DELL V36X Power Flex Security Configuration User Guide

Dell PowerFlex v3.6.x
Security Configuration Guide

Contents

V36X Power Flex Security Configuration

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.

Introduction

This guide provides an overview of the security settings available in PowerFlex to ensure secure operation of the product.

Security features
PowerFlex has a variety of security features.
Security settings are divided into the following categories:

- Access Control Settings describes the settings available to limit access by end-user or external product components.
- Log Settings describes settings related to the logging of events.
- Communication Security Settings describes settings related to security for the product’s network communications.
- Running Scripts on Hosts explains the ability to run user-provided scripts on servers hosting DM or SDS components.
- Data Security Settings describes settings available to ensure protection of the data handled by the product.

Data integrity
It is important to define the controls that prevent permanently stored data from being disclosed in an unauthorized manner.
To maintain integrity of data, it is recommended to use D@RE with CloudLink for data-at-rest encryption of both PowerFlex devices and Virtual Machines.

ⓘ **NOTE:** For secure erasure, you must use an external tool.

Good to know
Additional security aspects of the PowerFlex system
The following aspects of the PowerFlex system are hardened:

- Storage Virtual Machines (SVM) in ESXi-based systems
- Apache Tomcat (hardened through STIG)

Access Control Settings

The following topics describe access control settings, which are used to protect resources against unauthorized access.

Supported access control settings
Access control settings are used to protect resources against unauthorized access.
The following access control settings are supported:

MDM:

- User roles and passwords are needed to access the MDM. User roles with different access permissions can be assigned to users. Both local and LDAP authentication are supported. For more information, see “User

Management” in the Configure and Customize Dell PowerFlex.

- Limited MDM access mode—a system can be configured to allow read-only access to the MDM by remote clients. In this mode, only local users connecting to the MDM using the IP address 127.0.0.1 have full configuration privileges.
- Restricted SDC mode—a system can be configured to only allow approved SDCs to connect to the MDM. This mode forces you to map volumes only to SDCs which have been previously approved by the user, by configuring them using their GUID.
  To increase security, you can specify that only SDCs with preconfigured IP addresses can communicate with the MDM. For more information, see the Configure and Customize Dell PowerFlex.
- SSL authentication of internal components to the MDM—allows secure authentication of PowerFlex SDS components to the MDM using a Public and Private Key (Key-Pair) associated with a certificate. The trust is established when adding the SDS, and reconnecting will require reauthentication.
- Secure connectivity with external components—allows external components to authenticate the MDM with a certificate and authenticate back to the MDM with a username and password. After authentication, communication between the MDM and external components is performed using TLS (Transport Layer Security) protocols. External components include: PowerFlex Installer client, PowerFlex CLI client, PowerFlex GUI client, vSphere plug-in, and PowerFlex Gateway. The same method is used between the PowerFlex Installer client and LIAs.
- An RSA Lockbox is used to store MDM credentials on the PowerFlex Gateway. These credentials are required for authentication purposes by the SNMP trap sender and ESRS.
- PowerFlex can be used to run user-provided scripts on servers hosting MDM or SDS components. This feature is supported on Linux-based nodes only. This feature can be used for any purpose external to the PowerFlex system, such as running a set of Linux shell 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 Gateway:

- Access to the PowerFlex Gateway requires defining a dedicated user. This user may either be a local user or an LDAP user.
  For more information, see the Configure and Customize Dell PowerFlex, or Dell PowerFlex User Roles and LDAP Usage Technical Notes.
- Access to the PowerFlex Installer requires a username and password. This user may either be a local user or an LDAP user.
  For more information, see the Configure and Customize Dell PowerFlex, or Dell PowerFlex User Roles and LDAP Usage Technical Notes.
- A manually generated public-private key pair can be used to perform SSH key authentication, instead of passwords, between the PowerFlex Gateway and PowerFlex servers.
- LDAP support for the PowerFlex Gateway and the PowerFlex Installer now includes up to 8 LDAP servers.

LIA:

- PowerFlex Installer / PowerFlex Gateway access to the LIA may be restricted to predefined IP addresses, by configuring the list of trusted IP addresses in the file:
  - Windows: C:\ProgramFiles\emc\scaleio\LIA\cfg\conf.txt

  - Linux: /opt/emc/scaleio/lia/cfg/conf.txt
- Access to the LIA can use local authentication or LDAP authentication, with up to 8 LDAP servers.

REST API:

- REST authenticates user access, using the gatewayAdminPassword and mdmPassword (for more information, see the PowerFlex REST API Reference Guide).
- REST authenticates user access, using the AMSAdminPassword (for more information, see the VxFlex Ready Node REST API Reference Guide).
- REST feature enabler—access to the REST gateway can be blocked by configuring the gatewayUser.properties file located on the PowerFlex Gateway. The feature is enabled by default. For detailed information, see "Configuring the PowerFlex Gateway by editing the user properties file", in the Dell PowerFlex REST API Reference Guide.

SNMP:

- SNMP—the SNMP trap sender can be enabled or disabled using one of the methods listed below. The feature is disabled by default. For detailed information, see the Configure and Customize Dell PowerFlex.
  ○ During deployment (on Linux and Windows only)
  ○ Configuring the gatewayUser.properties file located on the PowerFlex Gateway.
  ○ Using the REST API
  ⓘ **NOTE:** OpenSSL 64-bit v1.0.2k-2l or v1.1.1i or higher is required for secure authentication. In Linux, this version of OpenSSL is only supported in CentOS and RHEL 6.5 or higher.

User authentication
User authentication settings control the process of verifying an identity claimed by a user for accessing the product.

Default accounts
The PowerFlex system has the following default accounts.

Table 1. Default accounts

User Account	**Password**	**Description**
PowerFlex Installer admin user	Password is created by the admin at the beginning of the installation process	Lets the user issue installation commands in the PowerFlex Installer web client. The PowerFlex Installer has a default admin user. For more information, see "Preparing the PowerFlex Installer and the PowerFlex Gateway" in the PowerFlex Deployment Guide.
SVM root user	Password is set in the plug-in	The account provides full administrator privileges to all configuration and monitoring activities via the vSphere plugin.
MDM admin	Admin	The MDM has only one default account ("admin") with a default password ("admin") with the Super User role. The password must be reset at first login during system deployment. This account is a Super User, and provides full administrator privileges to all configuration and monitoring activities via the CLI and the GUI.

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:\ProgramFiles\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 ResetAdmin, 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.

Authentication configuration

Local passwords must meet specific requirements.

NOTE: For LDAP users, the requirements are defined by the authenticating server according to the organization’s user policy.

User authentication is initially configured during PowerFlex installation, and users can be added and removed later, using the PowerFlex CLI (and only by a privileged user). The MDM and LIA passwords must meet the following criteria:

- Include at least 3 of the following 4 groups: [a-z], [A-Z], [0-9], special characters (!@#$ …)
- Contain between 6 and 31 characters
- No white spaces

  NOTE: The ESXi 6 password policy has the following additional requirements:
  - Passwords must contain characters from at least three character classes.
  - Passwords containing characters from three character classes must be at least seven characters long.
  - Passwords containing characters from all four character classes must be at least seven characters long.

  An uppercase character that begins a password does not count toward the number of character classes used.

  A number that ends a password does not count toward the number of character classes used.

For more information, see “Security” and “User Management” in the Configure and Customize Dell PowerFlex.

NOTE: ESXi 6 security policy is disabled.

User authorization
User authorization settings control the rights or permissions that are granted to a user to access a resource managed by the product. Local users and LDAP users are supported by the system.
When users are added to the MDM, user role definitions must be assigned to them.
NOTE: Local authentication can be disabled on the PowerFlex Installer / PowerFlex Gateway. For more information, see the “Security” in the Configure and Customize Dell PowerFlex.

Table 2. Local and LDAP User roles and permissions

User role	**Query**		**Configure parameters**		**Configure user credentials**	
	Local	**LDAP**	**Local**	**LDAP**	**Local**	**LDAP**
			Backend operations only (Protection Domains, Storage Pools, Fault Sets, SDSs, Devices, other system settings)			
Frontend Configurator	Yes	No	Yes Frontend operations only (Volumes, SDCs, Snapshots)		No	No
Administrator	Yes	No	Yes	No	May configure Configurator and Monitor users	
Security Roles	No	No	No	No	May define Administrator users and control LDAP	
Super User (only one Super User is allowed per system, and it must be a local user)	Yes	Not applicable	Yes	Not applicable	Yes	Not applicable

Login banner

A login banner can be configured for both PowerFlex GUI and CLI users.
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 in the CLI interfaces:

- 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.

If a login banner is not required, the feature can be disabled. For more information about configuring these banners, refer to the Configure and Customize Dell PowerFlex.

Component access control
Component access control settings define control over access to the product by external and internal systems or

components.

Component authentication

The system provides secure connectivity between internal and external components.

Secure connectivity with internal system SDS components

The SSL authentication feature allows secure authentication of PowerFlex SDS components using a Public and Private Key (Key-Pair) associated with a certificate. The feature works as follows:

- When an SDS is added to the PowerFlex system (for example, using the ––add_sdscommand), it generates its own certificate and a CSR to the MDM.
- The MDM acts as the Certificate Authority, and signs the certificates, using its own credentials.
- Every time that an SDS reconnects to the system, authentication occurs. If the challenge fails, that component will not be able to connect to the PowerFlex system.
- If necessary, or if a malfunction occurs, this feature provides a secure protected manner in which to disable secure authentication.

OpenSSL FIPS compliance

You can enable OpenSSL Federal Information Processing Standards (FIPS) compliance implementation in the MDM for communication between the external components, including the PowerFlex GUI, PowerFlex Gateway, and CLI, to the MDM.

It can also be enabled for any other usage of the OpenSSL library. For instructions on how to enable OpenSSL FIPS compliance implementation, see “Enable OpenSSL FIPS compliance.”

Secure connectivity with external components

This feature allows external components to authenticate the MDM with a certificate and authenticate back to the MDM with a user name and password. After authentication, communication between the MDM and external components is performed using TLS (Transport Layer Security) protocols. Secure communication with the MDM is authenticated by the following PowerFlex components:

- CLI client
- PowerFlex Gateway
- PowerFlex GUI client
- PowerFlex Installer client
- vSphere plug-in

The same method is employed between the PowerFlex Installer and all LIAs.

On the PowerFlex Gateway, setting the security.bypass_certificate_check property in the gateway properties file to true will result in the gateway blindly trusting the certificates of the hosts to which it is trying to connect. Typically, the gateway connects to the MDM or to LIA. This setting affects REST and PowerFlex Installer connections, because they are all included in the gateway. The default setting of this property is false.

Any actions relating to the acceptance of certificates will still add the certificates to the trust store file (truststore.jks) for future use, when this property is set to false. Such actions are:

- MDM certificate and LIA certificate approval during installation with the PowerFlex Installer
- The REST request trustHostCertificate

SSH

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.

NOTE: Whenever Apache Tomcat is shut down normally and restarted, or when an application reload is triggered, the standard Manager implementation will attempt to serialize all currently active sessions to a disk file located via the pathname (by default SESSIONS.SER) attribute. All such saved sessions will then be deserialized and activated (assuming they have not expired in the mean time) when the application reload is completed. To remove saved sessions after a PowerFlex Gateway restart, delete the following file: /opt/emc/scaleio/gateway/work/Catalina/localhost/_/SESSIONS.ser

LIA security configuration

Configure LIA parameters for component authorization.
All the configurable parameters of LIA are included in the file /opt/emc/scaleio/lia/cfg/conf.txt.
The list includes:
lia_token, lia_enable_install, lia_enable_uninstall, lia_enable_configure, lia_enable_fetch_logs, lia_auth_mode, and ldap0_uri.

Managing component certificates

PowerFlex supports replacing the certificates of the following components:

- PowerFlex Gateway
- MDM
- PowerFlex presentation server

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:\ProgramFiles\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–keyalgRSA–alias<YOUR_ALIAS>–filecertreq.txt
–keystore<PATH_TO_NEW_KEYSTORE_FILE>–storepass<KEYSTORE_P
ASSWORD>–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–aliasroot–keystore<PATH_TO_NEW_KEYSTORE_FILE>
   –trustcacerts
   –file<LOCATIONOF_YOUR_root.cer_FILE>–storepass<KEYSTORE_PAS
   SWORD>–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.

5. Import the intermediate certificates, by typing the command. (If you did not define a keystore password, omit the password flags.)

   ```
   keytool–import–aliasintermediateCA–keystore<PATH_TO_NEW_KEYST
   ORE_FILE>
   –trustcacerts–file<LOCATION_OF_YOUR_intermediate.cer_FILE>–stor
   epass<keystorepassword>–keypass<keystorepassword>
   ```

   You must provide a unique alias name for every intermediate certificate that you upload with this step.

6. 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_KEYST
   ORE_FILE>
   –trustcacerts–file<LOCATION_OF_SSL_CERTIFICATE>–storepass<key
   storepassword>
   –keypass<keystorepassword>
   ```

7. 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`.

8. Restart the PowerFlex Gateway service:

   - Windows: From the Windows Services window, restart the EMC ScaleIO Gateway.
   - Linux: Type the following command:

   ```
   servicescaleio–gatewayrestart
   ```

Replacement of the security certificate is complete.

Replace the default self-signed security certificate with your own selfsigned 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:\ProgramFiles\Java\jdk1.8.0_XX\bin\keytool.exe`
   - `/usr/bin/keytool`

2. Generate your RSA private key:

   ```
   keytool–genkey–alias<YOUR_ALIAS>–keyalgRSA–validity360–keysize2048–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.
   - Linux: Type the following command:

   ```
   servicescaleio–gatewayrestart
   ```

Results

Replacement of the security certificate is complete.

Configure OpenStack interoperation with the PowerFlex Gateway

Configure the PowerFlex Cinder driver to verify the PowerFlex Gateway SSL certificate.

About this task

The OpenStack PowerFlex Cinder driver communicates with the PowerFlex Gateway through HTTPS (in other words, over SSL). By default, the driver ignores the gateway SSL certificate verification. However, the PowerFlex Cinder driver can be configured to verify the certificate.

NOTE: You can generate a self-signed certificate (.PEM file), using the keytool utility.

To enable certificate verification, add the following parameters to the file `/etc/cinder/cinder_scaleio.config` on the Cinder node:

```
verify_server_certificate=true
server_certificate_path=<PATH_TO_PEM_FILE>
```

Generate a self-signed certificate using the keytool utility

Generate self-signed certificates using the keytool utility. The certificates can by used by the OpenStack PowerFlex driver to communicate with the PowerFlex Gateway.

About this task

To generate a self-signed certificate using the keytool utility, perform the following steps:

Steps

1. Create a keystore file (.JKS):
   ```
   keytool–genkeypair–keysize1024–aliasherong_key–keypasskeypass–keystoreherong.jks–storepassjkspass
   ```
2. Export the keystore file to a .PEM file:
   ```
   keytool–exportcert–aliasherong_key–keypasskeypass–keystoreherong.jks–storepassjkspass–rfc–filekeytool_crt.pem
   ```
   The certificate is stored in the file <keytool_crt.pem>. During configuration of the Cinder driver, the path to this .PEM file is required.

Workflow for externally signed security certificates

The system generates and signs self-signed certificates automatically when secure communication is enabled, and no user intervention is required. You can replace the certificates by an externally signed security certificate. A Certificate Authority (CA) uses the CSR (Certificate Signing Request) file to create an externally signed security certificate.

About this task

The workflow describes how to replace the certificates signed by an external CA for each MDM.

Steps

1. Log in to the primary MDM with a security or administrator user role:
   ```
   scli––mdm_ip<primary_mdm_ip>––login––usernameadmin––password<password>
   ```
2. Generate the CSR file on the primary MDM, for the specified MDM (target):
   ```
   scli––generate_mdm_csr_file––target_mdm_ip<mdm_ip>
   ```
   The file mdm–target_hostname.csr is created and saved to:

   ● Linux: /opt/emc/scaleio/mdm/cfg

   ● Windows: C:\ProgramFiles\emc\scaleio\mdm\cfg
3. Send the generated CSR file to the CA for signing.

   The CA returns the following files:

   a. A certificate for each MDM.

   b. A trusted/root certificate and its' intermediate certificate from the CA.
4. On each MDM, from the CLI, add the root and intermediate certificate to the truststore, using the ––add_certificate command. Refer to PowerFlex CLI Reference Guide for more information.
   ```
   scli––add_certificate––certificate_fileroot–ca.pem.crt
   ```
5. Run the following commands using Java's keytool to import all the certificates to each of the following components' truststore. It is recommended to restart the machine after running the commands.

   ● PowerFlex Gateway

   ○ Linux: /opt/emc/scaleio/gateway/webapps/ROOT/WEB–INF/classes/certif `icates/truststore.jks`

  - Windows (64 bit): `C:\Program Files\EMC\ScaleIO\Gateway\webapps\ROOT\WEBINF\classes\certificates\truststore.jks`

- PowerFlex presentation server

  NOTE: Refer to “Update the certificate for the PowerFlex presentation server” for detailed steps on how to import the certificate from the MDM to the PowerFlex presentation server.

  - Linux: `/etc/mgmt−server/.config/mdm−truststore.jks`

- vSphere plugin
  - Linux: `$HOME/.vmware/scaleio/certificates`
  - Windows: `C:\Users\[user_name]\AppData\Roaming\VMware\scaleio\certificates\truststore.jks` or `C:\Windows\System32\config\systemprofile\AppData\Roaming\VMware\scaleio\certificates`

Trust is now established.

6. Save the signed certificate for the MDM in `/opt/emc/scaleio/mdm/cfg`.
7. Rename the MDM certificate file to `mdm_signed_certificate.pem`.
8. From the MDM, remotely log in to the primary MDM with a security or administrator user role:

   ```
   scli−−mdm_ip<primary_mdm_ip>−−login−−usernameadmin−−password<password>
   ```

9. Run the following command to begin applying the signed certificate to each of the MDMs:

   ```
   /opt/emc/scaleio/mdm/bin/apply_signed_certificate.py−−mdm_ip<primary_mdm_ip>−local_mdm_ip<local_mdm_ip>
   ```

   If the remote read-only feature is enabled on the MDM, add `−−skip_cli_command` to the command, and later, while logged in with user that has security permissions, run the command `scli−−replace_mdm_security_files`.

   NOTE: This step changes the MDM certificate, and might cause a brief failure period (switch ownership).

Update certificate for PowerFlex presentation server

Import the CA certificates from the MDM to the PowerFlex presentation server.

Steps

1. Copy the root and intermediate CA certificate files `inter−ca.pem.crt` and `root−ca.pem.crt` to the server that is installed with the PowerFlex presentation server.
2. Run the following command for root and intermediate CA certificates and save the output:

   ```
   opensslx509−noout−inroot−ca.pem.crt−subject
   opensslx509−noout−ininter−ca.pem.crt−subject
   ```

3. Run the keytool command to import the root and intermediate CA certificate from the MDM:

   ```
   keytool−import−trustcacerts−alias“<thesubjectyougotastheoutputofthepreviouscommand>”−file/tmp/root−ca.pem.crt−keystore/etc/mgmt−server/.config/mdmt
   ruststore.jks
   ```

```
keytool–import–trustcacerts–alias”<thesubjectyougotastheoutputofthe
previouscommand>”–file/tmp/inter–ca.pem.crt–keystore/etc/mgmt–serv
er/.config/mdmt
ruststore.jks
```

–alias refers to a unique alias in the truststore, and –file is the path to the trusted/root certificate. It is recommended to use the certificates’ subject for the alias.

Example:

```
keytool–import–trustcacerts–alias”/C=AU/ST=CA/L=CA/O=CA/OU=CA/C
N=CA/
emailAddress=tom.smith@dell.com”–file/tmp/root–ca.pem.crt–keystore
/etc/mgmts
erver/.config/mdm–truststore.jks
keytool–import–trustcacerts–alias”/C=AU/ST=CA/O=CA/OU=CA/CN=CA/
emailAddress=tom.smith@dell.com”–file/tmp/inter–ca.pem.crt–keystor
e/etc/mgmts
erver/.config/mdm–truststore.jks
```

4. Restart the PowerFlex presentation server:

```
servicemgmt–serverrestart
```

NOTE: For RHEL6.10, use the command initctlrestartmgmt–server.

Results

CA signed certificates are now set up on the system.

There are several logs collected by PowerFlex.
A log is a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.

Log description

The various logs collected by different components of the system are saved in different locations.
NOTE: PowerFlex uses Apache Tomcat, which has its own set of standard logs. For more information about Tomcat logs, refer to Apache Tomcat documentation.

Table 3. Log files

Component	Location
MDM log The logs do not contain any user data (as the user data do not pass through the MDM) The logs may contain the MDM’s user names (but never passwords), IP addresses, MDM configuration commands, events etc.	Linux: /opt/emc/scaleio/mdm/logs

REST logs	<gateway installed folder>\logs For example: Windows—c:\Program Files\emc\scaleio\gateway\logs Linux—/opt/emc/scaleio/gateway/logs The following logs are available: ● scaleio.log ● scaleio-trace.log ● operations.log ● localhost_access_log.log ● audit.log ● api_operations.log
PowerFlex Installer logs	<gateway installed folder>\logs For example: ● Windows: ○ c:\Program Files\emc\scaleio\gateway\logs ● Linux: ○ /opt/emc/scaleio/gateway/logs The following logs are available: ● scaleio.log ● scaleio-trace.log ● operations.log ● localhost_access_log.log
LIA logs	Windows: ● C:\Program Files\emc\scaleio\lia\logs Linux: ● /opt/emc/scaleio/lia/logs
Tomcat logs	Windows: ● C:\Program Files\EMC\ScaleIO\Gateway\logs\tomcat.log Linux: ● /opt/emc/scaleio/gateway/logs
PowerFlex presentation server logs	Linux: ● opt/emc/scaleio/mgmt-server/logs
vSphere PowerFlex plug-in	
PowerFlex plug-in deployment log:	Windows: ● c:\Windows\System32\config\systemprofile\AppDdata\Roamin \VMware\scaleio\deployment.log Linux: ● /opt/.vmware/scaleio/deployment.log
PowerFlex plug-in rollback log:	Windows: ● c:\Windows\System32\config\systemprofile\AppData\Roaming \VMware\scaleio\rollback.log Linux: ● /opt/.vmware/scaleio/rollback.log
PowerFlex plug-in network creation log:	Windows: ● c:\Windows\System32\config\systemprofile\AppData\Roaming \VMware\scaleio\networkCreation.log Linux: ● /opt/.vmware/scaleio/networkCreation.log
vSphere Virgo log:	Windows: ● c:\ProgramData\Vmware\vSphere Web Client\serviceability\logsvsphere_client_virgo.logLinux: ● /storage/log/vmware/vsphere-client/logs/ vsphere_client_virgo.log

perrcli/storcli log:	Event logs

Log management and retrieval

The logs can be managed and retrieved in various ways.

- Log roll-over (REST):
  ○ In the configuration of the log’s behavior (logback.xml—see below), each log is defined to be no greater than 10 MB. Once it reaches this size, a new log file is created. Once the maximum (10) is reached, the oldest log is overwritten (roll-over). The log files are: name_xxx.log, name_xxx.1.log.zip, … name_xxx.10.log.zip.
- Configuration of an external Syslog server:
  ○ During PowerFlex installation, you can use the PowerFlex Installer web client to configure Syslog event reporting. You can also configure these features after installation, using the CLI.For more information, see “Viewing Events” in the Monitor Dell PowerFlex.
- Configuration of logging levels:
  ○ PowerFlex Gateway (REST)—The log can be configured by editing the file: <gatewayinstallationfolder>\webapps\ROOT\WEB–INF\classes\logback.xml
  ○ PowerFlex Installer—The log can be configured by editing the file: <gatewayinstallationfolder>\webapps\ROOT\WEB–INF\classes\logback.xml
- vSphere Web Client logging
  ○ To enable debug logging for the vSphere Web Client service:
  NOTE: Take a backup of the serviceability.xml file before modifying it.
  1. Stop the vSphere Web Client service.
  2. Navigate to the configuration folder:
  For vCenter Server 6.x— C:\ProgramData\VMware\vCenterServer\runtime\vsphereclient\server\configuration
  For vCenter Server Virtual Appliance 6.x— /usr/lib/vmware–vsphere–client/server/configuration
  3. Open the serviceability.xml file using a text editor.
  NOTE: Take a backup of the serviceability.xml file before modifying it.
  4. Edit the root level logging parameter by replacing the default INFO with DEBUG. For example, change the serviceability.xml default configuration from:

```
<rootlevel=”INFO”>
<appender–refref=”SIFTED_LOG_FILE”></appender–ref>
<appender–refref=”LOG_FILE”></appender–ref>
</root>
```

  to:

```
<rootlevel=”DEBUG”>
<appender–refref=”SIFTED_LOG_FILE”></appender–ref>
<appender–refref=”LOG_FILE”></appender–ref>
</root>
```

  5. To add a logging section for the PowerFlex plugin, create a section to increase logging to Debug levels:

```
<loggerlevel=”DEBUG”additivity=”false”name=”com.emc”>
<appender–refref=”SIFTED_LOG_FILE”/>
<appender–refref=”Log_FILE”/>
</logger>
```

- Save and close the file.
- Start the vSphere Web Client service. Additional logs will be written to the C:\ProgramData\VMware\vSphereWebClient\Logs folder
- SRS feature (Secure Remote Support)—SRS support enables secure, high-speed, 24×7, remote connection between Dell and customer installations, including:
  - Remote monitoring
  - Remote diagnosis and repair
  - Daily sending of system events (rsyslog output), alerts, and PowerFlex topology. For more information, see “Perform other SRS configuration activities” in the Configure and Customize Dell PowerFlex.
- Viewing events locally—Use the showevents.py command, using filter switches to control the severity of alerts. For more information, see “Viewing Events” in the Monitor Dell PowerFlex.
- Configuration for external log management tools like envision—NA
- Configuration of time synchronization with an external source (e.g. via NTP, Windows Time Service, etc.)—NA
- Get Info—Get Info allows you to assemble a ZIP file of system logs for troubleshooting. You can run this function from a local node for its own logs, or by using the PowerFlex Installer to assemble logs from all MDM and SDS nodes in the system. For more information, see “Retrieving logs for PowerFlex components” in the PowerFlex Log Collection Technical Notes.

Communication Security Settings

The following topics describe the PowerFlex system’s security settings. Communication security settings enable the establishment of secure communication channels between the product components, as well as between product componentsand external systems or components.

Replication security
There are new security features to ensure that PowerFlex replication can be used securely.
In addition, Challenge-Handshake Authentication Protocol (CHAP) authentication is used for authentication between the all of the SDRs of each peer system within each Protection Domain. This authentication is bidirectional. The authentication is at the network level. If authentication fails, the network socket is not created and there is no connection between the two SDRs. This also determines the authorization of an SDR to write to its target volumes on the peer system.

MDM to MDM encrypted communications
To ensure security between the two replication systems, the management communications between them must be encrypted.
This is achieved by running the communications between the two MDM clusters of the replicated systems over TLS 1.2. In order to implement TLS, it is required that both MDM clusters have the MDM certificate of the other cluster. You must perform a certificate exchange between the two peer systems. Without this certificate exchange, it is not possible to set up replication peer systems. The following steps are necessary:
between the twopeer systems. Withoutthis certificate exchange, it is impossible to set up replication peer systems. The following stepsare necessary:

1. Using the SCLI, extract the root certificate on each system: scli––extract_root_ca––certificate_file<FILE_NAME>
2. Copy the root certificates to peer system using scp or any file transfer method.

3. Using the SCLI, add the copied certificate as a trusted certificate: scli--add_trusted_ca--certificate_file<FILE_NAME>--comment<COMMENT(e.g.,NameOf_System)>

The certificate exchange between peer systems should be performed by a system administrator who has root access to all MDM nodes on both peer systems. Detailed instructions on performing this procedure are included in the “Post-deployment task” section of the Configure and Customize Dell PowerFlex.

SDR to SDC Authentication

In addition, Challenge-Handshake Authentication Protocol (CHAP) is used for authentication between the SDRs of each peer system within each Protection Domain. This authentication is bidirectional. The authentication is at the network level. If authentication fails, the network socket is not created and there is no connection between the two SDRs. This also determines the authorization of an SDR to write to its target volumes on the peer system.
NOTE: Access to a remote SDR does not grant access to the volumes maintained by the remote SDR unless they are determined as replicated by the source SDR.

SDC authentication

This feature ensures security by applying CHAP (Challenge-Handshake Authentication Protocol) based authentication of the SDC to the MDM for access to the system in general and to mapped volumes in particular. This prevents the SDC from accessing unauthorized volumes. Once enabled, the SDC internally performs mutual CHAP authentication with the SDSs and the SDRs with no manual intervention.

Prerequisites

Enable SDC authentication according to the following rules:

- v3.5 or later must be installed on the SDC
- For each SDC, a CHAP authentication password is generated by the MDM
- All SDCs must be configured with their generated passwords
- Run the --check_sdc_authentication_status command, to check the status of the SDCs and whether they are ready to authenticate

About this task

NOTE: Using CHAP authentication with SDC also means that an SDC can only perform I/O operations on volumes explicitly mapped to it. The SDS will block SDC I/O operations on unmapped volumes.

NOTE: CHAP authentication is also used internally for I/O authentication to the SDS and SDR, however it is always enabled and not controlled by the user.

This procedure describes how to enable SDC authentication.

Steps

1. Get the shared generated password for SDC from the MDM using the command: scli--generate_sdc_password--(sdc_id<ID>|sdc_name<NAME)|sdc_guid<GUID>|sdc_ip<IP>)[--reason<REASON>] The reason parameter (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:

   ● Linux:

   ```
   /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.

   ● **ESXi:**

   a. `cat/etc/vmware/esx.conf|grepscini|grepoptions`

   A string is returned representing all of the ESXi configuration parameters currently set. Copy the string with the enclosing quotation marks and paste in a text editor for editing.

   b. At the end of the string, add the following text, within the quotation marks:

   ```
   IoctlMdmPasswordStr=<MDM_IP>−<MDM_PASSWORD>
   ```

   where:

   ○ <MDM_IP> is the MDM IP address

   ○ <MDM_PASSWORD> is the MDM password

   For example:

   ```
   ”IoctlIniGuidStr=cd069ce3−bf2a−5dea−b50a−1a5ebc8ef3de
   IoctlMdmIPStr=192.169.217.165,172.17.217.165,192.169.217.166,172.
   17.217.166,192.1
   69.217.167,172.17.217.167IoctlMdmPasswordStr=192.169.217.165−AQ
   AAAAAAAADu/
   10fXW3BS1wPBDgnkR06tdneGoUK7VQ”
   ```

   c. Run the following command with the string appended to the end:

   ```
   esxclisystemmoduleparametersset−mscini−p<STRING>
   ```

   For example:

   ```
   esxclisystemmoduleparametersset−mscini−p”IoctlIniGuidStr=cd069ce3
   b
   f2a−5dea−b50a−1a5ebc8ef3de
   IoctlMdmIPStr=192.169.217.165,172.17.217.165,192.169.217.166,172.
   17.217.166,192.1
   69.217.167,172.17.217.167IoctlMdmPasswordStr=192.169.217.165−AQ
   AAAAAAAADu/
   10fXW3BS1wPBDgnkR06tdneGoUK7VQ“
   ```

3. To check SDC readiness for all SDCs in the system, before enabling SDC authentication, run the following command:

   NOTE: It is important to complete the previous steps for all SDCs before running the command. `scli−−check_sdc_authentication_status[−−run_test][−−file_name<FILENAME>]`

   Where:

   ● `−−run_test` runs a connectivity test to check whether the SDCs can successfully authenticate using CHAP

   ● `−−filename<FILENAME>` is the full file name and path for the generated report.

   The command sends a report that includes the SDCs authentication password status.

   NOTE: When running this command, the SDCs are disconnected for a very short period from the MDM. This does not interrupt running I/Os or have any impact on MDM/SDC activity. It is recommended to run the command when the system is in a healthy state and not during rebalancing or rebuilding operations.

4. To enable SDC authentication, run the following command:
   ```
   scli––set_sdc_authentication––enable
   ```
5. To disable SDC authentication, run the following command:
   ```
   scli––set_sdc_authentication––disable
   ```
6. Reboot the ESXi for the configuration to take effect.

Results

SDC authentication is enabled or disabled.

Related tasks

Gracefully reboot the ESXi host

Gracefully reboot the ESXi host

Perform the following steps to gracefully reboot the ESXi host.

Prerequisites

- Ensure that you have the ESXi host login credentials.
- Ensure that you have admin rights for accessing the PowerFlex GUI.

Steps

1. Log in to vCenter via the vSphere Web Client, and locate the relevant ESXi host.
2. Migrate the VMs associated with this ESXi host to another ESXi host.

   NOTE: To view the VMs associated with the ESXi host, select the ESXi host, and then click VMs.
3. Log in to the PowerFlex GUI as an admin user.
4. In the Backend > Storage view, select By SDSs table view.
5. Right-click the SDS node you are rebooting, and select Enter Maintenance Mode.
6. In the Enter maintenance mode window, ensure that there are no errors, and then click OK.
7. When the operation finishes successfully, click Close.

   The node’s IP address appears with a wrench next to it.
8. On the ESXi node, enter maintenance mode:

   a. Log in to the vCenter via the vSphere Client or Web Client, and locate the relevant ESXi IP address.

   b. Select the SVM, and from the Basic Tasks pane select Shut down the virtual machine.

   c. When the SVM is off, right-click the node and select Enter Maintenance Mode.
9. Gracefully reboot the node using the relevant API for the operating system.
10. Right-click the ESXi host and select Maintenance Mode > Enter Maintenance Mode.
11. Click OK to confirm.
12. Right-click the ESXi host, and select Actions > Power > Reboot to reboot the host.
13. Click OK to confirm.
14. Ensure that the ESXi host is displayed as on and connected in Hosts and Clusters view.
15. Right-click the node and select Maintenance Mode > Exit Maintenance Mode.
16. Expand the host and select the relevant VM. If the VM does not power on automatically, power it on manually.

17. After the node is up, from your internet browser, log in to the PowerFlex GUI as an admin user.
18. Perform the following checks:
    a. In the left pane, click Alerts, and then in the right pane confirm that no SDS disconnect message appears.
    b. In the left pane, click SDCs, and then in the right pane confirm that the SDC's connected status is Yes.
    c. In the left pane, click Dashboard, and validate that the system is in optimal state.
19. In the PowerFlex GUI Backend > Storage view, in By SDSs table view, right-click the SDS and select Exit Maintenance Mode.
20. In the Action window, click OK.
21. Wait for the rebalance operations to finish.

Results

The ESXi host is now operational and application I/O can be started on the node. You can migrate the VMs back to the node.

Related tasks

SDC authentication

Port usage and changing default ports

Before installing or upgrading PowerFlex, ensure that the ports listed in the table are not used by other processes. The following table lists the ports used by PowerFlex.

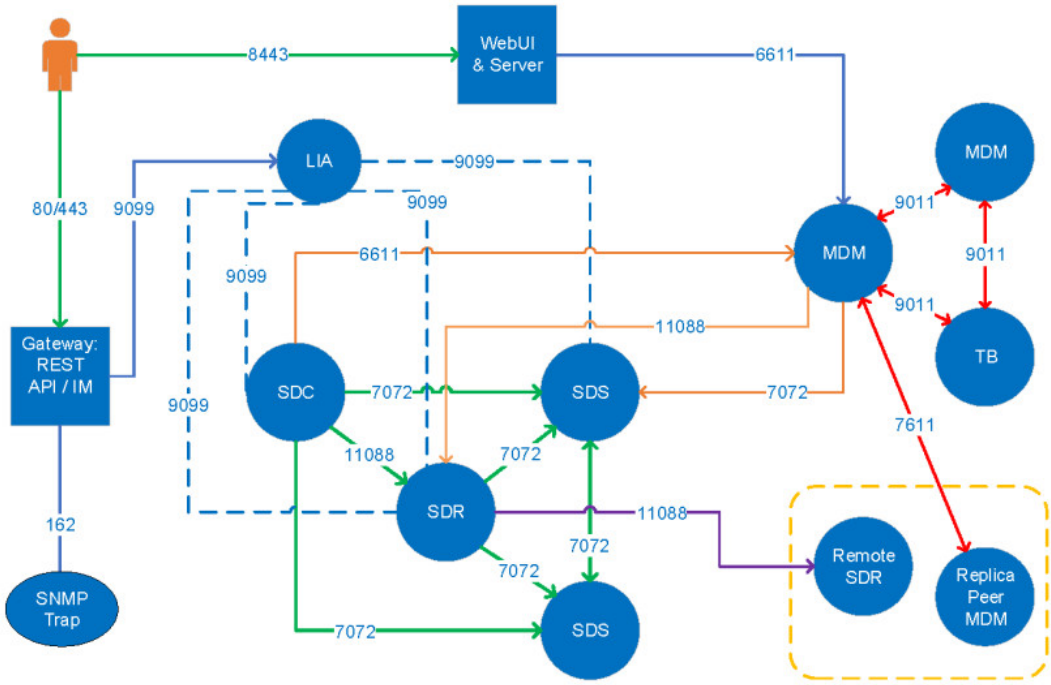
Table 4. Default ports

Port used by	Port #	Protocol	File to change	Field to modify (or to add, if it does not exist)	Notes
MDM listener	6611	Proprietary (Protobuf) over TCP	**NOTE:** Cannot be modified, and must be available		
MDM cluster member	9011	Proprietary (Protobuf) over TCP	/opt/emc/ scaleio/mdm/cfg/ conf.txt	actor_cluster_port=*<NEW_POR T>*	
MDM peer connection	7611	Proprietary (Protobuf) over TCP	/opt/emc/ scaleio/mdm/cfg/ conf.txt	mdm_ext ernal_p ort=<NE W_PORT>	To change the port assigned to the peer MDM system, first change the value of the mdm_external_port field. Then restart the MDM process. Finally, run the — modify_replication_peer_system_ port SCLI command. For more information on this command, see the Dell PowerFlex CLI Reference Guide.
SDS listener	7072	Proprietary protocol over TCP	/opt/emc/ scaleio/sds/ cfg/ conf.txt	tgt_port=<NE W _PORT>	SDCs and SDRs connect through this port for data communications and to the MDM for metadata communications.

SDR listener	11088	NEW_P OR T	/opt/emc/ scaleio/sdr/ cfg/ conf.txt	tgt_por t=<NE W _PO RT>	SDCs connect through this port for dat a communications and to the MDM fo r metadata communications. ⓘ NOTE: Incoming and outgoing p orts must be enabled.
Source SDR to target SD R	11088	NEW_P OR T	/opt/emc/ scaleio/sdr/ cfg/ conf.txt	tgt_por t=<NE W_POR T>	SDCs connect through this port for dat a communications and to the MDM fo r metadata communications. ⓘ NOTE: Incoming and outgoing p orts must be enabled. SDRs communicate with each other, a nd send replicated data to eachother, over TCP port 11088. This port must b e opened for egress in any firewall on t he source system side, and it must be open for ingress on the target system s ide. If replication is being performed in both directions between the two syste ms, then port 11088 must be open in t he firewall for both egress and ingress on both sides.
LIA listener	9099	Proprieta ry (Proto buf) over TCP	/opt/emc/ scaleio/lia/c fg/ conf.txt	lia_por t =<NEW _PORT >	The PowerFlex Installer connects to th e LIA to perform installation and maint enance- related operations.
PowerFlex G ateway- Inst allation Man ager/REST (not secure)	80 (or 80 80, toge ther wit h 8443)	REST ov er HTTPS	<gateway installation directory>/conf/ catal ina.propertie s	http.po rt=80 (o r 8080)	The ports mentioned in parentheses a re alternative ports, but can only be us ed if they were specified during system deployment. After changing a port, you must restart the PowerFlex Gateway service/daem on: ● Linux: Run service scaleio- gatewa y restart ● Windows: Restart the EMC ScaleI O Gateway service ⓘ NOTE: When deploying PowerFl ex Gateway, if one of the following por ts is not free, the deployment will fail: 80, 8080, 443, 8443. If this occurs, fre e
					the above-mentioned ports, and then r edeploy the PowerFlex Gateway.

PowerFlex presentation server	8443	HTTPS and WSS	/etc/mgmt- server/.config/ mgmt-server	MGMT_SERVER_OPTIONS=' https.port=<NEW_PORT>'	This is the port used to open a web connection to the WebUI in the browser. NOTE: It is not recommended to install the PowerFlex presentation server and PowerFlex Gateway on the same host due to conflict on port 8443. If it is unavoidable, change the port used for the PowerFlex presentation server to 9443. For instructions, see the Deploy Dell PowerFlex Guide.
SNMP	162	SNMP v2 over UDP	<gateway installation directory>/ webapps/ ROOT/WEB- INF/classes/ gatewayUserPropert ies	snmp.port	SNMP traps for system alerts are sent to a trap receiver via this port. The PowerFlex Gateway sends messages to: snmp.traps_receiver_ip on the port snmp.port If you change the port number, restart the PowerFlex Gateway afterwards.
SDBG for MDM (Manager)	25620				Used by PowerFlex internal debugging tools to extract live information from the system for debugging purposes.
SDBG for MDM (Tie Breaker)	25600				
SDBG for SDS	25640				

The following diagram illustrates the components and the ports they use.



Communication Security Settings

NOTE: For iDRAC security-related information, see “iDRAC Port Information” in the iDRAC User’s Guide.

Network encryption

The PowerFlex system performs network encryption for its different components.

The PowerFlex Installer client, CLI client, PowerFlex GUI client, vSphere plug-in, and PowerFlex Gateway (REST) use TLSv1.2

—after authentication, communication between the MDM and external components is performed using TLSv1.2 (Transport Layer Security) protocols. The same method is used between the PowerFlex Installer client and LIAs. For more information, see “Security” in the Configure and Customize Dell PowerFlex.

PowerFlex Gateway (REST) certificate validation—the OpenStack PowerFlex driver communicates with the PowerFlex Gateway through https, (over TLSv1.2). By default, the driver ignores verification of the PowerFlex Gateway’s TLSv1.2 certificate, but it can verify the certificate if the following configuration parameters are defined:

- verify_server_certificate—set to True, if the server’s certificate must be verified, and to False if no verification is required.
- server_certificate_path—If the parameter verify_server_certificate is set to True, specify the location of the .pem file containing the server’s certificate.

  For instructions for generating a self-signed certificate using Keytool, see the section “Generate a self-signed certificate using the keytool utility” in the Deploy Dell PowerFlex .

  The following encryption methods are approved for use with your system:
- MDM supported ciphers :
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
- PowerFlex Gateway supported ciphers (to the MDM):
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_RSA_WITH_AES_128_GCM_SHA256
- PowerFlex presentation server supported ciphers (to the MDM):
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_RSA_WITH_AES_128_GCM_SHA256

Remove TLSv1.0/1.1 from sslEnabledProtocols parameter

PowerFlex Gateway does not support TLSv1.0/1.1.

Steps

1. From the PowerFlex Gateway machine, go to:
   - Linux: /opt/emc/scalio/gateway/conf
   - Windows: C:\ProgramFiles\EMC\ScaleIO\Gateway\conf
2. Open the server.xml file and search for sslEnabledProtocols.
3. Delete TLSv1.0 or TLSv1.1 and save the file.
4. To restart the PowerFlex Gateway service, run:
   - Linux: servicescaleio–gatewayrestart
   - Windows: Restart the PowerFlex 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:

   ```
   servicescaleio–<COMPONENT>restart
   ```
8. Verify FIPS enablement

   a. Update the GRUB bootloader to include fips=1

   See the following example:

   ```
   cat/etc/default/grub|grepGRUB_CMDLINE_LINUX=
   GRUB_CMDLINE_LINUX=”crashkernel=autord.lvm.lv=vg_os/rootrd.lvm.l
   v=vg_os/swaprhgb
   quietfips=1”
   ```

   b. Update GRUB config

   ```
   grub2–mkconfig–o/boot/grub2/grub.cfg
   ```

   c. Update Initrd

   ```
   dracut–f
   ```

   d. Reboot node, after entering IMM/PMM to go active
9. 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.

Running scripts on hosts

PowerFlex can be used to run user-provided scripts on Linux-based servers hosting MDM or SDS components.

Running scripts on hosts

PowerFlex can be used to run user-provided scripts on servers hosting MDM or SDS components. This feature is supported on Linux-based 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 Linux shell 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. It also enables better security of the system and improved lifecycle management.

As a security precaution, the scripts are not automatically distributed to each node by the PowerFlex Installer. After verifying that the script is trustworthy, the admin user must manually copy the script to each node where the script is required.

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.

For details on how to run a script on one or more hosts, see the Configure and Customize Dell PowerFlex.

Known security issues

This section lists known security issues and workarounds.

Issues with Lockbox after OS upgrade

After an OS upgrade, the Lockbox may not be present or may lose content.

Issue

After upgrading the Operating System, the System Stable Values (SSVs) that Lockbox uses to fingerprint the system it is part of might change. In other words, the Lockbox may not be present or may lose content after the OS upgrade.

Resolution

To update or reconfigure the Lockbox:

1. Open Lockbox with the password that was used to create it.
2. Reconfigure the Lockbox.

   NOTE: If the Lockbox is not present, re-create the Lockbox using the command:

   ```
   /opt/emc/scaleio/gateway/bin/FOSGWTool.sh−−set_ldap_properties−−server_url
   ldap://<LDAPSERVERIP>−−base_dn”<BASE_DN>”−−group_name”<GROUPNAME>”−c
   reate_default_lockbox
   ```

   LDAPS users must use: `ldaps://<LDAPSERVERIP>`

   instead of `ldap://` in the example above.

Incorrect folder permissions on the SVM

The chrony user is used for configuring NTP using the chrony suite. The user has incorrect permissions for folder /

var/lib/chrony, which can lead to security vulnerabilities.

About this task

On the SVM, the chrony user’s home directory has a permission mode more permissive than 750 (Owner=READ/WRITE/ EXECUTE, Group=READ/EXECUTE, Other=NONE). This can allow a malicious user to gain access to user data by escalating privileges. Permission mode for “Other” should always have “READ” and “EXECUTE” disabled. To fix the permission mode:

Steps

1. Use root login to log into the SVM.
2. Manually run the following command: chmod 750 /var/lib/chrony

Results

The permission mode for the folder is secure.

Disabling IPMI

If you are not using IPMI over LAN for monitoring or management using third-party tools, disable IPMI on all nodes in the system in order to close a security vulnerability.

Disable IPMI on a R630/R730xd server

Use the following procedure to disable IPMI on PowerFlex R630/R730xd nodes.

About this task

You can run this procedure at any time post-deployment.

Prerequisites

Ensure that:

- You have network connectivity to the server.
- You know the IP address of the iDRAC port.
- You know the password for accessing iDRAC as root). If necessary, the customer can give you the credentials.

Steps

1. Open a new browser session and log in to iDRAC.
2. On the left menu, click iDRAC settings > Network.
3. On the Network page upper menu, click IPMI Settings.

   The page jumps to the IPMI settings area.
4. In the Value column, clear the Enable IPMI Over LAN check box, and then click Apply.

   The Network page refreshes.
5. On the upper menu, click IPMI Settings again, and then confirm that the Enable IPMI Over LAN check box is cleared .
6. Log out of iDRAC.
7. Repeat the above steps on every R630/R730xd node in the system.

Disable IPMI on a R640/R740xd/R840 server

Use the following procedure to disable IPMI on PowerFlex R640/R740xd/R840 nodes.

About this task

You can run this procedure at any time post-deployment.

Prerequisites

Ensure that:

- You have network connectivity to the server.
- You know the IP address of the iDRAC port.
- You know the password for accessing iDRAC as root). If necessary, the customer can give you the credentials.

Steps

1. Open a new browser session and log in to iDRAC.
2. On the main menu, click iDRAC settings > Connectivity.
3. In the Connectivity tab, select Network > IPMI Settings.

   The IPMI configuration settings appear.
4. Change the Enable IPMI Over LAN option to Disabled, and then click Apply.
5. In the Success message, click OK.
6. Log out of iDRAC.
7. Repeat the above steps on every R640/R740xd/R840 node in the system.

Deploying PowerFlex with SELinux

PowerFlex does not support native deployment on an operating system configured with Security-Enhanced Linux (SELinux) in enforcing mode. Therefore, prerequisites must be adhered to, and preparation guidelines must be followed prior to system deployment. These guidelines also apply to an existing system that is being moved to SELinux enforcing mode.

ⓘ **CAUTION:** If you are not sure whether all other processes have been configured with SELinux policies, do not enable SELinux in enforcing mode. Contact your system administrator for guidance.

For more information about SELinux, see **https://www.redhat.com/en/topics/linux/what-is-selinux**.

SELinux Prerequisites

The following packages are prerequisites for Security-Enhanced Linux (SELinux).

Table 5. SELinux prerequisites

Package	**Description**
policycoreutils	Provides utilities for managing SELinux
selinux-policy	Provides SELinux reference policy
selinux-policy-targeted	Provides SELinux targeted policy
libselinux	Provides SELinux configuration commands
libselinux-utils	Provides SELinux configuration commands
policycoreutils-python	Required to enable the semanage command
policycoreutils-devel	Provides troubleshooting capabilities in case an issue is encountered

Download and copy the SELinux module ZIP file

Initially, an administrator is required to download the Security-Enhanced Linux (SELinux) Policy for PowerFlex to the relevant operating systems.

Steps

1. Download the latest version of the file `PowerFlex_SELinux_DDMMYYYY.zip` from:
   https://www.dell.com/support/ home/en-us/product-support/product/scaleio/drivers
2. On all relevant nodes, create a folder called `/var/PowerFlex_SELinux/`.
   Use the command:
   ```
   mkdir/var/PowerFlex_SELinux/
   ```
   The relevant nodes are:
   - MDM
   - SDS
   - SDR (if used; this includes the relevant rules for LIA)
   - SDC
   - LIA
   - PowerFlex Gateway
   - PowerFlex presentation server
3. Copy or transfer the `PowerFlex_SELinux_DDMMYYYY.zip` file to the nodes that will be used for PowerFlex.
4. On each node, perform the following:
   a. Change the directory to the folder that you created:
   ```
   cd/var/PowerFlex_SELinux/
   ```
   b. Unzip the file:
   ```
   tar–xvfPowerFlex_SELinux_DDMMYYYY.zip
   ```

Verify that SELinux is enabled

Verify that Security-Enhanced Linux (SELinux) is enabled on all relevant nodes and operating systems.

Steps

1. Run the following command on all the nodes to check SELinux status:
   ```
   sestatus
   ```
   Expected output if SELinux is enabled and set to enforcing mode:
   ```
   SELinuxstatus:enabled
   SELinuxfsmount:/sys/fs/selinux
   SELinuxrootdirectory:/etc/selinux
   Loadedpolicyname:targeted
   Currentmode:enforcing
   Modefromconfigfile:enforcing
   PolicyMLSstatus:enabled
   Policydeny_unknownstatus:allowed
   Maxkernelpolicyversion:31
   ```
   Expected output if SELinux is disabled:
   ```
   SELinuxstatus:disabled
   ```

2. If SELinux is disabled, follow the corresponding operating system's guidelines in order to enable it.

   For example, for CentOS, the steps are:

   a. Run the command:

   ```
   b.vi/etc/selinux/config
   ```

   b. Change the SELINUX line to enforcing or permissive, as needed:

   ```
   SELINUX=enforcing
   ...
   SELINUXTYPE=targeted
   ```

   c. Schedule a reboot of the operating system.

   CAUTION: If this process is running on a pre-deployed PowerFlex system, follow graceful shutdown guidelines to reboot a node with MDM\SDS\SDR\SDC. Refer to "Shutdown or restart a node gracefully" the Upgrade Dell PowerFlex matching your system version.

Load the PowerFlex SELinux module

Load the PowerFlex Security-Enhanced Linux (SELinux) module and prepare to deploy it or run it on the system.

Steps

1. Ensure that you are in the correct folder for SELinux, using the command:

   ```
   pwd
   ```

   Expected location: `/var/PowerFlex_SELinux/`

   Go to the folder, if necessary.
2. To load the policy and additional settings without impacting a deployed system, run the following command to set the current state of SELinux to Permissive state:

   ```
   setenforce0
   ```
3. Run the following command to load the SELinux module:

   ```
   semodule–idell–vxflex.pp–vv
   ```

   Expected result:

   ```
   Attemptingtoinstallmodule‘dell–vxflex.pp‘:
   Ok:returnvalueof0.
   Committingchanges:
   Ok:transactionnumber0
   ```
4. Run the following command:

   ```
   restorecon–RF/opt/emc
   ```

   This command corrects any missing labels in all directories and files in `/opt/emc`.
5. Configure the PowerFlex ports in SELinux:

   NOTE: Only run commands on the relevant node. For example, if the PowerFlex presentation server or PowerFlex Gateway is on a stand-alone node, do not enable the MDM, SDS, SDR, or LIA ports.

   For relevant port information, see "Port usage and changing default ports" in the PowerFlex Security Guide corresponding to the PowerFlex version you are using.

   If the default ports settings were changed for any process, update the command below accordingly (for example, for the PowerFlex presentation server https port).

   ```
   /usr/sbin/semanageport–N–a–tvxflex_mdm_port_t–ptcp25620;
   ```

```
/usr/sbin/semanageport–N–a–tvxflex_mdm_port_t–ptcp9011;
/usr/sbin/semanageport–N–a–tvxflex_mdm_port_t–ptcp6611;
/usr/sbin/semanageport–N–a–tvxflex_mdm_port_t–ptcp7611;
/usr/sbin/semanageport–N–a–tvxflex_mdm_port_t–ptcp25600;
/usr/sbin/semanageport–N–a–tvxflex_lia_port_t–ptcp9099;
/usr/sbin/semanageport–N–a–tvxflex_sdr_port_t–ptcp11088;
/usr/sbin/semanageport–N–a–tvxflex_sds_port_t–ptcp7072;
/usr/sbin/semanageport–N–a–tvxflex_sds_port_t–ptcp25640;
/usr/sbin/semanageport–N–a–tvxflex_gateway_port_t–ptcp443;
/usr/sbin/semanageport–N–a–tvxflex_gateway_port_t–ptcp8080;
```

NOTE: Ports 443 and 8080 are usually enabled by default in SELinux and might return the following error:

```
ValueError:Porttcp/443alreadydefined
ValueError:Porttcp/8080alreadydefined
```

In this case, proceed. This is a valid error.

```
/usr/sbin/semanageport–N–a–tvxflex_mgmt_port_t–ptcp8443;
/usr/sbin/semanageport–N–a–tvxflex_mgmt_port_t–ptcp8080;
```

6. Run the following command:

   ```
   setenforce1
   ```

   This command changes the SELinux state to the targeted state for the current run time.
7. Repeat the steps above on all nodes that will run with SELinux.

Results

Preparation of the operating system on all nodes for PowerFlex running in SELinux is now complete. Proceed with deployment, or continue to use your system if it is already deployed.

Troubleshoot SELinux with PowerFlex issues

When troubleshooting Security-Enhanced Linux (SELinux) issues with PowerFlex, confirm that the issues are related to PowerFlex.

About this task

This procedure requires moving the relevant nodes from SELinux enforcing mode to permissive mode. To return to enforcing mode later on, use the command setenforce1.

Steps

1. Change the mode of the relevant nodes from SELinux enforcing mode to permissive mode:

   ```
   setenforce0
   ```

2. If the issue disappears in permissive mode, stay in this mode and run the following commands:

   ```
   semodule–l|grepvxflex
   audit2allow–a
   semanageport–l|grepvxflex
   ```

3. Save the output to file, for sharing when opening a customer support ticket.
4. Zip the /var/log/audit/ folder and share the file in the support ticket.

   In rare cases, the support person might ask you to change SELinux logging to a higher level using this command: ”

semodule

–DB

This might require repeating the failed operation with this setting enabled. After the information is collected, run the following command to revert to the standard logging level:

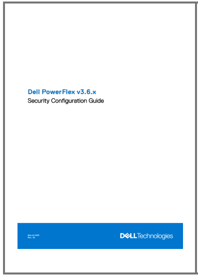
semodule

–B

See the following for troubleshooting information: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/using_selinux/troubleshooting-problems-related-to-selinux_using-selinux.

Deploying PowerFlex with SELinux

Documents / Resources

 Dell PowerFlex v3.6.x Security Configuration Guide	DELL V36X Power Flex Security Configuration [pdf] User Guide V36X Power Flex Security Configuration, V36X, Power Flex Security Configuration, Flex Security Configuration, Security Configuration, Configuration

References

- User Manual