Dell EMC PowerFlex

Security Configuration Guide

3.5.x

February 2021
Rev. 04

Notes, cautions, and warnings

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

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

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

Contents

Tables

Preface

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.

1

Introduction

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

Topics:

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 PowerFlexdevices and Virtual Machines.

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

2

Access Control Settings

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

Topics:

Supported access control settings

Access control settings are used to protect resources against unauthorized access.

The following access control settings are supported:

- 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 PowerFlex Guide*.
- 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 communicated with the MDM. For more information, see the *Configure and Customize PowerFlex Guide*.
- 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 PowerFlex Guide*, or *PowerFlex User Roles and LDAP Usage Technical Notes*.
- Access to the PowerFlex Installer requires a username and password. The user to be used is the PowerFlex Gateway user.
- Access to REST calls to the PowerFlex Gateway requires a password.
- REST authenticates user access, using the *gatewayAdminPassword* and *mdmPassword* (for more information, see the *PowerFlex REST API Reference Guide*).
- 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.
- 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:\Program Files\emc\scaleio\LIA\cfg\conf.txt`
  - Linux: `/opt/emc/scaleio/lia/cfg/conf.txt`
- 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.
- 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.
- 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 PowerFlex Guide*.
  - During deployment (on Linux and Windows only)
  - Configuring the `gatewayUser.properties` file located on the PowerFlex Gateway.
  - Using the REST API

- 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 *PowerFlex REST API Reference Guide*.
- 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.
- Access to the LIA can use local authentication or LDAP authentication, with up to 8 LDAP servers.
- LDAP support for the PowerFlex Gateway and the PowerFlex Installer now includes up to 8 LDAP servers.

NOTE: OpenSSL 64-bit v1.0.1 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.

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 PowerFlex Guide*.

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 PowerFlex Guide*.

Table 2. Local and LDAP User roles and permissions

User role	Query		Configure parameters		Configure user credentials	
	Local	**LDAP**	**Local**	**LDAP**	**Local**	**LDAP**
Monitor	Yes	Yes	No	No	No	
Configurator	Yes	Not Applicable	Yes (an aggregation of both Frontend and Backed Configurator)	Not applicable	No	Not applicable
Backend Configurator	Yes	No	Yes Backend operations only (Protection Domains, Storage Pools, Fault Sets, SDSs, Devices, other system settings)		No	No
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 PowerFlex Guide*.

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_sds command`), 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`

NOTE: 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:\Program Files\emc\scaleio\LIA\cfg\conf.txt`; Linux: `/opt/emc/scaleio/lia/cfg/conf.txt`

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`.

3

Log Settings

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.

Topics:

- Log description
- Log management and retrieval

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` Windows: `c:\Program Files\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:

Table 3. Log files (continued)

Component	Location
	• `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 GUI logs	Windows: • `%AppData%\EMC\ScaleIO\logs` Linux: • `%AppData%\EMC\ScaleIO\logs`
vSphere PowerFlex plug-in	
PowerFlex plug-in deployment log:	Windows: • `c:\Windows\System32\config\systemprofile\AppDdata\Roaming\VMware\scaleio\deployment.log` Linux: • `/opt/.vmware/scaleio/deployment.log`
PowerFlex plug-in rollbacklLog:	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.log` Linux: • `/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 the appendix "System Events and Alerts" in the *PowerFlex User Guide* for CLI commands, and the topic "Installing with the web client" in the *PowerFlex Deployment Guide*.
- Configuration of logging levels:
    - PowerFlex GUI—Logging levels can be modified. For more information, see the topic "Customizing System Preferences" in the chapter "Using the Graphical User Interface", in the *PowerFlex User Guide*.
    - PowerFlex Gateway (REST)—The log can be configured by editing the file: `<gateway installation folder>\webapps\ROOT\WEB-INF\classes\logback.xml`
    - PowerFlex Installer—The log can be configured by editing the file: `<gateway installation folder>\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 5.5—`C:\Program Files\VMware\Infrastructure\vSphereWebClient\Server\configuration`
          - For vCenter Server 5.1—`C:\Program Files\VMware\Infrastructure\vSphereWebClient\Server\config`
          - For vCenter Server 5.0—`C:\Program Files\VMware\ Infrastructure\vSphere Web Client\DMServer\config`
          - For vCenter Server Virtual Appliance 5.0—`/usr/lib/vmware-vsphere-client/server/configuration`
          - For vCenter Server Virtual Appliance 5.1—`/usr/lib/vmware-vsphere-client/server/config`
          - For vCenter Server Virtual Appliance 5.5—`/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:

         ```
         <root level="INFO">
         <appender-ref ref="SIFTED_LOG_FILE"></appender-ref>
         <appender-ref ref="LOG_FILE"></appender-ref>
         </root>
         ```

         to:

         ```
         <root level="DEBUG">
         <appender-ref ref="SIFTED_LOG_FILE"></appender-ref>
         <appender-ref ref="LOG_FILE"></appender-ref>
         </root>
         ```
      5. To add a logging section for the PowerFlex plugin, create a section to increase logging to Debug levels:

         ```
         <logger level="DEBUG" additivity="false" name="com.emc">
         <appender-ref ref="SIFTED_LOG_FILE" />
         <appender-ref ref="Log_FILE" />
         </logger>
         ```
      6. Save and close the file.
      7. Start the vSphere Web Client service. Additional logs will be written to the `C:\ProgramData\VMware\vSphere Web Client\Logs` folder
- SRS feature (Secure Remote Support)—SRS support enables secure, high-speed, 24x7, remote connection between Dell EMC 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 PowerFlex Guide*.
- Viewing events locally—Use the `showevents.py` command, using filter switches to control the severity of alerts. For more information, see the appendix "System Events and Alerts" in the *PowerFlex User Guide*.
- 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 PowerFlex component logs" in the *PowerFlex Log Collection Technical Notes*.

4

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 components and external systems or components.

Topics:

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 PowerFlex Guide.

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 | grep scini | grep options
     ```

     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
69.217.167,172.17.217.167 IoctlMdmPasswordStr=192.169.217.165-AQAAAAAAAADu/
10fXW3BS1wPBDgnkR06tdneGoUK7VQ"
```

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

```
esxcli system module parameters set -m scini -p <STRING>
```

For example:

```
esxcli system module parameters set -m scini -p "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
69.217.167,172.17.217.167 IoctlMdmPasswordStr=192.169.217.165-AQAAAAAAAADu/
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
```

Results

SDC authentication is enabled or disabled.

Port usage and change 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.

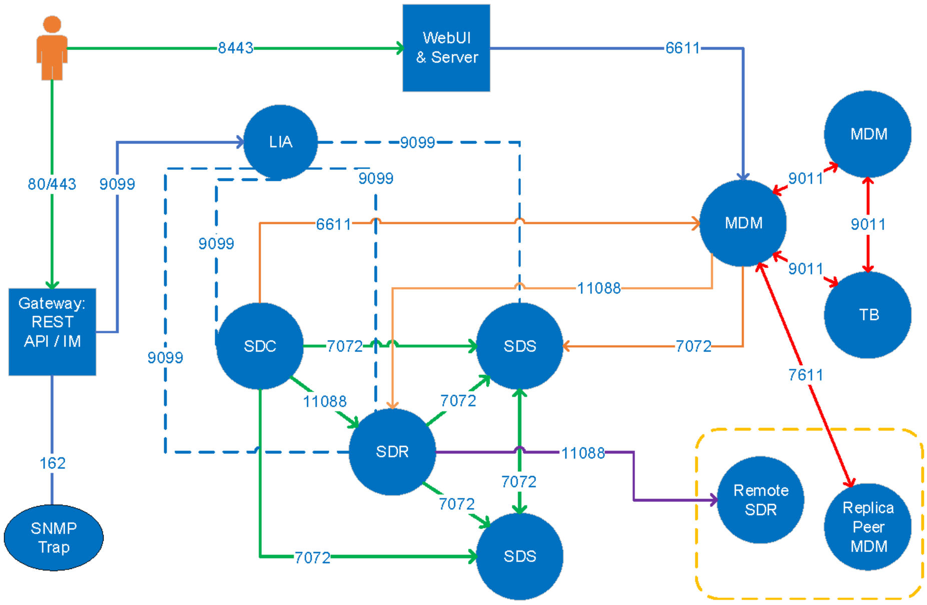
Table 4. Default ports

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_PORT>*	
MDM peer connection	7611	Proprietary (Protobuf) over TCP	/opt/emc/scaleio/mdm/cfg/conf.txt	mdm_external_port=*<NEW_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 *PowerFlex CLI Reference Guide*.
SDS listener	7072	Proprietary protocol over TCP	/opt/emc/scaleio/sds/cfg/conf.txt	tgt_port=*<NEW_PORT>*	SDCs connect through this port for data communications and to the MDM for metadata communications.
SDR listener	11088	NEW_PORT	/opt/emc/scaleio/sds/cfg/conf.txt	tgt_port=*<NEW_PORT>*	SDCs connect through this port for data communications and to the MDM for metadata communications.
LIA listener	9099	Proprietary (Protobuf) over TCP	/opt/emc/scaleio/lia/cfg/conf.txt	lia_port=*<NEW_PORT>*	The PowerFlex Installer connects to the LIA to perform installation and maintenance-related operations.
PowerFlex Gateway-Installation Manager/REST (not secure)	80 (or 8080, together with 8443)	REST over HTTPS	<gateway installation directory>/conf/catalina.properties	http.port=80 (or 8080)	The ports mentioned in parentheses are alternative ports, but can only be used if they were specified during system deployment. After changing a port, you must restart the PowerFlex Gateway service/daemon: ● Linux: Run service scaleio-gateway restart ● Windows: Restart the EMC ScaleIO Gateway service **NOTE:** When deploying PowerFlex Gateway, if one of the following ports is not free, the deployment will fail: 80, 8080, 443, 8443. If this occurs, free the above-mentioned ports, and then redeploy the PowerFlex Gateway.
PowerFlex Gateway-Installation Manager/REST (secure)	443 (or 8443, together with 8080)	REST over HTTPS	<gateway installation directory>/conf/catalina.properties	ssl.port=443 (or 8443)	
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

Table 4. Default ports (continued)

Port used by	Port #	Protocol	File to change	Field to modify (or to add, if it does not exist)	Notes
					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 PowerFlex Guide.
SNMP	162	SNMP v2 over UDP	`<gateway installation directory>/webapps/ROOT/WEB-INF/classes/gatewayUserProperties`	`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.



ⓘ **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 PowerFlex Guide*.

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 PowerFlex Guide*.

The following encryption methods are approved for use with your system:

- MDM-External components:
  - ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD
  - ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
  - ECDH-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH/RSA Au=ECDH Enc=AESGCM(256) Mac=AEAD
  - ECDH-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH/ECDSA Au=ECDH Enc=AESGCM(256) Mac=AEAD
  - ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
  - ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
  - ECDH-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH/RSA Au=ECDH Enc=AESGCM(128) Mac=AEAD
  - ECDH-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH/ECDSA Au=ECDH Enc=AESGCM(128) Mac=AEAD
  - DH-DSS-AES256-GCM-SHA384 TLSv1.2 Kx=DH/DSS Au=DH Enc=AESGCM(256) Mac=AEAD
  - DH-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH/RSA Au=DH Enc=AESGCM(256) Mac=AEAD
  - DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
  - DH-DSS-AES128-GCM-SHA256 TLSv1.2 Kx=DH/DSS Au=DH Enc=AESGCM(128) Mac=AEAD
  - DH-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH/RSA Au=DH Enc=AESGCM(128) Mac=AEAD
  - DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
  - ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
  - ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
  - ECDHE-RSA-AES256-SHA SSLv3 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA1
  - ECDHE-ECDSA-AES256-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA1
  - ECDH-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH/RSA Au=ECDH Enc=AES(256) Mac=SHA384
  - ECDH-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH/ECDSA Au=ECDH Enc=AES(256) Mac=SHA384
  - ECDH-RSA-AES256-SHA SSLv3 Kx=ECDH/RSA Au=ECDH Enc=AES(256) Mac=SHA1
  - ECDH-ECDSA-AES256-SHA SSLv3 Kx=ECDH/ECDSA Au=ECDH Enc=AES(256) Mac=SHA1
  - DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
  - DH-RSA-AES256-SHA256 TLSv1.2 Kx=DH/RSA Au=DH Enc=AES(256) Mac=SHA256
  - DH-DSS-AES256-SHA256 TLSv1.2 Kx=DH/DSS Au=DH Enc=AES(256) Mac=SHA256
  - DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
  - DH-RSA-AES256-SHA SSLv3 Kx=DH/RSA Au=DH Enc=AES(256) Mac=SHA1
  - DH-DSS-AES256-SHA SSLv3 Kx=DH/DSS Au=DH Enc=AES(256) Mac=SHA1
  - ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256
  - ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
  - ECDHE-RSA-AES128-SHA SSLv3 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA1
  - ECDHE-ECDSA-AES128-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA1
  - ECDH-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH/RSA Au=ECDH Enc=AES(128) Mac=SHA256
  - ECDH-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH/ECDSA Au=ECDH Enc=AES(128) Mac=SHA256
  - ECDH-RSA-AES128-SHA SSLv3 Kx=ECDH/RSA Au=ECDH Enc=AES(128) Mac=SHA1
  - ECDH-ECDSA-AES128-SHA SSLv3 Kx=ECDH/ECDSA Au=ECDH Enc=AES(128) Mac=SHA1
  - DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
  - DH-RSA-AES128-SHA256 TLSv1.2 Kx=DH/RSA Au=DH Enc=AES(128) Mac=SHA256
  - DH-DSS-AES128-SHA256 TLSv1.2 Kx=DH/DSS Au=DH Enc=AES(128) Mac=SHA256
  - DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
  - DH-RSA-AES128-SHA SSLv3 Kx=DH/RSA Au=DH Enc=AES(128) Mac=SHA1
  - DH-DSS-AES128-SHA SSLv3 Kx=DH/DSS Au=DH Enc=AES(128) Mac=SHA1
  - ECDHE-RSA-DES-CBC3-SHA SSLv3 Kx=ECDH Au=RSA Enc=3DES(168) Mac=SHA1

    - ECDHE-ECDSA-DES-CBC3-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=3DES(168) Mac=SHA1
    - ECDH-RSA-DES-CBC3-SHA SSLv3 Kx=ECDH/RSA Au=ECDH Enc=3DES(168) Mac=SHA1
    - ECDH-ECDSA-DES-CBC3-SHA SSLv3 Kx=ECDH/ECDSA Au=ECDH Enc=3DES(168) Mac=SHA1
    - EDH-RSA-DES-CBC3-SHA SSLv3 Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1
    - DH-RSA-DES-CBC3-SHA SSLv3 Kx=DH/RSA Au=DH Enc=3DES(168) Mac=SHA1
    - DH-DSS-DES-CBC3-SHA SSLv3 Kx=DH/DSS Au=DH Enc=3DES(168) Mac=SHA1
    - AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
    - AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
    - AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
    - AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
    - AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
    - AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
    - DES-CBC3-SHA SSLv3 Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1

- PowerFlex Gateway components other than MDM (Installer, REST):
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
    - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
    - TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
    - TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
    - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
    - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
    - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
    - TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
    - TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
    - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
    - TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
    - TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
    - TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
    - TLS_RSA_WITH_AES_256_CBC_SHA
    - TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
    - TLS_RSA_WITH_AES_128_CBC_SHA
    - TLS_EMPTY_RENEGOTIATION_INFO_SCSV
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, only for TLSv1.2 and later
    - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, only for TLSv1.2 and later
    - TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384, only for TLSv1.2 and later
    - TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384, only for TLSv1.2 and later
    - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, only for TLSv1.2 and later
    - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, only for TLSv1.2 and later
    - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, only for TLSv1.2 and later
    - TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256, only for TLSv1.2 and later
    - TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256, only for TLSv1.2 and later
    - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, only for TLSv1.2 and later
    - TLS_RSA_WITH_AES_256_CBC_SHA256, only for TLSv1.2 and later
    - TLS_RSA_WITH_AES_128_CBC_SHA256, only for TLSv1.2 and later
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
    - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
    - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
    - TLS_RSA_WITH_AES_256_GCM_SHA384
    - TLS_RSA_WITH_AES_128_GCM_SHA256

ⓘ **NOTE:** In order to use CURL on RHEL6 with PowerFlex Gateway v2.0.0.3 and higher, upgrade the NSS package to 3.21.0. (use the YUM update command).

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:\Program Files\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: `service scaleio-gateway restart`
   - 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:

   ```
   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.

5

Running scripts on hosts

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

Topics:

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 PowerFlex Guide*.

6

Known Security Issues

The following topics describe known security issues and workarounds.

Topics:

Known Issues

The following are known security issues and workarounds.

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://<LDAP SERVER IP> --base_dn "<BASE_DN>" --group_name "<GROUP NAME>" --
   create_default_lockbox
   ```

   LDAPS users must use: `ldaps://<LDAP SERVER IP>`

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

Issue

Dell EMC is aware of the side-channel analysis vulnerabilities (also known as Meltdown and Spectre) affecting many modern microprocessors that were publicly described by a team of security researchers on January 3, 2018. We encourage customers to review the Security Advisories in the References section at the following location for more information.

https://www.dell.com/support/article/en-uk/sln308588/microprocessor-side-channel-vulnerabilities-cve-2017-5715-cve-2017-5753-cve-2017-5754-impact-on-dell-emc-servers-storage-and-networking?lang=en

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.

Prevent certificate errors when ESXi hosts are added using hostnames

When hosts are added to the vCenter using hostnames, a certificate alert raised by the AMS, and certificate renewal fails. Edit the `ams.properties` file to prevent occurrence of this issue.

About this task

ⓘ **NOTE:** The change made to the file that is edited in this workaround is not saved during upgrades, and may need to be performed again.

Steps

1. On the host where AMS is installed, open the following file in a text editor:

Operating system	File path
Linux	`/opt/emc/scaleio/ams/webapps/ROOT/WEB-INF/classes/ams.properties`
Windows	`C:\Program Files\EMC\scaleio\AMS\webapps\ROOT\WEB-INF\classes\ams.properties`

2. Change the property `verifyEsxCertificates=True` to `verifyEsxCertificates=False`.
3. Save the `ams.properties` file.
4. Restart the VxFlex Ready Node AMS service:

Operating system	Action
Linux	Type the following command: `service scaleio-ams restart`
Windows	Restart the EMC ScaleIO AMS service.