks for servers with 12 cores or more for CloudLink deployments. After encryption is enabled, the template displays a warning message indicating that the template is missing some data. The template adds the **Cloud Link Center Settings** section to the PowerFlex cluster component to allow you to specify the required data. Some PowerFlex nodes might not be selected for deployment, depending on the encryption type that is selected. For example, if you choose **Software Encryption**, you cannot include a PowerFlex node with only SEDs. If you choose **Self Encrypting Drive**, you cannot include a PowerFlex node with only software encryption drives. PowerFlex Manager does not allow you to mix SEDs and software encryption drives in the same protection domain. Servers do not typically have this drive combination, but PowerFlex Manager verifies the drives and uses only servers of the specified type. **Validate Settings** detects PowerFlex nodes that do not match the specified **Drive Encryption Type**.
Enable Replication	Enables replication for a storage-only or hyperconverged resource group. Replication allows you to mirror the data across different geographical sites using native volume-level asynchronous replication. PowerFlex Manager deploys and configures the storage data replicator (SDR) on all SDS nodes. PowerFlex Manager configures the journal capacity before adding the SDR. If you enable replication for a template, you must have two different replication networks attached to the template before you can publish it. When replication is enabled, PowerFlex Manager lets you set the **Journal Capacity** at the time you deploy the resource group, or when you add a node to the resource group.
Drive Encryption Type	Specifies the type of encryption to use when encryption is enabled. The options are: • **Software Encryption** • **Self Encrypting Drive (SED)** Some nodes might not be selected for deployment, depending on the encryption type selected. For example, if you choose **Software Encryption**,

Setting	Description
	you cannot include a node with only SEDs. Similarly, if you choose **Self Encrypting Drive**, you cannot include a node with only software encryption drives. PowerFlex Manager does not allow you to mix SEDs and software encryption drives in the same protection domain. Servers should not typically have this mix, but PowerFlex Manager checks for this and uses only servers of the type you specify. **Validate Settings** detects nodes that do not match the specified **Drive Encryption Type**.
Switch Port Configuration	Specifies whether Cisco virtual PortChannel (vPC) or Dell Virtual Link Trunking (VLT) is enabled or disabled for the switch port. For hyperconverged templates, the options are: ● **Port Channel** turns on vPC or VLT. ● **Port Channel (LACP enabled)** turns on vPC or VLT with the link aggregation control protocol enabled. For storage-only and compute-only templates that use a Linux operating system image, the options are: ● **Port Channel (LACP enabled)** turns on vPC or VLT with the link aggregation control protocol enabled. For a compute-only template that uses an ESXi operating system image, the **Switch Port Configuration** setting includes all three options: ● **Port Channel** turns on vPC or VLT. ● **Port Channel (LACP enabled)** turns on vPC or VLT with the link aggregation control protocol enabled.
Teaming And Bonding Configuration	The teaming and bonding configuration options depend on the switch port configuration selected. For hyperconverged and compute-only templates, the following options are available: ● If you choose **Port Channel** (LACP enabled) as the switch port configuration, the only teaming and bonding option is **Route Based on IP hash**. For storage-only templates, the following options are available: ● If you choose **Port Channel (LACP enabled)** as the switch port configuration, the only teaming and bonding option is **Mode 4 (IEEE 802.3ad policy)**.
Hardware Settings	
Target Boot Device	Specifies the target boot device. ● **Local Flash Storage**: Installs the operating system to either the SATADOM or the BOSS flash storage device present in the node. With the **Local Flash Storage** option, only nodes with a BOSS storage controller and two attached hard drives or SATADOM are selected to be deployed as part of the resource group, depending on the Dell PowerEdge servers used. For PowerEdge servers that support BOSS, during deployment PowerFlex Manager creates RAID 1 with the two hard drives attached to the BOSS controller. ● **Local Flash storage for Dell PowerFlex**: Installs the operating system to either the SATADOM or the BOSS flash storage device that is present in the node and configures the node to support PowerFlex.

Setting	Description
	If you select the option to **Use Node for Dell PowerFlex** under **OS Settings**, the **Local Flash storage for Dell PowerFlex** option is automatically selected as the target boot device. ● **Local Hard Drive**: Installs the operating system to a local RAID storage device in a RAID 1 configuration if a PERC H730P or H740P device is present in the node.
Node Pool	Specifies the pool from which nodes are selected for the deployment.
BIOS Settings	
System Profile	Select the system power and performance profile for the node.
User Accessible USB Ports	Enables or disables the user-accessible USB ports.
Number of Cores per Processor	Specifies the number of enabled cores per processor.
Virtualization Technology	Enables the additional hardware capabilities of virtualization technology.
Logical Processor	Each processor core supports up to two logical processors. If enabled, the BIOS reports all logical processors. If disabled, the BIOS reports only one logical processor per core.
Execute Disable	Enables or disables execute disable memory protection.
Node Interleaving	Enable or disable the interleaving of allocated memory across nodes. ● If enabled, only nodes that support interleaving and have the read/write attribute for node interleaving set to enabled are displayed. Node interleaving is automatically set to enabled when a resource group is deployed on a node. ● If disabled, any nodes that support interleaving are displayed. Node interleaving is automatically set to disabled when a resource group is deployed on a node. Node interleaving is also disabled for a resource group with NVDIMM compression. ● If not applicable is selected, all nodes are displayed irrespective of whether interleaving is enabled or disabled. This setting is the default.
Network Settings	
Multi-Network Selection	Select the check-box to include multiple management networks of the same type. If you select multiple networks of the same type without selecting the check box, an error is displayed when you publish the template. The multiple network selection is supported on the following networks: ● Hypervisor Management ● PowerFlex Management ● Hypervisor Migration ● Replication Networks
Number of Replication Networks Per Node	This option is displayed only if the **Multi-Network Selection** and **Enable Replication** check boxes are enabled. Select the number of networks you want to add to the port. For example, if the selected number is 2, you can assign one network each to two ports—Port 1 and Port 2. It is recommended that the number of selected networks is always even.
Add New Interface	Click **Add New Interface** to create a network interface in a template component. Under this interface, all network settings are specified for a node. This interface is used to find a compatible node in the inventory. For example, if you add **`Two Port, 100 gigabit`** to the template, when the template is deployed PowerFlex Manager matches a node with a two-port 100-gigabit network card as its first interface.

Setting	Description
	To add one or more networks to the port, select **Add Networks to this Port**. Then, choose the networks to add, or mirror network settings defined on another port. To see network changes that are previously made to a template, you can click **View/Edit** under **Interfaces**. Or, you can click **View All Settings** on the template, and then click **View Networks**. To see network changes at resource group deployment time, click **View Networks** under **Interfaces**.
Add New Static Route	Click **Add New Static Route** to create a static route in a template. To add a static route, you must first select **Enabled** under **Static Routes**. A static route allows nodes to communicate across different networks. The static route can also be used to support replication in a storage-only or hyperconverged resource group. A static route requires a **Source Network** and a **Destination Network**, and a **Gateway**. The source and destination network must each be a PowerFlex data network or replication network that has the **Subnet** field defined. If you add or remove a network for one of the ports, the **Source Network** drop-down list does not get updated and still shows the old networks. In order to see the changes, save the node settings and edit the node again.
Validate Settings	Click **Validate Settings** to determine what can be chosen for a deployment with this template component. The **Validate Settings** wizard displays a banner to when one or more resources in the template do not match the configuration settings that are specified in the template. The wizard displays the following tabs: ● **Valid (*number*)** lists the resources that match the configuration settings. ● **Invalid (*number*)** lists the resources that do not match the configuration settings. The reason for the mismatch is shown at the bottom of the wizard. For example, you might see `Network Configuration Mismatch` as the reason for the mismatch if you set the port layout to use a 100-Gb network architecture, but one of the nodes is using a 25 GB architecture. If you set the encryption method to use self-encrypting drives (SEDs), but the nodes do not have these drives, you might see `Self Encrypting Drives are required but not found on the node, or software encryption requested but only available drives are SED`.

After entering the information about operating system Installation (PXE) network in the respective field as described in the table above, PowerFlex Manager untags vLANs entered in the operating system installation network on the switch node facing port. For vMotion and hypervisor networks, PowerFlex Manager tags these networks on the switch node-facing ports for the entered information. For rack node, PowerFlex Manager configures the vLANs on node facing ports (untag PXE vLANs, and tag other vLANs).

If you select **Import Configuration from Reference Node**, PowerFlex Manager imports basic settings, BIOS settings, and advanced RAID configurations from the reference node and enables you to edit the configuration. Some BIOS settings might no longer apply once new BIOS settings are applied. PowerFlex Manager does not correct these setting dependencies. When setting advanced BIOS settings, use caution and verify that BIOS settings on the hardware are applicable when not choosing **Not Applicable** as an option. For example, when disabling SD card, the settings for internal SD card redundancy become not applicable.

You can edit any of the settings visible in the template, but keep in mind that many settings are hidden when using this option. For example, only ten out of many BIOS settings that you can see and edit using template are displayed. However, you can configure all BIOS settings. If you want to edit any of the settings that are not visible through the template feature, edit them before importing or uploading the file.

Cluster component settings

This table describes the cluster component settings.

Field name	Description
Select a Component	Select **VMware Cluster** or **PowerFlex Cluster**.
Component Name	Indicates the cluster component name.
Related Components	Select **Associate All** or **Associate Selected** to associate all or specific components to the new component.
Cluster settings (for the VMware cluster component)	
Target Virtual Machine Manager	Select virtual machine manager from the **Target Virtual Machine Manager** list.
Data Center Name	Select the data center name from **Data Center Name** list.
Cluster Name	Select a new cluster name from **Cluster Name** list.
New Cluster Name	Select new cluster name from **New Cluster Name** list.
Cluster HA Enabled	Enables or disables a highly available cluster. You can either select or clear (default) the check box.
Cluster DRS Enabled	Enables or disables distributed resource scheduler (DRS). You can either select or clear (default) the check box.
PowerFlex settings (for the PowerFlex cluster component)	
Target PowerFlex Gateway	Select a target PowerFlex gateway, which acts as an endpoint for PowerFlex API calls. During the provisioning process, PowerFlex Manager connects to the PowerFlex gateway and uses its APIs to configure all SDS and SDC parameters.
Protection Domain Name	Provide a name for the protection domain. You can automatically generate the name (recommended), or specify a new name explicitly. A protection domain is a logical entity that contains a group of SDSs that provide backup for each other. Each SDS belongs to only one protection domain. Each protection domain is a unique set of SDSs. A protection domain may also contain SDTs and SDRs. If you automatically generate the protection domain name or specify a new name explicitly for a hyperconverged or storage-only template, the PowerFlex cluster must have at least three nodes before you can publish the template and deploy it as a resource group. However, if you select an existing protection domain that is associated with another previously deployed hyperconverged or storage-only resource group, and this protection domain has at least three nodes, PowerFlex Manager recognizes the new template as valid if the cluster has fewer than three nodes. You can publish the template successfully and deploy it as a resource group, since the protection domain it uses has enough nodes. **NOTE:** A compute-only resource group only requires a minimum of two nodes, since it does not have a protection domain. If you choose **Compute Only** as the **PowerFlex Role** for the node component, the **PowerFlex** settings do not include the **Protection Domain Name** field.
New Protection Domain Name	Specify a new name for the protection domain.
Protection Domain NameTemplate	If you choose to generate the protection domain name automatically, PowerFlex Manager fills this field with a default template that combines static text with variables for several pieces of the autogenerated name. If you modify the template, be sure to include the *${num}* variable to ensure that the name is unique. For details on the rules for defining a template, see the contextual help that appears when you hover over the field.

Field name	Description
	If you choose **Compute Only** as the **PowerFlex Role** for the node component, the **PowerFlex** settings do not include the **Protection Domain Name Template** field.
Acceleration Pool Name	Provide a name for the acceleration pool. You can automatically generate the name (recommended) or select from a list of existing acceleration pools. You can add acceleration pools to a protection domain to accelerate storage pool performance. An acceleration pool is a group of acceleration devices within a protection domain.
Acceleration Pool Name Template	Define a template for generating the acceleration pool name automatically. PowerFlex Manager fills this field with a default template that combines static text with variables for several pieces of the autogenerated name. If you modify the template, be sure to include the *$(num)* variable to ensure that the name is unique. For details on the rules for defining a template, see the contextual help that appears when you hover over the field.
Storage Pool Name	Provide a name for the storage pool. You can automatically generate the name (recommended), select from a list of existing storage pools for the selected protection domain, or specify a unique storage pool name. If you choose to automatically generate a name, you are prompted to define a storage pool name template. Storage pools allow the generation of different storage tiers in PowerFlex. A storage pool is a set of physical storage devices in a protection domain. Each storage device belongs to one (and only one) storage pool. The number of storage pools that are created at deployment time depends on the number of disks available.
Number Of Storage Pools	Select up to 6 storage pools per protection domain. The maximum number of nodes that can be added to a protection domain is 32. The maximum number of drives that can be added to a storage pool is 320.
Granularity	Set the granularity for compression by selecting **Fine** or **Medium**. The granularity setting applies to the storage pool.
Storage Pool Disk Type	Allows you to select the disk type - hard drive, SSD, or NVMe.
Storage Pool Name Template	Define a template for generating the storage pool name automatically. PowerFlex Manager fills this field with a default template that combines static text with variables for several pieces of the autogenerated name. If you modify the template, be sure to include the *${num}* variable to ensure that the name is unique. For details on the rules for defining a template, see the contextual help that appears when you hover over the field. If you choose **Compute Only** as the **PowerFlex Role** for the node component, the **PowerFlex** settings do not include the **Storage Pool Name Template** field.
Enable Fault Sets	Enables deployment with fault sets. This option allows you to deploy a fault set enabled resource group with a new protection domain or an existing protection domain.
Fault Set Name	Specify the fault set name. You can automatically generate the name (recommended), select from a list of existing fault sets for the selected protection domain, or specify a unique fault set name. If you choose to automatically generate a name, you are prompted to define a fault set name template.
Fault Set Name Template	If you choose to generate the fault set name automatically, PowerFlex Manager fills this field with a default template that combines static text with variables for several

Field name	Description
	pieces of the autogenerated name. If you modify the template, be sure to include the *${num}* variable to ensure that the name is unique. For details on the rules for defining a template, see the contextual help that appears when you hover over the field.
Number of Fault Sets	Specifies the number of fault sets to create at deployment time. PowerFlex requires a minimum of three fault sets for a protection domain, with at least two nodes in each fault set. For a new protection domain name, you must specify a number between 3 and 16. Each fault set acts as a single fault unit. If a fault set goes down, all nodes within the fault set go down as well. For an existing protection domain name, you must specify a number between 1 and 16. This allows you to add more fault sets to an existing protection domain. If the selected protection domain already has 3 fault sets, for example, you can specify a number as low as 1, to include an additional fault set for this protection domain. PowerFlex Manager ensures that each new deployment has only one MDM role for each fault set. For example, if you deploy 3 fault sets, one has the primary MDM, another has the secondary MDM, and the third has the tiebreaker. You can use the **Reconfigure MDM Roles** wizard to change the MDM role assignments after deployment.
CloudLink Center Settings	
Target CloudLink Center	Specifies the target CloudLink Center for an encrypted node. The **Cloud Link Center Settings** are only available when the **Enable Encryption** option is selected in the **OS Settings** for the node component. For any CloudLink Center that has encryption, you must either add an existing resource group to PowerFlex Manager, or use PowerFlex Manager to create the CloudLink encryption machine groups and keystores. PowerFlex Manager is only able to create the machine groups and keystores if the CloudLink Center exists in the management cluster. Ensure that CloudLink Center is available on the resource page. If you select an existing protection domain under the **PowerFlex Settings**, you must choose a **Target CloudLink Center**. The other CloudLink Center settings are not available, and PowerFlex Manager uses the machine group and keystore settings for the selected target. If you automatically generate the protection domain name or specify a new protection name explicitly, you can set the **Machine Group Name** and **Keystore Name** settings with the template. When you deploy a template with CloudLink settings, PowerFlex Manager creates the machine groups and keystores, and then assigns the machine groups to keystores and networks. Next, it adds the machines to the machine groups, and encrypts the drives. After deployment, you can see the machines that are added to machine groups by clicking **View Details** on the **Resources** page. When defining a template, you choose a single CloudLink Center as the target for the deployed resource group. If the CloudLink Center for the resource group shuts down, PowerFlex Manager loses communication with the CloudLink Center. If the CloudLink Center is part of a cluster, PowerFlex Manager moves to another CloudLink Center when you update the resource group details.
Machine Group Name	Allows you to provide a name for the machine group. The **Machine Group Name** is only available if you automatically generate the protection domain name or specify a new protection name explicitly. You can automatically generate the machine group name or specify a new machine group name explicitly.
New Machine Group Name	Specify a new name for the machine group.

Field name	Description
Keystore Name	Allows you to provide a name for the keystore. The **Keystore Name** is only available if you automatically generate the protection domain name or specify a new protection name explicitly. You can automatically generate the keystore name or specify a new keystore name explicitly. Alternatively, you can choose an existing keystore from the list.
Keystore Name Template	Specify a new name for the keystore.
vSphere VDS Settings	
Configure VDS Settings	Click **Configure VDS Settings** to create the virtual distributed switch (VDS) settings for the VMware cluster component in a template. PowerFlex Manager displays a wizard that allows you to provide a name for each VDS. The wizard also lets you specify how you want the port group names to be created. You can let PowerFlex Manager automatically create port group names based on the names of the networks, or you can enter the port group names yourself. To see VDS settings previously configured for a template, you can click **View VDS Settings** under **vSphere VDS Settings**. **NOTE:** When working with VMware vCenter in a multi data center configuration, VMware vSphere distributed switch names (vDS) must be unique. Work with the *Logical Configuration Survey* contact to plan vDSs based on the data center design.
PowerFlex File Settings	
PowerFlex File Gateway	Specifies the name of the NAS gateway.
Number of Protection Domains	Determines the number of protection domains that are used for PowerFlex file configuration data. Control volumes will be created automatically for every node in the PowerFlex file cluster, and spread across the number of protection domains specified for improved cluster resiliency. To add data volumes, you need to use the tools provided on the **File** tab. You can have between one and four protection domains.
Protection Domain <n>	Includes a separate section for each protection domain used in the template.
Storage Pool <n>	Includes a separate section for each storage pool used in the template.

Related information

Add cluster component settings to a template

VM settings

The table describes VM settings for the CloudLink Center and the PowerFlex gateway.

Field name	Description
Select a Component	Select **CloudLink Center** or **PowerFlex Gateway**.
Number of Instances	Select the number of instances of the VM that you want to deploy.
Related Components	Select **Associate Selected** and select the **VMware Cluster** check box to associate the selected VMware cluster with the CloudLink Center.
VM Settings	
Specify Datastore	Specify the storage location.
Specify Network	Select the network type.

Field name	Description
CloudLink Settings	
Host Name Selection	Defines how the hostname is selected at deployment time. There are two options: ● Auto Generate - Select to autogenerate the hostname at deployment time. ● Specify at Deployment Time - Select to provide a unique hostname at deployment time.
OS Credential	Select the operating system credential used to set the username and password on the operating system that is installed.
NTP Server	Specify the IP address of the NTP server for time synchronization. If adding more than one NTP server, ensure that you separate the IP addresses with commas.
Secadmin Credential	Select the secadmin credential, an element manager credential, which is used to set the password for the secadmin user of the CloudLink Center. The password should be minimum of ten characters with at least one special character.
Vault Password	Specify up to three unique passwords for the CloudLink Vault. You must specify at least one. The password should be minimum of ten characters with at least one special character.
Confirm Vault Password	Retype the vault password.
License File	Upload a new or additional software license file. If additional, the resource is added to your current total resources.
Additional CloudLink Settings	
Configure Syslog Forwarding	Select the check box to send syslog messages from the CloudLink to a remote network management system.
Syslog Facility	Select the remote server where the syslog messages are forwarded to.
Configure Email Notifications	Select the check box to configure email alerts.
Server Address	Specify the IP address of the email server.
Port	Specify the port number for the email server. The default port is 25. The port numbers must be entered in comma-separated list and must be 1–65535.
Sender Address	Specify the email address for the sender.
User Name	Specify the required username.
Password	Specify the required password.
Confirm Password	Retype the password.
PowerFlex Gateway Settings	
Host Name Selection	Defines how the hostname is selected at deployment time. There are two options: ● Auto Generate - Select to autogenerate the hostname at deployment time. ● Specify at Deployment Time - Select to provide a unique hostname at deployment time.
PowerFlex Credential	Select the operating system credential used to set the username and password.
NTP Server	Specify the IP address of the NTP server for time synchronization. If adding more than one NTP server, ensure that you separate the IP addresses with commas.

Support for full and partial network automation

This topic lists the supported configurations for full and partial network automation.

Template components	Full network automation	Partial network automation (Requires manual switch configuration)
OS Images	ESXi, CentOS, Red Hat Enterprise Linux	ESXi, CentOS, Red Hat Enterprise Linux
PowerFlex roles	Hyperconverged, compute-only, storage-only	Hyperconverged, compute-only, storage-only (CentOS only)
Switch Port Configuration	• Port channel (LACP enabled) • Port channel • Trunk port	Port channel (LACP enabled)
Target Boot Device	• Local flash storage for Dell PowerFlex • Local hard drive	Local flash storage for Dell PowerFlex
Network Settings	• Static bonding NIC port design or LACP bonding NIC port design • 10 GB, 25 GB, 100 GB • Required PXE network • Network Automation Type: Full	• LACP bonding NIC port design • 25 GB • No PXE network (using iDRAC virtual media) • Network Automation Type: Partial

Related information

Adding an existing resource group
Build and publish a template

Resources

This section provides reference information for the **Resources** page.

Related information

Deploying and provisioning
Managing components
Monitoring system health

Resource health status

PowerFlex Manager assigns health status to the resources based on the conditions described in the following table.

Icon	Health status	Description
	Healthy	Indicates that there is no issue with the resource and it is working as expected.
	Warning	Indicates that the resource is in a state that requires corrective action, but does not affect overall system health. For example, the firmware running on the resource is not at the required level or not compliant. For supported switches, a warning health status might be because the SNMP community string is invalid or not set correctly. In this case, PowerFlex Manager is unable to perform health monitoring for the switch.

Icon	Health status	Description
		NOTE: If the resource group has VMware ESXi and is set to maintenance mode, a message is displayed in the **View Details** pane.
	Critical	Indicates that an issue requiring immediate attention exists in one of the following hardware or software components in the device: • Battery • CPU • Fans • Power supply • Storage devices • Licensing For supported switches, a critical health status might indicate that the power supply is not working properly or a CPU has overheated. **NOTE:** If the resource group is in a power off state, a message displays in the **View Details** pane.
	Unknown	Indicates that the resource status is unknown. For example, for a supported switch, an unknown status might indicate that the switch has been turned off or is still being discovered.
	Pending	Indicates that the resource status is pending.
	Service Mode	Indicates that the resource is in **Service Mode**. **NOTE:** If the resource fails to exit **Service Mode**, an informational message displays in the recent activity.

Related information

Discover a resource
Removing resources
Exporting a compliance report for all resources

Resource operational state

After initiating resource discovery, PowerFlex Manager assigns one or more of the states to the resources. These operational states display on the **Resources** page, in the **Deployment Status** column of the **All Resources** tab.

Deployment status	Description
Not In Use	Resource is available for deployment.
Available	Resource is available. Applies only to switches, virtual machine, or gateway.
Deploying	Resource is in the process of being deployed in a resource group.
In Use	Resource is deployed in a resource group.
Pending Updates	One or more of the following tasks are in progress: • Discovering resource • Determining resource details, including firmware version • Applying template to the resource • Updating firmware

Deployment status	Description
	• Removing resource from PowerFlex Manager inventory
Deployment Failed	Resource group deployment failed.
Cancelled	Resource group deployment is cancelled.

PowerFlex Manager keeps track of which resources it is managing. These operational states display on the **Resources** page, in the **Managed State** column of the **All Resources** tab.

Managed state	Description
Managed	Indicates that PowerFlex Manager manages the firmware on that node, and the node can be used for deployments.
Unmanaged	Indicates that the resource is not managed by PowerFlex Manager. By default, the operational state for all discovered nodes is **Unmanaged**. If you want to perform firmware updates or deployments on a discovered node, you need to select the node and change the operational state to **Managed**. If you have not yet uploaded a license file, PowerFlex Manager is configured for monitoring and alerting only. All resources are restricted to the **Unmanaged** resource state, and you cannot change the state to **Managed** or **Reserved**.
Reserved	Indicates that PowerFlex Manager only manages the firmware on that particular node, but that node cannot be used for deployments. You can assign a host to the reserved state only if the host has been discovered, but is not part of a resource group.

Compliance status

PowerFlex Manager assigns one of the following firmware statuses to the resources:

Firmware status	Description
Compliant	The firmware running on the resource is compliant with the firmware version that is specified in the default compliance version.
Non–Compliant	The firmware running on the resource is less than or greater than the firmware version specified in the default compliance version. Indicates that firmware update is required.
Update Required	The firmware running on the resource is less than the minimum firmware version recommended in the default compliance version. Indicates that firmware update is required.

Related information

Discover a resource
Removing resources
Exporting a compliance report for all resources

Discovery overview

You can discover new resources or existing resources that are already configured within your environment. After discovery, you can deploy resource groups on these resources from a template. Only administrator-level users can discover resources.

By default, the operational state for all discovered nodes is **Unmanaged**. If you want to perform firmware updates or deployments on a discovered node, select the node and change the operational state to **Managed**.

If you have not yet uploaded a license, PowerFlex Manager is configured for monitoring and alerting only. In this case, all the resources are restricted to the **Unmanaged** resource state, and you cannot change the state to **Managed** or **Reserved**.

For some resources such as nodes, the default credentials are prepopulated in PowerFlex Manager. If the credentials are changed from the defaults, add the credential to PowerFlex Manager with the new login information.

Element Manager discovery

The IPI cabinet is discovered as an element manager. Once PowerFlex Manager discovers the IPI cabinet, you can view cabinet details or you can open the IPI appliance management application to view more details.

The CloudLink Center is discovered as an element manager. If you create your own username in CloudLink Center, you need the SecAdmin access role and the local user type for the new user to complete discovery. The client user type does not work for discovery in PowerFlex Manager. If one member of a cluster of CloudLink Center is shut down, the inventory still succeeds because PowerFlex Manager falls back to inventorying the other CloudLink Center members if the first one is down.

Node discovery

PowerFlex Manager supports PowerFlex node discovery and allows you to onboard nodes by configuring the initial management IP address and iDRAC credentials. To perform initial discovery and configuration, verify that the management IP address is set on the node and that PowerFlex Manager can access the IP address through the network. While configuring IP addresses on the node, verify that PowerFlex Manager can access any final IP address in a range used for hardware management, to complete discovery of these nodes.

PowerFlex Manager also allows you to use name-based searches to discover a range of nodes that were assigned IP addresses by DHCP to iDRAC. You can search for a range of DNS hostnames or a single hostname within the **Discovery Wizard**. After you perform a name-based discovery, PowerFlex Manager operations to the IDRAC continue to use name-based IP resolution, since DHCP may assign alternate addresses.

Switch discovery

If you attempt to discover a Cisco switch with terminal color configured, the discovery fails. To discover the switch successfully, disable the terminal color option by running `configure no terminal color persist`.

VM manager discovery

A VMware vCenter is discovered as a VM manager. PowerFlex Manager users with the administrator role can discover a vCenter in PowerFlex Manager. A vCenter read-only user can discover a vCenter in PowerFlex Manager only after the following requirements are met:

- The vCenter user who is specified in the vCenter credential is granted the `VirtualMachine.Provisioning.ReadCustSpecs` and `StorageProfie.View` privileges.
- The permission containing these privileges is granted to that user on the root vCenter object and the `Propogate to children` property is set to `True`.

PowerFlex Manager allows you to deploy new hyperconverged and compute-only resource groups and add existing resource groups to a vCenter that has an Enhanced Linked Mode (ELM) configuration. ELM connects multiple vCenter servers, allowing you to search across servers and perform other vCenter management functions. ELM does not provide clustering or redundancy.

If you are working with a vCenter that has an enhanced linked mode configuration, you must discover only the vCenter to which you want to deploy or add an existing resource group. You do not need to discover the other vCenters that are connected through the enhanced linked mode configuration.

Node pools

In PowerFlex Manager, a node pool is made up of nodes that are grouped for specific use cases such as business units or workload purposes. An administrator can specify which users can access these node pools.

Standard users can view details only for node pools for which they have permission.

From the **Node Pools** tab, you can view existing node pools.

Users with an administrator role can create, edit, or delete node pools.

Click a node pool from the list to view detailed information about the following tabs:

- **Nodes**: Displays the number of nodes that are associated with the node pool.
- **Users**: Displays the number of users with access rights to the node pool.

Configuration checks

When you initiate a resource group action, PowerFlex Manager performs critical configuration checks to ensure that the system is healthy before proceeding. A configuration check failure may result in the resource group action being blocked. You can export a PDF report at any time that shows detailed system health and configuration data. When you generate the report, PowerFlex Manager initiates the full set of configuration checks and reports the results.

Configuration checks for switches

Dell Networking OS9 switches are not covered by the configuration checks.

Configuration check	Resource group actions blocked if the check fails
PowerFlex gateway is powered off	None
PowerFlex cluster state is not normal	• Add node • Add volume • Delete node • Delete resource group • Add resource group with an existing PowerFlex cluster • Compliance upgrade • Enter service mode • Drive replacement
Secondary MDMs have a status not equal to normal	• Add nodes • Add volumes • Delete node • Delete resource group • Add resource group with an existing PowerFlex cluster • Compliance upgrade • Enter service mode • Drive replacement
SDS registered data network IP address count does not equal 2 or 4	• Compliance upgrade • Enter service mode • Drive replacement • Reconfigure MDM roles
SDS has a state not equal to connected	• Add volume • Compliance upgrade • Reconfigure MDM roles
SDS interfaces have incorrect MTU sizes	• Add node • Add resource group with an existing PowerFlex cluster • Compliance upgrade

Configuration check	Resource group actions blocked if the check fails
	• Reconfigure MDM roles
VMware ESXi vmks are not configured with an MTU size of 9000	• Add node • Add resource group with an existing PowerFlex cluster • Compliance upgrade
Interfaces are not configured with an MTU size of 9216, and QOS is enabled with MTU size	• Add node • Add resource group with an existing PowerFlex cluster • Compliance upgrade
SDS has a Performance Profile not equal to High Performance	None
SDC has a Performance Profile not equal to High Performance	None

Related information

Exporting a configuration report for all resources and resource groups

Settings

This section provides reference information for the **Settings** page.

Backup details

PowerFlex Manager backup files include the following information:

- Activity logs
- Credentials
- Deployments
- Resource inventory and status
- Events
- Initial setup
- IP addresses
- Jobs
- Licensing
- Networks
- Templates
- Users and roles
- Resource module configuration files
- Performance metrics

Network types

You can manage various network types in PowerFlex Manager.

- **General Purpose LAN**—Used to access network resources for basic networking activities.
- **Hypervisor Management**—Used to identify the management network for a hypervisor or operating system that is deployed on a node.
- **Hypervisor Migration**—Used to manage the network that you want to use for live migration. Live migration enables you to move running virtual machines from one node of the failover cluster to different node in the same cluster.
- **OS Installation**—Allows static or DHCP network for operating system imaging on nodes.
- **Hardware Management**—Used for out-of-band management of hardware infrastructure
- **PowerFlex Data**—Used for data traffic between storage data servers (SDS) and storage data clients (SDC)
- **PowerFlex Data (Client Traffic Only)**—Used for storage data client traffic only
- **PowerFlex Data (Server Traffic Only)**—Used for storage data server traffic only
- **PowerFlex Replication**—Used to support PowerFlex replication
- **NAS File Management**—Used to support PowerFlex file management traffic

- **NAS File Data**—Used to support PowerFlex file data traffic
- **PowerFlex Management**—Used for PowerFlex system management

14

Additional administration activities

This section describes additional administration activities that must be performed outside of PowerFlex Manager

Maintenance activities

This section includes procedures for performing general maintenance, such as shutting down and restarting nodes.

Shutdown or restart a node gracefully

When performing tasks on a node that require it to be shutdown or restarted, do so gracefully.

Operating system upgrades and patches, as well as other maintenance activities, like part replacement, require shutting down or rebooting a node.

Gracefully shut down or reboot a node

Prepare the node for a patching or maintenance operation (such as a part replacement) by entering the node into maintenance mode and shutting down/rebooting the node in a graceful fashion.

NOTE: Do not use **-f** in the shutdown or reboot command.

1. When shutting down/rebooting a node that is a primary MDM (manager), it is recommended that you manually switch MDM ownership to a different node:
   a. From the PowerFlex CLI (SCLI), run:

      ```
      scli --query_cluster
      ```

   b. If the node's IP addresses are included in the `--query_cluster` output, the faulty node has a role of either MDM or tiebreaker, in addition to its SDS role.

      If the node's IP address is located in the primary MDM role, a switch-over action is required.

   c. Switch MDM ownership to a different node:

      ```
      scli -switch_mdm_ownership (-new_primary_mdm_id <ID> | --new_primary_mdm_ip <IP> |
      --new_primary_mdm_name <NAME>)
      ```

      The node remains in the cluster. The cluster will be in degraded mode after it is powered off, until the faulty component or patch operation in the node is fixed and the node is powered back on.

   d. Verify that the cluster status shows that the node is not the primary MDM anymore:

      ```
      scli --query_cluster
      ```

      Output similar to the following should appear, with the relevant node configuration and IP addresses for your deployment:

      ```
      Cluster:
          Mode: 5_node, State: Normal, Active: 5/5, Replicas: 3/3
          Virtual IP Addresses: 9.20.10.100, 9.20.110.100
      Primary MDM:
          ID: 0x775afb2a65ef1f02
              IP Addresses: 9.20.10.104, 9.20.110.104, Management IP Addresses:
      10.136.215.239, Port: 9011, Virtual IP interfaces: sio_d_1, sio_d_2
              Version: 2.0.13000
      Secondary MDMs:
          ID: 0x5b2e9f273b7af9b0
      ```

```
        IP Addresses: 9.20.10.105, 9.20.110.105, Management IP Addresses:
10.136.215.223, Port: 9011, Virtual IP interfaces: sio_d_1, sio_d_2
        Status: Normal, Version: 2.0.13000
    ID: 0x5828f65b15e778f1
        IP Addresses: 9.20.10.102, 9.20.110.102, Management IP Addresses:
10.136.215.232, Port: 9011, Virtual IP interfaces: sio_d_1, sio_d_2
        Status: Normal, Version: 2.0.13000
Tiebreakers:
    ID: 0x6618e0b804644ca4
        IP Addresses: 9.20.10.101, 9.20.110.101, Port: 9011
        Status: Normal, Version: 2.0.13000
    ID: 0x12534ccb3d28fee3
        IP Addresses: 9.20.10.103, 9.20.110.103, Port: 9011
        Status: Normal, Version: 2.0.13000
```

In the example output, the primary MDM IP addresses are:

```
IP Addresses: 9.20.10.104, 9.20.110.104, Management IP Addresses: 10.136.215.239
```

The secondary IP addresses are:

```
IP Addresses: 9.20.10.105, 9.20.110.105, Management IP Addresses: 10.136.215.223
IP Addresses: 9.20.10.102, 9.20.110.102, Management IP Addresses: 10.136.215.232
```

2. Move all applications to a different node:
   - On an VMware ESXi node that is not a cluster member, and that is not configured for HA and DRS, migrate the VMs to another VMware ESXi.
   - On a Linux node, migrate the applications (or the VMs, if the node is running a hypervisor).
3. Log in to PowerFlex Manager as an admin user.
4. On the menu bar, click **Block** > **SDSs**.
5. Select the relevant SDS and click **More Actions** > **Enter Maintenance Mode**.
6. In the **Enter SDS <name> into Maintenance Mode** dialog box, select one of the following options:
   - **Instant**
   - **Protected**
7. Click **Enter Maintenance Mode**.
8. In the confirmation message dialog box, click **Dismiss**.
9. If you are applying a patch:
   a. Run the patch.
   b. Reboot the node, if necessary.

Return the node to operation

To return the node to operation, perform the following steps:

1. Power on the node and wait for the node to start booting.
   The operating system boots up for Linux operating systems. For Linux nodes, all PowerFlex processes start up automatically.
2. For an ESXi node, perform the following:
   a. From the vSphere Web Client, ensure that the node is displayed as on and connected in both **Hosts** and **Clusters** view.
   b. Right-click the node and select **Exit Maintenance Mode**.
3. After the node is up, perform the following checks in PowerFlex Manager:
   a. In the left pane, click **Alerts**. In the right pane, make sure that no SDS disconnect message appears.
      Verify that the SDCs are healthy, and if the node was an MDM cluster member, verify that the MDM cluster is no longer degraded.
4. On the menu bar, click **Block** > **SDSs**..
5. In the right pane, select the relevant SDS and click **More Actions** > **Exit Maintenance Mode**.
6. In the **Exit SDS <name> from Maintenance Mode** dialog box, click **Exit Maintenance Mode**.
7. In the confirmation message dialog box, click **Dismiss**.
8. Wait for the rebuild/rebalance operations to finish.

The node is now operational and application I/O can be started on the node. For ESXi nodes, you can migrate VMs to the node.

Running scripts on hosts via PowerFlex Manager

You can run operating system patch commands or firmware updates that are managed by scripts on servers hosting PowerFlex components.

Overview of running scripts on hosts

PowerFlex can be used to run user-provided scripts on nodes hosting MDM or SDS components. This feature is supported on Linux-based (bare-metal or virtual) nodes only.

The PowerFlex Installer can be used to run a user-provided script on a node where PowerFlex is deployed. This feature can be used for any purpose external to the PowerFlex system, such as running a set of CLI commands, patching an operating system, and more. The feature allows the running of scripts in a safe manner, both from a security and a data integrity perspective.

PowerFlex Installer orchestrates the running of the script, ensuring that SDSs are placed in Maintenance Mode, to protect data during the process. In addition, parallel execution of scripts is only permitted on SDSs located in different Protection Domains. After the scripts have been run on an SDS, it exits Maintenance Mode.

Optionally, servers can be set to reboot after execution of the script. The process can also run a verification script either after the reboot, or after execution of the script, when no reboot is required.

The execution phase of this feature can be summarized as follows:

1. The system validates the following:
   - The patching script exists on the node after it was uploaded from the PowerFlex Gateway
   - No failed capacity exists
   - Sufficient spare capacity exists
   - The MDM cluster is in a valid state
2. Run the script on one host, using the following priorities:
   a. SDS only hosts, each time on a single SDS, unless the option `In parallel on different Protection Domains` is enabled
   b. Tiebreaker
   c. MDMs

   NOTE: The script will not run on a primary MDM. A switch-over MDM command will be run prior to running the script on a primary MDM. The script will not be run in parallel on multiple MDMs or tiebreakers.
3. SDS enters Maintenance Mode.
4. The script runs on the host.
5. The host reboots (if configured to do so).
6. The validation script runs on the node (if configured to do so).
7. SDS exits Maintenance Mode.

Run script on host

Use this method to run a script on all or some of the Linux-based nodes with an optional reboot and an optional verification script.

CAUTION: PowerFlex Manager is required to perform run script on host operation. A target script is run without validation or verification.

The script files must be stored in the folder node folder: `/opt/emc/scaleio/lia/bin`. The script file used to run script on host operation must be named as `patch_script`.

If verification is required, a script to verify the work can be written and named `verification_script`.

The filenames are hard-coded and cannot be changed: `patch_script` and `verification_script`. The scripts are required to have these names. Alternatively, they can be uploaded by PowerFlex Manager to the PowerFlex node.

To copy the script file onto the block-legacy-gateway pods, use the kubectl cp command from any of the PowerFlex management platform hosts or VMs.

For example,

```
kubectl cp -n powerflex patch_script block-legacy-gateway-0:/usr/local/tomcat/temp/
kubectl cp -n powerflex patch_script block-legacy-gateway-1:/usr/local/tomcat/temp/
```

The scripts can be either taken from a gateway local folder or downloaded from HTTP or HTTPS share.

A list of SdsIds or mdmIds can be provided to explicitly choose the PowerFlex nodes to run on.

API command	Required parameters	Optional parameters
`/im/types/Configuration/actions/liaRunOsPatching` **NOTE:** Before running the liaRunOsPatching command, log in to PowerFlex and get the system configuration. For more information, see the example workflow below.	Either one of the following parameters is mandatory: • pdIds: Run on all PowerFlex nodes that are part of the following protection domains (PD Ids), in decimal format • fsIds: Run on all PowerFlex nodes that are part of the following fault sets (FS Ids), in decimal format • sdsIds: Run on all SDSs listed by Ids, in decimal format • mdmIds: Run on all MDMs listed by Ids, in decimal format • executeOnAllSdss: Run on all SDSs (true/false) • executeOnAllMdms: Run on all MDMs (true/false)	• isRebootRequired: Indicates if each node reboot required after running the patch script (values: true/false) **NOTE:** In earlier PowerFlex 4.x versions, all nodes running PowerFlex management platform processes will be skipped for reboots. The action must be performed manually. • isVerificationScriptRequired: Indicates if the verification script is run on each node (values: true/false) • isRunningInParallelOnPds: Indicates if the operation is run in a parallel way on nodes that belong to different PDs (values: true/false) • isStopProcessingOnScriptFailure: Indicates if the entire operation must be stopped if there is a script failure (values: true/false • TimeoutMs: Indicates timeout value for running the patch script in milliseconds • isUploadFileNeeded: Indicates if the gateway upload scripts to the PowerFlex nodes (values: true/false) The following fields are relevant when isUploadFileNeeded is true: ○ patchScriptFilePath: Either the local folder name or an http/https URL of the patch script ○ verificationScriptFilePath: Either the local folder name or an http/https URL of the verification script ○ maintenanceModeType: Maintenance Mode type (values: IMM/PMM) ○ verificationScriptTimeoutSec: Verification script timeout in seconds ○ rebootTimeoutSec: Node reboot timeout in seconds

The following are the example commands used during run script on host process:

1. Obtain an access token from the PowerFlex Manager instance. The easiest method is to create a shell script that can be sourced to add the proper variables to the user environment

```
INGRESS_IP=<powerflex manager IP>
INGRESS_USER=<powerflex manager user>
INGRESS_PASSWORD=<powerflex manager password>
```

   a. Get JWT token with POST /rest/auth/login.

```
TOKEN=$(curl -s -k --location --request POST "https://${INGRESS_IP}/rest/auth/
login" --header "Accept: application/json" --header "Content-Type: application/
json" --data "{\"username\": \"${INGRESS_USER}\",\"password\": \"${INGRESS_PASSWORD}
\"}")
```

b. Parse out the access token which is used to call the API and is valid for 5 minutes by default.

```
ACCESS_TOKEN=$(echo "${TOKEN}" | jq -r .access_token)
```

c. Parse out the refresh token which can be used to get a new JWT token if the access token has expired. It is valid for 30 minutes by default.

```
REFRESH_TOKEN=$(echo "${TOKEN}" | jq -r .refresh_token)
```

NOTE: The expiration time for access token is five minutes. If required, the above file can be sourced to refresh all variables.

2. Get the JSON of a system configuration, which will be the payload of the patch command (need to replace liaPassword and mdmPassword manually from null to some string).
   a. Create and save a JSON file like the following, replacing MDM addresses, MDM user, and MDM password with the appropriate values.

```
{
   "mdmIps":["<MDM IP-1>","<MDM-IP2>"],
   "mdmUser":"<mdm user>",
   "mdmPassword":"<mdm password>”,
   "securityConfiguration":
   {
      "allowNonSecureCommunicationWithMdm":"true",
      "allowNonSecureCommunicationWithLia":"true",
      "disableNonMgmtComponentsAuth":"false"
   }
}
```

   b. Insert the output of this command (with fixed passwords) into the config.json file:

```
curl -s -X POST -k -H "Content-Type: application/json" --data <json file>
-H "Authorization: Bearer ${ACCESS_TOKEN}" https://<powerflex manager IP>/im/types/
Configuration/instances > config.json
```

3. Run the patch command (loading the config.json):

NOTE: The `cookiefile` stores session cookies which keeps the command flows directed to the same gateway pod.

```
curl -v -k -c cookiefile -X -i POST -H "Content-Type:application/json" -H
"Authorization:
Bearer ${ACCESS_TOKEN}" "https://<powerflex manager IP>/im/types/Configuration/
actions/liaRunOsPatching?executeOnAllSdss=true
&isRebootRequired=true&isPatchScriptRequired=true&isVerificationScriptRequired=true&pa
tchScriptFilePath=”https://
<ipaddress>/patch_script”&verificationScriptFilePath=”https://<ip-address>/
verification_script”&maintenanceModeType=IMM&rebootTimeoutSec=600" -d @config.json
```

4. Query command state by running the following command:

```
curl -k -b cookiefile -X GET -H "Content-Type: application/json" -d @config.json
-H "Authorization: Bearer $ACCESS_TOKEN" "https://10.234.89.250/im/types/ProcessPhase/
actions/queryPhaseState" | jq
{
  "phaseStatus": "idle",
  "phase": "idle",
  "numberOfRunningCommands": 0,
  "numberOfPendingCommands": 0,
  "numberOfCompletedCommands": 0,
  "numberOfAbortedCommands": 0,
  "numberOfFailedCommands": 0,
  "failedCommands": []
}

or
{
  "phaseStatus": "running",
  "phase": "execute",
  "numberOfRunningCommands": 1,
  "numberOfPendingCommands": 1,
  "numberOfCompletedCommands": 35,
```

```
  "numberOfAbortedCommands": 0,
  "numberOfFailedCommands": 0,
  "failedCommands": []
}

or
{
  "phaseStatus": "completed",
  "phase": "validate",
  "numberOfRunningCommands": 0,
  "numberOfPendingCommands": 0,
  "numberOfCompletedCommands": 2,
  "numberOfAbortedCommands": 0,
  "numberOfFailedCommands": 0,
  "failedCommands": []
}

Look for:

{
  "phaseStatus": "completed",
  "phase": "execute",
  "numberOfRunningCommands": 0,
  "numberOfPendingCommands": 0,
  "numberOfCompletedCommands": 37,
  "numberOfAbortedCommands": 0,
  "numberOfFailedCommands": 0,
  "failedCommands": []
}
```

5. Move to NextPhase by running the following command.

```
curl -k -b cookiefile -X POST -H "Content-Type: application/json" -d ''
-H "Authorization: Bearer $ACCESS_TOKEN" https://10.234.89.250//im/types/ProcessPhase/
actions/moveToNextPhase
```

6. Cancel the phase by running the following command

```
curl -k -b cookiefile -X POST -H "Content-Type: application/json" -d
'' -H "Authorization: Bearer $ACCESS_TOKEN" https://10.234.89.250/im/types/Command/
instances/actions/abort
```

7. Clear the phase by running the following command

```
curl -k -b cookiefile -X POST -H "Content-Type: application/json" -d
'' -H "Authorization: Bearer $ACCESS_TOKEN" https://10.234.89.250/im/types/Command/
instances/actions/clear
```

8. Move to idle phase by running the following command

```
curl -k -b cookiefile -X POST -H "Content-Type: application/json" -d ''
-H "Authorization: Bearer $ACCESS_TOKEN" https://10.234.89.250/im/types/ProcessPhase/
actions/moveToIdlePhase
```

Logs

Gateway pod log locations:

- /usr/local/tomcat/logs/scaleio.log
- /usr/local/tomcat/logs/scaleio-trace.log

LIA log location: /opt/emc/scaleio/lia/logs/trc.x

NOTE: Special switch to keep the script in the node when troubleshooting or testing:

1. Edit file /usr/local/tomcat/webapps/ROOT/WEB-INF/classes/gatewayInternal.properties
2. Find the field "ospatching.delete.scripts=false"
3. Change to true for troubleshooting (Default is false)

15

Retrieving logs for the PowerFlex nodes

This section describes how to retrieve logs from an operating system running on PowerFlex nodes.

Retrieve logs from an VMware ESXi-based operating system

Use this task to retrieve the logs from a VMware ESXi-based PowerFlex node.

Ensure that you have access to the following:

- IP address of the node
- Password for the root user

When the OS is started, the ESXi operating system logs are collected in the system-defined folders `/var/log` and `/scratch/log/` on the local drive.

1. Log in to the PowerFlex node.
2. From ESXi, run the `scp` command to collect the ESXi operating system logs from the following folders on the local drive:
   - `/var/log`
   - `/scratch/log/`

   For additional data, see VMware KB article - VMware KB-653: Collecting diagnostic information for VMware ESX/ESXi.

Retrieve logs from a Linux-based operating system

Use this task to retrieve the logs from a Linux-based PowerFlex node.

Ensure that you have access to the following:

- IP address of the node
- Password for the root user
- Grab Utility, downloadable from the Dell Technologies Support site

When the Linux server is started, the Linux logs are collected in the system-defined directory `/var/log`, on the local drive. Operating system logs are also collected automatically when running the get_info log collection process.

For information on running get_info, see Collecting debug information using get_info.

1. Log in to the PowerFlex node.
2. Run the `scp` command to collect the Linux operating system logs from the `/var/log` directory on the local drive.

   The `/var/log` folder provides logs for preliminary system investigation.
3. To retrieve full logs, including customer- and OS-related information, run the Grab utility.

Retrieve logs from Windows-based operating system

Use this task to retrieve the logs from a Windows-based PowerFlex node.

Ensure that you have access to the following:

- IP address of the node
- Password for the administrator user
- Grab utility available on the Dell Technologies Support site.

1. Log in to the PowerFlex node.
2. Run the Windows Event Viewer.

The **Event Viewer** screen displays **Event Viewer (Local)** as the root node.

3. In the navigation pane, go to the **Windows Logs** node and select the **System** sub node.
   The **Actions** pane is displayed on the right side of the screen.
4. From the **Actions** pane, click **Save All Events As**.
   The navigation tree with your local folders is displayed.
5. Browse to the intended location on your local drive, give the file an appropriate name, and select the file format.
6. Click **Save**.
   The Windows OS-related log files are saved on your local drive.

   The file on the local drive provides logs for preliminary system investigation.
7. To retrieve full logs, including customer and OS-related information, run Grab utility.

Configure and retrieve operating system crash dumps

Use this task to configure and retrieve the operating system crash dumps.

Ensure that you have access to a web browser.

1. Open your web browser.
2. To configure and retrieve the crash dumps, click an appropriate link that matches with your operating system:

Operating System	Link for crash dump configuration procedure
ESXi	http://kb.vmware.com/kb/1000328
Linux (RedHat)	https://access.redhat.com/solutions/6038
Linux (SLES)	https://www.suse.com/support/kb/doc?id=3374462
Windows	https://support.microsoft.com/en-ie/kb/969028

3. To analyze the crash dumps, click an appropriate link that matches with your operating system:

Operating System	Link for crash dump configuration procedure
ESXi	http://kb.vmware.com/kb/1006796 or http://kb.vmware.com/kb/1004128
Linux (RedHat)	https://access.redhat.com/solutions/2121
Linux (SLES)	https://www.suse.com/support/kb/doc.php?id=7010484
Windows	https://support.microsoft.com/en-ie/kb/315263

16

Retrieving logs for PowerFlex components

You can retrieve the log files for PowerFlex components manually or automatically. You can collect the logs of one component at a time, or of all system components at one time. You can also enable automatic log collection that collects logs automatically when triggered by system alerts.

Retrieve the PowerFlex core component logs

You can retrieve the PowerFlex component logs manually, directly from the component server, one node at a time.

Ensure that you have the following user login credentials:

- IP address of the node
- Password for the root user in ESXi- and Linux-based systems and the administrator user in Windows-based systems

The PowerFlex logs relate to specific components (MDM, SDS, SDR, SDT, or LIA) on each server node and its operating system environment.

1. SSH or RDP to the PowerFlex node.

   In ESXi-based PowerFlex, log in to the Linux-based SVM.
2. Run the script for the PowerFlex component.

Operating System	Run this script
ESXi or Linux	`/opt/emc/scaleio/<PowerFlex component>/diag/get_info.sh` where the value of the PowerFlex component is mdm, sds, sdr, sdt, or lia
Windows	`"C:\Program Files\EMC\scaleio\sdc\diag\get_info.bat" -f`

   The get_info syntax is explained fully in Collecting debug information using get_info.

   - If the selected node is the primary MDM, use the flags `-u <MDMuser> -p <MDMpassword>`, instead of `-f`.
   - If the selected node contains more than one PowerFlex component, running any script will gather logs for all components on that node.

   When the log collection process is complete, an archive file (either TGZ or ZIP) containing the logs of all PowerFlex components in the node, is created in a temporary directory. By default, the directory is `/tmp/scaleio-getinfo` on Linux hosts or `C:\Windows\Temp\ScaleIO-getinfo` on Windows hosts.
3. Verify that output similar to the following is returned, which shows that the process of log collection was completed successfully:
   bundle available at `'/tmp/scaleio-getinfo/getInfoDump.tgz'`

   NOTE: The script can generate numerous lines of output. Therefore, look for this particular line in the output.
4. Retrieve the log file.

Collecting debug information using get_info

The get_info script is a debug utility which allows a technician to collect debug information for customer support analysis.

You can run the script once at a given time. If there is insufficient drive space then the script will not run.

Syntax

```
get_info.sh [OPTIONS]
```

Optional parameters:

-a, --all

Collect all data

-A, --analyse-diag-coll

Analyze diagnostic data collector (diag coll) data

-b[COMPONENTS], --collect-cores[=COMPONENTS]

Collect existing core dumps of the space-separated list of user-land components, COMPONENTS (default: all user-land components)

For example, `-b'mdm sds'` (no space between option name and COMPONENTS)

For example, `--collect-cores='mdm sds'` (separate option name and COMPONENTS with a single equal sign, "=")

-d OUT_DIR, --output-dir=OUT_DIR

Store collected bundle under directory OUT_DIR (default: <*WORK_DIR*>/scaleio-getinfo, see `--work-dir` for the value of <*WORK_DIR*>)

-f, --skip-mdm-login

Skip query of PowerFlex login credentials

The parameters `-k NUM` and `--max-cores=NUM` collects up to NUM core files from each component (default: all core files)

Implies --collect-cores -l, --light

Generate light bundle (not recommended)

--ldap-authentication

Log in to PowerFlex using LDAP-based authentication

-m NUM, --max-traces=NUM

Collect up to NUM PowerFlex trace file from each component (default: all files)

--management-system-ip=ADDRESS

Connect to SSO or management at `ADDRESS` for PowerFlex login (default: scli default)

--mdm-port=PORT

Connect to MDM using PORT for SCLI commands (default: scli default)

-n, --use-nonsecure-communication

Connect to the MDM in non-secure mode

-N, --skip-space-check

Skip free space verification

--overwrite-output-file

Overwrite output file if it already exists

-p PASSWORD, --password=PASSWORD

Use PASSWORD for PowerFlex login (default: scli default)

--p12-password=PASSWORD

Encrypt PowerFlex login PKCS#12 file using PASSWORD (default: scli default)

--p12-path=FILE

Store PowerFlex login PKCS#12 file as FILE (default: scli default)

-q, --quiet, --silent

Do not output messages to stdout

-r, --mdm-repository

Collect MDM repository files

-s, --skip-sdbg

Skip collection of SDBG output

-S, --pause-core-generation

Pause core generation of PowerFlex components during data collection

--tech

Include technician option in help message

-u USERNAME, --username=USERNAME

Use USERNAME for PowerFlex login (default: scli default)

-w WORK_DIR, --work-dir=WORK_DIR

Use directory `WORK_DIR` for temporary files (default: /tmp)

-x FILE, --output-file=FILE

Store collected bundle as FILE (default: getInfoDump). Appropriate file name suffix (.tgz, .zip) is added automatically

If FILE is '-', write bundle to standard output (implies --quiet)

-z, --zip

Use zip format for the collected bundle

-h, --help

Show this help message and exit

Collect PowerFlex management platform support data

Use the following procedure to collect PowerFlex management platform support data if the central log collection from PowerFlex Manager is not available or you are troubleshooting PowerFlex management platform install problems.

1. If required, transfer the data collection executable, `pfmp_support` to all PowerFlex management platform cluster member hosts.

   The data collection utility file is available in the PowerFlex management platform installer and Dell Technologies support site. To get the utility file from the PowerFlex management platform installer, go to the `PFMP_Installer/scripts` directory. To download the data collection utility from the support site, search for **PFMP log collection Script** file on the Dell Technologies Support site.

   NOTE: Depending on the transfer method, add the execution permissions using the `chmod +x <file name>` command.

2. On one of the cluster member nodes, execute the data collection utility as a user with superuser permissions, such as user root.

   In the following example, the utility's executable exists under `/root`.

```
# /root/pfmp_support
estimating required space
cleaning up temporary directories
collecting kubernetes data
collecting shared kubernetes data
collecting server data
collecting general hardware data
collecting network data
collecting storage data
preparing files for collection
generating bundle
cleaning up temporary directories
bundle available at '/tmp/powerflex-pfmpsupport/pfmpSupport.tgz'
```

3. If the PowerFlex management platform cluster consists of more than one node, on each of the remaining nodes, execute the utility as a user with superuser permissions, such as user root, skipping shared Kubernetes data collection.

```
# /root/pfmp_support --skip-kubernetes-shared
estimating required space
cleaning up temporary directories
collecting kubernetes data
collecting server data
collecting general hardware data
collecting network data
collecting storage data
preparing files for collection
generating bundle
cleaning up temporary directories
bundle available at '/tmp/powerflex-pfmpsupport/pfmpSupport.tgz'
```

4. From all cluster member nodes, provide the resulting support bundle files to Dell Technologies Support.
   By default, bundle files are named `/tmp/powerflex-pfmpsupport/pfmpSupport.tgz`.

Collect PowerFlex Manager platform installer support data

Use the following procedures to collect the PowerFlex Manager platform installer support data.

1. On the PowerFlex Manager Platform (PFMP) installer host, execute the data collection utility, `pfmp_support`, as a user with superuser permissions, such as user root.

   The utility is available in the location where the installer was extracted, under the `PFMP_Installer/scripts` directory.

   In the following example, the PFMP installer was extracted under `/tmp/PFMP2-4.0.0-161`.

```
# /tmp/PFMP2-4.0.0-161/PFMP_Installer/scripts/pfmp_support
estimating required space
cleaning up temporary directories
collecting kubernetes data
collecting shared kubernetes data
collecting server data
collecting general hardware data
collecting network data
collecting storage data
preparing files for collection
generating bundle
cleaning up temporary directories
bundle available at '/tmp/powerflex-pfmpsupport/pfmpSupport.tgz'
```

2. Provide the resulting support bundle file to PowerFlex Support.

   By default, bundle files are named `/tmp/powerflex-pfmpsupport/pfmpSupport.tgz`.

Generating a troubleshooting bundle

A troubleshooting bundle is a compressed file that contains logging information for PowerFlex Manager managed components. If necessary, download the bundle and send it to Dell Technologies Support for issue debugging.

The troubleshooting bundle includes the following logs:

- ASM deployer
- iDRAC life cycle
- Dell PowerSwitch switch
- Cisco Nexus switch
- VMware ESXi
- CloudLink Center
- NAS
- Standard output logs from all pods
- Kubernetes logs about pods, services, deployments, secrets, drivers, and volumes
- PowerFlex Block logs

NOTE: You can generate troubleshooting bundles from the **Resource Groups** page too.

1. On the menu bar, click **Settings** > **Serviceability**.
2. Click **Generate Troubleshooting Bundle**.
3. If you are using SupportAssist, **Send to Configured SupportAssist** is selected by default. Leave this default setting. If SupportAssist is not configured, this option is disabled.

   If you are not using SupportAssist, select **Download Locally** to download the troubleshooting bundle to a local file. Provide a path using the following format:

For...	Use this path...
CIFS	`\\IP Address\Any folder`

   For example:

   CIFS: `\\192.168.1.1\uploadDirectory`

   Also, provide a username and password.

4. Click **Test Connection** to verify the connection to the CIFS share before generating the bundle.
5. Optionally, select **Include PowerFlex File Core Dump logs**, if you want to include core dump logs for NAS.

   The NAS directory structure, nodes, and files are always collected regardless of whether this box is checked. When it is checked, the additional NAS core dump is collected.

6. To collect PowerFlex logs, select one of the following log level options:
   - Default Node Logs
   - Default Node Logs plus additional MDM information
   - Latest Logs only (Most recent copy of all logs)
7. To collect PowerFlex node logs, select one of the following options:
   - Logs from all nodes
   - Select Specific Nodes

   If you select the **Select Specific Nodes** option and select the number of nodes for which you want to generate the log, the **View/Select Nodes** button is displayed. Click the button to view the list of nodes in the **Node Selection** window. Select the required nodes from the **Available Nodes** list and click >> to view them in the **Selected Nodes** list. Click **Save** to return to the **Generate Troubleshooting bundle** page.

   For the **Select Specific Nodes** option, **Generate** is enabled only if a node is selected in the **Node Selection** window.

8. Click **Generate**.

Sometimes, the troubleshooting bundle does not include log information for all the nodes. The log collection may appear to succeed, but the log for one or more of the nodes may be missing. You may see an error message in the scaleio.trace.log file that says `Could not run get_info script`. If you see this message, you may need to generate the troubleshooting bundle again to include information for all the logs.

Selecting PowerFlex nodes for generating a troubleshooting bundle

1. From the **Available Nodes** list, select the check box next to the nodes you want to include in the troubleshooting bundle.
2. Click the right double arrow (>>) to move the selected nodes to the **Selected Nodes** list.
3. Click **Save** to save your selection.

Retrieve PowerFlex core component logs using REST API

Use the following procedures to collect logs using REST API.

- The (PFMP) cluster must be present.
- The PowerFlex cluster must be deployed.
- The cluster must be able to communicate with any host instance in the PowerFlex cluster. To test the connection, ping from a PowerFlex node to the data IP addresses of the instances.

- Ensure that you have mdm_ips, mno_username, mno_password, and mno_ip.

1. To log in to M&O, run the following API command:

   `POST https://<mno_ip>/rest/auth/login`

   For example:

   ```
   token=$(curl -k --silent 'https://<mno_ip>/rest/auth/login' --header 'Accept:
   application/json' --header 'Content-Type: application/json' -d '{"username":
   "<mno_username>","password": "<mno_password>"}' |jq -r '.access_token'); echo $token
   ```

   Save the access token received in the output.

2. To get configuration, run the following API command:

   `POST https://<mno_ip>/im/types/Configuration/instances`

   For example:

   ```
   curl --silent  -k -X POST  -H "Authorization: Bearer ${token}" -H
   'Content-Type: application/json' -d '{ "mdmIps":["10.234.177.103","10.234.177.153"],
   "mdmUser":<mno_username>, "mdmPassword":"<mno_password>",
   "securityConfiguration":{ "allowNonSecureCommunicationWithMdm":"false",
   "allowNonSecureCommunicationWithLia":"false", "disableNonMgmtComponentsAuth":"false"
   } }'  https://<mno_ip>/im/types/Configuration/instances>config.json
   ```

   Save the output of the request. This output is a JSON representation of the system configuration.

3. Add the M&O login information to the JSON. The get info script requires the login information to perform certain queries, to provide this information, add the following key value pairs to JSON:

   ```
   mnoUser : "<mno_username>"
   mnoPassword : "<mno_password>"
   mnoIp : "<mno_ip>"
   ```

   For example:

   ```
   {
   "mnoUser" : "<mno_username>" ,
   "mnoPassword": "<mno_password>" ,
   "mnoIp: "<mno_ip>"
   "snmpIp": null
   … (rest of the json)
   }
   ```

4. To collect logs, run the following API command:

   `POST https://<mno_ip>/im/types/NodeInfo/instances/actions/collectLogs`

   To run the collect logs request, ensure that you have a valid token and the configuration JSON. For more optional attributes, go to step 7.

   ```
   curl -k -X POST  -H "Authorization: Bearer ${token}" -H 'Content-Type:
   application/json' -d @config.json  https://<mno_ip> /im/types/NodeInfo/instances/
   actions/collectLogs
   ```

5. To monitor the log collection process, run the following API command:

   `GET https://<mno_ip>/im/types/ProcessPhase/actions/queryPhaseState`

   Monitor the `phaseStatus` value and wait until the operation is complete.

   For example:

   ```
   curl -s -k  -X GET -H "Content-Type:application/json" -H "Authorization: Bearer $
   {token}" https://<mno_ip> /im/types/ProcessPhase/actions/queryPhaseState
   ```

   Output example:

   ```
   {"phaseStatus":"completed","phase":"query","numberOfRunningCommands":0,"numberOfPendin
   gCommands":0,"numberOfCompletedCommands":6,"numberOfAbortedCommands":0,"numberOfFailed
   Commands":0,"failedCommand
   ```

6. To download the logs, run the following API command:

   `GET https://<mno_ip>/im/types/NodeInfo/instances`

   For example:

   ```
   curl -s -k -i -X  GET -H "Content-Type:application/json" -H "Authorization: Bearer
   ${token}" https://<mno_ip>/im/types/NodeInfo/instances -o "get_info.zip"
   ```

   In this example, the logs are downloaded to the current working directory under the name "get_info.zip".
7. (Optional) Add the following optional attributes to the log collection request as query parameters:
   - `targetIPs`—Filter the result to only part of the nodes (by their IPs)
   - `copyRepositories`—Copy MDM repositories (true/false, default is false)
   - `liteVersion`(lite version)—Collect trc.0, exp.0, and umt.0 files only and repository files (true/false, default is false)
   - `copyBinaries`—Collect MDM, SDS, SDR, SDT, LIA binaries and core dumps (true/false, default is false)
   - `collectSdbgScreens` (true/false, default is false)

   For example:

   ```
   curl  -k -X -i POST -H "Content-Type:application/json" -H "Authorization:
   Bearer ${token}"   "https://<mno_ip>/im/types/NodeInfo/instances/actions/collectLogs?
   copyRepositories=true&targetIPs=10.55.118.61&targetIPs=10.55.118.62"
   ```

8. To clear the operation and move to idle, run the following API commands:

   `POST https://<mno_ip>/im/types/Command/instances/actions/clear`

   `https://<mno_ip>/im/types/ProcessPhase/actions/moveToIdlePhase`

   After the log collection operation is complete, mark the completed operation as completed to allow the other jobs to run.

   For example:

   ```
   curl -s -k  -X POST -H "Content-Type:application/json" -d '{}' -H "Authorization:
   Bearer ${token}" https://<mno_ip>/im/types/Command/instances/actions/clear
   ```

   ```
   curl -s -k  -X POST -H "Content-Type:application/json" -d '{}' -H "Authorization:
   Bearer ${token}" https://<mno_ip>/im/types/ProcessPhase/actions/moveToIdlePhase
   ```

17

Retrieving additional PowerFlex logs

This section contains instructions for retrieving RAID controller, vSphere PowerFlex plug-in, PowerFlex Installer, and system event logs.

Retrieve RAID controller logs from VxFlex Ready Node systems

Perform this procedure to retrieve the RAID controller logs from ESXi- and Linux-based servers in a VxFlex Ready Node system.

Ensure that you have access to the following:

- IP address of the node
- Password for the root user in ESXi-based and Linux-based systems and the administrator user in Windows-based systems
- The RAID controller utility, which is enabled (for details, see the *Hardware Configuration and Operating System Installation Guide* of your system)

1. SSH or RDP to the VxFlex Ready Node.
2. Retrieve the controller information:

Operating System	Run this command

ESXi	`/opt/lsi/perccli/perccli /call show all > <file_name>`
	Example:
	`/opt/lsi/perccli/perccli /call show all > /var/tmp/store/RAIDinfo.txt`

Linux	`/opt/MegaRAID/perccli/perccli64 /call show all > <file_name>`
	Example:
	`/opt/MegaRAID/perccli/perccli64 /call show all > /var/tmp/store/RAIDinfo.txt`

3. Retrieve the `Show Events` log file:

Operating System	Run this command

ESXi	`/opt/lsi/perccli/perccli /call show events file=<file_name>`
	Example:
	`/opt/lsi/perccli/perccli /call show events file=/var/tmp/store/RAIDevents.txt`

Linux	`/opt/MegaRAID/perccli/perccli64 /call show events file=<file_name>`

Operating System	Run this command
	Example: `/opt/MegaRAID/perccli/perccli64 /call show events file=/var/tmp/store/RAIDevents.txt`

You can retrieve the `RAIDevents.txt` file from your local drive.

4. Retrieve the `Termlog` log file:

Operating System	Run this command

ESXi	`/opt/lsi/perccli/perccli /call show termlog file=<file_name>`
	Example:
	`/opt/lsi/perccli/perccli /call show termlog file=/var/tmp/store/RAIDtermlog.txt`

Linux	`/opt/MegaRAID/perccli/perccli64 /call show termlog file=<file_name>`
	Example:
	`/opt/MegaRAID/perccli/perccli64 /call show termlog file=/var/tmp/store/RAIDtermlog.txt`

You can retrieve the `RAIDtermlog.txt` file from your local drive.

Retrieve system event logs in VxFlex Ready Node servers

Perform this procedure to access the system events logs (SEL) in a VxFlex Ready Node server.

Ensure that you have access to the following:

- IP address of the iDRAC port
- Login credentials for the iDRAC (admin/admin as default username/password)

1. From a web browser, go to **`http://<IP_address_iDRAC_port>`**.
2. In the **Console Login** window, type the user name and password, then click **Login**.
3. To view the event log, select **View Logs** in the **Quick Launch Tasks** pane.
   The **System Event Log** is displayed with color-coded severity levels.
4. To save the event log, click the **Save As** button at the bottom of the table.
   The event log is saved in a `.CSV` file.

   The power supply- and fan-related errors in **Event Log** may be intermittent in nature, and therefore may display repetitive events for one module. For such errors, it is recommended that you remove the module and replace it in its socket. This might be a connection-related issue.

Collect logs from the management VM cluster

Perform the following procedure to collect logs from the management VM cluster.

1. SSH as root to the management installer node.

2. Run the following command: `/opt/dell/pfmp/PFMP_Installer/scripts/pfmp_support`

```
installer-30:/opt/dell/pfmp/PFMP_Installer/scripts # ./pfmp_support
estimating required space
cleaning up temporary directories
collecting kubernetes data
collecting shared kubernetes data
collecting server data
collecting general hardware data
collecting network data
collecting storage data
preparing files for collection
generating bundle
cleaning up temporary directories
bundle available at '/tmp/powerflex-pfmpsupport/pfmpSupport.tgz'
```

18

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.

For this policy, you do not need to define a source, since the required source for PowerFlex events is a built-in feature.

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.

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.

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 though the Ingress Controller will not be sent.

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.

19

Managing storage devices using CloudLink

This section describes how to manage the storage devices using CloudLink.

This capability is available on the PowerFlex appliance and PowerFlex rack offerings only.

Encrypt the SSD or NVMe storage devices

Encrypt SSDs or NVMes using one of the following methods.

CAUTION: Never attempt to encrypt or erase the devices that are currently attached to the SDS. Devices should only be encrypted before they are added to the SDS, or after removing them from the SDS. Any existing data on the device will be destroyed as a result of this procedure.

Encrypt the devices in CloudLink Center

Encrypt the device in CloudLink Center.

1. Click **Agent** > **Machines**.
2. Select the checkbox for the required machine.
3. Click **Actions** > **Encrypt**
4. Select the check box next to the device you want to encrypt.
5. Click **Encrypt**.
6. Repeat for each SSD requiring encryption.

Encrypt single devices using the CLI

Use this procedure to encrypt single devices using the CLI:

1. Connect to the SDS node using SSH.
2. Run the following command to encrypt the new drive.

   ```
   svm encrypt <device_name>
   ```

   where *<device_name>* is a variable.

   For example:

   ```
   svm encrypt /dev/sdX
   ```

   or

   ```
   svm encrypt /dev/nvmeXn0
   ```

   After about 60 seconds, the new device will be encrypted.

Encrypt multiple devices using the CLI

Use this procedure to encrypt multiple devices using the CLI.

1. Connect to the SDS node using SSH.
2. Encrypt the drives.
   - SAS-based SSDs:

a. Select the devices for encryption.

   For example, `/dev/sdX`, where *X* could be a b c - z.

b. Run the following command:

```
for i in b c {j..o} {r..v};do svm -y encrypt /dev/sd$i;done
```

- NVMe-based SSDs:
  a. Select the devices for encryption.

     For example, `/dev/nvmeXn1`, where *X* could be 0 1 2 - 24.

  b. Run the following command:

```
for i in {0..3} 6 7 {10..13} 16 17;do svm -y encrypt /dev/nvme$[i]n1;done
```

After about 60 seconds, the new device will be encrypted.

Verify that SSD or NVMe is encrypted

Find the new device path of the SSD or NVMe and confirm that the device is encrypted.

1. Run the following command to find the new device path:

```
svm status
```

   Output similar to the following should be displayed:

   - SSD: `/dev/mapper/svm_sdh`
   - NVMe: `/dev/mapper/svm_nvme6n1`

2. In CloudLink Center, click **Agents** > **Machines**.
3. In the **Devices** area, verify that the drive is visible and has a status of **Encrypted**.

Manage the SED storage devices

Manage the SEDs (self-encrypting devices) using one of the following methods:

CAUTION: Never attempt to manage or erase the devices that are currently attached to the SDS. Devices should only be managed before they are added to the SDS, or after removing them from the SDS. Any existing data on the device will be destroyed as a result of this procedure.

Manage the SEDs in CloudLink Center

Manage the device from CloudLink Center.

1. Click **Agent** > **Machines**.
2. Select the check box next to the SED you want to manage.
3. Click **Actions** > **Manage SED**.
   The **Manage SED** dialog box is displayed. It is populated with the first unmanaged SED device. You can add different device to encrypt.
4. Click **Manage**.
5. Repeat for each SED requiring encryption.

Manage single SEDs using the CLI

Manage individual devices using the CLI:

1. Connect to the SDS node using SSH.

2. Run the following command to discover the unencrypted and unmanaged SEDs:

```
svm status
```

3. Run the following command so that CloudLink will control the SED device:

```
svm manage /dev/sdX
```

For example:

```
svm manage /dev/sdh
```

4. Run `svm status` again to verify that the device is now managed:

The output should be similar to the following:

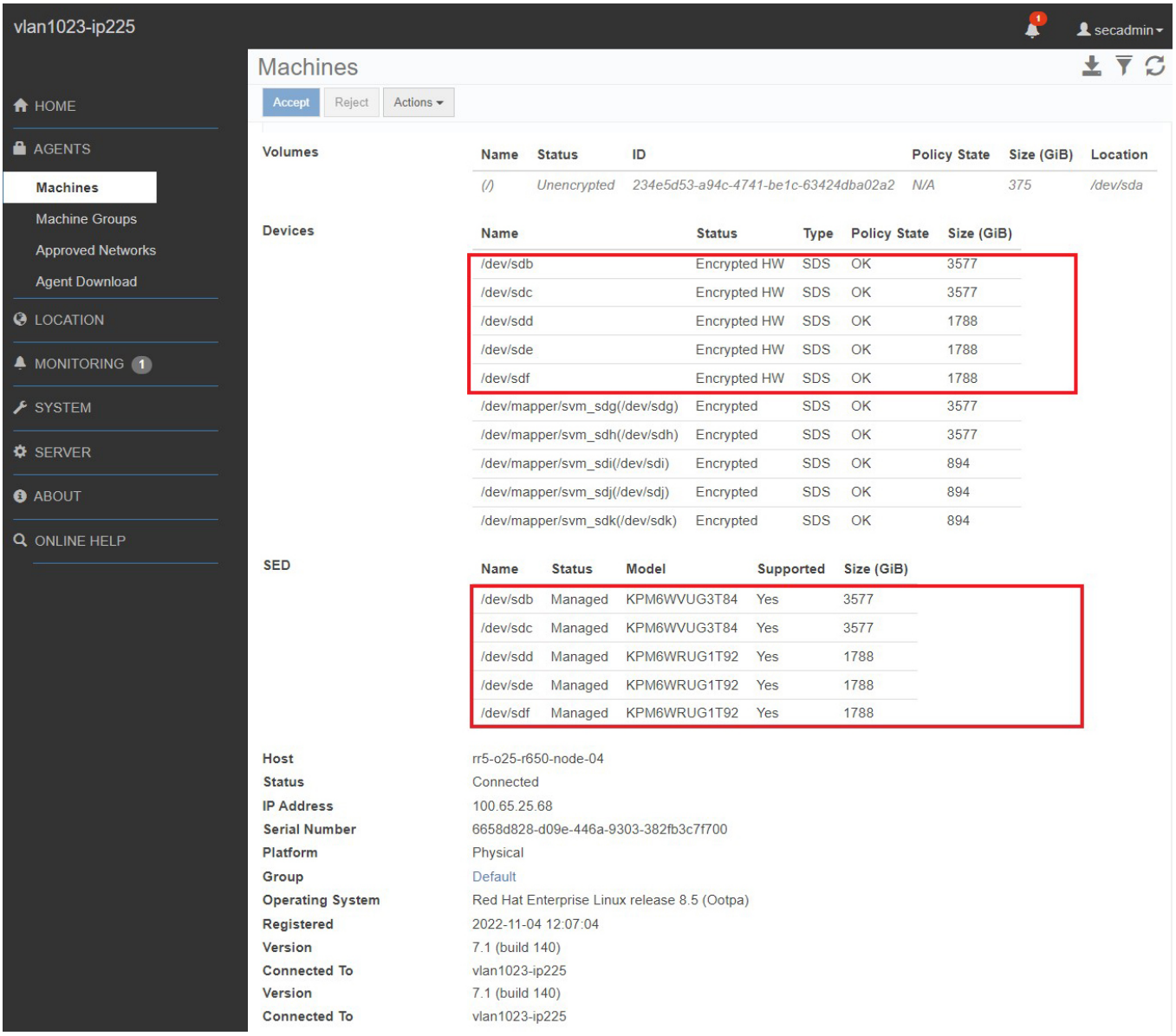
```
[root@rr5-o25-r650-node-03 ~]# svm status
State: Connected (server 100.65.23.225)
Group: Default
Policy: Manual
AES-NI HW acceleration: Yes

Volumes:
/                   unencrypted
swap                unencrypted

Devices:
/dev/sdf            managed             (sed   SZ: 1788G MOD: KPM6WRUG1T92     SPT:
Yes  )
/dev/sdd            managed             (sed   SZ: 1788G MOD: KPM6WRUG1T92     SPT:
Yes  )
/dev/sdb            managed             (sed   SZ: 3577G MOD: KPM6WVUG3T84     SPT:
Yes  )
/dev/sde            managed             (sed   SZ: 1788G MOD: KPM6WRUG1T92     SPT:
Yes  )
/dev/sdc            managed             (sed   SZ: 3577G MOD: KPM6WVUG3T84     SPT:
Yes  )
/dev/sdb            unencrypted       (sds   SN:94917674              )
/dev/sdc            unencrypted       (sds   SN:94917675              )
/dev/sdd            unencrypted       (sds   SN:94917676              )
/dev/sde            unencrypted       (sds   SN:94917677              )
/dev/sdf            unencrypted       (sds   SN:94917678              )
/dev/sdg            encrypted         (sds   SN:94917679             /dev/mapper/
svm_sdg)
/dev/sdh            encrypted         (sds   SN:94917680             /dev/mapper/
svm_sdh)
/dev/sdi            encrypted         (sds   SN:94917681             /dev/mapper/
svm_sdi)
/dev/sdj            encrypted         (sds   SN:94917682             /dev/mapper/
svm_sdj)
/dev/sdk            encrypted         (sds   SN:94917683             /dev/mapper/
svm_sdk)
```

NOTE: The status of the SED devices is displayed in the output as managed, but unencrypted.

Verify that SED is encrypted

Find the new device path and confirm that the SED is encrypted.

1. In CloudLink Center, click **Agents** > **Machines**.
2. Select the host of the encrypted device.
3. Use the device name listed in the `svm status` command output to perform the following verification checks:
   - In the **Devices** area, verify that the drive is visible and has a status of **Encrypted HW**.
   - In the **SED** area, verify that the drive's status is displayed as **Managed**.



Add the encrypted devices to an SDS

After the devices are encrypted, in the PowerFlex Manager add them to the relevant PowerFlex SDS. For software-encrypted SSDs, use their new `/dev/mapper/..` path when adding the device. SEDs use the normal `/dev/sdX` path.

NOTE: Do not add a software-encrypted SSD using its original path (`/dev/...`). Doing so can stop the device encryption (device erasure, in terms of CloudLink), and this can corrupt the data on the device.

Remove software-encrypted devices from an SDS and remove device encryption

Use this task to remove a device from an SDS and remove the device's encryption. Use this task for both software-encrypted devices and SEDs.

CAUTION: Never attempt to manage or erase the devices that are currently attached to the SDS. Devices should only be managed before they are added to the SDS, or after removing them from the SDS. Any existing data on the device will be destroyed as a result of this procedure.

1. Remove the device from the SDS:
   - PowerFlex CLI:

     Use the SCLI `--remove_sds_command`. For example:

     ```
     scli --remove_sds_device --sds_name MY_SDS --device_path /dev/mapper/svm_sdX
     ```

     or

     ```
     scli --remove_sds_device --sds_name MY_SDS --device_path /dev/mapper/svm_nvmeXn1
     ```

   - PowerFlex Manager:

     For more information, see Remove devices.

2. Remove the encryption through CloudLink Center GUI or using the svm `erase` command:

   NOTE: Removing (erasing) a device from CloudLink destroys all data on the device.

   ```
   svm erase <device_name>
   ```

   For example:

   ```
   svm erase /dev/sdX
   ```

   or

   ```
   svm erase /dev/nvmeXn0
   ```

3. Confirm that the device was erased.

20

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	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	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	1. On the menu bar, click **Settings** > **Networking**. 2. Click **System Data networks**. 3. Select the network and click **Remove**. 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	`scli --add_system_network --network_ip <IP> --network_mask <IP> [--network_name <NAME>] (--host_group_id <ID> | --host_group_name <NAME>)`
Rename system data networks	`scli --rename_system_network (--network_id <ID> | --network_name <NAME>) --new_name <NAME>`
Remove system data networks	`scli --remove_system_network (--network_id <ID> | --network_name <NAME>)`

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	`scli --add_host_group [--host_group_name <NAME>] [(--network_id <ID> | --network_name <NAME>)] [(--host_nqn <NQN> | --host_id <ID> | --host_name <NAME>)]`
Modify host group	`scli --modify_host_group (--host_group_id <ID> | --host_group_name <NAME>) [(--network_id <ID> | --network_name <NAME>)]`
Rename host group	`scli --rename_host_group (--host_group_id <ID> | --host_group_name <NAME>) [--new_name <NAME>]`
Remove host group	`scli --remove_host_group (--host_group_id <ID> | --host_group_name <NAME>)`
Assign host to group	`scli --assign_host_to_host_group (--host_nqn <NQN> | --host_id <ID> | --host_name <NAME>) (--host_group_id <ID> | --host_group_name <NAME>)`
Remove host from group	`scli --remove_host_from_host_group (--host_nqn <NQN> | --host_id <ID> | --host_name <NAME>)`
Query host group	`scli --query_host_group (--host_group_id <ID> | --host_group_name <NAME>)`
Query all host group	`scli --query_all_host_group`

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	`scli --add_network_set [--network_set_name <NAME>] [(--network_id <ID> | --network_name <NAME>)]`

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

21

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: • yes • no (default)
Pre-event failure policy	The policy applied when a pre-event notification fails. Valid values are: • 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: • 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: • 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.

Attributes	Description
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.
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: • 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).	• SMB/CIFS • NFS (v4)
OpenFileRead	Sends a notification when a file is opened for read access.	• SMB/CIFS • NFS (v4)
OpenFileReadOffline	Sends a notification when an offline file is opened for read access.	• SMB/CIFS • NFS (v4)
OpenFileWrite	Sends a notification when a file is opened for write access.	• SMB/CIFS • NFS (v4)
OpenFileWriteOffline	Sends a notification when an offline file is opened for write access.	• 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.	• SMB/CIFS • NFS (v3/v4)

Attributes	Definition	Protocol
`CreateDir`	Sends a notification when a directory is created.	• SMB/CIFS • NFS (v3/v4)
`DeleteFile`	Sends a notification when a file is deleted.	• SMB/CIFS • NFS (v3/v4)
`DeleteDir`	Sends a notification when a directory is deleted.	• SMB/CIFS • NFS (v3/v4)
`CloseModified`	Sends a notification when a file is changed before closing.	• SMB/CIFS • NFS (v3/v4)
`CloseUnmodified`	Sends a notification when a file is not changed before closing.	• 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.	• SMB/CIFS • NFS (v3/v4)
`RenameDir`	Sends a notification when a directory is renamed.	• 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.

22

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 fro 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 4.0 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.

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.

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.

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.

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.

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.

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.

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.

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
Scan for New Storage Devices	Rescan all adapters to discover new storage devices. If new devices are discovered, they appear in the device list.
Scan for New VMFS Volumes	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.

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