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.
Part IV: Configure and Customize

4 Configuration

Protection Domains...
Add Protection Domains...
Configure network throttling...
Activate a Protection Domain...
Inactivate a Protection Domain...
Set RFcache policy...
Remove a Protection Domain...

Fault Sets...
Add Fault Sets...
Enter and exit Fault Set into Maintenance Mode...

SDS...
Add SDSs...
Add storage devices...
Add acceleration devices...

Storage Pools...
Add Storage Pools...
Storage Pool settings...
Read Flash Cache and Read RAM Cache...
Set device capacity limits...
Using the background device scanner...
Set media type for Storage Pool...
Configuring I/O priorities and bandwidth use...
Create a VM storage policy for Virtual Volumes...
Configuring acceleration...
Set up a login banner using the CLI.................................................................145
Upload a login banner using the PowerFlex Installer................................145
Enable/disable preemptive acceptance of the login banner.....................145
Activate preemptive acceptance of the login banner..................................146
Change LIA authentication method to LDAP..................................................146
Add LDAP server..........................................................................................146
Remove LDAP server...................................................................................147

9 User Management.......................................................................................148
MDM and LDAP integration in an AMS managed system..........................148
User roles......................................................................................................148
Setting the User Authentication Method.......................................................149
set_user_authentication_method..................................................................149
Adding and modifying local users...............................................................150
add_user......................................................................................................150
delete_user..................................................................................................150
modify_user...............................................................................................151
query_users...............................................................................................151
query_user..................................................................................................151
reset_password.........................................................................................152
set_password..............................................................................................152
disable_admin..........................................................................................153
Reset the admin user password.................................................................153
Deploying PowerFlex using a non-root user..............................................154
Configure a non-root non-interactive sudo user........................................155

10 Fault reporting features.........................................................................156
General........................................................................................................156
Configure SNMP properties after deployment.............................................156
Configure Dynamic Host Name resolution for SNMP in PowerFlex...........156
Configure PowerFlex Gateway properties....................................................157

11 Add, Remove or Rename Components..................................................161
Using SSH authentication on the PowerFlex Gateway...............................161
Adding components to an existing PowerFlex environment........................162
Add components using the PowerFlex Installer........................................162
Add components using the VMware deployment wizard..........................162
Remove PowerFlex.....................................................................................163
Remove PowerFlex using the PowerFlex Installer......................................163
Unregister the PowerFlex plug-in..............................................................163
Renaming objects......................................................................................164

12 Logs........................................................................................................165
Enable automatic log collection.................................................................165
Set ESXi credentials for auto collect logs.................................................165

13 LIA.........................................................................................................166
Change LIA behavior..................................................................................166
Add LIA to a system to enable automated maintenance and upgrades........166
Part V: VMware environment specific tasks

14 PowerFlex plug-in
  Configure components
  Configure components—basic
  Configuring components—advanced

15 Manually performed tasks
  Clean the PowerFlex VMware environment
  SVM manual memory allocation
  Managing ESXi servers
  Modify parameters on ESXi servers
  Check the SDC state on ESXi servers

Part VI: Operating System Patching

16 Operating System Patching
  Upgrade the CentOS operating system on SVMs
  Running scripts on hosts—overview
  Run a script on one or more hosts— procedures
List of Figures

Figure 1. Test ping to ensure mtu setting..........................................................................................................44

Figure 2. Show interface output.........................................................................................................................44

Figure 3. Adapter properties............................................................................................................................... 45

Figure 4. Ping output........................................................................................................................................... 45

Figure 5. Test ping to ensure mtu setting......................................................................................................... 47

Figure 6. Virtual Machine Properties................................................................................................................. 49

Figure 7. System Event Log with failed DIMM.................................................................................................80

Figure 8. Before adding......................................................................................................................................125

Figure 9. After adding.........................................................................................................................................126

Figure 10. Set Virtual IPs for PowerFlex system screen................................................................................ 135
List of Tables

Table 1. NVDIMM information table.................................................................................................................... 71

Table 2. Local and LDAP user roles and permissions..................................................................................... 148

Table 3. Plug-in activity matrix..........................................................................................................................169
As part of an effort to improve its product lines, Dell EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your Dell EMC technical support professional if a product does not function properly or does not function as described in this document.

**NOTE:** This document was accurate at publication time. Go to Dell EMC Online Support (https://www.dell.com/support/home/en-us/product-support/product/scaleio/overview) to ensure that you are using the latest version of this document.

Previous versions of Dell EMC PowerFlex were marketed under the name Dell EMC ScaleIO and VxFlex OS. Similarly, previous versions of Dell EMC VxFlex Ready Node were marketed under the name Dell EMC ScaleIO Ready Node. References to the old names in the product, documentation, or software, etc. will change over time.

**NOTE:** Software and technical aspects apply equally, regardless of the branding of the product.

### Related documentation

The release notes for your version includes the latest information for your product.

To view the most up-to-date version of documentation for your product, go to https://cpsdocs.dellemc.com/.

### Where to get help

Dell EMC support, product, and licensing information can be obtained as follows:

**Product information**  
For documentation, release notes, software updates, or information about Dell EMC products, go to Dell EMC Online Support at https://www.dell.com/support/home/en-us/product-support/product/scaleio/overview.

**Technical support**  
Go to Dell EMC Online Support and click Support. You will see several options for contacting Dell EMC Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your Dell EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

### Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to techpubcomments@emc.com.
Getting Started
Log into PowerFlex

You can log into PowerFlex via the GUI or by using the CLI.

Post-deployment tasks and configuring and customizing required workflows can be done through the GUI or CLI.

**Log in to the PowerFlex GUI**

In a web browser, enter the IP address of the PowerFlex presentation server and use your user credentials to log in.

**Prerequisites**

Ensure that:

- The PowerFlex GUI software is installed on the PowerFlex presentation server. For more information about installing it, refer to the Deploy PowerFlex Guide.
- The system administrator has linked the PowerFlex GUI to the PowerFlex system. For more information, see the Configure and Customize PowerFlex Guide.
- The system administrator has configured users, including LDAP, when used. For more information, see "User Management" in the Configure and Customize PowerFlex Guide.
- You have these credentials (available from the administrator):
  - IP address of the PowerFlex presentation server, including the port number (default = 8443) and the https prefix. http can only be used if the system administrator specifically configured the system to allow its use.
  - Username
  - Password

**Steps**

1. In a web browser, enter the IP address of the PowerFlex presentation server. The PowerFlex GUI login page is displayed.
2. Enter the username and password and click Log In.

**Results**

The PowerFlex GUI is displayed.

**Log in**

To access the CLI, you must first log in to the management system using a terminal application.

If the CLI and the MDM do not reside on the same server, add the --mdm_ip parameter to all CLI commands.

In a non-clustered environment, use the MDM IP address. In a clustered environment, use the IP addresses of the master and slave MDMs, separated by a comma. For example:

```
sc1i --mdm_ip 10.10.10.3,10.10.10.4 --login --username supervisor1 --password password1
```

You will be prompted to enter the password.

When using LDAP, include the LDAP domain in the command. For more information on LDAP, see PowerFlex User Roles and LDAP Usage Technical Notes. For example:

```
sc1i --mdm_ip 10.10.10.3,10.10.10.4 --login --username JohnDoe@ldap.acme.com --password password1 --ldap_authentication
```

The default user created during setup is the SuperUser, with the admin username.
**login**

Log the specified user into the management system. Every user must log in before performing CLI commands.

When a user is authenticated by the system, all commands will be executed with the respective role until a logout is performed, or until the session expires, by reaching one of the following timeouts:

- Maximum session length (default: 8 hours)
- Session idle time (default: 10 minutes)

**Syntax**

```bash
scli --login --username <NAME>  
[--password <PASSWORD>]
[--ldap_authentication | --native_authentication]
[(---approve_certificate_once | --approve_certificate]
--accept_banner_by_scripts_only
```

**Parameters**

- **--username**
  Username

- **--password**
  User password. If you do not type your password, you will be prompted to do so.
  
  **NOTE:** In Linux, to prevent the password from being recorded in the history log, leave out the ```password``` flag and enter the password interactively.

- **--ldap_authentication**
  Log in using the LDAP authentication method. LDAP authentication parameters should be configured and LDAP authentication method should be set.

- **--native_authentication**
  Log in using the native authentication method (default).

- **--approve_certificate_once**
  One-time approval of the MDM’s certificate (without adding the certificate to the truststore)

- **--approve_certificate**
  Automatic approval of the MDM’s certificate for the next commands (adds the certificate to the truststore)

- **--accept_banner_by_scripts_only**
  Preemptive approval of login banner

**Examples**

```bash
scli --login --username siuser1 --password 1!2@3A
```

**NOTE:** During installation using the PowerFlex Installer or the VMware plug-in, the password for the admin user is reset, and you should log in with the new password. If you installed PowerFlex manually, after logging in the first time with the default password (admin), you must change the password and log in again. Once that is accomplished, the admin user can create additional users.

When logging in, if a login banner has been configured and enabled in your system, you are prompted to press any key, after which the banner is displayed. To continue, enter “q” to quit the login banner, and then enter “y” to approve the banner.
Log the current user out of the system.

Syntax

```
scli --logout
```

Example

```
scli --logout
```

Use SCLI in non-secure mode

If you want to run commands in PowerFlex in non-secure mode, you must first disable the secure communication setting on every MDM server.

About this task

You must make the following change to enable running commands.

Steps

On every MDM server, disable secure communication:

- Windows: In the SCLI conf.txt file, add `cli_use_secure_communication=0`
- Linux: Run `echo cli_use_secure_communication=0 >> ~/.scli/conf.txt`
Post-Deployment Activities
Post-deployment tasks

Perform post-deployment tasks described in this section. After performing these tasks, continue to the "Configure and Customize PowerFlex" section for further configuration steps as required.

### Post-deployment task checklist

Use the following checklist to verify that you complete the required and optional post-deployment procedures.

### Post-deployment procedures

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Notes</th>
<th>Mandatory?</th>
<th>Done</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add SDS devices</td>
<td>After deploying PowerFlex on ESXi servers with DirectPath device management, use the vSphere plug-in to add SDS devices.</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>Add and map volumes</td>
<td>Adding and mapping volumes can be performed using various PowerFlex management tools.</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>Review PowerFlex performance best practices</td>
<td></td>
<td>Recommended</td>
<td></td>
</tr>
<tr>
<td>Review PowerFlex best practice configurations</td>
<td></td>
<td>Recommended</td>
<td></td>
</tr>
<tr>
<td>Create a Lockbox, and add the MDM credentials to it</td>
<td>If you want to use SNMP, ESRS, LDAPS, or the Auto Collect Logs feature, your system must have a Lockbox. Recommended best practice is to create the Lockbox during installation with the PowerFlex Installer when selecting Set advanced options. Only when a Lockbox has not been created during installation, should you manually create a Lockbox.</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Configure EMC Secure Remote Support (ESRS)</td>
<td></td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>Define native users in the system and change the default admin password.</td>
<td></td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Define LDAP users (if using PowerFlex with LDAP)</td>
<td>For detailed information about setting up PowerFlex with LDAP, see &quot;Configure LDAP users&quot;.</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Enable SNMP and configure the SNMP trap receiver</td>
<td>If SNMP was not configured during installation using the advanced options in the PowerFlex Installer, it can be configured after deployment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable FIPS compliance</td>
<td>You can enable OpenSSL Federal Information Processing Standards (FIPS) compliance implementation in the MDM for communication between the SDSs and the SDCs to the MDM. For instructions on how to enable OpenSSL FIPS compliance implementation, see &quot;Enable OpenSSL FIPS compliance.&quot;</td>
<td>Optional</td>
<td></td>
</tr>
</tbody>
</table>
Prepare lockbox files for Java upgrade

Before changing the Java version of a node that is running the PowerFlex Gateway or AMS of PowerFlex v2.5 or later, you must prepare lockbox-related files.

About this task
The lockbox in PowerFlex v2.5 saves files in the Java folder of the PowerFlex Gateway and the AMS. These files need to be saved before any Java version update, then pasted back into the folder.

Steps
1. From the java\jre<VERSION>\lib\ext (for Windows) or java/jre<VERSION>/lib/ext (for Linux) Java folder, copy these files to a different folder:
   - commons-lang3-3.6.jar
   - cryptoj-6.2.3.jar

   **NOTE:** Only Java 8 is supported.
2. Update the Java version.
3. Paste these files back to the folder from where you copied them.

Create the lockbox

For security reasons, the lockbox is created on the PowerFlex Gateway during system deployment. If for some reason, this was not done, you must create a lockbox manually, and then add the MDM credentials, using FOSGWTool. Lockbox is required for the following features: ESRS, SNMP, LDAPS and automatic log collection.

Prerequisites
- Collect MDM username and password.

About this task

**NOTE:** The lockbox can also be created during system deployment, when the PowerFlex Installer customized installation procedure is used. This is the preferred method for creating the lockbox. To configure SNMP alerts during deployment or when setting up the installation, select Set advanced, enable the Configuration option called Enable alert service. If the PowerFlex Installer installation wizard was used to deploy the system, the lockbox was not created.

**NOTE:** To check whether a lockbox already exists, search for the following directory. If the lck_xml directory exists, a lockbox is configured in the system.
  - Linux: /opt/ EMC/ScaleIO/gateway/conf
  - Windows: C:\Program Files\EMC\ScaleIO\Gateway\conf

Use FOSGWTool to create or configure a lockbox. Only use FOSGWTool to create a lockbox if no lockbox exists. To use FOSGWTool, enter the appropriate path, based on your operating system, and append the commands to the end of the file path:

- Linux FOSGWTool default file path: /opt/EMC/ScaleIO/gateway/bin/FOSGWTool.sh
- Windows FOSGWTool default file path: C:\Program Files\EMC\ScaleIO\Gateway\bin\FOSGWTool.bat

Steps
1. Create a lockbox:

   ```
   <FOSGWTool_PATH> --change_lb_passphrase --new_passphrase <NEW_PASSPHRASE>
   ```

   **NOTE:** From system version 2.5 and later, the installation process assigns a random passphrase to this property, and it is highly recommended not to configure or use this property, because it could create a security breach.
2. Add MDM credentials to the lockbox:

```
<FOSGWTool_PATH> --set_mdm_credentials --mdm_user <MDM_USERNAME> --mdm_password <MDM_PASSWORD>
```

Windows example:

```
C:\Program Files\EMC\ScaleIO\Gateway\bin\FOSGWTool.bat --set_mdm_credentials --mdm_user admin --mdm_password Scaleio123
```

**Customer support**

Dell EMC provides immediate support via early detection of issues that are communicated by the Secure Remote Services (SRS) gateway or email alert notifications. You may choose which method best suits your business requirements.

For SRS configuration, refer to "Register PowerFlex system to SRS". For information on how to configure the email alert notifications, refer to "Email notifications".

**Register PowerFlex system to SRS**

Your PowerFlex system is not automatically registered to SRS following deployment. You need to manually register the PowerFlex system to SRS.

**About this task**

The following procedure describes how to register:

**Steps**

1. In the web browser, go to the IP address of your system's PowerFlex Gateway.
2. Log in to the PowerFlex Gateway.
3. From the Maintain tab, click System Logs & Analysis and select Register PowerFlex system to SRS. The Register PowerFlex system to SRS dialog box is displayed.
4. Enter the MDM password in the MDM admin password box.
5. Enter the SRS server address in the Server server URL box.
6. Enter a user name in the SRS Username box to register the system with the SRS service.
7. Enter a password in the SRS Password box to register the system with the SRS service.
8. Enter the PowerFlex Gateway IP address in the PowerFlex Gateway URL box.
9. Click the Register to SRS button to register the PowerFlex system to the SRS.

**Requirements for configuring SRS via CLI**

Before configuring SRS, ensure that your system meets the following requirements, and that you have the following information:

- **Requirements**:
  - SRS gateway v3 version 3.08 or higher must be installed and configured. It is recommended to create at least two SRS gateways and define them as a cluster via the backend server.
  - SRS gateway must be reachable from the PowerFlex Gateway node on port 9443.
  - A lockbox has already been created and the MDM credentials have been added.
  - Ensure that the PowerFlex Gateway can reach the SRS gateway by its hostname (not only by its IP address). For example, use DNS or /etc/hosts.
  - The PowerFlex license must be installed.
  - The Gateway Management IP address to be used as the Connect-In IP address must be an IP address that is accessible from the SRS gateway (for example, in case of NAT). Ensure that you know this IP address, because you will need it when you perform the registration procedure.
  - On the PowerFlex Gateway, in the gatewayUser.properties file, set the property features.enable_ESRS=true
  - A web browser is required for this procedure.

- **Information**:
  - One or more IP addresses of the SRS servers.
  - SRS user and password credentials for the PowerFlex command.
MDM user name and password.

**Configure SRS**

Enable Secure Remote Support (SRS) for remote support.

**Prerequisites**

Ensure that you have

- One or more IP addresses of the SRS gateway servers. Note that SRS does not currently support IPv6.
- SRS username and password.
- PowerFlex Gateway IP address, username, and password.
- The PowerFlex Management IP address to be used as the Connect-In IP address. It must be an IP address that is accessible from the SRS gateway (for example, in case of NAT).

**Register the system with the SRS gateway via CLI**

To enable the SRS feature on your PowerFlex system, you must add the SRS gateway's certificate to the trust store, and register your system on the SRS gateway.

**Prerequisites**

Refer to "Requirements for configuring SRS" in this section.

The following REST procedures described are performed using cURL. You may use other similar tools and their corresponding commands to perform the steps.

A web browser is required for this procedure.

**About this task**

To work with SRS, the Lockbox must be configured, and the MDM credentials must be added. The Lockbox is required for both SNMP and SRS. Refer to "Create the lockbox" for the procedure of how to create a lockbox.

**Steps**

1. Enable the SRS feature in the gatewayUser.properties file.
   a. Use a text editor to open the gatewayUser.properties file, located in the following directory on the PowerFlex Gateway server:

<table>
<thead>
<tr>
<th>PowerFlex Gateway installed on</th>
<th>Location of gatewayUser.properties file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>C:\Program Files\EMC\ScaleIO\Gateway\webapps\ROOT\WEB-INF\classes\</td>
</tr>
<tr>
<td>Linux</td>
<td>/opt/emc/scaleio/gateway/webapps/ROOT/WEB-INF/classes</td>
</tr>
</tbody>
</table>

   b. Change the enable_ESRS feature to "true":

   `features.enable_ESRS=true`

   c. Save the file.

2. Add the SRS gateway's SSL certificate to the truststore.
   a. Browse to `<ESRS_Gateway_IP_address:9443>`.
   b. View the SHA-1 certificate, and copy it to file. If a root certificate exists, copy it to file as well.
   c. Copy the sha-1.cer file (mandatory) and root.cer file (optional) to the `root` folder on the PowerFlex Gateway.
   d. Log in to REST and get a token from the PowerFlex Gateway. Save a copy of the token in a text editor.

   ```
   curl -k -v --basic --user admin:<mdm_admin_password> https://<POWERFLEX_GATEWAY_IP_ADDRESS>/api/login
   ```

   At the very end of the command output, the token is displayed. For example:

   "YWRtaW46MTQ4NjQyMzM2jg4MzpmOTdkYzcOTrjMGRjNzFjNTljNTljMzJiM2U5NWJjNmPhNA"
e. Using REST, add the SHA-1 certificate to the truststore.

```bash
curl -k -v --basic -u admin:<token_received_from_previous_command> --form "file=@<path_to_certificate_file>" https://<POWERFLEX_GATEWAY_IP_ADDRESS>/api/trustHostCertificate/Mdm
```

f. Optionally, use the same command as the previous step to add the root certificate to the truststore.

3. Restart the PowerFlex Gateway service.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Restart the EMC ScaleIO Gateway service</td>
</tr>
<tr>
<td>Linux</td>
<td>Type the command</td>
</tr>
<tr>
<td></td>
<td><code>service scaleio-gateway restart</code></td>
</tr>
</tbody>
</table>

4. Register PowerFlex on the SRS gateway. In command line, use the following FOSGWTool command:

```bash
<FOSGWTool_PATH> --register_ESRS_gateway --scaleio_gateway_ip <IP_ADDRESS:PORT> --scaleio_gateway_user <USER> --scaleio_gateway_password <PASSWORD> --ESRS_gateway_ip <IP_ADDRESS> --ESRS_gateway_user <USER> --ESRS_gateway_password <PASSWORD> --connect_in_ip <IP_ADDRESS>
```

where `--ESRS_gateway_user` is the user name used for EMC support (typically, an email address), and `--ESRS_gateway_password` is its corresponding password. `--connect_in_ip` is the MGMT IP address of the current Master MDM.

**Results**

SRS registration is complete.

**Perform other SRS configuration activities**

Use FOSGWTool in command line for SRS configuration activities.

**About this task**

FOSGWTool is located in:

- Linux: `/opt/emc/scaleio/gateway/bin/FOSGWTool.sh`
- Windows: `C:\Program Files\EMC\ScaleIO\Gateway\bin\FOSGWTool.bat`

**Steps**

The following activities can be performed with FOSGWTool:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>To unregister from all SRS gateways, type the command:</td>
<td><code>&lt;FOSGWTool_PATH&gt; --unregister_esrs_gateway --scaleio_gateway_ip &lt;ip address:port&gt; --scaleio_gateway_user &lt;user&gt; --scaleio_gateway_password &lt;password&gt;</code></td>
</tr>
<tr>
<td>To remove a specific SRS gateway from the PowerFlex Gateway configuration, type the command:</td>
<td><code>&lt;FOSGWTool_PATH&gt; --remove_esrs_gateway --scaleio_gateway_ip &lt;scaleio_gateway_ip_address&gt; --scaleio_gateway_user &lt;scaleio_gateway_user&gt; --scaleio_gateway_password &lt;scaleio_gateway_password&gt; --esrs_gateway_ip &lt;esrs_gateway_ip_address&gt;</code></td>
</tr>
<tr>
<td>To reset the PowerFlex Gateway admin password, type the command:</td>
<td><code>&lt;FOSGWTool_PATH&gt; --reset_password</code></td>
</tr>
<tr>
<td>To start SRS logic on the PowerFlex Gateway (alerts will be sent ot the SRS server), type the command:</td>
<td><code>&lt;FOSGWTool_PATH&gt; --start_esrs</code></td>
</tr>
<tr>
<td>Activity</td>
<td>Command</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
</tr>
<tr>
<td>To stop SRS logic from running on the PowerFlex Gateway (alerts will not be sent to the SRS server), type the command:</td>
<td><code>&lt;FOSGWTool_PATH&gt; --stop_esrs</code></td>
</tr>
<tr>
<td>To check the connection to a registered SRS gateway (probing will be done throughout the servers to find one that can be connected), type the command:</td>
<td><code>&lt;FOSGWTool_PATH&gt; --check_esrs_connectivity</code></td>
</tr>
<tr>
<td>To show a list of the available FOSGWTool commands, type the command:</td>
<td><code>&lt;FOSGWTool_PATH&gt; --help</code></td>
</tr>
</tbody>
</table>

**Email notifications**

Service Requests may be created via an email alert notification that is triggered by alerts sent from the PowerFlex system.

PowerFlex can send an email when alerts are triggered from the system. The email is sent from the PowerFlex Gateway via a designated SMTP server to the SRS which then notifies Dell EMC customer support.

**NOTE:** The default setting after an upgrade is SRS. So if you upgrade your system and the notification method property was set to email, you must update the setting after the upgrade.

There are two ways to configure the email notifications feature:

- Configure the gatewayUser.properties file and then restart the gateway service
- Configure and start the gateway service using the REST API

**NOTE:** Verify that a lockbox is configured. If it is not, refer to "Create the lockbox" for steps on how to manually create a lockbox. After creating the lockbox, you must add MDM credentials to the lockbox.

**Configure email alert notifications**

The setting for the notification method can be defined in the gatewayUser.properties file.

**About this task**

The following steps describe the properties that must be defined if the setting `features.notification_method=email`:

**Steps**

1. Use a text editor to open the `gatewayUser.properties` file, located in the following directory on the PowerFlex Gateway server:
   `/opt/emc/ scaleio/gateway/webapps/ROOT/WEB-INF/classes`
2. Set `features.notification_method=email`.
3. Add the following properties under `features.notification_method=email`:
   - `notifications.emailSID.1.type=callHome`. This is the email notification type. This is currently the default and the only option at this stage.
   - `notifications.emailSID.1.SID=<SID email>`. This is the email sender identification. This is the identity shown in the email's "From" field.
   - `notifications.emailSID.1.username=<SID username>`. This is the SMTP email notification username required when email notification uses SMTP server authentication.
   - `notifications.emailSID.1.smtp=<SMTP server name>`. The SMTP server's IP/hostname .
   - `notifications.emailSID.1.authentication=<true or false>`. Enables SMTP authentication mode for email notification
   - `notifications.emailSID.1.port=<port number>`. Add the port number used for email notification. Default is 25.
4. Save and close the file.
5. Restart the PowerFlex Gateway service

**Results**

Email notification is now set up to alert customer support with any issues from the PowerFlex system.
Configure email alert notification using REST API

You can configure email notifications using the REST API.

About this task

The following steps describe the REST API commands to configure for using email notifications.

Steps

1. Select the notification method you wish to use:

   ```bash
   ```

   where:
   - `<JSESSION_ID>` is the JSESSIONID returned in the response of the `j_spring_security_check` command. For more information, see "Working with the (IM) REST API" in the PowerFlex REST API Reference Guide.
   - `<IM_IP_ADDRESS>` is the IP address of the PowerFlex Installer
   - `<NOTIFICATION_METHOD>` is one of the options of the `notificationMethod` detailed above.

2. Add the sender identity and optionally configure SMTP server:

   ```bash
   ```

   where:
   - `<JSESSION_ID>` is the JSESSIONID returned in the response of the `j_spring_security_check` command. For more information, see "Working with the (IM) REST API" in the PowerFlex REST API Reference Guide.
   - `<IM_IP_ADDRESS>` is the IP address of the PowerFlex Installer
   - `<SID_TYPE>` is the type of sender identity. See the options available for `type` above
   - `<SID>` is the email address you which to use for the sender identity
   - `<SMTP_SERVER>` is the SMTP server address, if using SMTP authentication
   - `<USERNAME>` is the username for SMTP authentication
   - `<PASSWORD>` is the password for SMTP authentication
   - `<AUTHENTICATE>` indicates whether you want to use SMTP authentication

3. Start the email feature:

   ```bash
   ```

   where:
   - `<JSESSION_ID>` is the JSESSIONID returned in the response of the `j_spring_security_check` command. For more information, see "Working with the (IM) REST API" in the PowerFlex REST API Reference Guide.
   - `<IM_IP_ADDRESS>` is the IP address of the PowerFlex Installer

**NOTE:** You must stop the email notification feature before changing its configuration. After configuring the email notification feature, start the feature so that it begins sending out email notifications. Any time the feature is stopped, it needs to be started using this command. The email notification feature automatically restarts after a reboot.
4. You can retrieve the list of sender identity configurations:

```
curl -v -k -X POST -H "Content-Type:application/json" -H "Cookie:
JSESSIONID=<JSESSION_ID>" "https://<IM_IP_ADDRESS>/im/types/notifications/email/actions/
getEmailSIDs"
```

where:
- `<JSESSION_ID>` is the JSESSIONID returned in the response of the `j_spring_security_check` command. For more information, see "Working with the (IM) REST API" in the PowerFlex REST API Reference Guide.
- `<IM_IP_ADDRESS>` is the IP address of the PowerFlex Installer

5. You can remove an email sender identity:

```
curl -v -k -X POST -H "Content-Type:application/json" -H "Cookie:
JSESSIONID=<JSESSION_ID>" "https://<IM_IP_ADDRESS>/im/types/notifications/email/actions/
removeEmailSID?type=<SID_TYPE>&sid=<SID>"
```

where:
- `<JSESSION_ID>` is the JSESSIONID returned in the response of the `j_spring_security_check` command. For more information, see "Working with the (IM) REST API" in the PowerFlex REST API Reference Guide.
- `<IM_IP_ADDRESS>` is the IP address of the PowerFlex Installer
- `<SID_TYPE>` is the type of sender identity. See the options available for type above
- `<SID>` is the email address you which to use for the sender identity

6. Restart the PowerFlex Gateway service.

**Configure native users**

Configure native users using the PowerFlex CLI.

**About this task**

Use the following SCLI commands to create and modify native PowerFlex users. To run CLI commands, you must be logged in. Actual command syntax is operating-system dependent. For more information, see the PowerFlex CLI Reference Guide.

SCLI is installed as part of the MDM component and can be found in the following path:
- ESXi: scli
- Linux: scli
- Windows: C:\Program Files\emc\scaleio\MDM\bin
- XenServer: siocli

**Steps**

1. Log in as an admin user to the CLI:

```
scli --login --username <NAME> --password <PASSWORD>
```

where `<PASSWORD>` is the password used for the first login.

2. (Optional) Change the default admin user password:

```
scli --set_password --old_password <PASSWORD> --new_password <NEW_PASSWORD>
```

3. Add users:

```
scli --add_user --username <NAME> --user_role <ROLE>
```

A randomly generated password for the created user is returned.
4. (Optional) Log in with the new user and then change its password:

```bash
scli --login --username <NAME> --password <PASSWORD>
```

```bash
scli --set_password --old_password <OLD_PASSWORD> --new_password <NEW_PASSWORD>
```

This is optional because the PowerFlex GUI, CLI, or REST will enforce a password change if a user logs in with the original password.

## Configure LDAP users

Configure LDAP users if you are using LDAP with PowerFlex.

### About this task

For more information on using LDAP with PowerFlex, see the "Security" section. To run SCLI commands, you must be logged in. Actual command syntax is operating-system dependent. For more information, see the PowerFlex CLI Reference Guide and the User Roles and LDAP Usage Technical Notes for how to set up LDAP in your environment.

### Steps

1. Create Active Directory (AD) groups that correspond to the user roles offered by PowerFlex.
2. Use the CLI to add LDAP service to the MDM:

```bash
```

**NOTE:**
- PowerFlex systems support authentication by up to eight LDAP servers. When multiple LDAP servers are used, add each one separately using this command.
- FQDN is used to identify the LDAP service. By default it is derived from the base-DN, but there are cases when it must be defined explicitly.
- The `search_filter_format` is a search filter for the LDAP query. This is required only if it is different from the default. It must contain [USER] and [GROUP] as place holders for username and group-DN. Default:

  ```bash
  (&(objectClass=user)(sAMAccountName=[USER])(memberOf:1.2.840.113556.1.4.1941:=[GROUP]))
  ```

3. Use the CLI to assign an LDAP group to the user role:

```bash
scli --assign_ldap_groups_to_roles (--ldap_service_id <LDAP_SERVICE_ID> | --ldap_service_name <LDAP_NAME> | --security_role_dn <LDAP_GROUP_DN> | --backend_config_role_dn <LDAP_GROUP_DN> | --frontend_config_role_dn <LDAP_GROUP_DN> | --monitor_role_dn <LDAP_GROUP_DN>)
```

4. Use the CLI to set the system to mixed authentication method, LDAP and native:

```bash
scli --set_user_authentication_method --native_and_ldap_authentication
```

## Configure SNMP

Configure Simple Network Management Protocol (SNMP) for error reporting, if it was not configured during installation.

### Prerequisites

Ensure that a lockbox has already been created and that the MDM credentials have been added to it.

### About this task

Enable the SNMP feature in the gatewayUser.properties file.
Steps

1. Use a text editor to open the `gatewayUser.properties` file, located in the following directory on the PowerFlex Installer/PowerFlex Gateway server:
   - Linux: `/opt/emc/scaleio/gateway/webapps/ROOT/WEB-INF/classes`
   - Windows: `C:\Program Files\EMC\ScaleIO\Gateway\webapps\ROOT\WEB-INF\classes`

2. Locate the parameter `features.enable_snmp` and edit it as follows:
   ```
   features.enable_snmp=true
   ```

3. To add the trap receiver IP address or host name (to configure trap receivers using host names see "Configure Dynamic Host Name resolution for SNMP in PowerFlex"), edit the parameter `snmp.traps_receiver_ip`.
   The SNMP trap receivers’ IP address parameter supports up to two comma-separated or semi-colon-separated host names or IP addresses.

4. You can optionally change the following parameters:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp.sampling_frequency</code></td>
<td>The MDM sampling period. The default is 30.</td>
</tr>
<tr>
<td><code>snmp.resend_frequency</code></td>
<td>The frequency of resending existing traps. The default is 0, which means that traps for active alerts are sent every sampling cycle.</td>
</tr>
</tbody>
</table>

5. Save and close the file.

6. Restart the PowerFlex Gateway service:
   - Linux: Run the command `service scaleio-gateway restart`
   - Windows: Restart the gateway service.

Enable OpenSSL FIPS compliance

Enable the implementation of OpenSSL Federal Information Processing Standards (FIPS) compliance in the MDM for communication between the external components, including the PowerFlex GUI, PowerFlex Gateway, and CLI, to the MDM. It is also enabled for any other usage of the OpenSSL library.

Prerequisites

The MDM must be hosted on Linux with the OpenSSL package installed.

Steps

1. On each host running PowerFlex, open the configuration file of each component with a text editor.
   The configuration file is `/opt/emc/scaleio/<COMPONENT>/cfg/conf.txt`, where `<COMPONENT>` is the lowercase name of the component (e.g. "sds").

2. Add the parameter `security_enable_fips=1` to the file.

3. Save and close the file.

4. Open the SCLI configuration file with a text editor:
   The configuration file is located at: `~/.scli/conf.txt`.

5. Add the parameter `security_enable_fips=1` to the file.

6. Save and close the file.

7. On each host, restart each component's service:
   ```
   service scaleio-<COMPONENT> restart
   ```

8. Verify that OpenSSL FIPS compliance has been enabled by running:
   ```
   cat /proc/sys/crypto/fips_enabled
   ```
   If it has been enabled correctly, the output should be 1. If the output is not 1, enable OpenSSL FIPS at the operating system level.
Create and map volumes

Create volumes from devices added to SDS nodes, and then map the volumes to SDC nodes. You can create and map volumes using various management tools, including the CLI, PowerFlex GUI, vSphere web plug-in, and REST API. Creating and mapping volumes is necessary before applications can access the volumes. In addition, you may create additional volumes and map them as part of the maintenance of the virtualization layer.

Create and map volumes using the CLI

Use the CLI to create a volume and map it to an SDC.

About this task

Use the following SCLI commands to create and map volumes. For more details on SCLI command usage, see the PowerFlex CLI Reference Guide.

Steps

1. Create a volume:
   ```
   scli --add_volume --size_gb <SIZE> --volume_name <VOL_NAME> --protection_domain_name <PD_NAME> --storage_pool_name <SP_NAME>
   ```

2. Map a volume to an SDC:
   ```
   scli --map_volume_to_sdc --volume_name <VOL_NAME> --sdc_ip <SDC_IP>
   ```

Create and map volumes using the PowerFlex GUI

Use the PowerFlex GUI to create a volume and map it to an SDC.

Prerequisites

Ensure that you can authenticate to the PowerFlex GUI with a valid user.

About this task

For more information on creating and mapping volumes using the PowerFlex GUI, see "Volumes" in the "Configuration" chapter.

Steps

1. In the web browser, enter the IP address of the PowerFlex presentation server and log in with credentials:
   - Linux: Run the script `/opt/emc/Scaleio/gui/run.sh`.
   - The PowerFlex GUI is displayed.
2. Create volumes:
   a. In the left pane, click Configuration > Volumes.
   b. In the right pane, click Add.
      - The Add Volume window is displayed.
   c. In the Add Volume dialog box, enter the following details of the volume:
   d. Enter the number of volumes.
      - 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%% and the starting number value is 100, the name of the first volume created will be Vol100, and the second volume will be Vol101, and so on.
   e. Select either Thick (default) or Thin provisioning options.
   f. Enter the volume size in GB (basic allocation granularity is 8 GB) in the Size box.
   g. Select the Storage Pool.
h. Click Add Volume.

i. Verify that the operation completed successfully and click Dismiss.

3. Map volumes to an SDC:
   a. In the left pane, click Configuration > Volumes.
   b. In the right pane, select the volume and click Mapping > Map.
   c. In the Map Volume dialog box, select one or more SDCs to which you want to map the volumes.
   d. Click Map and then click Apply.
   e. Verify that the operation completed successfully and click Dismiss.

Create and map volumes using the vSphere plug-in

Use the vSphere plug-in to create a volume and map it to an SDC.

Steps
1. To open the plug-in, on the vSphere Web Client home tab, click the PowerFlex icon.
2. On the Storage Pools screen, click Actions > Create volumes.
3. In the Create Volume dialog box, enter the volume information.
4. To map the volume to ESXi servers, select Map volume to ESXs.
5. In the Select ESXs area, select the clusters or ESXi servers to which this volume should be mapped.

Enable storage, create and map volumes—XenServer

Enable storage in the XenServer environment.

Prerequisites
You must issue the command line commands from the Master MDM node, either directly, or via SSH. Ensure that you have the authentication credentials. You can also use the PowerFlex GUI.

About this task
The PowerFlex CLI is installed as part of the MDM component and can be found in the following path on XenServer: $ocicli

NOTE: All PowerFlex CLI commands for XenServer begin with $ocicli. When you use CLI commands described in the remainder of the system documentation, replace scli with $ocicli in the documented commands.

After PowerFlex is installed, follow these steps to add and map volumes, and enable their use in HA. This procedure is relevant for XenServer v6.5 and v7.x.

Steps
1. If you did not add storage devices during the deployment procedures, add them now:
   - You must add at least one device to at least 3 SDSs, with a minimum of 100 GB free storage capacity per device.
   - Balance the total device capacity over all SDSs.

   a. Log in to the PowerFlex cluster:

   ```
   $ocicli --login --username <MDM_USERNAME> --password <MDM_PASSWORD>
   ```

   b. Add devices using the following command:

   ```
   $ocicli --add_sds_device --sds_ip <IP> --protection_domain_name <NAME> --storage_pool_name <NAME> --device_path <DEVICE_PATH>
   ```

   Example:

   ```
   $ocicli --add_sds_device --sds_ip 192.168.212.10 --protection_domain_name default --storage_pool_name default --device_path g
   ```
2. Add a volume:

```bash
siocli --add_volume --protection_domain_name <NAME> --storage_pool_name <NAME> --size_gb <SIZE> --volume_name <NAME>
```

Example:

```bash
siocli --add_volume --protection_domain_name default --storage_pool_name default --size_gb 16 --volume_name vol01
```

3. Map a volume to an SDC:

```bash
siocli --map_volume_to_sdc --volume_name <NAME> --sdc_ip <IP>
```

Example:

```bash
siocli --map_volume_to_sdc --volume_name vol01 --sdc_ip 192.168.212.19
```

You can use the PowerFlex GUI or the CLI `--query_all` command to see the installed nodes and storage.

4. Get the host UUID by running the following command:

```bash
xe host-list
```

5. Edit the file `/etc/lvm/lvm.conf` by editing the lines that start with `types`, and adding "scini", 16 inside the square brackets.

Example:

```plaintext
types = ["nvme", 64, "mtip32xx", 64, "scini", 16]
```

6. For XenServer v7.x (only), edit `/etc/lvm/master/lvm.conf`, as follows:
   a. Locate the lines that begin with `types`.
   b. In each of these lines, add this string inside the square brackets: "scini", 16

   ```plaintext
types = ["nvme", 64, "mtip32xx", 64, "scini", 16]
```

7. Use the retrieved host UUID while running the `sr-create` command.

   **NOTE:** PowerFlex provides a unique ID to each volume. It is highly recommended to use the unique ID when running on XenServer. For example, the PowerFlex volume name in the hypervisor is `/dev/disk/by-id/scsi-emc-vol-4a7987a751237ae0-3d467d39000000000`.  

   Example

   ```bash
   xe sr-create host-uuid=09fa5d27-aa08-4c71-86bb-71dc73e9f59f content-type="ScaleIO" name-label="ScaleIO" shared=true device-config:SCSIid=emc-vol-4a7987a751237ae0-3d467d39000000000 type=lvmohba
   ```

   **NOTE:** To add a shared storage repository, the following conditions must be fulfilled:
   - All nodes in the XenServer Center Storage Pool must be installed with SDC.
   - The PowerFlex volume to be used as the shared SR must be mapped to all SDCs in the Storage Pool.

Results

You can now start using your storage.
Mount PowerFlex

The exposed PowerFlex volumes are connected to the servers via the network. To configure mounting options of PowerFlex devices, follow the instructions for your specific Linux-based operating system, below.

About this task

Use persistent device names since the /dev/sciniX names are not guaranteed to persist between reboots. How to use persistent device names is described in full in "Associating volumes with physical disks".

To mount PowerFlex:

Steps

1. Determine the /dev/disk/by-id correlation to /dev/sciniX:

   ```
   ls -l /dev/disk/by-id/ | grep scini
   ```

   Output similar to the following appears:

   ```
   lrwxrwxrwx 1 root root 12 Mar 2 05:35 emc-vol-7ec27ef55b8f2108-85a0f0330000000a -> ../../scinia
   lrwxrwxrwx 1 root root 12 Mar 2 05:35 emc-vol-7ec27ef55b8f2108-85a0f03200000009 -> ../../scinib
   lrwxrwxrwx 1 root root 12 Mar 2 05:35 emc-vol-7ec27ef55b8f2108-85a0f02c00000003 -> ../../scinic
   ```

2. Run the mount command:

   ```
   mount /dev/disk/by-id/<EMC-vol-id>
   ```

   Example:

   ```
   mount /dev/disk/by-id/emc-vol-7ec27ef55b8f2108-85a0f0330000000a /mnt_scinia
   ```

3. To make the mount command persistent, edit the /etc/fstab file according to the instructions for your operating system:

   - RHEL 6.x:
     a. In /etc/fstab, use a text editor to add the PowerFlex mount lines:

        ```
        /dev/disk/by-id/emc-vol-7ec27ef55b8f2108-85a0f0330000000a /mnt_scinia ext4 defaults 0 0
        ```

     b. In /etc/rc.local, use a text editor to add the mount commands:

        ```
        mount /mnt_scinia
        ```

   - RHEL 7.x:
     In /etc/fstab, use a text editor to add _netdev to the PowerFlex mount lines.

     Example:

     ```
     /dev/disk/by-id/emc-vol-7ec27ef55b8f2108-85a0f0330000000a /mnt_scinia ext4 defaults,_netdev 0 0
     ```

     Ensure that you comply with the netdev and syntax rules for your file system, as described in the man page.

   - SLES:
     In /etc/fstab, use a text editor to add nofail to the VxFlex Ready Node mount lines.

     Example:

     ```
     /dev/disk/by-id/emc-vol-7ec27ef55b8f2108-85a0f0330000000a /mnt_scinia ext3 nofail 0 0
     ```

     Ensure that you comply with the nofail and syntax rules for your file system, as described in the man page.
**Associate PowerFlex volumes with physical disks**

You can associate PowerFlex volumes with physical disks.

This following procedures describe how to associate volumes with physical disks.

To get PowerFlex volume information, run the `scli --query_all_volumes` (or `--query_all` or `--query_volume`) command.

Output similar to the following appears:

```
Query-all-volumes returned 10 volumes
Protection Domain 072810d000000000 Name: pd1
Storage Pool ad99eaaab00000000 Name: default
<No volumes defined>  
   Storage Pool ad99eaaab00000000 Name: sp1
  Volume ID: fac22a6300000001 Name: vol0 Size: 152.0 GB (155648 MB) Mapped to 1 SDC Thick-provisioned
  Volume ID: fac22a6400000001 Name: vol1 Size: 406.0 GB (409600 MB) Mapped to 1 SDC Thin-provisioned
  Volume ID: fac22a65000000002 Name: vol2 Size: 80.0 GB (81920 MB) Mapped to 1 SDC Thick-provisioned
  Volume ID: fac22a66000000003 Name: vol3 Size: 392.0 GB (401408 MB) Mapped to 1 SDC Thin-provisioned
  Volume ID: fac22a67000000004 Name: vol4 Size: 56.9 GB (58354 MB) Mapped to 1 SDC Thin-provisioned
  Volume ID: fac22a68000000005 Name: vol5 Size: 112.0 GB (114888 MB) Mapped to 1 SDC Thick-provisioned
  Volume ID: fac22a69000000006 Name: vol6 Size: 56.0 GB (58354 MB) Mapped to 1 SDC Thin-provisioned
  Volume ID: fac22a6a000000007 Name: vol7 Size: 176.0 GB (180224 MB) Mapped to 1 SDC Thin-provisioned
  Volume ID: fac22a6b000000008 Name: vol8 Size: 272.0 GB (278528 MB) Mapped to 1 SDC Thick-provisioned
  Volume ID: fac22a6c000000009 Name: vol9 Size: 360.0 GB (368640 MB) Mapped to 1 SDC Thin-provisioned
```

This output shows the Volume ID and name, and other volume information.

**Volume information - Linux**

You can retrieve volume information from the SDC host.

On the SDC host, run the following command to get the operating system volume information that correlates to the PowerFlex scini device name:

```bash
ls -l /dev/disk/by-id/ | grep scini
```

Output, similar to the following appears:

```
-rw-r---r-- 1 root root 12 Aug 25 19:40 /dev/mapper/vol0-fac22a6300000001 -> ../sciniA  
-rw-r---r-- 1 root root 12 Aug 25 19:40 /dev/mapper/vol1-fac22a6400000001 -> ../sciniB  
```

This output shows the scini volume name and the volume ID.

By matching the volume ID in both outputs, you can match the operating system names, sciniX, with the PowerFlex volume name.

For example:
- `scinia = fac22a63000000000 = vol0`
- `scinic = fac22a64000000001 = vol1`

Alternatively, run the `sg_inq /dev/sciniX` SCSI query command (requires that the sg3_utils be installed on the Linux host). The result of this command includes the EMC volume ID at the bottom of the output, as illustrated:

```
Vendor identification: EMC  
Product identification: Scale10  
Product revision level: 1.3  
Unit serial number: EMC-62c093a52d14aecc-fac22a63000000000
```

**NOTE:**
The product identification remains as ScaleIO (not PowerFlex).

Add PowerFlex devices to Linux LVM physical volumes

Add PowerFlex devices to Linux LVM physical volumes.

Steps

1. In the `/etc/lvm/lvm.conf` file add the following line:

   ```
   types = [ "scini", 16 ]
   ```

2. When PowerFlex scini devices are used, add the following filter:

   ```
   filter = [ "a|/dev/scini*|", "r/.*/" ]
   ```

3. After configured, the `lvmdiskscan` command should yield results similar to the following:

   ```
   /dev/scinia  [  96.00 GiB] LVM physical volume
   /dev/scinib  [ 320.00 GiB] LVM physical volume
   /dev/scinic1 [  56.00 GiB]
   /dev/scinid  [  32.00 GiB]
   1 disk
   1 partition
   2 LVM physical volume whole disks
   0 LVM physical volumes
   ```

4. Continue with normal LVM steps.

Volume information - Windows

You can retrieve volume information from the MDM.

About this task

The `sg_inq.exe` file was added to the MSI installation and can be found at `C:\Program Files\EMC\ScaleIO\SDC\diag\`.

Steps

1. Run the `sg_inq HardiskX` SCSI query command.
   The result of this command includes the EMC volume ID at the bottom of the output.

2. On the MDM, get the PowerFlex volume information:

   ```
   C:\Program Files\emc\scaleio\sdc\bin\drv_cfg --query_vol
   ```

   Output similar to the following is displayed:

   ```
   Retrieved 5 volume(s)
   VOL-ID 6acb5881000000cd MDM-ID 0b246c9a755ca3dd
   VOL-ID 6acb588200000001 MDM-ID 0b246c9a755ca3dd
   VOL-ID 6acb588300000002 MDM-ID 0b246c9a755ca3dd
   VOL-ID 6acb588400000003 MDM-ID 0b246c9a755ca3dd
   VOL-ID 6acb588500000004 MDM-ID 0b246c9a755ca3dd
   VOL-ID 6acb588500000004 MDM-ID 0b246c9a755ca3dd
   ```

   3. From the Windows command prompt, run this command:

      ```
      wmic diskdrive get deviceid,serialnumber | findstr "EMC"
      ```

      Output similar to the following is displayed:

      ```
      \\.\PHYSICALDRIVE13 EMC-0b246c9a755ca3dd=6acb988500000004
      ```

      The first part of the output is the disk name. In our example: PHYSICALDRIVE13

      The second part is the disk serial number. The last set of the second part (after the dash) is the PowerFlex volume ID. In our example: 6acb988500000004
Next steps

You can also get the volume ID from the PowerFlex GUI by displaying the **Identity** pane of the volume's properties sheet from **Frontend > Volumes**

### Volume information - AIX

On AIX servers, associate the PowerFlex volume ID with the AIX physical device.

**About this task**

Retrieve the CuAt volume value:

**Steps**

1. On the SDC host, run the following command to get the operating system volume information:

   ```
   #odmget -q "name like scinid* and attribute=vol_id" CuAt
   ```

   Output, similar to the following, is displayed:

   ```
   CuAt:
   name = "scinid0"
   attribute = "vol_id"
   value = "e120a92d00000000"
   type = "R"
   generic = "P"
   rep = "s"
   nls_index = 22
   
   [root@cnode02 /]#odmget -q "name like scinid* and attribute=vol_id" CuAt
   CuAt:
   name = "scinid2"
   attribute = "vol_id"
   value = "e120a92f00000002"
   type = "R"
   generic = "P"
   rep = "s"
   nls_index = 22
   
   CuAt:
   name = "scinid8"
   attribute = "vol_id"
   value = "e120a93500000008"
   type = "R"
   generic = "P"
   rep = "s"
   nls_index = 22
   
   CuAt:
   name = "scinid0"
   attribute = "vol_id"
   value = "e120a92d00000000"
   type = "R"
   generic = "P"
   rep = "s"
   nls_index = 22
   ```

   You can get information for a single volume, by using this command:

   ```
   #odmget -q "name=scinid0 and attribute=vol_id" CuAt
   ```

   2. Match the value of the **value** field with the PowerFlex volume ID.
Set up replication on peer systems

After deploying SDR packages on both peer systems, create peer connections, volume pairs and Consistency Groups. Then add the volume pairs to the Consistency Groups.

Prerequisites
Ensure that SDR packages are deployed on peer systems. A minimum of two SDRs are required on each system.
Ensure that you have network connectivity between the peer systems.

About this task
At various stages of the procedure, the following query commands can be used to verify replication configuration status:

• `scli --query_all` (to query asset capacity, system information)
• `scli --query_all_sdr`
• `scli --query_all_replication_peer_system`
• `scli --query_all_volumes`
• `scli --query_all_replication_pairs`
• `scli --query_all_replication_consistency_groups`

Most of the actions shown in this workflow can also be performed using the PowerFlex GUI.

NOTE: The CLI commands described in this workflow are typical examples, and for clarity, do not include all possible options. The full syntax and options for each command are described in the PowerFlex CLI Reference Guide.

Steps

1. Open a CLI session with each peer system.
   ```
scli --login --username <NAME> [--password <PASSWORD>] [--ldap_authentication | --native_authentication] [--approve_certificate_once | --approve_certificate] --accept_banner_by_scripts_only
   ```

2. Extract a root certificate from each system so that it can be imported into the other system. Perform this step on both systems.
   ```
scli --extract_root_ca --certificate_file <PATH_AND_CERTIFICATE_FILE_NAME>
   ```
The certificate file name is a user-defined name.

3. Copy each certificate to the other system either by physically loading it on the server, or over the network. For example:
   ```
scp <FILE_PATH_AND_FILE_NAME> <USER>@<PEER_SYSTEM_IP_ADDRESS>/FILE_PATH
   ```

4. On each system, add the certificate that you copied to it in the previous step.
   ```
scli --add_trusted_ca --certificate_file <PATH_AND_CERTIFICATE_FILE_NAME> --comment <COMMENT>
   ```
   NOTE: You can use the following command to check that the certificate was added successfully:
   ```
scli --list_trusted_ca
   ```

From this point and onwards, the procedures described below can also be performed using the PowerFlex GUI.

5. Obtain the MDM Master (data) IP addresses and system ID for both systems.
   a. Use the following command to find the system ID:
      ```
scli --query_all
      ```
      Look for the ID in the System Info section of the output.
b. Use the following command to find the MDM Master IP addresses:
scli --query_cluster

6. Ensure that at least two SDRs have been added to each peer system, and that they have "Connected" status.
   a. Query each system and check the SDRs:
scli --query_all_sdr

b. If SDRs are not present, add them to the system using the command:
scli --add_sdr --sdr_ip <IP_ADDRESS> [--sdr_ip_role <ROLE>] [--protection_domain_id <ID> | --protection_domain_name <NAME>] [--sdr_port <PORT>] [--profile <PROFILE>] [--force_clean [--i_am_sure]]

   Where:
   <ROLE> is the role used by the SDR IP address: application_only, storage_only, external_only, application_and_storage, application_and_external, storage_and_external, or all.
   <PROFILE> is the SDR performance profile: high or compact

c. If you are performing the initial setup of the replication system, you may need to set the replication journal capacity. For more information about calculating the replication journal capacity, refer to "Prepare the CSV file" in the Deploy PowerFlex Guide.
scli --set_replication_journal_capacity --protection_domain_name <NAME> --storage_pool_name <NAME> --replication_journal_capacity_max_ratio <VALUE_IN_PERCENTAGE>

   Where:

7. Create the connection between peer systems. On each system, use the command:
scli --add_replication_peer_system --peer_system_ip <MDM_IP_ADDRESSES> --peer_system_id <SYSTEM_ID> --peer_system_name <SYSTEM_NAME>

   where:
   <MDM_IP_ADDRESSES> are the IP addresses of the Master MDM of the peer system
   <SYSTEM_ID> is the System ID of the peer system
   <SYSTEM_NAME> is the name that will be assigned to the peer system

8. Create volume pairs to be used as source and destination volumes for replication. Each volume must have a matching pair of exactly the same size on the peer system. For example:
scli --add_volume --protection_domain_name <PROTECTION_DOMAIN_NAME> --storage_pool_name <STORAGE_POOL_NAME> --size_gb <SIZE> --volume_name <VOLUME_NAME>

9. Either now, or later, map the intended source side of a volume pair to SDCs. For example:
scli --map_volume_to_sdc --volume_name <NAME> --sdc_name <NAME>

   NOTE: On the destination side of a volume pair, do not map the volume. It will be read-only once replication configuration is complete. Do not create a pair containing a destination volume that is mapped to SDCs with read_write permission.

10. Create one or more Consistency Groups on the system which contains the source volumes. The data will be copied from this side to the peer system (destination).
   NOTE: Each Consistency Group aggregates communication between volume pairs, and parameters assigned to a Consistency Group apply to all the volume pairs in the Consistency Group.
   The system on which the Consistency Group is created is the source side of the volume pairs. It is possible to create Consistency Groups on both systems, therefore creating a scenario where data is being copied in both directions.
scli --add_replication_consistency_group --destination_system_name <DESTINATION_SYSTEM_NAME> --protection_domain_name <PROTECTION_DOMAIN_NAME> --
remote_protection_domain_name <REMOTE_PROTECTION_DOMAIN_NAME> --rpo <SECONDS> --replication_consistency_group_name <REPLICATION_CONSISTENCY_GROUP_NAME>

where:
<DESTINATION_SYSTEM_NAME> is the name of the destination replication system to which data will be copied

<PROTECTION_DOMAIN_NAME> is the name of the Protection Domain in the system that you are currently configuring (source side)

<REMOTE_PROTECTION_DOMAIN_NAME> is the name of the Protection Domain in the destination replication system

<SECONDS> is the Recovery Point Objective (RPO) in seconds. RPO is the point in time to which data can be restored following an event. If you performed a backup at 6 PM, and a server failed at 8 PM, your RPO would be two hours, and any data created during that two-hour time-span would be lost.

<REPLICATION_CONSISTENCY_GROUP_NAME> is the name of this Consistency Group

11. Add replication pairs to the Consistency Group. Repeat this command for each pair.

```bash
scli --add_replication_pair --destination_volume_name <DESTINATION_VOLUME_NAME> --source_volume_name <SOURCE_VOLUME_NAME> --replication_consistency_group_name <REPLICATION_CONSISTENCY_GROUP_NAME> --copy_type <TYPE>
```

where:
<DESTINATION_VOLUME_NAME> is the name of the volume to which data will be copied

<SOURCE_VOLUME_NAME> is the name of the source volume

<REPLICATION_CONSISTENCY_GROUP_NAME> is the name of the Consistency Group to which you are adding the replication pair

<Type> is the type of data copying used. Full = creates a full sequential copy.

**NOTE:** If the source volume is large, initial copying of the data to the destination volume may take some time.

Results

When all required Consistency Groups have been created, and replication pairs have been added to them, replication configuration is complete.

Post-deployment best practice suggestions

After you've deployed the PowerFlex system, refer to the recommended guides for best practice suggestions.

About this task

Recommended guides for best practice suggestions:
- Performance Fine Tuning section for an overview of how to enhance PowerFlex performance
- Security Configuration Guide for an overview of the security settings to ensure PowerFlex security
- Run the system analysis report as described in the Deployment Guide

Link PowerFlex presentation server to the MDM cluster

Initial setup of link between the PowerFlex presentation server and the MDM cluster of a PowerFlex system.

About this task

The following procedure describes how to link the PowerFlex presentation server to your PowerFlex system, in order to facilitate system management using the GUI. This is an initial setup activity performed by the system administrator. If LDAP only authentication method is defined, ensure that there is an LDAP Monitor user.
Steps

1. In a web browser, enter the IP address of the PowerFlex presentation server. The Link to PowerFlex Cluster dialog box is displayed.
2. In the Link to PowerFlex Cluster wizard, on the Connect to System page, enter the IP address of the PowerFlex presentation server and click Next.
3. In the Approve Certificates page, click Agree
4. In the Login page, enter the User Name and Password of an administrator or SuperUser.
5. Select the Click here if the system is configured to use the LDAP authentication method only check box.
6. Enter the Monitor LDAP username and Monitor LDAP password and click Login

Results

After a successful link, future logins to the PowerFlex presentation server will only require a User Name and Password, for any user with any user role.
PowerFlex Performance Fine-Tuning
PowerFlex performance fine-tuning

Tune PowerFlex for best performance

You can improve the PowerFlex system performance in terms of IOPs, latency, and bandwidth, by making environment-specific fine-tunings on the operating system, network, and PowerFlex components.

NOTE: Performance tuning is very case-specific. To prevent undesirable effects, it is highly recommended to thoroughly test all changes. For further assistance, contact https://support.emc.com.

Performance tuning post-installation

This section describes steps to take after completing a successful installation to enhance performance.

Upgrades

For any PowerFlex upgrade from 2.x to 3.x, profile parameters are preserved during the upgrade. If Fine Granularity is configured and the profile was compact, it changes to high performance. For a clean 3.x install, high performance is the default. Users should implement performance tunings by following the guidelines described in this document.

Fine Granularity (FG) layout performance considerations

Fine granularity layout enables 4KB granularity and compression. The benefit of the more efficient FG layout (pools) that allows 4KB granularity plus compression vs. 1MB of Medium Granularity (MG) layout (pools), comes at some performance cost. In most cases (but not all) FG is slower than MG. In FG layout, when compression is enabled, reads are about 20% slower than in cases where compression is disabled. There are exceptions to these rules. For example, small IO Write Response Time is similar in FG and MG. Another exception is using snapshots. In FG, the snapshots have no impact on the performance of applications and workloads running during the snapshot creation. In MG, snapshots might have an impact on performance in some cases.

In cases that are very sensitive to performance and do not require snapshots, MG would be a better choice. It would also be a good option for cases where the data can't be compressed as it may already be compressed or if the data is encrypted by the application.

See "Increase SDS threads" for reference on increasing SDS threads for better performance. For best performance, it is recommended to increase the number of SDS threads from eight to twelve when the CPUs have twelve or more physical cores.

NOTE: Increasing the SDS threads is expected to improve the performance in cases where the CPU is bound, for example: small IOs or FG layout. In cases where the performance is limited by the drive performance (too few drives) or the network (usually large IOs), changing the number of SDS threads does not help.

Fine-Granularity Metadata cache (FG MD_Cache)

FG MD_Cache helps improve the performance of the system when using the FG layout.

When using the FG layout, the FG MD_Cache feature provides the following performance benefits:

- 20-40% increase in read IOPs
- Reductions in response times for reads

FG MD_Cache allocates a small portion of system memory to each SDS in the Protection Domain, for caching the metadata. The following formula below shows the amount of memory needed for FG MD_Cache per SDS:

\[
\text{FGMC RAM in GiB} = (\text{Total drive capacity in TiB}/2) \times 4 \times \text{Compression Factor} \times \% \text{ of Metadata to cache}
\]
It is recommended to allocate 2 for Compression Factor and 2% for Metadata to cache. Use the sizer tool to assess the amount of memory to allocate for metadata to cache. The maximum amount of memory that can be allocated per SDS is 32GiB.

Run the following command to allocate the memory used by FG MD_Cache on each SDS in the Protection Domain.

```
scli --set_default_fgl_metadata_cache_size (--protection_domain_id <ID> | --protection_domain_name <NAME>) --metadata_cache_size_mb <SIZE>
```

Run the following command to enable FG MD_Cache:

```
scli --enable_fgl_metadata_cache (--protection_domain_id <ID> | --protection_domain_name <NAME>)
```

Run the following command to disable FG MD_Cache:

```
scli --disable_fgl_metadata_cache (--protection_domain_id <ID> | --protection_domain_name <NAME>)
```

Tuning considerations

In version 3.x, high_performance profile is the default. Medium Granularity configuration can be changed to compact which would require less memory and CPU resources, however it may have some impact on the performance of the setup. With Fine Granularity configuration, including a mixed Fine and Medium Granularity, only high_performance profile is allowed.

The main difference between the high_performance (default) and compact profiles are the amount of server resources (CPU and memory) that are consumed. A high_performance profile (or configuration) will always consume more resources.

This document will describe commands using the PowerFlex command line interface (scli) to quickly and easily modify the desired performance profile.

Users will achieve optimum performance by always setting the performance profile to high_performance. A complete list of parameters comparing the Default and the high_performance profiles is available in the "Performance Parameters".

PowerFlex system changes

This section describes the various system changes available for enhancing PowerFlex performance.

Using the set_performance_parameters utility for MDM and SDS

New installation procedures have been instituted from v2.x and later that eliminate many of the manual tasks involved with performance tuning PowerFlex.

The following table describes the commands for specific tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>To view current settings</td>
<td>Execute the command:</td>
</tr>
<tr>
<td></td>
<td>scli --query_performance_parameters</td>
</tr>
<tr>
<td>Default is High_performance. If otherwise, execute the</td>
<td>Execute the command:</td>
</tr>
<tr>
<td>command to change to High_performance</td>
<td>scli --set_performance_parameters</td>
</tr>
<tr>
<td></td>
<td>--all_sds --all_sdc --apply_to_mdm --profile</td>
</tr>
<tr>
<td></td>
<td>high_performance</td>
</tr>
</tbody>
</table>
### Task

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>To change the profile back to compact</td>
<td>Execute the command:</td>
</tr>
<tr>
<td></td>
<td><code>scli --set_performance_parameters --all_sds --all_sdc --apply_to_mdm --profile compact</code></td>
</tr>
<tr>
<td>To view full parameter settings for an MDM</td>
<td>Execute the command:</td>
</tr>
<tr>
<td></td>
<td><code>scli --query_performance_parameters --print_all</code></td>
</tr>
<tr>
<td>To view full parameter settings of a specific SDS (this also shows the MDM settings)</td>
<td>Execute the command:</td>
</tr>
<tr>
<td></td>
<td><code>scli --query_performance_parameters --sds_name &lt;NAME&gt; --print_all</code></td>
</tr>
<tr>
<td>To view full parameter settings of a specific SDC (this also shows the MDM settings)</td>
<td>Execute the command:</td>
</tr>
<tr>
<td></td>
<td><code>scli --query_performance_parameters --sdc_name &lt;NAME&gt; --print_all</code></td>
</tr>
</tbody>
</table>

**NOTE:** Refer to the "Performance Parameters" for a list containing all default and performance profile parameters.

### Caching Updates for PowerFlex 2.x/3.x

PowerFlex offers the following types of caching, for the purpose of enhancing system performance:

- RAM Read Cache (using a server’s DRAM memory)
- Read Flash Cache (using SSDs or flash PCI cards)

**NOTE:** SSDs used for caching cannot be used for storage purposes.

The following table summarizes information about the caching modes provided by the system.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
<th>Considerations</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM Read Cache (rmcache)</td>
<td>Read-only caching performed by server RAM.</td>
<td>RAM Read cache, the fastest type of caching, uses RAM that is allocated for caching. Its size is limited to the amount of allocated RAM. RMCache should only be used for HDD pools.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Read Flash Cache (RFCache)</td>
<td>Read-only caching performed by one or more dedicated SSD devices or flash PCI drives in the server.</td>
<td>Read Flash Cache uses the full capacity of SSD or flash PCI devices (up to eight) to provide a larger footprint of read-only LRU (least recently used) based-caching resources for the SDS. This type of caching reacts quickly to workload changes to speed up HDD Read performance. Several SSD devices can be allocated to a shared cache pool, and therefore the cache size is limited in size only to the amount of SSDs allocated for this purpose.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Mode</td>
<td>Description</td>
<td>Considerations</td>
<td>Default Setting</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> The RFCache driver must be installed during deployment. Caching devices can be defined either during the installation process, or after deployment.</td>
<td></td>
</tr>
</tbody>
</table>

### Read RAM Cache settings for SDS

From version 2.x Read RAM Cache is disabled by default on the Storage Pool. Recommendation: Keep it disabled for SSD/Flash pools. For HDD pools, Read RAM Cache can help increase performance. If the node is storage only (in other words; is the node is only used for PowerFlex), then the recommendation is to turn on Read RAM Cache for HDD pools and use as much of the server DRAM as possible.

In a converged configuration (where PowerFlex is sharing the server with other applications), depending on the available DRAM resources, it may also help to turn on Read RAM Cache for HDD pools and increase the cache size from the default.

If users wish to enable/disable Read RAM Cache, perform either of the following steps. Read RAM Cache may be enabled/disabled on the Protection Domain, or for each SDS in the cluster.

#### Task | Command
--- | ---
To enable Read RAM cache | Run one of the following commands:
- `scli --set_rmcache_usage --protection_domain_name <domain NAME> --storage_pool_name <pool NAME> --use_rmcache [--dont_use_rmcache]`
- `scli --enable_sds_rmcache [--disable_sds_rmcache] --sds_name <NAME>`

**NOTE:** Using this command would be required for every SDS in the cluster.

To increase the amount of Read RAM cache | Run the following command:
- `scli --set_sds_rmcache_size ((--sds_id <ID> | --sds_name <NAME> | --sds_ip <IP> [--sds_port <PORT>]) | (--protection_domain_id <ID> | --protection_domain_name <NAME>)) --rmcache_size_mb <SIZE> [--i_am_sure]`

Where `--rmcache_size_mb` is the size of rmcache in MB, and the range is between 128MB-300GB.

It is important to ensure that Read RAM cache is enabled at all levels (PD, SP, and SDS). When rmcache is properly enabled, query output will look like this:

```
Read Flash Cache settings for SDS

Read Flash Cache is available from version 2.x and later. This feature is a Read Cache used to increase read performance and buffers writes to increase the performance of Read-after-Write I/Os. It allows users to create and configure an "RFcache" device for any SSD or Flash card. PowerFlex will cache user data depending on the mode selected. This feature can greatly improve performance for specific workloads. The RFcache device is also referred to as an accelerated device.

To create an RFcache device and configure it, use the following steps:
1. Create an RFcache device (Recommendation: create 1 device per SDS).

```bash
scli --add_sds_rfcache_device --sds_name <NAME> --rfcache_device_path <device_path> --rfcache_device_name <RFcache device NAME>
```

2. Set the RFcache parameters (Recommendation: these parameters have a great impact on performance, therefore use the defaults).

```bash
scli --set_rfcache_parameters --protection_domain_name <domain NAME> --rfcache_pass_through_mode pass_through_write_miss
```

**NOTE:** The default settings are; Passthrough mode = Write_Miss, Page Size 64 KB, Max IO size 128 KB.

3. Enable acceleration of a Storage Pool—accelerate all SDS devices that are in the pool:

```bash
scli --set_rfcache_usage --protection_domain_name <domain NAME> --storage_pool_name <pool NAME> --use_rfcache
```

For Read Flash Cache, the available modes are as follows:
- pass_through_none
- pass_through_read
- pass_through_write
- pass_through_read_and_write
- pass_through_write_miss

The default caching mode is "write-miss". In this mode, it is essentially a write-through option where only reads and updates are cached. This mode buffers writes to the data that was already in cache.


### Jumbo Frames and the potential impact on performance

When enabling jumbo frames, one can expect approximately 10% improvement in performance if all network components fully support jumbo frames. If some network components do not fully support jumbo frames, it is recommended to use the default setting; mtu 1,500.

Prior to activating mtu settings on the logical level, set Jumbo frames = mtu 9000 on the physical switch ports that are connected to the server. Failure to do so may lead to network "disconnects" and packet drops.

Refer to your relevant vendor guidelines on how to configure jumbo frame support.

### Jumbo Frame configuration for Linux

Configure Jumbo Frames for NIC cards in the Linux-based PowerFlex servers.

**About this task**

Perform the following steps, for all the NIC cards in the PowerFlex system:

**Steps**

1. Run the `ifconfig` command to get the NIC information.
2. Depending on the OS, run the command:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL/CentOS</td>
<td>Edit /etc/sysconfig/network-scripts/ifcfg-&lt;NIC_NAME&gt;</td>
</tr>
<tr>
<td>SLES</td>
<td>Edit /etc/sysconfig/network/ifcfg-&lt;NIC_NAME&gt;</td>
</tr>
</tbody>
</table>

3. Add parameter `mtu=9000` to the file.
4. To apply the changes, type: `service network restart`
5. Execute `ifconfig` again to verify that the settings have been changed.
6. To test the command, type: `ping -M do -s 8972<DESTINATION_IP_ADDRESS>`

Output should look similar to this:
Jumbo Frame configuration for Windows

Configure Jumbo Frames for NIC cards in the Windows-based PowerFlex servers.

About this task

Perform the following steps, for all the NIC cards in the PowerFlex system:

Steps

1. Change the Maximum Transmission Unit (mtu) setting to 9,000, or the highest value that is supported by the switch and the connected nodes.

2. Determine the appropriate NIC name by typing the command:

   `netsh interface ipv4 show interface`

   Output similar to the following appears:

   ![Figure 2. Show interface output](image)

   In this example, index 17 is the appropriate network.

3. Type the command:

   `netsh interface ipv4 set subinterface <network_ID> mtu=9000 store=persistent`

   where, `network_ID` is the ID from the output in the previous step; in this case, the ID is 17.

4. In the Advanced tab of the Adapter Properties dialog for your vendor and driver, change the value of Jumbo Packet to 9000, as illustrated in the following figure:
5. Click **OK**. The network connection may disconnect briefly during this phase.

6. Verify that the configuration is working, by typing the command:

   ```bash
   ping -f -l 8972 <Destination_IP_Address>
   ```

   Output similar to the following should be displayed:

   ![Ping output](image)

   **NOTE:** Ensure that the switch supports 10 GB Ethernet.

---

### Jumbo Frame configuration for ESXi

Configure Jumbo Frames for NIC cards in the ESXi-based PowerFlex servers.

**About this task**

Perform the following steps, for all the NIC cards in the PowerFlex system:

**Steps**

Change the **Maximum Transmission Unit (mtu)** setting to **9,000** on the vSwitches and on the SVM (be sure to make the change in `/etc/sysconfig/network/ifcfg-ethX`):
a. Type the command:

```
esxcfg-vswitch -m 9000 <vSwitch>
```

b. Create VMKernel with jumbo frames support by typing the following commands:

i.  
```
esxcfg-vswitch -d
```

ii.  
```
esxcfg-vswitch -A vmkernel# vSwitch#
```

iii.  
```
esxcfg-vmknic -a -i <ip address> -n <netmask> -m 9000 <portgroup name>
```

**NOTE:** Changing Jumbo Frames on a vSwitch will not change the VMKernel MTU size. For older vCenter versions, check to ensure the MTU setting has been changed. If not successful, users may need to delete and recreate the VMKernel. For newer vCenter versions, modify the MTU of VMKernel by using the vsphere web client.

## Jumbo Frame configuration for Storage Virtual Machine

Configure Jumbo Frames for NIC cards in the Storage Virtual Machine (SVM)-based PowerFlex servers.

### About this task

Perform the following steps, for all the NIC cards in the PowerFlex system:

### Steps

1. Edit the `/etc/sysconfig/network/ifcfg-<NIC_NAME>`.
2. Add parameter `mtu=9000` to the file.
3. To apply the changes type:

```
service network restart
```

4. Execute `ifconfig` command again to confirm that the settings have been changed.
5. To test the command type:

```
ping -M do -s 8972 <DESTINATION_IP_ADDRESS>
```

Output should look similar to the following:
Increase SDS threads

The default number of SDS threads under a high performance profile is eight. For best performance, it is recommended to increase the number of SDS threads from eight to twelve when the CPUs have twelve or more physical cores.

Run the following command to view the current setting: `scli --query_performance_parameters --all_sds --print_all`

The parameter `Active profile: high_performance` shows the current SDS threads being used:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Current Value</th>
<th>Profile Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDS_NUMBER_OS_THREADS</td>
<td>8</td>
<td>8</td>
</tr>
</tbody>
</table>

This is logged per SDS and should to be changed across SDS nodes in the cluster.

Run the following command to change the SDS threads from eight to twelve: `scli --set_performance_parameters --all_sds --tech --sds_number_os_threads_12`

**NOTE:** Increasing the SDS threads is expected to improve the performance in cases where the CPU is bound, for example: small I/Os or FG layout. In cases where the performance is limited by the drive performance (too few drives) or the network (usually large I/Os), changing the number of SDS threads does not help.

Optimize Linux

When using the SSD devices, it is recommended that the I/O scheduler of the devices be modified.

Type the following on each server, for each SDS device:

```bash
echo noop > /sys/block/<device_name>/queue/scheduler
```

For example:

```bash
echo noop > /sys/block/sdb/queue/scheduler
```

When CPUs have more than twelve physical cores and more performance is required from the node. For example: when CloudLink is being used for SW encryption or when Fine Granularity is being used and more performance per node is required, type the following:

```bash
scli --set_performance_parameters --all_sds --tech --sds_number_os_threads_12
```
NOTE: To make these changes persistent after reboot, either create a script that runs on boot, or change the kernel default scheduler via kernel command line.

Change the GRUB template for Skylake CPUs

For Skylake GPUs on PowerEdge 14G models running RHEL 7.2 or later, change the GRUB template on every node to ensure that the CPUs maintain good performance in terms of latency.

Steps
1. Open the GRUB template for editing:

   ```bash
   vim /etc/default/grub
   ```

2. Find the `GRUB_CMDLINE_LINUX` configuration option and append the following to the line:

   ```bash
   intel_idle.max_cstate=1 intel_pstate=disable
   ```

   Example:

   ```bash
   GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb intel_idle.max_cstate=1 intel_pstate=disable quiet"
   ```

3. Compile the new GRUB:

   ```bash
   grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
   ```

4. Stop and then disable tuned:

   ```bash
   systemctl stop tuned
   systemctl disable tuned
   ```

5. Run reboot to reboot the node.

6. Ping the node to ensure that the GRUB change was implemented.
   The ping time should be in the 0.03 ms range.

7. Repeat the procedure on every 14G node with a Skylake CPU.

Optimize ESXi

To improve I/O concurrency, users may increase the per device queue length value on a per data store basis. Per device queue length is referred to as “No of outstanding IOs with competing worlds” in the display output.

Use the following command to increase the queue length:

```bash
esxcli storage core device set -d <DEVICE_ID> -O <Outstanding IOs>
```

where, `<Outstanding IOs>` can be a number ranging from 32-16384 (the default=32). We recommend increasing queue length to 256.

Example:

```bash
esxcli storage core device set -d eui.16bb852c56d3b93e3888003b00000000 -O 256
```

Optimize the SVM

Optimize the SVM

Steps
1. Configure the CPU and memory assigned to the Storage Virtual Machine (SVM).
• In general, 8 vCPUs are sufficient, but this may vary in your environment. It is recommended to increase vCPUs to 12 if CloudLink is installed. Note this is only relevant if the CPU has 12 or more physical cores.
• Cores per socket should be set to maximum so all vCPU will be allocated to a single virtual socket.

2. From the Resources tab of the Virtual Machine Properties window, select Reserve all guest memory (All locked).

The Virtual Machine Properties window is displayed:

![Virtual Machine Properties](image)

**Optimizing VM guests**

Select the VM guest to optimize.

**I/O scheduler**

When using SSD devices, it is recommended that you modify the devices' I/O scheduler.

Type the following on each server, for each SDS device:

```
echo noop > /sys/block/<device_name>/queue/scheduler
```

Example:

```
echo noop > /sys/block/sdb/queue/scheduler
```

**NOTE:** For most Linux distributions, NOOP is not the default. Different Linux versions have different default values. For RHEL7 and SLES 11/12, the default value is deadline, but for older versions, the default is CFQ.
**Paravirtual SCSI controller**

The Paravirtual SCSI (PVSCSI) controller should be used on guest VMs for high performance. It is important that users choose the correct PVSCSI controller, because choosing the wrong controller can adversely affect performance.

Current PVSCSI queue depth default values are 64 for the device and 254 for the adapter. Users can increase the PVSCSI queue depth to 256 for the device and 1024 for the adapter inside a Windows virtual machine.

Windows virtual machine:

1. From the command line run:
   ```
   REG ADD HKLM\SYSTEM\CurrentControlSet\services\pvscsi\Parameters\Device /v DriverParameter /t REG_SZ /d "RequestRingPages=32,MaxQueueDepth=254"
   ```
2. Reboot the virtual machine.
3. Verify the successful creation of a registry entry:
   a. Open the registry editor by running the REGEDIT command from the command line.
   b. Browse to HKLM\SYSTEM\CurrentControlSet\services\pvscsi\Parameters\Device.
   c. Verify that the DriverParameter key exists with a value of RequestRingPages=32, MaxQueueDepth=254.

Linux guests:

1. Edit the `vmw_pvscsi.conf` file:
   ```
   echo "options vmw_pvscsi cmd_per_lun=254 ring_pages=32" > /etc/modprobe.d/vmw_pvscsi.conf
   ```
2. Re-run `vmware-config-tools.pl`:
   ```
   vmware-config-tools.pl
   ```

You can add up to 4 PVSCSI controllers per guest. Allocating different PowerFlex volumes to different PVSCSI controllers can help realize the maximum potential of guest performance.

It is strongly recommended that you review this VMware Knowledge Base article (article 2053145) so that you can make educated decisions regarding PVSCSI values.

**PowerFlex Performance Parameters**

The following table describes all values for the v3.x “high_performance” and “compact” profiles and is applicable to installations on all of the platforms discussed in this document.

<table>
<thead>
<tr>
<th>Component</th>
<th>New Name (CLI)</th>
<th>Min Value</th>
<th>Max Value</th>
<th>Compact</th>
<th>High Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDM</td>
<td>mdm_net_alloc_rvc_buffer_wait_ms</td>
<td>100</td>
<td>100,000</td>
<td>500</td>
<td>500</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_net_break_do_io_loop</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_number_sdc_receive_umt</td>
<td>1</td>
<td>100</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_number_sds_receive_umt</td>
<td>1</td>
<td>100</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_number_sds_send_umt</td>
<td>1</td>
<td>100</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_number_sds_keepalive_receive_umt</td>
<td>1</td>
<td>100</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_sds_capacity_counters_update_interval</td>
<td>1</td>
<td>120</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_sds_capacity_counters_polling_interval</td>
<td>1</td>
<td>120</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_sds_volume_size_polling_interval</td>
<td>1</td>
<td>120</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_sds_volume_size_polling_retry_interval</td>
<td>1</td>
<td>120</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_number_sds_tasks_umt</td>
<td>1</td>
<td>2,048</td>
<td>1,024</td>
<td>1,024</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_initial_sds_snapshot_capacity</td>
<td>1</td>
<td>10^1024</td>
<td>1,024</td>
<td>1024</td>
</tr>
<tr>
<td>Component</td>
<td>New Name (CLI)</td>
<td>Min Value</td>
<td>Max Value</td>
<td>Compact</td>
<td>High Performance</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
<td>-----------</td>
<td>-----------</td>
<td>---------</td>
<td>------------------</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_sds_snapshot_capacity_chunk_size</td>
<td>1</td>
<td>50*1024</td>
<td>5*1024</td>
<td>5*1024</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_sds_snapshot_used_capacity_threshold</td>
<td>1</td>
<td>99</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_sds_snapshot_free_capacity_threshold</td>
<td>101</td>
<td>1000</td>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>SDS</td>
<td>mdm_number_sockets_per_sds_ip</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>SDS</td>
<td>mdm_sds_keepalive_time</td>
<td>2000</td>
<td>3600000</td>
<td>5000</td>
<td>5000</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_number_network_umn</td>
<td>2</td>
<td>16</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_tcp_send_buffer_size</td>
<td>4</td>
<td>128*1024</td>
<td>0 (dynamic)</td>
<td>0</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_tcp_receive_buffer_size</td>
<td>4</td>
<td>128*1024</td>
<td>0 (dynamic)</td>
<td>0</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_max_number_asyncronous_io_per_device</td>
<td>1</td>
<td>2000</td>
<td>8</td>
<td>60</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_number_sdc_io_umn</td>
<td>100</td>
<td>500</td>
<td>100</td>
<td>500</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_number_sds_io_umn</td>
<td>100</td>
<td>500</td>
<td>100</td>
<td>500</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_number_sds_copy_io_umn</td>
<td>100</td>
<td>164</td>
<td>164</td>
<td>164</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_number_copy_umn</td>
<td>100</td>
<td>164</td>
<td>164</td>
<td>164</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_number_os_threads</td>
<td>1</td>
<td>32</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_number_sockets_per_sds_ip</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_net_break_do_io_loop</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_number_io_buffers</td>
<td>1</td>
<td>10</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_net_alloc_rcv_buffer_wait_ms</td>
<td>100</td>
<td>10000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_tcp_send_buffer_size</td>
<td>4</td>
<td>128*1024</td>
<td>512</td>
<td>4*1024</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_tcp_receive_buffer_size</td>
<td>4</td>
<td>128*1024</td>
<td>512</td>
<td>4*1024</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_number_sockets_per_sds_ip</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_number_network_os_threads</td>
<td>1</td>
<td>10</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_max_inflight_requests</td>
<td>1</td>
<td>10000</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_max_in_flight_data</td>
<td>1</td>
<td>10000</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_number_io_retries</td>
<td>1</td>
<td>100</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_volume_statistics_interval</td>
<td>1000</td>
<td>600000</td>
<td>5000</td>
<td>5000</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_optimize_zero_buffers</td>
<td>0 (FALSE)</td>
<td>1 (TRUE)</td>
<td>0 (FALSE)</td>
<td>0 (FALSE)</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_number_unmap_blocks</td>
<td>1</td>
<td>200</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_number_non_io_os_threads</td>
<td>1</td>
<td>16</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

**RAID controller virtual disk settings**

RAID controller virtual disk settings and optimal policies regarding each type of disk.

For SSDs in use by a RAID controller

1. Create the Virtual Disk as a RAID0 device.
2. Disable the PD Cache for the HDD
3. Set the VD Caching attributes as NRWTD (No Read Ahead, Write Through, Direct).

**NOTE:** For VxFlex Ready Node based install, refer to the VxFlex Ready Node documentation.
Apply Performance Profiles to system components

You can use the PowerFlex GUI to apply performance profiles to system components.

About this task

The default configures a predefined set of parameters for very high performance use cases. When a container is provided in the command (System/Protection Domain/Fault Set), all the objects currently in the container are configured.

**NOTE:** For a complete list of parameters controlled by the profiles, refer to "PowerFlex Performance Fine-Tuning ".

The profiles are applied separately to:

- SDSs
- SDCs

**NOTE:** After changing the performance profile of an SDS (on an SVM), you must perform manual memory allocation on the SVM, as described in the *PowerFlex Deployment Guide*.

To apply a profile to system components, perform the following steps:

Steps

1. Depending on the system component that you want to configure, from the PowerFlex GUI in the left pane, click either **Configuration > SDSs** or **Configuration > SDCs**.
2. In the right pane, select the relevant object and click **Modify > Modify Performance Profile**.
3. In the **SDS or SDC <object name> Modify Performance Profile** dialog box, select a profile and click **Apply**.
4. Verify that the operation completed successfully and click **Dismiss**.

Results

The performance profile is set for the object.
This section contains tasks when setting up a PowerFlex system.

## Protection Domains

Add, modify, activate/inactivate or remove a Protection Domain in the PowerFlex environment.

### About this task

Inactivating a Protection Domain does not remove it from the system, but it makes all data stored in that Protection Domain inaccessible to the system. The inactivation feature is a much more effective way to shut down nodes, and is preferable to shutting them down manually.

### Add Protection Domains

Add a Protection Domain to a PowerFlex system.

#### Steps

1. From the PowerFlex GUI, in the left pane, click **Configuration > Protection Domains**.
2. In the right pane, click **Add**.
3. In the **Add Protection Domain** dialog box, enter the name of the Protection Domain and then click **Add Protection Domain**.
4. Verify that the operation completed successfully and click **Dismiss**.

#### Results

SDSs, Fault Sets, Storage Pools, and Acceleration Pools can now be added to the Protection Domain. Replication can also be set up to make sure the data is protected and saved to a remote cluster.

## Configure network throttling

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

### About this task

Network throttling is configured per 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 customer support before you change this configuration.

#### Steps

1. From the PowerFlex GUI, in the left pane, click **Configuration > Protection Domains**.
2. In the right pane, select the relevant Protection Domain check box, and click **Modify > Network Throttling**.
3. In the **Set Network Throttling for PD <PD name>** dialog box, enter the bandwidth for the following settings:
   - Rebalance throughput limit per SDS
   - Rebuild throughput limit per SDS
   - vTree migration throughput limit per SDS
   - vTree migration throughput limit per SDS
4. Click **Apply**.
5. Verify that the operation completed successfully and click **Dismiss**.

**Results**

Network throttling for the selected Protection Domain is set.

### Activate a Protection Domain

Activate an inactivated Protection Domain.

**Steps**

1. From the PowerFlex GUI, in the left pane, click **Configuration** > **Protection Domains**.
2. In the right pane, select the relevant Protection Domain check box, and click **More** > **Activate**.
3. In the **Activate Protection Domain <PD name>** 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 completed successfully and click **Dismiss**.

**Results**

The Protection Domain is activated.

### Inactivate a Protection Domain

Inactivate a Protection Domain.

**About this task**

1. **NOTE**: If the Protection Domain is inactive, the data remains on the SDSs. It is preferable to remove a Protection Domain if it is not being used.

When the inactivation feature is in effect, 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.
- Quiesce (temporarily disable) application I/O and disable access to volumes.
- Move the DRL mode of all SDSs to harden, in preparation for restarting the server.
- Reload of all SDSs before re-enabling data access.

**Steps**

1. From the PowerFlex GUI, in the left pane, click **Configuration** > **Protection Domains**.
2. In the right pane, select the relevant Protection Domain check box, and click **More** > **Inactivate**. Confirm by clicking **Inactivate**.
3. Verify that the operation completed successfully and click **Dismiss**.

**Results**

The Protection Domain is inactivated.

### Set RFcache policy

Enable or disable RFcache at Protection Domain level.

**About this task**

- Once this is enabled at Protection Domain or Storage Pool level, set the RFcache policy at SDS level.
- Once RFcache is enabled at both Protection Domain/Storage Pool and SDS levels, add RFcache devices to the SDS in order to commence caching.
Steps
1. From the PowerFlex GUI, in the left pane, click **Configuration** > **Protection Domains**.
2. In the right pane, select the relevant Protection Domain check box, and click **More** > **RFcache**.
3. In the **Set Read Flash Cache for PD <PD name>** dialog box, click **Enable** for RFcache and select the relevant settings for:
   - Page Size
   - Max IO Size
   - Pass Through Mode
4. Click **Apply**.
5. Verify that the operation completed successfully and click **Dismiss**.

Results
The RFcache is enabled for the Protection Domain.

**Remove a Protection Domain**
Remove a Protection Domain from the PowerFlex system.

Prerequisites
Ensure that all child nodes have been removed from the Protection Domain before removing it from the system.

Steps
1. From the PowerFlex GUI, in the left pane, click **Configuration** > **Protection Domains**.
   
   **NOTE:** Verify that all child nodes have been removed from the Protection Domain.
2. In the right pane, select the relevant Protection Domain check box, and click **More** > **Remove**.
3. In the **Remove Protection Domain <PD name>**, click **Remove**.
4. Verify that the operation completed successfully and click **Dismiss**.

Results
The Protection Domain is removed.

**Fault Sets**
Fault Sets provide additional safeguards for protecting data against hardware failure. Fault Sets are subsets of a given Protection Domain.

**Add Fault Sets**
Add a Fault Set to a Protection Domain to prevent data loss in case of a single failure.

About this task

**NOTE:** When defining Fault Sets, follow the guidelines described in "Fault Sets" in the *Getting to Know PowerFlex Guide*. Failure to do so may prevent creation of volumes.

Steps
1. From the PowerFlex GUI, in the left pane, click **Configuration** > **Fault Sets**.
2. In the right pane, click **Add**.
3. In the **Add Fault Set** dialog box, enter a name and select the Protection Domain, and click **Apply**.
   
The new Fault Set is a part of the Protection Domain.
Enter and exit Fault Set into Maintenance Mode

Place a Fault Set into Maintenance Mode, in order to perform non-disruptive maintenance on the group of SDSs.

About this task

This topic explains how to put a Fault Set into Maintenance Mode, and how to exit Maintenance Mode when you are finished.

There are two types of Maintenance Modes:

- **Instant**: Instant Maintenance Mode (IMM) is where 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 only the new writes to the node which was under maintenance.
- **Protected**: Protected Maintenance Mode (PMM) is an extra insurance where the entire data of the SDS is backed up before it actually goes into maintenance mode. Two complete copies of the SDS are available at all times as any node failure during maintenance leaves no room for discrepancy between the copies. This requires more storage capacity from the node.

Steps

1. From the PowerFlex GUI, in the left pane, click **Configuration > Fault Sets**.
2. In the right pane, select the relevant Fault Set check box and click **More > Enter Maintenance Mode**.
3. In the **Enter Fault Set <Fault Set name> to Maintenance Mode** dialog box, select one of the following options:
   - **Instant**
   - **Protected**
4. Click **Enter Maintenance Mode**.
5. Verify that the operation completed successfully and click **Dismiss**.
6. From the top right, click the **Running Jobs** icon and check the progress of the PMM.

Results

After the operation has been completed successfully, the Fault Set returns to normal operation, and data deltas collected during the maintenance period are copied back to the Fault Set.

SDS

SDSs and their devices can be added to a system one by one, or in bulk operations, using the **Add SDS** command. Up to eight IP addresses can be associated to each SDS. By default, performance tests are performed on the added devices, and the results are saved in the system.

Add SDSs

Add SDSs to the PowerFlex system.

Prerequisites

Ensure that at least one suitable Storage Pool is defined in the required Protection Domain. If you want to add Acceleration devices now, ensure that at least one Acceleration Pool is defined as well.

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. Ensure that the Storage Pool to which you are adding devices is configured to receive that media type.

About this task

Device data is erased when devices are added to an SDS. When adding a device to an SDS, PowerFlex will check that the device is clear before adding it. An error is returned, per device, if it is found not to be clear. 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 will be lost. For more information, see "Configuring direct attached storage" in the **Getting to Know PowerFlex Guide**.

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 name will remain constant, even if the path changes. SDS and device names must meet the following requirements:

- Contains less than 32 characters
Steps

1. From the PowerFlex GUI, in the left pane, click **Configuration** > **SDSs**.
2. In the right pane, click **Add**.
3. Configure the following settings:
   - Enter SDS name
   - Select the Protection Domain
   - Select the 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):
   - Select **Use Read RAM Cache** and enter the size in MB.
   - Click one of the options for **Performance Profile: Compact or High**. For information on Performance Profile, see "Tuning considerations".
   - Select if to **Force Clean SDS**.
6. Click **Add SDS**.

Results

An SDS is added to the system.

**Set RFcache policy at SDS level**

This topic describes how to enable RFcache policy for an SDS.

About this task

- To enable caching, ensure that the policy is also enabled at Protection Domain level.
- Once RFcache is enabled at both Protection Domain and SDS levels, add RFcache devices to the dedicated Acceleration Pool in order to commence caching.

To set RFcache policy on an SDS, perform these steps:

Steps

1. From the PowerFlex GUI, in the left pane, click **Configuration** > **SDSs**.
2. In the right pane, select the relevant SDS check box and click **Modify** > **Cache Settings**.
3. In the **SDS <SDS name> Cache Settings** dialog box, click the **Enable RFcache** check box.
4. Click **Apply**.
5. Verify that the operation completed successfully and click **Dismiss**.

Results

RFcache policy is enabled for the SDS.
Configure RMcache

The RMcache feature improves your system’s application performance for storage-related activities. By default, caching is disabled.

About this task

To use RMcache, you need to configure settings at two levels:

- **Storage Pool**—controls RMcache for all the SDSs in the selected Storage Pool. Caching can be enabled or disabled, and either Cached (default) or Passthrough Write Handling modes can be selected. When RMcache is enabled in a Storage Pool, the feature is enabled at Storage Pool level. However, caching must also be set to Enabled in each SDS in the Storage Pool. Caching will only begin once storage devices have been added to the SDSs. It is possible to enable RAM caching for a Storage Pool and then disable caching on one or more SDSs individually.
- **Per SDS**—controls RMcache for one or more SDSs. Caching can be enabled or disabled for the specified SDS, and the capacity allocated for caching on an SDS can be specified. Caching will only begin after one or more storage devices are added to the SDSs. Ensure that the feature is also enabled at Storage Pool level.

**NOTE:** By default, RMcache is disabled in all volumes. You can enable them from the Frontend > Volumes view.

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

To configure caching, perform these steps:

**Steps**

1. From the PowerFlex GUI, in the left pane, click **Configuration > Storage Pools**.
2. In the right pane, select the relevant Storage Pool check box, and click **Settings > Cache**.
3. In the **Storage Pool <SP name> Cache Settings** dialog box, select the **Use RMcache** check box.
4. Click **Apply**.

**Results**

RMcache is set for the Storage Pool

Remove SDSs

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

About this task

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

The system has job queues for operations that take a long time to execute. You can view the jobs in the Planned Rebuilds and Planned Rebalancing table views. 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** command from the Command menu.

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

**Steps**

1. From the PowerFlex GUI, in the left pane, click **Configuration > SDSs**.
2. In the right pane, select the relevant SDS check box and click **More > Remove**.
3. In the **Remove SDS <name>** dialog box, click **Remove**.
4. In the confirmation message dialog box, click **Dismiss**.

**Results**

The SDS has been removed.
Enter and exit SDS Maintenance Mode

Place an SDS into Maintenance Mode, in order to perform non-disruptive maintenance on the SDS.

About this task

This topic explains how to put an SDS into Maintenance Mode, in order to perform non-disruptive maintenance on the SDS, and how to cancel Maintenance Mode when you are finished.

There are two types of Maintenance Modes:

- **Instant** - Instant Maintenance Mode (IMM) is where 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 only the new writes to the node which was under maintenance.
- **Protected** - Protected Maintenance Mode (PMM) is an extra insurance where the entire data of the SDS is backed up before the SDS actually goes into maintenance mode. Two complete copies of the SDS are available at all times as any node failure during maintenance leaves no room for discrepancy between the copies. This requires more storage capacity from the node.

Steps

1. From the PowerFlex GUI, in the left pane, click **Configuration > SDSs**.
2. In the right pane, select the relevant SDS check box, and click **More > Enter Maintenance Mode**.
3. In the **Enter SDS <SDS name> into Maintenance Mode** dialog box, select one of the following options:
   - **Instant**
   - **Protected**
4. Click **Enter Maintenance Mode**.
5. Verify that the operation completed successfully and click **Dismiss**.
6. From the top right, click the **Running Jobs** icon and check the progress of PMM.

Results

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

Add storage devices

Storage devices can be added to a system one by one, or in bulk operations, using the **Add Device** command. By default, performance tests are performed on the added devices, and the results are saved in the system.

Prerequisites

Ensure that at least one suitable Storage Pool is defined in the required Protection Domain.

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

About this task

Device data is erased when devices are added to an SDS. When adding a device to an SDS, PowerFlex will check that the device is clear before adding it. An error will be returned, per device, if it is found not to be clear. 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 will be lost. For more information, see "Configuring direct attached storage" in the **Getting to Know PowerFlex Guide**.

You can assign a name to devices. This can be particularly helpful for identifying SDS devices in the future, because the name will remain 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

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

1. From the PowerFlex GUI, in the left pane, click Configuration > SDSs.
2. In the right pane, click Add Device.
3. In the Add Device to SDS <SDS name> dialog box, in the Storage Devices tab, add the following required parameters for the storage device:
   a. Enter the file path of the device.
   b. Enter the name of the device.
   c. Select the relevant Storage Pool.
   d. Click the media type of the device, HDD or SSD.
   e. Click Add Device.
   The device is added to the Devices list.
4. Expand Advanced for more options. Configure the following options (recommended for advanced users):
   a. Select one of the device testing options:
      • Test and activate device. Enter the timeout in seconds.
      • Test only
      • Activate without test
   b. Click Yes to force device takeover. This option erases data from a device that was previously used.
5. Click Add Devices.
6. Verify that the operation completed successfully and click Dismiss.

Results

Storage devices are added to the SDS.

Add acceleration devices

Acceleration devices can be added to a system.

Prerequisites

Ensure that at least one suitable Acceleration Pool is defined.

All devices in a Storage Pool must be the same media type. Ensure that you know the type of devices that you are adding to the system, and that the Storage Pool to which you are adding devices is configured to receive that media type. RFcache can only be used for medium granularity Storage Pools.

**NOTE:** The RFcache feature is only supported by 512 Byte devices for the cache use case. RFcache is not supported on 4K devices used for cache. However, RFcache acceleration of 4K storage devices is supported.

About this task

Device data is erased when devices are added to an SDS. When adding a device to an SDS, PowerFlex will check that the device is clear before adding it. An error will be returned, per device, if it is found not to be clear. 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 will be lost. For more information, see "Configuring direct attached storage" in the Getting to Know PowerFlex Guide.

You can assign a name to devices. This can be particularly helpful for identifying SDS devices in the future, because the name will remain 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

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

Steps

1. From the PowerFlex GUI, in the left pane, click Configuration > SDSs.
2. In the right pane, click Add Device.
3. In the Add Device to SDS <SDS name> dialog box, in the Acceleration Devices tab, add the following required parameters for the storage device:
   a. Enter the file path of the device.
   b. Enter the name of the device
   c. Select the relevant Acceleration Pool.
   d. Click Add Device
      The device is added to the Devices list.
4. Expand Advanced for more options. Configure the following options (recommended for advanced users):
   a. Select one of the device testing options:
      • Test and activate device. Enter the timeout in seconds.
      • Test only
      • Activate without test
   b. Click Yes to force device takeover. This option erases data from a device that was previously used
5. Click Add Devices.
6. Verify that the operation completed successfully and click Dismiss.

Results
Acceleration devices are added to the SDS.

Storage Pools
Add, modify, or remove a Storage Pool in the PowerFlex environment.
Each Storage Pool belongs to a single Protection Domain. The Storage Pool consists of a Magnetic Storage Pool (for HDDs) or a High Performance Storage (for SSDs). It supports medium or fine granularity data layouts.

Add Storage Pools
Add Storage Pools to a PowerFlex system. A Storage Pool is a group of devices within a Protection Domain.

Prerequisites
- Before adding a Storage Pool, 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. For more information, see the Getting to Know PowerFlex Guide.
- For Storage Pools with Fine Granularity data layout, at least one NVDIMM configured as a DAX device is required. In addition, ensure that you have already configured an NVDIMM Acceleration Pool.

About this task
Create Storage Pools before you start adding storage devices to the system, because each time that you add devices to the system, you must map them to either Storage Pools or Acceleration Pools.

NOTE: You cannot enable zero padding to Medium Granularity Storage Pools after adding the devices. For more information, see "Storage Pools" in the Getting to Know PowerFlex Guide.

Steps
1. From the PowerFlex GUI, in the left pane, click Configuration > Storage Pools.
2. In the right pane, click Add.
3. In the Add Storage Pool dialog box, define the following settings for the Storage Pool:
   a. Enter a name for the Storage Pool.
   b. Select the relevant Protection Domain
   c. Select the media type: HDD or SSD.
      All the devices that you add to this Storage Pool must be the same type of device.
   d. If you selected SSD, choose a Data Layout type:
      • Medium Granularity
      • Fine Granularity
1. Select the relevant option from the **Acceleration Pool** list.

4. Select **Use Read RAM Cache** to use Read RAM Cache for caching.

   **NOTE:** The Read RAM Cache features are advanced features, and it is usually recommended to accept the default values. You can configure these features later, if necessary, using the **Configure Read RAM Cache** command. For more information about Read RAM Cache features, see "Managing RAM read cache".

5. Select the **Write Handling Mode** type: **Cached** or **Passthrough**.

6. Select **Use Inflight Checksum** to enable validation of the checksum value of in-flight data reads and writes.

7. Click **Add Storage Pool**.

8. Verify the operation completed successfully and click **Dismiss**.

**Results**

The Storage Pool is added to the PowerFlex system.

---

**Storage Pool settings**

Update Storage Pool settings to maintain an up-to-date PowerFlex environment.

**Enable and disable Rebuild/Rebalance**

Use the Rebuild/Rebalance features to maintain system health, optimal performance and data protection.

**About this task**

By default, the Rebuild/Rebalance features are enabled in the system because they are essential for system health, optimal performance, and data protection. These features should only be disabled temporarily in very specific circumstances, and should not be left disabled for long periods of time. Rebuild/Rebalance features are enabled and disabled per Storage Pool.

**NOTE:** Rebuilding is an essential part of PowerFlex, which provides protection for your data. It is not recommended to disable the Rebuild feature, except in very special circumstances. Rebalancing is an essential part of PowerFlex, and should only be disabled, temporarily, in special circumstances. Disabling Rebalance may cause the system to become unbalanced even if no capacity is added or removed. For example, during a recovery from an SDS or device failure, some Rebalance activity may be needed to ensure optimal balancing.

To enable or disable Rebuild/Rebalance features, perform these steps:

**Steps**

1. From the PowerFlex GUI, in the left pane, click **Configuration > Storage Pools**.
2. In the right pane, select the relevant Storage Pool check box, and click **Settings > General**.
3. In the **Storage Pool <SP name> Settings** dialog box, select or clear **Enable Rebuild/Rebalance** check box.
4. Click **Apply**.
5. Verify the operation completed successfully and click **Dismiss**.
6. From the top right, click the **Running Jobs** icon and check the progress of the rebuild/rebalance.

**Results**

Rebuild/Rebalance is enabled or disabled for the Storage Pool.

**Configure inflight/persistent checkum**

Inflight checksum protection mode can be used to validate data reads and writes in Storage Pools, in order to protect data from data corruption. Persistent checksum is used to support the MG layout for protecting the storage device from data corruption.

**Prerequisites**

Disable background device scanner from Storage Pool before enabling/disabling persistent checksum.
About this task
To modify this setting, perform the following steps:

Steps
1. From the PowerFlex GUI, in the left pane, click Configuration > Storage Pools.
2. In the right pane, select the relevant Storage Pool check box, and click Settings > General.
3. In the Storage Pool <SP name> Settings dialog box, select the Enable Inflight Checksum check box and select one or both options:
   - Inflight
   - Persistent
4. Select validate on read to validate data reads in the Storage Pool and click Apply.
5. Verify the operation completed successfully and click Dismiss.
6. From the top right, click the Running Jobs icon and check the progress of the persistent checksum.

Results
The inflight/persistent checksum protection mode is enabled for the Storage Pool.

Enable or disable zero-padding policy
Use the zero-padded policy when the Storage Pool data layout is Fine Granularity (FG). The zero-padded policy ensures that every read from an area previously not written to, returns zeros.

Steps
1. From the PowerFlex GUI, in the left pane, click Configuration > Storage Pools.
2. In the right pane, select the relevant Storage Pool check box, and click Settings > General.
3. In the Storage Pool <SP name> Settings dialog box, select or clear the Enable Zero Padding Policy check box.
4. Click Apply.
5. Verify the operation completed successfully and click Dismiss.

Results
The zero padded policy is enabled for FG and disabled when the data layout is Medium Granularity (MG).

Compression Mode for Fine Granularity Storage Pools
Enable Compression Mode for FG Storage Pools.
In-line compression reduces the data footprint and allows you to gain more effective capacity from less physical hardware (SSDs).

Enable Compression for Fine Granularity
Enable compression for Fine Granularity (FG) Storage Pools. The Storage Pool must be configured for FG.

Steps
1. From the PowerFlex GUI, in the left pane, click Configuration > Storage Pools.
2. In the right pane, select the relevant Storage Pool check box, and click Settings > General.
3. In the Storage Pool <SP name> Settings dialog box, select Enable Compression (FG layout only).
4. Click Apply.
5. Verify the operation completed successfully and click Dismiss.

Results
Compression Mode is now enabled for the FG Storage Pool.

Read Flash Cache and Read RAM Cache
Set Read Flash Cache and Read RAM Cache for the Storage Pool
Set RFcache policy

Enable or disable RFcache at Storage Pool level.

About this task

- Once this is enabled, set the RFcache policy at PD level.
- Once RFcache is enabled at both Protection Domain/Storage Pool and SDS levels, add RFcache devices to the SDS in order to commence caching.

Steps

1. From the PowerFlex GUI, in the left pane, click **Configuration > Storage Pools**.
2. In the right pane, select the relevant Storage Pool check box, and click **Settings > General**.
3. In the **Storage Pool <SP name> Cache Settings** dialog box, select **RFcache Policy**, and then click **Apply**.
4. Verify that the operation completed successfully and click **Dismiss**.

Results

The RFcache is enabled for the Storage Pool.

Configure RMcache

The RMcache feature improves your system’s application performance for storage-related activities. By default, caching is disabled.

About this task

To use RMcache, you need to configure settings at two levels:

- **Storage Pool**—controls RMcache for all the SDSs in the selected Storage Pool. Caching can be enabled or disabled, and either Cached (default) or Passthrough Write Handling modes can be selected. When RMcache is enabled in a Storage Pool, the feature is enabled at Storage Pool level. However, caching must also be set to Enabled in each SDS in the Storage Pool. Caching will only begin once storage devices have been added to the SDSs. It is possible to enable RAM caching for a Storage Pool and then disable caching on one or more SDSs individually.
- **Per SDS**—controls RMcache for one or more SDSs. Caching can be enabled or disabled for the specified SDS, and the capacity allocated for caching on an SDS can be specified. Caching will only begin after one or more storage devices are added to the SDSs. Ensure that the feature is also enabled at Storage Pool level.

**NOTE:** By default, RMcache is disabled in all volumes. You can enable them from the Frontend > Volumes view.

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

To configure caching, perform these steps:

Steps

1. From the PowerFlex GUI, in the left pane, click **Configuration > Storage Pools**.
2. In the right pane, select the relevant Storage Pool check box, and click **Settings > Cache**.
3. In the **Storage Pool <SP name> Cache Settings** dialog box, select the **Use RMcache** check box.
4. Click **Apply**.

Results

RMcache is set for the Storage Pool

Set device capacity limits

When replacing a storage device in the system with a storage device of a smaller capacity, set the capacity limit of the device to be removed to less than its full capacity.

About this task

In such a case, capacity will be decreased, but the size of the disk remains unchanged. The capacity assigned to the storage device must be smaller than its actual physical size.
NOTE: Decreased capacity is shown on the Dashboard, using pale gray, on the outer ring on the Capacity tile.

Steps
1. From the PowerFlex GUI, in the left pane, click Configuration > Storage Pools.
2. In the right pane, select the relevant Storage Pool check box, and click Settings > Capacity.
3. In the Storage Pool <SP name> Capacity Settings dialog box, type the percentage for the following options:
   - Spare Percentage Policy
   - Set Capacity Alert Thresholds: High
   - Set Capacity Alert Thresholds: Critical
4. Click Apply.
5. Verify that the operation completed successfully and click Dismiss.

Results
Capacity limits for the Storage Pool are set.

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 will be provided in event reports. For more information about viewing events, see "Viewing events" in the Monitoring PowerFlex Guide.

Reset error counters

Reset the background device scanner error counters for specified Storage Pools. Counters for data comparison errors, or fixed read errors, or both counter types can be reset.

About this task
There are two modes: Fixed Read Errors mode, and Compare Error mode:

- Fixed Read Errors—Perform read operations. Fix from peer on errors. This is the default mode for both Fine and Medium Granularity for all new Storage Pools.
- Compare Error—Perform the device-only test, and compare the data content with peer. Zero padding must be enabled in order to set the background device scanner to data comparison mode.

To reset error counters, follow these steps:

Steps
1. From the PowerFlex GUI, in the left pane, click Configuration > Storage Pools.
2. In the right pane, select the relevant Storage Pool check box, and click More > Reset Error Counters.
3. In the Reset Error Counters for <SP name> dialog box, select the relevant option:
   a. Reset Fixed Read Error Counters
   b. Reset Compare Error Counters
4. Click Apply.
5. Verify that the operation completed successfully and click Dismiss.

Results
The error counters are reset.

Enable the background device scanner

The scanner can be enabled on all the devices in the specified Storage Pool.

About this task
To enable the scanner, follow these steps:
Steps

1. From the PowerFlex GUI, in the left pane, click Configuration > Storage Pools.
2. In the right pane, select the relevant Storage Pool check box, and click More > Background Device Scanner.
3. In the Set Background Device Scanner for Storage Pool <SP name> dialog box, select the relevant option for the following settings:
   - Enable Background Device Scanner
   - Select Fix Local Device Errors to automatically clear device errors.
   - Enter the Bandwidth Limit in KB/S.
   (NOTE: High bandwidth should be used very carefully for extreme cases only (such as an urgent need to check some devices), as it may create negative impact on the system performance. Setting the background device scanner bandwidth should take into account maximum bandwidth of the devices.
   - Select Compare Data to 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.
4. Click Apply.
5. Verify that the operation completed successfully and click Dismiss.

Set media type for Storage Pool

Update the media type of the Storage Pool. This might be required if FG data layout is being used. This requires an SSD media type.

Steps

1. From the PowerFlex GUI, in the left pane, click Configuration > Storage Pools.
2. In the right pane, select the relevant Storage Pool check box, and click Modify > Media Type.
3. In the Set Media Type for Storage Pool <SP name> dialog box, from the Media Type list, select the media type for the Storage Pool.
   - HDD
   - SSD
   - Transitional - this option allows for migration flows
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 completed successfully and click Dismiss.

Results

The media type is set for the Storage Pool.

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

Configure bandwidth and concurrent I/Os for Rebuild, Rebalance, Migration and Protected Maintenance Mode (PMM) of jobs.

About this task

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

Steps

1. From the PowerFlex GUI, in the left pane, click Configuration > Storage Pools.
2. In the right pane, select the relevant Storage Pool check box, and click Modify > IO Priority.
3. For each of the tabs Rebuild, Rebalance, Migration, Maintenance Mode in the Set IO Priority for Storage Pool <SP name> dialog box, select one of the following IO Priority options:
4. Click **Apply**.
5. Verify that the operation completed successfully and click **Dismiss**.

**Results**

IO Priority is set for the Storage Pool.

---

**Create a VM storage policy for Virtual Volumes**

Define the VM storage policy in the vSphere Client using the Create VM Storage Policy wizard and enable datastore specific rules for vVols in PowerFlex.

**Prerequisites**

- Verify that the VASA storage provider is registered and active

**Steps**

1. In the vSphere Client, open the **Create VM Storage Policy** wizard.
   a. Click **Menu > Policies and Profiles**.
   b. Under **Policies and Profiles**, click **VM Storage Policies**.
   c. Click **Create VM Storage Policy**.
2. In the **Name and description** page, enter the vCenter server, policy name, and description, and click **Next**.
3. In the **Policy structure** page, under **Datastore specific rules**, select Enable rules for PowerFlex vVols storage.
4. In the **PowerFlex vVols rules** page, define storage placement rules for the target vVols datastore.
   - In the **Placement** tab, from the **Tier** drop-down menu, select the appropriate storage policy.

<table>
<thead>
<tr>
<th>Tier</th>
<th>Used for storage type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compression enabled</td>
<td>Fine granularity layout</td>
</tr>
<tr>
<td>Gold</td>
<td>Medium granularity layout, SSD drives</td>
</tr>
<tr>
<td>Silver</td>
<td>Medium granularity layout, cached</td>
</tr>
<tr>
<td>Bronze</td>
<td>Medium granularity layout, HDD</td>
</tr>
</tbody>
</table>

5. In the **Storage compatibility** page, review the list of Storage Pools that match the policy you selected in the previous page.
6. In the **Review and finish** page, review the storage policy settings and click **Finish**.

**Results**

The new VM storage policy compatible with vVols appears on the storage policy list. You can now associate this policy with a virtual machine, or designate the policy as default.

---

**Configuring acceleration**

PowerFlex supports different types of acceleration to enhance storage performance. Depending on your system, you can configure PowerFlex for acceleration using NVDIMM, RFcache or RMcache.
Prepare acceleration devices and software

Prepare NVDIMM acceleration devices so that they can be used to accelerate Fine Granularity Storage Pools. If the `xcache` package was not installed during initial deployment, install the package on SDSs where the RFcache feature will be used to accelerate Medium Granularity Storage Pools.

**NOTE:** When NVDIMM acceleration is used, the node interleaving setting must be disabled in the server's system BIOS. Node interleaving is disabled by default on VxFlex Ready Node servers. However, the setting may be impacted during component replacement or firmware upgrade, or for other reasons. For instructions on verifying or disabling node interleaving on a node, refer to the Owner's Guide for your specific system.

Add acceleration pools

You can add Acceleration Pools to a Protection Domain, to accelerate Storage Pool performance.

**About this task**

An Acceleration Pool is a group of acceleration devices within a Protection Domain.

**Steps**

1. From the PowerFlex GUI, in the left pane, click **Configuration > Acceleration Pools**.
2. In the right pane, click **Add**.
3. In the **Add Acceleration Pool** dialog box, define the following settings for the Acceleration Pool:
   a. Enter a name for the Acceleration Pool.
   b. Select one of the following pool types:
      - NVDIMM - this option is when using FG data layout. There must be at least one NVDIMM installed in order to select this option.
      - SSD - this option is when using MG data layout. There must be at least one SSD installed that can be used for the RFcache feature in order to select this option.
4. Select the relevant Protection Domain.
5. In the **Add Devices** section, enter the following details of the device to add to the SDS:
   a. Enter the path of the acceleration device.
   b. Enter the name of the acceleration device.
   c. Select the relevant SDS.
   d. Click **Add Devices**.
      The acceleration device is added to the **Devices** table.
   e. If you want to add more devices, click the **Add device** button and enter the details of the device.
6. Click **Add Acceleration Pool**.
7. Verify that the operation completed successfully and click **Dismiss**.

**Results**

The Acceleration Pool has been created, and acceleration devices have been added.

**Next steps**

For RFcache Acceleration Pools, ensure that caching is enabled, using the **Cache Settings > Set Read Flash Cache Policy** command. This feature can be enabled at Protection Domain, Storage Pool, or SDS level.

Add acceleration device on RHEL nodes

You can add an one or more acceleration devices to an SDS.

**Prerequisites**

When adding NVDIMMs to a node, the enumeration of the DAX devices may change in the node.

<table>
<thead>
<tr>
<th>Name: /dev/dax0.0</th>
<th>Path: /dev/dax2.0</th>
<th>Original-path: /dev/dax0.0</th>
<th>ID: ff9e65d600010000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceleration Pool: acl, Capacity: 15.7 GB (16052 MB), Used: 2.9 GB (3003 MB), State: Normal</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
When adding a new NVDIMM DAX path to the acceleration pool it fails with the error:

```
cli --add_sds_device --sds_id <SDS-ID> --acceleration_pool_name acl --device_path /dev/dax2.0
Error: MDM failed command. Status: A device with the given
```

This is a very common scenario where the name of the device changes, especially in Linux and any disk including NVDIMM devices. To fix this, run the following command:

```
scli --update_sds_original_paths --sds_id <SDS-ID>
```

The update is displayed:

```
Name: /dev/dax0.0 Path: /dev/dax2.0 Original-path: /dev/dax2.0 ID: ff9e65d600010000
Acceleration Pool: acl, Capacity: 15.7 GB (16052 MB), Used: 2.9 GB (3003 MB), State: Normal
```

Also if the current SDS device includes the name field, you must update it to match the new path so that it is reflected in the GUI. For example:

```
scli --rename_device --sds_id <SDS-ID> --device_path /dev/dax2.0 --new_name /dev/dax2.0
Successfully renamed device to /dev/dax2.0
```

The following steps describe how to update from two to four NVDIMMs

1. Gracefully shutdown node (place SDS in maintenance mode and move application workload to other node)
2. Add two NVDIMMs
3. Boot up node.
4. Login and run Exit SDS maintenance mode from the GUI or CLI.
5. Run the following command:

```
scli --update_sds_original_paths --sds_id <SDS-ID>
```

6. For each existing NVDIMM DAX mount point run the command:

```
scli --rename_device --sds_id <SDS-ID> --device_path /dev/dax2.0 --new_name /dev/dax2.0
```

**NOTE:** This is only required if name was assigned.

7. Run `ndctl` to create the DAX device. Repeat for each new device.
8. Add the `/dev/daxDevice` name to Acceleration pool

**Steps**

1. In the left pane, click **Configuration > SDSs**.
2. In the right pane, select the relevant SDS and click **Add Device**.
3. In the **Add Device to SDS name** dialog, click the **Acceleration Devices** tab, and enter the following details of the acceleration device to add to the SDS:
   a. Enter the location of the acceleration device.
   b. Enter the name of the acceleration device.
   c. Select the relevant SDS.
   d. Click **Add Devices**.
      The acceleration device is added to the **Devices** table.
   e. If you want to add more devices, click the **Add device** button and enter the details of the device.
   f. The **Advanced** option provides additional items, such as device testing and forced device takeover. Optionally, click the drop-down button to display and configure the settings (recommended for advanced users only):
      - Select one of the device testing options: Test and activate device, Test only, Activate without test
      - Enter timeout in seconds
      - Click **Yes** to force device takeover. This option erases data from a device that was previously used
4. Click **Add Devices** to add acceleration device to the SDS.

**Prepare the DAX devices**

If the deployment will be using NVDIMM devices for acceleration, perform the following tasks to prepare the NVDIMMs as DAX acceleration devices.
Before you prepare the NVDIMM as a DAX device, create or print the following NVDIMM information table. Use it to record the information that you discover while performing the following task. You will need the information to add the acceleration device to PowerFlex.

**Table 1. NVDIMM information table**

<table>
<thead>
<tr>
<th>Item</th>
<th>Replacement NVDIMM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td></td>
</tr>
<tr>
<td>Device name (NMEM)</td>
<td></td>
</tr>
<tr>
<td>Namespace</td>
<td></td>
</tr>
<tr>
<td>DAX device name (chardev)</td>
<td></td>
</tr>
<tr>
<td>Acceleration device path</td>
<td></td>
</tr>
</tbody>
</table>

Prepare an NVDIMM as a DAX (Acceleration) device in a Linux system

Prepare a new or replacement NVDIMM as a DAX/Acceleration device before adding it to the SDS in a Linux system. This step is optional when replacing an NVDIMM battery.

**Prerequisites**

**NOTE:** If you evacuated the node from PowerFlex, skip this task.

If the node is running on RHEL 7.6, ensure that the package `kmod-redhat-nfit-3.10.0-957-1.el7_6.x86_64.rpm` is installed.

For more information, see [here](#).

**About this task**

**NOTE:** If you replaced the system board, perform the following steps for each NVDIMM mounted on the server.

**Steps**

1. Using SSH, log in to the Linux server.
2. View information for the new/replacement NVDIMM:
   
   ```
   dmidecode --type memory | grep "Non-" -B 3 -A 3 | grep -E 'Locator|Serial' | grep -v Bank
   ```

   Output similar to the following appears:
   
   ```
   Locator: A7
   Serial Number: 17496594
   Locator: B7
   Serial Number: 174965AC
   ```

3. Find the serial number in the output and record it in the NVDIMM information table.
4. Display the correlation between the ID and NMEM device name of each NVDIMM mounted on the server:
   
   ```
   ndctl list -Dvvv | jq ".[].dimms[]'
   ```

   Output similar to the following appears:
   
   ```
   
   
   ```
In the output from the previous step, find the device (dev) with the id that partially correlates with the serial number you discovered previously for the failed device.

For example:

- The NVDIMM output displays serial number 16492521 for the NVDIMM device.
- In the previous step, the output displays the ID of device nmem0 as 802c-0f-1711-16492521.

<table>
<thead>
<tr>
<th>Serial number</th>
<th>Device ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locator: A7</td>
<td>&quot;dev&quot;: &quot;nmem0&quot;,</td>
</tr>
<tr>
<td>Serial Number: 16492521</td>
<td>&quot;id&quot;: &quot;802c-0f-1722-17496594&quot;,</td>
</tr>
<tr>
<td>Locator: B7</td>
<td>&quot;handle&quot;: 1,</td>
</tr>
<tr>
<td>Serial Number: 1649251B</td>
<td>&quot;phys_id&quot;: 4358,</td>
</tr>
<tr>
<td></td>
<td>&quot;health&quot;: {</td>
</tr>
<tr>
<td></td>
<td>&quot;health_state&quot;: &quot;ok&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;temperature_celsius&quot;: 255,</td>
</tr>
<tr>
<td></td>
<td>&quot;life_used_percentage&quot;: 30</td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>

In the above example, the NMEM name is nmem0.

6. Record the NMEM name in the Device name row of the NVDIMM information table.

7. Correlate between the NMEM DIMM and the namespace/DAX device (Acceleration device):

```
ndctl list -Dvvv | jq '.[].dimms[]'
```

Output similar to the following appears:

```
{
  "dev": "nmem1",
  "id": "802c-0f-1722-174965ac",
  "handle": 4097,
  "phys_id": 4370,
  "health": {
    "health_state": "ok",
    "temperature_celsius": 255,
    "life_used_percentage": 30
  }
}
{
  "dev": "nmem0",
  "id": "802c-0f-1722-17496594",
  "handle": 1,
  "phys_id": 4358,
  "health": {
    "health_state": "ok",
    "temperature_celsius": 255,
    "life_used_percentage": 30
  }
}
```

```
ndctl list -Dvvv | jq '.[].regions[].namespaces[]'
```

```
{
  "dev": "namespace1.0",
  "mode": "raw",
  "size": 17179869184,
  "sector_size": 512,
  "blockdev": "pmem1",
  "numa_node": 1
}
{
  "dev": "namespace0.0",
  "mode": "raw",
  "size": 17179869184,
  "sector_size": 512,
  "blockdev": "pmem0",
  "numa_node": 1
}
```
8. In the output displayed in the previous step, locate the namespace that correlates with the NMEM name and DIMM serial number, and record it in the NVDIMM information table.

In the above example, nmem0's namespace is namespace0.0.

9. Destroy the default namespace that was created for the replacement NVDIMM, using the namespace discovered in the previous step:

   ndctl destroy-namespace namespaceX.0

For example, if the replacement NVDIMM maps to namespace0.0, the command is:

   ndctl destroy-namespace namespace0.0

10. Create a new, raw nmemp device using the region associated with namespace of the failed device, as recorded in the NVDIMM information table:

   ndctl create-namespace -r regionX -m raw -f

For example, if the NVDIMM you replaced mapped to region 0, the command is:

   ndctl create-namespace -r region0 -m raw -f

11. Convert the namespace device to the acceleration device name of type /dev/daxX.X:

   ndctl create-namespace -f -e namespaceX.X --mode=devdax -align=4K

For ndctl build 62 or later, run:

   ndctl create-namespace -f -e namespaceX.X --mode=dax -align=4K --no-autolabel

where namespaceX.X is the actual namespace of the NVDIMM.

For example, to convert namespace0.0 to /dev/dax0.0, where /dev/daxX.X is the acceleration device name, depending on the ndctl build run:

   ndctl create-namespace -f -e namespace0.0 --mode=dax -align=4K

or

   ndctl create-namespace -f -e namespace0.0 --mode=dax -align=4K --no-autolabel

**NOTE:** --no-autolabel is only required for RHEL7.6.

12. Record the acceleration device name in the NVDIMM information table.

13. Run the namespace-to-dax-device correlation command to find the DAX/Acceleration device name of the replacement NVDIMM:

   ndctl list -Dvvv | jq '.[].regions[].namespaces[]'

Output similar to the following appears:

   
   
   {  
     "dev": "namespace1.0",  
     "mode": "devdax",  
     "map": "dev",  
     "size": 16909336576,  
     "uuid": "c59d6a2d-7eeb-4f32-b27a-9960a327e734",  
     "daxregion": {  
       "id": 1,  
       "size": 16909336576,  
       "align": 4096,  
       "devices": [  
       ]  
   }  

   

Configuration 73
The DAX/Acceleration device name appears in the output as the chardev value.
In the example output above, the DAX/Acceleration device name is dax0.0.

14. Record the DAX/Acceleration device name in the NVDIMM information table.

15. Find the full acceleration device path:

```
ls -ltr /dev/ | grep dax
```

The following output should appear:
```
/dev/daxX.X
```
For example:
```
/dev/dax0.0
```

16. Record the acceleration device path in the NVDIMM information table.

Results

You are now ready to add the DAX/Acceleration device to the NVDIMM Acceleration Pool.

Check NVDIMM capacity compatibility for future upgrades

Check your system for the recommended NVDIMM capacity, to prepare it in advance for future upgrades of Fine Granularity Storage Pools. You will not be able to upgrade your system to versions higher than v3.0.1 unless sufficient NVDIMMs are installed in the system.

Prerequisites

- Ensure that you have the tool for checking upgrade readiness: `FlexOS_PreUpgrade_Readiness_Checker.py`. It is supplied with the PowerFlex complete software package, and on the Dell EMC support site.
- Ensure that the server from which you will run the tool has the following:
  - Linux operating system (the tool cannot be used on Windows-based servers)
  - Access to the MDM
  - Python version 2.7 or higher must be installed
  - PowerFlex CLI is installed
- Ensure that you know the IP addresses of the MDMs, and know the user name and password required for accessing them.
- Ensure that your user role includes monitor privileges. Monitor privileges are used to query the system for SDSs that require additional NVDIMMs.
About this task

If your PowerFlex system does not contain enough NVDIMM capacity to support Fine Granularity Storage Pools in PowerFlex versions later than v3.0.1, your system will generate alerts to warn you about this issue. You will not be able to upgrade your system to versions higher than v3.0.1 until you have addressed this issue. You can check your system now to find out if it has enough NVDIMM capacity. If there is insufficient capacity, Dell EMC recommends that you contact your account manager now in order to prepare your hardware in advance for future software versions.

Steps

1. Save the `FlexOS_PreUpgrade_Readiness_Checker.py` tool on the MDM, or on a node with connectivity with the MDM.
2. In command line, run the command:

   ```bash
   ```

   where:
   
   `<USERNAME>` is the user name used to query the MDM
   
   `<PASSWORD>` is the user’s password
   
   `<CLI_BIN>` is the location of the PowerFlex CLI on the server
   
   `<MDM_IP_ADDRESSES>` is a comma-separated list of MDM IP addresses

   The tool will output one of the following messages:

   - Your system has insufficient NVDIMM capacity on SDS {XXX} to support future version upgrades. The required total NVDIMM capacity for the upgrade is {YYY}. Contact your account manager for more information.
     (This message may appear several times, depending on the number of SDSs with insufficient NVDIMM capacity.)
   - System is ready for upgrade

   If the output is System is ready for upgrade, no further actions are required now. Your system contains enough NVDIMM capacity to support Fine Granularity storage acceleration in future software versions.

   If the output is Your system has insufficient NVDIMM capacity on SDS {XXX} to support future version upgrades. The required total NVDIMM capacity for the upgrade is {YYY}. Contact your account manager for more information., continue to the next step.

3. Use one of the following methods to determine which SDSs need more NVDIMM capacity.

<table>
<thead>
<tr>
<th>Option</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CLI</strong></td>
<td>a. Prepare a list of the SDSs in your system. You can use the <code>--query_all_sds</code> to collect this information. For example:</td>
</tr>
<tr>
<td></td>
<td>scli --query_all_sds</td>
</tr>
<tr>
<td></td>
<td>b. Using the CLI, run the following command for every SDS that uses NVDIMM acceleration for Fine Granularity storage:</td>
</tr>
<tr>
<td></td>
<td>scli --query_sds (--sds_id &lt;ID&gt;</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>scli --query_sds --sds_name sds1948</td>
</tr>
<tr>
<td></td>
<td>Look for output similar to the following:</td>
</tr>
<tr>
<td></td>
<td>Acceleration device information (total 2 devices)</td>
</tr>
<tr>
<td></td>
<td>1: Name: N/A Path: /dev/dax0.0 Original-path: /dev/dax0.0 ID dfeff27800010000 Acceleration Pool: accp1, Capacity: 15.7 GB (16052 MB), Used: 21.7 GB (22170 MB), State: Normal</td>
</tr>
<tr>
<td></td>
<td>c. If the <code>Used</code> value is greater than the <code>Capacity</code> value, as shown in the output example above, more NVDIMM capacity is required in order to upgrade the system.</td>
</tr>
<tr>
<td></td>
<td>d. Make a note of all the SDSs where more NVDIMM capacity is required.</td>
</tr>
<tr>
<td>Option</td>
<td>Procedure</td>
</tr>
<tr>
<td>--------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
| GUI    | a. From the PowerFlex GUI, open the **Alerts** pane, and look for alerts for insufficient NVDIMM capacity for future version upgrades.  
|        | b. Prepare a list of all the SDSs where these alerts occur. |

4. Contact your account manager for sales and technical assistance.

## Add NVDIMM in an ESXi environment

Add NVDIMMs for acceleration in an ESXi environment.

### Prerequisites for adding an NVDIMM to an ESXi 6.7 system

Meet the following prerequisites before adding an NVDIMM to an ESXi 6.7 based PowerFlex system.

Before you begin adding an NVDIMM to an ESXi 6.7 based PowerFlex system, ensure the following:

- You are using VMware version 6.7 for the ESXi host and the vCenter server.
- The VM version of your SVM is version 14 or higher.
- The firmware of the NVDIMM is updated to the version supported by your server. For example, for compatible Dell EMC PowerEdge servers, use NVDIMM firmware version 9324 or higher.
- The ESXi host can detect the NVDIMM.
- You calculate required NVDIMM capacity, according to number of FG devices and their size.
- There is enough NVDIMM capacity on the ESXi host.
- The appropriate VMware licensing is required for persistent memory support; an Enterprise Plus license might be required. To check whether your license supports persistent memory, refer to VMware **Compare vSphere Editions and Features**.

### Verify that the ESXi host can detect the NVDIMM

Before adding an NVDIMM to an ESXi-based PowerFlex system, verify that the ESXi host can detect the NVDIMM.

**Prerequisites**

**Steps**

1. Login to the vCenter.
2. Select your ESXi host.
3. Navigate to the **Summary** tab.
4. In the **Hardware** section, verify that the required amount of **Persistent Memory** is listed.

### Calculate required NVDIMM and RAM capacity for FG SDS

Use the following formulas to calculate the necessary capacity for NVDIMM and RAM.

**About this task**

**NOTE:** When adding NVDIMM capacity to the SVM, the complete capacity of the NVDIMM must be allocated in a single device when adding to the SVM. For example 16 GB + 2 of NVDIMM will be added as 31 GB (rounded down, since VMware uses some of the capacity for datastore management).

**Steps**

1. Calculate the required NVDIMM and RAM capacity using the following table, where X is the total capacity of SDS devices used for the FG storage pool, and Y is the total RAM needed:

<table>
<thead>
<tr>
<th>FG capacity</th>
<th>Required NVDIMM capacity</th>
<th>Required RAM capacity (rounded)</th>
<th>Additional memory for MDM, LIA, and SVM OS</th>
<th>Total RAM (rounded)</th>
</tr>
</thead>
</table>
| 51.2 TB     | 32 GB NVDIMM (in SVM it will be 31 GB) | >41 GB | MDM: 5.4 GB  
LIA: 350 MB  
OS Base: 1 G | 53 GB |
<table>
<thead>
<tr>
<th>FG capacity</th>
<th>Required NVDIMM capacity</th>
<th>Required RAM capacity (rounded)</th>
<th>Additional memory for MDM, LIA, and SVM OS</th>
<th>Total RAM (rounded)</th>
</tr>
</thead>
<tbody>
<tr>
<td>51.2 TB &lt; X &lt; 96 TB</td>
<td>64 GB NVDIMM (in SVM it will be 62 GB)</td>
<td>&gt;41 GB &lt;64.5 GB</td>
<td>Buffer : 1 G</td>
<td>53 GB &lt; Y &lt; 73 GB</td>
</tr>
<tr>
<td>96 TB &lt; X &lt; 128 TB (122.88 is actual limit)</td>
<td>96 GB NVDIMM (in SVM it will be 93 GB)</td>
<td>&gt;64.5 GB &lt;81.5 GB</td>
<td></td>
<td>87 GB</td>
</tr>
</tbody>
</table>

2. Alternatively, you can calculate NVDIMM capacity and RAM capacity using the following formulas:

**NOTE:**

The calculation is in binary MiB, GiB, and TiB

- \[ \text{NVDIMM\_capacity\_in\_GiB} = \left(\frac{100 \times \text{Number\_Of\_Drives}}{} + \frac{700 \times \text{Capacity\_in\_TiB}}{1024}\right) \]
- \[ \text{RAM\_capacity\_in\_GiB} = 10 + \left(\frac{100 \times \text{Number\_Of\_Drives}}{} + \frac{550 \times \text{Capacity\_in\_TiB}}{1024}\right) \]

**Enter the SDS into Maintenance Mode**

Place the SDS into Maintenance Mode before adding the NVDIMM.

**Steps**

1. From the PowerFlex GUI, in the left pane, click **Alerts** and verify that there are no SDS disconnect messages.
2. Click **MDM > Cluster Settings** and verify that the cluster is healthy.
3. Refer to "Enter and exit SDS Maintenance Mode" for steps on how to set an SDS into maintenance mode.

**Results**

NVDIMM device can now be added to PowerFlex.

**Use vCenter to shut down the SVM**

In vCenter, shut down the Storage VM (SVM) before adding the NVDIMM.

**Steps**

1. In vCenter, verify that the SDS data IP address matches the SVM IP address.
2. Log in to vCenter using the vSphere client, and locate the relevant IP address or SVM name (which should include the host serial number).
   **NOTE:** Verify that the SVM IP address displayed in vCenter is the same as the SVM management IP address you recorded.
3. Select the SVM, and from the **Basic Tasks** pane select **Shut down the virtual machine**.
4. In the PowerFlex GUI **Alerts** view, verify that you received an alert that the SDS is disconnected. If the SVM is a cluster member, also verify that you received an alert that the MDM cluster is being degraded.

**Add an NVDIMM device to a PowerFlex system**

Use the vCenter client and the PowerFlex GUI to add an NVDIMM device to PowerFlex.

**Steps**

1. Add the NVDIMM device to the Storage VM (SVM):
   a. Edit the SVM settings.
   b. Add a new NVDIMM device.
   c. Set the desired size of the NVDIMM device according to the following:
### Table: Number of NVDIMMs vs Capacity

<table>
<thead>
<tr>
<th>Number of NVDIMMs</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>31 GB</td>
</tr>
<tr>
<td>4</td>
<td>62 GB</td>
</tr>
<tr>
<td>6</td>
<td>93 GB</td>
</tr>
</tbody>
</table>

**NOTE:**

VCenter does not allow adding more than three virtual NVDIMM devices. If you are expanding NVDIMM capacity, add a second NVDIMM device based on the rules above.

**d.** If additional RAM is needed (see Calculate required NVDIMM and RAM capacity for FG SDS on page 76), modify the memory size to match the necessary value.

**e.** Click OK.

2. In the vCenter client view, expand the server and select the Storage VM (SVM). Power-on the SVM manually.

3. Using the PowerFlex GUI, verify the following:
   
   **a.** From the PowerFlex GUI, in the left pane, click Alerts and verify that there are no SDS disconnect messages.

   **NOTE:** After the SVM has powered on, it might take approximately 10-20 seconds for the SDS to power up and remove the disconnection alerts.

   **b.** If the node was an MDM cluster member, in the MDM > Cluster Settings, verify that the cluster is no longer degraded and that no alert on a degraded cluster appears.

   **NOTE:** If "could not connect to HOST" alerts appear, wait a few minutes for the alerts to disappear.

4. Refer to "Enter and exit SDS Maintenance Mode" for steps on how to exit an SDS from maintenance mode.

5. In the Action window, click OK.

6. Wait for the rebuild/rebalance operations to complete.

   The SVM is now operational and you can add the NVDIMM capacity using the next set of steps.

7. Create a namespace on the NVDIMM:
   
   **a.** Connect using SSH to the SVM.
   
   **b.** Run the following:

   ```
   ndctl create-namespace -f -e namespace0.0 --mode=dax --align=4K
   ```

   **c.** Perform these steps for creating a namespace for every node with an NVDIMM device.

8. Create an Acceleration Pool for the NVDIMM devices:
   
   **a.** Connect using SSH to the Master MDM.
   
   **b.** Use the SCLI to create the Acceleration Pool:

   ```
   scli --add_acceleration_pool --protection_domain_name <PD_NAME> --media_type NVRAM --acceleration_pool_name <ACCP_NAME>
   ```

   **c.** For each SDS with NVDIMM, add the NVDIMM devices to the Acceleration Pool:

   ```
   scli --add_sds_device --sds_name <SDS_NAME> --device_path /dev/dax0.0 --acceleration_pool_name <ACCP_NAME> --force_device_takeover
   ```

9. Create a Storage Pool for SSD devices accelerated by NVDIMM Acceleration Pool with Fine Granularity data layout:
   
   **a.** Connect using SSH to the Master MDM and run the following SCLI command:

   ```
   scli --add_storage_pool --protection_domain_name <PD_NAME> --storage_pool_name <SP_NAME> --media_type SSD --compression_method normal --fgl_acceleration_pool_name <ACCP_NAME> --fglprofile high_performance --data_layout fine_granularity
   ```

10. Add SSD devices to the Fine Granularity Storage Pool that you created.

11. Set the Spare Capacity for the Fine Granularity Storage pool based on the number of nodes of equal capacity, allowing for at least one node to fail.

    Ten nodes of 20-TB SSD capacity each use a 10% Spare policy.
Removing acceleration devices

Acceleration devices must be removed in a graceful manner. Specific procedures are required for NVDIMM acceleration devices and for RFcache acceleration devices.

Remove an RFcache acceleration device

Remove an RFcache acceleration device from an Acceleration Pool.

About this task

To remove an RFcache acceleration device from the system, perform these steps:

Steps

1. Refer to "Set RFcache policy" for steps on how to clear the RFcache policy at the SDS level.
2. From the PowerFlex GUI, in the left pane, click Configuration > Acceleration Pools.
3. In the right pane, click the corresponding Acceleration Pool check box, and click Remove.
4. In the confirmation message dialog box, click Dismiss.

Results

The acceleration device is removed.

Physically remove an NVDIMM from a node

To remove an NVDIMM from a node, identify the NVDIMM to be removed and then use the GUI to remove it from the PowerFlex system. The procedures that follow are for removing a failed device, which is the most common scenario for removing an NVDIMM device.

Identify an NVDIMM module and correlate its storage devices in a Linux system

Identify the failed NVDIMM-N memory module and the correlating storage devices that interact with the module in the PowerFlex Fine Granularity Storage Pool in a Linux-based system. This task is also required when replacing the NVDIMM battery on the node or replacing the system board on a system with NVDIMMs used for acceleration.

Prerequisites

Ensure that you know:

- The IP address of the iDRAC port.
- The username and password for the iDRAC portal.

About this task

NOTE: In the following task, the term "failed NVDIMM" also refers to all NVDIMMs mounted on the server in cases of a failed NVDIMM battery or failed system board.

Steps

1. From a web browser go to http://<iDRAC_IP_address>.
2. In the Dell Console Login window, enter the username and password, and then click Login.
   
   The Dashboard displays the high-level status of all hardware devices in the System Health pane. The Memory icon should display an alert, signifying a failed device.
   
   If you are replacing an NVDIMM or NVDIMM battery, proceed to the following step. Otherwise, skip to step 6.
3. Double-click the icon of the failed memory device to display more information about the failed NVDIMM.
4. From the Maintenance tab, select System Event Log.
   
   The System Event Log displays events with color-coded severity levels. The event for the failed DIMM displays the slot number of the DIMM module that failed.
   
   In the following example, the error occurred on DIMM-A7, meaning that the DIMM is located in slot A7.
5. Record the slot number of the failed NVDIMM device in the NVDIMM information table.

**NOTE**: If the slot number points to a regular DIMM as faulty, use the DIMM replacement procedure instead.

6. From the Dell console main window, select **System > Inventory > Hardware Inventory**.

7. Expand the entry for the relevant DIMM.

The console displays information regarding the DIMM you identified in the previous steps.

The DIMM's **PrimaryStatus** should appear as Degraded.

8. Using SSH, log in to the Linux server.

9. View information for the faulty DIMM:

   ```bash
dmidecode --type memory | grep "Non-" -B 3 -A 3 | grep -E 'Locator|Serial' | grep -v Bank
   
   Output similar to the following appears:
   
   Locator: A7
   Serial Number: 16492521
   Locator: B7
   Serial Number: 1649251B
   
   The example output displays the DIMM's **Type Detail** as Non-Volatile, signifying that it is an NVDIMM. The output also displays the NVDIMM serial numbers.

10. In the command output, find the **Locator** and **Serial Number**, and record their values in the NVDIMM information table.

11. Display the list of DIMMs mounted on the server:

    ```bash
    ndctl list -Dvvv | jq '.[].dimms'
    
    Output similar to the following should appear:
    
    ```
12. In the output from the previous step, find the device (dev) with the id that partially correlates with the serial number you discovered previously for the failed device.

For example:

- The NVDIMM output displays serial number 16492521 for the NVDIMM device.
- In the previous step, the output displays the ID of device nmem0 as 802c-0f-1746-802c-0f-1711-16492521.

<table>
<thead>
<tr>
<th>Serial number</th>
<th>Device ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locator: A7</td>
<td></td>
</tr>
<tr>
<td>Serial Number: 16492521</td>
<td>&quot;dev&quot;: &quot;nmem0&quot;,</td>
</tr>
<tr>
<td>Locator: B7</td>
<td></td>
</tr>
<tr>
<td>Serial Number: 1649251B</td>
<td>&quot;id&quot;: &quot;802c-0f-1711-16492521&quot;,</td>
</tr>
</tbody>
</table>

In the above example, the NMEM name is nmem0.

13. Record the NMEM name in the Device name row of the NVDIMM information table.

14. To help correlate nmem mapping, region, and namespace configuration information, enter:

```
ndctl list -Dvvv | jq '.[].regions[]'
```

Output similar to the following appears:

```
{
  "dev": "region1",
  "size": 17179869184,
  "available_size": 0,
  "max_available_extent": 0,
  "type": "pmem",
  "numa_node": 1,
  "mappings": [
    {
      "dimm": "nmem1",
      "offset": 0,
      "length": 17179869184,
      "position": 0
    }
  ],
  "persistence_domain": "unknown",
  "namespaces": [
    {
      "dev": "namespace1.0",
      "mode": "devdax",
      "map": "dev",
      "size": 16909336576,
      "uuid": "0a438fbc-91e4-427d-8068-1f26330d85cc",
      "daxregion": {
        "id": 1,
        "size": 16909336576,
        "align": 4096,
        "devices": [
```

Configuration
The order of the list in the output reflects the order for correlating between an NMEM DIMM and a namespace/DAX device (or Acceleration device). For example, in the above output:

- The first block of devices is the DIMMs. Under each DIMM, there is an NMEM device grouping. In the example output, the device groupings are `nmem1` and `nmem0`. Each bracket contains a device.
- Each grouping also displays the region corresponding to the NMEM device group. In the example output, the regions are `region1` and `region0`.
- The order of the NMEM devices correlates to the namespace grouping that follows, in which `nmem1` correlates to `namespace1.0` and `nmem0` correlates to `namespace0.0`.
- The output displaying the namespace also includes the DAX/Acceleration device name (chardev), which is displayed as `daxX.X`.

15. In the output from the previous step, locate the namespace and subsequent DAX/Acceleration device name (chardev) that correlates with the NMEM and DIMM serial number displayed in the output in Step 11.

In the above example, where `nmem0`'s namespace is `namespace0.0`, the DAX/Acceleration device name is `dax0.0`.

16. Record the device's region, namespace and DAX device name in the NVDIMM information table.

Results

You have discovered the region, namespace and DAX device name for the storage devices that interact with the failed NVDIMM (or, in the case of a failed NVDIMM battery, all NVDIMMs mounted on the server). You can now remove these storage devices from the NVDIMM Acceleration Pool and FG Storage Pool.
Remove the storage devices from PowerFlex in a Linux-based system

Identify and remove the storage devices that interact with the failed NVDIMM or Failed NVDIMM battery from the relevant PowerFlex FG Storage Pool and Acceleration Pool in a Linux-based system.

Prerequisites

Ensure that you have the following credentials (available from the administrator):

- PowerFlex presentation server IP address or hostname, used for accessing the PowerFlex GUI.
- Admin rights for accessing the PowerFlex GUI. If necessary, the customer can give you the credentials.

About this task

NOTE: In the following task, the term "failed NVDIMM" also refers to all NVDIMMs mounted on the server in cases of a failed NVDIMM battery or failed system board.

NOTE: When replacing an NVDIMM battery, all NVDIMM devices in the node are affected. Ensure that you have performed the following steps to remove the storage devices for NVDIMMs associated with the battery.

Steps

1. From your internet browser, go to https://<Management_Server_IP_address/hostname>:<management_server_port> and log in to the PowerFlex GUI as an admin user.
   If a certificate notice is displayed, review and accept the certificate.

2. In the left pane, click Configuration > Acceleration Pools.

3. Find the Acceleration Pool associated with the failed acceleration device, and its corresponding Fine Granularity (FG) Storage Pool, SDS, and storage devices:

   a. In the right pane, click the Acceleration Pool configured for NVDIMM devices.
      A map of the Acceleration Pool’s topology appears in the Overview tab in the lower pane.

   b. In the topology map, click Devices.
      A list of devices configured to the Acceleration Pool appears in the right pane. Verify that the acceleration device associated with the failed NVDIMM is included in the list. For example, if you discovered dax0.0 in the previous step, select /dev/dax0.0 from the list of acceleration devices.

      Record the name of the Acceleration Pool, Storage Pool (displayed in the Storage Pool column), and the acceleration device in the NVDIMM information table.

   c. In the right pane, click the failed acceleration device.

   d. In the Overview tab in the lower pane, find the SDS and Protection Domain (PD) associated with the Acceleration Pool in the topology map, and then record the name of the SDS and PD in the NVDIMM information table.

   e. In the topology map, click the SDS.
      The PowerFlex GUI takes you to the SDS’s configuration page.

   f. In the right pane, click the SDS, and then in the topology map in the lower pane, click Devices under the SDS.
      The PowerFlex GUI displays the list of storage devices configured to the SDS.

   g. Record the list of storage devices in the NVDIMM information table.

   NOTE: When replacing an NVDIMM battery, repeat this step for the acceleration devices and their associated storage devices.

   The NVDIMM information table should now include the name of the Acceleration Pool, Storage Pool, Protection Domain, storage devices, and acceleration device associated with the DAX device.

4. Remove the storage devices you identified in the previous step from the relevant Storage Pool. Refer to the NVDIMM information table for the list of devices, as necessary.

   a. In the PowerFlex GUI left pane, click Configuration > Devices.

   b. In the right pane, find the devices associated with the relevant SDS and FG Storage Pool.

   c. Select the check box for every storage device you identified.

   CAUTION: Ensure that the storage devices you select are the same storage devices you listed in the NVDIMM information table.
d. In the upper-right menu click More > Remove.
e. In the Remove Device dialog box, click Remove to confirm.
f. In the pop-up window, click Dismiss.
g. In the left pane, click Dashboard. Wait until the rebuild/rebalance operation is complete and all counters are at 0.

You have removed the storage devices from the FG Storage Pool.

5. Remove the acceleration devices (DAX devices) corresponding to the failed NVDIMM from the relevant Acceleration Pool. Refer to the NVDIMM information table, as necessary.
   a. In the PowerFlex GUI left pane, click Configuration > Devices.
   b. In the right pane, find the device you recorded in the NVDIMM information table.
   c. Select the check box for every acceleration device you identified.

   CAUTION: Ensure that the acceleration devices you select are the same acceleration devices you listed in the NVDIMM information table.

   d. In the upper-right menu click More > Remove.
   e. In the Remove Device dialog box, click Remove to confirm.
   f. In the pop-up window, click Dismiss.
   g. In the left pane, click Dashboard. Wait until the rebuild/rebalance operation is complete and all counters are at 0.

6. If you are replacing the NVDIMM battery, perform the previous steps to remove the storage devices and acceleration devices associated with every NVDIMM module mounted on the server.

Results
The acceleration devices and storage devices associated with the faulty NVDIMM have been removed from the Acceleration Pool and Storage Pool.

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 device and acceleration device.

Activate devices
Activate a device that was inactivated, or that was added to a system using the Test only option.

About this task
Use the Activate Device command in the following situations:

- Storage devices were added to the system using the Test only option for Device Tests, and successfully passed the tests.
- Storage devices were inactivated, and you want to bring them back online.

Steps
1. From the PowerFlex GUI, in the left pane, click Configuration > Devices.
2. In the right pane, select the relevant device check box, and click More > Activate.
3. In the Activate Device <device name> dialog box, click Activate.
4. Verify that the operation completed successfully and click Dismiss.

Results
The device is activated.

Clear device errors
Clear device errors.

About this task
Steps
1. From the PowerFlex GUI, in the left pane, click **Configuration > Devices**.
2. In the right pane, select the relevant device check box, and click **More > Clear Errors**.
3. In the **Clear device errors on <Device name>** dialog box, click **Clear Errors**.
4. Verify that the operation completed successfully and click **Dismiss**.

Results
Errors are cleared from the device.

Volumes
You can define, configure and manage volumes in the PowerFlex system.

Add volumes
Add volumes to a system.

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

**NOTE:** For the minimum size of an SDS, see "System Requirements" in the *Getting to Know guide*.

About this task
Define volume names according to the following rules:
- Contains less than 32 characters
- Contains only alphanumeric and punctuation characters
- Is unique within the object type

PowerFlex objects are assigned a unique ID that can be used to identify the object in CLI commands. You can retrieve the ID via a query, or via the object’s property sheet in the PowerFlex GUI. It is highly recommended to give each volume a meaningful name associated with its operational role.

To add one or multiple volumes, perform these steps:

Steps
1. From the PowerFlex GUI, in the left pane, click **Configuration > Volumes**.
2. In the right pane, click **Add**.
3. In the **Add Volume** dialog box, enter the following details of the volume:
   a. Enter the number of volumes.
      - 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%1%` and the starting number value is 100, the name of the first volume created will be `Vol100`, and the second volume will be `Vol101`, and so on.
   b. Select either **Thick** (default) or **Thin** provisioning options.
   c. Enter the volume size in GB (basic allocation granularity is 8 GB) in the **Size** box.
   d. Select the Storage Pool.
4. Click **Add Volume**.
5. Verify that the operation completed successfully and click **Dismiss**.

Results
A volume is created.
Next steps

To use the created volume, you must map it to (at least) one SDC. If the restricted SDC mode is enabled for the system, you must approve SDCs prior to mapping volumes to them. For more information on approving SDCs, see "Approve SDCs using the PowerFlex GUI". For more information on mapping volumes, see "Map a volume to an SDC".

Remove volumes

Remove volumes from Storage Pools.

Prerequisites

Ensure that the volume you are removing is not mapped to any SDCs. If it is, unmap it before removing. For information, see "Unmap volumes". Also, ensure that the volume is not the source volume of any Snapshot Policy. You must first remove the volume from the Snapshot Policy before you can remove the volume.

About this task

If you want to remove a volume’s related snapshots, or just the snapshots, see "Remove Snapshots". Best practice is to avoid deleting volumes or snapshots while the MDM cluster is being upgraded, to avoid causing a Data Unavailability status.

NOTE: Removal of a volume erases all the data on the corresponding volume.

Steps

1. From the PowerFlex GUI, in the left pane, click Configuration > Volumes.
2. In the right pane, select the relevant volume check box, and click More > Remove.
3. In the Remove Volume <volume name> dialog box, verify the volumes to be removed and click Remove.
4. In the warning dialog confirming the volumes to remove, click Remove.
5. Verify that the operation completed successfully and click Dismiss.

Results

The volume is removed from the system.

Overwrite volume content

You can overwrite the contents of a volume with the content from another volume.

About this task

NOTE: If the destination volume is an auto snapshot, it must be locked before you can continue to overwrite volume content. This is also relevant to auto snapshots. You can’t overwrite a volume if it is an unlocked.

Steps

1. From the PowerFlex GUI, in the left pane, click Configuration > Volumes.
2. Select the volume and click More > Overwrite Content.
3. In the Overwrite Content of Volume <name> dialog box, in the Target Volume tab, select the target volume from which to overwrite the content of the volume and click Next.
4. In the Select Source Volume tab, select the source volume to overwrite the content and click Next.
5. In the Review tab, review the details and click Overwrite Content.
6. Verify that the operation completed successfully and click Dismiss.

Results

The content from the volume is overwritten.
Create volume snapshots

Take a snapshot of one or more volumes.

About this task

This topic describes how to take a snapshot of one or more volumes.

When specifying more than one volume (a list), a consistency group is generated by default, and can be viewed in the snapshot’s detail pane. The snapshots under the consistency group are taken simultaneously for all listed volumes, thus ensuring their consistency.

Secure snapshots prohibits anyone from deleting the snapshot until the expiration time that is defined.

You can accept the default name, or define snapshot names according to the following rules:

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

PowerFlex objects are assigned a unique ID that can be used to identify the object in CLI commands. You can retrieve the ID via a query, or via the details pane in the PowerFlex GUI.

**NOTE:**
The consistency group is for convenience purposes ONLY. There are no protection measures to conserve the consistency group. You can delete members from it.

To take a snapshot, perform these steps:

Steps

1. From the PowerFlex GUI, in the left pane, click Configuration > Volumes.
2. In the right pane, select the relevant volume check box and click More > Create Snapshot.
3. In the Create snapshot of volume <volume name> dialog box, enter the following information for the snapshot:
   a. Enter the Name of the snapshot.
   b. Enter the number in the Index that is used to append to the snapshot names.
   c. Select the Read Only check box to define permissions for the snapshot.
   d. Select the Use secure snapshot check box and enter the Expiration Time that the snapshot can not be deleted.
4. Click Create Snapshot.
5. Verify that the operation completed successfully and click Dismiss.

Results

A snapshot of the volume is created.

Remove snapshots

You can remove a volume together with its snapshots, or remove individual snapshots.

About this task

Before removing a volume or snapshots, you must ensure that they are not mapped to any SDCs. If they are, unmap them before removing them. Snapshots are unmapped in the same way as volumes are unmapped. For information, see "Unmap volumes".

Best practice is to avoid deleting volumes or snapshots while the MDM cluster is being upgraded, to avoid causing a Data Unavailability status.

**NOTE:** Removal of a volume or snapshot erases all the data on the corresponding volume or snapshot.

Steps

1. From the PowerFlex GUI, in the left pane, click Configuration > Volumes.
2. In the right pane, select the snapshot and click More > Remove.
3. In the Remove Volume <volume name> dialog box, click Remove.
4. In the Remove volume <volume name> confirmation dialog box, click Remove.
5. Verify that the operation completed successfully and click **Dismiss**.

**Results**

The snapshot is removed.

### Set volume bandwidth and IOPS limits

Set bandwidth and IOPS limits for volumes on a per-SDC basis. This enables you to control the quality of service (QoS).

**Prerequisites**

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

**About this task**

**Steps**

1. From the PowerFlex GUI, in the left pane, click **Configuration > Volumes**.
2. In the right pane, select the relevant volume check box and click **More > Set Limits**.
3. In the **Set IO limits for volume <volume name>** enter the required values for **BW Limit (MB/s)** and **IOPS Limits**, or select the corresponding **Unlimited** check box.
4. In the **Bandwidth Limits** and **IOPS Limits** boxes, type the required values, or select the corresponding **Unlimited** check box.
   - The number of IOPS must be larger than 10.
   - The volume network bandwidth is in MB/sec.
   - The IO limits are applied to every mapped SDC.
5. In the **SDC** panel, select the SDCs to which you want to apply the changes.
6. Click **Apply**.
7. Verify that the operation completed successfully and click **Dismiss**.

**Results**

IO limits are set for the volume.

### Increase a volume's 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.

**About this task**

**Steps**

1. From the PowerFlex GUI, in the left pane, click **Configuration > Volumes**.
2. In the right pane, select the volume and click **Modify > Resize**.
3. In the **Resize Volume <volume name>**, enter a number representing the new volume size in GB (basic allocation granularity is 8 GB).
4. Click **Apply**.
5. Verify that the operation completed successfully and click **Dismiss**.

**Results**

The volume size is increased.
Map volumes

Map one or more volumes to SDCs.

About this task

Mapping exposes the volume to the specified SDC, effectively creating a block device on the SDC.

For Linux devices, the scini device name can change on reboot. It is recommended to mount a mapped volume to the VxFlex Ready Node unique ID, a persistent device name, rather than to the scini device name.

To identify the unique ID, run the ls -l /dev/disk/by-id/ command. For more information, see “Associate PowerFlex volumes with physical disks”. 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 can’t map a volume if the volume is an auto snapshot that is not locked.

To map volumes, perform these steps:

Steps

1. From the PowerFlex GUI, in the left pane, click Configuration > Volumes.
2. In the right pane, select the volume check box, and then click Mapping > Map.
3. In the Map Volume dialog box, select one or more SDCs to which you want to map the volumes.
4. Click Map and then click Apply.
5. Verify that the operation completed successfully and click Dismiss.

Results

The volume is mapped to the selected SDC.

Unmap volumes

Unmap one or more volumes from SDCs.

Steps

1. From the PowerFlex GUI, in the left pane, click Configuration > Volumes.
2. In the right pane, select the volume check box, and then click Mapping > Unmap.
3. From the Unmap dialog box, select the SDC to unmap and click Unmap.
4. Verify that the operation completed successfully and click Dismiss.

Results

The volume is unmapped from the selected SDC.

Remove a snapshot consistency group

Remove a consistency group with all its snapshots using the PowerFlex GUI.

About this task

NOTE: You can’t remove the consistency group if it contains auto snapshots.

Steps

1. From the PowerFlex GUI, in the left pane, click Configuration > Volumes.
2. In the right pane, select the relevant snapshot check box, and then in the Details pane, click the Consistency Group tab.
3. Click Remove CG.
4. In the Remove <snapshot name> CG dialog box, click Remove CG.
5. Verify that the operation completed successfully and click Dismiss.
Results

The snapshot consistency group is removed.

**Migrating V-Trees**

Migrating a V-Tree allows you to move the V-Tree to a different Storage Pool.

Migrating a V-Tree frees up capacity in the source Storage Pool. For example, from an HDD Storage Pool to an SSD Storage Pool or different attributes (for example, from thin to thick). For more information, see "Volume Tree" in the Getting to Know Guide.

There are several motives for migrating a V-Tree to a different Storage Pool:

- In order to move the volumes to a Storage Pool with a different performance tier
- 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
- In order to move the volumes from a Medium Granularity Storage Pool to a Fine Granularity Storage Pool
- To clear a Protection Domain for maintenance and then return the volumes to it

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

**NOTE:** You cannot create snapshots when migrating from a Medium Granularity Storage Pool to a Fine Granularity Storage Pool.

When the user requests a V-Tree migration, the MDM first estimates whether the destination Storage Pool has enough capacity for the migration to complete successfully. The MDM bases the estimation on its information of the current capacity of the V-Tree. 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 hold onto source capacity once it has been migrated, but releases it immediately.

Use the following table to understand which V-Tree migrations are possible and under what specific conditions:

V-Tree migration can take a long time, depending on the size of the V-Tree and the system workload. During migration, the V-Tree is fully available for user I/O. V-Tree 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 V-Tree 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 (GoS). The default favors applications with one concurrent I/O and 10 MB/sec per device. Increasing the 10 MB/sec 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. For more information on zero padding, see "Storage Pools" in the Getting to Know Guide.

You can pause a V-Tree 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 resume the V-Tree migration, or to roll back the migration and have all volume blocks returned to the original Storage Pool.

V-Tree migration can 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 V-Tree 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.

Prerequisites

Note the following limitations:

- vTree migration is a long process and can take days or weeks, depending on the vTree's size.
- Migration between Storage Pools of different data layouts is only allowed if there is a single volume in the vTree. (If you manually created a snapshot, the vTree cannot be migrated).
- You cannot migrate a volume that is a source volume of a Snapshot Policy between Storage Pools of different data layouts.
- Volumes involved in replication cannot be migrated.
- Volumes involved in replication cannot be migrated.

Steps

1. From the PowerFlex GUI, in the left pane, click Configuration > Volumes.
2. In the right pane, select the relevant volume check box, and then in the Details pane, click the vTree tab.
3. Click the vTree button and select Migrate vTree.
4. In the Migrate vTree of <volume name> dialog box, 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.
5. Optionally, expand Advanced to select one or several of the following advanced options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add migration at the head of the migration queue</td>
<td>Give this vTree migration the highest priority in the migration priority queue.</td>
</tr>
<tr>
<td>Ignore destination capacity</td>
<td>Allow the migration to start regardless of whether there is enough capacity at the destination.</td>
</tr>
<tr>
<td>Enable compression</td>
<td>Compression is done by applying a compression-algorithm to the data. For more information on compression mode, see &quot;V-Trees&quot; in the Getting to Know guide.</td>
</tr>
<tr>
<td>Convert vTree from...</td>
<td>Convert a thin-provisioned vTree to thick-provisioned, or vice-versa, at the destination, depending on the provisioning of the source volume.</td>
</tr>
</tbody>
</table>

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 rebooting the SDC. The SDC
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save current vTree provisioning state during migration</td>
<td>The provisioning state is returned to its original state before the migration took place.</td>
</tr>
</tbody>
</table>

6. Click **Migrate VTree**.
7. From the top right, click the **Running Jobs** icon and check the progress of the migration of the Vtree.
8. Verify that the operation completed successfully and click **Dismiss**.

**Results**
The vTree migration is initiated and the vTree appears in both the source and the destination Storage Pools.

**Pause vTree migration**
You can pause a vTree migration at any time.

**About this task**
The following ways are used to pause the vTree migration:

- Gracefully: To allow all data blocks currently being migrated to finish migration before pausing.
- Forcefully: To abort the migration of all blocks currently in progress and carries a potential risk to data.

**Steps**
1. From the PowerFlex GUI, in the left pane, click **Configuration > Volumes**.
2. In the right pane, select the relevant volume check box, and then in the **Details** pane, click the **vTree** tab.
3. Click the **vTree** button and select **Pause migration**.
4. In the **Volume <volume name> Pause VTree Migration** dialog box, select whether you want to pause gracefully or forcefully and click **Pause Migration**.
   
   If you selected to pause the migration gracefully, the migration icon is colored blue until the migration pauses successfully. A gray migration icon indicates that the migration is paused. Once paused, you can choose to roll back the vTree migration or resume the vTree migration from the Command menu.
5. Verify that the operation completed successfully and click **Dismiss**.

**Results**
Volume migration is paused. Once paused, you can choose to roll back the vTree migration or resume the vTree migration from the vTree menu.

**Roll back V-Tree migration**
You can roll back to the source Storage Pool.

**About this task**
When a V-Tree migration is paused, you can roll back the migration so that the volume and all of its snapshots are returned to the source Storage Pool.

**Steps**
1. From the PowerFlex GUI, in the left pane, click **Configuration > Volumes**.
2. In the right pane, select the relevant volume check box, and then in the **Details** pane, click the **vTree** tab.
3. Click the **vTree** button and select **Rollback migration**.
4. In the **Volume <volume name> Rollback VTree Migration** dialog box, verify the source and target for the rollback and click **Rollback Migration**.
5. Verify that the operation completed successfully and click **Dismiss**.
Results
The migration resumes in the reverse direction so that any data already migrated to the destination Storage Pool is now migrating to the source Storage Pool.

Set vTree migration priority
Set the priority of a vTree migration to be at the head or the tail of the migration queue.

About this task

Steps

1. From the PowerFlex GUI, in the left pane, click Configuration > Volumes.
2. In the right pane, select the relevant volume check box, and then in the Details pane, click the vTree tab.
3. Click the vTree button and select Set Priority.
4. In the Volume <volume name> Set VTree Migration Policy dialog box, select whether to move the current vTree migration to the head or the tail of the migration queue and click Set Priority.
5. Verify that the operation completed successfully and click Dismiss.

Results
The priority of the migration is set.

Volumes in the vSphere environment
The following topics describe how to use the PowerFlex plug-in to add, map, and unmap volumes in the vSphere environment. You can map volumes to SDCs in the same step, or you can map the volume after it has been created.

Create and map volumes

About this task
Volumes are created from devices in a Storage Pool.

Steps

1. From the Storage Pools screen, click Actions > Create volume.
   The Create Volume dialog appears.
2. Enter the following information:
   - Volume name: Enter a name for the new volume.
   - Number of volumes to create: Enter the number of volumes to create. Multiple volumes appear as volume_name-X.
   - Volume size: Enter the size of the volume. This must be in multiples of 8 GB.
   - Volume provisioning: Select thick or thin provisioning.
   - Use RAM Read Cache: Select to enable RAM Read Cache for the created volumes. Use of RAM Read Cache is determined by the policy for the Storage Pool and the volume.
   - Obfuscation: Select whether the volume should be obfuscated.
3. To map the volume to ESXs, perform the following steps:
   a. Select Map volume to ESXs.
   b. In the Select ESXs area, select the clusters or ESXs to which this volume should be mapped.
   c. Click OK.
   d. Enter the password for the PowerFlex administrative user.
      The following figure illustrates multiple volumes created:
Map volumes

About this task
Manually map volumes after they have been created, from the Volumes screen.

Steps
1. From the Volumes screen, select a volume to map, then choose Actions > Map a volume.
2. In the Map Volume to ESXs dialog box, select the clusters or ESXis to which this volume should be mapped.
3. To configure the LUN identifier manually, select Manually configure LUN identifier to and enter the identifier ID.
4. Click OK.

Unmap a volume

About this task
You can use the PowerFlex plug-in to unmap a volume from an ESXi.

Steps
1. From the Volumes screen, select the volume to unmap, and click Actions > Unmap volume.
2. In the Unmap Volume from ESXis dialog box, select the ESXis or clusters from which to unmap the volume, then click OK.

Configuring SDCs

This section describes how to map an SDC to a volume, how to set the SDC restriction mode and how to approve SDCs before mapping volumes.

Manual SDC configuration/verification

If there are problems connecting to a PowerFlex system after a reboot, users can modify the drv_cfg.txt file or use the drv_cfg utility to ensure that the SDC reconnects to the MDM automatically upon node restart/reboot.

To do this, perform one of the following procedures:

- Edit /bin/emc/scaleio/drv_cfg.txt and change the #MDM line to include each IP address for any node(s) containing an MDM in your cluster.

  For example, change the line:

  From:
  #mdm 10.20.30.40
  To:
  mdm 10.108.158.48,10.108.158.49

  where .48 is the master node, and .49 is the slave node. The Tie-Breaker node should not be included.
Configure approved SDC IP addresses using the PowerFlex GUI

When the system's restricted SDC mode is set to approved IP restriction, you must configure SDC IP addresses before you can map volumes.

Prerequisites
Ensure that the SDCs have been approved by GUID.

Steps
1. From the PowerFlex GUI, in the left pane, click Configuration > SDCs.
2. In the right pane, select the relevant SDC check box, and click Modify > Modify Approved IP Addresses.
3. In the SDC <SDC name> Modify IP addresses dialog box, add the IP addresses of the SDCs you want to approve and click Add IP Address.
   You can add up to a total of four IP addresses.
4. Click Apply.
5. Verify that the operation completed successfully and click Dismiss.

Results
The SDC IP addresses are approved and you can map volumes.

Approve SDCs using the PowerFlex GUI

When the system's restricted SDC mode is set to GUID restriction, you must approve SDCs before you can map volumes.

Steps
1. From the PowerFlex GUI, in the left pane, click Configuration > SDCs.
2. In the right pane, select one or several SDCs that you want to approve and click More > Approve.
3. In the Approve SDC <SDC name> dialog box, verify that the SDCs listed are the ones you want to approve and click Approve.
4. Verify that the operation completed successfully and click Dismiss.

Results
The SDCs are approved and you can map volumes.

Restricted SDC mode

Enabling restricted SDC mode gives you more control over PowerFlex.

Restricted SDC mode is set at the system level. When enabled, you must approve SDCs prior to mapping volumes to them. The restricted SDC setting has the following modes:

- No restriction — Volumes can be mapped without pre-approving SDCs.
- GUID restriction — SDCs are approved using their GUID. Only once the SDC is approved can it be used for mapping volumes.
- Approved IP restriction — SDCs must be approved using their GUID and IP address. Only once the SDC is approved using both GUID and IP address can it be used for mapping volumes.

You can set the restricted SDC mode using the CLI, or REST API.

**NOTE:** In a system that has been upgraded and already has volumes mapped to SDCs, if you want to enable restricted SDC mode, you must first approve the SDCs and only then enable restricted SDC mode.
Add an external SDC to an existing PowerFlex system

You can add an external SDC to an existing PowerFlex system.

During manual installation, you can install the SDC according to the operating system-specific instructions in the following section, and it will be connected to the existing PowerFlex system.

Install the SDC on an ESXi server and connect it to PowerFlex using esxcli

Install the SDC with the appropriate parameters to connect it to an existing PowerFlex system. This procedure is relevant both for adding more SDCs to an existing system, and for adding SDCs to a two-layer system during initial deployment activities.

Prerequisites

Ensure that you have:

- The virtual IP address or MDM IP address of the existing system. If an MDM virtual IP address is not in use, obtain the IP addresses of all the MDM managers.
- Login credentials for the intended SDC host
- The required installation software package for your SDC's operating system (available from the zipped software packages that can be downloaded from the Customer Support site)
- A GUID string for the SDC. These strings can be generated by tools that are freely available online. The GUID needs to conform to OSF DCE 1.1. The expected format is xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx where each x can be a digit (0–9) or a letter (a–f).

About this task

The following procedure explains how to manually install an external SDC on an ESXi server using esxcli in command line.

**NOTE:** This procedure requires two server reboots.

**Steps**

1. On the ESXi on which you are installing the SDC, set the acceptance level:

   ```
   esxcli --server=<SERVER_NAME> software acceptance set --level=PartnerSupported
   ```

   where `<SERVER_NAME>` is the ESXi on which you are installing the SDC.

2. Install the SDC:

   **Option** | **Description**
   --- | ---
   **ESXi 6.x** | `esxcli software vib install -d <full_path_to_offline_bundle>`
   where `<full_path_to_offline_bundle>` is the absolute path to the SDC VIB file.
   **NOTE:** The SDC offline ESXi 6.0 bundle is the same for all ESXi 6.x versions.
   **ESXi 7** | `esxcli software component apply -d <path_to_zip> -n scaleio-sdc-esx7`
   where `<path_to_zip>` is the path to the SDC zip file.

3. Get permission to reboot the ESXi server, and perform a graceful reboot cycle to load the SDC driver on the server.

   In a first-time install, the SDC will not automatically boot up at this point. Further configuration and an additional reboot are required, as described in this procedure.

4. Set the IP address of the MDM:

   ```
   esxcli system module parameters set -m scini -p "IocctlIniGuidStr=<XXXXXX>
   IocctlMdmIPStr=<LIST_VIP_MDM_IPS> IocctlMdmPasswordStr=<ip>-><password>"
   ```

   where
   
   - `<LIST_VIP_MDM_IPS>` is a comma-separated list of the MDM IP addresses or the virtual IP address of the MDM
Separate the IP addresses of the same MDM cluster with a "," symbol.
Separate multiple MDM clusters with the "+" symbol.

In the following example, there are two MDM clusters. The first has two IP addresses and the second has only one:

10.20.30.40,50.60.70.80+11.22.33.44

- `<XXXXXX>` is the user-generated GUID string. Example GUID: 12345678-90AB-CDEF-1234-567890ABCDEF

**NOTE:** Include the IP addresses of as many potential manager MDMs as possible at this time, to make it easier to switch MDMs in the future. You can add a total of eight IP addresses.
- Optional: loctMdmPasswordStr is used for SDC authentication to the MDM for access. PowerFlex.

5. Back up the parameters:

```
/bin/auto-backup.sh
```

6. Perform another graceful reboot cycle.

7. Ensure that the driver is loaded:

```
vmkload_mod -l | grep scini
```

Output similar to the following indicates that the driver is loaded:

```
scini 2 808
```

The SDC component is installed on the ESXi host.

**Results**
The SDC is installed on the ESXi server and is connected to PowerFlex.

**Next steps**
In newly deployed systems, perform the post-deployment tasks described in this guide.
In existing systems, map volumes to the new SDCs that you added to the system.

### Install SDC on a Linux server and connect it to PowerFlex

Install the SDC with the appropriate parameters to connect it to an existing PowerFlex system. This procedure is relevant both for adding more SDCs to an existing system, and for adding SDCs to a two-layer system when deploying a new system.

**Prerequisites**
Ensure that you have:
- The virtual IP address or MDM IP address of the existing system. If an MDM virtual IP address is not in use, obtain the IP addresses of all the MDM managers.
- Login credentials for the intended SDC host
- The required installation software package for your SDC’s operating system (available from the zipped software packages that can be downloaded from the Customer Support site)

**About this task**
The following procedure explains how to manually install an external SDC on a Linux server. On most servers (with the exception of hLinux), you can install the external SDC using the PowerFlex Installer. For more information about adding components to an existing system, see the Deploy PowerFlex Guide.

The steps in the procedure below are relevant for Linux RHEL/CentOS/Oracle Linux operating systems. Deployment on other operating systems require the modifications described in the following table:

<table>
<thead>
<tr>
<th>OS</th>
<th>Modifications required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubuntu/hLinux/OL</td>
<td>Before installing PowerFlex, ensure that you have followed the required preparation procedures relating to various types of Linux operating systems.</td>
</tr>
<tr>
<td></td>
<td>- PowerFlex component packages are delivered as TAR files. Before installing, perform the following:</td>
</tr>
</tbody>
</table>
## Modifications required

<table>
<thead>
<tr>
<th>OS</th>
<th>Modifications required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Untar all the packages: <code>tar -xvf &lt;tar_file&gt;</code>&lt;br&gt;This yields SIOB files.</td>
</tr>
<tr>
<td></td>
<td>2. Extract the DEB from the SIOB files: <code>siob_extract &lt;siob_file&gt;</code></td>
</tr>
<tr>
<td></td>
<td>3. The DEB file is in the following format: <code>EMC-ScaleIO-mdm-3.5-X.&lt;build&gt;..&lt;operating_system&gt;.X.X.x86_64.deb</code>&lt;br&gt;You will use the extracted DEB files for the installation.&lt;br&gt;• Some commands are a bit different, noted where applicable.</td>
</tr>
</tbody>
</table>
| CoreOS              | Before installing PowerFlex, ensure that you have followed the required preparation procedures relating to various types of Linux operating systems.  
|                     | • PowerFlex component CoreOS packages are delivered as TAR files. Before installing, perform the following:  
|                     | 1. Untar all the packages: `tar -xvf <tar_file>`<br>This yields SIOB files.            |
|                     | 2. Extract the BSX from the SIOB files: `siob_extract <siob_file>`                     |
|                     | 3. The BSX file is in the following format: `EMC-ScaleIO-mdm-3.5-X.<build>.CoreOS.x86_64.bsx`<br>You will use the extracted BSX files for the installation.<br>• Some commands are a bit different, noted where applicable. |

## Steps

1. Install the GPG key on every server on which SDC will be installed. From the PowerFlex installation folder, run the following command on every server:

   ```
   rpm --import RPM-GPG-KEY-ScaleIO
   ```

2. In command line, install the SDC:
   - RHEL/CentOS /Oracle Linux
     ```
     MDM_IP=<LIST_VIP_MDM_IPS> rpm -i <SDC_PATH>.rpm
     ```
   - Ubuntu/hLinux. These files must be extracted before use, as described above.
     ```
     MDM_IP=<LIST_VIP_MDM_IPS> dpkg -i <SDC_PATH>.deb
     ```
   - CoreOS
     ```
     MDM_IP=<LIST_VIP_MDM_IPS> ./<LIST_VIP_MDM_IPS>.bsx
     ```

   where  
   - `<LIST_VIP_MDM_IPS>` is a comma-separated list of the MDM IP addresses or the virtual IP address of the MDM  
   - `<SDC_PATH>` is the path where the SDC installation package is located

## Results

The SDC is installed on the Linux server and is connected to PowerFlex.

## Next steps

In newly deployed systems, perform the post-deployment tasks described in this guide.  
In existing systems, map volumes to the new SDCs that you added to the system.
Install SDC on an AIX server and connect it to PowerFlex

Install the SDC with the appropriate parameters to connect it to an existing PowerFlex system. These instructions are relevant both for adding more SDCs to an existing system, and for adding SDCs to a two-layer system when deploying a new system.

Prerequisites
Ensure that you have:

- The virtual IP address or MDM IP address of the existing system. If an MDM virtual IP address is not in use, obtain the IP addresses of all the MDM managers.
- Login credentials for the intended SDC host
- The required installation software package for your SDC's operating system (available from the zipped software packages that can be downloaded from the Customer Support site)

About this task
The following procedure explains how to manually install an external SDC on an AIX server. The PowerFlex Installer cannot be used.

Steps
1. In command line, install the SDC:

   ```
   MDM_IP=<LIST_VIP_MDM_IPS> rpm -i <SDC_PATH>.rpm
   ```

   where
   - `<LIST_VIP_MDM_IPS>` is a comma-separated list of the MDM IP addresses or the virtual IP address of the MDM.
   - `<SDC_PATH>` is the path where the SDC installation package is located.

   The SDC package is in a format similar to this: `EMC-ScaleIO-sdc-3.5-X.<build>.aix7.aix7.2.ppc.rpm`

2. Optional: For SDC authentication to the MDM for access, in the command line, enter:

   ```
   chdev -l scini -a "mdm_password=<ip>-<password>"
   ```

Results
The SDC is installed on the AIX server and is connected to PowerFlex.

Next steps
In newly deployed systems, perform the recommended post-deployment tasks described in this guide.
In existing systems, map volumes to the new SDCs that you added to the system.

Install SDC on a Windows server and connect it to PowerFlex

Install the SDC with the appropriate parameters to connect it to an existing PowerFlex system. This procedure is relevant both for adding more SDCs to an existing system, and for adding SDCs to a two-layer system when deploying a new system.

Prerequisites
Ensure that you have:

- The virtual IP address or MDM IP address of the existing system. If an MDM virtual IP address is not in use, obtain the IP addresses of all the MDM managers.
- Login credentials for the intended SDC host
- The required installation software package for your SDC's operating system (available from the zipped software packages that can be downloaded from the Customer Support site)

About this task
The following procedure explains how to manually install an external SDC on a Windows server. Alternatively, you can install the external SDC using the PowerFlex Installer. For more information about adding system components to an existing system, see the Configure and Customize PowerFlex Guide.
Steps
1. On the Windows server on which you are installing the SDC, run the following command in command line:

   msiexec /i <SDC_PATH>.msi MDM_IP=<LIST_VIP_MDM_IPS>

   where
   - <SDC_PATH> is the path where the SDC installation package is located
   - <LIST_VIP_MDM_IPS> is a comma-separated list of the MDM IP addresses or the virtual IP address of the MDM

2. Get permission to reboot the Windows server, and perform a reboot to load the SDC driver on the server.

Results
The SDC is installed on the Windows server and is connected to PowerFlex.

Next steps
In newly deployed systems, perform the post-deployment tasks described in this guide.
In existing systems, map volumes to the new SDCs that you added to the system.

SDC operations
Many SDC operations use drv_cfg. The drv_cfg command line is a local CLI utility that affects only the client on which the SDC is running. Possible SDC operations include updating the SDC driver with IP changes, detecting new volumes, querying volumes, loading a configuration file, adding an MDM, modifying an MDM IP address, enabling support of PDL state, and more.

Update the SDC driver with IP address changes
Steps
1. Edit drv_cfg.txt and change the IP address in the last line to the new IP address.

   Location of drv_cfg.txt:
   - Linux: /etc/emc/scaleio/
   - Windows: In the following registry key - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\scini\Parameters\mdms

   NOTE: On ESXi, GUID and MDM lists are stored as module parameters, and not in a drv_cfg.txt file. To modify these parameters, use esxcli commands.

2. Save and close the file.
3. Type the following command:

   /etc/init.d/scini restart

   NOTE: ESXi guidelines described in the PowerFlex plug-in chapter.

Detecting new volumes
Command

drv_cfg --rescan

NOTE:
This is not a CLI command, but rather an executable that is run on the SDC server.

**Syntax**

```
/opt/emc/scaleio/sdc/bin/drv_cfg --rescan
```

**Description/Notes**

Volumes are always exposed to the operating system as devices with the prefix `scini` (such as `/dev/scinia`, `/dev/scinib` and so on). Unique names can be found under `/dev/disk/by-id/`.

PowerFlex periodically scans the system to detect new volumes. You can initiate a scan for the most up-to-date status on a particular SDC node. This command is unique because it is not a CLI command, but rather a command issued on the specific SDC.

Location of `drv_cfg` command:

- Linux: `/opt/emc/scaleio/sdc/bin/drv_cfg`
- Windows: `C:\Program Files\emc\scaleio\sdc\bin\drv_cfg`
- ESXi: refer to the vSphere Client VMware guidelines on how to detect new storage. If troubleshooting is needed, contact customer support.

For further details on how to set the mounting options see "Mount PowerFlex".

---

### Query volumes using `drv_cfg`

**Command**

```
drv_cfg --query_vols
```

**Syntax**

```
/opt/emc/scaleio/sdc/bin/drv_cfg --query_vols
```

**Description/Notes**

This utility retrieves information about all known active volume objects in kernel mode. You can use this utility to determine which volumes are mapped, and the ID of each volume in PowerFlex.

Location of `drv_cfg` command:

- Linux: `/opt/emc/scaleio/sdc/bin/drv_cfg`
- Windows: `C:\Program Files\emc\scaleio\sdc\bin\drv_cfg`
- ESXi: Refer to "Update the SDC parameters in VMware based HCI or Compute node".

**Example**

```
/opt/emc/scaleio/sdc/bin/drv_cfg --query_vols
```

---

### Query tgt objects using `drv_cfg`

**Command**

```
drv_cfg --query_tgts
```

**Syntax**

```
/opt/emc/scaleio/sdc/bin/drv_cfg --query_tgts
```

**Description/Notes**

This utility retrieves information about all known active volume objects in kernel mode. You can use this utility to determine which volumes are mapped, and the ID of each volume in PowerFlex.

Location of `drv_cfg` command:

- Linux: `/opt/emc/scaleio/sdc/bin/drv_cfg`
- Windows: `C:\Program Files\emc\scaleio\sdc\bin\drv_cfg`
- ESXi: Refer to "Update the SDC parameters in VMware based HCI or Compute node".

**Example**

```
/opt/emc/scaleio/sdc/bin/drv_cfg --query_tgts
```
Syntax

```
/opt/emc/scaleio/sdc/bin/drv_cfg --query_tgts
```

Description/Notes
This utility retrieves information about all known active tgt objects (SDSs) in kernel mode.

Location of `drv_cfg` command:
- Linux: `/opt/emc/scaleio/sdc/bin/drv_cfg`
- Windows: `C:\Program Files\emc\scaleio\sdc\bin\drv_cfg`
- ESXi: Refer to "Update the SDC parameters in VMware based HCI or Compute node".

Example

```
/opt/emc/scaleio/sdc/bin/drv_cfg --query_tgts
```

Query GUID using `drv_cfg`

Command

```
drv_cfg --query_guid
```

**NOTE:**
This is not a CLI command, but rather an executable that is run on the SDC server.

Syntax

```
/opt/emc/scaleio/sdc/bin/drv_cfg --query_guid
```

Description/Notes
This utility retrieves the unique ID of the kernel module. The utility can be used to verify that all SDC GUIDs in the system are unique.

Location of `drv_cfg` command:
- Linux: `/opt/emc/scaleio/sdc/bin/drv_cfg`
- Windows: `C:\Program Files\emc\scaleio\sdc\bin\drv_cfg`
- ESXi: Refer to "Update the SDC parameters in VMware based HCI or Compute node".

**NOTE:**
If the SDC was removed and reinstalled, the GUID of the SDC will be different to its original GUID. In such a case, you may need to remove the SDC, if two SDCs now have the same GUID.

Example

```
/opt/emc/scaleio/sdc/bin/drv_cfg --query_guid
```

Query MDMs using `drv_cfg`

Command

```
drv_cfg --query_mdms
```

**NOTE:**
This is not a CLI command, but rather an executable that is run on the SDC server.
Syntax

/opt/emc/scaleio/sdc/bin/drv_cfg --query_mdms

Description/Notes

This utility retrieves information about all known MDM objects in kernel mode. This utility is typically used to determine to which MDM an SDC is connected.

Location of drv_cfg command:

- Linux: /opt/emc/scaleio/sdc/bin/drv_cfg
- Windows: C:\Program Files\emc\scaleio\sdc\bin\drv_cfg
- ESXi: Refer to "Update the SDC parameters in VMware based HCI or Compute node".

Example

/opt/emc/scaleio/sdc/bin/drv_cfg --query_mdms

Loading a configuration file using drv_cfg

Command

drv_cfg --load_cfg_file

NOTE:

This is not a CLI command, but rather an executable that is run on the SDC server.
This command can not be used on ESXi servers. Instead, follow the steps described in "Modify parameters on ESXi servers".

Syntax

/opt/emc/scaleio/sdc/bin/drv_cfg
--load_cfg_file <FILE_NAME>

Description/Notes

This utility reads a configuration file containing MDM IP addresses, and calls the kernel to connect to them.

Location of drv_cfg command:

- Linux: /opt/emc/scaleio/sdc/bin/drv_cfg
- Windows: C:\Program Files\emc\scaleio\sdc\bin\drv_cfg
- ESXi: Refer to "Update the SDC parameters in VMware based HCI or Compute node".

The configuration file that is loaded when using the drv_cfg --load_cfg_file utility is not persistent; when you restart the SDC, the changes will be lost.

To make the changes persistent, perform either of the following:

- Install the SDC on every server that will expose PowerFlex volumes to the application running, by executing the following command:

  MDM_IP=<IP of the MDM> rpm -i <full rpm file path>

- Use the following drv_cfg command:

  /opt/emc/scaleio/sdc/bin/drv_cfg --mod_mdm_ip
  --ip <EXISTING_MDM_IP_ADDRESS> --new_mdm_ip <NEW_MDM_IP_ADDRESSES>
Adding an MDM using `drv_cfg`

**Command**

```bash
drv_cfg --add_mdm
```

**NOTE:**

This is not a CLI command, but rather an executable that is run on the SDC server.
This command can not be used on ESX servers.

**Syntax**

```bash
/opt/emc/scaleio/sdc/bin/drv_cfg --add_mdm
--ip <MDM_IP_ADDRESS_LIST>
```

**Description/Notes**

This utility calls the kernel module to connect to an MDM. This command is typically used in cases where an SDC is connected to more than one PowerFlex system.

Location of `drv_cfg` command:

- **Linux:** /opt/emc/scaleio/sdc/bin/drv_cfg
- **Windows:** C:\Program Files\emc\scaleio\sdc\bin\drv_cfg
- **ESXi:** Refer to "Update the SDC parameters in VMware based HCI or Compute node".

**NOTE:**

Extending your PowerFlex system with another MDM requires that you update all SDCs in your system with the new MDM IP address. Run the `drv_cfg` utility with the `--mod_mdm_ip` option (see "Modifying an MDM IP address using `drv_cfg"), and to make the change persistent, use the `--file` parameter. In addition, any additional objects or systems which interface with the MDM must also be updated. For more information, see "Modifying an MDM's management IP address" in the PowerFlex CLI Reference Guide.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--ip &lt;MDM_IP_ADDRESS_LIST&gt;</code></td>
<td>List of IP addresses (comma delimited) for this Master or Slave MDM</td>
</tr>
<tr>
<td>Optional:</td>
<td></td>
</tr>
<tr>
<td><code>--file &lt;CONFIG_FILE_NAME&gt;</code></td>
<td>Name of the configuration file to which the MDM information should be written</td>
</tr>
<tr>
<td><code>--only_cfg</code></td>
<td>Do not call the kernel to actually connect</td>
</tr>
</tbody>
</table>

**Example**

```bash
/opt/emc/scaleio/sdc/bin/drv_cfg --add_mdm
--ip 10.100.22.20,10.100.22.30
--file /etc/emc/scaleio/drv_cfg.txt
```
Modifying an MDM IP address using drv_cfg

Command
drv_cfg --mod_mdm_ip

NOTE:
This is not a CLI command, but rather an executable that is run on the SDC server. This command can not be used on ESX servers. Instead, follow the steps described in "Modify parameters in ESXi servers".

Syntax

```
/opt/emc/scaleio/sdc/bin/drv_cfg --mod_mdm_ip
--ip <EXISTING_MDM_IP_ADDRESS>
--new_mdm_ip <NEW_MDM_IP_ADDRESSES> [--file <CONFIG_FILE_NAME>] ["-n" | "only_cfg"]
```

Description/Notes

This utility calls the kernel to modify an MDM’s IP address list. It is typically used in cases when an MDM IP address has changed, or when MDMs are added/removed from/to the system. The command must be run on every SDC in the system. To bring the changes into effect, a server restart is required.

Location of drv_cfg command:
- Linux: /opt/emc/scaleio/sdc/bin/drv_cfg
- Windows: C:\Program Files\emc\scaleio\sdc\bin\drv_cfg
- ESXi: Refer to "Update the SDC parameters in VMware based HCI or Compute node".

NOTE:
Extending your PowerFlex system with another MDM requires that you update all SDCs in your system with the new MDM IP address.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--ip &lt;EXISTING_MDM_IP_ADDRESS&gt;</td>
<td>One of the existing MDM IP addresses</td>
</tr>
<tr>
<td>--new_mdm_ip &lt;NEW_MDM_IP_ADDRESSES&gt;</td>
<td>The new IP address list (comma delimited) for this MDM. If you want to retain the existing address(es), include them in this list.</td>
</tr>
</tbody>
</table>

Optional:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--file &lt;CONFIG_FILE_NAME&gt;</td>
<td>The name of the configuration file to which the MDM information should be written</td>
</tr>
<tr>
<td>--only_cfg</td>
<td>Do not call the kernel to actually connect</td>
</tr>
</tbody>
</table>

Example

```
/opt/emc/scaleio/sdc/bin/drv_cfg --mod_mdm_ip
--ip 10.100.20.20
--new_mdm_ip 10.100.20.20,10.100.20.30,10.100.20.40
```

Permanent Device Loss state

When the MDM has disconnected from the SDC and a volume mapped to this SDC has experienced an I/O error, the ESXi host continuously sends I/Os to the device to determine if the device has become accessible. This can subsequently cause a high I/O-error load that can lead to the host freezing. In cases where the device is disconnected long-term, such as when the entire MDM cluster is down during a network upgrade, the SDC can change the volume state to Permanent Device Loss (PDL) to prevent more I/O errors coming from the ESXi.
PDL is an ESXi state, which, once enabled, is supported in PowerFlex. Once the ESXi host loses connectivity with a device, if a timeout value is reached, the ESXi will be notified that the device is in a PDL state. The timeout value can be manually set. Once a device is in a PDL state, the ESXi host no longer attempts to re-establish connectivity or issue commands to the device.

Recovering a device from PDL state is described in the VMware documentation for your operating system version. The following link is for ESXi v6.5: https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.storage.doc/GUID-A513D44C-71DE-47ED-B781-327F78659404.html

Use the instructions that match your environment.

**Enabling support of PDL state on the ESXi**

Enable support of Permanent Device Loss (PDL) state on the ESXi host.

**Steps**

1. On the ESXi host:

   ```
   esxcli system module parameters set -m scini "<<PREVIOUS_MODULE_PARAMS>>
   bBlkDevIsPdlActive=1 blkDevPdlTimeoutMillis=<TIMEOUT_VALUE>"
   ```

   where:
   - `<<PREVIOUS_MODULE_PARAMS>>` is any previous module parameters being used for this ESXi host.
   - `<TIMEOUT_VALUE>` is the timeout time in milliseconds. Its value can be 1000-3600000 (default is 60000) and including it in the command is optional.

2. Reboot the host.

**Disabling support of PDL state on the ESXi**

Disable support of Permanent Device Loss (PDL) state on the ESXi host.

**Steps**

1. On the ESXi host:

   ```
   esxcli system module parameters set -m scini "<<PREVIOUS_MODULE_PARAMS>>
   bBlkDevIsPdlActive=0"
   ```

   where `<<PREVIOUS_MODULE_PARAMS>>` is any previous module parameters being used for this ESXi host.

2. Reboot the host.

**Update the SDC parameters in VMware based HCI or compute node**

Update the SDC parameters to maintain SDC-MDM communication.

**About this task**

This procedure describes how to use the VMware plug-in to update the SDCs that are needed to maintain SDC-MDM communication.

**Steps**

1. From the plug-in **Advanced tasks** menu, click **Update SDC parameters**, and follow instructions to complete the process.
2. Check that the SDC parameters were updated by running this command on each ESXi:

   ```
   cat /etc/vmware/esx.conf |grep scini|grep -i mdm
   ```

**Run the SDC driver on SLES12.2 with multipath enabled**

Run the SDC driver on SLES12.2 with multipath enabled.

**Steps**

1. On the SLES machine where the SDC is running, open `/etc/udev/rules.d/20-scini.rules` for editing
2. In the first line at the end add:

```plaintext
ENV{ID_WWN}="%c"
```

The line should read like this:

```plaintext
KERNEL=="scini*[!0-9]", SUBSYSTEM=="block", PROGRAM="/bin/emc/scaleio/drv_cfg --query_block_device_id --block_device $tempnode", SYMLINK+="disk/by-id/emc-vol-%c", ENV{ID_BUS}="scsi", ENV{ID_SERIAL}="%c", ENV{ID_WWN}="%c"
```

3. Open `/etc/multipath.conf` and add the following:

```plaintext
defaults {
  retain_attached_hw_handler "no"
}
```

This option is turned off by default on RHEL 7.x

4. From the command line, run `dracut -f`.
   This includes the changes in initrd.

5. Restart the system.

### SDC authentication

This feature ensures security by enforcing password-based authentication of the SDC to the MDM for access to mapped volumes. This prevents the SDC from accessing unauthorized volumes.

#### Prerequisites

Enable SDC authentication according to the following rules:
- v3.5 must be installed on the SDC
- For each SDC, a password is generated in the MDM
- All SDCs must be configured with their generated passwords

#### About this task

**NOTE:** Access to an SDS does not grant access to the volumes maintained by the SDS unless they are explicitly mapped to the SDC.

This procedure describes how to enable SDC authentication.

#### Steps

1. Get the password for SDC from the MDM using the command:

   ```bash
   scli --generate_sdc_password --(sdc_id <ID> | sdc_name <NAME> | sdc_guid <GUID> | sdc_ip <IP>) [--reason <REASON>]
   
   The reason flag (mandatory) is used to verify that the SDC password is being reset and not changed by accident. The reason is stored in the MDM events log.
   **NOTE:** SDCs not configured with a password are disconnected after the feature is enabled in step 3.
   
   Copy the password that was generated in `<SDC_PASSWORD_STRING>`, used in the next step.
   
2. On the SDC, run the following command:

   ```bash
   /opt/emc/scaleio/sdc/bin/drv_cfg --set_mdm_password --ip <MDM_IP> --password <SDC_PASSWORD_STRING> --file/etc/emc/scaleio/drv_cfg.txt
   
   **NOTE:** The file option is required for password persistency, for cases such as service scini restart or SDC reboot.
   
   Open the file to verify the `<SDC_PASSWORD_STRING>` is logged at the end of the MDM line.
3. To enable SDC authentication, run the following command:

```
scli --set_sdc_authentication --enable
```

4. To disable SDC authentication, run the following command:

```
scli --set_sdc_authentication --disable
```

Results
SDC authentication is enabled or disabled.

**Apply Performance Profiles to system components**

You can use the PowerFlex GUI to apply performance profiles to system components.

**About this task**

The default configures a predefined set of parameters for very high performance use cases. When a container is provided in the command (System/Protection Domain/Fault Set), all the objects currently in the container are configured.

**NOTE:** For a complete list of parameters controlled by the profiles, refer to "PowerFlex Performance Fine-Tuning".

The profiles are applied separately to:

- SDSs
- SDCs

**NOTE:** After changing the performance profile of an SDS (on an SVM), you must perform manual memory allocation on the SVM, as described in the *PowerFlex Deployment Guide*.

To apply a profile to system components, perform the following steps:

**Steps**

1. Depending on the system component that you want to configure, from the PowerFlex GUI in the left pane, click either Configuration > SDSs or Configuration > SDCs.
2. In the right pane, select the relevant object and click Modify > Modify Performance Profile
3. In the SDS or SDC <object name> Modify Performance Profile dialog box, select a profile and click Apply.
4. Verify that the operation completed successfully and click Dismiss.

Results
The performance profile is set for the object.

**RFcache (xcache) package installation**

If the RFcache (xcache) package was not installed during the initial system deployment, you can also install the RFcache (xcache) package on physical or virtual servers in an existing PowerFlex system. The package is required on SDSs in order to accelerate Medium Granularity data layout Storage Pools.

**Install the RFcache (xcache) package on physical servers**

You can install the RFcache (xcache) package on physical servers using PowerFlex Installer and the CSV topology file.

**About this task**

To install RFcache, perform the following:
Steps
1. Update the RFcache fields in the CSV file used to deploy the system, as described in the "Preparing the CSV topology file" section of the Deploy PowerFlex Guide.
2. Follow the instructions in "Add components in the PowerFlex Installer".

Enable RFcache on ESXi servers
You can manually enable RFcache on ESXi servers using the vSphere PowerFlex plug-in.

About this task
You must first copy the RFcache (xcache) package to the SVMs, and then use the PowerFlex plug-in to configure its use.

Steps
1. Copy the RFcache package (xcache) to all SVMs running an SDS:

   EMC-ScaleIO-xcache-x.x-x.0.slesxx.x.x86_64

2. Install the file:

   rpm -i EMC-ScaleIO-xcache-x.x-x.0.slesxx.x.x86_64

3. From the PowerFlex plug-in, click SDSs.
4. Right-click an SDS, and select Add devices to a single SDS
5. Click a device in the Use for drop-down list, and select RFcache.
6. Click OK.
7. Repeat the previous steps for every SDS on which you want to enable RFcache.

Increase SVM memory to accommodate additional SDS device
When adding additional disks to an SDS, you may need to add additional memory to the SVM.

About this task
After an initial partial population of disks (less than the SDS full capacity), when adding more disks, you may need to add SVM memory. If the SDS doesn't have enough memory, error messages will be displayed.

(You can avoid this procedure by using the deployment wizard to allocate adequate memory during initial deployment.)

Perform this procedure in a maintenance window.

Steps
1. From the PowerFlex GUI, put an SDS in maintenance mode.
2. From the vCenter, power off the SVM.
3. From the vCenter, edit the SVM and increase the SVM memory by 300 MB for each 5 TB of added storage capacity.
4. Power on the SVM.
5. From the PowerFlex GUI, remove the SDS from maintenance mode.
6. Wait for the rebalance to complete.
7. Repeat the entire procedure for each SVM, one-at-a-time.

Next steps
You can now use any of the PowerFlex management tools to add more drives to the SDS.
Modify an SDS port during I/O

You can modify an SDS port while there is I/O running without interrupting I/O.

About this task

NOTE: Sometimes, your network topology needs to be prepared for the addition of new port, and this may take some time. PowerFlex does not prevent unnecessary degraded status or disconnection of SDS. Therefore, in such situations, it is recommended to place the SDS in Maintenance Mode before commencing this procedure.

Steps

1. On the SDS, perform one of the following as appropriate for your operating system:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>Run the script: <code>/opt/emc/scaleio/sds/bin/close_firewall_port.sh</code></td>
</tr>
<tr>
<td>Windows</td>
<td>From command line, run the batch file C:\Program Files\EMC\scaleio\sds\bin \close_firewall_port.bat</td>
</tr>
</tbody>
</table>

2. Open the following SDS file with a text editor, and change the port number shown there to the new port number:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td><code>/opt/emc/scaleio/sds/bin/port</code></td>
</tr>
<tr>
<td>Windows</td>
<td>C:\Program Files\EMC\scaleio\sds\bin\port</td>
</tr>
</tbody>
</table>

3. Open the following SDS configuration file with a text editor:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td><code>/opt/emc/scaleio/sds/cfg/conf.txt</code></td>
</tr>
<tr>
<td>Windows</td>
<td>C:\Program Files\EMC\scaleio\sds\cfg\conf.txt</td>
</tr>
</tbody>
</table>

4. Add the parameter `tgt_port = <NEW_PORT_NUM>` to the file, where `<NEW_PORT_NUM>` represents the new port number.

5. Perform one of the following:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>Run the script: <code>/opt/emc/scaleio/sds/bin/open_firewall_port.sh</code></td>
</tr>
<tr>
<td>Windows</td>
<td>From command line, run the batch file C:\Program Files\EMC\scaleio\sds\bin \open_firewall_port.bat</td>
</tr>
</tbody>
</table>

6. On the SDS, perform one of the following:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>Run the command: <code>Pkill sds</code></td>
</tr>
<tr>
<td>Windows</td>
<td>From command line, run the command: <code>net stop sds_service &amp; net start sds_service</code></td>
</tr>
</tbody>
</table>

7. On the MDM, modify the SDS port using the command:

```bash
csli --modify_sds_port (--sds_id <ID> | --sds_name <NAME> | --sds_ip <IP>) --new_sds_port <PORT>
```
For example, for an SDS called "sds198" where the new port number is 7071, type:

```
scsi --modify_sds_port --sds_name sds198 --new_sds_port 7071
```

**NOTE:** If you modify the SDS port on the MDM first, instead of following the above procedure, I/O errors might be encountered.
Replication ensures data protection of the PowerFlex environment. It creates a remote copy of one volume from one cluster to another. PowerFlex supports asynchronous replication.

Setting up the peer system is the first step when configuring replication. The volumes from each of the systems must be the same size. If the network is up, then the systems should be connected.

The journal capacity is a percentage of the total storage capacity. There are a number of factors that should be taken into consideration when defining the journal capacity.

- 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 RPO (Recovery Point Objective)
- When the total storage capacity in the system increases, a small percentage is needed for the journal capacity
- As application workload increases, the journal capacity needs to be increased

Data writes are accumulated in the journal until half the RPO time has reached to ensure data is not lost and a consistent copy is maintained between the volumes.

The SDR component is installed during deployment of PowerFlex. It manages replication activity within the system and between the source and target. It is recommended to install 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. At the same time 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) 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.

Replication Consistency Group (RCG) is a set of volumes which must maintain a consistent copy on the remote site where write order is maintained between volumes. This pair share the same attributes. There is the RPO (Recovery Point Objective). This defines the max amount time that data is lost. It is recommended to set 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 a minute is set as the RPO, you will not lose more than 30 seconds of data. It is highly recommended that the RPO be low as this ensures that minimal data is lost. There is no replication unless the source volume is consistent with the data from the target volume.

The following sections describe how to set up replication from the PowerFlex GUI:

Add a peer system

Add the connection information to enable replication between the peer systems.

Steps

1. From the PowerFlex GUI, in the left pane, click Replication > Peer Systems.
2. In the right pane, click Add.
3. In the Add Peer System dialog box, enter the connection information of the peer system:
   a. Enter the name.
   b. Enter the IP/Hostname of the peer system.
   c. Enter the system ID of the remote site. This can be copied either from the top-left of the menu bar or from MDM > Cluster Settings.
   d. Enter the port number used to connect the systems.
   e. Click Add Peer to initiate a connection with the peer system.

Results

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

**NOTE:** Verify that the certificate is copied and uploaded (on source and target).
Add journal capacity

Journal capacity is defined as a percentage of the total storage capacity of the Storage Pool. It is recommended to set 10% of the total capacity and it must be equal to at least 16 GB per SDR. It is important to assign enough storage capacity for the replication journal.

About this task

When assigning the percentage, you should take into consideration the following:
- As the total storage capacity increases, a small percentage is needed for the journal capacity. Default size of journal capacity is 5% of the replicated capacity
- RPO - as the RPO increases, the journal capacity needs to be increased
- Application workload - as the workload increases, the journal capacity needs to be increased

The minimum requirement of the journal capacity should take into consideration when the connection is comprised between the peer systems. The capacity should amount to at least three recovery sessions. The calculation for minimal journal capacity to add is - 100 GB x (SDRs + 3).

NOTE: The minimum recommended journal capacity should be twice the default journal session size.

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.

Steps
1. From the PowerFlex GUI, in the left pane, click Replication > Journal Capacity.
2. In the right pane, click Add.
3. In the Add Journal Capacity dialog box, select the relevant Storage Pool and add the percentage for journal capacity.
4. Click Add to allocate journal capacity from the storage pool.
5. Verify the operation completed successfully and click Dismiss.

Results
Journal capacity has been set.

Restart the replication cluster

The Protection Domain must be inactive before shutting down and activated after starting up the nodes in the replication cluster.

About this task

This procedure describes how to restart the nodes in the replication cluster:

Steps
1. From the PowerFlex GUI, inactivate the Protection Domain first on the source and then on the target system, as described in "Inactivate a Protection Domain".
2. Shutdown all nodes within the replication cluster.
3. Power on all nodes within the replication cluster.
4. Activate the Protection Domain first on the target and then on the source system, as described in "Activate a Protection Domain".
5. Validate that the RCG in the replication cluster returns to a working state.

SDR

The Storage Data Replication (SDR) is one of the main components that must be installed on each of the systems for replication. It is used to transfer data from the source volume to the target volume.

SDRs are added during the installation process. When logging in to PowerFlex Web UI, the SDRs for replication are listed. At least three SDRs must be installed on each system for failure and backup purposes. The SDR communicates data between the host to the journal.
When the journal has reached half the RPO time, the SDR transfers the data to the target journal. The SDR then applies the data from the target journal to the volume.

The memory (RAM) requirement of the SDR is up to 22.5 GB.

**Add SDR**

Add an SDR to the PowerFlex system.

**Prerequisites**

The IP address of the node must be configured for SDR. The SDR communicates with several components: SDC (application), SDS (Storage) and remote SDR (External). When setting the IP address, the role of the IP defines the component it takes on.

**About this task**

Add an SDR if an SDR component was added to an existing PowerFlex system or if a previously added SDR was removed. A minimum of three SDRs are required on each system.

**Steps**

1. From the PowerFlex GUI, in the left pane, click **Replication > SDRs**.
2. In the right pane, click **Add**.
3. In the **Add SDR** dialog box, enter the connection information of the SDR:
   a. Enter the name.
   b. Update the SDR Port if required.
   c. Select the relevant Protected Domain
   d. Enter the IP Address of the SDR.
   e. Click the relevant roles of the SDR.
   f. Click the **Add SDR** to initiate a connection with the peer system.
4. Verify that the operation completed successfully and click **Dismiss**.

**Results**

An SDR is added to PowerFlex.

**Modify IP role**

Update the IP role of the SDR. The SDR communicates with several components: SDC (application), SDS (Storage) and remote SDR (External). When setting the IP address, the role of the IP defines the component it takes on.

**About this task**

The default of the role is all.

**Steps**

1. From the PowerFlex GUI, in the left pane, click **Replication > SDRs**.
2. In the right pane, select the relevant SDR check box, and click **Modify > Modify IP Role**
3. In the **<SDR name> Modify IPs Role** dialog box, select the relevant role for the IPs listed.
4. Click **Apply**.
5. Verify that the operation completed successfully and click **Dismiss**

**Results**

The IP role for the SDR has been updated.
Apply performance profile

The default performance profile is high. Ensure system architecture is equipped to handle enhanced system performance of SDR activities.

Prerequisites

Steps

1. From the PowerFlex GUI, in the left pane, click Replication > SDRs.
2. In the right pane, select the relevant SDR check box, and click Modify > Modify Performance Profile.
3. In the SDR <SDR name> Modify Performance Profile dialog box, click High or Compact
4. Click Apply.
5. Verify that the operation completed successfully and click Dismiss.

Results

Performance profile is set for the SDR.

Enter maintenance mode

Enter the SDR into maintenance mode. This state allows for maintenance of the SDR.

Prerequisites

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

About this task

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

Steps

1. From the PowerFlex GUI, in the left pane, click Replication > SDRs.
2. In the right pane, select the relevant SDR check box, and click More > Enter Maintenance Mode.
3. In the Enter SDR <SDR name> to Maintenance Mode dialog box, click Enter Maintenance Mode
4. Verify that the operation completed successfully and click Dismiss.

Results

The SDR is in maintenance mode.

Remote Consistency Group

Remote 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 RCG on both the source and target systems.
Add a RCG

Add a RCG to the system.

Steps
1. From the PowerFlex GUI, in the left pane, click Replication > RCGs.
2. In the right pane, click Add.
3. In the Add RCG wizard, enter the information for the RCG:
   a. On the General page:
      • Enter the RCG Name.
      • Enter the number of RPO (recovery point objective) minutes. This is the amount of time of data loss tolerated if replication between the systems is compromised.
      • Enter the RPO minutes. It is recommended to enter the minimal amount of time the feature allows. In this case it is one minute.
      • Select the Source Protection Domain.
      • Select the Target System.
      • Select the Target Protection Domain.
      • Click Next.
   b. On the Add Replication Pairs page:
      • Click the volume from the Source column and then click the same size volume from the Target column.
      • Click Add Pair. The volume pair is added.
      • Click Next.
   c. On the Review Pairs page:
      • Ensure the correct source and volume pair are selected and click Add RCG & Start Replication.
   d. From the top right, click the Running Jobs icon and check the progress of the initial copy state
   e. Verify that the operation completed successfully and click Dismiss.

Results
The RCG is added to both the source and target systems.

Modify RPO

Update RPO time as required.

Steps
1. From the PowerFlex GUI, in the left pane, click Replication > RCGs.
2. In the right pane, select the relevant RCG check box, and click Modify > Modify RPO.
3. In the Modify RPO for RCG <rcg name> dialog box, enter the updated RPO time and then click Apply.
4. Verify that the operation completed successfully and click Dismiss.

Results
The RPO time for the RCG has been updated.

Example

Add a replication pair to RCG

Add a replication pair to the RCG.

Steps
1. From the PowerFlex GUI, in the left pane, click Replication > RCGs.
2. In the right pane, select the relevant RCG check box, and click Modify > Add Pair.
3. In the **Add Pairs** wizard, on the **Add Replication Pairs** page, select a volume from the source and a volume from the target and then click **Add Pair**.

4. Click **Next**.

5. In the **Review Pairs** page, verify the selected volumes are the correct volumes and click **Add Pairs**.

**Results**
A replication pair has been added to the RCG.

---

**Unpair from RCG**

Remove pair from the RCG.

**Steps**

1. From the PowerFlex GUI, in the left pane, click **Replication > RCGs**.
2. In the right pane, select the relevant RCG check box, and in the **Details** pane, in the **Volume Pairs** tab, click **Unpair**.
3. In the **Remove Pair from RCG <RCG name>** dialog box, click **Remove Pair**.
4. Verify the operation completed successfully and click **Dismiss**.

**Results**
The pair is removed from the selected RCG.

---

**Freeze RCG**

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

**Steps**

1. From the PowerFlex GUI, in the left pane, click **Replication > RCGs**.
2. In the right pane, select the relevant RCG check box, and click **More > Freeze Apply**.
3. Click **Freeze Apply**.
4. Verify that the operation completed successfully and click **Dismiss**.

**Results**
Freezing of the replication is applied.

---

**Unfreeze RCG**

Select Unfreeze Apply to resume data transfer from target journal to target volume.

**Steps**

1. From the PowerFlex GUI, in the left pane, click **Replication > RCGs**.
2. In the right pane, select the relevant RCG check box, and click **More > Unfreeze Apply**.
3. Click **Unfreeze Apply**.
4. Verify that the operation completed successfully and click **Dismiss**.

**Results**
Data transfer is resumed from target journal to target volume.
Set target to consistent mode

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

Steps
1. From the PowerFlex GUI, in the left pane, click Replication > RCGs.
2. In the right pane, select the relevant RCG check box, and click Manage > Set Target to Consistent Mode.
3. In the Set Target to Consistent Mode RCG <RCG name> dialog box, click Apply.
4. Verify that the operation completed successfully and click Dismiss.

Results
The target volume has been set to consistent mode.

Set target to inconsistent mode

Set target to inconsistent mode to pause apply 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, then the system does not apply.

About this task

NOTE: It is recommended to take a snapshot of the target before setting the target to inconsistent mode for recovery purposes of a consistent snapshot.

Steps
1. From the PowerFlex GUI, in the left pane, click Replication > RCGs.
2. In the right pane, select the relevant RCG check box, and click Manage > Set Target to Inconsistent Mode.
3. In the Set Target to Inconsistent Mode RCG <RCG name> dialog box, click Apply.
4. Verify that the operation completed successfully and click Dismiss.

Results
The target volume has been set to inconsistent mode.

Test failover stop

Stop test failover.

Steps
1. From the PowerFlex GUI, in the left pane, click Replication > RCGs.
2. In the right pane, select the relevant RCG check box, and click Manage > Test Failover Stop.
3. Click Approve.
4. Verify that the operation completed successfully and click Dismiss.

Results
Test failover has stopped.

Test Failover

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

About this task

Replication is still running.
Steps
1. From the PowerFlex GUI, in the left pane, click Replication > RCGs.
2. In the right pane, select the relevant RCG check box, and click Manage > Test Failover.
3. In the Failover <RCG name> Test Failover dialog box, click Start Test Failover.
4. In the RCG <RCG name> Test Failover using target volumes dialog box, click Proceed.
5. Verify that the operation completed successfully and click Dismiss.

Results
Test failover has started.

**Restore replication**

Once 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. This option may be selected from either source or target systems.

Prerequisites
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 destination before restoring the replication for backup purposes.

Steps
1. From the PowerFlex GUI, in the left pane, click Replication > RCGs.
2. In the right pane, select the relevant RCG check box, and click Manage > Restore.
3. In the Failover <RCG name> Restore Replication dialog box, click Apply.
4. Verify that the operation completed successfully and click Dismiss.

Results
The replication direction of the system has been restored.

**Reverse replication**

Once the replication consistency group 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. This option may be selected from either source or target systems.

Prerequisites
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.

About this task

Steps
1. From the PowerFlex GUI, in the left pane, click Replication > RCGs.
2. In the right pane, select the relevant RCG check box, and click Manage > Reverse.
3. In the RCG <RCG name> Reverse Replication dialog box, click Apply.
4. Verify that the operation completed successfully and click Dismiss.

Results
The replication direction of the system has been reversed.
**Failover**

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

**Prerequisites**

Before performing failover, make sure to stop the application and unmount the file-systems at the source (if the source is available).

**About this task**

There are two options when choosing failover of an RCG:

- **Switchover** - This option is a complete sync and failover between the source and the target. This means I/Os are stopped to the source, and then source and target volumes are synced. Access mode is changed of the target volumes to the target host, roles are switched and finally new source volumes access mode is changed to read-write.
- **Latest PiT** - The system prevents any write to the source volumes

**Steps**

1. From the PowerFlex GUI, in the left pane, click **Replication > RCGs**.
2. In the right pane, select the relevant RCG check box, and click **Manage > Failover**.
3. In the **Failover RCG <RCG name>** dialog box, select one of the following options: Switchover (Sync & Failover) or Latest PiT: (date & time).
4. Click **Apply Failover**.
5. In the **RCG <rcg name> Sync & Failover** dialog box, click **Proceed**.
6. Verify that the operation completed successfully and click **Dismiss**.
7. From the top right, click the **Running Jobs** icon and check the progress of the switchover.

**Results**

Failover is applied to the RCG.

**Create snapshot of RCG volume**

Create a snapshot of the RCG volume from the target system. The latest image of the volume is used for the snapshot. When creating a snapshot, the RCG enters a freeze mode.

**Steps**

1. From the PowerFlex GUI, in the left pane, click **Replication > RCGs**.
2. In the right pane, select the relevant RCG check box, and click **Manage > Create Snapshots**.
3. Click **Create Snapshots**.
4. Verify that the operation completed successfully and click **Dismiss**.

**Results**

A snapshot of the target RCG volume has been taken.

**Pause RCG**

Pause replication for the RCG. Pause stops the transfer of data from the source to target.

**Steps**

1. From the PowerFlex GUI, in the left pane, click **Replication > RCGs**.
2. In the right pane, select the relevant RCG check box, and click **Manage > Pause RCG**.
3. In the **Pause RCG <RCG name>** dialog box, click one of the following options:
   - **Stop Data Transfer** - this option saves all the data in the source journal volumes until there isn't any available capacity
- Track Changes - this option enables manual slim mode where only meta data in the source journal volumes is saved

4. Click Pause.
5. Verify that the operation completed successfully and click Dismiss.

Results
The replication between the source and target system is paused.

**Pause initial copy**

Pause replication of initial copy from source to target.

**Steps**

1. From the PowerFlex GUI, in the left pane, click Replication > RCGs.
2. In the right pane, select the relevant RCG check box, and in the Details pane, in the Volume Pairs tab, click Initial Copy > Pause Initial Copy.
3. In the Pause Initial Copy <RCG name> dialog box, click Pause Initial Copy.
4. Verify the operation completed successfully and click Dismiss.

Results
Replication of initial copy has been paused.

**Resume initial copy**

Resume replication of initial copy from source to target.

**Steps**

1. From the PowerFlex GUI, in the left pane, click Replication > RCGs.
2. In the right pane, select the relevant RCG check box, and in the Details pane, in the Volume Pairs tab, click Initial Copy > Resume Initial Copy.
3. In the Resume Initial Copy <RCG name> dialog box, click Resume Initial Copy.
4. Verify the operation completed successfully and click Dismiss.

Results
Replication of initial copy has been resumed.

**Set priority**

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

**Steps**

1. From the PowerFlex GUI, in the left pane, click Replication > RCGs.
2. In the right pane, select the relevant RCG check box, and in the Details pane, in the Volume Pairs tab, click Initial Copy > Set Priority.
3. In the Set Priority for Pair <RCG name> dialog box, select Default or High and then click Save.
4. Verify the operation completed successfully and click Dismiss.

Results
Priority of volume pair has been set.
PowerFlex VASA's limitations and prerequisites

Note the following limitations when using PowerFlex's VASA.

Limitations

- Deployment of PowerFlex's VASA is not prevented on ESXi 5.5, despite the fact that VMware no longer supports ESXi 5.5.
- The maximum number of volumes is 130K (8,192 mapped volumes per ESXi).
- The VASA provider can be mapped to a single instance of PowerFlex.
- A cluster may contain a single VASA provider or three VASA providers.
- The VASA provider must be installed only on a node which contains an SDC. The VASA provider nodes can be standalone or shared with other PowerFlex components.
- The VASA provider must be registered with a single vCenter.
- The VASA provider hostname must begin with a letter character.
- The maximum snapshot hierarchy of a vVol is 31.

Before you begin

Ensure that:

- Each host that runs the VASA provider has sufficient memory. The minimum required amount is 8 GB, though 16 GB is recommended.
- JRE 8u241 must be installed on every host that will run the VASA provider. Alternatively, you can use the latest OpenJDK 8. The correct Java executables must be found using the PATH environment variable.
- The DNS server must be configured, and for every VASA server, a DNS record should be created. Ensure that all VASA servers have a valid DNS resolution from all ESXi hosts and the vCenter Server, and that the vCenter Server has a valid DNS resolution from all VASA servers.
- Each VASA VM's hostname must match the VASA FQDN (the output of commands hostname and hostname -f should be the same).
- All components of your environment, including ESXis and vCenters, have their time synchronized.
- SDC should be installed on each ESXi which will consume PowerFlex vVols.
- PowerFlex is deployed.

vVols in PowerFlex

When the VASA provider is installed in the PowerFlex system, you can use and manage vVols using PowerFlex.


Logs are located in the following directory: /opt/emc/caleio/vasa/log/. For support, you can use the script /opt/emc/caleio/vasa/get_vasa_info.sh, which creates a tar.gz archive in the current directory. It includes the following diagnostic information on VASA:

- Actual process environment
- Command line
- File with additional environment variables
- VASA logs
Using storage policies

A virtual machine that runs on a Virtual Volumes datastore requires a VM storage policy. A VM storage policy is a set of rules that contains placement and quality-of-service requirements for a virtual machine.

PowerFlex has its own specific set of rules for assigning storage policies to Storage Pools. For more information on creating storage policies, see Create a VM storage policy for Virtual Volumes on page 68.

Register the PowerFlex VASA in the vCenter

Register the PowerFlex VASA as a Storage Provider in the vCenter.

About this task

When using one instance of the VASA provider, register it in the vCenter. When you are using three instances of the VASA provider, you must register at least two out of the three VASA providers. In that case, one of the two VASA providers is displayed in the vSphere Web Client in Active state and the other is displayed in Standby state.

Steps

1. Enable TLSv1.0:
   a. Edit the `/opt/emc/scaleio/vasa/setenv.sh`.
   b. Delete the following parameters from the file: `-Dserver.ssl.enabled-protocols=TLSv1.2,-Dhttps.protocols=TLSv1.2, and Dserver.ssl.protocol=TLS`.
   c. Restart the VASA service:
      ```
      service vasa-provider-vxflexos restart
      ```

2. In the vSphere Web Client, navigate to the Hosts and Clusters inventory object.
3. Locate the vCenter inventory object and select it.
4. Click the Configure tab, and click More > Storage Providers.
5. Click the Register a Storage Provider icon.
6. In the New Storage Provider dialog, define the connection information for the storage provider:
   a. Enter a name for the VASA provider.
   b. Enter the VASA URL: `https://<VASA_FQDN>:443/version.xml` where `<VASA_FQDN>` is the fully-qualified domain name of the VASA, as registered in the DNS server.
   c. Enter the MDM admin username and password.

7. Click OK to complete the registration.
8. Click Yes to confirm the VASA certificate.

Results

The vCenter Server has registered the PowerFlex VASA as a storage provider.
Next steps
Verify that the status of the VASA Storage Provider in the Storage Provider table is online. If the status is offline, it most likely indicates an issue with the DNS or a communication issue with the ESXi.

Enable autostart of the VASA provider after reboot
Enable automatic restarting of the VASA provider service after reboot.

Steps
1. Connect with SSH to each VASA provider host.
2. Run the following command to enable automatic restart of the VASA provider service after reboot:

   ```
   systemctl enable vasa-provider-vxflexos
   ```
You can configure the MDM cluster in the PowerFlex system.

**Configuring MDM cluster**

You can configure the MDM cluster to allow for efficient load balancing to enable high availability of the servers that are configured within the cluster. You can add members, replace or remove members as well as update configuration settings. Members refer to the servers within the cluster.

**Extend an existing PowerFlex system**

Options for adding nodes to an existing system.

You can add nodes to an existing system, as well as extend the MDM cluster from a 3-node to a 5-node cluster. Depending on your system, you can use the PowerFlex Installer (for physical servers) or the vSphere plug-in (for ESXi servers).

These topics are described in the sections of the *Deploy PowerFlex Guide*:

- "Extend an existing PowerFlex system"
- "Extend the MDM cluster from 3 to 5-node"

**Add Linux servers to the MDM cluster**

Add Linux servers to the MDM cluster to expand a 3-node cluster mode to a 5-node cluster mode.

**About this task**

This procedure describes how to add Linux servers to the MDM cluster in the CSV topology file.

**Steps**

1. Obtain the CSV topology file from one of the following options:
   - CSV used to deploy the v2.0 system in its current 3-node cluster mode
   - Complete or minimal CSV (provided in the ISO, or can be downloaded from the PowerFlex Installer) and fill-in the current system topology fields in the CSV

2. Edit, and save the CSV with one of these options:
   - Add two new hosts (two new lines) to the system topology, and in the *Is MDM/TB* column for those lines, designate one as a Slave and one as a Tie Breaker (TB) role
   - In the *Is MDM/TB* column of two existing hosts that were not part of the MDM cluster, add a Slave and a Tie Breaker (TB) role.

   This option is displayed in the following figure

   **NOTE:** If you need to change the roles of the current nodes, do so only after adding to the cluster.

   ![Figure 8. Before adding](image_url)
3. In the **Packages** tab, upload all PowerFlex packages, per the host OS.
4. In the **Install** tab, select the edited CSV file, and select **Add to existing system** from the drop-down menu.
5. Click **Upload installation CSV**.
6. Start the installation, and monitor as normal.

### Add ESXi servers to the MDM cluster

Add additional ESXi servers, and assign them roles within the cluster.

**About this task**

When you add a new MDM manager, to ensure continued SDC-MDM communication, you must update the SDCs in the system with the new MDM IP address. You can do this using the vSphere plug-in, as described in "Update the SDC parameters".

**Steps**

1. If the ESXi servers to be added do not have the SDC component, install the SDC on each of the servers, as described in the "Update the SDC parameters".
2. From the **Basic tasks** section, click **Deploy PowerFlex environment**.
   The PowerFlex VMware deployment wizard runs. If you exited the wizard before completing the deployment, the wizard continues from the point you left off.
   
   **NOTE:** The deployment wizard assumes that you are using the provided PowerFlex OVA template to create the Storage Virtual Machines (SVMs).
3. In the **Select Installation** screen, select **Add servers to a registered PowerFlex system**, and select the system you want to extend.
4. In the Select Management Components screen, select **5-node mode**.
5. In the **Manager MDM** and **Tie Breaker MDM** fields, select the nodes to add to the cluster.
6. Click Next, and continue the deployment.

**NOTE:** When adding components, the wizard adjusts the displayed screens to options that are relevant to the current PowerFlex system.

**Update the SDC parameters in VMware based HCI or compute node**

Update the SDC parameters to maintain SDC-MDM communication.

**About this task**

This procedure describes how to use the VMware plug-in to update the SDCs that are needed to maintain SDC-MDM communication.

**Steps**

1. From the plug-in **Advanced tasks** menu, click **Update SDC parameters**, and follow instructions to complete the process.
2. Check that the SDC parameters were updated by running this command on each ESXi:

   ```
   cat /etc/vmware/esx.conf |grep scini|grep -i mdm
   ```

**Replace a cluster member**

Replace a member of an MDM cluster to replace a faulty server or change the server IP address.

The current server is the server that needs to be replaced.

If you have an extra server to replace the current server, then there is no need to change the cluster mode (3-node or 5-node). If you do not have an additional server, you will need to reduce the cluster mode, from 5-node to 3-node, or from 3-node to single node.

**NOTE:**

- It is not recommended to use single mode in production systems, except in temporary situations.

The following rules are true regardless of the circumstances:

- To remove a cluster member, you first need to make it a standby, then remove the standby. To add a member to a cluster, you first make it a standby, then add the standby to the cluster.
• The cluster must always have 5, 3, or 1 members, never any other amount. For a further understanding of this subject, see "The MDM cluster" in the Architecture section of Getting to Know PowerFlex Guide. Proceed to the section that describes your environment:
  ○ "Replace a cluster member by adding a new server"
  ○ "Replace a cluster member without adding a new server to the cluster"

**Add a new server to the MDM cluster**

Add or replace a server to the MDM cluster.

**About this task**

This procedure describes how to replace or add a new member to the MDM cluster.

**Before you begin**, perform the following:

- Assign the necessary IP addresses to the replacement server.
- Install the MDM package on the server.

In this example, we are replacing the server whose IP address is 10.3.1.179, currently a member of a 5-node MDM cluster, with a server a server whose IP address is 10.3.1.57, which is currently external to any PowerFlex system. This process can be used to replace any role in the MDM cluster.

**Steps**

1. Check that the current server (179) is not the Master MDM by running the following command:

   ```
   scli --query_cluster
   ```

   The output similar to the following is displayed:

   ```
   # scli --query_cluster
   Cluster:
   Mode: 5_node, State: Normal, Active: 5/5, Replicas: 3/3
   Master MDM:
   Name: mdm17, ID: 0x5d07497754427fd0
   IPs: 10.3.1.17, 192.168.1.17, Management IPs: 10.3.1.17, Port: 9011
   Version: 2.0.972
   Slave MDMs:
   Name: mdm19, ID: 0x26ee566356362451
   IPs: 10.3.1.19, 192.168.1.19, Management IPs: 10.3.1.19, Port: 9011
   Status: Normal, Version: 2.0.972
   Name: mdm18, ID: 0x5843c4d16d8f1082
   IPs: 10.3.1.18, 192.168.1.18, Management IPs: 10.3.1.18, Port: 9011
   Status: Normal, Version: 2.0.972
   Tie-Breakers:
   Name: mdm179, ID: 0x7380b70e2f73d346
   IPs: 10.3.1.179, 192.168.1.179, Port: 9011
   Status: Normal, Version: 2.0.972
   Name: mdm20, ID: 0x6dfe1c5f4062b5b3
   IPs: 192.168.1.20, 10.3.1.20, Port: 9011
   Status: Normal, Version: 2.0.972
   ```

   In this case server 179 is a Tie Breaker.

2. If the current server is the Master MDM, change its state using the `switch_mdm_ownership` command, as described in the PowerFlex CLI Reference Guide.

3. Make the replacement MDM server a standby MDM, and assign it a name (mdm57, in our example) by running the following command, on the Master MDM:

   ```
   scli --add_standby_mdm --mdm_role tb --new_mdm_ip 10.3.1.179,192.168.1.179 --new_mdm_management_ip 192.168.1.179, Port: 9011 --new_mdm_name mdm57
   ```

4. You can see the result of the command by running the following command:

   ```
   scli --query_cluster
   ```
### Reassign a member within the MDM cluster

Reassign a member to a new role within the MDM cluster.

**About this task**

This procedure describes how to remove a member and then add the node back and reassign it to a different role within the cluster. You must first reduce the amount of nodes in the cluster, change to a 3-node cluster and then add the member back to the cluster and reassign it to its new role.

In the following example, we are removing the current server whose IP address is 10.3.1.179, currently a Tie Breaker member of a 5-node MDM cluster. To retain a majority in the MDM cluster, we must also remove one of the Slave MDMs in the cluster, in this case the MDM whose IP address is 10.3.1.19. This process can be used to replace any role in the MDM cluster.

**Steps**

1. Verify that the current server (179) is not the Master MDM:

   ```bash
   scli --query_cluster
   
   # scli --query_cluster
   Cluster:
   Mode: 5_node, State: Normal, Active: 5/5, Replicas: 3/3
   Master MDM:
   Name: mdm17, ID: 0x5d07497754427fd0
   IPs: 10.3.1.17, 192.168.1.17, Management IPs: 10.3.1.17, Port: 9011
   Version: 2.0.972
   Slave MDMs:
   Name: mdm19, ID: 0x26ee566356362451
   IPs: 10.3.1.19, 192.168.1.19, Management IPs: 10.3.1.19, Port: 9011
   Status: Normal, Version: 2.0.972
   Name: mdm18, ID: 0x5843c4d16d8f1082
   IPs: 10.3.1.18, 192.168.1.18, Management IPs: 10.3.1.18, Port: 9011
   Status: Normal, Version: 2.0.972
   Tie-Breakers:
   Name: mdm179, ID: 0x7380b70e2f73d346
   IPs: 10.3.1.179, 192.168.1.179, Port: 9011
   ```

   The current server has been replaced.

   mdm57 has been added as a standby MDM. When it is a standby MDM, it can be added to the cluster.

5. Replace the current mdm179 with the standby mdm57 by running the following command:

   ```bash
   scli --replace_cluster_mdm --remove_tb_name mdm179
   --add_tb_name mdm57
   
   The following output is displayed:
   Successfully replaced the cluster MDM
   ```
In this case server 179 is a Tie Breaker.

2. If the current server is the Master MDM, change its state using the `switch_mdm_ownership` command, as described in the PowerFlex CLI Reference Guide.

3. Switch to a 3-node cluster:

   `scli --switch_cluster_mode --cluster_mode 3_node --remove_tb_name mdm179 --remove_slave_mdm_name mdm19`

   The following output is displayed:

   Successfully switched the cluster mode.

4. To view the result of the command, run:

   `scli --query_cluster`

   The output similar to the following is displayed:

   ```
   # scli --query_cluster
   Cluster:
   Mode: 3_node, State: Normal, Active: 3/3, Replicas: 2/2
   ...
   Slave MDMs:
   Name: mdm18, ID: 0x5843c4d168f1082
   IPs: 10.3.1.18, 192.168.1.18, Management IPs: 10.3.1.18, Port: 9011
   Status: Normal, Version: 2.0.972
   Tie-Breakers:
   Name: mdm20, ID: 0x6dfe1c5f406b5b3
   IPs: 192.168.1.20, 10.3.1.20, Port: 9011
   Status: Normal, Version: 2.0.972
   Standby MDMs:
   Name: mdm19, ID: 0x26ee566356362451, Manager
   IPs: 10.3.1.19, 192.168.1.19, Management IPs: 10.3.1.19, Port: 9011
   Name: mdm179, ID: 0x7380b70e2f73d346, Tie Breaker
   IPs: 10.3.1.179, 192.168.1.179, Port: 9011
   ```

   The cluster has been changed to 3-node mode, as a Slave MDM (`mdm19`) and a TB MDM (`tb179`) have been removed and are now standby MDMs.

   Now that the current server is a standby MDM, it can be removed from PowerFlex.

5. Remove the current server from PowerFlex:

   `scli --remove_standby_mdm --remove_mdm_name mdm179`

   The following output is displayed:

   Successfully removed the standby MDM.

6. To view the result of the command, run:

   `scli --query_cluster`

   The output similar to the following is displayed:

   ```
   Cluster:
   Mode: 3_node, State: Normal, Active: 3/3, Replicas: 2/2
   ...
   Tie-Breakers:
   Name: mdm20, ID: 0x6dfe1c5f406b5b3
   IPs: 192.168.1.20, 10.3.1.20, Port: 9011
   Status: Normal, Version: 2.0.972
   Standby MDMs:
   ```
The current server is no longer a standby MDM.

7. Reassign IP addresses to the current server, as required.
   In our case, we will assign the following IP address to the current server: 10.3.1.57.

8. Add the current server (57) back to the system as a standby MDM, and assign it the name mdm57:

   `scli --add_standby_mdm --mdm_role tb --new_mdm_ip 10.3.1.57,192.168.1.57 --new_mdm_management_ip 10.3.1.57 --new_mdm_name mdm57`

   The output similar to the following is displayed:

   Successfully added a standby MDM. Object ID 13c925450656db74

9. To view the result of the command, run:

   `scli --query_cluster`

   The output similar to the following is displayed:

   Cluster:
   Mode: 3_node, State: Normal, Active: 3/3, Replicas: 2/2
   ...
   Tie-Breakers:
   Name: mdm20, ID: 0x6dfe1c5f4062b5b3
   IPs: 192.168.1.20, 10.3.1.20, Port: 9011
   Status: Normal, Version: 2.0.972
   Standby MDMs:
   Name: mdm19, ID: 0x26ee566356362451, Manager
   IPs: 10.3.1.19, 192.168.1.19, Management IPs: 10.3.1.19, Port: 9011
   Name: mdm57, ID: 0x13c925450656db74, Tie Breaker
   IPs: 10.3.1.57, 192.168.1.57, Port: 9011

   The server mdm57 is now a standby MDM, so it can be promoted to the MDM cluster.

10. Switch to 5-node cluster by adding the standby MDMs to the cluster:

    `scli --switch_cluster_mode --cluster_mode 5_node --add_slave_mdm_name mdm19 --add_tb_name mdm57`

    The following output is displayed:

    Successfully switched the cluster mode.

11. To view the result of the command, run:

    `scli --query_cluster`

    The output similar to the following is displayed:

    Cluster:
    Mode: 5_node, State: Normal, Active: 5/5, Replicas: 3/3
    Master MDM:
    Name: mdm17, ID: 0x5d07497754427fd0
    IPs: 10.3.1.17, 192.168.1.17, Management IPs: 10.3.1.17, Port: 9011
    Version: 2.0.972
    Slave MDMs:
    Name: mdm18, ID: 0x5843c4d16d8f1082
    IPs: 10.3.1.18, 192.168.1.18, Management IPs: 10.3.1.18, Port: 9011
    Status: Normal, Version: 2.0.972
    Name: mdm19, ID: 0x26ee566356362451
    IPs: 10.3.1.19, 192.168.1.19, Management IPs: 10.3.1.19, Port: 9011
    Status: Normal, Version: 2.0.972
    Tie-Breakers:
    Name: mdm20, ID: 0x6dfe1c5f4062b5b3
    IPs: 192.168.1.20, 10.3.1.20, Port: 9011
12. When changing an MDM IP address, it is mandatory to update and restart all the SDCs in the system as well.
   a. Update the IP addresses:
      Windows:
      ```
      C:\Program Files\emc\scaleio\sdc\bin\drv_cfg --mod_mdm_ip
      --ip <EXISTING_MDM_IP_ADDRESS>
      --new_mdm_ip <NEW_MDM_IP_ADDRESSES>
      ```
      Linux:
      ```
      /opt/emc/scaleio/sdc/bin/drv_cfg --mod_mdm_ip
      --ip <EXISTING_MDM_IP_ADDRESS>
      --new_mdm_ip <NEW_MDM_IP_ADDRESSES>
      ```
   b. Restart the SDC.
   c. Verify the changes:
      Windows:
      ```
      C:\Program Files\emc\scaleio\sdc\bin\drv_cfg --query_mdms
      ```
      Linux:
      ```
      /opt/emc/scaleio/sdc/bin/drv_cfg --query_mdms
      ```
      The output similar to the following should appear:
      ```
      Retrieved 1 mdm(s)
      MDM-ID 043925027bbed30e SDC ID 28c5479b00000000 INSTALLATION ID
      7214f7ca647c185b IPs [0]-9.4.4.12 [1]-9.4.4.11
      ```

**Remove members from the MDM cluster**

Change from 5-node to 3-node mode, or 3-node to single node mode

There are different scenarios for replacing a server, depending on whether an extra server is available to temporarily take over the role of the one being replaced, or not. For more information on changing servers, refer to "Replace a cluster member".

**Configure virtual IP addresses**

Configure virtual IP addresses for the MDMs in PowerFlex.

You can configure virtual IP addresses during deployment or post-deployment. Use the following management tools to configure virtual IP addresses:

<table>
<thead>
<tr>
<th>Management tool</th>
<th>Actions</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerFlex Installer</td>
<td>Add virtual IP addresses only.</td>
<td>For details, see the deployment documentation.</td>
</tr>
<tr>
<td>vSphere Web plug-in</td>
<td>Add virtual IP addresses only.</td>
<td>For details, see the PowerFlex User Guide.</td>
</tr>
<tr>
<td>CLI</td>
<td>Add, modify, and remove virtual IP addresses.</td>
<td>For details, see the PowerFlex CLI Reference Guide.</td>
</tr>
<tr>
<td>REST API</td>
<td>Add, modify, and remove virtual IP addresses.</td>
<td>For details, see PowerFlex REST API Reference Guide.</td>
</tr>
</tbody>
</table>
Add another IP address subnet to an MDM cluster

Add an IP network to an existing MDM cluster.

About this task

This procedure describes how to add another IP address subnet for use by the MDM cluster. This addresses scenarios where the MDM cluster uses a single network, or when an existing network needs to be replaced by a different one or to simply add another network (to an already multiple-network cluster). The MDM supports up to 8 networks.

Steps

1. Query the system to get the current cluster state/health:
   
   | scli --query_cluster |

   Cluster status is returned, where you can identify the Master, the Slave, and the Tie Breaker.

2. Switch to single cluster mode:
   
   | scli --switch_cluster_mode --cluster_mode 1_node --remove_slave_mdm_id <mdm_slave_id> --remove_tb_id <tb_id> |

3. Remove the standby MDM:
   
   | scli --remove_standby_mdm --remove_mdm_id <mdm_slave_id> |

4. Remove the Tie Breaker:
   
   | scli --remove_standby_mdm --remove_mdm_id <tb_id> |

5. Add the MDM as standby with its IP addresses (including the additional IP addresses):
   
   | scli --add_standby_mdm --new_mdm_ip ip_1,<,ip_2,...> --mdm_role manager --new_mdm_management_ip ip_1,<,ip_2,...> --allow_asymmetric_ips --force_clean |

   For example:

   | scli --add_standby_mdm --new_mdm_ip 10.89.9.6,10.89.11.6 --mdm_role manager --new_mdm_management_ip 10.89.9.6,10.89.11.6 --allow_asymmetric_ips --force_clean |

6. Add the Tie Breaker as standby with its IP addresses (including the additional IP addresses):
   
   | scli --add_standby_mdm --new_mdm_ip ip_1,<,ip_2,...> --mdm_role tb --new_mdm_management_ip ip_1,<,ip_2,...> --allow_asymmetric_ips --force_clean |

7. Switch cluster operation back to a 3-node cluster:
   
   | scli --switch_cluster_mode --cluster_mode 3_node --add_slave_mdm_id <slave_id> --add_tb_id <tb_id> |

   For example:

   | scli --switch_cluster_mode --cluster_mode 3_node --add_slave_mdm_id 0x4520631c7262bbf1 --add_tb_id 0x3cde0ef515f61162 |

8. Query the system to get the current cluster state/health.
   
   | scli --query_cluster |

   Cluster status is returned, where you can check that the cluster is configured and operating as expected.
9. Switch MDM ownership to verify cluster functionality:

```bash
scli --switch_mdm_ownership --new_master_mdm_id <new_master_mdm_id>
```

For example:

```bash
scli --switch_mdm_ownership --new_master_mdm_id 0x4520631c7262bbf1
```

10. Query the system to get the current cluster state/health.

```bash
scli --query_cluster
```

Cluster status is returned, where you can check that the cluster is operating as expected.

11. Add IP addresses for the Master MDM (presently Slave MDM) by following steps 2, 3, 5, 7, and 8.

12. Optional: Switch MDM ownership back to the original MDM:

```bash
scli --switch_mdm_ownership --new_master_mdm_id MDM_ID
```

### Configure SDC access to the MDM

Configure SDC access to the MDM through the system.

To harden SDC access to the MDM, it is possible to restrict access, pending approval of the SDC by the system. The default system setting is full access (restricted SDC mode is disabled). When the restricted SDC mode is enabled, volumes can only be mapped to “approved” SDCs. Approval is obtained by issuing the `--add_sdc` command for each SDC. You can set restricted mode before or after SDCs have been added to your network.

You can use the following commands:

<table>
<thead>
<tr>
<th>Action</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable restricted SDC mode</td>
<td>set_restricted_sdc_mode command</td>
</tr>
<tr>
<td>Add an SDC to the approved list, when restricted SDC mode is enabled</td>
<td>--add_sdc</td>
</tr>
</tbody>
</table>

For more information, see the PowerFlex CLI Reference Guide.

### Configure management session timeout parameters

Configure the management session idle timeout on each MDM as required by your organization.

When a user is authenticated by the system, all commands are performed with the user's respective role until a logout is performed, or until the session expires by reaching one of the following timeouts:

- Maximum session length (default: 8 hours)
- Session idle time (default: 10 minutes)

You can modify these parameters, by editing the MDM `conf.txt` file:

- Linux: `/opt/emc/caleio/mdm/cfg/conf.txt`
- Windows: `C:\Program Files\emc\caleio\mdm\cfg\conf.txt`

1. To configure maximum session length, edit the value of the `user_session_hard_timeout_secs` parameter. The minimum is 10 seconds, maximum 10 years, and default 8 hours.
2. To configure session idle time, edit the value of the `user_session_timeout_secs` parameter. The minimum is 10 seconds, maximum 3 months, default 10 minutes.
3. After changing the parameters, restart the MDM slaves. After the MDM slaves are up, reassign the Master MDM to one of the slaves and then restart the MDM service (delete and create service).
4. To ensure persistence, make these changes on every MDM.
Configure virtual IP addresses using the PowerFlex Installer

Configure virtual IP addresses using the Maintain menu in the PowerFlex Installer.

Prerequisites

For data networks using IPv6, if you plan to implement a floating virtual IP address for the MDM, disable the IPv6 DAD setting on the server’s relevant interfaces, using the command:

```
sysctl net.ipv6.conf.<interface_name>.dad_transmits=0
```

About this task

You can assign a virtual IP address for each possible MDM manager, which is used for communications between the MDM cluster and SDCs. Only one virtual IP address can be mapped to each NIC, with a maximum of four virtual IP addresses per system. The PowerFlex Installer can be used to assign new virtual IP addresses only; to change or remove existing virtual IP addresses, use the appropriate CLI commands.

Steps

1. From the PowerFlex Installer, select Maintain.
2. Select Set Virtual IPs.
3. In the Set Virtual IPs for PowerFlex system screen, type the MDM password.

4. For each MDM that you wish to set a virtual IP address, enter a virtual IP address and the NIC to which it will be mapped. For each new virtual IP address, enter the virtual IP address and NIC name for each MDM to which it will be mapped.
With the PowerFlex Installer, you can configure NIC names that contain the following characters only: a-z, A-Z, 0-9. If a NIC name contains the "-_" or "-" character (for example eth-01), don't use PowerFlex Installer. Configure this IP address with the CLI `modify_virtual_ip_interfaces` command and the `--new_mdm_virtual_ip_interface <INTF>` parameter.

5. Click **Set Virtual IPs**.

**Results**

The virtual IP address is configured and all of the SDCs are updated with the new virtual IP address. See section PowerFlex plug-in for information on "Configuring virtual IP addresses - PowerFlex plug-in".
Approving pending security certificates

Approve pending security certificates, and view approved certificates in the System Settings window.

About this task

**NOTE:** When there are pending certificates in the system, they are listed in the Backend > Storage view > State Summary table, and in the Monitor > Alerts view.

Steps

1. From the System Settings menu in the top right corner, select System Settings.
   The System Settings window appears, showing approved and pending certificates.
2. Scroll to connections that are Pending Approval, and expand the rows.
3. For each one, scroll to the bottom of the information about the required certificate, and click Confirm.

Default self-signed certificate expires

The default self-signed security certificate used on the PowerFlex Gateway expires after approximately one year. A new one can be created using the Java keytool utility.

The self-signed security certificate used on the PowerFlex Gateway expires after approximately one year, and needs to be replaced. If your self-signed security certificate expires, you can create a new one using the Java keytool utility.

When you upgrade the PowerFlex Gateway, the self-signed certificate is automatically replaced with a new one, and therefore will only need to be replaced after one year from the upgrade date.

Upgrade the PowerFlex Gateway when a custom certificate is used

Save a copy of the certificate before upgrading the PowerFlex Gateway.

If a custom security certificate is used on the PowerFlex Gateway (Windows and Linux environments), you must save a copy of the file where certificates are stored (*.keystore file) and the catalina.properties file before you upgrade the PowerFlex Gateway.

After the upgrade is complete, you must copy these files back to their original location.

The default file locations, per operating system, are:

Linux:
/opt/emc/scaleio/gateway/conf/catalina.properties
/opt/emc/scaleio/gateway/conf/certificates/.keystore

Windows (64 bit):
C:\Program Files\EMC\ScaleIO\Gateway\conf\catalina.properties
C:\Program Files\EMC\ScaleIO\Gateway\conf\certificates\.keystore
Enable LIA security

You can enable LIA security.

Steps

1. In the PowerFlex Installer, select the Maintain tab.
2. Click Security Settings and select Enable LIA Security.
3. Enter the MDM password in the Confirm Enable LIA security of your PowerFlex system box.
4. Click Enable LIA Security.

Certificate management for PowerFlex Gateway

This section explains how to replace the PowerFlex Gateway’s self-signed security certificate with your organization’s “trusted” certificate, and how to create a new “trusted” certificate. The PowerFlex Gateway automatically creates its own self-signed security certificate when it is installed or upgraded. If your organization has no special security certificate requirements, you can keep working with the default certificate.

Replace the default self-signed security certificate with your own trusted certificate

Create your own trusted certificate, and then replace the default certificate with the one that you created.

Steps

1. Find the location of keytool on your server, and open it.
   It is a part of the Java (JRE or JDK) installation on your server, in the bin directory. For example:
   - C:\Program Files\Java\jdk1.8.0_XX\bin\keytool.exe
   - /usr/bin/keytool
2. Generate your RSA private key:

   keytool -genkey -alias <YOUR_ALIAS> -keyalg RSA -keystore <PATH_TO_NEW_KEYSTORE_FILE>

   a. If you want to define a password, add the following parameters to the command. Use the same password for both parameters.

   -storepass <KEYSTORE_PASSWORD> -keypass <KEYSTORE_PASSWORD>

   NOTE: Specify a directory outside the PowerFlex Gateway installation directory for the newly created keystore file. This will prevent it from being overwritten when the PowerFlex Gateway is upgraded or reinstalled.

3. If you already have a Certificate Signing Request (CSR), skip this step.
   If you need a CSR, generate one by typing the following command. (If you did not define a keystore password in the previous step, omit the password flags.)

   keytool -certreq -keyalg RSA -alias <YOUR_ALIAS> -file certreq.txt -keystore <PATH_TO_NEW_KEYSTORE_FILE> -storepass <KEYSTORE_PASSWORD> -keypass <KEYSTORE_PASSWORD>

4. If you already have an SSL certificate, skip this step.
   If you need an SSL certificate, use your CSR to obtain a new certificate from a third-party trusted SSL certificate provider. Save the certificate file on your server, outside the PowerFlex Gateway installation directory.

5. Import the Trusted Root, by typing this command. (If you did not define a keystore password, omit the password flags.)

   keytool -import -alias root -keystore <PATH_TO_NEW_KEYSTORE_FILE> -trustcacerts -file <LOCATION_OF_YOUR_root.cer_FILE> -storepass <KEYSTORE_PASSWORD> -keypass <KEYSTORE_PASSWORD>

   NOTE: The certificate must be in x.509 format.
If a message appears saying that the root is already in the system-wide store, import it anyway.

6. Import the intermediate certificates, by typing the command. (If you did not define a keystore password, omit the password flags.)

```
keytool -import -alias intermediateCA -keystore <PATH_TO_NEW_KEYSTORE_FILE> -trustcacerts -file <LOCATION_OF_YOUR_intermediate.cer_FILE> -storepass <keystore password> -keypass <keystore password>
```

You must provide a unique alias name for every intermediate certificate that you upload with this step.

7. Install the SSL Certificate under the same alias that the CSR was created from (<YOUR_ALIAS> in previous steps), by typing the command (if you did not define a keystore password, omit the password flags):

```
keytool -import -alias <YOUR_ALIAS> -keystore <PATH_TO_NEW_KEYSTORE_FILE> -trustcacerts -file <LOCATION_OF_SSL_CERTIFICATE> -storepass <keystore password> -keypass <keystore password>
```

8. Edit the following items in the file <POWERFLEX_GATEWAY_INSTALLATION_DIRECTORY>/conf/catalina.properties:

   a. `keystore.file=PATH_TO_NEW_KEYSTORE_FILE`
   b. `keystore.password=PASSWORD_DEFINED_DURING_KEYSTORE_CREATION`

   If you did not define a password, the default password is `changeit`.

9. Restart the PowerFlex Gateway service:

   - Windows: From the Windows Services window, restart the EMC ScaleIO Gateway.
   - Linux: Type the following command:

     ```
     service scaleio-gateway restart
     ```

Replacement of the security certificate is complete.

---

**Replace the default self-signed security certificate with your own self-signed certificate**

Replace the default self-signed security certificate with your own self-signed security certificate.

**Steps**

1. Find the location of keytool on your server, and open it.
   It is usually a part of the Java (JRE or JDK) installation on your server, in the bin directory. For example:
   - `C:\Program Files\Java\jdk1.8.0_XX\bin\keytool.exe`
   - `/usr/bin/keytool`

2. Generate your RSA private key:

   ```
   keytool -genkey -alias <YOUR_ALIAS> -keyalg RSA -validity 360 -keysize 2048 -keystore <PATH_TO_NEW_KEYSTORE_FILE>
   ```

   a. If you want to define a password, add the following parameters to the command. Use the same password for both parameters.

      ```
      -storepass <KEYSTORE_PASSWORD> -keypass <KEYSTORE_PASSWORD>
      ```

   **NOTE:** Specify a directory outside the PowerFlex Gateway installation directory for the newly created keystore file. This will prevent it from being overwritten when the PowerFlex Gateway is upgraded or reinstalled.

3. Edit the following items in the file <POWERFLEX_GATEWAY_INSTALLATION_DIRECTORY>/conf/catalina.properties:

   a. `keystore.file=PATH_TO_NEW_KEYSTORE_FILE`
   b. `keystore.password=PASSWORD_DEFINED_DURING_KEYSTORE_CREATION`

   If you did not define a password, the default password is `changeit`.

4. Restart the PowerFlex Gateway service:

   - Windows: From the Windows Services window, restart the EMC ScaleIO Gateway.
Non-default certificate use before and after a PowerFlex Gateway upgrade

When using a non-default security certificate, you must perform certain actions before and after upgrading the PowerFlex Gateway.

About this task

If a non-default security certificate is used on the PowerFlex Gateway in Windows and Linux environments (for example, if the certificate is signed by the user organization CA), you must save a copy of the certificate and the catalina file before the upgrade, and restore them to their original location after the upgrade.

Steps

1. Before commencing the PowerFlex Gateway upgrade, locate the *.keystore file and the catalina.properties file, and save a copy of them in another location.

   The default file locations, per operating system, are:
   - Linux:
     - /opt/emc/scaleio/gateway/conf/catalina.properties
     - /opt/emc/scaleio/gateway/conf/certificates/.keystore
   - Windows (64 bit):
     - C:\Program Files\EMC\ScaleIO\Gateway\conf\catalina.properties
     - C:\Program Files\EMC\ScaleIO\Gateway\conf\certificates\.keystore

2. After the upgrade is complete, copy these files back to their original location.

Setting up SSH authentication on the PowerFlex Gateway

A manually generated public-private key pair can be used to perform SSH key authentication, instead of passwords, between the PowerFlex Gateway and PowerFlex system servers. For more information, see “Using SSH authentication on the PowerFlex Gateway” in the PowerFlex Deployment Guide.

Configuring SSL component authentication

PowerFlex uses SSL authentication to authenticate both internal system components, and communication between the MDM and external components such as the PowerFlex Gateway, PowerFlex GUI clients, vSphere plug-in, and CLI clients. Secure communication is typically installed and configured by default during system deployment.

NOTE:

If your system has been upgraded from a version earlier than version 2.0, or if secure communication between components was disabled during installation, follow the instructions provided in the section “Switching to secured authentication mode” in the PowerFlex Deployment Guide.

Internal component authentication

When this feature is enabled, the MDM generates a self-signed certificate for itself, and the SDSs generate certificates signed by the MDM’s certificate. The MDM has a single certificate for the entire cluster. The certificate is stored in the MDM repository.
Each SDS has its own SSL certificate file:

- Linux: `/opt/emc/scaleio/sds/cfg/sds_certificate.pem`
- Windows: `C:\Program Files\emc\scaleio\sds\cfg\sds_certificate.pem`

When an SDS is added to the cluster, the MDM receives a CSR (Certificate Signing Request) from the SDS, signs it with its own internal certificate and returns it to the SDS to be stored in its local key-store. If the SDS disconnects and reconnects, the MDM must authenticate it.

### External component authentication

Secure communications can be performed between the MDM and the following external components, and are typically enabled during deployment of the system:

- PowerFlex Gateway—The PowerFlex Gateway maintains the SSL certificates for itself and for the following components:
  - SNMP
  - REST API
  - PowerFlex Installer
- vSphere plug-in
- PowerFlex GUI
- CLI

### Workflow for self-signed security certificates

**About this task**

The system generates and signs self-signed certificates automatically when secure communication is enabled, and no user intervention is required. If you want to replace these certificates with new self-signed ones, follow this workflow:

**Steps**

1. Run the command `scli --generate_mdm_certificate`.

   To run CLI commands, you must be logged in. Actual command syntax is operating-system dependent. For more information, see the *PowerFlex CLI Reference Guide*.

2. When using the CLI, on the first connection to the MDM, the CLI will display the MDM's certificate and will prompt the user to approve the certificate.

   Upon approval, the trusted certificate will be saved.

3. When using the PowerFlex GUI, approve the MDM certificate at login, and then approve other certificates using the *System Settings* menu, *Renew Certificates* option.

### Workflow for externally signed security certificates

**About this task**

The system generates and signs self-signed certificates automatically when secure communication is enabled, and no user intervention is required. If you want to replace these certificates with ones signed by an external Certificate Authority, follow this workflow:

**Steps**

1. Log in to the system using the `scli --login` command as either a root user (on Linux) or as an administrator (on Windows).

2. Generate a CSR file, using the command `scli --generate_mdm_csr_file --target_mdm_ip <IP_ADDRESS>`.

   A file called `mdm-target_hostname.csr` will be created in the location:
   - Linux: `/opt/emc/scaleio/mdm/cfg`
   - Windows: `C:\Program Files\emc\scaleio\mdm\cfg`

   To run CLI commands, you must be logged in. Actual command syntax is operating-system dependent. For more information, see the *PowerFlex CLI Reference Guide*.

3. Submit the CSR file created in the previous step to your Certificate Authority.
The Certificate Authority must sign your CSR and return two files to you:

**a.** Certificate for your MDM  
**b.** Certificate Authority "Trusted" or "Root" certificate

4. Save the signed certificate for the MDM in the location:
   - **a.** Linux: `/opt/emc/scaleio/mdm/cfg`
   - **b.** Windows: `C:\Program Files\emc\scaleio\mdm\cfg`

5. Manually change the MDM certificate's file name to `mdm_signed_certificate.pem`.

6. Run the following script on the directory:
   ```
   ./apply_signed_certificate.py --mdm_ip <IP_address> --local_mdm_ip <IP_address>
   ```
   where `--mdm_ip` is the IP address of the Master MDM, and `--local_mdm_ip` is the IP address of the MDM where you want to change the certificate.

   If the remote read-only feature is enabled on the MDM, add `--skip_cli_command` to the command, and later, while logged in with security permissions, run the command `scli --replace_mdm_security_files`.

   **NOTE:**  
   This step changes the MDM certificate, and might cause a brief single point of failure period (switch ownership).

7. For all external components that will communicate with the MDM (PowerFlex GUI, CLI, vSphere Plugin, REST, PowerFlex Installer) add the Trusted or Root certificate from the Certificate Authority to each component.

   The Trusted/Root certificate must be added to the file called `truststore.jks`, using Keytool.

   For more information, see "Using Keytool to add certificates to external components".

8. When using the CLI, on the first connection to the MDM, the CLI will display a message similar to the following:
   ```
   [root@112CC-4 ~]# scli --login --username admin --password Scaleio018 Certificate required for issuer: /C=US/ST=MA/L=Hopkinton/O=EMC-Scaleio1213/CN=Scaleio018
   Please add the certificate with scli --add_certificate
   ```

   Add the Trusted/Root certificate using the `--add_certificate` command. For more information, see the PowerFlex CLI Reference Guide.

### Using Keytool to add certificates to external components

This topic explains how to add Certificate Authority certificates to PowerFlex external components. The `truststore.jks` file located on all components saves all the MDM/LIA certificates approved by the client. The file's location depends on the management client and operating system:

**PowerFlex Gateway**

- **Linux:**
  ```
  /opt/emc/scaleio/gateway/webapps/ROOT/WEB-INF/classes/certificates
  ```
- **Windows (64-bit):**
  ```
  C:\Program Files\EMC\ScaleIO\Gateway\webapps\ROOT\WEB-INF\classes\certificates
  ```

**PowerFlex GUI**

- **Linux:**
  ```
  /opt/emc/scaleio/gui/certificates
  ```
- **Windows:**
  ```
  C:\Users\[user_name]\AppData\Roaming\EMC\scaleio\certificates
  ```

**vSphere**

- **Linux:**
  ```
  $HOME/.vmware/scaleio/certificates
  ```
Using Keytool

Use the Java Keytool utility to modify or view the content of the trust store file. The remainder of this topic lists some useful Keytool commands. Keytool is a part of the Java (JRE or JDK) installation and can be found in the bin directory. You can add -storepass changeit to all commands that require a password. The password for the trust store is “changeit” (Java default).

NOTE:
The certificate alias must be unique in the trust store file. We usually use the certificate’s full subject.
For example: givenname=mdm, ou=asd, o=emc, l=hopkinton, st=massachusetts, c=us, cn=centos-6.4-adi5

- List the certificates in the trust store:
  ```
  keytool -list -v -keystore [path_to_certificates_folder]/truststore.jks
  ```
  Example:
  ```
  keytool -list -v -keystore C:\Users\cj\AppData\Roaming\EMC\scaleio\certificates\truststore.jks
  ```
- Check a particular entry using an alias:
  ```
  keytool -list -v -keystore [path_to_certificates_folder]/truststore.jks -alias [unique_alias] -storepass changeit
  ```
  Example:
  ```
  keytool -v -list -keystore C:\Users\cj\AppData\Roaming\EMC\scaleio\certificates\truststore.jks \truststore.jks -alias "givenname=mdm, ou=asd, o=emc, l=hopkinton, st=massachusetts, c=us, cn=centos-6.4-adi5"
  ```
- Add a new trusted certificate to the trust store:
  ```
  ```
  Example:
  ```
  keytool -import -trustcacerts -alias "givenname=mdm, ou=asd, o=emc, l=hopkinton, st=massachusetts, c=us, cn=centos-6.4-adi5" -file c:\temp\centos-6.4-adi5.cer -keystore C:\Users\cj\AppData\Roaming\EMC\scaleio\certificates\truststore.jks
  ```
- Delete a certificate from the trust store:
  ```
  keytool -delete -alias [unique_alias] -keystore [path_to_certificates_folder]/truststore.jks
  ```
  Example:
  ```
  keytool -delete -alias "givenname=mdm, ou=asd, o=emc, l=hopkinton, st=massachusetts, c=us, cn=centos-6.4-adi5" -keystore C:\Users\cj\AppData\Roaming\EMC\scaleio\certificates\truststore.jks
  ```
- Export a certificate from the trust store:
  ```
  ```
  Example:
  ```
  keytool -export -alias "givenname=mdm, ou=asd, o=emc, l=hopkinton, st=massachusetts, c=us, cn=centos-6.4-adi5" -file c:\temp\centos-6.4-adi5.cer -keystore C:\Users\cj\AppData\Roaming\EMC\scaleio\certificates\truststore.jks
  ```
Configure SDC access to the MDM

Configure SDC access to the MDM through the system.

To harden SDC access to the MDM, it is possible to restrict access, pending approval of the SDC by the system. The default system setting is full access (restricted SDC mode is disabled). When the restricted SDC mode is enabled, volumes can only be mapped to “approved” SDCs. Approval is obtained by issuing the `--add_sdc` command for each SDC. You can set restricted mode before or after SDCs have been added to your network.

You can use the following commands:

<table>
<thead>
<tr>
<th>Action</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable restricted SDC mode</td>
<td>set_restricted_sdc_mode command</td>
</tr>
<tr>
<td>Add an SDC to the approved list, when restricted SDC mode is enabled</td>
<td><code>--add_sdc</code></td>
</tr>
</tbody>
</table>

For more information, see the PowerFlex CLI Reference Guide.

Approved encryption methods

A specific set of encryption methods are approved for use with your system. These approved methods are:

- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256

NOTE: In order to use CURL with PowerFlex Gateway v2.0.0.3 and higher on a server running RHEL6, upgrade the NSS package to 3.21.0. (using YUM).

Login banner overview

A login banner is a text file that is displayed upon login to the system. It can be used to communicate messages or to obtain user consent to real-time monitoring of information and retrieval of stored files.

When the login banner is set up, it appears during the system login process before the login credential prompts. The login banner displays differently in the PowerFlex GUI and CLI interfaces:

- **PowerFlex GUI:**
  - When logging in, the login banner is displayed, and must be approved.
- **CLI:**
  - When logging in, the user is prompted to press any key, after which the banner is displayed.
  - To continue, the banner must be approved.

Limitations:

- Only users with administrative security rights can set up, update, or remove the login banner.
- Supported in Windows and RHEL operating systems.
- Text files up to 16 bytes are supported.
- Only one login banner is supported.
Set up a login banner using the CLI

Use the CLI to set up, modify, or stop displaying a login banner.

Prerequisites
Ensure that you have access to the IP address of the Master MDM.

Steps
1. Log in to PowerFlex using the IP address of the Master MDM.
2. Perform the desired operation:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Create (or modify) a new banner | a. Create a text file (or modify an existing file) with the message that you want to display in the login banner.  
  b. Run the following command:  
    
    `scli --set_login_banner --filename <FILENAME>`  
    
    where `<FILENAME>` is the path of the login banner text file.  
    
    The login banner is displayed the next time a user logs in to PowerFlex. |
| Stop displaying the banner  | a. Run the following command:  
  
  `scli --set_login_banner --remove_banner` |

Upload a login banner using the PowerFlex Installer

Use the Installer to upload a login banner that displays upon logging into the PowerFlex system.

About this task
The MDM credentials are stored in the Lockbox.

Steps
1. In the PowerFlex Installer, select the Maintain tab.
2. Click Security Settings and select Set Login Banner.
3. In the Set Login Banner for PowerFlex system, type the MDM password.
4. Click Set Login Banner

Enable/disable preemptive acceptance of the login banner

Preemptive acceptance of the login banner allows the user to bypass the login banner, for example, when running scripts. A user with admin security rights can enable or disable the option of preemptive acceptance. By default, preemptive acceptance is enabled and the login banner can be bypassed using a CLI command.

Prerequisites
To enable or disable the preemptive acceptance option, you must have administrative rights.

Steps
1. Log in to PowerFlex:

   `scli --login --username admin --password <PASSWORD>`
2. Run the following command to enable preemptive acceptance:

```bash
scli --set_cli_login_banner_preemptive_acceptance --enable
```

3. Run the following command to disable preemptive acceptance:

```bash
scli --set_cli_login_banner_preemptive_acceptance --disable
```

**Activate preemptive acceptance of the login banner**

When preemptive acceptance of the login banner is enabled (default), you can log in to PowerFlex in a special way that activates preemptive acceptance of the login banner.

**Prerequisites**

Preemptive acceptance of the login banner is enabled.

**Steps**

Log in to PowerFlex with the `accept_banner_by_scripts_only` parameter:

```bash
scli --login --username <USERNAME> --accept_banner_by_scripts_only
```

where `<USERNAME>` is the user running the script.

**Change LIA authentication method to LDAP**

Use the PowerFlex Installer to change the LIA authentication method to LDAP.

**About this task**

After upgrade, you can update the configuration from a native user to LDAP user. You first must add an LDAP Server to the system.

**Steps**

1. In the web browser, go to the IP address of your system's PowerFlex Gateway.
2. Log in to the PowerFlex Gateway.
3. From the **Maintain** tab, click **Security Settings** and select **Change LIAs authentication method to LDAP**. The **Change LIAs authentication method to LDAP for PowerFlex system** window is displayed.
4. Enter the admin password to the MDM in the **MDM admin password** box.
5. Enter the user name in the **LDAP User Name** box.
6. Enter the password to access the LDAP server in the **LDAP password** box.
7. Select **Force LDAP authentication mode** to force users to enter LDAP User Name and LDAP password when logging in to the PowerFlex system.
8. Click **Change LIAs authentication method to LDAP**.

**Results**

Use LDAP credentials to login to system.

**Add LDAP server**

Add LDAP servers to your PowerFlex system post installation.

**About this task**

**NOTE:** You can only add a max of eight servers.
**Steps**

1. In the web browser, go to the IP address of your system’s PowerFlex Gateway.
2. Log in to the PowerFlex Gateway.
3. From the **Maintain** tab, click **Security Settings** and select **Add LDAP Server**
   The **Add LDAP Server to PowerFlex system** dialog box is displayed.
4. Enter the admin password to the MDM in the **MDM admin password** box.
5. Enter the URI of the LDAP server in the **Server URI** box.
6. Enter the LDAP group identifier that you can retrieve from the LDAP server in the **Group** box.
7. Enter the LDAP BaseDN identifier that you can retrieve from the LDAP server in the **BaseDN** box. Run the query on the server to retrieve the BaseDN.
8. Click **Add LDAP Server**.

**Remove LDAP server**

You can remove LDAP servers from the PowerFlex system.

**Steps**

1. In the web browser, go to the IP address of your system’s PowerFlex Gateway.
2. Log in to the PowerFlex Gateway.
3. From the **Maintain** tab, click **Security Settings** and select **Remove LDAP Server**
   The **Remove LDAP Server from PowerFlex system** dialog box is displayed.
4. Enter the admin password from the MDM in the **MDM admin password** box.
5. Enter the URI of the LDAP server in the **LDAP Server URI** box.
6. Click **Remove LDAP Server**.
MDM and LDAP integration in an AMS managed system

PowerFlex supports local domain user authentication, and LDAP domain authentication. In addition, secure authentication is used between system internal and external components. This chapter provides the CLI commands used to create and manage PowerFlex users. The REST API can also be used to configure LDAP. For more information, see the operations for MDM clusters in the PowerFlex REST API Reference Guide.

- To set up local domain users, follow the instructions in this chapter.
- To set up LDAP users, see a detailed explanation in the document PowerFlex User Roles and LDAP Technical Notes. In general, the following steps must be performed:
  1. Add LDAP service to the MDM.
  2. Create Active Directory (AD) groups that correspond to the user roles offered by PowerFlex.
  3. Set the system-wide authentication method (use with caution, because it is complex to roll-back this operation).
  4. Log in again to apply the changes that you made.

User roles

The authorization permissions of each user role are defined differently for local authentication, and for LDAP authentication. Although the role names are similar, the permissions granted to them are not.

User roles defined in the LDAP domain are mutually exclusive, with no overlap—with the exception of the Configurator role. If you want to give an LDAP user permission to perform both monitoring and configuration roles, for example, assign that user to both the Backend/Frontend Configurator and Monitor LDAP groups.

The Configurator and Super User roles do not exist at all for LDAP.

The following table describes the permissions that can be defined for local domain users and for LDAP domain users.

<table>
<thead>
<tr>
<th>User role</th>
<th>Query</th>
<th>Configure parameters</th>
<th>Configure user credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Local</td>
<td>LDAP</td>
<td>Local</td>
</tr>
<tr>
<td>Monitor</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Configurator (this role is only applicable for local users)</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Yes (an aggregation of both Frontend and Backend Configurator)</td>
</tr>
<tr>
<td>Backend Configurator</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Backend operations only (Protection Domains, Storage Pools, Fault Sets, SDSs, Devices, other system settings)</td>
</tr>
<tr>
<td>Frontend Configurator</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Frontend operations only (Volumes, SDCs, Snapshots)</td>
</tr>
</tbody>
</table>
Table 2. Local and LDAP user roles and permissions (continued)

<table>
<thead>
<tr>
<th>User role</th>
<th>Query</th>
<th>Configure parameters</th>
<th>Configure user credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Local</td>
<td>LDAP</td>
<td>Local</td>
</tr>
<tr>
<td>Administrator</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Security Roles</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Super User</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Yes</td>
</tr>
</tbody>
</table>

(only one Super User is allowed per system, and it must be a local user)

Setting the User Authentication Method

`set_user_authentication_method`

Set the user authentication method for the system.

⚠️ **WARNING:** Use this command with caution. The operation is complex to roll back.

💡 **NOTE:** For details about setting up LDAP, refer to the *PowerFlex User Roles and LDAP Usage Technical Notes*.

**Syntax**

```
scli --set_user_authentication_method (--ldap_authentication | --native_authentication | --native_and_ldap_authentication | allow_ldap_without_admin) [--i_am_sure]
```

**Parameters**

`--ldap_authentication`

LDAP-based authentication method where users are managed on an LDAP-compliant server. Configure LDAP service and LDAP user before switching to this authentication method.

`--native_authentication`

Native authentication method where users are managed locally in the system

`--native_and_ldap_authentication`

A hybrid authentication method. Both LDAP and native users may log in to the system after it is set.

`--allow_ldap_without_admin`

Allow setting LDAP authentication method even if there is no LDAP service with administrator role.

`--i_am_sure`

Skip the safety questions for command execution. (For example: “This could damage the stored data. Are you sure?”)

**Example**

```
scli --set_user_authentication_method --native_and_ldap_authentication --i_am_sure
```
Adding and modifying local users

Users with the administrator role can manage system users, including adding new users and deleting existing users, modifying user credentials, and resetting user passwords.

The following CLI commands allow you to manage local users.

**add_user**

Add a user to the system. A randomly generated password for the created user is returned.

This command is available only to administrator users.

Each user name should conform to the following rules:

1. Contains fewer than 32 characters
2. Contains only alphanumeric and punctuation characters (when punctuation characters are being used, you may need to use the " or ' characters in order to allow it).
3. Is unique within the object type

**Syntax**

```
scli --add_user --username <NAME> --user_role {Monitor | Configure | BackEndConfigure | FrontEndConfigure | Security | Administrator} [--password <PASSWORD>]
```

**Parameters**

- **--username <NAME>**
  
  Username to add to the system

- **--user_role (Monitor | Configure | BackEndConfigure | FrontEndConfigure | Security | Administrator)**
  
  Role of the user: Monitor, Configurator, Backend Configurator, Frontend Configurator, Security, or Administrator. For information on user roles, see the PowerFlex User Guide.

- **--password <PASSWORD>**
  
  User's password. If the password parameter is not included, you will be prompted to enter the password.

**Example**

```
scli --add_user --username siuser2 --user_role Configure --password 3snU8fw7M
```

**delete_user**

Delete the specified user from the system.

This command is available only to administrator users.

**Syntax**

```
scli --delete_user (--user_id <ID> | --username <NAME>)
```

**Parameters**

- **--user_id <ID>**
  
  ID of the user to be deleted

- **--username <NAME>**
  
  Username of the user to be deleted
modify_user
Modify the user role of the specified user in the system.
This command is available only to administrator users.

Syntax
```
scli --modify_user (--user_id <ID> | --username <NAME>) --user_role {Monitor | Configure | BackEndConfigure | FrontEndConfigure | Security | Administrator}
```

Parameters
```
--user_id <ID>
User ID of the user to modify

**NOTE:** The user ID is displayed when you create the user. To find this ID at a later time, use the query_user command.

--username <NAME>
User name of the user to modify

--user_role {Monitor | Configure | BackEndConfigure | FrontEndConfigure | Security | Administrator}
Role of the user: Monitor, Configurator, Backend Configurator, Frontend Configurator, Security, or Administrator. For information on user roles, see the PowerFlex User Guide.
```

Example
```
scli --modify_user --username siuser3 --user_role Monitor
```

query_users
Display all the users defined in the system, with their roles and user ID.

Syntax
```
scli --query_users
```

Parameters
None.

Example
```
scli --query_users
```

query_user
Display information about the specified user.
This command is available only to administrator users.
Syntax

```
scli --query_user (--user_id <ID> | --username <NAME>)
```

**Parameters**

**--user_id <ID>**
User's ID number

**NOTE:** The user ID is displayed when you create the user. To find this ID at a later time, use the `query_user` command.

**--username <NAME>**
Name of the user

**Example**

```
scli --query_user --username sio_user
```

**reset_password**
Generate a new password for the specified user. The user must change the password again after logging in with the generated password. This command is available only to administrator users.

Syntax

```
scli --reset_password (--user_id <ID> | --username <NAME>) [--password <PASSWORD>]
```

**Parameters**

**--user_id <ID>**
User ID of the user whose password will be reset

**NOTE:** The user ID is displayed when you create the user. To find this ID at a later time, use the `query_user` command.

**--username <NAME>**
Username of the user whose password will be reset

**--new_password <PASSWORD>**
User's new password. If password is missing, the admin will be prompted to enter the password.

**Example**

```
scli --reset_password --username siouser3
```

**set_password**
Change the password of the user currently logged in to the system. This command is available only to administrator users.

Syntax

```
scli --set_password [--old_password <OLD_PASSWORD>] [--new_password <NEW_PASSWORD>]
```
Parameters

None.

--old_password <OLD_PASSWORD>
  User's current password

--new_password <NEW_PASSWORD>
  User's new password

**NOTE:** In Linux, to prevent the password from being recorded in the history log, omit the old_password or new_password flag and enter the password interactively.

Example

```
scli --set_password --old_password 1!2@3A --new_password P9*7&6
```

Password rules

The password must conform to the following rules:

1. Contains between six and 31 characters.
2. Contains characters from at least three of the following groups: [a-z], [A-Z], [0-9], special characters (!@#$ …)
3. The current password is not allowed.

**disable_admin**

Disables the default Superuser.

The Superuser is the default user for setting up the system, and has all the privileges of all user roles. In some cases you may need to disable the Superuser in order to ensure that all users are associated with specific user roles.

**NOTE:** To re-enable the Superuser, use the reset_admin command.

Syntax

```
scli --disable_admin
    [--i_am_sure]
```

Parameters

--i_am_sure
  Skip the safety questions for command execution.

Example

```
scli --disable_admin --i_am_sure
```

Reset the admin user password

You can reset the password of the default admin user (Superuser) using the combination of a file written to the MDM and the reset_admin CLI command.

**Prerequisites**

Ensure that you are using the admin user with Superuser permissions.
About this task

NOTE: The procedure refers only to the default admin user with Superuser permissions, which was created during the system setup.

Steps

1. Create a text file named MDM_SERVICE_MODE on the MDM in the location corresponding to your operating system:
   • Windows: C:\Program Files\emc\scaleio\MDM\logs\MDM_SERVICE_MODE
   • Linux: /opt/emc/scaleio/mdm/logs/MDM_SERVICE_MODE

2. In the body of the file, type the text Reset Admin, and save the file.

3. From the CLI, run the reset_admin command:
   
   ```
   scli --reset_admin
   ```

Results

The admin user password is reset to admin.

reset_admin

Reset the default Superuser.
Reset the password of the default admin user with Superuser permissions.

Syntax

```
 scli --reset_admin
   [--i_am_sure]
```

Parameters

--i_am_sure

Skip the safety questions for command execution.

Example

```
 scli --reset_admin --i_am_sure
```

Deploying PowerFlex using a non-root user

PowerFlex can be deployed or extended in Linux environments using a non-root sudo user in non-interactive mode.

Sudo is a program that allows a user to run or install a program as the root user. A sudo user can be created to deploy PowerFlex.

In order to successfully deploy or extend PowerFlex with a non-root user, the non-root user must meet the following conditions:

- The username included in the CSV file must already exist.
- The non-root user must be a sudo user.
- The non-root user must be in non-interactive mode.
- The requirement for TTY must be disabled.

In the CSV file used for deployment, you must indicate that you are intending to use a sudo non-root username by appending the string "(sudo)" to the user name in the Username field. For example, if you are using a non-root user with the username "non_root", enter the string "non_root(sudo)" in the username field of the CSV file.
Configure a non-root non-interactive sudo user

In Linux, you can deploy or extend PowerFlex with a non-root user. You must configure a non-root sudo user in non-interactive mode.

About this task

The following procedure details one method for configuring a non-root non-interactive sudo user. Perform the commands from the operating system console of where you want the PowerFlex Gateway to deploy PowerFlex.

Steps

1. Create a user group named "admin".
   ```bash
   groupadd admin
   ```

2. Create a user named "non_root" and add it to the admin group.
   ```bash
   useradd -G admin non_root
   ```

3. Change the password of the non_root user.
   ```bash
   passwd non_root
   ```
   When prompted, enter the new password and then confirm it by entering it again.

4. Open the sudoers /etc/sudoers file for editing.
   ```bash
   vi /etc/sudoers
   ```

5. Search the sudoers file for "## Same thing without a password".
   ```bash
   :s/## Same thing without a password
   ```

6. In the line below the search result, add the text %admin ALL=(ALL) NOPASSWD: ALL to the file.

7. Search the sudoers file for "Defaults requiretty", and replace it with Defaults ! requiretty.

8. Exit the vi editor by typing the following command to exit: :wq!

9. Create a hidden directory in the non_root user's home directory to store the SSH configuration.
   ```bash
   mkdir /home/non_root/.ssh
   ```

10. Copy the SSH configuration from the root user to the non_root user's directory.
    ```bash
    cp -rf /root/.ssh/* /home/non_root/.ssh/
    ```
Fault reporting features

General

SNMP traps are implemented as part of the PowerFlex Gateway, using SNMP v2. UDP transport is used for SNMP, and the default port for trap communication is 162. The SNMP feature is disabled by default. If you want to use the SNMP feature, enable it by editing the gatewayUser.properties file. For more information, see "Configure SNMP properties after deployment" in the Customize and Configure Guide.

The SNMP trap sender uses a proprietary/custom MIB called scaleio.mib. This MIB file is located on the PowerFlex Gateway server, in the webapps/ROOT/WEB-INF/classes folder under the PowerFlex Gateway installation directory. All traps are sent using a single notification type with a unique identification number (OID). All the SNMP traps contain variable bindings for severity; alert type, which is the alert classification text; the ID of the source object for which the alert was created; and an action code, which is the event number.

When using HP OpenView, ensure that the Dell EMC MIB file is loaded together with the PowerFlex MIB file, or save the Dell EMC MIB file in the same directory as the PowerFlex MIB file.

The alerts are calculated based on MDM polling. A trap will be sent the first time that an event occurs, and will be sent again if the resend interval has passed and the alert is still in effect. The resend frequency parameter can be configured using the Settings window in the PowerFlex GUI.

Only SNMP traps are supported, and are initiated by the PowerFlex SNMP traps manager. GET/SET operations are not supported (or more specifically, GET/GET NEXT/GET BULK/SET/INFORM/RESPONSE).

In addition to SNMP traps, alert messages are also displayed in the PowerFlex GUI.

To enable SNMP-based fault reporting, both the PowerFlex Gateway and the SNMP trap receivers must be configured. Traps can be sent to up to two SNMP trap receivers. The PowerFlex Gateway service must be restarted after configuration.

Configure SNMP properties after deployment

These procedures are mandatory for VMware-based systems where the SNMP feature is required. For other operating systems, configuration can be done either during deployment, or afterwards, using the instructions in this section.

The following procedures are required to enable the SNMP feature:

1. Create the Lockbox
2. Configure SNMP

Configure Dynamic Host Name resolution for SNMP in PowerFlex

Dynamic Host Name resolution and SNMP must be configured in the PowerFlex Gateway and on the DNS server to enable SNMP to forward traps to the SNMP trap receiver.

Prerequisites

Ensure that SNMP is already enabled and that SNMP traps are being received by at least one SNMP trap receiver, configured with an IP address.

About this task

The following procedures are required in order to set up a Dynamic Host Name resolution:

- On the PowerFlex Gateway, add the host name of the SNMP trap receiver to the appropriate parameter in the gatewayUser.properties file
- On the DNS server, configure the SNMP trap receiver properties, in order to support dynamic host name resolution
- On the DNS server, reduce the "Time To Live" (TTL) setting for the SNMP trap receiver
Steps
1. On the PowerFlex Gateway, open the gatewayUser.properties file.
   - From Linux: /opt/emc/scaleio/gateway/webapps/ROOT/WEB-INF/classes/gatewayUser.properties
2. Add the host name of the SNMP trap receiver to the property snmp.traps_receiver_ip=. If there is more than one IP address or host name, use a comma-separated list.
3. Save the file and restart the PowerFlex Gateway service.
4. Verify that traps are being received at all configured trap receiver hosts.
5. On the DNS server, configure dynamic host name resolution support for the trap receiver.
6. On the DNS server, reduce the TTL setting for the trap receiver. For example, on Windows, perform the following:
   a. Open the DNS manager window.
   b. Click View, and select the Advanced option.
   c. Right-click the trap receiver, and select Properties. A window similar to the following is displayed:
   d. At the bottom of the window, in the Time to live (TTL) field, change the value from one hour to one or two seconds.
   e. Click OK.

Results
Dynamic Host Name resolution configuration is complete.

Configure PowerFlex Gateway properties

Configure PowerFlex Gateway properties and additional PowerFlex features, using the gatewayUser.properties file.

Steps
1. Using a text editor, open the gatewayUser.properties file, located in the following directory on the PowerFlex Gateway server:

<table>
<thead>
<tr>
<th>PowerFlex Gateway operating system</th>
<th>Location of gatewayUser.properties file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>C:\Program Files\EMC\ScaleIO\Gateway\webapps\ROOT\WEB-INF\classes\</td>
</tr>
<tr>
<td>Linux</td>
<td>/opt/emc/scaleio/gateway/webapps/ROOT/WEB-INF/classes\</td>
</tr>
</tbody>
</table>
2. Edit the file with the desired changes, as follows:

<table>
<thead>
<tr>
<th>Use case</th>
<th>Property</th>
<th>Action</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable the reuse of previously used devices in the following use cases:</td>
<td>add.sds.with.force.on.next.run</td>
<td>Default: false</td>
<td>add.sds.with.force.on.next.run=true</td>
</tr>
<tr>
<td>• Add SDS devices that were used in a previous PowerFlex system. (Adding them without the true flag will cause deployment failure.)</td>
<td></td>
<td>To enable, set to true.</td>
<td></td>
</tr>
<tr>
<td>• Extend a system with an SDS whose devices were used in a previous system.</td>
<td></td>
<td>To disable, set to false.</td>
<td></td>
</tr>
<tr>
<td>• Extend a system by adding SDSs that are already installed on hosts</td>
<td></td>
<td><strong>NOTE:</strong> After finishing and marking the deployment as complete, the flag will revert to false, so you will need to set it again for future deployments, as necessary.</td>
<td></td>
</tr>
<tr>
<td>Use a PowerFlex Gateway that did not initially deploy your PowerFlex system</td>
<td>mdm.ip.addresses</td>
<td>Add the IP addresses of the system's MDM Master and Slaves, separated by semicolons, to this property. Both management and data IP addresses must be listed.</td>
<td>mdm.ip.addresses=10.76.60.232;10.76.60.233;10.76.60.234;10.76.30.10;10.76.30.11;10.76.30.12</td>
</tr>
<tr>
<td>Enable or disable the PowerFlex Installer</td>
<td>features.enable_IM</td>
<td>Default: true</td>
<td>features.enable_IM=false</td>
</tr>
<tr>
<td>You can completely disable the use of the PowerFlex Installer default port, 443, by setting both this property and the features.enable_gateway property to false.</td>
<td></td>
<td>To disable, set to false.</td>
<td></td>
</tr>
<tr>
<td>Enable PowerFlex Gateway</td>
<td>features.enable_gateway</td>
<td>Default: true</td>
<td>features.enable_gateway=false</td>
</tr>
<tr>
<td>You can disable the use of the default port, 443, by setting both this property and the features.enable_IM property to false.</td>
<td></td>
<td>To disable, set to false.</td>
<td></td>
</tr>
<tr>
<td>Enable SNMP</td>
<td>features.enable_snmp</td>
<td>Default: false</td>
<td>features.enable_snmp=true</td>
</tr>
<tr>
<td>To enable, set to true.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable SRS or email alert notifications</td>
<td>features.notification_method</td>
<td>Default: srs</td>
<td>features.notification_method=srs</td>
</tr>
<tr>
<td>To enable SRS, set to srs. To enable email notifications, set to email. Perform additional configurations for the other email notification properties in this configuration file.</td>
<td></td>
<td>To disable, set to none. To enable SRS, set to srs. To enable email notifications, set to email.</td>
<td></td>
</tr>
<tr>
<td>Set email notification type</td>
<td>notifications.emailSID.1.type</td>
<td>Default (only option currently available): callHome</td>
<td>notifications.emailSID.1.type=callHome</td>
</tr>
<tr>
<td>Use case</td>
<td>Property</td>
<td>Action</td>
<td>Example</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>---------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Set email notification SID: email sender identification (identity shown in the email’s &quot;From&quot; field)</td>
<td>notifications.emailSID.1.SID</td>
<td></td>
<td>notifications.emailSID.1.SID=<a href="mailto:DDD@dell.com">DDD@dell.com</a></td>
</tr>
<tr>
<td>Set email notification user name, required only when email notification uses SMTP server authentication</td>
<td>notifications.emailSID.1.username</td>
<td></td>
<td>notifications.emailSID.1.username=user123</td>
</tr>
<tr>
<td>Set email notification SMTP server name</td>
<td>notifications.emailSID.1.smtp</td>
<td></td>
<td>notifications.emailSID.1.smtp=mailhub.iss.emc.com</td>
</tr>
<tr>
<td>Enable SMTP authenticated mode for email notification</td>
<td>notifications.emailSID.1.authenticate</td>
<td>Default: false</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>To disable, set to false</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>To enable, set to true</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>In addition, configure the user name, using the property notifications.emailSID.1.username, and configure the password using REST API, as described in the Configure and Customize PowerFlex Guide</td>
<td></td>
</tr>
<tr>
<td>Set a custom port for email notification (optional; will override default port number 25)</td>
<td>notifications.emailSID.1.port</td>
<td>Default: 25</td>
<td>notifications.emailSID.1.port=25</td>
</tr>
<tr>
<td>To restrict login to LDAP users only (disable local user login)</td>
<td>gateway-admin.disable.local.login</td>
<td>Default: false</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>To enable, set to true</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information about setting up the PowerFlex Gateway admin login credentials for using LDAP server\servers, see the PowerFlex User Roles and LDAP Usage Technical Notes.</td>
<td></td>
</tr>
<tr>
<td>Change the name of the VASA Provider replica set. When there are three VASA Providers, a replica set is created during deployment to facilitate communication between VASA Providers.</td>
<td>vasa.provider.replica.set.name</td>
<td>Default: vasa-rs</td>
<td>vasa.provider.replica.set.name=vasa-rs</td>
</tr>
<tr>
<td>Enable or disable monitoring of VASA Providers</td>
<td>features.enable_vasa_monitor</td>
<td>Default: true</td>
<td>features.enable_vasa_monitor=true</td>
</tr>
<tr>
<td>Set the list of IP addresses for VASA Providers</td>
<td>vasa.provider.ips</td>
<td>A comma-separated list of IP addresses of all the VASA Providers. The installation process sets this property, but it can also be set manually.</td>
<td>vasa.provider.ips=&lt;ip&gt;,&lt;ip&gt;,...</td>
</tr>
<tr>
<td>Set the port of the VASA Providers’ REST service, in order to monitor the page</td>
<td>vasa.provider.monitor.port</td>
<td>Default: 8080</td>
<td>vasa.provider.monitor.port=8080</td>
</tr>
<tr>
<td>Use case</td>
<td>Property</td>
<td>Action</td>
<td>Example</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------</td>
<td>---------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>http://&lt;ip&gt;:&lt;port&gt;/actuator/health</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set the number of seconds to sleep between each sample</td>
<td>vasa.provider.monitor.interval.seconds</td>
<td>Default: 60</td>
<td>vasa.provider.monitor.interval.seconds=60</td>
</tr>
<tr>
<td>When installing VASA in a VMware environment, set this property to false in order to enable extending the system with the PowerFlex Installer.</td>
<td>vmware</td>
<td>In a Linux environment, default: false. In a VMware environment, default: true When installing VASA in a VMware environment, set the value to false.</td>
<td>vmware=false</td>
</tr>
</tbody>
</table>

3. Save and close the file.
4. Restart the PowerFlex Gateway service:
   - Windows: From the Windows Services window, restart the EMC ScaleIO Gateway.
   - Linux: Type the following command:
     
```
     service scaleio-gateway restart
     ```

**Results**

Configuration is complete.
Add, Remove or Rename Components

Using SSH authentication on the PowerFlex Gateway

Create SSH keys for servers in a new or existing PowerFlex system.

Prerequisites
Lockbox must be configured on the PowerFlex Gateway.

About this task
A manually generated public-private key pair can be used to perform SSH key authentication, instead of passwords, between the PowerFlex Gateway and PowerFlex system servers. The public key is placed on all servers that will allow access to the PowerFlex Gateway. The PowerFlex Gateway is the owner of the matching private key.

FOSGWTool is used to upload the private key to the PowerFlex Gateway. FOSGWTool is located in:
- Linux: /opt/emc/scaleio/gateway/bin/FOSGWTool.sh
- Windows: C:\Program Files\EMC\ScaleIO\Gateway\bin\ FOSGWTool.bat

NOTE: For systems using SSH key authentication, there is no need to add node user name and password credentials to the CSV file used for system deployment.

Steps
1. Create the private and public key pair on the node where the PowerFlex Gateway is installed:
   a. In command line, run the command:
      
      ```
      cd ~/.ssh/
      
      ssh-keygen -t rsa
      ```
      
      This command generates a private and public key. When performing this command, you can add a passphrase, or generate the key without a passphrase. Two SSH keys are produced: id_rsa and id_rsa.pub.
   
2. On one of the PowerFlex servers, run this command to store the public key in the authorized_keys file:
   
   ```
   cat ~/.ssh/id_rsa.pub | cat >> ~/.ssh/authorized_keys
   ```

3. Copy the .ssh directory to the rest of the PowerFlex servers.
4. Copy id_rsa.pub to the file system on the rest of the PowerFlex servers.
5. Use FOSGWTool in command line to upload the private key to thePowerFlex Gateway:
   
   ```
   FOSGWTool --update_ssh_key --ssh_key <PATH_TO_SSH_KEY_FILES> [--key_passphrase <KEY_PASSPHRASE>]
   ```
   
   The --key_passphrase is optional. Add this if you generated it when you created the key pair. During deployment, the gateway will use the private key for authentication.

6. Restart the PowerFlex Gateway service:
   - Windows: From the Windows Services window, restart the EMC ScaleIO Gateway.
Adding components to an existing PowerFlex environment

You can expand your PowerFlex environment as you require.

This section describes how to add components to an existing PowerFlex installation.

In physical environments, you add components with the PowerFlex Installer. In VMware environments, you add components with the VMware deployment wizard.

Add components using the PowerFlex Installer

You can add components using the PowerFlex Installer

About this task

You first need to update the CSV topology file with the new components, then you can use the PowerFlex Installer to add them.

The secure communication mode of components must match the mode of the system to which the components are being added. If they do not match, you must either change the mode of the components to be added or change the mode of the system so that they match.

Steps

1. Follow the procedure described in "Customizable installation using CSV file - hyper-converged system" or "Customizable installation using CSV file - 2-layer system" in the Deploy PowerFlex Guide.

   **NOTE:**
   Use the same LIA password that was configured during initial installation.

2. In the Upload CSV stage, browse to the updated CSV file, and select Add to existing sys.
3. Upload the CSV, and continue as normal.

Add components using the VMware deployment wizard

You can add PowerFlex components to an existing system using the VMware deployment wizard.

About this task

**NOTE:** The following procedure cannot be used to add an SDS component to an existing SVM. To do so, contact Dell EMC Support.

Steps

1. From the Basic tasks section of the screen, click Deploy PowerFlex environment.

   The PowerFlex VMware deployment wizard begins. If you exited the previous deployment before completion, you will be able to return from where you left off.

   **NOTE:** The deployment wizard assumes that you are using the provided PowerFlex OVA template to create the Storage Virtual Machines (SVMs).

2. In the Select Installation screen, select Add servers to a registered PowerFlex system, and select the system you want to extend.
3. Continue with the deployment steps, adding the new nodes.

   You can skip steps that do not need to be changed.

   **NOTE:** When adding components, the wizard adjusts the displayed screens to options that are relevant to the current PowerFlex system.
4. Complete the deployment.

**NOTE:** After extending an existing SVM with a new PowerFlex role/component, you must perform manual memory allocation on the SVM, as described in "SVM manual memory location" in the *Deployment Guide.*

## Remove PowerFlex

You can remove PowerFlex components and the vSphere plug-in from servers.

To uninstall PowerFlex, use the PowerFlex Installer. This requires that the LIA be installed in all nodes to be changed.

When removing RFcache (the `xcache` package) on a Windows server, a server restart is necessary after the removal.

To unregister the vSphere plug-in, see "Unregistering the PowerFlex plug-in".

### Remove PowerFlex using the PowerFlex Installer

You can remove PowerFlex using the PowerFlex Installer.

#### About this task

All PowerFlex components in the system that are being accessed are removed. This information is attained from the LIA that is installed on every node.

#### Steps

1. Log in to the PowerFlex Installer:
   a. Point your browser to this URL: https://<GW_Server_IP>
      where `<GW_Server_IP>` is the IP address of the server where you installed the PowerFlex Gateway package.
   b. Accept the certificate warning; alternatively, install your own certificate for the Tomcat server.
   c. Enter the default user name, `admin`, and the password defined when the PowerFlex Gateway was prepared, and then click **Login**.

2. From the PowerFlex Installer, select the **Maintain** tab.

3. In the **Maintenance operation** screen, type the authentication credentials, then click **Retrieve system topology**.
   The system topology is displayed.

4. Click the **Show Uninstall button** link, and confirm enabling this option.
   The uninstall operation may take some time, depending on your system topology. This operation cannot be rolled back.

5. Click **Uninstall**.
   A confirmation dialog is displayed.

   **NOTE:** Uninstalling an SDC component requires a machine restart. If you are uninstalling SDC components on Windows servers, select to enable automatic restart (on those servers only). Alternatively, you can manually restart these servers after removing the SDC.

   On Linux servers, if the kernel module is busy, perform a manual restart.

6. Enter the MDM password, select to reboot servers (optional), and click **Uninstall**.
7. To monitor the uninstallation progress, click **Monitor**.
8. When the uninstallation is complete, click **Mark operation completed**.

### Unregister the PowerFlex plug-in

Remove a registered vSphere PowerFlex plug-in.

#### About this task

To remove the currently registered PowerFlex plug-in, perform the following:

#### Steps

1. Run the script to remove the PowerFlex plug-in:
a. From the folder where you extracted the current PowerFlex plug-in ZIP file (for example: EMC-ScaleIO-vSphere-plugin-installer-3.5-<build>.<X>.zip), use PowerCLI to run the PowerFlex plug-in script (for example: VxFlexOSPluginSetup.ps1).

b. Select option 2. Unregister PowerFlex plug-in.

2. Enter the vCenter credentials and confirm the script actions.
3. Log out, then log back in to the vSphere web client.
4. The PowerFlex plug-in is no longer registered.

Renaming objects

About this task

Object names are used to identify the objects in the PowerFlex GUI, and can also be used to specify objects in CLI commands. You can view an object’s name in its Property Sheet, in the Identity section.

NOTE: It is not possible to rename a Read Flash Cache device using this command.

You can define object names according to the following rules:

1. Contain less than 32 characters
2. Contain only alphanumeric and punctuation characters
3. Be unique within the object type

When a name has not been defined, the system may display default system-defined names, as follows:

- SDC—its first IP address
- SDS—its first IP address
- Device—the path to the device
- All other objects—the object’s ID

NOTE: A name must be assigned to a volume when it is initially created. You can rename the volume later, using the Rename command.

Steps

1. In the Dashboard left pane, click the relevant object type (for example: SDSs, Storage Pools, Devices).
2. Select the relevant row and click Modify > Rename.
3. In the Rename object name dialog box, enter the new name and click Apply.
4. Verify that the operation completed successfully and click Dismiss.
Enable automatic log collection

You can enable auto collect logs in the PowerFlex system.

Automatic log collection allows the PowerFlex Gateway to automatically collect information from a PowerFlex system when alerts of severity level 5 (critical) are raised.

The log is saved to a known directory under a name which includes the date the log was created, the alert name and severity.

For this feature to work, the MDM credentials and LIA password must be defined in the lockbox. If a LIA password is not defined in the lockbox, an error appears when selecting the Auto Collect Logs checkbox.

Set ESXi credentials for auto collect logs

Select the files to collect from the PowerFlex system according to your requirements.

1. From the Maintain tab, click System Logs & Analysis and select Set ESXi Credentials for Auto Collect Logs.
   The Confirm Set Credentials of your PowerFlex system dialog box is displayed.
2. Enter the admin password to the MDM in the MDM admin password box.
3. Select the option according to the files that you require from the PowerFlex system:
   - Collect debug information
     - Latest logs only - collects the files that are checked in the Show Collected Information drop-down list.
     - Add repositories - collects all the files from the Show Collected Information drop-down list. We recommend this option, as all files are collected.

   When both options are selected, the files that are checked in the Show Collected Information drop-down list are collected.
   - Collect exceptions only - only the All exp.* files option is collected.
4. Select Include all nodes in log collection to collect logs from all nodes in your PowerFlex system.
5. Click Set Credentials to save the log configuration settings.
Change LIA behavior

You can change the default behavior of the LIA by editing its configuration file.

The default location of the LIA configuration file is host operating system dependent, as follows:

- Windows: C:\Program Files\emc\scaleio\LIA\cfg\conf.txt
- Linux: /opt/emc/scaleio/ lia/cfg/conf.txt

The following are some values relevant to LIA behavior:

```
lia_token=5
lia_enable_install=1
lia_enable_uninstall=1
lia_enable_configure_fetch_logs=1
```

To restrict which PowerFlex Gateway IP addresses can access the LIA, add those IP addresses to this line in the `conf.txt` file:

```
lia_trusted_ips=<IP_ADDRESS_1>,<IP_ADDRESS_2>
```

To set this during LIA installation, set the TRUSTED_IPS environment variable. For example:

```
TRUSTED_IPS=1.2.3.4,5.6.7.8 rpm -i lia.rpm
```

Add LIA to a system to enable automated maintenance and upgrades

Add the LIA, a component that is required to use the PowerFlex Installer to upgrade and maintain PowerFlex physical server system components.

**Prerequisites**

To determine if the LIA is installed, run the following command on any server in the system:

```
rpm -qa | grep -i LIA
```

If LIA is not installed, you must install it before proceeding.

**About this task**

Physical machine upgrade uses the PowerFlex Installer (part of the PowerFlex Gateway), together with the LIA of the new version, to orchestrate the upgrade.

**Steps**

1. Install the LIA component on every node, by running the following command:

   ```
   TOKEN=<LIA_password> rpm -i <full rpm path to LIA file>
   ```

   **Example:**

   ```
   TOKEN=Scaleio123 rpm -i EMC-ScaleIO-lia-3.5-X.<build>.<flavor>.x86_64.rpm
   ```

   The password must meet the following criteria:
The LIA password must be identical in all LIAs within the same system.

2. Import the system installation ID into the LIA:
   a. Create the following file:
      `/opt/emc/scaleio/lia/cfg/installation_id.txt`
   b. Query the MDM for the installation ID by running the following command:
      ```
      scli --query_all|grep "Installation ID"
      ```
   c. Copy the installation ID into the new file.
   d. Restart the LIA service by running the following command:
      ```
      pkill lia
      ```

3. Repeat the previous steps on every node in the system.

**Results**
LIA is installed.
VMware environment specific tasks
The following topics describe how to configure PowerFlex plug-in.

**Configure components**

You can configure settings for PowerFlex from the PowerFlex plug-in. The main summary view of the PowerFlex plug-in only shows MDM cluster members: Master, Slave, Tie-Breaker, and Standby, but many other components of the system can be configured using the PowerFlex plug-in.

There are two levels of component configurations:

- **Basic**: The basic configurations are all performed the same way. The process is described just once.
- **Advanced**: Each advanced configuration setting has a unique dialog box, which is described in "Configuring components-advanced".

The following table lists the activities you can perform and categorizes each as basic or advanced:

**Table 3. Plug-in activity matrix**

<table>
<thead>
<tr>
<th>Object</th>
<th>Perform this activity</th>
<th>Basic or advanced</th>
<th>Access from this screen</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Deploy PowerFlex</td>
<td>Advanced. See the PowerFlex Deployment Guide.</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>Register an existing system</td>
<td>Basic. Enter the system Master MDM IP address, user name, and password.</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>Unregister a system</td>
<td>Basic</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>Update system credentials</td>
<td>Basic. Enter new username and password.</td>
<td></td>
</tr>
<tr>
<td>PowerFlex Gateway</td>
<td>Register/Update Gateway</td>
<td>Basic. Enter IP address, operating system username, and operating system password.</td>
<td></td>
</tr>
<tr>
<td>PowerFlex Gateway</td>
<td>Open Gateway</td>
<td>Basic. Navigates to the PowerFlex Installer.</td>
<td></td>
</tr>
<tr>
<td>Protection Domain</td>
<td>Create a Protection Domain</td>
<td>Basic</td>
<td></td>
</tr>
<tr>
<td>Protection Domain</td>
<td>Remove a Protection Domain</td>
<td>Basic</td>
<td></td>
</tr>
<tr>
<td>Storage Pool</td>
<td>Create a Storage Pool</td>
<td>Basic</td>
<td></td>
</tr>
<tr>
<td>Storage Pool</td>
<td>Remove a Storage Pool</td>
<td>Basic</td>
<td></td>
</tr>
<tr>
<td>Storage Pool</td>
<td>Configure Read RAM Cache</td>
<td>Basic</td>
<td></td>
</tr>
<tr>
<td>SDS</td>
<td>Add a device to an SDS</td>
<td>Advanced</td>
<td></td>
</tr>
<tr>
<td>SDS</td>
<td>Remove a device from an SDS</td>
<td>Basic</td>
<td></td>
</tr>
</tbody>
</table>
Table 3. Plug-in activity matrix (continued)

<table>
<thead>
<tr>
<th>Object</th>
<th>Perform this activity</th>
<th>Basic or advanced</th>
<th>Access from this screen</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDC</td>
<td>Install SDC on ESX</td>
<td>Advanced</td>
<td>SDCs</td>
</tr>
<tr>
<td></td>
<td>Upgrade SDC</td>
<td>Advanced</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Update SDC Parameters</td>
<td>Advanced</td>
<td></td>
</tr>
<tr>
<td>Volume</td>
<td>Create and map volumes</td>
<td>Advanced</td>
<td>Storage Pools</td>
</tr>
<tr>
<td></td>
<td>Map a volume</td>
<td>Advanced</td>
<td>Volumes</td>
</tr>
<tr>
<td></td>
<td>Remove a volume</td>
<td>Basic</td>
<td>Volumes</td>
</tr>
<tr>
<td></td>
<td>(must be unmapped first)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unmap a volume</td>
<td>Advanced</td>
<td>Volumes</td>
</tr>
<tr>
<td></td>
<td>Configure Read RAM Cache</td>
<td>Basic</td>
<td>Volumes</td>
</tr>
<tr>
<td>Fault Set</td>
<td>Create a Fault Set</td>
<td>Basic</td>
<td>Protection Domains</td>
</tr>
<tr>
<td>Device</td>
<td>Clear a device error</td>
<td>Basic</td>
<td>Devices</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Removes the error message. Can be performed only after clearing the error.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Add a device to an SDS</td>
<td>Advanced</td>
<td>SDSs</td>
</tr>
<tr>
<td></td>
<td>Remove a device from an SDS</td>
<td>Basic</td>
<td>Devices</td>
</tr>
</tbody>
</table>

a. For Read RAM Cache to work on a volume, both the volume and its Storage Pool must have the feature enabled.
b. When defining Fault Sets, you must follow the guidelines described in “Fault Sets”. Failure to do so may prevent creation of volumes.

### Configure components—basic

Create a Protection Domain in the PowerFlex system from the PowerFlex plug-in.

**About this task**

Basic configuration activities are all performed in a similar manner. All activities are performed from the **Actions** menu in each screen and by entering simple information.

Following is an example on how to create a Protection Domain from the **PowerFlex Systems** screen.

**Steps**

1. From the **PowerFlex Systems** screen, click **Actions > Create Protection Domain**:
NOTE: You can also click the action icons in the menu or right-click the item to choose options from a list.

2. In the Create Protection Domain dialog box, enter a name for the Protection Domain, and then click OK.

   The process is similar for the rest of the basic activities.

   NOTE: If you intend to enable zero padding on a Storage Pool, you must do so before you add any devices to the Storage Pool. For more information, see "Storage Pools" in the Getting to Know PowerFlex Guide.

Configuring components—advanced

This section describes how to use the PowerFlex vSphere plug-in to perform activities that require a little more attention.

Register an existing system

Use the PowerFlex plug-in to register an existing PowerFlex.

About this task

Enter the following information of the existing PowerFlex system.

Steps

1. From the main PowerFlex plug-in window, click Register PowerFlex system.
2. Enter the following information, then click OK:
   a. Master MDM IP: The IP address of the existing system's Master MDM
   b. User name: The username of the existing system
   c. Password: The password of the existing system

Volumes in the vSphere environment

The following topics describe how to use the PowerFlex plug-in to add, map, and unmap volumes in the vSphere environment. You can map volumes to SDCs in the same step, or you can map the volume after it has been created.

Add devices to an SDS—PowerFlex plug-in

Use the vSphere PowerFlex plug-in to add devices to an SDS in PowerFlex.

About this task

In a DirectPath-based system, you add devices only after the deployment. In an RDM/VMDK-based PowerFlex, you can add devices during and after the deployment.

You can add a Storage device or an Acceleration device to an SDS or to all SDSs in the system. For a Storage device, you must define the Storage Pool and Media Type for each device you add. For Acceleration device, you must select the Acceleration Pool (which may be RFCache or NVDIMM) for each device added. For Fine Granularity (FG), an Acceleration device must be configured with NVDIMM. For more information on FG, see "Data layout" in the Getting to Know Guide.

All data on added devices will be erased.
NOTE: If you intend to enable zero padding on a Storage Pool, you must do so before you add any devices to the Storage Pool.

**Steps**

1. From the **SDSs** screen of the PowerFlex plug-in, select one of the following:
   - Right-click a specific SDS, and then select **Add devices to a single SDS**.
   - Right-click any SDS, and then select **Add devices to PowerFlex system**.

   The **Add Device** dialog box is displayed. All devices that can be attached to the selected SDS are listed. For the system view, all SDSs are listed, and you can choose devices to add for each SDS. It may take a few moments to load the list of devices from the vCenter.

2. Add devices:
   - One-at-a-time:
     a. Select whether the device should be used for storage or to provide acceleration.
     b. Select the Storage Pool to which the devices should be assigned.
     c. To enable the use of devices that may have been part of a previous PowerFlex system, select **Allow the take over of devices with existing signature**.
     d. Click **OK**.
   - All devices on a server at once:
     a. Click **Select all devices**.
     b. Select whether to use the devices for storage or to provide acceleration.
     c. Select the Storage Pool to which the devices should be assigned.
     d. To enable the use of devices that may have been part of a previous PowerFlex system, select **Allow the take over of devices with existing signature**.
     e. Click **Assign**.

3. Confirm the action by typing the PowerFlex password.

4. When the add operation is complete, click **Close**.

**Results**

The devices are added.

---

**Upgrading an SDC—PowerFlex plug-in**

Upgrading an SDC is performed with the PowerFlex plug-in. This topic is described in the Upgrade PowerFlexGuide.

**Modify SDC-MDM communication parameters on SDCs**

When MDM IP addresses have been added or changed, use the vSphere PowerFlex plug-in to update the SDCs with system parameters that are needed to ensure continued SDC-MDM communication.

**Steps**

1. From the PowerFlex plug-in **Advanced tasks** menu, click **Update SDC parameters**, and follow the on-screen instructions to complete the process.

2. Ensure that the parameters were updated on the SDC by running this command on each ESXi host:
   ```bash
   cat /etc/vmware/esx.conf |grep scini|grep -i mdm
   ```

**Configuring virtual IP addresses—PowerFlex plug-in**

Configure virtual IP addresses in the vSphere PowerFlex plug-in.

**Steps**

1. From the **PowerFlex Systems** screen, click **Actions** and select **Configure virtual IPs**.

2. In the **Configure virtual IPs** dialog box, select the network and enter a virtual IP address.
Next steps

To update the SDC configuration, update the SDC parameters.
Manually performed tasks

The following tasks describe how to manually perform certain tasks in your PowerFlex environment.

Clean the PowerFlex VMware environment

For 2-layer systems, or ESXi-based systems, clean the PowerFlex VMware environment in order to perform a clean installation. This procedure is recommended for cases when previously defined networks will be used again, or when PowerFlex components such as SDCs that ran on other networks exist in the environment.

Prerequisites

Before you begin, unmap and delete any PowerFlex volumes in your system.

If necessary, unregister PowerFlex from within the vSphere PowerFlex plug-in, and delete all the PowerFlex SVMs.

Steps

1. Close the existing PowerCLI sessions, set PowerCLI to **Run as administrator**, and then open a new session.
2. Using the PS1 script, unregister the PowerFlex plug-in.
3. Stop the vSphere web client service:
   - VC Linux: `service-control --stop vsphere-client`
4. Delete the contents of the PowerFlex plug-in folder.
   - The vSphere web client (Virgo) plug-in folders are located at:

<table>
<thead>
<tr>
<th>vCenter</th>
<th>Operating system</th>
<th>Path to file</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.x</td>
<td>Windows</td>
<td>C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
<td>/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity</td>
</tr>
</tbody>
</table>
5. Delete the **scaleio** folder or its contents.
   - The **scaleio** folders are located at:

<table>
<thead>
<tr>
<th>vCenter</th>
<th>Operating system</th>
<th>Path to file</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.x</td>
<td>Windows</td>
<td>C:\Users\vspherewebclientsvc\AppData\Roaming\VMware\scaleio</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
<td>/etc/vmware/vsphere-client/vc-packages/scaleio</td>
</tr>
</tbody>
</table>
6. Start the vSphere web client service:
   - VC Linux: `service-control --start vsphere-client`
7. Clear your web browser’s cache and cookies, or open a different web browser.
8. Using the PS1 script in PowerCLI, register the PowerFlex plug-in.
   - **NOTE:** Do not press ENTER at this point.
9. After you have logged in to the vSphere web client to complete the registration and you see the PowerFlex icon
   - press ENTER in the PowerCLI session.
If necessary, remove the SDC module parameters and VIB from the ESXi servers:

a. Connect to each ESXi server via SSH.

b. Run:

```
~ # esxcli system module parameters set -m scini -p ""
~ # esxcli software vib remove -n scaleio-sdc-esx6.0
```

c. Reboot each ESXi server.

11. Proceed to the procedures for re-registering the PowerFlex plug-in, and then deploy PowerFlex.

**SVM manual memory allocation**

Manual memory allocation for SVMs is required in a number of scenarios. However, when using the plug-in for a clean deployment, SVM memory allocation is performed automatically.

**About this task**

The formula for calculating SVM memory requirements can be found in the *Getting to Know PowerFlex Guide*.

In the following cases, SVM memory allocation must be performed manually:

- Manual deployment on VMware.
- Extending an existing SVM with a new PowerFlex role/component, whether this is being done with the plug-in or manually.
  
  Workaround: Perform all the parts of step 1 and step 2 before extending the additional role/component on the SVM. Perform the steps on one SVM at a time.
- Changing the SDS performance profile, post deployment.
  
  Workaround: Perform all the parts of step 1, one SVM at a time.

**Steps**

1. For SVMs that are SDS-only, perform the following:
   
   a. Move the SDS to maintenance mode (MM).
   
   b. Shut down the SVM.
   
   c. Increase SVM memory, according to the formula below.
   
   d. Power up the SVM.
   
   e. Exit MM.

2. For SVMs that are MDM (Master, Slave, or TB, may contain SDS, also):
   
   a. Start with Slaves and TBs:
      
      i. Move the SDS to maintenance mode (MM).
      
      ii. Shut down the SVM.
      
      iii. Increase SVM memory, according to the formula below.
      
      iv. Power up the SVM.
      
      v. Exit MM.

   b. Proceed with the Master MDM:
      
      i. Switch ownership, so the Master MDM is now a Slave MDM.
      
      ii. Move the SDS to maintenance mode (MM).
      
      iii. Shut down the SVM.
      
      iv. Increase SVM memory, according to the formula below.
      
      v. Power up the SVM.
      
      vi. Exit MM.
Managing ESXi servers

Using the following procedures, you can modify parameters on ESXi servers and check the SDC state on ESXi servers.

Modify parameters on ESXi servers

Use esxcli commands on an SDC running on an ESXi server to update parameters.

About this task

The following esxcli commands can be used in the following cases:

- MDM IP addresses need to be added to the existing list on an SDC
- MDM IP addresses need to be replaced on an SDC
- The SDC’s GUID needs to be changed

Specifically, the SDC’s GUID or IP address needs to be identified, and then used to add or modify the MDM IP addresses or GUID (depending on the parameter that you want to modify). If you want to add additional MDM IP addresses to existing ones, you must list both old and additional IP addresses in the esxcli command.

For more information about SDC tuning, see PowerFlex Performance Fine-Tuning Technical Notes.

If the current configuration of PowerFlex is registered with a v2.0 VMware plug-in, you can use the plug-in Update SDC parameters to update the MDM IP addresses. For more information, see the Deploy PowerFlex Guide.

NOTE: These procedures require a server restart to apply the new configuration. The configuration will remain persistent after future server restarts.

To configure MDM IP addresses on the SDC, perform these steps:

Steps

1. Find the SDC’s GUID and the MDM IP addresses configured on the ESX, by typing the command:

   ```
esxcli system module parameters list -m scini
   
   esxcli system module parameters list -m scini
   ```

2. In the output of the command, find the existing GUID and MDM IP addresses.

   For example, in the output excerpt below, the GUID and IP addresses are marked in bold:

   ```
   IocltlniGuidStr string
   39b89295-5cfc-4a42-bf89-4cc7e55a1e5b
   Ini Guid, for example: 12345678-90AB-CDEF-1234-567890ABCDEF
   
   IocltlMdmIPStr string
   Mdms IPs, IPs for MDM in same cluster should be comma-separated. To configure more than one cluster use '+' to separate between IPs. For Example: 10.20.30.40,50.60.70.80+11.22.33.44. Max 1024 characters
   ```

3. To configure the MDM IP addresses on the SDC, type the command

   ```
esxcli system module parameters set -m scini -p "IocltlniGuidStr=<GUID> IocltlMdmIPStr=<MDM_IPS>"
   ```

   where `<GUID>` is the existing SDC GUID that you identified in the previous step, and `<MDM_IPS>` is the list of MDM IP addresses. A maximum of 1024 characters is allowed.

   a. To replace the old MDM IP addresses with new MDM IP addresses, omit the old addresses from the command.
   b. To add MDM IP addresses to the existing IP addresses, type both the existing IP addresses and the new IP addresses in the command.
MDM IP addresses for MDMs in same cluster must be comma-separated. To configure more than one cluster, use '+' to separate between IP addresses in different clusters. For example:

```bash
esxcli system module parameters set -m scini -p "IoctlIniGuidStr=39b89295-5cfc-4a42-bf89-4cc7e55a1e5b
IoctlMdmIPStr=10.20.30.40,50.60.70.80+11.22.33.44"
```

4. To apply the new configuration, restart the ESX server.

5. To change the GUID of the SDC, perform these steps:

   a. Find the SDC’s GUID and the MDM IP addresses configured on the ESX, by typing the command

   ```bash
   esxcli system module parameters list -m scini
   ```

   b. In the output of the command, find the existing GUID and MDM IP addresses.

   For example, in the output excerpt below, the GUID and IP addresses are marked in bold:

   ```
   IoctlIniGuidStr string 39b89295-5cfc-4a42-bf89-4cc7e55a1e5b Ini Guid, for example: 12345678-90AB-CDEF-1234-567890ABCDEF
   IoctlMdmIPStr string 9.99.101.22,9.99.101.23 Mdm IPs, IPs for MDM in same cluster should be comma-separated. To configure more than one cluster use '+' to separate between IPs. For Example: 10.20.30.40,50.60.70.80+11.22.33.44. Max 1024 characters
   ```

   7. To change the GUID on the SDC, type the command

   ```bash
   esxcli system module parameters set -m scini -p "IoctlIniGuidStr=<NEW_GUID> IoctlMdmIPStr=<MDM_IPS>
   ```

   where `<NEW_GUID>` is the new SDC GUID, and `<MDM_IPS>` is the list of MDM IP addresses that you identified in the previous step. You must include these IP addresses in the command.

   For example:

   ```bash
   esxcli system module parameters set -m scini -p "IoctlIniGuidStr=28a78184-4beb-4a42-bf89-4cc7e55a1e5b IoctlMdmIPStr=9.99.101.22,9.99.101.23"
   ```

8. To apply the new configuration, restart the ESX server.

**Check the SDC state on ESXi servers**

Use `esxcli` commands on an SDC running on an ESXi server to check the current state of the SDC.

To display the SDC state on the ESX server, type the following command:

```bash
esxcli system module list |grep scini
```

The following examples show typical outputs of the command:

- Output where driver is installed and enabled to load, but not loaded:

  ```
  Name Is Loaded Is Enabled
  ----------------------------- --------- ----------
  scini false true
  ```

- Example of SDC in correct state (enabled and loaded):

  ```
  Name Is Loaded Is Enabled
  ----------------------------- --------- ----------
  scini true true
  ```
Operating System Patching
Upgrade the CentOS operating system on SVMs

Use the PowerFlex Installer to upgrade the SVM's CentOS operating system to the latest security level of operating system security patching. This procedure only upgrades the operating system on the SVM. It does not upgrade PowerFlex.

NOTE: SVM operating system patching is applicable even if the SVM replacement procedure was performed. The latest patch bundle has the latest security patches that were released after the latest version of PowerFlex was officially launched (the refresh of the package is done on a monthly basis based on continuous security scans and input from customers).

Use the PowerFlex Installer to upgrade the CentOS operating system on multiple SVMs. This procedure is required when upgrading an ESXi-based PowerFlex system where SVMs are currently running on CentOS 7.5. (PowerFlex v3.0, or v3.0.0.x)

Ensure that you have the latest SVM operating system upgrade ZIP file. It is available from the support site, on the PowerFlex page.

The patch_script file that you require is part of the VMware complete software package (which is in the Complete SW download ZIP) and also as a separate artifact that is refreshed from time to time (usually once a month). The ZIP file name is: SVM_OS_Patching_package_MMDDYYYY.zip

Running scripts on hosts—overview

PowerFlex can be used to run user-provided scripts on servers 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 host 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.

Workflow overview (for reference purposes only)

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 gateway host
   - 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. Tie-Breaker
   c. MDMs
      NOTE: The script will not run on a master MDM. A switch-over MDM command will be run prior to running the script on a master MDM. The script will not be run in parallel on multiple MDMs or Tie-Breakers.
3. SDS enters Maintenance Mode.
4. The script runs on the host.
5. The host reboots (if configured to do so).
Run a script on one or more hosts—procedures

Run a script on one or multiple hosts where PowerFlex is deployed, using the PowerFlex Installer.

Prerequisites

- Prepare the script file to be run on one or more servers hosting SDSs or MDMs, and optionally, a verification script to be run automatically after execution of the script. Specific file names are required for use of this feature. IM can only upload scripts up to 500 MB in size. Name the files as follows:
  - Script: patch_script
  - Verification script: verification_script
- This feature is only supported on Linux-based (bare-metal or virtual) nodes.
- Ensure that you have the IP address and login credentials for the PowerFlex Gateway and the Master MDM.
- Ensure that you have the login credentials for the LIA.
- Ensure that you have enough disk space to run the script.

About this task

- This procedure is a long operation that cannot be rolled back automatically.
- Certificate approval messages may be displayed during the procedure. Approve all the certificates, and click Retry failed to complete the operation.

Steps

1. Configure the PowerFlex Installer to upload files from the PowerFlex Gateway host to all selected hosts.

   a. Verify that all components in the PowerFlex system are upgraded to the latest version.

   b. On the PowerFlex Gateway host, go to /opt/emc/scaleio/gateway/webapps/ROOT/WEB-INF/classes/gatewayUser.properties file.

   c. Uncomment the following lines (verification script is optional):

      ```
      os.patching.is.upload.needed=true (Default is false)
      os.patching.patch.script.source.path=<enter the full path to the file>
      os.patching.verification.script.source.path=<enter the full path to the file>
      ```

      Example of PowerFlex Gateway on Linux:

      ```
      os.patching.is.upload.needed=true
      os.patching.patch.script.source.path=/opt/patch_script
      os.patching.verification.script.source.path=/opt/verification_script
      ```

      Example of PowerFlex Gateway on Windows:

      ```
      os.patching.is.upload.needed=true
      os.patching.patch.script.source.path=C:\\temp\\patch_script
      os.patching.verification.script.source.path=C:\\temp\\verification_patch
      ```

   d. Restart the PowerFlex Gateway service.

      For example, in ESXi:

      ```
      systemctl stop scaleio-gateway.service and systemctl start scaleio-gateway.service
      ```

   e. Copy the patch_script and verification_script files to the relevant folder on the gateway host.

   f. In the Security settings of the files, allow read, write and execute permissions.

2. In your browser, navigate to the IP address of the PowerFlex Gateway, and log in.
3. Click the Maintain tab.
4. Enter the IP address and login credentials for the Master MDM, and for LIA.
5. At the bottom right of the screen, click **Retrieve system topology**.

The system topology is displayed.

6. Click **System Logs & Analysis**, and select the **Run Script on Hosts** option.

The **Run script on hosts** dialog box is displayed.

7. Enter the MDM password again.

8. For **Running script on** options, select one from the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Entire System</strong></td>
<td>Run the script on all MDM and SDS nodes in the system.</td>
</tr>
<tr>
<td></td>
<td>If you choose this option, you can also choose whether to run the script at the same time on SDSs that belong to different Protection Domains. To do so, select the check box for <strong>In parallel on different Protection Domains</strong>.</td>
</tr>
<tr>
<td><strong>Protection Domain</strong></td>
<td>Run the script on MDM and SDS nodes in a single Protection Domain. Select the required Protection Domain from the drop-down list.</td>
</tr>
<tr>
<td><strong>Fault Set</strong></td>
<td>Run the script on MDM and SDS nodes in a single Fault Set. Select the required Fault Set from the drop-down list.</td>
</tr>
<tr>
<td><strong>SDS</strong></td>
<td>Run the script on a single SDS. Select the required SDS from the drop-down list.</td>
</tr>
</tbody>
</table>

9. For **Running configuration**, select the **Stop process on script failure** option, if desired.

If problems occur, see the troubleshooting notes following these steps.

10. In the **Script time-out** box, enter the number of minutes that should elapse before the PowerFlex Installer stops waiting for a response about the running script, and prints a timeout message.

11. In the **Verification script** box, select one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run a verification script after the script.</td>
<td>Select Run</td>
</tr>
<tr>
<td>If a reboot is performed, the verification script is executed after the reboot.</td>
<td></td>
</tr>
<tr>
<td>Do not run a verification script after the script</td>
<td>Select Do not run</td>
</tr>
</tbody>
</table>

12. In the **Post script action** box, select one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot the server after execution of the script</td>
<td>Select Reboot</td>
</tr>
<tr>
<td>Do not reboot the server after execution of the script</td>
<td>Select Do not reboot</td>
</tr>
</tbody>
</table>

13. Click **Run Script on Hosts**.

14. Click the **Monitor** tab, - validate state starts.

   During this phase, the system verifies certificates and builds an execution phase for the nodes list.

15. Click **Start** execute phase - the execute phase starts.

16. When the execute phase is complete, click **Mark operation completed**.

   Troubleshooting notes:

   If a failure in executing the patch_script occurs, it may be due to one of the following reasons. Rectify the problem and then try again.

   - Script timeout
   - Script file permissions
   - Syntax error in the script
   - Degraded capacity, or MDM cluster in degraded state
   - An SDS is already in Maintenance Mode

Results

Upgrade of the CentOS operating system on all SVMs except for the PowerFlex Gateway is now complete. Upgrade the PowerFlex Gateway using the steps described in "Deploy and replace the PowerFlex Gateway SVM operating system using the PowerFlex plug-in" in the Upgrade PowerFlex Guide.