Configure and Customize Dell EMC VxFlex OS
Version 3.x

Rev 03
November 2019
# CONTENTS

## Figures

| Figures | 9 |

## Tables

| Tables | 11 |

## Preface

| Preface | 13 |

## Part 1 Getting Started

| Chapter 1 | Log into VxFlex OS | 17 |
| Log in to the VxFlex OS GUI | 18 |
| Log in | 18 |
| login | 19 |
| logout | 20 |
| Use SCLI in non-secure mode | 20 |

## Part 2 Post-Deployment Activities

| Chapter 2 | Post-deployment tasks | 23 |
| Post-deployment task checklist | 24 |
| Prepare lockbox files for Java upgrade | 25 |
| Create the lockbox | 25 |
| Customer support | 26 |
| Register VxFlex OS system to SRS | 26 |
| Email notifications | 30 |
| Configure native users | 33 |
| Configure LDAP users | 34 |
| Configure SNMP | 35 |
| Enable OpenSSL FIPS compliance | 35 |
| Create and map volumes | 36 |
| Create and map volumes using the CLI | 36 |
| Create and map volumes using the VxFlex OS GUI | 37 |
| Create and map volumes using the vSphere plug-in | 38 |
| Enable storage, create and map volumes—XenServer | 38 |
| Mount VxFlex OS | 40 |
| Associate VxFlex OS volumes with physical disks | 41 |

## Part 3 VxFlex OS Performance Fine-Tuning

| Chapter 3 | VxFlex OS performance fine-tuning | 49 |
| Tune VxFlex OS for best performance | 50 |
| Performance tuning post-installation | 50 |
| Upgrades | 50 |
| Fine granularity layout performance considerations | 50 |
Tuning considerations................................................................. 50
VxFlex OS system changes.........................................................51
   Using the set_performance_parameters utility for MDM and SDS........51
   Caching Updates for VxFlex OS 2.x/3.x...........................................52
   Read RAM Cache settings for SDS..................................................53
   Read Flash Cache settings for SDS..................................................54
   Jumbo Frames and the potential impact on performance..............55
Optimize Linux..................................................................................59
   Change the GRUB template for Skylake CPUs...............................60
Optimize ESXi....................................................................................61
Optimize the SVM..............................................................................61
Optimizing VM guests........................................................................62
   I/O scheduler..................................................................................62
   Paravirtual SCSI controller..............................................................63
VxFlex OS Performance Parameters..................................................63
   RAID controller virtual disk settings...............................................65
Apply Performance Profiles to system components..........................65

Part 4 Configure and Customize 67

Chapter 4 Creating and Mapping Volumes 69

Volumes..........................................................................................70
   Add volumes..................................................................................70
   Remove volumes...........................................................................71
   Overwrite volume content...............................................................72
   Create volume snapshots..................................................................72
   Remove snapshots...........................................................................73
   Map volumes..................................................................................73
   Unmap volumes................................................................................74
   Increase a volume's size...................................................................74
   Change Read RAM Cache volume settings......................................75
   Set volume bandwidth and IOPS limits.........................................76
   Remove a snapshot consistency group............................................76
Configuring volumes, volume trees, SDCs, and snapshots..................76
   Restricted SDC mode.....................................................................77
Migrating V-Trees..............................................................................78
   Migrate volume trees (vTree)...........................................................80
   Pause V-Tree migration....................................................................81
   Roll back V-Tree migration..............................................................82
   Set V-Tree migration priority..........................................................82
Set V-Tree compression mode...........................................................82
Snapshot Policies..............................................................................83
   Add Snapshot Policy.......................................................................84
   Remove Snapshot Policy.................................................................84
   Edit Snapshot Policy........................................................................85
   Rename Snapshot Policy.................................................................85
   Pause/Resume Snapshot Policy.......................................................85
   Lock/unlock auto-snapshots............................................................85
Apply Performance Profiles to system components..........................86
Volumes in the vSphere environment................................................86
   Create and map volumes.................................................................86
   Map volumes..................................................................................87
   Unmap a volume.............................................................................88
   Add an external SDC to an existing VxFlex OS system....................88
Install the SDC on an ESXi server and connect it to VxFlex OS using `esxcli`........................................88
Install SDC on a Linux server and connect it to VxFlex OS...............89
Install SDC on an AIX server and connect it to VxFlex OS...........91
Install SDC on a Windows server and connect it to VxFlex OS....92

**SDC operations**.................................................................................................................................92
Update the SDC driver with IP address changes........................93
Detecting new volumes..........................................................................................................................93
Query volumes using `drv_cfg`.........................................................................................................94
Query tgt objects using `drv_cfg`.................................................................................................94
Query GUID using `drv_cfg`.........................................................................................................95
Query MDMs using `drv_cfg`........................................................................................................95
Loading a configuration file using `drv_cfg`................................................................................96
Adding an MDM using `drv_cfg`..................................................................................................97
Modifying an MDM IP address using `drv_cfg`........................................................................98
Permanent Device Loss state...........................................................................................................99
Update the SDC parameters in VMware based HCI or compute node.100
Run the SDC driver on SLES12.2 with multipath enabled..............100

**Chapter 5**  **Backend**  103
Configuring storage............................................................................................................................104
Configuring capacity..........................................................................................................................104
Enter and exit SDS Maintenance Mode..........................................................119
Configuring I/O priorities and bandwidth use (advanced)..................120
  Configure application IOPS and bandwidth (advanced)....................120
  System IOPS and bandwidth (advanced)...........................................121
Configuring acceleration....................................................................................................................121
  Prepare acceleration devices and software.......................................121
  RFcache (xcache) package installation..............................................141
    Install the RFcache (xcache) package on physical servers.............141
    Enable RFcache on ESXi servers..................................................141
Increase SVM memory to accommodate additional SDS device........142
Modify an SDS port during I/O........................................................................................................142

**Chapter 6**  **VASA and vVols**  145
VxFlex OS VASA's limitations and prerequisites.................................146
vVols in VxFlex OS........................................................................................................................146
Using storage policies........................................................................................................................147
Register the VxFlex OS VASA in the vCenter.................................147
Enable autostart of the VASA provider after reboot......................148

**Chapter 7**  **MDM Cluster**  149
Configuring MDM cluster................................................................................................................150
  Extend an existing VxFlex OS system.............................................150
  Add Linux servers to the MDM cluster...........................................150
  Add ESXi servers to the MDM cluster.............................................151
Replace a cluster member.................................................................................................................152
Remove members from the MDM cluster........................................159
Configure virtual IP addresses..........................................................159
Add another IP address subnet to an MDM cluster.........................159
Configure SDC access to the MDM..................................................161
Configure management session timeout parameters....................161
Configure virtual IP addresses using the VxFlex OS Installer........162
Chapter 8  Security  165
Approving pending security certificates.......................................................... 166
Default self-signed certificate expires............................................................. 166
Upgrade the VxFlex OS Gateway when a custom certificate is used............... 166
Enable LIA security.......................................................................................... 167
Certificate management for VxFlex OS Gateway.............................................167
Replace the default self-signed security certificate with your own trusted certificate...............................................................................167
Replace the default self-signed security certificate with your own self-signed certificate................................................................................169
Non-default certificate use before and after a VxFlex OS Gateway upgrade..............................................................................................................170
Configure OpenStack interoperation with the VxFlex OS Gateway....170
Generate a self-signed certificate using the keytool utility................................170
Setting up SSH authentication on the VxFlex OS Gateway.............................. 171
Configuring SSL component authentication..................................................... 171
Internal component authentication......................................................................171
External component authentication....................................................................171
Workflow for self-signed security certificates................................................. 172
Workflow for externally signed security certificates...........................................172
Using Keytool to add certificates to external components.......................... 173
Configure SDC access to the MDM................................................................. 175
Approved encryption methods.........................................................................176
Login banner overview.....................................................................................176
Set up a login banner using the CLI............................................................... 177
Upload a login banner using the VxFlex OS Installer....................................... 177
Enable/disable preemptive acceptance of the login banner.......................... 177
Activate preemptive acceptance of the login banner...................................... 178
Change LIA authentication method to LDAP................................................. 178
Add LDAP server............................................................................................ 179
Remove LDAP server .................................................................................. 179

Chapter 9  User Management  181
MDM and LDAP integration in an AMS managed system.................................182
User roles........................................................................................................ 182
Setting the User Authentication Method......................................................... 183
set_user_authentication_method......................................................................183
Adding and modifying local users.....................................................................184
add_user............................................................................................. 184
delete_user........................................................................................ 185
modify_user......................................................................................... 185
query_users.......................................................................................... 186
query_user........................................................................................ 186
reset_password.................................................................................. 186
set_password..................................................................................... 187
disable_admin.................................................................................. 188
Reset the admin user password.......................................................... 188
Deploying VxFlex OS using a non-root user..................................................... 189
Configure a non-root non-interactive sudo user........................................... 189

Chapter 10  Fault reporting features  191
General............................................................................................................ 192
Configure SNMP properties after deployment............................................... 192
Configure Dynamic Host Name resolution for SNMP in VxFlex OS.............. 192
Configure VxFlex OS Gateway properties........................................................194

Chapter 11 Add, Remove or Rename Components 199
Adding components to an existing VxFlex OS environment..............................200
   Add components using the VxFlex OS Installer.................................. 200
   Add components using the VMware deployment wizard.................... 200
Remove VxFlex OS.......................................................................................... 201
   Remove VxFlex OS using the VxFlex OS Installer............................... 201
Unregister the VxFlex OS plug-in............................................................... 202
Renaming objects........................................................................................... 202

Chapter 12 Logs 205
Enable automatic log collection........................................................................206
Set ESXi credentials for auto collect logs....................................................... 206

Chapter 13 LIA 207
Change LIA behavior.......................................................................................208
Add LIA to a system to enable automated maintenance and upgrades............ 208

Chapter 14 Setting up GUI system preferences 211
Customize system preferences........................................................................212

Part 5 VMware environment specific tasks 217

Chapter 15 VxFlex OS plug-in 219
Configure components....................................................................................220
   Configure components—basic........................................................... 222
   Configuring components—advanced................................................. 222

Chapter 16 Manually performed tasks 225
Clean the VxFlex OS VMware environment.....................................................226
SVM manual memory allocation...................................................................... 227
Managing ESXi servers................................................................................... 228
   Modify parameters on ESXi servers.................................................. 228
   Check the SDC state on ESXi servers................................................. 230

Part 6 Operating System Patching 231

Chapter 17 Operating System Patching 233
Upgrade the CentOS operating system on SVMs............................................234
   Running scripts on hosts—overview.................................................. 234
   Run a script on one or more hosts—procedures................................. 235
Contents
FIGURES

1 Test ping to ensure mtu setting................................................................. 56
2 Show interface output.................................................................................. 57
3 Adapter properties....................................................................................... 57
4 Ping output................................................................................................. 58
5 Test ping to ensure mtu setting................................................................. 59
6 Virtual Machine Properties......................................................................... 62
7 Set Volume Use Read RAM Cache window.............................................. 75
8 Add SDS window........................................................................................ 108
9 Add Device window showing command validation.................................... 110
10 System Event Log with failed DIMM......................................................... 136
11 FG Storage Pool with DAX device.............................................................. 140
12 Before adding............................................................................................ 150
13 After adding.............................................................................................. 151
14 Set Virtual IPs for VxFlex OS system screen........................................ 163
15 User Preferences window.......................................................................... 213
TABLES

1  NVDIMM information table................................................................. 124
2  Local and LDAP user roles and permissions................................. 182
3  User Preferences.............................................................................. 214
4  Plug-in activity matrix................................................................... 220
Tables
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://support.emc.com) to ensure that you are using the latest version of this document.

Previous versions of Dell EMC VxFlex OS were marketed under the name Dell EMC ScaleIO. 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.

The following Dell EMC publication sets provide information about your VxFlex OS or VxFlex Ready Node product:

- VxFlex OS software (downloadable as VxFlex OS Software <version> Documentation set)
- VxFlex Ready Node with AMS (downloadable as VxFlex Ready Node with AMS Documentation set)
- VxFlex Ready Node no AMS (downloadable as VxFlex Ready Node no AMS Documentation set)
- VxRack Node 100 Series (downloadable as VxRack Node 100 Series Documentation set)

You can download the release notes, the document sets, and other related documentation from Dell EMC Online Support.

Typographical conventions
Dell EMC uses the following type style conventions in this document:

**Bold**
Used for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks).

*Italic*
Used for full titles of publications referenced in text.

*Monospace*
Used for:
- System code
- System output, such as an error message or script
- Pathnames, filenames, prompts, and syntax
- Commands and options

*Monospace italic*
Used for variables.
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://support.emc.com](https://support.emc.com).

**Technical support**
Go to Dell EMC Online Support and click Service Center. 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.
PART 1
Getting Started

This section describes the tasks required to get started with your VxFlex OS system.

Chapter 1, "Log into VxFlex OS"
CHAPTER 1

Log into VxFlex OS

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

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

- Log in to the VxFlex OS GUI ................................................................. 18
- Log in ............................................................................................... 18
Log in to the VxFlex OS GUI

Open and log in to the VxFlex OS GUI.

Before you begin

Ensure that:

• The VxFlex OS GUI software is installed on the workstation. To install the VxFlex OS GUI, see "Install the VxFlex OS GUI."

• You have these credentials (available from the administrator):
  • MDM management IP address or hostname
  • Username (the admin user exists by default)
  • Password (defined during deployment)

Procedure

1. Open the VxFlex OS GUI:
   • Linux: Run the script /opt/emc/scaleio/gui/run.sh.
   • Windows: Click Start > All Programs > EMC > VxFlex OS GUI
   • MacOS: From the command line, run /Applications/VxFlexOS-gui-3.0-x.x.app/Contents/MacOS/VxFlexOS-gui-3.x.x.x

   The initial login screen is displayed.

2. Type the IP address or hostname and click Connect.

   If a certificate notice is displayed, review and accept the certificate.

   If a login banner is displayed, confirm it to continue.

3. In the login screen, type the username and password, and click Login.

Results

The VxFlex OS GUI is displayed.

After you finish

Users and passwords are configured with the VxFlex OS CLI. For more information, see the "Security" chapter of the VxFlex OS User Guide.

Log in

To access the CLI, you must first log in to the management system using a terminal application. If the CLI and the MDM do not reside on the same server, add the --mdm_ip parameter to all CLI commands.

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

```bash
scli --mdm_ip 10.10.10.3,10.10.10.4 --login --username supervisor1 --password password1
```

You will be prompted to enter the password.
When using LDAP, include the LDAP domain in the command. For more information on LDAP, see VxFlex OS User Roles and LDAP Usage Technical Notes. For example:

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

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

### login

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

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

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

### Syntax

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

**Note:** Actual command syntax is operating-system dependent.

### Parameters

- **--username**
  
  Username

- **--password**
  
  User password. If you do not type your password, you will be prompted to do so.

  **Note:** In Linux, to prevent the password from being recorded in the history log, leave out the `password` flag and enter the password interactively.

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

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

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

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

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

Examples

```
scli --login --username siouser1 --password 1!2@3A
```

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

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

**logout**

Log the current user out of the system.

**Syntax**

```
scli --logout
```

**Example**

```
scli --logout
```

Use SCLI in non-secure mode

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

**About this task**

You must make the following change to enable running commands.

**Procedure**

1. On every MDM server, disable secure communication:
   - Windows - In the SCLI `conf.txt` file, add `cli_use_secure_communication=0`
   - Linux - Run `echo cli_use_secure_communication=0 >> ~/.scli/conf.txt`
PART 2

Post-Deployment Activities

This section contains activities that are performed after deployment of a VxFlex OS system.

Chapter 2, "Post-deployment tasks"
CHAPTER 2

Post-deployment tasks

Perform post-deployment tasks described in this section.

After performing these tasks, continue to the "Configure and Customize VxFlex OS" section for further configuration steps as required.

- Post-deployment task checklist ................................................................. 24
- Prepare lockbox files for Java upgrade .................................................. 25
- Create the lockbox .................................................................................. 25
- Customer support .................................................................................... 26
- Configure native users ............................................................................. 33
- Configure LDAP users ............................................................................. 34
- Configure SNMP ...................................................................................... 35
- Enable OpenSSL FIPS compliance ....................................................... 35
- Create and map volumes ........................................................................ 36
- Post-deployment best practice suggestions ....................................... 45
## Post-deployment task checklist

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

### Post-deployment procedures

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

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

About this task

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

Procedure

1. From the `java\jre<VERSION>\lib\ext` (for Windows) or `java/ jre<VERSION>/lib/ext` (for Linux) Java folder, copy these files to a different folder:
   - commons-lang3-3.6.jar
   - cryptoj-6.2.3.jar
   \[Note: Only Java 8 is supported.\]

2. Update the Java version.
3. Paste these files back to the folder from where you copied them.

Create the lockbox

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

Before you begin

- Collect MDM username and password.

About this task

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

\[Note: To check whether a lockbox already exists, search for the following directory. If the lck_xml directory exists, a lockbox is configured in the system.\]

- Linux: `/opt/emcSCALEIO/gateway/conf`
- Windows: `C:\Program Files\EMC\SCALEIO\Gateway\conf`

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

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

1. Create a lockbox:

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

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

2. Add MDM credentials to the lockbox:

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

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

Customer support

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

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

Register VxFlex OS system to SRS

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

**About this task**

The following procedure describes how to register:

**Procedure**

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

**Requirements for configuring SRS via CLI**

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

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

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

**Configure SRS**

Enable Secure Remote Support (SRS) for remote support.

**Before you begin**

Ensure that you have

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

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

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

**Before you begin**

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

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

A web browser is required for this procedure.
About this task

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

Procedure

1. Enable the SRS feature in the gatewayUser.properties file.
   a. Use a text editor to open the gatewayUser.properties file, located in the following directory on the VxFlex OS Gateway server:
      
      | VxFlex OS Gateway installed on | Location of gatewayUser.properties file |
      |--------------------------------|-----------------------------------------|
      | Windows                       | C:\Program Files\EMC\ScaleIO\Gateway\webapps\ROOT\WEB-INF\classes\ |
      | Linux                         | /opt/emc/scaleio/gateway/webapps/ROOT/WEB-INF/classes |

   b. Change the enable_ESRS feature to "true":
      
      features.enable_ESRS=true

   c. Save the file.

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

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

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

      "YWRtaW46MTQ4NjQyMzM2jg4MzpOTdkYzcOTRjMGRjNT1jNT1jMzJiM2U5NWJjNmFh"

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

      curl -k -v --basic -uadmin:<token_received_from_previous_command> --form "file=@<path_to_certificate_file>" https://<VxFlex_OS_Gateway_IP_address>/api/trustHostCertificate/Mdm

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

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

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

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

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

**Results**

SRS registration is complete.

**Perform other SRS configuration activities**

Use FOSGWTool in command line for SRS configuration activities.

**About this task**

FOSGWTool is located in:

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

**Procedure**

1. The following activities can be performed with FOSGWTool:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>To unregister from all SRS gateways, type the command:</td>
<td><code>&lt;FOSGWTool_PATH&gt; --unregister_esrs_gateway --scaleio_gateway_ip &lt;ip address:port&gt; --scaleio_gateway_user &lt;user&gt; --scaleio_gateway_password &lt;password&gt;</code></td>
</tr>
<tr>
<td>To remove a specific SRS gateway from the VxFlex OS Gateway configuration, type the command:</td>
<td><code>&lt;FOSGWTool_PATH&gt; --remove_esrs_gateway --scaleio_gateway_ip &lt;scaleio_gateway_ip_address&gt; --scaleio_gateway_user &lt;scaleio_gateway_user&gt; --scaleio_gateway_password &lt;scaleio_gateway_password&gt; --esrs_gateway_ip &lt;esrs_gateway_ip_address&gt;</code></td>
</tr>
<tr>
<td>To reset the VxFlex OS Gateway admin password, type the command:</td>
<td><code>&lt;FOSGWTool_PATH&gt; --reset_password</code></td>
</tr>
</tbody>
</table>
To start SRS logic on the VxFlex OS Gateway (alerts will be sent to the SRS server), type the command:

```
<FOSGWTool_PATH> --start_esrs
```

To stop SRS logic from running on the VxFlex OS Gateway (alerts will not be sent to the SRS server), type the command:

```
<FOSGWTool_PATH> --stop_esrs
```

To check the connection to a registered SRS gateway (probing will be done throughout the servers to find one that can be connected), type the command:

```
<FOSGWTool_PATH> --check_esrs_connectivity
```

To show a list of the available FOSGWTool commands, type the command:

```
<FOSGWTool_PATH> --help
```

---

**Email notifications**

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

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

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

There are two ways to configure the email notifications feature:

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

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

**Configure email alert notifications**

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

**About this task**

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

**Procedure**

1. Use a text editor to open the `gatewayUser.properties` file, located in the following directory on the VxFlex OS Gateway server:

   `/opt/emc/scaleio/gateway/webapps/ROOT/WEB-INF/classes`

2. Set `features.notification_method=email`.
3. Add the following properties under features.notification_method=email:
   - notifications.emailSID.1.type=callHome. This is the email notification type. This is currently the default and the only option at this stage.
   - notifications.emailSID.1.SID=<SID email>. This is the email sender identification. This is the identity shown in the email's "From" field.
   - notifications.emailSID.1.username=<SID username>. This is the SMTP email notification username required when email notification uses SMTP server authentication.
   - notifications.emailSID.1.smtp=<SMTP server name>. The SMTP server's IP/hostname.
   - notifications.emailSID.1.authentication=<true or false>. Enables SMTP authentication mode for email notification.
   - notifications.emailSID.1.port=<port number>. Add the port number used for email notification. Default is 25.

4. Save and close the file.
5. Restart the VxFlex OS Gateway service

Results
Email notification is now set up to alert customer support with any issues from the VxFlex OS system.

Configure email alert notification using REST API
You can configure email notifications using the REST API.

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

Procedure
1. Select the notification method you wish to use:


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

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

notifications/email/actions/setEmailSID? type=<SID_TYPE>&sid=<SID>&smtpServer=<SMTP_SERVER>&username=<USERNAME>&password=<PASSWORD>&authenticate=<AUTHENTICATE>

where:

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

3. Start the email feature:

```
```

where:

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

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

4. You can retrieve the list of sender identity configurations:

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

where:

- `<JSESSION_ID>` is the JSESSIONID returned in the response of the `j_spring_security_check` command. For more information, see "Working with the (IM) REST API" in the VxFlex OS REST API Reference Guide.
- `<IM_IP_ADDRESS>` is the IP address of the VxFlex OS Installer
5. You can remove an email sender identity:

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

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

6. Restart the VxFlex OS Gateway service.

---

**Configure native users**

Configure native users using the VxFlex OS CLI.

**About this task**

Use the following SCLI commands to create and modify native VxFlex OS users. To run CLI commands, you must be logged in. Actual command syntax is operating-system dependent. For more information, see the VxFlex OS CLI Reference Guide. SCLI is installed as part of the MDM component and can be found in the following path:

- **ESXi**: `scli`
- **Linux**: `scli`
- **Windows**: `C:\Program Files\emc\scaleio\MDM\bin`
- **XenServer**: `siocli`

**Procedure**

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

   ```
scli --login --username <NAME> --password <PASSWORD>
   
   where `<PASSWORD>` is the password used for the first login.
   ```

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

   ```
scli --set_password --old_password <PASSWORD> --new_password <NEW_PASSWORD>
   
   where `<NEW_PASSWORD>` is the password used for the first login.
   ```

3. Add users:

   ```
scli --add_user --username <NAME> --user_role <ROLE>
   
   A randomly generated password for the created user is returned.
   ```
Configure LDAP users

Configure LDAP users if you are using LDAP with VxFlex OS.

**About this task**

For more information on using LDAP with VxFlex OS, see the "Security" section. To run SCLI commands, you must be logged in. Actual command syntax is operating-system dependent. For more information, see the *VxFlex OS CLI Reference Guide*.

**Procedure**

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

```bash
scli --add_ldap_service --ldap_service_uri <URI> --ldap_base_dn <LDAP_DN>
```

**Note:** VxFlex OS systems support authentication by up to eight LDAP servers. When multiple LDAP servers are used, add each one separately using this command.

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

```bash
scli --assign_ldap_groups_to_roles (--ldap_service_id <LDAP_SERVICE_ID> | --ldap_service_name <LDAP_SERVICE_NAME>) [--administrator_role_dn <LDAP_GROUP_DN>] [--security_role_dn <LDAP_GROUP_DN>] [--backend_config_role_dn <LDAP_GROUP_DN>] [--frontend_config_role_dn <LDAP_GROUP_DN>] [--monitor_role_dn <LDAP_GROUP_DN>]
```

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

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

5. Log in again to apply these changes.
Configure SNMP

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

Before you begin

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

About this task

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

Procedure

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

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

   `features.enable_snmp=true`

3. To add the trap receiver IP address or host name (to configure trap receivers using host names see "Configure Dynamic Host Name resolution for SNMP in VxFlex OS"), edit the parameter `snmp.traps_receiver_ip`.

   The SNMP trap receivers’ IP address parameter supports up to two comma-separated or semi-colon-separated host names or IP addresses.

4. You can optionally change the following parameters:

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

5. Save and close the file.

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

Enable OpenSSL FIPS compliance

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

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

Procedure

1. On each host running VxFlex OS, 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.

Create and map volumes

Create volumes from devices added to SDS nodes, and then map the volumes to SDC nodes. You can create and map volumes using various management tools, including the CLI, VxFlex OS GUI, vSphere web plug-in, and REST API.

Creating and mapping volumes is necessary before applications can access the volumes. In addition, you may create additional volumes and map them as part of the maintenance of the virtualization layer.

Create and map volumes using the CLI

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

About this task

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

Procedure

1. Create a volume:

   ```
   scli --add_volume --size_gb <SIZE> --volume_name <VOL_NAME> --protection_domain_name <PD_NAME> --storage_pool_name <SP_NAME>
   ```
Create and map volumes using the VxFlex OS GUI

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

Before you begin
Ensure that you can authenticate to the VxFlex OS GUI with an admin user.

About this task
For more information on creating and mapping volumes using the VxFlex OS GUI, see the user documentation.

Procedure

1. Open the VxFlex OS GUI and log in with credentials:
   - Linux: Run the script /opt/emc/scaleio/gui/run.sh.
   - Windows: Click Start > All Programs > VxFlex OS GUI
     The VxFlex OS GUI is displayed.

2. Create volumes:
   a. In the Frontend > Volumes view, select a Storage Pool to which to add the volume.
   b. From the Command menu or context-sensitive menu, select Add Volume.
      The Add Volume window is displayed.
   c. To create more than one volume, select Create multiple volumes and type the number of volumes in the Copies box.
   d. Type a name in the Name box.
   e. To start from a specific number other than 1, type it in the Start numbering at box.
      This number will be the first number in the series that will be appended to the volume name.
   f. Type a number in the Size box, representing the volume size in GB (allocation granularity is 8 GB).
   g. Select Thick (default) or Thin provisioning options.
   h. Enable or disable the Read RAM Cache feature by selecting or clearing Use Read RAM Cache.
   i. Click OK.

3. Map volumes to an SDC:
   a. In the Frontend > Volumes view, select the volumes.
   b. From the Command menu or context-sensitive menu, select Map Volumes.
      The Map Volumes window is displayed, showing a list of the volumes that will be mapped.
   c. In the Select Nodes panel, select one or more SDCs to which you want to map the volumes.
d. Click **Map Volumes**.

The progress of the operation is displayed at the bottom of the window. It is recommended to keep the window open until the operation is completed, and until you can see the result of the operation.

### Create and map volumes using the vSphere plug-in

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

**Procedure**

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

### Enable storage, create and map volumes—XenServer

Enable storage in the XenServer environment.

**Before you begin**

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

**About this task**

The VxFlex OS CLI is installed as part of the MDM component and can be found in the following path on XenServer: `siocli`

**Note:** All VxFlex OS CLI commands for XenServer begin with `siocli`. When you use CLI commands described in the remainder of the system documentation, replace `scli` with `siocli` in the documented commands.

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

**Procedure**

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

   ```bash
   siocli --login ---username <MDM_USERNAME> --password <MDM_PASSWORD>
   ```

   b. Add devices using the following command:

   ```bash
   siocli --add_sds_device --sds_ip <IP> --protection_domain_name <NAME> --storage_pool_name <NAME> --device_path <DEVICE_PATH>
   ```
Example:

```bash
siocli --add_sds_device --sds_ip 192.168.212.10 --
protection_domain_name default --storage_pool_name default --
device_path g
```

2. Add a volume:

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

Example:

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

3. Map a volume to an SDC:

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

Example:

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

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

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

```bash
xe host-list
```

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

Example:

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

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

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

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

Note: VxFlex OS provides a unique ID to each volume. It is highly recommended to use the unique ID when running on XenServer. For example, the VxFlex OS volume name in
the hypervisor is /dev/disk/by-id/scsi-emc-vol-4a7987a751237ae0-3d467d3900000000.

Example

```
xen sr-create host-uuid=09fa5d27-aa08-4c71-86bb-71dc73e9f59f content-type="ScaleIO" name-label="ScaleIO" shared=true device-config:SCSIid=emc-vol-4a7987a751237ae0-3d467d3900000000 type=lvmohba
```

**Note:** To add a shared storage repository, the following conditions must be fulfilled:

- All nodes in the XenServer Center Storage Pool must be installed with SDC.
- The VxFlex OS volume to be used as the shared SR must be mapped to all SDCs in the Storage Pool.

**Results**

You can now start using your storage.

### Mount VxFlex OS

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

**About this task**

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

**To mount VxFlex OS:**

**Procedure**

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

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

   Output similar to the following appears:

   ```
   lrwxrwxrwx 1 root root 12 Mar 2 05:35 emc-vol-7ec27ef55b8f2108-85a0f0330000000a -> ../../scinia
   lrwxrwxrwx 1 root root 12 Mar 2 05:35 emc-vol-7ec27ef55b8f2108-85a0f030200000009 -> ../../scinib
   lrwxrwxrwx 1 root root 12 Mar 2 05:35 emc-vol-7ec27ef55b8f2108-85a0f02c00000003 -> ../../scinic
   ```

2. Run the mount command:

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

   Example:

   ```
   mount /dev/disk/by-id/emc-vol-7ec27ef55b8f2108-85a0f0330000000a /mnt_scinia
   ```
3. To make the mount command persistent, edit the `/etc/fstab` file according to the instructions for your operating system:

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

  ```
  /dev/disk/by-id/emc-vol-7ec27ef55b8f2108-85a0f03300000000a /mnt_scinia ext4 defaults 0 0
  ```

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

  ```
  mount /mnt_scinia
  ```

- **RHEL 7.x:**
  In `/etc/fstab`, use a text editor to add `_netdev` to the VxFlex OS mount lines.
  Example:

  ```
  /dev/disk/by-id/emc-vol-7ec27ef55b8f2108-85a0f03300000000a /mnt_scinia ext4 defaults,_netdev 0 0
  ```

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

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

  ```
  /dev/disk/by-id/emc-vol-7ec27ef55b8f2108-85a0f03300000000a /mnt_scinia ext3 nofail 0 0
  ```

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

### Associate VxFlex OS volumes with physical disks

You can associate VxFlex OS volumes with physical disks.

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

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

Output similar to the following appears:
Volume information - Linux

You can retrieve volume information from the SDC host.

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

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

Output, similar to the following appears:

```
lrwxrwxrwx 1 root root 12 Aug 25 19:40 emc-vol-62c093a52d14aecd7-fac22a6300000000 -> ../../../scinia
lrwxrwxrwx 1 root root 12 Aug 25 19:40 emc-vol-62c093a52d14aecd7-fac22a6400000001 -> ../../../scinic
```

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

By matching the volume ID in both outputs, you can match the operating system names, sciniaX, with the VxFlex OS volume name.

For example:

- `scinia = fac22a6300000000 = vol0`
- `scinic = fac22a6400000001 = vol1`

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

```
Vendor identification: EMC
Product identification: ScaleIO
Product revision level: 1.3
Unit serial number: EMC-62c093a52d14aecd7-fac22a6300000000
```

Note:
The product identification remains as ScaleIO (not VxFlex OS).
Add VxFlex OS devices to Linux LVM physical volumes

Add VxFlex OS devices to Linux LVM physical volumes.

Procedure

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

   types = [ "scini", 16 ]

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

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

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

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

4. Continue with normal LVM steps.

Volume information - Windows

You can retrieve volume information from the MDM.

About this task

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

Procedure

1. Run the sg_inq HardiskX SCSI query command.
   The result of this command includes the EMC volume ID at the bottom of the output.
2. On the MDM, get the VxFlex OS volume information:

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

   Output similar to the following is displayed:
   Retrieved 5 volume(s)
   VOL-ID 6ac988100000000 MDM-ID 0b246c9a755ca3dd
   VOL-ID 6ac9882000000001 MDM-ID 0b246c9a755ca3dd
   VOL-ID 6ac9883000000002 MDM-ID 0b246c9a755ca3dd
   VOL-ID 6ac9884000000003 MDM-ID 0b246c9a755ca3dd
   VOL-ID 6ac9885000000004 MDM-ID 0b246c9a755ca3dd

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

   wmic diskdrive get deviceid,serialnumber | findstr "EMC"
Output similar to the following is displayed:
\\\PHYSICALDRIVE13 EMC-0b246c9a755ca3dd-6acb988500000004

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

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

After you finish

You can also get the volume ID from the VxFlex OS GUI by displaying the Identity pane of the volume’s properties sheet from Frontend > Volumes

Volume information - AIX

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

About this task

Retrieve the CuAt volume value:

Procedure

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

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

Output, similar to the following, is displayed:

CuAt:
name = "scinid0"
attribute = "vol_id"
value = "e120a92d00000000"
type = "R"
generic = "D"
rep = "a"
nls_index = 22

CuAt:
name = "scinid2"
attribute = "vol_id"
value = "e120a92f00000002"
type = "R"
generic = "D"
rep = "a"
nls_index = 22

CuAt:
name = "scinid8"
attribute = "vol_id"
value = "e120a93500000008"
type = "R"
generic = "D"
rep = "a"
nls_index = 22

CuAt:
name = "scinid0"
attribute = "vol_id"
value = "e120a92d00000000"
type = "R"
generic = "D"
You can get information for a single volume, by using this command:

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

2. Match the value of the `value` field with the VxFlex OS volume ID.

**Post-deployment best practice suggestions**

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

**About this task**

Recommended guides for best practice suggestions:

- Performance Fine Tuning section for an overview of how to enhance VxFlex OS performance
- *Security Configuration Guide* for an overview of the security settings to ensure VxFlex OS security
- Run the system analysis report as described in the *Deployment Guide*
Post-deployment tasks
PART 3

VxFlex OS Performance Fine-Tuning

This section provides an overview of the different tasks required to enhance VxFlex OS performance.

Chapter 3, "VxFlex OS performance fine-tuning"
VxFlex OS Performance Fine-Tuning
CHAPTER 3

VxFlex OS performance fine-tuning

This section provides an overview of VxFlex OS performance fine-tuning.

- Tune VxFlex OS for best performance ................................................................. 50
- Performance tuning post-installation ................................................................. 50
- VxFlex OS system changes ................................................................................ 51
- Optimize Linux .................................................................................................... 59
- Optimize ESXi ..................................................................................................... 61
- Optimize the SVM ............................................................................................ 61
- Optimizing VM guests ....................................................................................... 62
- VxFlex OS Performance Parameters ............................................................... 63
- RAID controller virtual disk settings ............................................................... 65
- Apply Performance Profiles to system components ........................................ 65
Tune VxFlex OS for best performance

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

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

Performance tuning post-installation

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

Upgrades

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

Fine granularity layout performance considerations

Fine granularity layout enables 4KB granularity and compression.

The benefit of the more efficient FG layout (pools) that allow 4KB granularity plus compression vs. 1MB of MG layout (pool) come at some performance cost. In most cases (but not all) FG will be slower than MG. In FG layout, when compression is enabled, Reads are slower than in cases where compression is disabled. There are exceptions to these rules. For example Write Response Time is similar in FG and MG. Another exception is using snaps. In FG the snaps have no impact on the performance of applications and workloads running during the snap creation. In MG snaps might have an impact on performance in some cases.

For this reason, in cases that are very sensitive to performance and do not require snaps, MG would be a better choice. It would also be a good option for cases where the data is uncompressible for example if it is already compressed or if the data is encrypted by the application.

Tuning considerations

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

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

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

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

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

Using the set_performance_parameters utility for MDM and SDS

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

The following table describes the commands for specific tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
</table>
| To view current settings | Execute the command:  
  `scli --query_performance_parameters` |
| Default is High_performance. If otherwise, execute the command to change to High_performance | Execute the command:  
  `scli --set_performance_parameters --all_sds --all_sdc --apply_to_mdm --profile high_performance` |
| To change the profile back to compact | Execute the command:  
  `scli --set_performance_parameters --all_sds --all_sdc --apply_to_mdm --profile compact` |
| To view full parameter settings for an MDM | Execute the command:  
  `scli --query_performance_parameters --print_all` |
To view full parameter settings of a specific SDS (this also shows the MDM settings)

Execute the command:

```
scli --query_performance_parameters --sds_name <NAME> --print_all
```

To view full parameter settings of a specific SDC (this also shows the MDM settings)

Execute the command:

```
scli --query_performance_parameters --sdc_name <NAME> --print_all
```

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

### Caching Updates for VxFlex OS 2.x/3.x

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

- RAM Read Cache (using a server’s DRAM memory)
- DAS Cache or Cachecade (for information on DAS Cache, see VxFlex Ready Node documentation)
- Read Flash Cache (using SSDs or flash PCI cards)

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

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

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
<th>Considerations</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM Read Cache (rmcache)</td>
<td>Read-only caching performed by server RAM.</td>
<td>RAM Read cache, the fastest type of caching, uses RAM that is allocated for caching. Its size is limited to the amount of allocated RAM. RMCache should only be used for HDD pools.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Read Flash Cache (RFCache)</td>
<td>Read-only caching performed by one or more dedicated SSD devices or flash PCI drives in the server.</td>
<td>Read Flash Cache uses the full capacity of SSD or flash PCI devices (up to eight) to provide a larger footprint of read-only LRU (least recently used) based-caching resources for the SDS. This type of caching reacts quickly to workload changes to speed up HDD Read performance.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Mode</td>
<td>Description</td>
<td>Considerations</td>
<td>Default Setting</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td></td>
<td>Several SSD devices can be allocated to a shared cache pool, and therefore the cache size is limited in size only to the amount of SSDs allocated for this purpose.</td>
<td><strong>Note:</strong> The RFCache driver must be installed during deployment. Caching devices can be defined either during the installation process, or after deployment.</td>
<td></td>
</tr>
<tr>
<td>DAS Cache</td>
<td>Read and write-back caching performed by one or more dedicated SSD devices in the server</td>
<td>DAS Cache uses the full capacity of one or more SSD devices to provide a large footprint of both read and write-back caching resources to the SDS. This caching mode moves &quot;hot&quot; (active) chunks of data from HDDs to cache, for Read and Write buffering. For write-back caching, the write is temporarily written to the SSD, which is much faster than an HDD, allowing faster response of the SDS to write acknowledgment. One SSD device can accelerate several HDDs (in DAS Cache they are called &quot;Volumes&quot;). Striping the Cache on two devices is not supported in the VxFlex Ready Node solution. <strong>Note:</strong> If a fault occurs in the caching device before the writes have been offloaded, all the HDD devices cached by DAS Cache acquire failed status, and a rebuild process commences in VxFlex OS. Once the rebuild is over, the caching disk can be replaced, all caching has stopped in the storage pool, and the HDD members in the storage pool can be cleared of errors.</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Read RAM Cache settings for SDS**

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

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

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>To enable Read RAM cache</td>
<td>Run one of the following commands:</td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>l</td>
<td>lscli --set_rmcache_usage -- protection_domain_name &lt;domain NAME&gt; -- storage_pool_name &lt;pool NAME&gt; --use_rmcache [--dont_use_rmcache]</td>
</tr>
<tr>
<td>l</td>
<td>lscli --enable_sds_rmcache [--disable_sds_rmcache] --sds_name &lt;NAME&gt;</td>
</tr>
</tbody>
</table>

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

To increase the amount of Read RAM cache

Run the following command:

```
scil --set_sds_rmcache_size {(--sds_id <ID> | --sds_name <NAME> | --sds_ip <IP> | --sds_port <PORT>) | (--protection_domain_id <ID> | --protection_domain_name <NAME>)} --rmcache_size_mb <SIZE> [--i_am_sure]
```

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

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

```
root@[116.87-1]:# scil --query_sds --sds_name 00048
Sds  T64e71bb000000025 Name: SDBR Version: 2.0.906
Protection Domain: dc(a5ed500000000000, Name: domain
bd mode: volatile
Authentication error: None
IP information (1/1 IPs):
   1: [11.1.14.2.18] Role: All (S bs and Sd)
   Port: 7072
RAM Read Cache Information:
   128.6 MB (131.72 GB) total size.
   Cache is enabled.
   RAM Read Cache memory allocation state is SUCCESSFUL.
```

**Read Flash Cache settings for SDS**

Read Flash Cache is available from version 2.x and later. This feature is a Read Cache used to increase read performance and buffers writes to increase the performance of Read-after-Write I/Os. It allows users to create and configure an "RFcache" device for any SSD or Flash card.

VxFlex OS will cache user data depending on the mode selected. This feature can greatly improve performance for specific workloads. The RFcache device is also referred to as an accelerated device.

To create an RFcache device and configure it, use the following steps:

1. Create an RFcache device (Recommendation: create 1 device per SDS).

```
scll --add_sds_rfcache_device --sds_name <NAME> --rfcache_device_path <device_path> --rfcache_device_name <RFcache device NAME>
```
2. Set the RFcache parameters (Recommendation: these parameters have a great impact on performance, therefore use the defaults).

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

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

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

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

For Read Flash Cache, the available modes are as follows:

- pass_through_none
- pass_through_read
- pass_through_write
- pass_through_read_and_write
- pass_through_write_miss

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

For more information related to using and configuring Read Flash Cache, refer to the *VxFlex OS Deployment Guide* and *VxFlex OS User Guide* at [https://support.emc.com](https://support.emc.com).

### Jumbo Frames and the potential impact on performance

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

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

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

#### Jumbo Frame configuration for Linux

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

**About this task**

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

**Procedure**

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

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

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

3. Add parameter `mtu=9000` to the file.

4. To apply the changes, type: `service network restart`

5. Execute `ifconfig` again to verify that the settings have been changed.

6. To test the command, type: `ping -M do -s 8972<DESTINATION_IP_ADDRESS>`

   Output should look similar to this:

   ![Test ping output](image)

**Figure 1 Test ping to ensure mtu setting**

---

### Jumbo Frame configuration for Windows

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

**About this task**

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

**Procedure**

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

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

   ```
   netsh interface ipv4 show interface
   ```

   Output similar to the following appears:
In this example, index 17 is the appropriate network.

3. Type the command:

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

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

4. In the Advanced tab of the Adapter Properties dialog for your vendor and driver, change the value of Jumbo Packet to 9000, as illustrated in the following figure:

5. Click OK.

The network connection may disconnect briefly during this phase.

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

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

Output similar to the following should be displayed:
Jumbo Frame configuration for ESXi

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

About this task
Perform the following steps, for all the NIC cards in the VxFlex OS system:

Procedure

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

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

   b. Create VMKernel with jumbo frames support by typing the following commands:
      a. `esxcfg-vswitch -d`
      b. `esxcfg-vswitch -A vmkernel# vSwitch#`
      c. `esxcfg-vmknic -a -i <ip address> -n <netmask> -m 9000 <portgroup name>`

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

Jumbo Frame configuration for Storage Virtual Machine

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

About this task
Perform the following steps, for all the NIC cards in the VxFlex OS system:
Procedure

1. **Edit the** `/etc/sysconfig/network/ifcfg-<NIC_NAME>`.
2. **Add parameter** `mtu=9000 to the file`.
3. To apply the changes type:
   ```
   service network restart
   ```
4. **Execute `ifconfig` command** again to confirm that the settings have been changed.
5. To test the command type:
   ```
   ping -M do -s 8972 <DESTINATION_IP_ADDRESS>
   ```

Output should look similar to the following:

![Figure 5 Test ping to ensure mtu setting](image)

**Optimize Linux**

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

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

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

For example:

```
echo noop > /sys/block/sdb/queue/scheduler
```
When CPUs have more than twelve physical cores and more performance is required from the node. For example: when CloudLink is being used for SW encryption or when Fine Granularity is being used and more performance per node is required, type the following:

```
scli --set_performance_parameters --all_sds --tech --sds_number_os_threads 12
```

Note: To make these changes persistent after reboot, either create a script that runs on boot, or change the kernel default scheduler via kernel command line.

### Change the GRUB template for Skylake CPUs

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

**Procedure**

1. Open the GRUB template for editing:

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

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

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

   Example:

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

3. Compile the new GRUB:

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

4. Stop and then disable tuned:

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

5. Run `reboot` to reboot the node.

6. Ping the node to ensure that the GRUB change was implemented.

   The ping time should be in the 0.03 ms range.

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

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

Use the following command to increase the queue length:

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

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

Example:

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

Optimize the SVM

Optimize the SVM

Procedure

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

2. From the Resources tab of the Virtual Machine Properties window, select Reserve all guest memory (All locked).
   - The Virtual Machine Properties window is displayed:
Optimizing VM guests

Select the VM guest to optimize.

I/O scheduler

When using SSD devices, it is recommended that you modify the devices' I/O scheduler. Type the following on each server, for each SDS device:

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

Example:

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

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

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

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

Windows virtual machine:

1. From the command line run:

   ```cmd
   REG ADD HKLM\SYSTEM\CurrentControlSet\services\pvscsi\Parameters \Device /v DriverParameter /t REG_SZ /d "RequestRingPages=32,MaxQueueDepth=254"
   ```

2. Reboot the virtual machine.

3. Verify the successful creation of a registry entry:
   a. Open the registry editor by running the REGEDIT command from the command line.
   b. Browse to HKLM\SYSTEM\CurrentControlSet\services\pvscsi\Parameters \Device.
   c. Verify that the DriverParameter key exists with a value of RequestRingPages=32, MaxQueueDepth=254.

Linux guests:

1. Edit the `vmw_pvscsi.conf` file:

   ```
   echo "options vmw_pvscsi cmd_per_lun=254 ring_pages=32" > /etc/modprobe.d/vmw_pvscsi.conf
   ```

2. Re-run `vmware-config-tools.pl`:

   ```
   vmware-config-tools.pl
   ```

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

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

VxFlex OS Performance Parameters

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

<table>
<thead>
<tr>
<th>Component</th>
<th>New Name (CLI)</th>
<th>Min Value</th>
<th>Max Value</th>
<th>Compact</th>
<th>High Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDM</td>
<td>mdm_net_alloc_rcv_buffer_wait_ms</td>
<td>100</td>
<td>10000</td>
<td>500</td>
<td>500</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_net_break_do_io_loop</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Component</td>
<td>New Name (CLI)</td>
<td>Min Value</td>
<td>Max Value</td>
<td>Compact</td>
<td>High Performance</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
<td>-----------</td>
<td>-----------</td>
<td>---------</td>
<td>------------------</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_number_sdc_receive_umt</td>
<td>1</td>
<td>100</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_number_sds_send_umt</td>
<td>1</td>
<td>100</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_number_sds_keepalive_receive_umt</td>
<td>1</td>
<td>100</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_sds_capacity_counters_update_interval</td>
<td>1</td>
<td>120</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_sds_capacity_counters_polling_interval</td>
<td>1</td>
<td>120</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_sds_volume_size_polling_interval</td>
<td>1</td>
<td>120</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_sds_volume_size_polling_retry_interval</td>
<td>1</td>
<td>120</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_number_sds_tasks_umt</td>
<td>1</td>
<td>2048</td>
<td>1024</td>
<td>1536</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_initial_sds_snapshot_capacity</td>
<td>1</td>
<td>10*1024</td>
<td>1024</td>
<td>1024</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_sds_snapshot_capacity_chunk_size</td>
<td>1</td>
<td>50*1024</td>
<td>5*1024</td>
<td>5*1024</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_sds_snapshot_used_capacity_threshold</td>
<td>1</td>
<td>99</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>MDM</td>
<td>mdm_sds_snapshot_free_capacity_threshold</td>
<td>101</td>
<td>1000</td>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>SDS</td>
<td>mdm_number_sockets_per_sds_ip</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>SDS</td>
<td>mdm_sds_keepalive_time</td>
<td>2000</td>
<td>3600000</td>
<td>5000</td>
<td>5000</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_number_network_umt</td>
<td>2</td>
<td>16</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_tcp_send_buffer_size</td>
<td>4</td>
<td>128*1024</td>
<td>0 (dynamic)</td>
<td>0</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_tcp_receive_buffer_size</td>
<td>4</td>
<td>128*1024</td>
<td>0 (dynamic)</td>
<td>0</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_max_number_asynchronous_io_per_device</td>
<td>1</td>
<td>2000</td>
<td>8</td>
<td>60</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_number_sdc_io_umt</td>
<td>100</td>
<td>500</td>
<td>100</td>
<td>500</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_number_sds_io_umt</td>
<td>100</td>
<td>500</td>
<td>100</td>
<td>500</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_number_sds_copy_io_umt</td>
<td>100</td>
<td>164</td>
<td>164</td>
<td>164</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_number_copy_umt</td>
<td>100</td>
<td>164</td>
<td>164</td>
<td>164</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_number_os_threads</td>
<td>1</td>
<td>32</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_number_sockets_per_sds_ip</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>
### RAID controller virtual disk settings

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

For SSDs in use by a RAID controller:
1. Create the Virtual Disk as a RAID0 device.
2. Disable the PD Cache for the HDD.
3. Set the VD Caching attributes as NRWTD (No Read Ahead, Write Through, Direct).

**Note:** For VxFlex Ready Node based install, refer to the VxFlex Ready Node documentation. The virtual disk configuration guidelines are different for external caching solutions such as DAS Cache.

---

### Apply Performance Profiles to system components

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

**About this task**

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

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

The profiles are applied separately to:

- SDSs

---

<table>
<thead>
<tr>
<th>Component</th>
<th>New Name (CLI)</th>
<th>Min Value</th>
<th>Max Value</th>
<th>Compact</th>
<th>High Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDS</td>
<td>sds_net_break_do_io_loop</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_number_io_buffers</td>
<td>1</td>
<td>10</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>SDS</td>
<td>sds_net_alloc_rcv_buffer_wait_ms</td>
<td>100</td>
<td>10000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_tcp_send_buffer_size</td>
<td>4</td>
<td>128*1024</td>
<td>512</td>
<td>4*1024</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_tcp_receive_buffer_size</td>
<td>4</td>
<td>128*1024</td>
<td>512</td>
<td>4*1024</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_number_sockets_per_sds_ip</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_number_network_os_threads</td>
<td>1</td>
<td>10</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_max_inflight_requests</td>
<td>1</td>
<td>10000</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_max_in_flight_data</td>
<td>1</td>
<td>10000</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_number_io_retries</td>
<td>1</td>
<td>100</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_volume_statistics_interval</td>
<td>1000</td>
<td>600000</td>
<td>5000</td>
<td>5000</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_optimize_zero_buffers</td>
<td>0 (FALSE)</td>
<td>1 (TRUE)</td>
<td>0 (FALSE)</td>
<td>0 (FALSE)</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_number_unmap_blocks</td>
<td>1</td>
<td>200</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>SDC</td>
<td>sdc_number_non_io_os_threads</td>
<td>1</td>
<td>16</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
To apply a profile to system components, perform the following steps:

**Procedure**

1. Depending on the system component that you want to configure, in either the **Backend > Storage** or **Frontend > SDCs** view, navigate to, and select the desired objects.

   - **Note:** If you want to apply the Performance Profile to MDMs, select the System object.

2. Right-click the object and select **Set Performance Profile for XXX**, where XXX represents one of the following:
   - MDMs
   - All SDSs
   - SDS
   - All SDCs
   - SDC

   The **Set Performance Profile for** window is displayed.

3. Select a profile from the drop-down list, and click **OK**.
PART 4

Configure and Customize

This section provides answers to common questions or scenarios when working with the VxFlex OS system.

Chapter 4, "Creating and Mapping Volumes"
Chapter 5, "Backend"
Chapter 6, "VASA and vVols"
Chapter 7, "MDM Cluster"
Chapter 8, "Security"
Chapter 9, "User Management"
Chapter 10, "Fault reporting features"
Chapter 11, "Add, Remove or Rename Components"
Chapter 12, "Logs"
Chapter 13, "LIA"
Chapter 14, "Setting up GUI system preferences"
CHAPTER 4
Creating and Mapping Volumes

The following topics describe how to create volumes from devices added to SDS nodes, and then to map the volumes to SDC nodes. Devices may have been added during, or after, the installation process.

- Volumes.................................................................................................................................70
- Configuring volumes, volume trees, SDCs, and snapshots.....................................................76
- Migrating V-Trees................................................................................................................. 78
- Set V-Tree compression mode.............................................................................................. 82
- Snapshot Policies.................................................................................................................. 83
- Apply Performance Profiles to system components..............................................................86
- Volumes in the vSphere environment.................................................................................... 86
- Add an external SDC to an existing VxFlex OS system.......................................................... 88
- SDC operations..................................................................................................................... 92
Volumes

You can define, configure and manage volumes in the VxFlex OS system.

Add volumes

Add volumes to a system.

Before you begin

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

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

About this task

The adding and mapping volume process is necessary, as part of the getting started process, before applications can access the volumes. In addition, you may create additional volumes and map them as part of the maintenance of the virtualization layer.

You can configure the caching option when creating the volumes, or you can change the Read RAM Cache feature later. If you want to enable the caching feature, ensure that the feature is also enabled in the backend of the system, for the corresponding Storage Pool and SDSs. For more information, see "Change Read RAM Cache volume settings".

Define volume names according to the following rules:

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

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

To add one or multiple volumes, perform these steps:

Procedure

1. In any of the Frontend > Volumes views, navigate to the Storage Pool to which you want to add the volume, and select it.
2. From the Command menu or context-sensitive menu, select Add Volume.
3. In the Add Volume window, if you want to create more than one volume, select Create multiple volumes and type the number of volumes you would like to add in the Copies box.
   - If you type 1, only one volume will be created (optional—can be left blank).
   - If you type a number greater than 1, the characters %i% will be added to the Name box, and multiple volumes will be created, accordingly. The volumes will be named and numbered automatically, starting from 1. If you want the numbering to start from a different number, type it in the Start numbering at box, as described in step 5. The remaining options in the window will be assigned to all the volumes created in this operation.
4. Type a name for the volume:
   - If you are adding one volume, enter the name in the Name box.
• If you are adding multiple volumes, enter the base name in the **Base name** box.
  The volumes will all be created with the same name, and a number will be appended instead of the characters `%i%`. These characters can be positioned anywhere in the name. The names that will be created are displayed in the right pane of the window, as shown in the figure later in this topic.

5. If you want the numbering to start from a specific number other than 1, type it in the **Start numbering at** box.
   This number will be the first number in the series that will be appended to the volume name. For example, if the **Name** is `Vol%i%` and the **Start numbering at** value is `100`, the name of the first volume created will be `Vol100`, and the second volume will be `Vol101`, and so on.

6. Type a number in the **Size** box, representing the volume size in GB (basic allocation granularity is 8 GB).

7. Select either **Thick** (default) or **Thin** provisioning options.

8. If you want to enable the RMcache feature (disabled by default), select **Use RMcache**.

9. Click **OK**.

  **Note:** The progress of the operation is displayed at the bottom of the window. It is recommended to keep the window open until the operation is completed, and until you can see the result of the operation.

**After you finish**

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

### Remove volumes

Remove volumes from Storage Pools.

**Before you begin**

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

**About this task**

If you want to remove a volume’s related snapshots, or just the snapshots, see "Remove Snapshots".

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

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

**Procedure**

1. In any of the views of the **Frontend > Volumes** view, navigate to the volume or volumes you want to remove, and select them.

2. From the **Command menu** or context-sensitive menu, select **Remove**.
   The **Remove Volumes** window is displayed, showing a list of the volumes that will be removed.

3. Click **OK**.
The progress of the operation is displayed at the bottom of the window. It is recommended to keep the window open until the operation is completed, and until you can see the result of the operation.

**Overwrite volume content**

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

**About this task**

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

**Procedure**

1. In any of the **Frontend > Volumes** views, navigate to the Storage Pool.
2. From the Command menu or context-sensitive menu, select **Overwrite Content**.
3. In the **Overwrite volume content** window, select the source volume from which to overwrite the content of the volume.
4. In the **Overwrite volume content** dialog box, in the **Password Confirmation** field, enter the admin password.
5. Click **OK**.

**Results**

The content from the volume is overwritten.

**Create volume snapshots**

Take a snapshot of one or more volumes.

**About this task**

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

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

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

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

VxFlex OS objects are assigned a unique ID that can be used to identify the object in CLI commands. You can retrieve the ID via a query, or via the object’s property sheet in the VxFlex OS GUI.

**Note:**

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

To take a snapshot, perform these steps:

**Procedure**

1. In the **Frontend > Volumes** view, navigate to the volumes, and select them.
2. From the **Command menu** or context-sensitive menu, select **Snapshot Volume**.
The **Snapshot Volume** window is displayed, showing the volumes for which snapshots will be created.

3. In the Index box, type the number that you want to append to the snapshot names.

4. If you want the snapshots to belong to a consistency group, ensure that the **Create Consistency Group** check box is selected.

5. Click OK.

The progress of the operation is displayed at the bottom of the window. It is recommended to keep the window open until the operation is completed, and until you can see the result of the operation.

### Remove snapshots

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

**About this task**

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

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

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

**Procedure**

1. In the **Frontend > Volumes > V-Trees** view, navigate to the volume from which you want to remove snapshots, and select it.

2. From the **Command menu** or context-sensitive menu, select one of the following options:
   - To remove both the parent volume and all volumes that were created as snapshots of the specified volume or one of its descendants, select **Remove with Descendants**
   - To retain the parent volume, and remove only its snapshots, select **Remove Descendants Only**

   The **Remove Volumes** window is displayed, showing a list of the objects that will be removed.

3. Click OK.

The progress of the operation is displayed at the bottom of the window. It is recommended to keep the window open until the operation is completed, and until you can see the result of the operation.

### Map volumes

Map one or more volumes to SDCs.

**About this task**

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

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

**To identify the unique ID, run the `ls -l /dev/disk/by-id/` command.** For more information, see "Associate VxFlex OS volumes with physical disks". You can also identify the unique ID using
VMware. In the VMware management interface, the device is called **EMC Fibre Channel Disk**, followed by an ID number starting with the prefix **eui**.

**Note:** You can’t map a volume if the volume is an auto snapshot that is not locked.

To map volumes, perform these steps:

**Procedure**

1. In the **Frontend > Volumes** view, navigate to the volumes, and select them.
2. From the **Command menu** or context-sensitive menu, select **Map**.
   
   The **Map Volumes** window is displayed, showing a list of the volumes that will be mapped.
3. In the **Select Nodes** panel, select one or more SDCs to which you want to map the volumes.
   
   - You can use the search box to find SDCs.
   - If you select an SDC that is already mapped to the volume, a green icon will appear in the mapping matrix on the right side of the window.
4. Click **Map Volumes**.

**Note:** The progress of the operation is displayed at the bottom of the window. It is recommended to keep the window open until the operation is completed, and until you can see the result of the operation.

### Unmap volumes

Unmap one or more volumes from SDCs.

**Procedure**

1. In any of the **Frontend > Volume** views, navigate to the volumes, and select them.
2. From the **Command menu** or context-sensitive menu, select **Unmap Volumes**.
   
   The **Unmap Volumes** window is displayed, showing a list of the volumes that will be unmapped.
3. If you want to exclude some SDCs from the unmap operation, in the **Select Nodes** panel, select one or more SDCs for which you want to retain mapping.
   
   You can use the search box to find SDCs.
4. Click **Unmap Volumes**.

The progress of the operation is displayed at the bottom of the window. It is recommended to keep the window open until the operation is completed, and until you can see the result of the operation.

### Increase a volume's size

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

**About this task**

**Procedure**

1. In **Frontend > Volumes**, select the **Volumes** or **Volumes Monitor** view.
2. Navigate to the volumes, and select them.
3. From the **Command menu** or context-sensitive menu, select **Increase Volumes’ Size**.
The Increase Volumes' Size window is displayed, showing a list of the volumes that will be modified.

4. In the **New Size** box, type a number representing the new volume size in GB (basic allocation granularity is 8 GB).

5. Click **OK**.

   The progress of the operation is displayed at the bottom of the window. It is recommended to keep the window open until the operation is completed, and until you can see the result of the operation.

### Change Read RAM Cache volume settings

Enable or disable Read RAM Cache per volume.

**About this task**

By default, Read RAM Cache is disabled on volumes.

**Note:** RMcache should only be used for HDD pools.

To change Read RAM Cache settings on volumes, perform these steps:

**Procedure**

1. In **Frontend > Volumes**, select the **Volumes** or **Volumes Monitor** view.
2. Navigate to the volumes, and select them.
3. Right-click the volumes and select **Settings > Set Read RAM Cache**.
   
   The **Set Volume Use Read RAM Cache** window is displayed, showing a list of the volumes that will be modified.

4. Select or clear the **Use Read RAM Cache** check box as follows:
   
   - To disable Read RAM Cache on the volumes, clear the check box.
   - To enable Read RAM Cache on the volumes, select the check box.

5. Click **OK**.

   The progress of the operation is displayed at the bottom of the window. It is recommended to keep the window open until the operation is completed, and until you can see the result of the operation.
Set volume bandwidth and IOPS limits

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

Before you begin

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

About this task

Procedure

1. In Frontend > Volumes view, select the Volumes or Volumes Monitor view.
2. Navigate to the volumes, and select them.
3. From the Command menu or context-sensitive menu, select Set Limits.
   The Set Volume Limits window is displayed, showing a list of the volumes to be modified.
4. In the Bandwidth Limits and IOPS Limits boxes, type the required values, or select the corresponding Unlimited check box.
   • The number of IOPS must be larger than 10.
   • The volume network bandwidth is in MB/sec.
5. In the Select Nodes panel, select the SDCs to which you want to apply the changes.
6. Click Set Limits.
   The progress of the operation is displayed at the bottom of the window. It is recommended to keep the window open until the operation is completed, and until you can see the result of the operation.

Remove a snapshot consistency group

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

About this task

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

Procedure

1. In the Frontend > Volumes > V-Trees view, navigate to the snapshot whose consistency group you want to remove, and select the snapshot.
2. From the Command menu or context-sensitive menu, select Remove Consistency Group.
   The Remove Consistency Group window is displayed, showing the selected snapshot.
3. Click OK.
   The progress of the operation is displayed at the bottom of the window. It is recommended to keep the window open until the operation is completed, and until you can see the result of the operation.

Configuring volumes, volume trees, SDCs, and snapshots

This section contains procedures for adding, removing, and managing volumes and snapshots. It explains how to remove volumes, create snapshots, and set volume bandwidth and IOPS limits. It
also describes setting the SDC restriction mode and how to approve SDCs before mapping volumes.

**Restricted SDC mode**

Enabling restricted SDC mode gives you more control over VxFlex OS. Restricted SDC mode is set at the system level. When enabled, you must approve SDCs prior to mapping volumes to them. The restricted SDC setting has the following modes:

- **No restriction** — Volumes can be mapped without pre-approving SDCs.
- **GUID restriction** — SDCs are approved using their GUID. Only once the SDC is approved can it be used for mapping volumes.
- **Approved IP restriction** — SDCs must be approved using their GUID and IP address. Only once the SDC is approved using both GUID and IP address can it be used for mapping volumes.

You can set the restricted SDC mode using the VxFlex OS GUI, CLI, or REST API.

**Note:** In a system that has been upgraded and already has volumes mapped to SDCs, if you want to enable restricted SDC mode, you must first approve the SDCs and only then enable restricted SDC mode.

Set the system’s restricted SDC mode using the VxFlex OS GUI

Use the VxFlex OS GUI to set the restricted SDC mode.

**About this task**

The system's restricted SDC mode can also be set using the CLI or the REST API. For details, see the *CLI Reference Guide* or the *REST API Reference Guide*.

**Note:** In a system that has been upgraded and already has volumes mapped to SDCs, if you want to enable restricted SDC mode, you must first approve the SDCs and only then enable restricted SDC mode.

**Procedure**

1. In the **Frontend > SDCs** view, right-click on the System and select **Set Restricted SDC Mode**.
2. In the **Set Restricted SDC Mode** dialog box, select one of the following options and click **OK**.
   - No restriction
   - GUID restriction
   - Approved IP restriction

**Results**

The restricted SDC mode is set for the system. If you enabled restricted SDC mode by selecting either **GUID restriction** or **Approved IP restriction**, you must configure approved SDCs before you can map volumes.

Approve SDCs using the VxFlex OS GUI

When the system's restricted SDC mode is set to GUID restriction, you must approve SDCs before you can map volumes.

**Procedure**

1. In the **Frontend > SDCs** view, right-click on one or several SDCs that you want to approve and select **Approve SDC**.
2. In the **Approve SDC** window, verify that the SDCs listed are the ones you want to approve and click **OK**.

**Results**
The SDCs are approved and you can map volumes. The **Approved IPs** column in the **Frontend > SDCs** displays which SDCs are approved.

**Configure approved SDC IP addresses using the VxFlex OS GUI**

When the system's restricted SDC mode is set to **approved IP restriction**, you must configure SDC IP addresses before you can map volumes.

**Before you begin**
Ensure that the SDCs have been approved by GUID.

**Procedure**
1. In the **Frontend > SDCs** view, right-click on the SDCs that you want to approve and select **Configure Approved IP Addresses**.
2. In the **Configure Approved IP Addresses** window, add the IP addresses of the SDCs you want to approve.
   - You can click the **Add IP Address** button to add up to a total of four IP addresses.
3. Click **OK** and then click **Close**.

**Results**
The SDC IP addresses are approved and you can map volumes. The **Approved IPs** column in the **Frontend > SDCs** view displays which SDC are approved.

**Manual SDC configuration/verification**

If there are problems connecting to a VxFlex OS system after a reboot, users can modify the **drv_cfg.txt** file or use the **drv_cfg** utility to ensure that the SDC reconnects to the MDM automatically upon node restart/reboot.

To do this, perform one of the following procedures:
- Edit **/bin/emc/scaleio/drv_cfg.txt** and change the **#MDM** line to include each IP address for any node(s) containing an MDM in your cluster.
  - For example, change the line:
    - From:
      ```
      #mdm 10.20.30.40
      ```
    - To:
      ```
      mdm 10.108.158.48,10.108.158.49
      ```
    - where .48 is the master node, and .49 is the slave node. The Tie-Breaker node should not be included.
- Use the **drv_cfg** binary or **drv_cfg.exe** on Windows to re-attach the MDM.
- Rescan all volumes using the **drv_cfg** utility.

**Migrating V-Trees**

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

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

- In order to move the volumes to a Storage Pool with a different performance tier
- To move to a different Storage Pool or Protection Domain due to multitenancy
- To decrease the capacity of a system by moving out of a specific Storage Pool
- To change from a thin-provisioned volume to a thick-provisioned volume or the reverse
- In order to move the volumes from a Medium Granularity Storage Pool to a Fine Granularity Storage Pool
- To clear a Protection Domain for maintenance and then return the volumes to it

During V-tree migration, you can run other tasks such as creating snapshots, deleting snapshots, and entering maintenance mode. **Note:** You cannot create snapshots when migrating from a Medium Granularity Storage Pool to a Fine Granularity Storage Pool.

When the user requests a V-Tree migration, the MDM first estimates whether the destination Storage Pool has enough capacity for the migration to complete successfully. The MDM bases the estimation on its information of the current capacity of the V-Tree. If there is insufficient capacity at the destination based on that estimate, migration does not start. (An advanced option allows you to force the migration even if there is insufficient capacity at the destination, with the intention to increase the capacity as required during the migration.) The MDM does not reserve the estimated capacity at the destination (since the capacity of the source volume can grow during migration and the reserved capacity does not guarantee success). The MDM does not hold onto source capacity once it has been migrated, but releases it immediately.

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

<table>
<thead>
<tr>
<th>Source SP</th>
<th>Destination SP</th>
</tr>
</thead>
<tbody>
<tr>
<td>MG Non Zero Padded</td>
<td>MG Non Zero Padded</td>
</tr>
<tr>
<td>Thick</td>
<td>Thin</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Thin</td>
<td>Thick</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Thick</td>
<td>Thin</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Note: When migrating to a Fine Granularity Storage Pool, the MDM does not reserve the capacity of the source volume during migration, which might affect the performance of the application that is using the migrated volume.

**Note:** You can speed up the migration by adjusting the volume migration I/O priority (GoS). The default favors applications with one concurrent I/O and 10 MB/sec per device. Increasing the 10 MB/sec increases the migration speed in most cases. The maximum value that can be reached is 25 MB/sec. The faster the migration, the higher the impact might be on applications.
To avoid significant impact, the value of concurrent I/O operations per second should not be increased.

When migrating from a Medium Granularity Storage Pool to a Fine Granularity Storage Pool, volumes must be zero padded. For more information on zero padding, see "Storage Pools" in the Getting to Know Guide.

You can pause a V-Tree migration at any time, in the following ways:

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

Once paused, you can choose to resume the V-Tree migration, or to roll back the migration and have all volume blocks returned to the original Storage Pool.

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

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

### Migrate volume trees (vTree)

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

**Before you begin**

Note the following limitations:

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

**Procedure**

1. In the left pane, click **Configuration > Volumes**.
2. In the right pane, select the relevant volume and then in the Details pane, click the vTree tab.
3. Click the vTree button and select **Migrate vTree**.
4. In the **Migrate vTree of <volume name>** dialog box, select the destination Storage Pool. The Storage Pool's free capacity is displayed. Ensure that you select a Storage Pool with enough capacity for the vTree size.
5. Optionally, expand **Advanced** to select one or several of the following advanced options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add migration at the head of the migration queue</strong></td>
<td>Give this vTree migration the highest priority in the migration priority queue.</td>
</tr>
<tr>
<td><strong>Ignore destination capacity</strong></td>
<td>Allow the migration to start regardless of whether there is enough capacity at the destination.</td>
</tr>
<tr>
<td><strong>Enable compression</strong></td>
<td>Compression is done by applying a compression-algorithm to the data. For more information on compression mode, see &quot;V-Trees&quot; in the <strong>Getting to Know</strong> guide.</td>
</tr>
<tr>
<td><strong>Convert vTree from...</strong></td>
<td>Convert a thin-provisioned vTree to thick-provisioned, or vice-versa, at the destination, depending on the provisioning of the source volume.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> SDCs with a version earlier than v3.0 do not fully support converting a thick-provisioned vTree to a thin-provisioned vTree during migration; after migration, the vTree will be thin-provisioned, but the SDC will not be able to trim it. These volumes can be trimmed by unmapping and then remapping them, or by rebooting the SDC. The SDC version will not affect capacity allocation and a vTree converted from thick to thin provisioning will be reduced in size accordingly in the system.</td>
</tr>
<tr>
<td><strong>Save current vTree provisioning state during migration</strong></td>
<td>The provisioning state is returned to it's original state before the migration took place.</td>
</tr>
</tbody>
</table>

6. Click **Migrate Vtree**.
7. Verify that the operation completed successfully and click **Dismiss**.

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

**Pause V-Tree migration**
You can pause a V-Tree migration at any time.

**About this task**
The following ways are used to pause the V-Tree migration:
- **Gracefully:** To allow all data blocks currently being migrated to finish migration before pausing.
- **Forcefully:** To abort the migration of all blocks currently in progress and carries a potential risk to data.

**Procedure**
1. In the **Frontend > Volumes** view, select the **V-Trees** display.
2. Expand the list of Protection Domains and Storage Pools and select the V-Tree whose migration you want to pause.
   To easily identify the V-Tree, search the **Migration** column for the following icon, which indicates volumes that are currently being migrated:
3. Right-click the volume and select **Pause V-Tree Migration**.
4. In the **Pause V-Tree Migration** dialog box, select whether you want to pause gracefully or forcefully and click **OK**.
   
   If you selected to pause the migration gracefully, the migration icon is colored blue until the migration pauses successfully. A gray migration icon indicates that the migration is paused. Once paused, you can choose to roll back the V-Tree migration or resume the V-Tree migration from the Command menu.

**Roll back V-Tree migration**

You can roll back to the source Storage Pool.

**About this task**

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

**Procedure**

1. In the **Frontend > Volumes** view, select the **V-Trees** display.
2. Expand the list of Protection Domains and Storage Pools and select the V-Tree whose migration you wish to roll back.
   
   To easily identify the V-Tree, search the **Migration** column for the following icon, which indicates a V-Tree migration that is currently paused:

3. Right-click the volume and select **Roll back V-Tree migration**.
   
   The migration resumes in the reverse direction so that any data already migrated to the destination Storage Pool is now migrating to the source Storage Pool.

**Set V-Tree migration priority**

Set the priority of a V-Tree migration to be at the head or the tail of the migration queue.

**About this task**

**Procedure**

1. In the **Frontend > Volumes** view, select the **V-Trees** display.
2. Expand the list of Protection Domains and Storage Pools and select the V-Tree whose migration priority you want to set.
   
   To easily identify the V-Tree, search the **Migration** column for the following icon, which indicates volumes that are currently being migrated:

3. Right-click the volume and select **Set V-Tree Migration Priority**.
4. In the **Set V-Tree Migration Policy** dialog box, select whether to move the current V-Tree migration to the head or the tail of the migration queue and click **OK**.

**Set V-Tree compression mode**

You can enable compression per V-Tree for Fine Granularity Storage Pools.

**About this task**

Compression is done by applying a compression-algorithm to the data. For more information on compression mode, see “V-Trees” on the *Getting to Know* guide.
Procedure
1. From Frontend > Volumes > V-Tree Migration view or V-Tree Capacity Utilization view, drill down to the relevant volume.
2. Right-click on the volume and select Set V-Tree Compression Mode.
   The Set V-Tree Compression Mode dialog box is displayed.
3. Select the Enable Compression check-box.
4. Click OK.
5. In the Are you sure? dialog box, click OK.
6. Click Close.

Results
Compression mode is enabled for the V-Tree.

Snapshot Policies
Snapshot Policies enable you to define policies where you can configure the number of snapshots to take at a given time for one or more volumes.

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

Example:
Rule: Take snapshots every 60 minutes
Retention Levels:
- 24 snapshots
- 7 snapshots
- 4 snapshots

After defining the parameters, you must then select the source volume to add to the Snapshot Policy. You can add multiple source volumes to a Snapshot Policy, but a specific volume can only be the source volume of a single policy. Only one volume per VTree may be used as a source volume of a policy (any policy). For more information on V-Trees, see "Snapshots" in the Getting to Know Guide.

When you remove the source volume from the policy, you must choose how to handle auto-snapshots. Snapshots created by the policy are referred to as auto-snapshots. Your selection depends on if there are locked auto snapshots.

- If the source volume has no auto snapshots, it doesn’t matter if you select Detach auto snapshots or Remove auto snapshots.
- If the source volume has auto snapshots but none of them are locked, you can choose to detach all snapshots. They become regular snapshots as if the user created them manually. If you select Remove auto snapshots, they are deleted.
- If the source volume has locked auto snapshots, you can choose to detach all snapshots. They become regular snapshots, as if the user created them manually. If you remove them, those that are not locked are removed, while the auto snapshots which are locked are detached.
Add Snapshot Policy

You can create Snapshot Policies that include the time interval and number of snapshots per retention level, and then add source volumes to the policy.

About this task

Note: Create paused policy is optional

Procedure
1. From Frontend > Volumes, select the Snapshot Policy view.
2. Click Add New Policy.
   The New Policy dialog box is displayed.
3. Enter a name in the Policy Name box.
4. Select the Create Paused Policy check box to put policy on hold.
5. Enter the time interval to take snapshots in the Take snapshot every box.
6. Enter the number of snapshots to keep according to the time interval defined in the Retention Levels box.
7. Click Create.
8. Select one or more volumes to add to the snapshot policy.
9. Click Add and then Close.

Remove Snapshot Policy

You can remove a snapshot policy.

About this task

Procedure
1. From Frontend > Volumes, select the Snapshot Policy view.
2. Select the relevant policy and from the Command menu or context-sensitive menu, select View/Edit Policy details.
3. In the Source Volumes section, drill down from the protection domain to the connected volumes.
4. Right-click on the volume and select Remove source Volume.
   The Remove Source Volumes from Snapshot Policy dialog box is displayed.
5. (Optional) From Choose how to handle auto snapshots already created for removed source volumes select Detach auto snapshots or Remove auto snapshots.
6. Click OK and then Close.
7. Click Close.
8. Right-click on the snapshot policy and select Remove policy.
   The Remove Snapshot Policy dialog box is displayed.
9. Click OK and then Close.
**Edit Snapshot Policy**

You can edit a Snapshot Policy as well as add/remove a volume to/from the policy.

1. From **Frontend > Volumes**, select the **Snapshot Policy** view.
2. Select the relevant policy and from the Command menu or context-sensitive menu, select **View/Edit Policy details**.
3. Click **Edit policy** to update the policy fields.
4. Click **Add Volumes** to select or clear source volumes and then click **Add**.
5. Click **Close**.

**Rename Snapshot Policy**

You can rename the Snapshot Policy.

1. From **Frontend > Volumes**, select the **Snapshot Policy** view.
2. Select the relevant policy and from the Command menu or context-sensitive menu, select **Rename Policy**
   The **Rename Snapshot Policy** dialog box is displayed.
3. Enter a new name for the policy in the **Snapshot Policy Name** box.
4. Click **OK**.
   The policy is renamed.

**Pause/Resume Snapshot Policy**

You can pause or resume an active Snapshot Policy.

1. From **Frontend > Volumes**, select the **Snapshot Policy** view.
2. Select the relevant policy and from the Command menu or context-sensitive menu, select **Pause Policy** or **Resume Policy**
   The **Pause Snapshot Policy** or **Resume Snapshot Policy** dialog box is displayed.
3. Click **OK**.
   The policy is paused or resumed to active state.

**Lock/unlock auto-snapshots**

You can lock/unlock auto-snapshots.

**About this task**

**Procedure**

1. From **Frontend > Volumes**, select the **Snapshot Policy** view.
2. Select the relevant policy and from the Command menu or context-sensitive menu, select **View/Edit Policy details**.
3. From the **Source Volumes** pane, click the **Auto Snapshots grouped by Storage Pools** or the **Auto Snapshots grouped by time** button.
4. Drill down to the relevant snapshot and then right-click and select **Lock Snapshot** or **Unlock Snapshot**.
   The **Lock/Unlock Auto Snapshots** dialog is displayed.
5. Click **OK** to confirm you would like to lock/unlock the selected Snapshots.
Apply Performance Profiles to system components

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

**About this task**

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

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

The profiles are applied separately to:

- SDSs
- SDCs
- MDM cluster

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

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

**Procedure**

1. Depending on the system component that you want to configure, in either the Backend > Storage or Frontend > SDCs view, navigate to, and select the desired objects.

   **Note:** If you want to apply the Performance Profile to MDMs, select the System object.

2. Right-click the object and select Set Performance Profile for XXX, where XXX represents one of the following:
   - MDMs
   - All SDSs
   - SDS
   - All SDCs
   - SDC

   The Set Performance Profile for window is displayed.

3. Select a profile from the drop-down list, and click OK.

Volumes in the vSphere environment

The following topics describe how to use the VxFlex OS plug-in to add, map, and unmap volumes in the vSphere environment. You can map volumes to SDCs in the same step, or you can map the volume after it has been created.

**Create and map volumes**

**About this task**

Volumes are created from devices in a Storage Pool.
Procedure

1. From the Storage Pools screen, click Actions > Create volume.
   The Create Volume dialog appears.

2. Enter the following information:
   - **Volume name**: Enter a name for the new volume.
   - **Number of volumes to create**: Enter the number of volumes to create. Multiple volumes appear as `volume_name-X`.
   - **Volume size**: Enter the size of the volume. This must be in multiples of 8 GB.
   - **Volume provisioning**: Select thick or thin provisioning.
   - **Use RAM Read Cache**: Select to enable RAM Read Cache for the created volumes. Use of RAM Read Cache is determined by the policy for the Storage Pool and the volume.
   - **Obfuscation**: Select whether the volume should be obfuscated.

3. To map the volume to ESXs, perform the following steps:
   a. Select **Map volume to ESXs**.
   b. In the Select ESXs area, select the clusters or ESXs to which this volume should be mapped.
   c. Click **OK**.
   d. Enter the password for the VxFlex OS administrative user.

The following figure illustrates multiple volumes created:

![Multiple Volumes Created](image)

Map volumes

About this task

Manually map volumes after they have been created, from the Volumes screen.

Procedure

1. From the Volumes screen, select a volume to map, then choose Actions > Map a volume.
2. In the Map Volume to ESXs dialog box, select the clusters or ESXs to which this volume should be mapped.
3. To configure the LUN identifier manually, select **Manually configure LUN identifier** to and enter the identifier ID.
4. Click **OK**.
Unmap a volume

About this task
You can use the VxFlex OS plug-in to unmap a volume from an ESXi.

Procedure
1. From the Volumes screen, select the volume to unmap, and click Actions > Unmap volume.
2. In the Unmap Volume from ESXi dialog box, select the ESXi or clusters from which to unmap the volume, then click OK.

Add an external SDC to an existing VxFlex OS system

You can add an external SDC to an existing VxFlex OS system.
During manual installation, you can install the SDC according to the operating system-specific instructions in the following section, and it will be connected to the existing VxFlex OS system.

Install the SDC on an ESXi server and connect it to VxFlex OS using esxcli
Install the SDC with the appropriate parameters to connect it to an existing VxFlex OS system. This procedure is relevant both for adding more SDCs to an existing system, and for adding SDCs to a 2-layer system during initial deployment activities.

Before you begin
Ensure that you have:

- The virtual IP address or MDM IP address of the existing system. If an MDM virtual IP address is not in use, obtain the IP addresses of all the MDM managers.
- Login credentials for the intended SDC host
- The required installation software package for your SDC’s operating system (available from the zipped software packages that can be downloaded from the Customer Support site)
- A GUID string for the SDC. These strings can be generated by tools that are freely available online. The GUID needs to conform to OSF DCE 1.1. The expected format is xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx where each x can be a digit (0–9) or a letter (a–f).

About this task
The following procedure explains how to manually install an external SDC on an ESXi server using esxcli in command line. Alternatively, you can install the external SDC using the vSphere VxFlex OS plug-in.

Note: This procedure requires two server reboots.

Procedure
1. On the ESXi on which you are installing the SDC, set the acceptance level:

   ```
esxcli --server=<SERVER_NAME> software acceptance set --level=PartnerSupported
   
   where <SERVER_NAME> is the ESXi on which you are installing the SDC.
   ```

2. Install the SDC:

   ```
esxcli software vib install -d "<SDC_PATH>"
   ```
where `<SDC_PATH>` is the absolute path to the SDC VIB.

3. Get permission to reboot the ESXi server, and perform a reboot to load the SDC driver on the server.

4. Set the IP address of the MDM:

   ```
esxcli system module parameters set -m scini -p
"IoctlIniGuidStr=<XXXXXX> IoctlMdmIPStr=<LIST_VIP_MDM_IPS>"
```

   where
   - `<LIST_VIP_MDM_IPS>` is a comma-separated list of the MDM IP addresses or the virtual IP address of the MDM
   - `<XXXXXX>` is the user-generated GUID string

5. Reboot the ESXi server again.

**Results**

The SDC is installed on the ESXi server and is connected to VxFlex OS.

**After you finish**

In newly deployed systems, perform the post-deployment tasks described in this guide. It is highly recommended to run the VxFlex OS system analysis tool to analyze the system immediately after deployment, before you provision volumes, and before using the system in production.

In existing systems, map volumes to the new SDCs that you added to the system.

## Install SDC on a Linux server and connect it to VxFlex OS

Install the SDC with the appropriate parameters to connect it to an existing VxFlex OS system. This procedure is relevant both for adding more SDCs to an existing system, and for adding SDCs to a 2-layer system when deploying a new system.

**Before you begin**

Ensure that you have:

- The virtual IP address or MDM IP address of the existing system. If an MDM virtual IP address is not in use, obtain the IP addresses of all the MDM managers.
- Login credentials for the intended SDC host
- The required installation software package for your SDC's operating system (available from the zipped software packages that can be downloaded from the Customer Support site)

**About this task**

The following procedure explains how to manually install an external SDC on a Linux server. On most servers (with the exception of hLinux), you can install the external SDC using the VxFlex OS Installer. For more information about adding components to an existing system, see the *Deploy VxFlex OS Guide*.

The steps in the procedure below are relevant for Linux RHEL/CentOS/oracle Linux operating systems. Deployment on other operating systems require the modifications described in the following table:

<table>
<thead>
<tr>
<th>OS</th>
<th>Modifications required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubuntu/hLinux/OL</td>
<td>Before installing VxFlex OS, ensure that you have followed the required preparation procedures relating to various types of Linux operating systems.</td>
</tr>
<tr>
<td>OS</td>
<td>Modifications required</td>
</tr>
<tr>
<td>----</td>
<td>------------------------</td>
</tr>
<tr>
<td></td>
<td>• VxFlex OS component packages are delivered as TAR files. Before installing, perform the following:</td>
</tr>
</tbody>
</table>
|    | 1. Untar all the packages: `tar -xvf <tar_file>`  
This yields SIOB files. |
|    | 2. Extract the DEB from the SIOB files: `siob_extract <siob_file>` |
|    | 3. The DEB file is in the following format: `EMC-ScaleIO-mdm-3.0-X.<build>.<operating_system>.X.X.x86_64.deb`  
You will use the extracted DEB files for the installation. |
|    | • Some commands are a bit different, noted where applicable. |
| CoreOS | Before installing VxFlex OS, ensure that you have followed the required preparation procedures relating to various types of Linux operating systems. |
|    | • VxFlex OS component CoreOS packages are delivered as TAR files. Before installing, perform the following: |
|    | 1. Untar all the packages: `tar -xvf <tar_file>`  
This yields SIOB files. |
|    | 2. Extract the BSX from the SIOB files: `siob_extract <siob_file>` |
|    | 3. The BSX file is in the following format: `EMC-ScaleIO-mdm-3.0-X.<build>.CoreOS.x86_64.bsx`  
You will use the extracted BSX files for the installation. |
|    | • Some commands are a bit different, noted where applicable. |

**Procedure**

1. Install the GPG key on every server on which SDC will be installed. From the VxFlex OS installation folder, run the following command on every server:

   ```sh
rpm --import RPM-GPG-KEY-ScaleIO
   ```

2. In command line, install the SDC:
   - RHEL/CentOS /Oracle Linux
     ```sh
     MDM_IP=<LIST_VIP_MDM_IPS> rpm -i <SDC_PATH>.rpm
     ```
   - CoreOS
     ```sh
     MDM_IP=<LIST_VIP_MDM_IPS> ./<LIST_VIP_MDM_IPS>.bsx
     ```

   where
   - `<LIST_VIP_MDM_IPS>` is a comma-separated list of the MDM IP addresses or the virtual IP address of the MDM
Install SDC on an AIX server and connect it to VxFlex OS

Install the SDC with the appropriate parameters to connect it to an existing VxFlex OS system. These instructions are relevant both for adding more SDCs to an existing system, and for adding SDCs to a 2-layer system when deploying a new system.

Before you begin

Ensure that you have:

- The virtual IP address or MDM IP address of the existing system. If an MDM virtual IP address is not in use, obtain the IP addresses of all the MDM managers.
- Login credentials for the intended SDC host
- The required installation software package for your SDC's operating system (available from the zipped software packages that can be downloaded from the Customer Support site)

About this task

The following procedure explains how to manually install an external SDC on an AIX server. The VxFlex OS Installer cannot be used.

Procedure

1. In command line, install the SDC:

   ```bash
   MDM_IP=<LIST_VIP_MDM_IPS> rpm -i <SDC_PATH>.rpm
   ```

   where

   - `<LIST_VIP_MDM_IPS>` is a comma-separated list of the MDM IP addresses or the virtual IP address of the MDM.
   - `<SDC_PATH>` is the path where the SDC installation package is located.

   The SDC package is in a format similar to this: EMC-ScaleIO-sdc-3.0-X.<build>.aix7.aix7.2.ppc.rpm

Results

The SDC is installed on the AIX server and is connected to VxFlex OS.

After you finish

In newly deployed systems, perform the recommended post-deployment tasks described in this guide. It is highly recommended to run the VxFlex OS system analysis tool to analyze the system immediately after deployment, before you provision volumes, and before using the system in production.

In existing systems, map volumes to the new SDCs that you added to the system.
Install SDC on a Windows server and connect it to VxFlex OS

Install the SDC with the appropriate parameters to connect it to an existing VxFlex OS system. This procedure is relevant both for adding more SDCs to an existing system, and for adding SDCs to a 2-layer system when deploying a new system.

**Before you begin**

Ensure that you have:

- The virtual IP address or MDM IP address of the existing system. If an MDM virtual IP address is not in use, obtain the IP addresses of all the MDM managers.
- Login credentials for the intended SDC host
- The required installation software package for your SDC's operating system (available from the zipped software packages that can be downloaded from the Customer Support site)

**About this task**

The following procedure explains how to manually install an external SDC on a Windows server. Alternatively, you can install the external SDC using the VxFlex OS Installer. For more information about adding system components to an existing system, see the Configure and Customize VxFlex OS Guide.

**Note:** This procedure requires a server reboot.

**Procedure**

1. On the Windows server on which you are installing the SDC, run the following command in command line:

```
msiexec /i <SDC_PATH>.msi MDM_IP=<LIST_VIP_MDM_IPS>
```

   where

   - `<SDC_PATH>` is the path where the SDC installation package is located
   - `<LIST_VIP_MDM_IPS>` is a comma-separated list of the MDM IP addresses or the virtual IP address of the MDM

2. Get permission to reboot the Windows server, and perform a reboot to load the SDC driver on the server.

**Results**

The SDC is installed on the Windows server and is connected to VxFlex OS.

**After you finish**

In newly deployed systems, perform the post-deployment tasks described in this guide. It is highly recommended to run the VxFlex OS system analysis tool to analyze the system immediately after deployment, before you provision volumes, and before using the system in production. In existing systems, map volumes to the new SDCs that you added to the system.

**SDC operations**

Many SDC operations use drv_cfg. The drv_cfg command line is a local CLI utility that affects only the client on which the SDC is running. Possible SDC operations include updating the SDC driver with IP changes, detecting new volumes, querying volumes, loading a configuration file, adding an MDM, modifying an MDM IP address, enabling support of PDL state, and more.
Update the SDC driver with IP address changes

Procedure

1. Edit `drv_cfg.txt` and change the IP address in the last line to the new IP address.
   
   **Location of `drv_cfg.txt`:**
   
   - **Linux:** `/etc/emc/scaleio/`
   - **Windows:** In the following registry key - `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\services\scini\Parameters\mdms`  

   **Note:**
   On ESXi, GUID and MDM lists are stored as module parameters, and not in a `drv_cfg.txt` file. To modify these parameters, use `esxcli` commands.

2. Save and close the file.
3. Type the following command:

   ```bash
   /etc/init.d/scini restart
   ```

   **Note:** ESXi guidelines described in the VxFlex OS plug-in chapter.

Detecting new volumes

Command

```
drv_cfg --rescan
```

**Note:**
This is not a CLI command, but rather an executable that is run on the SDC server.

Syntax

```
/opt/emc/scaleio/sdc/bin/drv_cfg --rescan
```

Description/Notes

Volumes are always exposed to the operating system as devices with the prefix `scini` (such as `/dev/scinia`, `/dev/scinib` and so on). Unique names can be found under `/dev/disk/by-id/`.

VxFlex OS periodically scans the system to detect new volumes. You can initiate a scan for the most up-to-date status on a particular SDC node. This command is unique because it is not a CLI command, but rather a command issued on the specific SDC.

**Location of `drv_cfg` command:**

- **Linux:** `/opt/emc/scaleio/sdc/bin/drv_cfg`
- **Windows:** `C:\Program Files\emc\scaleio\sdc\bin\drv_cfg`
- **ESXi:** refer to the vSphere Client VMWare guidelines on how to detect new storage. If troubleshooting is needed, contact customer support.
For further details on how to set the mounting options see "Mount VxFlex OS".

**Query volumes using `drv_cfg`**

**Command**

```
drv_cfg --query_vols
```

**Note:**
This is not a CLI command, but rather an executable that is run on the SDC server.

**Syntax**

```
/opt/emc/scaleio/sdc/bin/drv_cfg --query_vols
```

**Description/Notes**

This utility retrieves information about all known active volume objects in kernel mode. You can use this utility to determine which volumes are mapped, and the ID of each volume in VxFlex OS.

**Location of `drv_cfg` command:**

- **Linux:** /opt/emc/scaleio/sdc/bin/drv_cfg
- **Windows:** C:\Program Files\emc\scaleio\sdc\bin\drv_cfg
- **ESXi:** Refer to "Update the SDC parameters in VMware based HCI or Compute node".

**Example**

```
/opt/emc/scaleio/sdc/bin/drv_cfg --query_vols
```

**Query tgt objects using `drv_cfg`**

**Command**

```
drv_cfg --query_tgts
```

**Note:**
This is not a CLI command, but rather an executable that is run on the SDC server.

**Syntax**

```
/opt/emc/scaleio/sdc/bin/drv_cfg --query_tgts
```

**Description/Notes**

This utility retrieves information about all known active tgt objects (SDSs) in kernel mode.

**Location of `drv_cfg` command:**

- **Linux:** /opt/emc/scaleio/sdc/bin/drv_cfg
- **Windows:** C:\Program Files\emc\scaleio\sdc\bin\drv_cfg
- **ESXi:** Refer to "Update the SDC parameters in VMware based HCI or Compute node".
Example

```
/opt/emc(scaleio/sdc/bin/drv_cfg --query_tgts
```

Query GUID using `drv_cfg`

**Command**

```
drv_cfg --query_guid
```

**Note:**
This is not a CLI command, but rather an executable that is run on the SDC server.

**Syntax**

```
/opt/emc(scaleio/sdc/bin/drv_cfg --query_guid
```

**Description/Notes**

This utility retrieves the unique ID of the kernel module. The utility can be used to verify that all SDC GUIDs in the system are unique.

**Location of `drv_cfg` command:**

- **Linux:** /opt/emc(scaleio/sdc/bin/drv_cfg
- **Windows:** C:\Program Files\emc\scaleio\sdc\bin\drv_cfg
- **ESXi:** Refer to "Update the SDC parameters in VMware based HCI or Compute node".

**Note:**
If the SDC was removed and reinstalled, the GUID of the SDC will be different to its original GUID. In such a case, you may need to remove the SDC, if two SDCs now have the same GUID.

Example

```
/opt/emc(scaleio/sdc/bin/drv_cfg --query_guid
```

Query MDMs using `drv_cfg`

**Command**

```
drv_cfg --query_mdms
```

**Note:**
This is not a CLI command, but rather an executable that is run on the SDC server.

**Syntax**

```
/opt/emc(scaleio/sdc/bin/drv_cfg --query_mdms
```
Description/Notes

This utility retrieves information about all known MDM objects in kernel mode. This utility is typically used to determine to which MDM an SDC is connected.

Location of `drv_cfg` command:

- **Linux:** `/opt/emc/scaleio/sdc/bin/drv_cfg`
- **Windows:** `C:\Program Files\emc\scaleio\sdc\bin\drv_cfg`
- **ESXi:** Refer to "Update the SDC parameters in VMware based HCI or Compute node".

Example

```
/opt/emc/scaleio/sdc/bin/drv_cfg --query_mdms
```

Loading a configuration file using `drv_cfg`

Command

```
drv_cfg --load_cfg_file
```

**Note:**

This is not a CLI command, but rather an executable that is run on the SDC server.

This command can not be used on ESXi servers. Instead, follow the steps described in "Modify parameters on ESXi servers".

Syntax

```
/opt/emc/scaleio/sdc/bin/drv_cfg
--load_cfg_file <FILE_NAME>
```

Description/Notes

This utility reads a configuration file containing MDM IP addresses, and calls the kernel to connect to them.

Location of `drv_cfg` command:

- **Linux:** `/opt/emc/scaleio/sdc/bin/drv_cfg`
- **Windows:** `C:\Program Files\emc\scaleio\sdc\bin\drv_cfg`
- **ESXi:** Refer to "Update the SDC parameters in VMware based HCI or Compute node".

The configuration file that is loaded when using the `drv_cfg --load_cfg_file` utility is not persistent; when you restart the SDC, the changes will be lost.

To make the changes persistent, perform either of the following:

- Install the SDC on every server that will expose VxFlex OS volumes to the application running, by executing the following command:

```
MDM_IP=<IP of the MDM> rpm -i <full rpm file path>
```
- Use the following `drv_cfg` command:

```
/opt/emi/scaleio/sdc/bin/drv_cfg --mod_mdm_ip --ip <EXISTING_MDM_IP_ADDRESS> --new_mdm_ip <NEW_MDM_IP_ADDRESSES>
```

Example

```
/opt/emi/scaleio/sdc/bin/drv_cfg --load_cfg_file /etc/emi/scaleio/drv_cfg.txt
```

### Adding an MDM using `drv_cfg`

**Command**

```
drv_cfg --add_mdm
```

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is not a CLI command, but rather an executable that is run on the SDC server.</td>
</tr>
<tr>
<td>This command can not be used on ESX servers. Instead, follow the steps described in &quot;Modifying parameters on ESXi servers&quot; in the VxFlex Ready NodeAMS User Guide.</td>
</tr>
</tbody>
</table>

**Syntax**

```
/opt/emi/scaleio/sdc/bin/drv_cfg --add_mdm --ip <MDM_IP_ADDRESS_LIST>
```

**Description/Notes**

This utility calls the kernel module to connect to an MDM. This command is typically used in cases where an SDC is connected to more than one VxFlex OS system.

**Location of `drv_cfg` command:**

- **Linux:** `/opt/emi/scaleio/sdc/bin/drv_cfg`
- **Windows:** `C:\Program Files\emi\scaleio\sdc\bin\drv_cfg`
- **ESXi:** Refer to "Update the SDC parameters in VMware based HCI or Compute node".

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extending your VxFlex OS system with another MDM requires that you update all SDCs in your system with the new MDM IP address. Run the <code>drv_cfg</code> utility with the <code>--mod_mdm_ip</code> option (see &quot;Modifying an MDM IP address using <code>drv_cfg&quot;), and to make the change persistent, use the </code>--file` parameter. In addition, any additional objects or systems which interface with the MDM must also be updated. For more information, see &quot;Modifying an MDM's management IP address&quot; in the VxFlex OS CLI Reference Guide.</td>
</tr>
</tbody>
</table>

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--ip &lt;MDM_IP_ADDRESS_LIST&gt;</code></td>
<td>List of IP addresses (comma delimited) for this Master or Slave MDM</td>
</tr>
<tr>
<td>Optional:</td>
<td></td>
</tr>
</tbody>
</table>

---

Configure and Customize Dell EMC VxFlex OS 97
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--file &lt;CONFIG_FILE_NAME&gt;</td>
<td>Name of the configuration file to which the MDM information should be written</td>
</tr>
<tr>
<td>--only_cfg</td>
<td>Do not call the kernel to actually connect</td>
</tr>
</tbody>
</table>

### Example

```
/opt/emi/scaleio/sdc/bin/drv_cfg --add_mdm
--ip 10.100.22.20,10.100.22.30
--file /etc/emi/scaleio/drv_cfg.txt
```

### Modifying an MDM IP address using drv_cfg

**Command**

```
drv_cfg --mod_mdm_ip
```

**Note:**

This is not a CLI command, but rather an executable that is run on the SDC server. This command can not be used on ESX servers. Instead, follow the steps described in "Modify parameters in ESXi servers".

**Syntax**

```
/opt/emi/scaleio/sdc/bin/drv_cfg --mod_mdm_ip
--ip <EXISTING_MDM_IP_ADDRESS>
--new_mdm_ip <NEW_MDM_IP_ADDRESSES> [--file <CONFIG_FILE_NAME>] [-n|--only_cfg]
```

**Description/Notes**

This utility calls the kernel to modify an MDM’s IP address list. It is typically used in cases when an MDM IP address has changed, or when MDMs are added/removed from/to the system. The command must be run on every SDC in the system. To bring the changes into effect, a server restart is required.

**Location of drv_cfg command:**

- **Linux:** `/opt/emi/scaleio/sdc/bin/drv_cfg`
- **Windows:** `C:\Program Files\emi\scaleio\sdc\bin\drv_cfg`
- **ESXi:** Refer to “Update the SDC parameters in VMware based HCI or Compute node”.

**Note:**

Extending your VxFlex OS system with another MDM requires that you update all SDCs in your system with the new MDM IP address.

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--ip &lt;EXISTING_MDM_IP_ADDRESS&gt;</td>
<td>One of the existing MDM IP addresses</td>
</tr>
</tbody>
</table>
### Permanent Device Loss state

When the MDM has disconnected from the SDC and a volume mapped to this SDC has experienced an I/O error, the ESXi host continuously sends I/Os to the device to determine if the device has become accessible. This can subsequently cause a high I/O-error load that can lead to the host freezing. In cases where the device is disconnected long-term, such as when the entire MDM cluster is down during a network upgrade, the SDC can change the volume state to Permanent Device Loss (PDL) to prevent more I/O errors coming from the ESXi.

PDL is an ESXi state, which, once enabled, is supported in VxFlex OS. Once the ESXi host loses connectivity with a device, if a timeout value is reached, the ESXi will be notified that the device is in a PDL state. The timeout value can be manually set. Once a device is in a PDL state, the ESXi host no longer attempts to re-establish connectivity or issue commands to the device.

Recovering a device from PDL state is described in the VMware documentation for your operating system version. The following link is for ESXi v6.5: [https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.storage.doc/GUID-A513D44C-71DE-47ED-B781-327F78659404.html](https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.storage.doc/GUID-A513D44C-71DE-47ED-B781-327F78659404.html)

Use the instructions that match your environment.

### Enabling support of PDL state on the ESXi

Enable support of Permanent Device Loss (PDL) state on the ESXi host.

**Procedure**

1. On the ESXi host:

   ```
   esxcli system module parameters set -m scini "<<PREVIOUS_MODULE_PARAMS>> bBlkDevIsPdlactive=1 blkDevPdlTimoutMillis=<TIMEOUT_VALUE>"
   ```

   where:

   - `<<PREVIOUS_MODULE_PARAMS>>` is any previous module parameters being used for this ESXi host.
   - `<TIMEOUT_VALUE>` is the timeout time in milliseconds. Its value can be 1000-3600000 (default is 60000) and including it in the command is optional.
2. Reboot the host.

Disabling support of PDL state on the ESXi

Disable support of Permanent Device Loss (PDL) state on the ESXi host.

Procedure
1. On the ESXi host:

   ```bash
   esxcli system module parameters set -m scini "<<PREVIOUS_MODULE_PARAMS>> bBlkDevIsPdlActive=0"
   ```

   where `<<PREVIOUS_MODULE_PARAMS>>` is any previous module parameters being used for this ESXi host.

2. Reboot the host.

Update the SDC parameters in VMware based HCI or compute node

Update the SDC parameters to maintain SDC-MDM communication.

About this task

This procedure describes how to use the VMware plug-in to update the SDCs that are needed to maintain SDC-MDM communication.

Procedure
1. From the plug-in Advanced tasks menu, click Update SDC parameters, and follow instructions to complete the process.

2. Check that the SDC parameters were updated by running this command on each ESXi:

   ```bash
   cat /etc/vmware/esx.conf |grep scini|grep -i mdm
   ```

Run the SDC driver on SLES12.2 with multipath enabled

Run the SDC driver on SLES12.2 with multipath enabled

Procedure
1. On the SLES machine where the SDC is running, open `/etc/udev/rules.d/20-scini.rules` for editing

2. In the first line at the end add:

   ```bash
   ENV{ID_WWN}="%c"
   ```

The line should read like this:

```bash
KERNEL="scini*[^0-9]", SUBSYSTEM="block", PROGRAM="/bin/emi/scaleio/drv_cfg --query_block_device_id --block_device $tempnode", SYMLINK +="disk/by-id/emc-vol-%c", ENV{ID_BUS}="scsi", ENV{ID_SERIAL}="%c", ENV{ID_WWN}="%c"
```
3. Open `/etc/multipath.conf` and add the following:

```plaintext
defaults {
    retain_attached_hw_handler "no"
}
```

This option is turned off by default on RHEL 7.x

4. From the command line, run `dracut -f`.
   This includes the changes in initrd.

5. Restart the system.
You can configure and monitor the storage and devices in the VxFlex OS system.

- Configuring storage .................................................................................................................. 104
- Enter and exit SDS Maintenance Mode .................................................................................. 119
- Configuring I/O priorities and bandwidth use (advanced) .................................................... 120
- Configuring acceleration .......................................................................................................... 121
- RFcache (xcache) package installation ................................................................................... 141
- Increase SVM memory to accommodate additional SDS device ........................................... 142
- Modify an SDS port during I/O ............................................................................................. 142
Configuring storage
Add and remove storage devices, and configure storage features.

Configuring capacity
Add, remove, and configure capacity.
The following topics explain how to add, remove, activate, and inactivate capacity, activate devices, clear device errors, and set device capacity limits.
The Dashboard Capacity tile, some Backend table views (such as Capacity Usage, Configuration), and Property Sheets help you to better understand the amount of raw capacity and net free capacity currently available in the system.

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

About this task

Add a Protection Domain
Add a Protection Domain to a VxFlex OS system.

Before you begin

About this task

Procedure
1. In one of the Backend views, right-click the System row and select Add Protection Domain.
The Add Protection Domain window is displayed.
2. Type a name in the Name box, and click OK.
   When the operation is complete, the Protection Domain is active. You can now add SDSs, Fault Sets, Storage Pools, and Acceleration Pools to the Protection Domain. Before you add storage devices, ensure that at least one suitable Storage Pool is defined in the Protection Domain.

Activate a Protection Domain
Activate an inactive Protection Domain.

Procedure
1. In the Backend > Storage view, use the drop-down list at the top right side of the window to ensure that the table is displaying rows according to By SDSs.
2. Select one or more Protection Domains.
3. Right-click the Protection Domains and select Activate.
The Activate Protection Domain window is displayed.
4. Click OK.
Inactivate a Protection Domain

Inactivate a Protection Domain.

About this task

† Note: If you inactivate a Protection Domain, the data remains on the SDSs, and therefore, it is preferable to remove a Protection Domain if you no longer need it.

When the inactivation feature is in effect, the following activities can take place, behind the scenes:

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

Procedure

1. In the Backend > Storage view, use the drop-down list at the top right side of the window to ensure that the table is displaying rows according to By SDSs.
2. Right-click the Protection Domain and select Inactivate.
   The Inactivate Protection Domain window is displayed.
3. If you want to force deactivation, select the Force check box.
   Use the Force option with caution.
4. Click OK.
   If a confirmation window appears, confirm the operation, and type your password if requested to do so.

Remove a Protection Domain

Remove a Protection Domain from a VxFlex OS system.

Before you begin

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

Procedure

1. In the Backend > Storage view, use the drop-down list at the top right side of the window to ensure that the table is displaying rows according to By SDSs.
2. Verify that you have removed all child nodes from the Protection Domain.
3. Right-click the Protection Domain and select Remove.
4. Click OK.
5. If a confirmation window appears, confirm the operation, and type your password if requested to do so.
Setting number of concurrent I/O

Set the number of concurrent I/O per protection domain that has a fine granularity layout.

1. From Backend > Storage, right-click on the relevant protection domain.
2. Select Settings > Fine Granularity Layout > Set Number of Concurrent I/O
   The Set Protection Domain Number of Concurrent I/O dialog box is displayed.
3. Enter a valid range between 64-1000 in the Number of concurrent I/O box.
4. Click OK.
5. In the Are you sure? dialog box, click OK.

Add SDSs

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

Before you begin

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

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

About this task

Device data is erased when devices are added to an SDS. When adding a device to an SDS, VxFlex OS will check that the device is clear before adding it. An error will be returned, per device, if it is found not to be clear. A device that has been used in the past can be added to the SDS by using the Force Device Takeover option. When this option is used, any data that was previously saved on the device will be lost. For more information, see "Configuring direct attached storage" in the Getting to Know VxFlex OS Guide.

Fields that contain orange explanation marks are mandatory.

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

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

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

Note: Acceleration settings can be configured later, using the Backend > Devices By Pools view.

Note: You cannot enable zero padding after adding the devices. For more information, see "Storage Pools" in the Getting to Know VxFlex OS Guide.

Procedure

1. In one of the Backend views, navigate to the desired Protection Domain, and select it.
2. From the Command menu or context-sensitive menu, choose the Add option, then Add SDS.
The **Add SDS to Protection Domain** dialog box is displayed.

3. Optionally, type a name for the SDS in the **Name** box.

4. In the **IP addresses** table, enter IP addresses, and select the corresponding communication roles in the relevant check boxes. Click the plus icon to add more rows to the table.

5. Use the **New Devices** table to add storage devices. Click the plus icon to add rows to the table. You must add at least one storage device to the new SDS at this stage. Add a new row for each device, and enter the required parameters in each row. You can add more devices later.

   **Note:** If you want to add an SDS without any devices, you can do so using the CLI. To run CLI commands, you must be logged in. Actual command syntax is operating-system dependent. For more information, see the *VxFlex OS CLI Reference Guide*.

6. Optionally, add acceleration devices to the SDS, using the **Acceleration Devices** table. Click the plus icon to add rows to the table. Add a new row for each device, and enter the required parameters in each row.

7. The **Advanced** option provides additional items, such as device testing, forced device takeover, and Read RAM Cache acceleration options. Optionally, click its **Expand** button to display and configure them (recommended for advanced users only).

8. Click **OK**.

   The progress of the operation is displayed at the bottom of the dialog box. It is recommended to keep it open until the operation is completed, and until you can see the result of the operation.

9. Click **Close**.

   If you chose the **Test only** advanced option, activate the devices as described in "Activate devices".
Add storage devices

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

Before you begin

Ensure that at least one suitable Storage Pool is defined in the required Protection Domain. All devices in a Storage Pool must be the same media type. Ensure that you know the type of devices that you are adding to the system, and that the Storage Pool to which you are adding devices is configured to receive that media type.
About this task
Device data is erased when devices are added to an SDS. When adding a device to an SDS, VxFlex OS will check that the device is clear before adding it. An error will be returned, per device, if it is found not to be clear. A device that has been used in the past can be added to the SDS by using the Force Device Takeover option. When this option is used, any data that was previously saved on the device will be lost. For more information, see "Configuring direct attached storage" in the *Getting to Know VxFlex OS Guide*.

Fields that contain orange explanation marks are mandatory.

You can assign a name to devices. This can be particularly helpful for identifying SDS devices in the future, because the name will remain constant, even if the path changes. Device names must meet the following requirements:

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

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

Procedure

1. In one of the *Backend* views, navigate to the desired SDS, and select it.
2. From the Command menu or context-sensitive menu, choose the Add Device option.
   
The Add device to SDS dialog box is displayed.
3. In the New Devices table, add storage devices. Click to add more rows to the table, and enter the required parameters in each row.
4. The Advanced option provides additional items, such as device testing and forced device takeover. Optionally, click its Expand button to display and configure them (recommended for advanced users only).
5. Click OK.
   
The progress of the operation is displayed at the bottom of the dialog box. It is recommended to keep it open until the operation is completed, and until you can see the result of the operation.
6. Click Close.
   
   If you chose the Test only option, activate the devices as described in "Activate devices".
Activate devices
Activate a device that was inactivated, or that was added to a system using the Test only option.

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

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

Procedure
1. In one of the Backend views, navigate to the device or devices in the table, and select the corresponding rows.
2. Right-click and select Activate.

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

About this task
If you plan to replace a device with a device containing less storage capacity, you can configure the device to a smaller capacity than its actual capacity, in preparation for replacement. This will reduce rebuild and rebalance operations in the system later on. For more information, see Setting device capacity limits on page 113.

The system has job queues for operations that take a long time to execute. You can view the jobs in the Planned Rebuilds and Planned Rebalancing table views. Operations that are waiting in the
job queue are shown as Pending. If a job in the queue will take a long time, and you do not want to wait, you can cancel the operation using the **Abort** button in the **Remove** command window (if you left it open), or using the **Abort** command from the **Command menu**.

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

**Procedure**

1. In the **Backend > Storage** view, navigate to the desired object in the table, and select its row.
2. Right-click the row and select the desired **Remove** command.
   
   In the confirmation window, click **OK**. The progress of the operation is displayed at the bottom of the window. It is recommended to keep the window open until the operation is completed, and until you can see the result of the operation. For some objects, an **Abort** button is available in the window, which can be used if you decide to abort the operation. There is also an **Abort** command accessible from the **Command menu**.
3. Click **Close**.

**Add Storage Pools**

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

**Before you begin**

- Before adding a Storage Pool, familiarize yourself with the types of Storage Pool that are available, and ensure that you know the media type of the devices that will be used in the Storage Pool. Each Storage Pool must contain devices of only one media type. For more information, see the Getting to Know VxFlex OS Guide.
- For Storage Pools with Fine Granularity data layout, at least one NVDIMM configured as a DAX device is required. In addition, ensure that you have already configured an NVDIMM Acceleration Pool.

**About this task**

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

**Note:** You cannot enable zero padding to Medium Granularity Storage Pools after adding the devices. For more information, see “Storage Pools” in the *Getting to Know VxFlex OS Guide*.

**Procedure**

1. In the **Backend > Storage** view, select the required Protection Domain.
2. Right-click the Protection Domain, choose **Add**, then **Add Storage Pool**.
   
   The **Add Storage Pool** dialog box is displayed.
3. Type a name in the **Name** field.
4. Select a media type: **HDD** or **SSD**.
   
   All the devices that you add to this Storage Pool must be the same type of device.
5. If you selected SSD, choose a **Data Layout** type:
   
   - **Medium Granularity**
     
     a. Optionally, select **Use Read RAM Cache** to use Read RAM Cache for caching.
Note: The Read RAM Cache features are advanced features, and it is usually recommended to accept the default values. You can configure these features later, if necessary, using the Configure Read RAM Cache command. For more information about Read RAM Cache features, see "Managing RAM read cache".

b. Select the required **Write Handling Mode**: Cached or Passthrough.

- **Fine Granularity**
  a. Select the relevant option from the **Acceleration Pool** list.
  b. Select the **Enable Compression** check box, to enable compression.

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

7. Click **OK**.

**Compression Mode for Fine Granularity Storage Pools**

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

**Set Default Compression Mode**

You can set the Default Compression Mode of Fine Granularity Storage Pools

**Procedure**

1. From **Backend > Storage**, drill down to the relevant Protection Domain or Storage Pool
2. Right-click on the Storage Pool and select **Settings > Fine Granularity Layout > Set Default Compression Mode**.
   The **Set Storage Pool Default Compression Mode** dialog box is displayed.
3. Select the **Enable Compression** check-box.
4. Click **OK**.
5. In the **Are you sure?** dialog box, click **OK**.
6. Click **Close**.

**Results**

Compression Mode is now enabled for the Fine Granularity Storage Pool.

**Enable and disable Rebuild/Rebalance (advanced)**

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

**About this task**

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

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

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

**Procedure**

1. In the **Backend > Storage** view, navigate to, and select the desired Storage Pools.
2. Right-click the Storage Pool and select **Enable/Disable Rebuild/Rebalance**. The **Enable or Disable Rebuild and Rebalance** window is displayed.
3. Select or clear the options that you require (selected=enable; clear=disable), and click **OK**.

**Clear device errors**

**Clear device errors.**

**About this task**

**Procedure**

1. In one of the **Backend** views, navigate to the device in the table, and select its row.
2. Right-click the row and select **Clear Device Errors**.

**Setting device capacity limits**

In circumstances when you need to replace a storage device in your system with a storage device of a smaller capacity, you should first set the capacity limit of the device to be removed to less than its full capacity.

**About this task**

In such a case, capacity will be decreased, but the size of the disk remains unchanged. The capacity assigned to the storage device must be smaller than its actual physical size.

**Note:** Decreased capacity is shown on the **Dashboard**, using pale gray, on the outer ring on the Capacity tile.

**Procedure**

1. In one of the **Backend** views, navigate to the device in the table, and select its row.
2. Right-click the row and select **Settings**, then **Set Device Capacity Limit**.
3. Type the desired value and click **OK**.

**Configure Read RAM Cache (advanced, Backend)**

The Read RAM Cache feature improves your system's application performance for storage-related activities. By default, caching is disabled.

**About this task**

To use Read RAM Cache, you need to configure settings at two levels:

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

1. **Note:** By default, Read RAM Cache is disabled in all volumes. You can enable them from the **Frontend > Volumes** view.

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

To configure caching, perform these steps:

**Procedure**

1. In the **Backend > Storage** view, navigate to, and select the desired Storage Pools.

2. Right-click the selected Storage Pools, select **Configure Caching** and then **Configure Read RAM Cache**.

   The **Configure Read RAM Cache** dialog box appears. The right pane of the lists the Storage Pools that you are configuring.

3. Select or clear the **Read RAM Cache Enabled** check box (selected=used; clear=not used).

4. Click **OK**.

   Read RAM Cache at Storage Pool level is done. To configure the feature at SDS level, go to the next step.

5. To enable, disable, or configure cache size for SDSs, in the **Backend > Storage** view, navigate to, and select the desired SDS(s).

6. Right-click the SDS and select **Configure Caching** and then **Configure Read RAM Cache**.

   The **Configure Read RAM Cache** window appears. The right pane of the window lists the SDSs that you are configuring.

7. Select or clear the **Read RAM Cache Enabled** checkbox (selected=enable; clear=disable).

8. If necessary, edit the value in the **Read RAM Cache Size** box (default=128 MB).

9. Click **OK**.

**Configure inflight checksum protection**

Inflight checksum protection mode can be used to validate data reads and writes in Storage Pools, in order to protect data from data corruption.

**About this task**

To modify this setting, perform the following steps:

**Procedure**

1. In any of the **Backend** views, navigate to, and right click the desired Storage Pool.

2. From the context-sensitive menu, select **Configure Inflight Checksum**.

   The **Configure Inflight Checksum** window is displayed.

3. Do one of the following:

   a. To enable the Checksum feature, select the **Enable Inflight Checksum** check box.

   b. To disable the Checksum feature, clear the **Enable Inflight Checksum** check box.

4. Click **OK**.
Using the background device scanner

The background device scanner scans devices in the system to check for errors.
You can enable and disable the background device scanner, as well as reset the background device scanner counters. Information about errors will be provided in event reports. For more information about viewing events, see "Viewing events" in the Monitoring VxFlex OS Guide.

Enable and disable the background device scanner

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

About this task

There are two modes: **device only** mode, and **data comparison** mode:

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

To enable or disable the background device scanner, follow these steps:

Procedure

1. In the **Backend > Storage** view, navigate to, and select the desired Storage Pools.
2. From the **Command menu** or context-sensitive menu, select **Set Background Device Scanner Mode**.
   
   The **Configure Storage Pool Background Device Scanner** window is displayed. The right pane of the window displays the Storage Pools that you are configuring.
3. For the **Enable Background Device Scanner** option, perform one of the following:
   - To enable the scanner, select the check box, and proceed to the next step.
   - To disable the scanner, clear the check box, and click **OK** to finish.
4. Select an option (selected=enable; clear=disable):
   - **Device only**
   - **Data comparison**
5. In the **Bandwidth Limit** box, accept the default or type a number in KB per second (per device).
   
   The given value should be in the range 10 KB-10 MB (default = 1 MB).
   
   *Note*: High bandwidth should be used very carefully for extreme cases only (such as an urgent need to check some devices), as it may create negative impact on system performance. Setting the background device scanner bandwidth should take into account maximum bandwidth of the devices.
6. Click **OK**.

Reset the background device scanner counters

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

About this task

To reset counters, follow these steps:
Procedure
1. In the **Backend > Storage** view, navigate to, and select the desired Storage Pools.
2. Right-click the Storage Pools and select **Reset Background Device Scanner Counters**.
   The **Reset Background Device Scanner Counters** window is displayed. The right pane of the window shows the Storage Pools that you are configuring.
3. Select or clear the option that you require, or both options (selected=enable; clear=disable).
4. Click **OK**.

Configuring Oscillating Failure counters
Oscillating failure handling provides the ability to handle error situations, and to reduce their impact on normal system operation.

This feature detects and reports various oscillating failures, in cases when components fail repeatedly and cause unnecessary failovers. You can configure the time interval associated with each window type, and the number of failures allowed before reporting commences for each window type, per counter.

You can reset specified oscillating failure counters to zero. This can be useful when you have fixed a problem and want to ensure that an alert is no longer active in the system.

### Configure Oscillating Failure counter parameters
Configure Oscillating Failure counter parameters for the entire system, or for specific Protection Domains or Storage Pools.

### About this task

### Procedure

1. Perform one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To configure counter parameters for all SDCs, Protection Domains or Storage Pools in the system:</td>
<td>In the <strong>Backend &gt; Storage</strong> view, select the <strong>System</strong> icon.</td>
</tr>
<tr>
<td>To configure counter parameters for a specific Protection Domain or Storage Pool:</td>
<td>In the <strong>Backend &gt; Storage</strong> view, navigate to, and select the desired Protection Domain or Storage Pool.</td>
</tr>
</tbody>
</table>

2. From the **Command menu** or context-sensitive menu, select **Set Oscillating Failure Properties**.
3. Perform one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>For system level:</td>
<td>In the <strong>For All</strong> box, select an option: SDCs, Protection Domains, or Storage Pools.</td>
</tr>
<tr>
<td>For a Protection Domain or a Storage Pool:</td>
<td>Go to the next step.</td>
</tr>
</tbody>
</table>

4. In the **Counter Type** box, select a counter. Options vary, depending on the item selected in the previous step.
5. In the **Window Type** box, select an option for the sliding window interval: **Short**, **Medium** or **Long**.
6. Perform one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you want to remove the selected counter definition from the system:</td>
<td>Select the Remove the counter check box.</td>
</tr>
<tr>
<td>If you want to modify the threshold for the selected counter definition:</td>
<td>Enter a number in the fields for:</td>
</tr>
<tr>
<td></td>
<td>• failures (the maximum number of failures per time interval before reporting begins)</td>
</tr>
<tr>
<td></td>
<td>• seconds (the number of seconds per time interval)</td>
</tr>
</tbody>
</table>

7. Click OK.

The currently configured counter parameters are displayed in the corresponding Property Sheet, in the Oscillating Failure Parameters section.

**Reset Oscillating Failure counters**

You can reset specified oscillating failure counters to zero. This can be useful when you have fixed a problem and want to ensure that an alert is no longer active in the system. You can reset counters for the entire system, per Protection Domain, or per Storage Pool.

**About this task**

- To reset oscillating failure counters for all SDCs, Protection Domains or Storage Pools in the system, go to step 1.
- To reset counters for a specific Protection Domain or Storage Pool, in the Backend > Storage view, navigate to and select the relevant Protection Domain or Storage Pool.

**Procedure**

1. In the Backend > Storage view, select the System icon.
2. Right-click and select Reset Oscillating Failure Counters.
3. In the For All box, select an option.
   - If you want to reset counters for all object types, select Objects.
4. Perform one of the following:
   - For a specific counter, in the Counter Type box, select the required counter.
   - For all counters, in the Counter Type box, select None, and select the Reset All Counters check box.
5. Click OK.

To reset counters for a specific Protection Domain or Storage Pool, perform the following steps:

6. In the Backend > Storage view, navigate to, and select the desired Protection Domain or Storage Pool.
7. Right-click and select Reset Oscillating Failure Counters.
8. Perform one of the following:
   - For a specific counter, in the Counter Type box, select the required counter.
   - For all counters, select the Reset All Counters check box.
9. Click OK.
**View Oscillating Failure counters**

View Oscillating Failure counters for network related issues, for SDCs, for SDSs and for devices.

**About this task**

You can view Oscillating Failure counters for network related issues, for SDCs, for SDSs and for devices in the following ways:

- **Network:**
  1. In the **Backend > Storage** view, select the **System** icon.
  2. From the **Command menu** or context-sensitive menu, select **Download Network Failure Counters**.
  3. Browse to the location in which the file will be saved, and click **OK**. A JSON file containing the counters is saved in the location that you specified.
     - In Windows, view the file in a text editor, such as Notepad++.
     - In Linux, use the `more` command to view the file (for example, `more Oscillating_Network_Failures_Counters_2016-01-28-13-31-57.json`)

- **SDCs:**
  1. In the **Frontend > SDCs** view, select the required SDC.
  2. Open the Property Sheet, and click the **Oscillating Failure Counters** section.
     
     **Note:** When there are no oscillating failures counters for SDC, the **Oscillating Failures Counters** section displays **None Found**.

- **SDSs and devices:**

**Procedure**

1. In the **Backend > Storage** view, navigate to and select the required SDS or device.
2. Open the Property Sheet, and click the **Oscillating Failure Counters** section.
   
   a. If there is an active alert, you can view the oscillating failures alert in the **Alerts** section of the Property Sheet.

   **Note:** When there are no oscillating failures counters for SDS or device, the **Oscillating Failures Counters** section displays **None Found**.

---

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

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

**Before you begin**

- Verify that the VASA storage provider is registered and active

**Procedure**

1. In the vSphere Client, open the **Create VM Storage Policy** wizard.
   
   a. Click **Menu > Policies and Profiles**.
   
   b. Under **Policies and Profiles**, click **VM Storage Policies**.
   
   c. Click **Create VM Storage Policy**.

2. In the **Name and description** page, enter the vCenter server, policy name, and description, and click **Next**.
3. In the **Policy structure** page, under **Datastore specific rules**, select Enable rules for VxFlex OS VVols storage.

4. In the **VxFlex OS VVols rules** page, define storage placement rules for the target VVols datastore.

   In the **Placement** tab, from the **Tier** drop-down menu, select the appropriate storage policy.

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

5. In the **Storage compatibility** page, review the list of Storage Pools that match the policy you selected in the previous page.

6. In the **Review and finish** page, review the storage policy settings and click **Finish**.

**Results**

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

---

**Enter and exit SDS Maintenance Mode**

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

**About this task**

This topic explains how to put an SDS into Maintenance Mode, in order to perform non-disruptive maintenance on the SDS, and how to cancel Maintenance Mode when you are finished. Maintenance Mode lets you restart a server that hosts an SDS, without initiating data migration or exposing the system to the danger of having only a single copy of data. The system displays the SDSs that are in Maintenance Mode at any given time (but does not provide the total number of SDSs).

While SDSs are in Maintenance Mode, you should avoid both unnecessary rebuilds and operations that require taking an SDS offline temporarily. It is recommended to use Maintenance Mode when there is relatively low system activity, as the time it takes for an SDS to exit Maintenance Mode depends on the amount of data that needs to be synchronized back into the server. This might impact performance.

Maintenance Mode is targeted for short maintenance windows. If a long window is required, we recommend that you drain the node and then deal with the maintenance.

**Note:** Functional operations, such as configuration, cannot be performed on an SDS while it is in Maintenance Mode. If an active full copy is lost, its data will be unavailable until the SDS is brought back into the system, but that data will not be lost; it will be rebuilt using the temporary copy.

**Procedure**

1. To put an SDS into Maintenance Mode, perform these steps:
   a. In the **Backend > Storage** view, navigate to, and select the desired SDS.
   b. From the **Command menu** or context-sensitive menu, select **Enter Maintenance Mode**.

   The **Enter Maintenance Mode** window is displayed.
c. If you want to force entry into Maintenance Mode even though there is insufficient space or degraded/failed capacity, select the corresponding check box:
   - **Force Insufficient Space**—allow entry into maintenance mode, even without enough available capacity
   - **Force Degraded or Failed**—allow entry into maintenance mode, even with degraded or failed data

d. Click OK.

The status area at the bottom of the window indicates when the operation is complete. Once the SDS is in Maintenance Mode, this will be indicated both on the Dashboard, and in Backend tables and Property Sheets, using the symbol, and the Maintenance Mode color code (green).

2. To put an SDS back into regular service (cancel Maintenance Mode), perform these steps:
   a. In the **Backend > Storage** view, navigate to, and select the desired SDS.
   b. From the **Command menu** or context-sensitive menu, select **Exit Maintenance Mode**.
      The **Exit Maintenance Mode** window is displayed.
   c. If you want to force exit from Maintenance Mode even though there is a failed SDS, select the **Force Failed SDS** check box.
   d. Click OK.

The status area at the bottom of the window indicates when the operation is complete. Once the operation has been successfully completed, the SDS returns to normal operation, and data deltas collected on other SDSs during the maintenance period are copied back to the SDS.

### Configuring I/O priorities and bandwidth use (advanced)

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

#### Configure application IOPS and bandwidth (advanced)

Configure the number of concurrent Rebuild, Rebalance and Migration of jobs, along with the bandwidth used for these jobs.

**About this task**

Priority can be given to different types of I/Os in the system, including application I/Os. The number of concurrent Rebuild, Rebalance and Migration of jobs can be configured, along with bandwidth used for these jobs. I/O prioritization is configured per Storage Pool.

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

Give priority to Application I/Os during Rebuild, Rebalance and Migration of jobs, by performing these steps:

**Procedure**

1. In the **Backend > Storage** view, navigate to, and select the desired Storage Pool.
2. Right-click the Storage Pool and select **Settings > Set I/O Priority**.
3. Select **Favor Application I/O for Rebalance, Rebuild and Migration**, and click **OK**.

### System IOPS and bandwidth (advanced)

You can prioritize different types of I/O in the system, as well as configure network throttling per Protection Domain.

#### I/O prioritization

**About this task**

Priority can be given to different types of I/Os in the system. The number of concurrent Rebuild and Rebalance jobs can be configured, and bandwidth for Rebalance jobs can be configured. You can also control I/O priority for Migration. Refer to "V-Tree migration" for more information. If the Dynamic Bandwidth Throttling option is selected, additional items can be configured, such as Application IOPS threshold, Application bandwidth threshold, and Application threshold quiet period. Default values for these features are provided in the VxFlex OS CLI Reference Guide.

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

Configure I/O prioritization for Rebuild, Rebalance and Migration by performing these steps:

**Procedure**

1. In the **Backend > Storage** view, navigate to, and select the desired Storage Pool.
2. Right-click the Storage Pool and select **Settings > Set I/O Priority**.
3. Select the desired options and edit values, and click **OK**.

### Configuring acceleration

VxFlex OS supports different types of acceleration to enhance storage performance. Depending on your system, you can configure VxFlex OS for acceleration using NVDIMM, RFcache or RMcache.

#### Prepare acceleration devices and software

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

**Note:** The NVDIMM Interleaving setting should be disabled in the BIOS by default (configured in the relevant VxFlex iDM). To verify or set, refer to the following: https://www.dell.com/support/manuals/us/en/04/poweredge-t640/nvdimm-n_ug_pub/bios-configuration-settings-for-nvdimm-n?guid=guid-a69462d3-b86c-4f6b-903e-269f19af591f&lang=en-us

#### Add acceleration pools

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

**About this task**

An Acceleration Pool is a group of acceleration devices within a Protection Domain.
Procedure
1. In the **Backend > Devices** view, select the required Protection Domain.
2. Right-click the Protection Domain and select **Add Acceleration Pool**.
   The **Add Acceleration Pool** window is displayed.
3. Enter a name in the **Acceleration Pool Name** box.
4. Select a pool type.
   - For Fine Granularity data layout, select **NVDIMM**. You must have at least one NVDIMM installed in order to select this option.
   - For Medium Granularity data layout, select **SSD**. You must have at least one SSD installed that can be used for the RFcache feature in order to select this option.
5. Click **Add Devices** and then click the **Add device** icon to add a row to the **New Devices** table.
6. Enter the following information in the relevant row of the table:
   - In the **Path** cell, enter the location of the acceleration device
   - In the **Name** cell, enter the name of the acceleration device
   - From the **SDS** drop-down list, select the relevant SDS
7. Click **Advanced** and configure the optional settings:
   - **Test and activate device**
   - **Device test timeout: x seconds**
   - **Force devices takeover** (takes over devices that were previously used in a VxFlex OS system.
8. If you want to add more devices, click the **Add device** icon again and configure the fields in the new row.
9. Click **OK**.

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

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

Add acceleration device on RHEL nodes
You can add one or more acceleration devices to an SDS.

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

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

When adding a new NVDIMM DAX path to the acceleration pool it fails with the error:
cli --add_sds_device --sds_id <SDS-ID> --acceleration_pool_name acl --device_path /dev/dax2.0 Error: MDM failed command. Status: A device with the given

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

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

The update is displayed:

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

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

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

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

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

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

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

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

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

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

Procedure

1. From **Backend > Devices**, select an SDS.
2. At the top right side of the window, ensure that the display is set to **By Pools**.
3. Expand the desired Storage Pool, right-click the SDS where the device is installed, and select **Add Acceleration Device**.

   The **Add acceleration device to SDS** dialog box is displayed.

4. In the table, add the following information:
   - In the **Path** cell, enter the location of the acceleration device
In the Name cell, enter the name of the acceleration device

From the Acceleration Pool drop-down list, select the Acceleration Pool to which to add the device

5. Click Advanced and configure the optional settings:
   - Test and activate device
   - Device test timeout: x seconds
   - Force devices takeover (takes over devices that were previously used in a VxFlex OS system.

6. If you want to add more devices, click the Add device icon again and configure the fields in the new row.

7. Click OK.

**Prepare the DAX devices**

If the deployment will be using NVDIMM devices for acceleration, perform the following tasks to prepare the NVDIMMs as DAX acceleration devices.

**NVDIMM information table**

Before you prepare the NVDIMM as a DAX device, create or print the following NVDIMM information table. Use it to record the information that you discover while performing the following task. You will need the information to add the acceleration device to VxFlex OS.

*Note: If the failed and replacement NVDIMM share a column, the value for both entries must be the same.*

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

**Prepare an NVDIMM as a DAX device in a Linux system**

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

**Before you begin**

If the node is running on RHEL 7.6 or higher, ensure that the package `kmod-redhat-nfit-3.10.0_957-1.el7_6.x86_64.rpm` is installed.

The package can be downloaded from this location.

For more information, see here.

**About this task**

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

**Procedure**

1. Using SSH, log in to the Linux server.
2. View information for the new/replacement NVDIMM:

```
dmidecode --type memory | grep "Non-" -B 3 -A 3 | grep -E 'Locator| Serial' | grep -v Bank
```

Output similar to the following appears:

```
Locator: A7
Serial Number: 17496594
Locator: B7
Serial Number: 174965AC
```

3. Find the serial number in the output and record it in the NVDIMM information table.

4. Display the correlation between the ID and NMEM device name of each NVDIMM mounted on the server:

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

Output similar to the following appears:

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

5. In the output from the previous step, find the device (dev) with the id that partially correlates with the serial number you discovered previously for the failed device.

For example:

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

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

In the above example, the NMEM name is nmem0.
6. Record the NMEM name in the Device name row of the NVDIMM information table.

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

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

Output similar to the following appears:

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

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

```
{
  "dev": "namespace1.0",
  "mode": "raw",
  "size": 17179869184,
  "sector_size": 512,
  "blockdev": "pmem1",
  "numa_node": 1
}
{
  "dev": "namespace0.0",
  "mode": "raw",
  "size": 17179869184,
  "sector_size": 512,
  "blockdev": "pmem0",
  "numa_node": 0
}
```

8. In the output displayed in the previous step, locate the namespace that correlates with the NMEM name and DIMM serial number, and record it in the NVDIMM information table. In the above example, nmem0's namespace is namespace0.0.

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

```
ndctl destroy-namespace namespace
```

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

```
ndctl destroy-namespace namespace0.0
```
10. Create a new, raw nmem device using the region associated with namespace of the failed device, as recorded in the NVDIMM information table:

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

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

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

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

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

For ndctl build 62 or later, run:

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

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

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

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

or

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

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

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

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

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

Output similar to the following appears:

```json
{
    "dev": "namespace1.0",
    "mode": "devdax",
    "map": "dev",
    "size": 1690936576,
    "uuid": "c59d6a2d-7eeb-4f32-b27a-9960a327e734",
    "daxregion": {
        "id": 1,
        "size": 1690936576,
        "align": 4096,
        "devices": [ ...
```
The DAX device name appears in the output as the chardev value.
In the example output above, the DAX device name is dax0.0.

14. Record the DAX device name in the NVDIMM information table.
15. Find the full acceleration device path:

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

The following output should appear:

```
/dev/daxX.X
```

For example:

```
/dev/dax0.0
```

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

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

**Check NVDIMM capacity compatibility for future upgrades**

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

**Before you begin**

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

About this task

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

Procedure

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

   ```
   ```

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

   The tool will output one of the following messages:

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

     (This message may appear several times, depending on the number of SDSs with insufficient NVDIMM capacity.)

   - System is ready for upgrade

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

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

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

Configure and Customize Dell EMC VxFlex OS
### Option | Procedure
--- | ---
**CLI** | a. Prepare a list of the SDSs in your system. You can use the `--query_all_sds` to collect this information. For example:

```
scli --query_all_sds
```

b. Using the CLI, run the following command for every SDS that uses NVDIMM acceleration for Fine Granularity storage:

```
scli --query_sds (--sds_id <ID> | --sds_name <NAME> | --sds_ip <IP>)
```

For example:

```
scli --query_sds --sds_name sds1948
```

Look for output similar to the following:

```
Acceleration device information (total 2 devices)
1: Name: N/A Path: /dev/dax0.0 Original-path: /dev/dax0.0 ID ddef278000010000
Acceleration Pool: accp1, Capacity: 15.7 GB (16052 MB), Used: 21.7 GB (22170 MB), State: Normal
```

c. If the `Used` value is greater than the `Capacity` value, as shown in the output example above, more NVDIMM capacity is required in order to upgrade the system.

d. Make a note of all the SDSs where more NVDIMM capacity is required.

**GUI** | a. In the GUI, open the Monitor > Alerts view, and look for alerts for insufficient NVDIMM capacity for future version upgrades.

b. Prepare a list of all the SDSs where these alerts occur.

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

---

### Add NVDIMM in an ESXi environment

Add NVDIMMs for acceleration in an ESXi environment.

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

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

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

- You are using VMware version 6.7 for the ESXi host and the vCenter server.
- The VM version of your SVM is version 14 or higher.
- The firmware of the NVDIMM is updated to the version supported by your server. For example, for compatible Dell EMC PowerEdge servers, use NVDIMM firmware version 9324 or higher.
- The ESXi host can detect the NVDIMM.
- You calculate required NVDIMM capacity, according to number of FG devices and their size.
There is enough NVDIMM capacity on the ESXi host.

Verify that the ESXi host can detect the NVDIMM

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

Before you begin

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

Calculate required NVDIMM and RAM capacity for FG SDS

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

About this task

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

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

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

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

Note: The calculation is in binary MiB, GiB, and TiB

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

**Enter the SDS into Maintenance Mode**

Place the SDS into Maintenance Mode before adding the NVDIMM.

**Procedure**

1. Check that the VxFlex OS system is in an optimal state:
   a. From the VxFlex OS GUI Monitor > Alerts view, ensure that there are no SDS disconnect messages.
   b. If the node is an MDM cluster member, in the Dashboard > Management tile, verify that the cluster is optimal.
2. In Backend > Storage > By SDSs view, right-click the SDS you are upgrading and select Enter Maintenance Mode.
3. In the Enter Maintenance Mode window, ensure there are no errors, and then click OK.
   The status area at the bottom of the window indicates when the operation is complete.
   Once the SDS is in Maintenance Mode, this will be indicated both on the Dashboard, and in Backend tables and Property Sheets, using the symbol, and the Maintenance Mode color code (green).

**Use vCenter to shut down the SVM**

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

**Procedure**

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

**Add an NVDIMM device to a VxFlex OS system**

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

**Procedure**

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

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

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

d. If additional RAM is needed (see Calculate required NVDIMM and RAM capacity for FG SDS on page 131), modify the memory size to match the necessary value.

e. Click OK.

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

3. Using the VxFlex OS GUI, verify the following:
   a. In the Monitor > Alerts view, verify that no SDS disconnect messages appear.

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

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

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

4. In the Backend > Storage > By SDSs view, right-click the SDS and select Exit Maintenance Mode.

5. In the Action window, click OK.

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

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

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

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

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

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

   ```
   scli --add_acceleration_pool --protection_domain_name <PD_NAME> --media_type NVRAM --acceleration_pool_name <ACCP_NAME>
   ```
c. For each SDS with NVDIMM, add the NVDIMM devices to the Acceleration Pool:

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

9. Create a Storage Pool for SSD devices accelerated by NVDIMM Acceleration Pool with Fine Granularity data layout:

a. Connect using SSH to the Master MDM and run the following SCLI command:

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

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

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

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

Removing acceleration devices

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

**Remove an RFcache acceleration device**

Remove an RFcache acceleration device from an Acceleration Pool.

**About this task**

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

**Procedure**

1. From the Backend > Devices view, right-click the Storage Pool being accelerated by the device, and choose Configure Cache, and then Set Read Flash Cache Policy.
2. In the Set Read Flash Cache Policy window, clear the Enable Read Flash Cache check box, and click OK.
3. When the status shows that the operation was successful, click Close.
4. From the Backend > Devices view, navigate to the corresponding Acceleration Pool, and locate the device that you want to remove.
5. Right-click the device, and choose Remove.
6. In the dialog box that is displayed, click OK.
7. When the status shows that the operation was successful, click Close.
8. In some cases, a rebuild/rebalance begins.

Use the Dashboard view to determine when that is complete. The device is removed from the VxFlex OS system. You may now either remove the physical drive from the system, or add it to the SDS as a storage device. If you have other RFcache acceleration devices installed in the SDS, or in other SDSs in the Storage Pool, set the Read Flash Cache policy back to Enabled at both levels.
Physically remove an NVDIMM from a node

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

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

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

Before you begin

Ensure that you know:

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

About this task

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

Procedure

1. From a web browser go to http://<iDRAC_IP_address>.
2. In the Dell Console Login window, enter the username and password, and then click Login.
   
   The Dashboard displays the high-level status of all hardware devices in the System Health pane. The Memory icon should display an alert, signifying a failed device.

3. Double-click the icon of the failed memory device to display more information about the failed NVDIMM.

4. From the Maintenance tab, select System Event Log.
   
   The System Event Log displays events with color-coded severity levels. The event for the failed DIMM displays the slot number of the DIMM module that failed.

   In the following example, the error occurred on DIMM-A7, meaning that the DIMM is located in slot A7.
5. Record the slot number of the failed NVDIMM device in the NVDIMM information table.

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

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

7. Expand the entry for the relevant DIMM.

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

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

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

9. View information for the faulty DIMM:

   ```
   dmidecode --type memory | grep "Non-" -B 3 -A 3 | grep -E 'Locator|Serial' | grep -v Bank
   ```

   Output similar to the following appears:

   ```
   Locator: A7
   Serial Number: 16492521
   Locator: B7
   Serial Number: 1649251B
   ```

   The example output displays the DIMM’s **Type Detail** as Non-Volatile, signifying that it is an NVDIMM. The output also displays the NVDIMM serial numbers.

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

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

   ```
   ndctl list -Dvvv | jq '.[].dimms'
   ```
Output similar to the following should appear:

```
[
  {
    "dev": "nmem1",
    "id": "802c-0f-1711-1649251b",
    "handle": 4097,
    "phys_id": 4370,
    "state": "disabled",
    "health": {
      "health_state": "ok",
      "temperature_celsius": 255,
      "life_used_percentage": 32
    }
  },
  {
    "dev": "nmem0",
    "id": "802c-0f-1711-",
    "handle": 1,
    "phys_id": 4358,
    "state": "disabled",
    "health": {
      "health_state": "ok",
      "temperature_celsius": 255,
      "life_used_percentage": 32
    }
  }
]
```

12. In the output from the previous step, find the device (dev) with the id that partially correlates with the serial number you discovered previously for the failed device.

For example:

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

<table>
<thead>
<tr>
<th>Serial number</th>
<th>Device ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locator: A7</td>
<td>Serial Number: 16492521</td>
</tr>
<tr>
<td>Locater: B7</td>
<td>Serial Number: 1649251B</td>
</tr>
</tbody>
</table>

In the above example, the NMEM name is nmem0.

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

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

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

Output similar to the following appears:

```
{
  "dev": "region1",
  "size": 17179869184,
  "available_size": 0,
  "max_available_extent": 0,
  "type": "pmem",
  "numa_node": 1,
}
"mappings": [
  {
    "dimm": "nmem1",
    "offset": 0,
    "length": 17179869184,
    "position": 0
  }
],
"persistence_domain": "unknown",
"namespaces": [
  {
    "dev": "namespace1.0",
    "mode": "devdax",
    "map": "dev",
    "size": 16909336576,
    "uuid": "0a438fbc-91e4-427d-8068-1f26330d85cc",
    "daxregion": {
      "id": 1,
      "size": 16909336576,
      "align": 4096,
      "devices": [
        {
          "chardev": "dax1.0",
          "size": 16909336576
        }
      ],
      "numa_node": 1
    }
  }
],
"dev": "region0",
"size": 17179869184,
"available_size": 0,
"max_available_extent": 0,
"type": "pmem",
"numa_node": 0,
"mappings": [
  {
    "dimm": "nmem0",
    "offset": 0,
    "length": 17179869184,
    "position": 0
  }
],
"persistence_domain": "unknown",
"namespaces": [
  {
    "dev": "namespace0.0",
    "mode": "devdax",
    "map": "dev",
    "size": 16909336576,
    "uuid": "38cbd555-3f5b-4f4f-8d83-bf77db7553d",
    "daxregion": {
      "id": 0,
      "size": 16909336576,
      "align": 4096,
      "devices": [
        {
          "chardev": "dax0.0",
          "size": 16909336576
        }
      ],
      "numa_node": 0
    }
  }
]
The order of the list in the output reflects the order for correlating between an NMEM DIMM and a namespace/DAX device. For example, in the above output:

- The first block of devices is the DIMMs. Under each DIMM, there is an NMEM device grouping. In the example output, the device groupings are nmem1 and nmem0. Each bracket contains a device.

- Each grouping also displays the region corresponding to the NMEM device group. In the example output, the regions are region1 and region0.

- The order of the NMEM devices correlates to the namespace grouping that follows, in which nmem1 correlates to namespace1.0 and nmem0 correlates to namespace0.0.

- The output displaying the namespace also includes the DAX device name (chardev), which is displayed as daxX.X.

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

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

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

Results

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

Remove the storage devices from VxFlex OS in a Linux system
Remove the storage devices that interact with the failed NVDIMM from the relevant VxFlex OS FG Storage Pool and Acceleration Pool in a Linux-based system.

Before you begin

Ensure that you have admin rights for accessing the VxFlex OS GUI. If necessary, the customer can give you the credentials.

About this task

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

Procedure

1. Log in to the VxFlex OS GUI as an admin user.
2. Go to Backend > Storage > Acceleration view.
3. Expand the SDSs in the Protection Domains.
4. In the Accelerated On column, find the FG Storage Pool that contains the DAX devices you discovered in the previous task and recorded in the NVDIMM information table.

For example, if you discovered DAX device name dax0.0, in the Accelerated On column look for /dev/dax0.0.

In the following image, /dev/dax0.0 is located in FG Storage Pool sp2_FG. It is also located in Acceleration Pool accp_for_sp2_NVDIMM.
5. Record the name of the FG Storage Pool, the Acceleration Pool, the storage devices, and the DAX devices in the relevant rows in the NVDIMM information table.

In the above example, the information you need to record is:
- Storage Pool: sp2_FG
- Acceleration Pool: accp_for_sp2_NVDIMM
- Storage devices: /dev/sdb, dev/sdc
- Acceleration devices: /dev/dax0.0, /dev/dax1.0.

6. Remove the storage devices you identified in the previous step from the relevant Storage Pool:

   **Note:** Ensure that you remove only the storage devices impacted by the failed NVDIMM.

   a. Navigate to Backend > Devices view and find the SDS with the storage devices you identified in the previous step.

   b. Right-click the storage devices you identified in the previous step, select Remove, and then click OK.

      **Note:** You can select all the relevant storage devices and remove them simultaneously.

      A confirmation message appears when the process is complete, and a rebuild/rebalance operation may be triggered.

   c. In GUI Dashboard view, wait until the rebuild/rebalance operation is complete and all counters are at 0.

7. Remove the acceleration devices corresponding to the failed NVDIMM from the relevant Acceleration Pool:
a. In Backend > Devices view in the relevant Storage Pool, right-click the acceleration devices you identified previously, select Remove, and then click OK. A confirmation message appears when the process is complete.

8. If you are replacing the NVDIMM battery, perform the previous steps for every NVDIMM module mounted on the server.

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

RFcache (xcache) package installation
If the RFcache (xcache) package was not installed during the initial system deployment, you can also install the RFcache (xcache) package on physical or virtual servers in an existing VxFlex OS system. The package is required on SDSs in order to accelerate Medium Granularity data layout Storage Pools.

Install the RFcache (xcache) package on physical servers
You can install the RFcache (xcache) package on physical servers using VxFlex OS Installer and the CSV topology file.

About this task
To install RFcache, perform the following:

Procedure
1. Update the RFcache fields in the CSV file used to deploy the system, as described in the "Preparing the CSV topology file" section of the Deploy VxFlex OS Guide.
2. Follow the instructions in "Add components in the VxFlex OS Installer".

Enable RFcache on ESXi servers
You can manually enable RFcache on ESXi servers using the vSphere VxFlex OS plug-in.

About this task
You must first copy the RFcache (xcache) package to the SVMs, and then use the VxFlex OS plug-in to configure its use.

Procedure
1. Copy the RFcache package (xcache) to all SVMs running an SDS:

   EMC-ScaleIO-xcache-x.x-x.0.slesxx.x.x86_64

2. Install the file:

   rpm -i EMC-ScaleIO-xcache-x.x-x.0.slesxx.x.x86_64

3. From the VxFlex OS plug-in, click SDSs.
4. Right-click an SDS, and select Add devices to a single SDS.
5. Click a device in the Use for drop-down list, and select RFcache.
6. Click OK.
7. Repeat the previous steps for every SDS on which you want to enable RFcache.

Increase SVM memory to accommodate additional SDS device

When adding additional disks to an SDS, you may need to add additional memory to the SVM.

About this task
After an initial partial population of disks (less than the SDS full capacity), when adding more disks, you may need to add SVM memory. If the SDS doesn't have enough memory, error messages will be displayed. (You can avoid this procedure by using the deployment wizard to allocate adequate memory during initial deployment.)

Perform this procedure in a maintenance window.

Procedure
1. From the VxFlex OS GUI, put an SDS in maintenance mode.
2. From the vCenter, power off the SVM.
3. From the vCenter, edit the SVM and increase the SVM memory by 300 MB for each 5 TB of added storage capacity.
4. Power on the SVM.
5. From the VxFlex OS GUI, remove the SDS from maintenance mode.
6. Wait for the rebalance to complete.
7. Repeat the entire procedure for each SVM, one-at-a-time.

After you finish
You can now use any of the VxFlex OS management tools to add more drives to the SDS.

Modify an SDS port during I/O

You can modify an SDS port while there is I/O running without interrupting I/O.

About this task

Note: Sometimes, your network topology needs to be prepared for the addition of new port, and this may take some time. VxFlex OS does not prevent unnecessary degraded status or disconnection of SDS. Therefore, in such situations, it is recommended to place the SDS in Maintenance Mode before commencing this procedure.

Procedure
1. On the SDS, perform one of the following as appropriate for your operating system:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>Run the script: /opt/emc/scaleio/sds/bin/close_firewall_port.sh</td>
</tr>
<tr>
<td>Windows</td>
<td>From command line, run the batch file C:\Program Files\EMC\scaleio\sds\bin\close_firewall_port.bat</td>
</tr>
</tbody>
</table>

2. Open the following SDS file with a text editor, and change the port number shown there to the new port number:
3. Open the following SDS configuration file with a text editor:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>/opt/emc/scaleio/sds/cfg/conf.txt</td>
</tr>
<tr>
<td>Windows</td>
<td>C:\Program Files\EMC\scaleio\sds\cfg\conf.txt</td>
</tr>
</tbody>
</table>

4. Add the parameter `tgt_port = <NEW_PORT_NUM>` to the file, where `<NEW_PORT_NUM>` represents the new port number.

5. Perform one of the following:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>Run the script: /opt/emc/scaleio/sds/bin/open_firewall_port.sh</td>
</tr>
<tr>
<td>Windows</td>
<td>From command line, run the batch file C:\Program Files\EMC\scaleio\sds\bin\open_firewall_port.bat</td>
</tr>
</tbody>
</table>

6. On the SDS, perform one of the following:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>Run the command: <code>Pkill sds</code></td>
</tr>
<tr>
<td>Windows</td>
<td>From command line, run the command: <code>net stop sds_service &amp; net start sds_service</code></td>
</tr>
</tbody>
</table>

7. On the MDM, modify the SDS port using the command:

```
scli --modify_sds_port (--sds_id <ID> | --sds_name <NAME> | --sds_ip <IP>) --new_sds_port <PORT>
```

For example, for an SDS called "sds198" where the new port number is 7071, type:

```
scli --modify_sds_port --sds_name sds198 --new_sds_port 7071
```

**Note:** If you modify the SDS port on the MDM first, instead of following the above procedure, I/O errors might be encountered.
CHAPTER 6

VASA and vVols

Configure VxFlex OS to use VMware's vSphere API for Storage Awareness (VASA).

- VxFlex OS VASA's limitations and prerequisites .......................................................... 146
- vVols in VxFlex OS ........................................................................................................ 146
- Using storage policies .................................................................................................... 147
- Register the VxFlex OS VASA in the vCenter .............................................................. 147
- Enable autostart of the VASA provider after reboot .................................................... 148
VxFlex OS VASA's limitations and prerequisites

Note the following limitations when using VxFlex OS's VASA.

**Limitations**

- Deployment of VxFlex OS's VASA is not prevented on ESXi 5.5, despite the fact that VMware no longer supports ESXi 5.5.
- The maximum number of volumes is 200K (4,096 mapped volumes per ESXi).
- The VASA can be mapped to a single instance of VxFlex OS.
- A cluster may contain a single VASA provider or three Vasa providers.
- The VASA provider may be installed only on a node which contains an SDC.
- The VASA should be registered with a single vCenter.
- The VASA provider hostname must begin with a letter character.
- The maximum snapshot hierarchy of a vVol is 31.

**Before you begin**

Ensure that:

- Oracle Java Development Kit 1.8.x must be installed on every host that will run the VASA provider, and no other Java distribution should be installed.
- For each VASA VM, the DNS server is configured and all ESXis, vCenters, and VASA Storage Virtual Machines (SVM) are registered on it.
- Each VASA VM's hostname must match the VASA FQDN.
- All components of your environment, including ESXis and vCenters, have their time synchronized.
- A Storage Data Client (SDC) is installed on the ESXi on which you want to deploy VASA.
- VxFlex OS is deployed and registered in the vCenter.

*vVols in VxFlex OS*

When the VASA provider is installed in the VxFlex OS system, you can use and manage vVols using VxFlex OS.


By default, vVols are not visible in the VxFlex OS GUI. In order to have the vVols displayed, you must change the system preferences to show externally managed volumes. For more information on changing system preferences, see Customize system preferences on page 212. Once the externally managed volumes are visible, you can see the vVols listed in the VxFlex OS GUI Frontend view. Note that management of the vVols from the VxFlex OS GUI is prohibited.

Logs are located in the following directory: /opt/emc/caleio/vasa/logs/. For support, you can use the script /opt/emc/caleio/vasa/get_vasa_info.sh, which creates a tar.gz archive in the /tmp directory. It includes the following diagnostic information on VASA:
Using storage policies

A virtual machine that runs on a Virtual Volumes datastore requires a VM storage policy. A VM storage policy is a set of rules that contains placement and quality-of-service requirements for a virtual machine.

VxFlex OS has its own specific set of rules for assigning storage policies to Storage Pools. For more information on creating storage policies, see Create a VM storage policy for Virtual Volumes on page 118.

Register the VxFlex OS VASA in the vCenter

Register the VxFlex OS VASA as a Storage Provider in the vCenter.

About this task

When using one instance of the VASA, register it in the vCenter. When you are using three instances of the VASA provider, you must register at least two out of the three VASA providers. In that case, one of the two VASA providers is displayed in the vSphere Web Client in Active state and the other is displayed in Standby state.

Procedure

1. When using vSphere 6.0, 6.0 U1, and 6.0 U2, enable TLSv1.0:
   a. Edit the /opt/emc/scaleio/vasa/setenv.sh.
   b. Delete the following parameters from the file: -Dserver.ssl.enabled-protocols=TLSv1.2,-Dhttps.protocols=TLSv1.2, and Dserver.ssl.protocol=TLS.
   c. Restart the VASA service:

   ```
   service vasa-provider-vxflexos restart
   ```

2. In the vSphere Web Client, navigate to the Hosts and Clusters inventory object.
3. Locate the vCenter inventory object and select it.
   - In vSphere 6.0: Click the Manage tab, and click Storage Providers.
   - In vSphere 6.5: Click the Configure tab, and click More > Storage Providers.
4. Click the Register a Storage Provider icon.
5. In the New Storage Provider dialog, define the connection information for the storage provider:
   a. Enter a name for the VASA provider.
   b. Enter the VASA URL: https://<VASA_FQDN>/version.xml where <VASA_FQDN> is the fully-qualified domain name of the VASA, as registered in the DNS server.
   c. Enter the MDM admin username and password.
6. Click OK to complete the registration.
7. Click Yes to confirm the VASA certificate.

Results
The vCenter Server has registered the VxFlex OS VASA as a storage provider.

After you finish
Verify that the status of the VASA Storage Provider in the Storage Provider table is online. If the status is offline, it most likely indicates an issue with the DNS or a communication issue with the ESXis.

Enable autostart of the VASA provider after reboot

Enable automatic restarting of the VASA provider service after reboot.

Procedure
1. Connect with SSH to each VASA provider host.
2. Run the following command to enable automatic restart of the VASA provider service after reboot:

   systemctl enable vasa-provider-vxflexos
CHAPTER 7

MDM Cluster

You can configure the MDM cluster in the VxFlex OS system.

- Configuring MDM cluster ........................................................................................................ 150
- Configure virtual IP addresses using the VxFlex OS Installer .............................................. 162
Configuring MDM cluster

You can configure the MDM cluster to allow for efficient load balancing to enable high availability of the servers that are configured within the cluster. You can add members, replace or remove members as well as update configuration settings. Members refer to the servers within the cluster.

Extend an existing VxFlex OS system

Options for adding nodes to an existing system.

You can add nodes to an existing system, as well as extend the MDM cluster from a 3-node to a 5-node cluster. Depending on your system, you can use the VxFlex OS Installer (for physical servers) or the vSphere plug-in (for ESXi servers).

These topics are described in the sections of the *Deploy VxFlex OSGuide*.

- "Extend an existing VxFlex OS system"
- "Extend the MDM cluster from 3 to 5-node"

Add Linux servers to the MDM cluster

You can add Linux servers to the MDM cluster to expand your 3-node cluster mode to a 5-node cluster mode.

**About this task**

This procedure describes how to add Linux servers to the MDM cluster in the CSV topology file.

**Procedure**

1. Obtain the CSV topology file from one of the following options:
   - CSV used to deploy the v2.0 system in its current 3-node cluster mode
   - Complete or minimal CSV (provided in the ISO, or can be downloaded from the VxFlex OS Installer) and fill-in the current system topology fields in the CSV
2. Edit, and save the CSV with one of these options:
   - Add two new hosts (two new lines) to the system topology, and in the **Is MDM/TB** column for those lines, designate one as a Slave and one as a Tie Breaker (TB) role
   - In the **Is MDM/TB** column of two existing hosts that were not part of the MDM cluster, add a Slave and a Tie Breaker (TB) role. This option is displayed in the following figure

**Note:** If you need to change the roles of the current nodes, do so only after adding to the cluster.

**Figure 12 Before adding**

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IPs</td>
<td>Password</td>
<td>Operating System</td>
<td>Is MDM/TB</td>
<td>Is SDS</td>
<td>SDS Device List</td>
</tr>
<tr>
<td>2</td>
<td>10.76.60.1</td>
<td>password1</td>
<td>linux</td>
<td>Primary</td>
<td>Yes</td>
<td>/dev/sdb</td>
</tr>
<tr>
<td>3</td>
<td>10.76.60.2</td>
<td>password1</td>
<td>linux</td>
<td>Secondary</td>
<td>Yes</td>
<td>/dev/sdb</td>
</tr>
<tr>
<td>4</td>
<td>10.76.60.3</td>
<td>password1</td>
<td>windows</td>
<td>TB</td>
<td>Yes</td>
<td>g</td>
</tr>
<tr>
<td>5</td>
<td>10.76.60.4</td>
<td>password1</td>
<td>linux</td>
<td>Yes</td>
<td>/dev/sdb</td>
<td>Yes</td>
</tr>
<tr>
<td>6</td>
<td>10.76.60.5</td>
<td>password1</td>
<td>windows</td>
<td>Yes</td>
<td>g</td>
<td>Yes</td>
</tr>
</tbody>
</table>
3. In the Packages tab, upload all VxFlex OS packages, per the host OS.

4. In the Install tab, select the edited CSV file, and select Add to existing system from the drop-down menu.

5. Click Upload installation CSV.

6. Start the installation, and monitor as normal.

Add ESXi servers to the MDM cluster

You can add additional ESXi servers, and assign them roles within the cluster.

About this task

When you add a new MDM manager, to ensure continued SDC-MDM communication, you must update the SDCs in the system with the new MDM IP address. You can do this using the vSphere plug-in, as described in "Update the SDC parameters".

Procedure

1. If the ESXi servers to be added do not have the SDC component, install the SDC on each of the servers, as described in the "Update the SDC parameters".

2. From the Basic tasks section, click Deploy VxFlex OS environment.

   The VxFlex OS VMware deployment wizard runs. If you exited the wizard before completing the deployment, the wizard continues from the point you left off.

   NOTICE

   The deployment wizard assumes that you are using the provided VxFlex OS OVA template to create the Storage Virtual Machines (SVMs).

3. In the Select Installation screen, select Add servers to a registered VxFlex OS system, and select the system you want to extend.

4. In the Select Management Components screen, select 5-node mode.

5. In the Manager MDM and Tie Breaker MDM fields, select the nodes to add to the cluster.
6. Click **Next**, and continue the deployment.

**Note:**
When adding components, the wizard adjusts the displayed screens to options that are relevant to the current VxFlex OS system.

**Update the SDC parameters in VMware based HCI or compute node**

Update the SDC parameters to maintain SDC-MDM communication.

**About this task**
This procedure describes how to use the VMware plug-in to update the SDCs that are needed to maintain SDC-MDM communication.

**Procedure**
1. From the plug-in **Advanced tasks** menu, click **Update SDC parameters**, and follow instructions to complete the process.
2. Check that the SDC parameters were updated by running this command on each ESXi:

   ```bash
   cat /etc/vmware/esx.conf | grep scini | grep -i mdm
   ```

**Replace a cluster member**

You might need to replace a member of an MDM cluster to replace a faulty server or change the server IP address.

The current server is the server that needs to be replaced.

If you have an extra server to replace the current server, then there is no need to change the cluster mode (3-node or 5-node). If you do not have an additional server, you will need to reduce the cluster mode, from 5-node to 3-node, or from 3-node to single node.
Note:
It is not recommended to use single mode in production systems, except in temporary situations.

The following rules are true regardless of the circumstances:

- To remove a cluster member, you first need to make it a standby, then remove the standby. To add a member to a cluster, you first make it a standby, then add the standby to the cluster.

- The cluster must always have 5, 3, or 1 members, never any other amount. For a further understanding of this subject, see "The MDM cluster" in the Architecture section of Getting to Know VxFlex OS. Proceed to the section that describes your environment:
  - "Replace a cluster member by adding a new server"
  - "Replace a cluster member without adding a new server to the cluster"

Add a new server to the MDM cluster

Add or replace a server to the MDM cluster.

About this task
This procedure describes how to replace or add a new member to the MDM cluster.

Before you begin, perform the following:

- Assign the necessary IP addresses to the replacement server.

- Install the MDM package on the server.

  In this example, we are replacing the server whose IP address is 10.3.1.179, currently a member of a 5-node MDM cluster, with a server whose IP address is 10.3.1.57, which is currently external to any VxFlex OS system. This process can be used to replace any role in the MDM cluster.

Procedure

1. Check that the current server (179) is not the Master MDM by running the following command:

   ```bash
   scli --query_cluster
   ```

   The output similar to the following is displayed:

   ```
   # scli --query_cluster
   Cluster:
   Mode: 5_node, State: Normal, Active: 5/5, Replicas: 3/3
   Master MDM:
   Name: mdm17, ID: 0x5d07497754427fd0
   IPs: 10.3.1.17, 192.168.1.17, Management IPs: 10.3.1.17, Port: 9011
   Version: 2.0.972
   Slave MDMs:
   Name: mdm19, ID: 0x26ee566356362451
   IPs: 10.3.1.19, 192.168.1.19, Management IPs: 10.3.1.19, Port: 9011
   Status: Normal, Version: 2.0.972
   Name: mdm18, ID: 0x5843c4d16d8f1082
   IPs: 10.3.1.18, 192.168.1.18, Management IPs: 10.3.1.18, Port: 9011
   Status: Normal, Version: 2.0.972
   Tie-Breakers:
   Name: mdm179, ID: 0x7380b70e2f73d346
   IPs: 10.3.1.179, 192.168.1.179, Port: 9011
   Status: Normal, Version: 2.0.972
   Name: mdm20, ID: 0x6dfel1c5f4062b5b3
   ```
IPs: 192.168.1.20, 10.3.1.20, Port: 9011  
Status: Normal, Version: 2.0.972

In this case server 179 is a Tie Breaker.

2. If the current server is the Master MDM, change its state using the `switch_mdm_ownership` command, as described in the VxFlex OS CLI Reference Guide.

3. Make the replacement MDM server a standby MDM, and assign it a name (mdm57, in our example) by running the following command, on the Master MDM:

   ```bash
   scli --add_standby_mdm --mdm_role tb --new_mdm_ip 10.3.1.57,192.168.1.57 --new_mdm_management_ip 10.3.1.57 --new_mdm_name mdm57
   ```

4. You can see the result of the command by running the following command:

   ```bash
   scli --query_cluster
   ```

   The output similar to the following is displayed:

   ```text
   # scli --query_cluster
   Cluster:
   Mode: 5_node, State: Normal, Active: 5/5, Replicas: 3/3
   ...
   Tie-Breakers:
   Name: mdm179, ID: 0x7380b70e2f73d346
   IPs: 10.3.1.179, 192.168.1.179, Port: 9011
   Status: Normal, Version: 2.0.972
   Name: mdm20, ID: 0x6dfe1c5f4062b5b3
   IPs: 192.168.1.20, 10.3.1.20, Port: 9011
   Status: Normal, Version: 2.0.972
   Standby MDMs:
   Name: mdm57, ID: 0x073e4c8b1d20d124, Tie Breaker
   IPs: 10.3.1.57, 192.168.1.57, Port: 9011
   ```

   mdm57 has been added as a standby MDM. When it is a standby MDM, it can be added to the cluster.

5. Replace the current mdm179 with the standby mdm57 by running the following command:

   ```bash
   scli --replace_cluster_mdm --remove_tb_name mdm179 --add_tb_name mdm57
   ```

   The following output is displayed:

   ```text
   Successfully replaced the cluster MDM
   ```

   The current server has been replaced.

Reassign a member within the MDM cluster

You can reassign a member to a new role within the MDM cluster.

**About this task**

This procedure describes how to remove a member and then add the node back and reassign it to a different role within the cluster. You must first reduce the amount of nodes in the cluster,
change to a 3-node cluster and then add the member back to the cluster and reassign it to its new role.

In the following example, we are removing the current server whose IP address is 10.3.1.179, currently a Tie Breaker member of a 5-node MDM cluster. To retain a majority in the MDM cluster, we must also remove one of the Slave MDMs in the cluster, in this case the MDM whose IP address is 10.3.1.19. This process can be used to replace any role in the MDM cluster.

**Procedure**

1. Verify that the current server (179) is not the Master MDM:

   ```
   scli --query_cluster
   ```

   The output similar to the following is displayed:

   ```
   # scli --query_cluster
   Cluster:
   Mode: 5_node, State: Normal, Active: 5/5, Replicas: 3/3
   Master MDM:
   Name: mdm17, ID: 0x5d07497754427fd0
   IPs: 10.3.1.17, 192.168.1.17, Management IPs: 10.3.1.17, Port: 9011
   Version: 2.0.972
   Slave MDMs:
   Name: mdm19, ID: 0x26ee566356362451
   IPs: 10.3.1.19, 192.168.1.19, Management IPs: 10.3.1.19, Port: 9011
   Status: Normal, Version: 2.0.972
   Name: mdm18, ID: 0x5843c4d16d8f1082
   IPs: 10.3.1.18, 192.168.1.18, Management IPs: 10.3.1.18, Port: 9011
   Status: Normal, Version: 2.0.972
   Tie-Breakers:
   Name: mdm179, ID: 0x7380b70e2f73d346
   IPs: 10.3.1.179, 192.168.1.179, Port: 9011
   Status: Normal, Version: 2.0.972
   Name: mdm20, ID: 0x6dfe1c5f4062b5b3
   IPs: 192.168.1.20, 10.3.1.20, Port: 9011
   Status: Normal, Version: 2.0.972
   ```

   In this case server 179 is a Tie Breaker.

2. If the current server is the Master MDM, change its state using the `switch_mdm_ownership` command, as described in the *VxFlex OS CLI Reference Guide*.

3. Switch to a 3-node cluster:

   ```
   scli --switch_cluster_mode --cluster_mode 3_node
   --remove_tb_name mdm179 --remove_slave_mdm_name mdm19
   ```

   The following output is displayed:

   ```
   Successfully switched the cluster mode.
   ```

4. To view the result of the command, run:

   ```
   scli --query_cluster
   ```
The output similar to the following is displayed:

```
# scli --query_cluster
Cluster:
  Mode: 3_node, State: Normal, Active: 3/3, Replicas: 2/2
  ...
Slave MDMs:
  Name: mdm18, ID: 0x5843c4d16d8f1082
  IPs: 10.3.1.18, 192.168.1.18, Management IPs: 10.3.1.18, Port: 9011
  Status: Normal, Version: 2.0.972
  Tie-Breakers:
  Name: mdm20, ID: 0x6dfe1c5f4062b5b3
  IPs: 192.168.1.20, 10.3.1.20, Port: 9011
  Status: Normal, Version: 2.0.972
Standby MDMs:
  Name: mdm19, ID: 0x26ee566356632451, Manager
  IPs: 10.3.1.19, 192.168.1.19, Management IPs: 10.3.1.19, Port: 9011
  Name: mdm179, ID: 0x7380b70e2f73d346, Tie Breaker
  IPs: 10.3.1.179, 192.168.1.179, Port: 9011
```

The cluster has been changed to 3-node mode, as a Slave MDM (mdm19) and a TB MDM (tb179) have been removed and are now standby MDMs.

Now that the current server is a standby MDM, it can removed from VxFlex OS.

5. Remove the current server from VxFlex OS:

```
scli --remove_standby_mdm --remove_mdm_name mdm179
```

The following output is displayed:

```
Successfully removed the standby MDM.
```

6. To view the result of the command, run:

```
scli --query_cluster
```

The output similar to the following is displayed:

```
Cluster:
  Mode: 3_node, State: Normal, Active: 3/3, Replicas: 2/2
  ...
Tie-Breakers:
  Name: mdm20, ID: 0x6dfe1c5f4062b5b3
  IPs: 192.168.1.20, 10.3.1.20, Port: 9011
  Status: Normal, Version: 2.0.972
Standby MDMs:
  Name: mdm19, ID: 0x26ee566356632451, Manager
  IPs: 10.3.1.19, 192.168.1.19, Management IPs: 10.3.1.19, Port: 9011
```

The current server is no longer a standby MDM.

7. Reassign IP addresses to the current server, as required.

In our case, we will assign the following IP address to the current server: 10.3.1.57.
8. Add the current server (57) back to the system as a standby MDM, and assign it the name mdm57:

```
scli --add_standby_mdm --mdm_role tb --new_mdm_ip 10.3.1.57,192.168.1.57 --new_mdm_management_ip 10.3.1.57 --new_mdm_name mdm57
```

The output similar to the following is displayed:

```
Successfully added a standby MDM. Object ID 13c925450656db74
```

9. To view the result of the command, run:

```
scli --query_cluster
```

The output similar to the following is displayed:

```
Cluster:
  Mode: 3_node, State: Normal, Active: 3/3, Replicas: 2/2
  ... 
  Tie-Breakers:
    Name: mdm20, ID: 0x6dfe1c5f4062b5b3
    IPs: 192.168.1.20, 10.3.1.20, Port: 9011
    Status: Normal, Version: 2.0.972

Standby MDMs:
  Name: mdm19, ID: 0x26ee566356362451, Manager
  IPs: 10.3.1.19, 192.168.1.19, Management IPs: 10.3.1.19, Port: 9011
  Name: mdm57, ID: 0x13c925450656db74, Tie Breaker
  IPs: 10.3.1.57, 192.168.1.57, Port: 9011
```

The server *mdm57* is now a standby MDM, so it can be promoted to the MDM cluster.

10. Switch to 5-node cluster by adding the standby MDMs to the cluster:

```
scli --switch_cluster_mode --cluster_mode 5_node --add_slave_mdm_name mdm19 --add_tb_name mdm57
```

The following output is displayed:

```
Successfully switched the cluster mode.
```

11. To view the result of the command, run:

```
scli --query_cluster
```

The output similar to the following is displayed:

```
Cluster:
  Mode: 5_node, State: Normal, Active: 5/5, Replicas: 3/3
  Master MDM:
    Name: mdm17, ID: 0x5d07497754427fd0
    IPs: 10.3.1.17, 192.168.1.17, Management IPs: 10.3.1.17, Port: 9011
    Version: 2.0.972
```

Configure and Customize Dell EMC VxFlex OS
Slave MDMs:
Name: mdm18, ID: 0x5843c4d16d8f1082
IPs: 10.3.1.18, 192.168.1.18, Management IPs: 10.3.1.18, Port: 9011
Status: Normal, Version: 2.0.972
Name: mdm19, ID: 0x26ee566356362451
IPs: 10.3.1.19, 192.168.1.19, Management IPs: 10.3.1.19, Port: 9011
Status: Normal, Version: 2.0.972
Tie-Breakers:
Name: mdm20, ID: 0x6dfe1c5f4062b5b3
IPs: 192.168.1.20, 10.3.1.20, Port: 9011
Status: Normal, Version: 2.0.972
Name: mdm57, ID: 0x13c925450656db74
IPs: 10.3.1.57, 192.168.1.57, Port: 9011
Status: Normal, Version: 2.0.972

12. When changing an MDM IP address, it is mandatory to update and restart the all the SDCs in the system as well.

   a. Update the IP addresses:
      Windows:
      
      C:\Program Files\emc\scaleio\sdc\bin\drv_cfg --mod_mdm_ip
          --ip <EXISTING_MDM_IP_ADDRESS>
          --new_mdm_ip <NEW_MDM_IP_ADDRESSES>

      Linux:

      /opt/emc/scaleio/sdc/bin/drv_cfg --mod_mdm_ip
          --ip <EXISTING_MDM_IP_ADDRESS>
          --new_mdm_ip <NEW_MDM_IP_ADDRESSES>

   b. Restart the SDC.

   c. Verify the changes:
      Windows:

      C:\Program Files\emc\scaleio\sdc\bin\drv_cfg --query_mdms

      Linux:

      /opt/emc/scaleio/sdc/bin/drv_cfg --query_mdms

The output similar to the following should appear:

Retrieved 1 mdm(s)
MDM-ID 043925027bb30e SDC ID 28c5479b00000000 INSTALLATION ID
7214f7ca647c185b IPs [0]-9.4.4.12 [1]-9.4.4.11
Remove members from the MDM cluster

You can change from 5-node to 3-node mode, or 3-node to single node mode

There are different scenarios for replacing a server, depending on whether an extra server is available to temporarily take over the role of the one being replaced, or not. For more information on changing servers, refer to "Replace a cluster member".

Configure virtual IP addresses

Configure virtual IP addresses for the MDMs in VxFlex OS.

You can configure virtual IP addresses during deployment or post-deployment. Use the following management tools to configure virtual IP addresses:

<table>
<thead>
<tr>
<th>Management tool</th>
<th>Actions</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>VxFlex OS Installer</td>
<td>Add virtual IP addresses only.</td>
<td>For details, see the deployment documentation.</td>
</tr>
<tr>
<td>vSphere Web plug-in</td>
<td>Add virtual IP addresses only.</td>
<td>For details, see the VxFlex OS User Guide.</td>
</tr>
<tr>
<td>CLI</td>
<td>Add, modify, and remove virtual IP addresses.</td>
<td>For details, see the VxFlex OS CLI Reference Guide.</td>
</tr>
<tr>
<td>REST API</td>
<td>Add, modify, and remove virtual IP addresses.</td>
<td>For details, see VxFlex OS REST API Reference Guide.</td>
</tr>
</tbody>
</table>

Add another IP address subnet to an MDM cluster

Add an IP network to an existing MDM cluster.

About this task

This procedure describes how to add another IP address subnet for use by the MDM cluster. This addresses scenarios where the MDM cluster uses a single network, or when an existing network needs to be replaced by a different one or to simply add another network (to an already multiple-network cluster). The MDM supports up to 8 networks.

**Note:** The procedure describes an example for a for 3-node cluster, however, the procedure for a 5-node cluster is similar.

Procedure

1. Query the system to get the current cluster state/health:

   ```
scli --query_cluster
   ```

   Cluster status is returned, where you can identify the Master, the Slave, and the Tie Breaker.

2. Switch to single cluster mode:

   ```
scli --switch_cluster_mode --cluster_mode 1_node --remove_slave_mdm_id <mdm_slave_id> --remove_tb_id <tb_id>
   ```
3. Remove the standby MDM:

```bash
scli --remove_standby_mdm --remove_mdm_id <mdm_slave_id>
```

4. Remove the Tie Breaker:

```bash
scli --remove_standby_mdm --remove_mdm_id <tb_id>
```

5. Add the MDM as standby with its IP addresses (including the additional IP addresses):

```bash
scli --add_standby_mdm --new_mdm_ip ip_1<,ip_2,...> --mdm_role manager --new_mdm_management_ip ip_1<,ip_2,...> --allow_asymmetric_ips --force_clean
```

For example:

```bash
scli --add_standby_mdm --new_mdm_ip 10.89.9.6,10.89.11.6 --mdm_role manager --new_mdm_management_ip 10.89.9.6,10.89.11.6 --allow_asymmetric_ips --force_clean
```

6. Add the Tie Breaker as standby with its IP addresses (including the additional IP addresses):

```bash
scli --add_standby_mdm --new_mdm_ip ip_1<,ip_2,...> --mdm_role tb --new_mdm_management_ip ip_1<,ip_2,...> --allow_asymmetric_ips --force_clean
```

7. Switch cluster operation back to a 3-node cluster:

```bash
scli --switch_cluster_mode --cluster_mode 3_node --add_slave_mdm_id <slave_id> --add_tb_id <tb_id>
```

For example:

```bash
scli --switch_cluster_mode --cluster_mode 3_node --add_slave_mdm_id 0x4520631c7262bbf1 --add_tb_id 0x3cde0ef516f61162
```

8. Query the system to get the current cluster state/health.

```bash
scli --query_cluster
```

Cluster status is returned, where you can check that the cluster is configured and operating as expected.

9. Switch MDM ownership to verify cluster functionality:

```bash
scli --switch_mdm_ownership --new_master_mdm_id <new_master_mdm_id>
```
For example:

```
scsi --switch_mdm_ownership --new_master_mdm_id 0x4520631c7262bbf1
```

10. Query the system to get the current cluster state/health.

```
scsi --query_cluster
```

Cluster status is returned, where you can check that the cluster is operating as expected.

11. Add IP addresses for the Master MDM (presently Slave MDM) by following steps 2, 3, 5, 7, and 8.

12. Optional: Switch MDM ownership back to the original MDM:

```
scsi --switch_mdm_ownership --new_master_mdm_id MDM_ID
```

### Configure SDC access to the MDM

You can configure SDC access to the MDM through the system.

To harden SDC access to the MDM, it is possible to restrict access, pending approval of the SDC by the system. The default system setting is full access (restricted SDC mode is disabled). When the restricted SDC mode is enabled, volumes can only be mapped to “approved” SDCs. Approval is obtained by issuing the `--add_sdc` command for each SDC. You can set restricted mode before or after SDCs have been added to your network.

You can use the following commands:

<table>
<thead>
<tr>
<th>Action</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable restricted SDC mode</td>
<td><code>set_restricted_sdc_mode</code> command</td>
</tr>
<tr>
<td>Add an SDC to the approved list, when restricted SDC mode is enabled</td>
<td><code>--add_sdc</code></td>
</tr>
</tbody>
</table>

For more information, see the *VxFlex OS CLI Reference Guide*.

### Configure management session timeout parameters

You can configure the management session idle timeout on each MDM as required by your organization.

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

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

You can modify these parameters, by editing the MDM `conf.txt` file:

- **Linux**: `/opt/emc/scaleio/mdm/cfg/conf.txt`
- **Windows**: `C:\Program Files\emc\scaleio\mdm\cfg\conf.txt`
1. To configure maximum session length, edit the value of the `user_session_hard_timeout_secs` parameter. The minimum is 10 seconds, maximum 10 years, and default 8 hours.

2. To configure session idle time, edit the value of the `user_session_timeout_secs` parameter. The minimum is 10 seconds, maximum 3 months, default 10 minutes.

3. After changing the parameters, restart the MDM slaves. After the MDM slaves are up, reassign the Master MDM to one of the slaves and then restart the MDM service (delete and create service).

4. To ensure persistence, make these changes on every MDM.

**Configure virtual IP addresses using the VxFlex OS Installer**

Configure virtual IP addresses using the Maintain menu in the VxFlex OS Installer.

**Before you begin**

For data networks using IPv6, if you plan to implement a floating virtual IP address for the MDM, disable the IPv6 DAD setting on the server's relevant interfaces, using the command:

```
sysctl net.ipv6.conf.<interface_name>.dad_transmits=0
```

**About this task**

You can assign a virtual IP address for each possible MDM manager, which is used for communications between the MDM cluster and SDCs. Only one virtual IP address can be mapped to each NIC, with a maximum of four virtual IP addresses per system. The VxFlex OS Installer can be used to assign new virtual IP addresses only; to change or remove existing virtual IP addresses, use the appropriate CLI commands.

**Procedure**

1. From the VxFlex OS Installer, select Maintain.
2. Select Set Virtual IPs.
3. In the Set Virtual IPs for VxFlex OS system screen, type the MDM password.
4. For each MDM that you wish to set a virtual IP address, enter a virtual IP address and the NIC to which it will be mapped. For each new virtual IP address, enter the virtual IP address and NIC name for each MDM to which it will be mapped.

With the VxFlex OS Installer, you can configure NIC names that contain the following characters only: a-z, A-Z, 0-9. If a NIC name contains the "-" or "_" character (for example eth-01), don’t use VxFlex OS Installer. Configure this IP address with the CLI modify_virtual_ip_interfaces command and the --new_mdm_virtual_ip_interface <INTF> parameter.

5. Click Set Virtual IPs.

Results

The virtual IP address is configured and all of the SDCs are updated with the new virtual IP address. See section VxFlex OS plug-in for information on "Configuring virtual IP addresses - VxFlex OS plug-in".
CHAPTER 8
Security

The following topics describe how to configure security for the VxFlex OS system.

- Approving pending security certificates ................................................................. 166
- Default self-signed certificate expires ....................................................................... 166
- Upgrade the VxFlex OS Gateway when a custom certificate is used .................... 166
- Enable LIA security .................................................................................................. 167
- Certificate management for VxFlex OS Gateway .................................................. 167
- Setting up SSH authentication on the VxFlex OS Gateway ..................................... 171
- Configuring SSL component authentication ............................................................. 171
- Configure SDC access to the MDM .......................................................................... 175
- Approved encryption methods ................................................................................ 176
- Login banner overview ......................................................................................... 176
- Change LIA authentication method to LDAP ......................................................... 178
- Add LDAP server .................................................................................................... 179
- Remove LDAP server ............................................................................................. 179
Approving pending security certificates

Approve pending security certificates, and view approved certificates in the System Settings window.

About this task

Note: When there are pending certificates in the system, they are listed in the Backend > Storage view > State Summary table, and in the Monitor > Alerts view.

Procedure

1. From the System Settings menu in the top right corner, select System Settings.
   The System Settings window appears, showing approved and pending certificates.
2. Scroll to connections that are Pending Approval, and expand the rows.
3. For each one, scroll to the bottom of the information about the required certificate, and click Confirm.

Default self-signed certificate expires

The default self-signed security certificate used on the VxFlex OS Gateway expires after approximately one year. A new one can be created using the Java keytool utility.

The self-signed security certificate used on the VxFlex OS Gateway expires after approximately one year, and needs to be replaced. If your self-signed security certificate expires, you can create a new one using the Java keytool utility.

When you upgrade the VxFlex OS Gateway, the self-signed certificate is automatically replaced with a new one, and therefore will only need to be replaced after one year from the upgrade date.

Upgrade the VxFlex OS Gateway when a custom certificate is used

Save a copy of the certificate before upgrading the VxFlex OS Gateway.

If a custom security certificate is used on the VxFlex OS Gateway (Windows and Linux environments), you must save a copy of the file where certificates are stored (* .keystore file) and the catalina.properties file before you upgrade the VxFlex OS Gateway. After the upgrade is complete, you must copy these files back to their original location.

The default file locations, per operating system, are:

Linux:
/opt/emc/scaleio/gateway/conf/catalina.properties
/opt/emc/scaleio/gateway/conf/certificates/.keystore

Windows (64 bit):
C:\Program Files\EMC\ScaleIO\Gateway\conf\catalina.properties
C:\Program Files\EMC\ScaleIO\Gateway\conf\certificates\.keystore
Enable LIA security

You can enable LIA security.

Procedure

1. In the VxFlex OS Installer, select the Maintain tab.
2. Click Security Settings and select Enable LIAs Security.
3. Enter the MDM password in the Confirm Enable LIAs security of your VxFlex OS system box.
4. Click Enable LIAs Security.

Certificate management for VxFlex OS Gateway

This section explains how to replace the VxFlex OS Gateway’s self-signed security certificate with your organization’s “trusted” certificate, and how to create a new “trusted” certificate. The VxFlex OS 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.

Procedure

1. Find the location of keytool on your server, and open it.
   It is a part of the Java (JRE or JDK) installation on your server, in the bin directory. For example:
   - C:\Program Files\Java\jdk1.8.0_25\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 VxFlex OS Gateway installation directory for the newly created keystore file. This will prevent it from being overwritten when the VxFlex OS Gateway is upgraded or reinstalled.

3. If you already have a Certificate Signing Request (CSR), skip this step.
If you need a CSR, generate one by typing the following command. (If you did not define a keystore password in the previous step, omit the password flags.)

```
keytool -certreq -keyalg RSA -alias <YOUR_ALIAS> -file certreq.txt -keystore <PATH_TO_NEW_KEYSTORE_FILE> -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 VxFlex OS Gateway installation directory.

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

```
keytool -import -alias root -keystore <PATH_TO_NEW_KEYSTORE_FILE> -trustcacerts -file <LOCATION_OF_YOUR_root.cer_FILE> -storepass <KEYSTORE_PASSWORD> -keypass <KEYSTORE_PASSWORD>
```

**Note:** The certificate must be in x.509 format.

If a message appears saying that the root is already in the system-wide store, import it anyway.

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

```
keytool -import -alias intermediateCA -keystore <PATH_TO_NEW_KEYSTORE_FILE> -trustcacerts -file <LOCATION_OF_YOUR_intermediate.cer_FILE> -storepass <keystore password> -keypass <keystore password>
```

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

7. Install the SSL Certificate under the same alias that the CSR was created from (<YOUR_ALIAS> in previous steps), by typing the command (if you did not define a keystore password, omit the password flags):

```
keytool -import -alias <YOUR_ALIAS> -keystore <PATH_TO_NEW_KEYSTORE_FILE> -trustcacerts -file <LOCATION_OF_SSL_CERTIFICATE> -storepass <keystore password> -keypass <keystore password>
```

8. Edit the following items in the file `<VxFlex_OS_GATEWAY_INSTALLATION_DIRECTORY>\conf\catalina.properties`:

   a. `keystore.file=<PATH_TO_NEW_KEYSTORE_FILE>`
   b. `keystore.password=<PASSWORD_DEFINED_DURING_KEYSTORE_CREATION>`

   If you did not define a password, the default password is `changeit`.

9. Restart the VxFlex OS Gateway service:

   - Windows: From the Windows *Services* window, restart the *EMC ScaleIO Gateway*. 

   - Linux: Execute the following command:
     ```
     systemctl restart vxflexos-gateway
     ```
Replace the default self-signed security certificate with your own self-signed certificate

Replace the default self-signed security certificate with your own self-signed security certificate.

About this task

Procedure

1. Find the location of keytool on your server, and open it.
   
   It is usually a part of the Java (JRE or JDK) installation on your server, in the bin directory. For example:
   
   - C:\Program Files\Java\jdk1.7.0_25\bin\keytool.exe
   - /usr/bin/keytool

2. Generate your RSA private key:

   keytool -genkey -alias <YOUR_ALIAS> -keyalg RSA -validity 360 -keysize 2048 -keystore <PATH_TO_NEW_KEYSTORE_FILE>

   a. If you want to define a password, add the following parameters to the command. Use the same password for both parameters.

   -storepass <KEYSTORE_PASSWORD> -keypass <KEYSTORE_PASSWORD>

   Note: Specify a directory outside the VxFlex OS Gateway installation directory for the newly created keystore file. This will prevent it from being overwritten when the VxFlex OS Gateway is upgraded or reinstalled.

3. Edit the following items in the file VxFlex_OS_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 VxFlex OS Gateway service:

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

   service scaleio-gateway restart

Results

Replacement of the security certificate is complete.
Non-default certificate use before and after a VxFlex OS Gateway upgrade

When using a non-default security certificate, you must perform certain actions before and after upgrading the VxFlex OS Gateway.

About this task

If a non-default security certificate is used on the VxFlex OS Gateway in Windows and Linux environments (for example, if the certificate is signed by the user organization CA), you must save a copy of the certificate and the catalina file before the upgrade, and restore them to their original location after the upgrade.

Procedure

1. Before commencing the VxFlex OS Gateway upgrade, locate the *.keystore file and the catalina.properties file, and save a copy of them in another location.

   The default file locations, per operating system, are:
   - Linux:
     - /opt/emc(scaleio/gateway/conf/catalina.properties
     - /opt/emc(scaleio/gateway/conf/certificates/.keystore
   - Windows (64 bit):
     - C:\Program Files\EMC\ScaleIO\Gateway\conf\catalina.properties
     - C:\Program Files\EMC\ScaleIO\Gateway\conf\certificates\keystore

2. After the upgrade is complete, copy these files back to their original location.

Configure OpenStack interoperation with the VxFlex OS Gateway

Configure the VxFlex OS Cinder driver to verify the VxFlex OS Gateway SSL certificate.

About this task

The OpenStack VxFlex OS Cinder driver communicates with the VxFlex OS Gateway through HTTPS (in other words, over SSL). By default, the driver ignores the gateway SSL certificate verification. However, the VxFlex OS 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 VxFlex OS driver to communicate with the VxFlex OS Gateway.

About this task

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

1. Create a keystore file (.JKS):
   ```
   keytool -genkeypair -keysize 1024 -alias herong_key -keypass keypass -keystore herong.jks -storepass jkspass
   ```

2. Export the keystore file to a .PEM file:
   ```
   keytool -exportcert -alias herong_key -keypass keypass -keystore herong.jks -storepass jkspass -rfc -file keytool_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.

Setting up SSH authentication on the VxFlex OS Gateway

A manually generated public-private key pair can be used to perform SSH key authentication, instead of passwords, between the VxFlex OS Gateway and VxFlex OS system servers. For more information, see “Using SSH authentication on the VxFlex OS Gateway” in the VxFlex OS Deployment Guide.

Configuring SSL component authentication

VxFlex OS uses SSL authentication to authenticate both internal system components, and communication between the MDM and external components such as the VxFlex OS Gateway, VxFlex OS GUI clients, vSphere plug-in, and CLI clients. Secure communication is typically installed and configured by default during system deployment.

**Note:**
If your system has been upgraded from a version earlier than version 2.0, or if secure communication between components was disabled during installation, follow the instructions provided in the section “Switching to secured authentication mode” in the VxFlex OS Deployment Guide.

Internal component authentication

When this feature is enabled, the MDM generates a self-signed certificate for itself, and the SDSs generate certificates signed by the MDM’s certificate. The MDM has a single certificate for the entire cluster. The certificate is stored in the MDM repository.

Each SDS has its own SSL certificate file:
- **Linux:** `/opt/emi/cscaleio/sds/fgf/sds_certificate.pem`
- **Windows:** `C:\Program Files\emc\scaleio\sds\cfg\sds_certificate.pem`

When an SDS is added to the cluster, the MDM receives a CSR (Certificate Signing Request) from the SDS, signs it with its own internal certificate and returns it to the SDS to be stored in its local key-store. If the SDS disconnects and reconnects, the MDM must authenticate it.

External component authentication

Secure communications can be performed between the MDM and the following external components, and are typically enabled during deployment of the system:
VxFlex OS Gateway—The VxFlex OS Gateway maintains the SSL certificates for itself and for the following components:

- SNMP
- REST API
- VxFlex OS Installer
- vSphere plug-in
- VxFlex OS GUI
- CLI

Workflow for self-signed security certificates

About this task

The system generates and signs self-signed certificates automatically when secure communication is enabled, and no user intervention is required. If you want to replace these certificates with new self-signed ones, follow this workflow:

Procedure

1. Run the command `scli --generate_mdm_certificate`.

   To run CLI commands, you must be logged in. Actual command syntax is operating-system dependent. For more information, see the VxFlex OS CLI Reference Guide.

2. When using the CLI, on the first connection to the MDM, the CLI will display the MDM's certificate and will prompt the user to approve the certificate.

   Upon approval, the trusted certificate will be saved.

3. When using the VxFlex OS GUI, approve the MDM certificate at login, and then approve other certificates using the System Settings menu, Renew Certificates option.

Workflow for externally signed security certificates

About this task

The system generates and signs self-signed certificates automatically when secure communication is enabled, and no user intervention is required. If you want to replace these certificates with ones signed by an external Certificate Authority, follow this workflow:

Procedure

1. Log in to the system using the `scli --login` command as either a root user (on Linux) or as an administrator (on Windows).

2. Generate a CSR file, using the command `scli --generate_mdm_csr_file --target_mdm_ip <IP_ADDRESS>`.

   A file called `mdm-target_hostname.csr` will be created in the location:

   a. Linux: `/opt/emc/scaleio/mdm/cfg`

   b. Windows: `C:\Program Files\emc\scaleio\mdm\cfg`

   To run CLI commands, you must be logged in. Actual command syntax is operating-system dependent. For more information, see the VxFlex OS CLI Reference Guide.

3. Submit the CSR file created in the previous step to your Certificate Authority.

   The Certificate Authority must sign your CSR and return two files to you:
a. Certificate for your MDM
b. Certificate Authority “Trusted” or “Root” certificate

4. Save the signed certificate for the MDM in the location:
   a. Linux: /opt/emc/scaleio/mdm/cfg
   b. Windows: C:\Program Files\emc\scaleio\mdm\cfg

5. Manually change the MDM certificate’s file name to mdm_signed_certificate.pem.

6. Run the following script on the directory:

   ```
   ./apply_signed_certificate.py --mdm_ip <IP_address> --local_mdm_ip <IP_address>
   ```

   where --mdm_ip is the IP address of the Master MDM, and --local_mdm_ip is the IP address of the MDM where you want to change the certificate.

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

   ! Note:
   This step changes the MDM certificate, and might cause a brief single point of failure period (switch ownership).

7. For all external components that will communicate with the MDM (VxFlex OS GUI, CLI, vSphere Plugin, REST, VxFlex OS Installer) add the Trusted or Root certificate from the Certificate Authority to each component.

   The Trusted/Root certificate must be added to the file called `truststore.jks`, using Keytool.

   For more information, see "Using Keytool to add certificates to external components".

8. When using the CLI, on the first connection to the MDM, the CLI will display a message similar to the following:

   ```
   [root@112CC-4~]# scli --login --username admin --password Scaleio018
   Certificate required for issuer: /C=US/ST=MA/L=Hopkinton/O=EMC-Scaleio1213/CN=Scaleio018
   Please add the certificate with scli --add_certificate
   ```

   Add the Trusted/Root certificate using the --add_certificate command. For more information, see the VxFlex OS CLI Reference Guide.

Using Keytool to add certificates to external components

This topic explains how to add Certificate Authority certificates to VxFlex OS external components. The `truststore.jks` file located on all components saves all the MDM/LIA certificates approved by the client. The file's location depends on the management client and operating system:

VxFlex OS Gateway
- Linux:
Security

/opt/emc/scaleio/gateway/webapps/ROOT/WEB-INF/classes/certificates

- **Windows (64-bit):**
  C:\Program Files\EMC\ScaleIO\Gateway\webapps\ROOT\WEB-INF\classes\certificates

**VxFlex OS GUI**

- **Linux:**
  /opt/emc/scaleio/gui/certificates

- **Windows:**
  C:\Users\[user_name]\AppData\Roaming\EMC\scaleio\certificates

**vSphere**

- **Linux:**
  $HOME/.vmware/scaleio/certificates

- **Windows:**
  C:\Users\[user_name]\AppData\Roaming\VMware\scaleio\certificates\truststore.jks
  C:\Windows\System32\config\systemprofile\AppData\Roaming\VMware\scaleio\certificates

**Using Keytool**

Use the Java Keytool utility to modify or view the content of the trust store file. The remainder of this topic lists some useful Keytool commands. Keytool is a part of the Java (JRE or JDK) installation and can be found in the bin directory. You can add -storepass changeit to all commands that require a password. The password for the trust store is "changeit" (Java default).

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The certificate alias must be unique in the trust store file. We usually use the certificate's full subject.</td>
</tr>
<tr>
<td>For example: givenname=mdm, ou=asd, o=emc, l=hopkinton, st=massachusetts, c=us, cn=centos-6.4-adi5</td>
</tr>
</tbody>
</table>

- **List the certificates in the trust store:**

  ```bash
dkeytool -list -v -keystore [path_to_certificates_folder]/truststore.jks
  ```

  **Example:**

  ```bash
dkeytool -list -v -keystore C:\Users\cj\AppData\Roaming\EMC\scaleio\certificates\truststore.jks
  ```

- **Check a particular entry using an alias:**

  ```bash
dkeytool -list -v -keystore [path_to_certificates_folder]/truststore.jks -alias [unique_alias] -storepass changeit
  ```
Configure SDC access to the MDM

You can configure SDC access to the MDM through the system.

To harden SDC access to the MDM, it is possible to restrict access, pending approval of the SDC by the system. The default system setting is full access (restricted SDC mode is disabled). When the restricted SDC mode is enabled, volumes can only be mapped to “approved” SDCs. Approval is obtained by issuing the `--add_sdc` command for each SDC. You can set restricted mode before or after SDCs have been added to your network.

You can use the following commands:

<table>
<thead>
<tr>
<th>Action</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable restricted SDC mode</td>
<td><code>set_restricted_sdc_mode command</code></td>
</tr>
</tbody>
</table>
Add an SDC to the approved list, when restricted SDC mode is enabled --add_sdc

For more information, see the VxFlex OS CLI Reference Guide.

Approved encryption methods

A specific set of encryption methods are approved for use with your system. These approved methods are:

- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256

Note: In order to use CURL with VxFlex OS Gateway v2.0.0.3 and higher on a server running RHEL6, upgrade the NSS package to 3.21.0. (using YUM).

Login banner overview

A login banner is a text file that is displayed upon login to the system. It can be used to communicate messages or to obtain user consent to real-time monitoring of information and retrieval of stored files.

When the login banner is set up, it appears during the system login process before the login credential prompts. The login banner displays differently in the VxFlex OS GUI and CLI interfaces:

- **VxFlex OS GUI:**
  - When logging in, the login banner is displayed, and must be approved.
- **CLI:**
  - When logging in, the user is prompted to press any key, after which the banner is displayed.
  - To continue, the banner must be approved.

Limitations:
- Only users with administrative security rights can set up, update, or remove the login banner.
Set up a login banner using the CLI

Use the CLI to set up, modify, or stop displaying a login banner.

Before you begin

Ensure that you have access to the IP address of the Master MDM.

Procedure

1. Log in to VxFlex OS using the IP address of the Master MDM.
2. Perform the desired operation:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Create (or modify) a new banner | a. Create a text file (or modify an existing file) with the message that you want to display in the login banner.  
|                               | b. Run the following command:  
|                               | scli --set_login_banner --filename <FILENAME>  
|                               | where <FILENAME> is the path of the login banner text file. The login banner is displayed the next time a user logs in to VxFlex OS. |

| Stop displaying the banner   | a. Run the following command:  
|-------------------------------| scli --set_login_banner --remove_banner |

Upload a login banner using the VxFlex OS Installer

Use the Installer to upload a login banner that displays upon logging into the VxFlex OS system.

About this task

The MDM credentials are stored in the Lockbox

Procedure

1. In the VxFlex OS Installer, select the Maintain tab.
2. Click Security Settings and select Set Login Banner.
3. In the Set Login Banner for VxFlex OS system, type the MDM password.
4. Click Set Login Banner

Enable/disable preemptive acceptance of the login banner

Preemptive acceptance of the login banner allows the user to bypass the login banner, for example, when running scripts. A user with admin security rights can enable or disable the option.
of preemptive acceptance. By default, preemptive acceptance is enabled and the login banner can be bypassed using a CLI command.

**Before you begin**

To enable or disable the preemptive acceptance option, you must have administrative rights.

**Procedure**

1. Log in to VxFlex OS:

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

2. Run the following command to enable preemptive acceptance:

   ```
   scli --set_cli_login_banner_preemptive_acceptance --enable
   ```

3. Run the following command to disable preemptive acceptance:

   ```
   scli --set_cli_login_banner_preemptive_acceptance --disable
   ```

**Activate preemptive acceptance of the login banner**

When preemptive acceptance of the login banner is enabled (default), you can log in to VxFlex OS in a special way that activates preemptive acceptance of the login banner.

**Before you begin**

Preemptive acceptance of the login banner is enabled.

**Procedure**

1. Log in to VxFlex OS with the `accept_banner_by_scripts_only` parameter:

   ```
   scli --login --username <USERNAME> --accept_banner_by_scripts_only
   ```

   where `<USERNAME>` is the user running the script.

**Change LIA authentication method to LDAP**

Use the VxFlex OS Installer to change the LIA authentication method to LDAP.

**About this task**

After upgrade, you can update the configuration from a native user to LDAP user. You first must add an LDAP Server to the system.

**Procedure**

1. In the web browser, go to the IP address of your system's VxFlex OS Gateway.

2. Log in to the VxFlex OS Gateway.

3. From the **Maintain** tab, click **Security Settings** and select **Change LIAs authentication method to LDAP**.

   The **Change LIAs authentication method to LDAP for VxFlex OS system** window is displayed.
4. Enter the admin password to the MDM in the **MDM admin password** box.
5. Enter the user name in the **LDAP User Name** box.
6. Enter the password to access the LDAP server in the **LDAP password** box.
7. Select **Force LDAP authentication mode** to force users to enter LDAP User Name and LDAP password when logging in to the VxFlex OS system.
8. Click **Change LIAs authentication method to LDAP**.

**Results**
Use LDAP credentials to login to system.

**Add LDAP server**
Add LDAP servers to your VxFlex OS system post installation.

**About this task**

> **Note:** You can only add a max of eight servers.

**Procedure**
1. In the web browser, go to the IP address of your system's VxFlex OS Gateway.
2. Log in to the VxFlex OS Gateway.
3. From the **Maintain** tab, click **Security Settings** and select **Add LDAP Server**
   The **Add LDAP Server to VxFlex OS system** dialog box is displayed.
4. Enter the admin password to the MDM in the **MDM admin password** box.
5. Enter the URI of the LDAP server in the **Server URI** box.
6. Enter the LDAP group identifier that you can retrieve from the LDAP server in the **Group** box.
7. Enter the LDAP BaseDN identifier that you can retrieve from the LDAP server in the **BaseDN** box. Run the query on the server to retrieve the Base DN.
8. Click **Add LDAP Server**.

**Remove LDAP server**
You can remove LDAP servers from the VxFlex OS system.

**Procedure**
1. In the web browser, go to the IP address of your system's VxFlex OS Gateway.
2. Log in to the VxFlex OS Gateway.
3. From the **Maintain** tab, click **Security Settings** and select **Remove LDAP Server**
   The **Remove LDAP Server from VxFlex OS system** dialog box is displayed.
4. Enter the admin password to the MDM in the **MDM admin password** box.
5. Enter the URI of the LDAP server in the **LDAP Server URI** box.
6. Click **Remove LDAP Server**.
The following topics describe how to create and manage users.

- MDM and LDAP integration in an AMS managed system ..................................................... 182
- User roles ............................................................................................................................. 182
- Setting the User Authentication Method ............................................................................ 183
- Adding and modifying local users ..................................................................................... 184
- Deploying VxFlex OS using a non-root user ........................................................................ 189
MDM and LDAP integration in an AMS managed system

VxFlex OS supports local domain user authentication, and LDAP domain authentication. In addition, secure authentication is used between system internal and external components. This chapter provides the CLI commands used to create and manage VxFlex OS users. The REST API can also be used to configure LDAP. For more information, see the operations for MDM clusters in the VxFlex OS REST API Reference Guide.

- To set up local domain users, follow the instructions in this chapter.
- To set up LDAP users, see a detailed explanation in the document VxFlex OS User Roles and LDAP Technical Notes. In general, the following steps must be performed:
  1. Add LDAP service to the MDM.
  2. Create Active Directory (AD) groups that correspond to the user roles offered by VxFlex OS.
  3. Set the system-wide authentication method (use with caution, because it is complex to roll-back this operation).
  4. Log in again to apply the changes that you made.

User roles

The authorization permissions of each user role are defined differently for local authentication, and for LDAP authentication. Although the role names are similar, the permissions granted to them are not.

User roles defined in the LDAP domain are mutually exclusive, with no overlap—with the exception of the Configurator role. If you want to give an LDAP user permission to perform both monitoring and configuration roles, for example, assign that user to both the Backend/Frontend Configurator and Monitor LDAP groups.

The Configurator and Super User roles do not exist at all for LDAP.

The following table describes the permissions that can be defined for local domain users and for LDAP domain users.

<table>
<thead>
<tr>
<th>User role</th>
<th>Query</th>
<th>Configure parameters</th>
<th>Configure user credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Local</td>
<td>LDAP</td>
</tr>
<tr>
<td>Monitor</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Configurator (this role is only applicable for local users)</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Yes (an aggregation of both Frontend and Backend Configurator)</td>
</tr>
<tr>
<td>Backend Configurator</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 2 Local and LDAP user roles and permissions (continued)

<table>
<thead>
<tr>
<th>User role</th>
<th>Query</th>
<th>Configure parameters</th>
<th>Configure user credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td></td>
<td>Local</td>
<td>LDAP</td>
</tr>
<tr>
<td>LDAP</td>
<td></td>
<td>Local</td>
<td>LDAP</td>
</tr>
<tr>
<td>SDSs, Devices, other</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system settings)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frontend Configurator</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrator</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Roles</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Super User (only one</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Yes</td>
</tr>
<tr>
<td>Super User is allowed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>per system, and it must</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>be a local user)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Setting the User Authentication Method

set_user_authentication_method

Set the user authentication method for the system.

⚠️ **WARNING** Use this command with caution. The operation is complex to roll back.

ℹ️ **Note:** For details about setting up LDAP, refer to the *VxFlex OS User Roles and LDAP Usage Technical Notes.*

**Syntax**

```
scli --set_user_authentication_method (--ldap_authentication | --native_authentication | --native_and_ldap_authentication) [--i_am_sure]
```

**Parameters**

--ldap_authentication

LDAP-based authentication method where users are managed on an LDAP-compliant server. Configure LDAP service and LDAP user before switching to this authentication method.

--native_authentication

Native authentication method where users are managed locally in the system
--native_and_ldap_authentication
A hybrid authentication method. Both LDAP and Native users may log in to the system after it is set.

--i_am_sure
Skip the safety questions for command execution. (For example: “This could damage the stored data. Are you sure?”)

Example

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

**Adding and modifying local users**

Users with the administrator role can manage system users, including adding new users and deleting existing users, modifying user credentials, and resetting user passwords.

The following CLI commands allow you to manage local users.

**add_user**

Add a user to the system. A randomly generated password for the created user is returned.

This command is available only to administrator users.

Each user name should conform to the following rules:

1. Contains fewer than 32 characters
2. Contains only alphanumeric and punctuation characters (when punctuation characters are being used, you may need to use the " or ' characters in order to allow it).
3. Is unique within the object type

**Syntax**

```bash
scli --add_user --username <NAME> --user_role {Monitor | Configure | BackEndConfigure | FrontEndConfigure | Security | Administrator}
```

**Parameters**

--username <NAME>
User name to add to the system

--user_role {Monitor | Configure | BackEndConfigure | FrontEndConfigure | Security | Administrator}
Role of the user: Monitor, Configurator, Backend Configurator, Frontend Configurator, Security, or Administrator. For information on user roles, see the VxFlex OS User Guide.

**Example**

```bash
scli --add_user --username siuser2 --user_role Configure
```
delete_user

Delete the specified user from the system.
This command is available only to administrator users.

Syntax

```
scli --delete_user (--user_id <ID> | --username <NAME>)
```

Parameters

--user_id <ID>
ID of the user to be deleted

--username <NAME>
Username of the user to be deleted

Example

```
scli --delete_user --username siuser2
```

modify_user

Modify the user role of the specified user in the system.
This command is available only to administrator users.

Syntax

```
scli --modify_user (--user_id <ID> | --username <NAME>) --user_role {Monitor | Configure | BackEndConfigure | FrontEndConfigure | Security | Administrator}
```

Parameters

--user_id <ID>
User ID of the user to modify

**Note:** The user ID is displayed when you create the user. To find this ID at a later time, use the `query_user` command.

--username <NAME>
User name of the user to modify

--user_role {Monitor | Configure | BackEndConfigure | FrontEndConfigure | Security | Administrator}
Role of the user: Monitor, Configurator, Backend Configurator, Frontend Configurator, Security, or Administrator. For information on user roles, see the VxFlex OS User Guide.

Example

```
scli --modify_user --username siuser3 --user_role Monitor
```
**query_users**

Display all the users defined in the system, with their roles and user ID.

**Syntax**

```bash
scli --query_users
```

**Parameters**

None.

**Example**

```bash
scli --query_users
```

**query_user**

Display information about the specified user.
This command is available only to administrator users.

**Syntax**

```bash
scli --query_user (--user_id <ID> | --username <NAME>)
```

**Parameters**

```
--user_id <ID>
User's ID number

---Note: The user ID is displayed when you create the user. To find this ID at a later time, use the query_user command.

--username <NAME>
Name of the user
```

**Example**

```bash
scli --query_user --username sio_user
```

**reset_password**

Generate a new password for the specified user. The user must change the password again after logging in with the generated password.

This command is available only to administrator users.

**Syntax**

```bash
scli --reset_password (--user_id <ID> | --username <NAME>)
```
Parameters

--user_id <ID>
User ID of the user whose password will be reset

| Note: The user ID is displayed when you create the user. To find this ID at a later time, use the query_user command. |

--username <NAME>
User name of the user whose password will be reset

Example

```
scli --reset_password --username siuser3
```

set_password

Change the password of the user currently logged in to the system.

This command is available only to administrator users.

Syntax

```
scli --set_password [--old_password <OLD_PASSWORD>] [--new_password <NEW_PASSWORD>]
```

Parameters

None.

--old_password <OLD_PASSWORD>
User's current password

--new_password <NEW_PASSWORD>
User's new password

| Note: In Linux, to prevent the password from being recorded in the history log, omit the old_password or new_password flag and enter the password interactively. |

Example

```
scli --set_password --old_password 1!2@3A --new_password P9*7&6
```

Password rules

The password must conform to the following rules:

1. Contains between six and 31 characters.
2. Contains characters from at least three of the following groups: [a-z], [A-Z], [0-9], special characters (!@#$ …)
3. The current password is not allowed.
disable_admin

Disables the default Superuser.

The Superuser is the default user for setting up the system, and has all the privileges of all user roles. In some cases you may need to disable the Superuser in order to ensure that all users are associated with specific user roles.

⚠️ Note: To re-enable the Superuser, use the reset_admin command.

Syntax

```bash
scli --disable_admin
[--i_am_sure]
```

Parameters

`--i_am_sure`

Skip the safety questions for command execution.

Example

```bash
scli --disable_admin --i_am_sure
```

Reset the admin user password

You can reset the password of the default admin user (Superuser) using the combination of a file written to the MDM and the reset_admin CLI command.

Before you begin

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.

Procedure

1. Create a text file named `MDM_SERVICE_MODE` on the MDM in the location corresponding to your operating system:
   - Windows: `C:\Program Files\emc\scaleio\MDM\logs\MDM_SERVICE_MODE`
   - Linux: `/opt/emc/scaleio/mdm/logs/MDM_SERVICE_MODE`
2. In the body of the file, type the text `Reset Admin`, and save the file.
3. From the CLI, run the `reset_admin` command:

   ```bash
   scli --reset_admin
   ```

Results

The admin user password is reset to admin.
reset_admin

Reset the default Superuser.
Reset the password of the default admin user with Superuser permissions.

```
scli --reset_admin
  [--i_am_sure]
```

**Syntax**

```
scli --reset_admin
  [--i_am_sure]
```

**Parameters**

```
--i_am_sure
  Skip the safety questions for command execution.
```

**Example**

```
scli --disable_admin --i_am_sure
```

---

## Deploying VxFlex OS using a non-root user

VxFlex OS can be deployed or extended in Linux environments using a non-root sudo user in non-interactive mode.

Sudo is a program that allows a user to run or install a program as the root user. A sudo user can be created to deploy VxFlex OS.

In order to successfully deploy or extend VxFlex OS with a non-root user, the non-root user must meet the following conditions:

- The username included in the CSV file must already exist.
- The non-root user must be a sudo user.
- The non-root user must be in non-interactive mode.
- The requirement for TTY must be disabled.

In the CSV file used for deployment, you must indicate that you are intending to use a sudo non-root username by appending the string "(sudo)" to the user name in the Username field. For example, if you are using a non-root user with the username "non_root", enter the string "non_root(sudo)" in the username field of the CSV file.

---

## Configure a non-root non-interactive sudo user

In Linux, you can deploy or extend VxFlex OS with a non-root user. You must configure a non-root sudo user in non-interactive mode.

**Before you begin**
About this task
The following procedure details one method for configuring a non-root non-interactive sudo user. Perform the commands from the operating system console of where you want the VxFlex OS Gateway to deploy VxFlex OS.

Procedure
1. Create a user group named "admin".
   ```bash
groupadd admin
   ```
2. Create a user named "non_root" and add it to the admin group.
   ```bash
useradd -G admin non_root
   ```
3. Change the password of the non_root user.
   ```bash
passwd non_root
   ```
   When prompted, enter the new password and then confirm it by entering it again.
4. Open the sudoers /etc/sudoers file for editing.
   ```bash
vi /etc/sudoers
   ```
5. Search the sudoers file for "## Same thing without a password".
   ```bash
:s/## Same thing without a password
   ```
6. In the line below the search result, add the text %admin ALL=(ALL) NOPASSWD: ALL to the file.
7. Search the sudoers file for "Defaults requiretty", and replace it with Defaults ! requiretty.
8. Exit the vi editor by typing the following command to exit: :wq!
9. Create a hidden directory in the non_root user's home directory to store the SSH configuration.
   ```bash
mkdir /home/non_root/.ssh
   ```
10. Copy the SSH configuration from the root user to the non_root user's directory.
    ```bash
    cp -rf /root/.ssh/* /home/non_root/.ssh/
    ```
CHAPTER 10
Fault reporting features

The following topics describe how to configure fault reporting features in the VxFlex OS system.

- General................................................................................................................................ 192
- Configure SNMP properties after deployment.....................................................................192
- Configure Dynamic Host Name resolution for SNMP in VxFlex OS...................................... 192
- Configure VxFlex OS Gateway properties............................................................................ 194
General

SNMP traps are implemented as part of the VxFlex OS Gateway, using SNMP v2. UDP transport is used for SNMP, and the default port for trap communication is 162. The SNMP feature is disabled by default. If you want to use the SNMP feature, enable it by editing the `gatewayUser.properties` file. For more information, see "Configure SNMP properties after deployment" in the Customize and Configure Guide.

The SNMP trap sender uses a proprietary/custom MIB called `scaleio.mib`. This MIB file is located on the VxFlex OS Gateway server, in the `webapps/ROOT/WEB-INF/classes` folder under the VxFlex OS Gateway installation directory. All traps are sent using a single notification type with a unique identification number (OID). All the SNMP traps contain variable bindings for severity; alert type, which is the alert classification text; the ID of the source object for which the alert was created; and an action code, which is the event number.

When using HP OpenView, ensure that the Dell EMC MIB file is loaded together with the VxFlex OS MIB file, or save the Dell EMC MIB file in the same directory as the VxFlex OS MIB file.

The alerts are calculated based on MDM polling. A trap will be sent the first time that an event occurs, and will be sent again if the resend interval has passed and the alert is still in effect. The resend frequency parameter can be configured using the Settings window in the VxFlex OS GUI.

Only SNMP traps are supported, and are initiated by the VxFlex OS SNMP traps manager. GET/SET operations are not supported (or more specifically, GET/GET NEXT/GET BULK/SET/INFORM/RESPONSE).

In addition to SNMP traps, alert messages are also displayed in the VxFlex OS GUI.

To enable SNMP-based fault reporting, both the VxFlex OS Gateway and the SNMP trap receivers must be configured. Traps can be sent to up to two SNMP trap receivers. The VxFlex OS Gateway service must be restarted after configuration.

Configure SNMP properties after deployment

These procedures are mandatory for VMware-based systems where the SNMP feature is required. For other operating systems, configuration can be done either during deployment, or afterwards, using the instructions in this section.

The following procedures are required to enable the SNMP feature:

1. Create the Lockbox
2. Configure SNMP

Configure Dynamic Host Name resolution for SNMP in VxFlex OS

Dynamic Host Name resolution and SNMP must be configured in the VxFlex OS Gateway and on the DNS server to enable SNMP to forward traps to the SNMP trap receiver.

Before you begin

Ensure that SNMP is already enabled and that SNMP traps are being received by at least one SNMP trap receiver, configured with an IP address.

About this task

The following procedures are required in order to set up a Dynamic Host Name resolution:
- On the VxFlex OS Gateway, add the host name of the SNMP trap receiver to the appropriate parameter in the `gatewayUser.properties` file
- On the DNS server, configure the SNMP trap receiver properties, in order to support dynamic host name resolution
- On the DNS server, reduce the "Time To Live" (TTL) setting for the SNMP trap receiver

Procedure

1. On the VxFlex OS Gateway, open the `gatewayUser.properties` file.
   - From Linux: `/opt/emc/scaleio/gateway/webapps/ROOT/WEB-INF/classes/gatewayUser.properties`
2. Add the host name of the SNMP trap receiver to the property `snmp.traps_receiver_ip=`. If there is more than one IP address or host name, use a comma-separated list.
3. Save the file and restart the VxFlex OS Gateway service.
4. Verify that traps are being received at all configured trap receiver hosts.
5. On the DNS server, configure dynamic host name resolution support for the trap receiver.
6. On the DNS server, reduce the TTL setting for the trap receiver. For example, on Windows, perform the following:
   a. Open the **DNS manager** window.
   b. Click **View**, and select the **Advanced** option.
   c. Right-click the trap receiver, and select **Properties**. A window similar to the following is displayed:

```
Host (A)

Host (uses parent domain if left blank):

sles12-47

Fully qualified domain name (FQDN):

sles12-47.avib-dns.local

IP address:

10.136.221.47

Update associated pointer (PTR) record

Delete this record when it becomes stale

Record time stamp:

Time to live (TTL):

0:0:0:0.2 (DDDD:HH:MM:SS)
```

   d. At the bottom of the window, in the **Time to live (TTL)** field, change the value from one hour to one or two seconds.
Configure VxFlex OS Gateway properties

Configure VxFlex OS Gateway properties and additional VxFlex OS features, using the gatewayUser.properties file.

Procedure

1. Using a text editor, open the gatewayUser.properties file, located in the following directory on the VxFlex OS Gateway server:

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

2. Edit the file with the desired changes, as follows:

<table>
<thead>
<tr>
<th>Use case</th>
<th>Property</th>
<th>Action</th>
<th>Example</th>
</tr>
</thead>
</table>
|          | add.sds.with.force.on.next.run | Default: false
To enable, set to true.
To disable, set to false. |
| Enable or disable the reuse of previously used devices in the following use cases: | | |
| • Add SDS devices that were used in a previous VxFlex OS system. (Adding them without the true flag will cause deployment failure.) | | |
| • Extend a system with an SDS whose devices were used in a previous system. | | |
| • Extend a system by adding SDSs that are already installed on hosts | | |
| Use a VxFlex OS Gateway that did not initially deploy your VxFlex OS system | mdm.ip.addresses | Add the IP addresses of the system's MDM Master and Slaves, separated by semicolons, to this property. Both management and data IP addresses must be listed. | mdm.ip.addresses=10.76.60.232;10.76.60.233;10.76.60.234;10.76.30.10;10.76.30.11;10.76.30.12 |
| Enable or disable the VxFlex OS Installer | features.enable_IM | Default: true
To disable, set to false. |
| | | | features.enable_IM=false |

Note: After finishing and marking the deployment as complete, the flag will revert to false, so you will need to set it again for future deployments, as necessary.
<table>
<thead>
<tr>
<th>Use case</th>
<th>Property</th>
<th>Action</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use case</strong></td>
<td><strong>Property</strong></td>
<td><strong>Action</strong></td>
<td><strong>Example</strong></td>
</tr>
<tr>
<td>You can completely disable the</td>
<td>features.enable_gateway</td>
<td>Default: true</td>
<td>features.enable_gateway=false</td>
</tr>
<tr>
<td>use of the VxFlex OS Installer</td>
<td></td>
<td>To disable, set to false</td>
<td></td>
</tr>
<tr>
<td>default port, 443, by setting</td>
<td></td>
<td>You can disable the use of the default</td>
<td></td>
</tr>
<tr>
<td>both this property and the</td>
<td></td>
<td>port, 443, by setting both this property</td>
<td></td>
</tr>
<tr>
<td>features.enable_gateway property</td>
<td></td>
<td>and the features.enable_gateway property to</td>
<td></td>
</tr>
<tr>
<td>to false.</td>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Enable VxFlex OS Gateway</td>
<td>features.enable_gateway</td>
<td>Default: true</td>
<td>features.enable_gateway=true</td>
</tr>
<tr>
<td>Default: false</td>
<td></td>
<td>To enable, set to true</td>
<td></td>
</tr>
<tr>
<td>Enable SNMP</td>
<td>features.enable_snmp</td>
<td>Default: false</td>
<td>features.enable_snmp=true</td>
</tr>
<tr>
<td>Set email notification type</td>
<td>notifications.emailSID.1.type</td>
<td>Default (only option currently available):</td>
<td>notifications.emailSID.1.type=callHome</td>
</tr>
<tr>
<td>Set email notification SID:</td>
<td>notifications.emailSID.1.SID</td>
<td>callHome</td>
<td></td>
</tr>
<tr>
<td>email sender identification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(identity shown in the email's</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;From&quot; field)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set email notification user name</td>
<td>notifications.emailSID.1.username</td>
<td>user123</td>
<td></td>
</tr>
<tr>
<td>required only when email</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>notification uses SMTP server</td>
<td>notifications.emailSID.1.smtp</td>
<td>mailhub.lss.emc.com</td>
<td></td>
</tr>
<tr>
<td>authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable SMTP authenticated mode</td>
<td>notifications.emailSID.1.authenticate</td>
<td>Default: false</td>
<td>notifications.emailSID.1.authenticate=false</td>
</tr>
<tr>
<td>for email notification</td>
<td></td>
<td>To disable, set to false</td>
<td></td>
</tr>
<tr>
<td>In addition, configure the user</td>
<td></td>
<td>To enable, set to true</td>
<td></td>
</tr>
<tr>
<td>name, using the property</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>name, and configure the</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP server name</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Use case | Property | Action | Example
--- | --- | --- | ---
Set a custom port for email notification (optional; will override default port number 25) | notifications.emailSID.1.port | Default: 25 | notifications.emailSID.1.port=25
To restrict login to LDAP users only (disable local user login) | gateway-admin.disable.local.login | Default: false To enable, set to true | gateway-admin.disable.local.login=true
Change the name of the VASA Provider replica set. When there are three VASA Providers, a replica set is created during deployment to facilitate communication between VASA Providers. | vasa.provider.replica.set.name | Default: vasa-rs | vasa.provider.replica.set.name=vasa-rs
Enable or disable monitoring of VASA Providers | features.enable_vasa_monitor | Default: true | features.enable_vasa_monitor=true
Set the list of IP addresses for VASA Providers | vasa.provider.ips | A comma-separated list of IP addresses of all the VASA Providers. The installation process sets this property, but it can also be set manually. | vasa.provider.ips=<ip>,<ip>,...
Set the port of the VASA Providers’ REST service, in order to monitor the page http://<ip>:<port>/actuator/health | vasa.provider.monitor.port | Default: 8080 | vasa.provider.monitor.port=8080
Set the number of seconds to sleep between each sample | vasa.provider.monitor.interval.seconds | Default: 60 | vasa.provider.monitor.interval.seconds=60
When installing VASA in a VMware environment, set this property to false in order to enable extending the system | vmware | In a Linux environment, default: false. In a VMware environment, default: true | vmware=false
<table>
<thead>
<tr>
<th>Use case</th>
<th>Property</th>
<th>Action</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>with the VxFlex OS Installer.</td>
<td></td>
<td>When installing VASA in a VMware environment, set the value to false.</td>
<td></td>
</tr>
</tbody>
</table>

3. Save and close the file.

4. Restart the VxFlex OS Gateway service:
   - Windows: From the Windows Services window, restart the **EMC ScaleIO Gateway**.
   - Linux: Type the following command:

   ```
   service scaleio-gateway restart
   ```

**Results**

Configuration is complete.
Fault reporting features
CHAPTER 11

Add, Remove or Rename Components

The following topics describe how to add or remove components from the VxFlex OS system, or rename components.

- Adding components to an existing VxFlex OS environment ................................................. 200
- Remove VxFlex OS .............................................................................................................. 201
- Renaming objects ................................................................................................................ 202
Adding components to an existing VxFlex OS environment

You can expand your VxFlex OS environment as you require.

This section describes how to add components to an existing VxFlex OS installation.

In physical environments, you add components with the VxFlex OS Installer. In VMware environments, you add components with the VMware deployment wizard.

Add components using the VxFlex OS Installer

You can add components using the VxFlex OS Installer

About this task

You first need to update the CSV topology file with the new components, then you can use the VxFlex OS Installer to add them.

The secure communication mode of components must match the mode of the system to which the components are being added. If they do not match, you must either change the mode of the components to be added or change the mode of the system so that they match.

Procedure

1. Follow the procedure described in "Customizable installation using CSV file - hyper-converged system" or "Customizable installation using CSV file - 2-layer system" in the Deploy VxFlex OS Guide.

   ![Note:]
   Use the same LIA password that was configured during initial installation.

2. In the Upload CSV stage, browse to the updated CSV file, and select Add to existing sys.

3. Upload the CSV, and continue as normal.

Add components using the VMware deployment wizard

You can add VxFlex OS components to an existing system using the VMware deployment wizard.

About this task

![Note:]
The following procedure cannot be used to add an SDS component to an existing SVM. To do so, contact Dell EMC Support.

Procedure

1. From the Basic tasks section of the screen, click Deploy VxFlex OS environment.

   The VxFlex OS VMware deployment wizard begins. If you exited the previous deployment before completion, you will be able to return from where you left off.

   ![NOTICE]
The deployment wizard assumes that you are using the provided VxFlex OS OVA template to create the Storage Virtual Machines (SVMs).

2. In the Select Installation screen, select Add servers to a registered VxFlex OS system, and select the system you want to extend.

3. Continue with the deployment steps, adding the new nodes.

   You can skip steps that do not need to be changed.

   ![Note:]
   When adding components, the wizard adjusts the displayed screens to options that are relevant to the current VxFlex OS system.
4. Complete the deployment.

**Note:** After extending an existing SVM with a new VxFlex OS role/component, you must perform manual memory allocation on the SVM, as described in "SVM manual memory location" in the *Deployment Guide*.

### Remove VxFlex OS

You can remove VxFlex OS components and the vSphere plug-in from servers.

To uninstall VxFlex OS, use the VxFlex OS Installer. This requires that the LIA be installed in all nodes to be changed.

When removing RFcache (the `xcache` package) on a Windows server, a server restart is necessary after the removal.

To unregister the vSphere plug-in, see "Unregistering the VxFlex OS plug-in".

### Remove VxFlex OS using the VxFlex OS Installer

You can remove VxFlex OS using the VxFlex OS Installer.

**About this task**

All VxFlex OS components in the system that are being accessed are removed. This information is attained from the LIA that is installed on every node.

**Procedure**

1. Log in to the web client, as described in "Install with the VxFlex OS Installer" from the *Deployment Guide*.
2. From the VxFlex OS Installer, select the **Maintain** tab.
3. In the Maintenance operation screen, type the authentication credentials, then click **Retrieve system topology**.
   
   The system topology is displayed.
4. Click the **Show Uninstall button** link, and confirm enabling this option.
   
   The uninstall operation may take some time, depending on your system topology. This operation cannot be rolled back.
5. Click **Uninstall**.
   
   A confirmation dialog is displayed.

**NOTICE**

Uninstalling an SDC component requires a machine restart. If you are uninstalling SDC components on Windows servers, select to enable automatic restart (on those servers only). Alternatively, you can manually restart these servers after removing the SDC.

On Linux servers, if the kernel module is busy, perform a manual restart.

6. Enter the MDM password, select to reboot servers (optional), and click **Uninstall**.
7. To monitor the uninstallation progress, click **Monitor**.
8. When the uninstallation is complete, click **Mark operation completed**.
Unregister the VxFlex OS plug-in

Remove a registered vSphere VxFlex OS plug-in.

About this task

To remove the currently registered VxFlex OS plug-in, perform the following:

Procedure

1. Run the script to remove the VxFlex OS plug-in:
   a. From the folder where you extracted the current VxFlex OS plug-in ZIP file (for example: EMC-ScaleIO-vSphere-plugin-installer-3.0-X.<build>.X.zip), use PowerCLI to run the VxFlex OS plug-in script (for example: VxFlexOSPluginSetup.ps1).
   b. Select option 2, Unregister VxFlex OS plug-in.
2. Enter the vCenter credentials and confirm the script actions.
3. Log out, then log back in to the vSphere web client.
4. The VxFlex OS plug-in is no longer registered.

Renaming objects

About this task

Object names are used to identify the objects in the VxFlex OS GUI, and can also be used to specify objects in CLI commands. You can view an object’s name in its Property Sheet, in the Identity section.

Note: It is not possible to rename a Read Flash Cache device using this command.

You can define object names according to the following rules:

1. Contain less than 32 characters
2. Contain only alphanumeric and punctuation characters
3. Be unique within the object type

When a name has not been defined, the system may display default system-defined names, as follows:

- SDC—its first IP address
- SDS—its first IP address
- Device—the path to the device
- All other objects—the object’s ID

Note: A name must be assigned to a volume when it is initially created. You can rename the volume later, using the Rename command.

Procedure

1. Depending on the object type, in the Backend > Storage or any of the Frontend views, navigate to the object in the table, and select its row.
2. Right-click the object and select Rename.
   An editing window is displayed, showing the current name, and an editable field for the new name.
3. Type the new name in the field, and click OK.
Add, Remove or Rename Components
CHAPTER 12

Logs

The following topics describe how to configure logs in the VxFlex OS system.

- Enable automatic log collection................................................................. 206
- Set ESXi credentials for auto collect logs............................................... 206
Enable automatic log collection

You can enable auto collect logs in the VxFlex OS system. Automatic log collection allows the VxFlex OS Gateway to automatically collect information from a VxFlex OS system when alerts of severity level 5 (critical) are raised. The log is saved to a known directory under a name which includes the date the log was created, the alert name and severity.

For this feature to work, the MDM credentials and LIA password must be defined in the lockbox. If a LIA password is not defined in the lockbox, an error appears when selecting the Auto Collect Logs checkbox.

Set ESXi credentials for auto collect logs

Select the files to collect from the VxFlex OS system according to your requirements.

1. From the Maintain tab, click System Logs & Analysis and select Set ESXi Credentials for Auto Collect Logs. The Confirm Set Credentials of your VxFlex OS system dialog box is displayed.
2. Enter the admin password to the MDM in the MDM admin password box.
3. Select the option according to the files that you require from the VxFlex OS system:
   - Collect debug information
     - Latest logs only - collects the files that are checked in the Show Collected Information drop-down list.
     - Add repositories - collects all the files from the Show Collected Information drop-down list. We recommend this option, as all files are collected.
     When both options are selected, the files that are checked in the Show Collected Information drop-down list are collected.
   - Collect exceptions only - only the All exp.* files option is collected.
4. Select Include all nodes in log collection to collect logs from all nodes in your VxFlex OS system.
5. Click Set Credentials to save the log configuration settings.
CHAPTER 13

LIA

The following topics describe how to configure LIA in the VxFlex OS system.

- Change LIA behavior ........................................................................................................... 208
- Add LIA to a system to enable automated maintenance and upgrades ......................... 208
Change LIA behavior

You can change the default behavior of the LIA by editing its configuration file. The default location of the LIA configuration file is host operating system dependent, as follows:

- **Windows:** C:\Program Files\emc\scaleio\LIA\cfg\conf.txt
- **Linux:** /opt/emc/scaleio/ lia/cfg/conf.txt

The following are some values relevant to LIA behavior:

```
lia_token=5
lia_enable_install=1
lia_enable_uninstall=1
lia_enable_configure_fetch_logs=1
```

To restrict which VxFlex OS Gateway IP addresses can access the LIA, add those IP addresses to this line in the `conf.txt` file:

```
lia_trusted_ips=<IP_ADDRESS_1>,<IP_ADDRESS_2>
```

To set this during LIA installation, set the TRUSTED_IPS environment variable. For example:

```
TRUSTED_IPS=1.2.3.4,5.6.7.8 rpm -i lia.rpm
```

Add LIA to a system to enable automated maintenance and upgrades

Add the LIA, a component that is required to use the VxFlex OS Installer to upgrade and maintain VxFlex OS physical server system components.

**Before you begin**

To determine if the LIA is installed, run the following command on any server in the system:

```
rpm -qa | grep -i LIA
```

If LIA is not installed, you must install it before proceeding.

**About this task**

Physical machine upgrade uses the VxFlex OS Installer (part of the VxFlex OS Gateway), together with the LIA of the new version, to orchestrate the upgrade.

**Procedure**

1. Install the LIA component on every node, by running the following command:

```
TOKEN=<LIA_password> rpm -i <full rpm path to LIA file>
```
Example:

```
TOKEN=Scaleio123 rpm -i EMC-ScaleIO-lia-3.0-\nX.<build>.<flavor>.x86_64.rpm
```

The password must meet the following criteria:
- Between 6 and 31, ASCII-printable characters
- No blank spaces
- Include at least 3 of the following groups: [a-z], [A-Z], [0-9], special chars (!@#$ …)

**Note:** If you use special characters on a Linux-based server, you must escape them when issuing the command.

The LIA password must be identical in all LIAs within the same system

2. Import the system installation ID into the LIA:
   a. Create the following file:
      ```
      /opt/emc/scaleio/lia/cfg/installation_id.txt
      ```
   b. Query the MDM for the installation ID by running the following command:
      ```
      scli --query_all|grep "Installation ID"
      ```
   c. Copy the installation ID into the new file.
   d. Restart the LIA service by running the following command:
      ```
      pkill lia
      ```

3. Repeat the previous steps on every node in the system.

**Results**

LIA is installed.
CHAPTER 14

Setting up GUI system preferences

Set up your preferences for using the VxFlex OS GUI.

- **Customize system preferences** .................................................................................. 212
Customize system preferences

Use VxFlex OS GUI to customize various features.

About this task

You can customize various features in the VxFlex OS GUI using the User Preferences window. The following features can be customized:

- Refresh data rate
- Clear host history from previous sessions
- Calculation of I/O workload average rate shown on the Dashboard
- System clock display
- Advanced display mode for Dashboard, Backend internal views, Frontend internal views, and Property Sheet
- Log level

Procedure

1. From any location in the VxFlex OS GUI, open the System Settings menu in the top right corner, and select User Preferences.

   The User Preferences window is displayed.

2. Edit the options according to your needs, and click Apply.
Figure 15 User Preferences window

User Preferences

General
- Refresh data every 1 seconds

Login
- Clear host history

Dashboard I/O Workload
- Average calculation will include the last 60 seconds
- Show advanced dashboard

System Clock
- Show system clock

Property Sheet
- Show property sheet in advanced mode

Frontend internals
- Show externally managed volumes

Backend internals
- Show internal backend views

Support
- Log level: Info
- Pop-up in case of uncaught exception

Apply Close
### Table 3 User Preferences

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General:</strong>&lt;br&gt;Refresh data every ( n ) seconds</td>
<td>Controls the rate at which data displayed in the VxFlex OS GUI is refreshed, in seconds (Default: 10 seconds) The refresh occurs at least at the specified rate. It is not intended to be used as a means of limiting client traffic, although it would actually do so.</td>
</tr>
<tr>
<td><strong>Login:</strong>&lt;br&gt;Clear host history</td>
<td>When selected, the VxFlex OS GUI does not save and present host connection details from previous sessions</td>
</tr>
<tr>
<td><strong>Dashboard I/O workload:</strong>&lt;br&gt;Average calculation will include the last ( n ) seconds</td>
<td>Controls the time period used when averages are computed and displayed by the VxFlex OS GUI (default: 10 seconds)</td>
</tr>
</tbody>
</table>
| Show advanced dashboard | When selected, (default), includes more details on some tiles in the Dashboard view. The toggle buttons switch between the statistics displayed in large fonts and small fonts. The upper button toggles between average values and sample values. The lower button toggles between display of bandwidth or IOPs in large fonts on this tile.  

The \( \bigtriangleup \) symbol means that the number displayed is the average taken during the last \( n \) seconds. \( n \) can be configured in **Dashboard I/O Workload** in this window.  

The \( \bigtriangleup \) symbol means that the number displayed is from the last data sample that was taken. The period between automatic refreshes can be configured in **Dashboard I/O Workload** in this window. |
| System Clock | Show system clock on the Dashboard |
| **Show Property Sheet in advanced mode** | Displays additional details in Property Sheets:  
- Capacity section—Snapshot Capacity Reserved  
- Rebuild/Rebalance—Data Movement Jobs  
- RAM Read Cache—Cache Evictions, Cache Entry, and Cache Skip tables  

These details are usually only relevant for advanced users and technical support purposes. |
| Frontend Internals:<br>Show VVols | Displays additional information for VVols |
| Backend Internals:<br>Show internal Backend views | Displays additional options for Backend table views. These options are recommended only for advanced users and technical support purposes. |
### Table 3 User Preferences (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support: Log level</td>
<td>Controls the type of data saved in system logs, which may be required by Customer Support for troubleshooting purposes. The default setting recommended for regular operation is Info. Other options include: Trace, Debug, Warn, and Error. Note: Trace and Debug options may affect system performance, and are usually only recommended for technical support purposes. For more information about logs, see your system's Log Collection Technical Notes.</td>
</tr>
</tbody>
</table>
Setting up GUI system preferences
PART 5

VMware environment specific tasks

This section contains VMware environment specific tasks.

Chapter 15, "VxFlex OS plug-in"

Chapter 16, "Manually performed tasks"
VMware environment specific tasks
The following topics describe how to configure VxFlex OS plug-in:

- Configure components
Configure components

You can configure settings for VxFlex OS from the VxFlex OS plug-in.

There are two levels of component configurations:

- **Basic**: The basic configurations are all performed the same way. The process is described just once.
- **Advanced**: Each advanced configuration setting has a unique dialog box, which is described in "Configuring components-advanced".

The following table lists the activities you can perform and categorizes each as basic or advanced:

<table>
<thead>
<tr>
<th>Object</th>
<th>Perform this activity</th>
<th>Basic or advanced</th>
<th>Access from this screen</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Deploy VxFlex OS</td>
<td>Advanced. See the VxFlex OS Deployment Guide.</td>
<td><img src="VxFlex.png" alt="VxFlex OS" /></td>
</tr>
<tr>
<td></td>
<td>Register an existing system</td>
<td>Basic. Enter the system Master MDM IP address, username, and password.</td>
<td><img src="VxFlex.png" alt="VxFlex OS" /></td>
</tr>
<tr>
<td></td>
<td>Unregister a system</td>
<td>Basic</td>
<td>![VxFlex OS Systems](VxFlex Systems.png)</td>
</tr>
<tr>
<td></td>
<td>Update system credentials</td>
<td>Basic. Enter new username and password.</td>
<td>![VxFlex OS Systems](VxFlex Systems.png)</td>
</tr>
<tr>
<td></td>
<td>Configure virtual IPs</td>
<td>Advanced</td>
<td>![VxFlex OS Systems](VxFlex Systems.png)</td>
</tr>
<tr>
<td>VxFlex OS Gateway</td>
<td>Register/Update Gateway</td>
<td>Basic. Enter IP address, operating system username, and operating system password.</td>
<td>![VxFlex OS Systems](VxFlex Systems.png)</td>
</tr>
<tr>
<td></td>
<td>Open Gateway</td>
<td>Basic. Navigates to the VxFlex OS Installer.</td>
<td>![VxFlex OS Systems](VxFlex Systems.png)</td>
</tr>
<tr>
<td>Protection Domain</td>
<td>Create a Protection Domain</td>
<td>Basic</td>
<td>![VxFlex OS Systems](VxFlex Systems.png)</td>
</tr>
<tr>
<td></td>
<td>Remove a Protection Domain</td>
<td>Basic</td>
<td>![Protection Domains](Protection Domains.png)</td>
</tr>
<tr>
<td>Storage Pool</td>
<td>Create a Storage Pool</td>
<td>Basic</td>
<td>![Protection Domains](Protection Domains.png)</td>
</tr>
<tr>
<td></td>
<td>Remove a Storage Pool</td>
<td>Basic</td>
<td>![Storage Pools](Storage Pools.png)</td>
</tr>
<tr>
<td></td>
<td>Configure Read RAM Cache</td>
<td>Basic*</td>
<td>![Storage Pools](Storage Pools.png)</td>
</tr>
</tbody>
</table>
### Table 4 Plug-in activity matrix (continued)

<table>
<thead>
<tr>
<th>Object</th>
<th>Perform this activity</th>
<th>Basic or advanced</th>
<th>Access from this screen</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDS</td>
<td>Add a device to an SDS</td>
<td>Advanced</td>
<td><a href="#">SDSs</a></td>
</tr>
<tr>
<td></td>
<td>Remove a device from an SDS</td>
<td>Basic</td>
<td><a href="#">Devices</a></td>
</tr>
<tr>
<td>SDC</td>
<td>Install SDC on ESX</td>
<td>Advanced. See the <a href="#">VxFlex OS Deployment Guide</a></td>
<td><a href="#">Dell EMC VxFlex OS</a></td>
</tr>
<tr>
<td></td>
<td>Upgrade SDC</td>
<td>Advanced</td>
<td><a href="#">SDCs</a></td>
</tr>
<tr>
<td></td>
<td>Update SDC Parameters</td>
<td>Advanced. See the <a href="#">VxFlex OS Deployment Guide</a></td>
<td><a href="#">Dell EMC VxFlex OS</a></td>
</tr>
<tr>
<td>Volume</td>
<td>Create and map volumes</td>
<td>Advanced</td>
<td><a href="#">Storage Pools</a></td>
</tr>
<tr>
<td></td>
<td>Map a volume</td>
<td>Advanced</td>
<td><a href="#">Volumes</a></td>
</tr>
<tr>
<td></td>
<td>Remove a volume (must be unmapped first)</td>
<td>Basic</td>
<td><a href="#">Volumes</a></td>
</tr>
<tr>
<td></td>
<td>Unmap a volume</td>
<td>Advanced</td>
<td><a href="#">Volumes</a></td>
</tr>
<tr>
<td></td>
<td>Configure Read RAM Cache</td>
<td>Basic&lt;sup&gt;a&lt;/sup&gt;</td>
<td><a href="#">Volumes</a></td>
</tr>
<tr>
<td>Fault Set</td>
<td>Create a Fault Set</td>
<td>Basic&lt;sup&gt;b&lt;/sup&gt;</td>
<td><a href="#">Protection Domains</a></td>
</tr>
<tr>
<td>Device</td>
<td>Clear a device error</td>
<td>Basic</td>
<td><a href="#">Devices</a></td>
</tr>
<tr>
<td></td>
<td>Add a device to an SDS</td>
<td>Advanced</td>
<td><a href="#">SDSs</a></td>
</tr>
<tr>
<td></td>
<td>Remove a device from an SDS</td>
<td>Basic</td>
<td><a href="#">Devices</a></td>
</tr>
</tbody>
</table>

<sup>a</sup> For Read RAM Cache to work on a volume, both the volume and its Storage Pool must have the feature enabled.

<sup>b</sup>
Configure components—basic

Create a Protection Domain in the VxFlex OS system from the VxFlex OS plug-in.

About this task

Basic configuration activities are all performed in a similar manner. All activities are performed from the Actions menu in each screen and by entering simple information. Following is an example on how to create a Protection Domain from the VxFlex OS Systems screen.

Procedure

1. From the VxFlex OS Systems screen, click Actions > Create Protection Domain:

   ![Create Protection Domain](image)

   Note: You can also click the action icons in the menu or right-click the item to choose options from a list.

2. In the Create Protection Domain dialog box, enter a name for the Protection Domain, and then click OK.

   The process is similar for the rest of the basic activities.

   Note: If you intend to enable zero padding on a Storage Pool, you must do so before you add any devices to the Storage Pool. For more information, see "Storage Pools" in the Getting to Know Guide.

Configuring components—advanced

This section describes how to use the VxFlex OS vSphere plug-in to perform activities that require a little more attention.

Register an existing system

Use the VxFlex OS plug-in to register an existing VxFlex OS.

About this task

Enter the following information of the existing VxFlex OS system.
Procedure

1. From the main VxFlex OS plug-in window, click **Register VxFlex OS system**.
2. Enter the following information, then click **OK**:
   a. **Master MDM IP**: The IP address of the existing system's Master MDM
   b. **User name**: The username of the existing system
   c. **Password**: The password of the existing system

Volumes in the vSphere environment

The following topics describe how to use the VxFlex OS plug-in to add, map, and unmap volumes in the vSphere environment. You can map volumes to SDCs in the same step, or you can map the volume after it has been created.

Add devices to an SDS—VxFlex OS plug-in

Use the vSphere VxFlex OS plug-in to add devices to an SDS in VxFlex OS.

About this task

In a DirectPath-based system, you add devices only after the deployment. In an RDM/VMDK-based VxFlex OS, you can add devices during and after the deployment.

You can add a Storage device or an Acceleration device to an SDS or to all SDSs in the system. For a Storage device, you must define the Storage Pool and Media Type for each device you add. For Acceleration device, you must select the Acceleration Pool (which may be RFCache or NVDIMM) for each device added. For Fine Granularity (FG), an Acceleration device must be configured with NVDIMM. For more information on FG, see "Data layout" in the *Getting to Know Guide*.

All data on added devices will be erased.

**Note:** If you intend to enable zero padding on a Storage Pool, you must do so before you add any devices to the Storage Pool.

Procedure

1. From the **SDSs** screen of the VxFlex OS plug-in, select one of the following:
   - Right-click a specific SDS, and then select **Add devices to a single SDS**.
   - Right-click any SDS, and then select **Add devices to VxFlex OS system**.
   
   The Add Device dialog box is displayed. All devices that can be attached to the selected SDS are listed. For the system view, all SDSs are listed, and you can choose devices to add for each SDS. It may take a few moments to load the list of devices from the vCenter.

2. Add devices:
   - One-at-a-time:
     a. Select whether the device should be used for storage or to provide acceleration.
     b. Select the Storage Pool to which the devices should be assigned.
     c. To enable the use of devices that may have been part of a previous VxFlex OS system, select **Allow the take over of devices with existing signature**.
     d. Click **OK**.
   - All devices on a server at once:
     a. Click **Select all devices**.
     b. Select whether to use the devices for storage or to provide acceleration.
     c. Select the Storage Pool to which the devices should be assigned.
d. To enable the use of devices that may have been part of a previous VxFlex OS system, select **Allow the take over of devices with existing signature**.

e. Click **Assign**.

3. Confirm the action by typing the VxFlex OS password.

4. When the add operation is complete, click **Close**.

**Results**
The devices are added.

**Upgrading an SDC—VxFlex OS plug-in**
Upgrading an SDC is performed with the VxFlex OS plug-in. This topic is described in the Upgrade VxFlex OS Guide.

**Modify SDC-MDM communication parameters on SDCs**
When MDM IP addresses have been added or changed, use the vSphere VxFlex OS plug-in to update the SDCs with system parameters that are needed to ensure continued SDC-MDM communication.

**Procedure**
1. From the VxFlex OS plug-in **Advanced tasks** menu, click **Update SDC parameters**, and follow the on-screen instructions to complete the process.

2. Ensure that the parameters were updated on the SDC by running this command on each ESXi host:

```bash
cat /etc/vmware/esx.conf |grep scini|grep -i mdm
```

**Configuring virtual IP addresses—VxFlex OS plug-in**
Configure virtual IP addresses in the vSphere VxFlex OS plug-in.

**Procedure**
1. From the **VxFlex OS Systems** screen, click **Actions** and select **Configure virtual IPs**.

2. In the **Configure virtual IPs** dialog box, select the network and enter a virtual IP address.

**After you finish**
To update the SDC configuration, update the SDC parameters. For more information, see "Updating SDC parameters".
CHAPTER 16

Manually performed tasks

The following tasks describe how to manually perform certain tasks in your VxFlex OS environment.

- **Clean the VxFlex OS VMware environment** ......................................................... 226
- **SVM manual memory allocation** ........................................................................... 227
- **Managing ESXi servers** ......................................................................................... 228
Clean the VxFlex OS VMware environment

For 2-layer systems, or ESXi-based systems, clean the VxFlex OS VMware environment in order to perform a clean installation. This procedure is recommended for cases when previously defined networks will be used again, or when VxFlex OS components such as SDCs that ran on other networks exist in the environment.

Before you begin

Before you begin, unmap and delete any VxFlex OS volumes in your system. If necessary, unregister VxFlex OS from within the vSphere VxFlex OS plug-in, and delete all the VxFlex OS SVMs.

Procedure

1. Close the existing PowerCLI sessions, set PowerCLI to Run as administrator, and then open a new session.
2. Using the PS1 script, unregister the VxFlex OS plug-in.
3. Stop the vSphere web client service:
   VC Linux: service-control --stop vsphere-client
4. Delete the contents of the VxFlex OS plug-in folder.
   The vSphere web client (Virgo) plug-in folders are located at:

<table>
<thead>
<tr>
<th>Vcenter</th>
<th>Operating system</th>
<th>Path to file</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.x</td>
<td>Windows</td>
<td><code>C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity</code></td>
</tr>
<tr>
<td></td>
<td>Linux</td>
<td><code>/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity</code></td>
</tr>
</tbody>
</table>

5. Delete the scaleio folder or its contents.
   The scaleio folders are located at:

<table>
<thead>
<tr>
<th>Vcenter</th>
<th>Operating system</th>
<th>Path to file</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.x</td>
<td>Windows</td>
<td><code>C:\Users\vspherewebclientsvc\AppData\Roaming\VMware\scaleio</code></td>
</tr>
<tr>
<td></td>
<td>Linux</td>
<td><code>/etc/vmware/vsphere-client/vc-packages/scaleio</code></td>
</tr>
</tbody>
</table>

6. Start the vSphere web client service:
   VC Linux: service-control --start vsphere-client
7. Clear your web browser's cache and cookies, or open a different web browser.
8. Using the PS1 script in PowerCLI, register the VxFlex OS plug-in.
   **Note:** Do not press ENTER at this point.
9. After you have logged in to the vSphere web client to complete the registration and you see the VxFlex OS icon, press ENTER in the PowerCLI session.
This stops the embedded Tomcat server.

10. If necessary, remove the SDC module parameters and VIB from the ESXi servers:
   a. Connect to each ESXi server via SSH.
   b. Run:

   ```
   ~ # esxcli system module parameters set -m scini -p ""
   ~ # esxcli software vib remove -n scaleio-sdc-esx6.0
   ```
   c. Reboot each ESXi server.

11. Proceed to the procedures for re-registering the VxFlex OS plug-in, and then deploy VxFlex OS.

**SVM manual memory allocation**

Manual memory allocation for SVMs is required in a number of scenarios. However, when using the plug-in for a clean deployment, SVM memory allocation is performed automatically.

**About this task**

The formula for calculating SVM memory requirements can be found in the *Getting to Know VxFlex OS Guide*.

In the following cases, SVM memory allocation must be performed manually:

- Manual deployment on VMware.
- Extending an existing SVM with a new VxFlex OS role/component, whether this is being done with the plug-in or manually.
  Workaround: Perform all the parts of step 1 and step 2 before extending the additional role/component on the SVM. Perform the steps on one SVM at a time.
- Changing the SDS performance profile, post deployment.
  Workaround: Perform all the parts of step 1, one SVM at a time.

**Procedure**

1. For SVMs that are SDS-only, perform the following:
   a. Move the SDS to maintenance mode (MM).
   b. Shut down the SVM.
   c. Increase SVM memory, according to the formula below.
   d. Power up the SVM.
   e. Exit MM.

2. For SVMs that are MDM (Master, Slave, or TB, may contain SDS, also):
   a. Start with Slaves and TBs:
      a. Move the SDS to maintenance mode (MM).
      b. Shut down the SVM.
      c. Increase SVM memory, according to the formula below.
      d. Power up the SVM.
Managing ESXi servers

Using the following procedures, you can modify parameters on ESXi servers and check the SDC state on ESXi servers.

Modify parameters on ESXi servers

Use esxcli commands on an SDC running on an ESXi server to update parameters.

About this task

The following esxcli commands can be used in the following cases:

- MDM IP addresses need to be added to the existing list on an SDC
- MDM IP addresses need to be replaced on an SDC
- The SDC’s GUID needs to be changed

Specifically, the SDC’s GUID or IP address needs to be identified, and then used to add or modify the MDM IP addresses or GUID (depending on the parameter that you want to modify). If you want to add additional MDM IP addresses to existing ones, you must list both old and additional IP addresses in the esxcli command.

For more information about SDC tuning, see VxFlex OS Performance Fine-Tuning Technical Notes.

If the current configuration of VxFlex OS is registered with a v2.0 VMware plug-in, you can use the plug-in Update SDC parameters to update the MDM IP addresses. For more information, see the VxFlex OS Deployment Guide.

Note: These procedures require a server restart to apply the new configuration. The configuration will remain persistent after future server restarts.

To configure MDM IP addresses on the SDC, perform these steps:

Procedure

1. Find the SDC’s GUID and the MDM IP addresses configured on the ESX, by typing the command:

   esxcli system module parameters list -m scini

2. In the output of the command, find the existing GUID and MDM IP addresses.
For example, in the output excerpt below, the GUID and IP addresses are marked in bold:

<table>
<thead>
<tr>
<th>_IOCTLIniGuidStr string</th>
<th>39b89295-5cfc-4a42-bf89-4cc7e55a1e5b</th>
<th>Ini Guid, for example: 12345678-90AB-CDEF-1234-567890ABCDEF</th>
</tr>
</thead>
</table>

|_IOCTLMdmIPStr string   | 9.99.101.22, 9.99.101.23 | Mdms IPs, IPs for MDM in same cluster should be comma-separated. To configure more than one cluster use '+' to separate between IPs. For example: 10.20.30.40,50.60.70.80+11.22.33.44. Max 1024 characters |

3. To configure the MDM IP addresses on the SDC, type the command

```
esxcli system module parameters set -m scini -p "IoctlIniGuidStr=<GUID> IoctlMdmIPStr=<MDM_IPS>"
```

where `<GUID>` is the existing SDC GUID that you identified in the previous step, and `<MDM_IPS>` is the list of MDM IP addresses. A maximum of 1024 characters is allowed.

a. To replace the old MDM IP addresses with new MDM IP addresses, omit the old addresses from the command.

b. To add MDM IP addresses to the existing IP addresses, type both the existing IP addresses and the new IP addresses in the command.

MDM IP addresses for MDMs in same cluster must be comma-separated. To configure more than one cluster, use '+' to separate between IP addresses in different clusters. For example:

```
esxcli system module parameters set -m scini -p "IoctlIniGuidStr=39b89295-5cfc-4a42-bf89-4cc7e55a1e5b IoctlMdmIPStr=10.20.30.40,50.60.70.80+11.22.33.44""
```

4. To apply the new configuration, restart the ESX server.

5. To change the GUID of the SDC, perform these steps:

6. In the output of the command, find the existing GUID and MDM IP addresses.

   For example, in the output excerpt below, the GUID and IP addresses are marked in bold:

<table>
<thead>
<tr>
<th>_IOCTLIniGuidStr string</th>
<th>39b89295-5cfc-4a42-bf89-4cc7e55a1e5b</th>
<th>Ini Guid, for example: 12345678-90AB-CDEF-1234-567890ABCDEF</th>
</tr>
</thead>
<tbody>
<tr>
<td>_IOCTLMdmIPStr string</td>
<td>9.99.101.22, 9.99.101.23</td>
<td>Mdms IPs, IPs for MDM in same cluster should be comma-separated. To configure more than one cluster...</td>
</tr>
</tbody>
</table>
7. To change the GUID on the SDC, type the command

```bash
esxcli system module parameters set -m scini -p "IoctlIniGuidStr=<NEW_GUID> IoctlMdmIPStr=<MDM_IPs>
```

where `<NEW_GUID>` is the new SDC GUID, and `<MDM_IPs>` is the list of MDM IP addresses that you identified in the previous step. You must include these IP addresses in the command.

For example:

```bash
esxcli system module parameters set -m scini -p "IoctlIniGuidStr=28a78184-4beb-4a42-bf89-4cc7e55a1e5b IoctlMdmIPStr=9.99.101.22,9.99.101.23"
```

8. To apply the new configuration, restart the ESX server.

**Check the SDC state on ESXi servers**

Use `esxcli` commands on an SDC running on an ESXi server to check the current state of the SDC.

To display the SDC state on the ESX server, type the following command:

```bash
esxcli system module list | grep scini
```

The following examples show typical outputs of the command:

- Output where driver is installed and enabled to load, but not loaded:

  ```
  Name Is Loaded Is Enabled
  ----------------------------- --------- ----------
  scini false true
  ```

- Example of SDC in correct state (enabled and loaded):

  ```
  Name Is Loaded Is Enabled
  ----------------------------- --------- ----------
  scini true true
  ```
PART 6

Operating System Patching

Use the VxFlex OS Gateway to run scripts that patch hosts' operating systems in a safe and orchestrated manner.

Chapter 17, "Operating System Patching"
Run scripts on servers hosting VxFlex OS components, for patching purposes.

- Upgrade the CentOS operating system on SVMs
Upgrade the CentOS operating system on SVMs

Use the VxFlex OS Installer to upgrade the SVM’s CentOS operating system to the latest security level of operating system security patching. This procedure only upgrades the operating system on the SVM. It does not upgrade VxFlex OS.

**Note:** SVM operating system patching is applicable even if the SVM replacement procedure was performed. The latest patch bundle has the latest security patches that were released after the latest version of VxFlex OS was officially launched (the refresh of the package is done on a monthly basis based on continuous security scans and input from customers).

Use the VxFlex OS Installer to upgrade the CentOS operating system on multiple SVMs. This procedure is required when upgrading an ESXi-based VxFlex OS system where SVMs are currently running on CentOS 7.5. (VxFlex OS v3.0, or v3.0.0.x)

Ensure that you have the latest SVM operating system upgrade ZIP file. It is available from the support site, on the VxFlex OS page: [https://support.emc.com/products/33925](https://support.emc.com/products/33925).

The `patch_script` file that you require is part of the VMware complete software package (which is in the Complete SW download ZIP) and also as a separate artifact that is refreshed from time to time (usually once a month). The ZIP file name is: `SVM_OS_Patching_package_MMDDYYYY.zip`

Running scripts on hosts—overview

VxFlex OS can be used to run user-provided scripts on servers hosting MDM or SDS components. This feature is supported on Linux-based (bare-metal or virtual) nodes only.

The VxFlex OS Installer can be used to run a user-provided script on a host where VxFlex OS is deployed. This feature can be used for any purpose external to the VxFlex OS system, such as running a set of CLI commands, patching an operating system, and more. The feature allows the running of scripts in a safe manner, both from a security and a data integrity perspective.

VxFlex OS Installer orchestrates the running of the script, ensuring that SDSs are placed in Maintenance Mode, to protect data during the process. In addition, parallel execution of scripts is only permitted on SDSs located in different Protection Domains. After the scripts have been run on an SDS, it exits Maintenance Mode.

Optionally, servers can be set to reboot after execution of the script. The process can also run a verification script either after the reboot, or after execution of the script, when no reboot is required.

**Workflow overview** (for reference purposes only)

The execution phase of this feature can be summarized as follows:

1. The system validates the following:
   - The patching script exists on the node after it was uploaded from the gateway host
   - No failed capacity exists
   - Sufficient spare capacity exists
   - The MDM cluster is in a valid state

2. Run the script on one host, using the following priorities:
   a. SDS only hosts, each time on a single SDS, unless the option **In parallel on different Protection Domains** is enabled
   b.
Run a script on one or more hosts—procedures

Run a script on one or more hosts where VxFlex OS is deployed, using the VxFlex OS Installer.

**Before you begin**

- Prepare the script file to be run on one or more servers hosting SDSs or MDMs, and optionally, a verification script to be run automatically after execution of the script. Specific file names are required for use of this feature. IM can only upload scripts up to 500 MB in size. Name the files as follows:
  - **Script**: patch_script
  - **Verification script**: verification_script
- This feature is only supported on Linux-based (bare-metal or virtual) nodes.
- Ensure that you have the IP address and login credentials for the VxFlex OS Gateway and the Master MDM.
- Ensure that you have the login credentials for the LIA.
- Ensure that you have enough disk space to run the script.

**About this task**

- This procedure is a long operation that cannot be rolled back automatically.
- Certificate approval messages may be displayed during the procedure. Approve all the certificates, and click **Retry failed** to complete the operation.

**Procedure**

1. Configure the VxFlex OS Installer to upload files from the VxFlex OS Gateway host to all selected hosts.

   **Note:** Alternatively you can copy the script file to each host in the system under the file path ~/lia/bin/<folder>. Follow the steps to make sure the script file runs on each of the hosts.

   a. Verify that all components in the VxFlex OS system are upgraded to the latest version.
   b. On the VxFlex OS Gateway host, go to /opt/emc/scaleio/gateway/webapps/ROOT/WEB-INF/classes/gatewayUser.properties file.
   c. Uncomment the following lines (verification script is optional):

   ```
   os.patching.is.upload.needed=true (Default is false)
   os.patching.patch.script.source.path=<enter the full path to the file>
   os.patching.verification.script.source.path=<enter the full path to the file>
   ```
Example of VxFlex OS Gateway on Linux:

```plaintext
os.patching.is.upload.needed=true
os.patching.patch.script.source.path=/opt/patch_script
os.patching.verification.script.source.path=/opt/verification_script
```

Example of VxFlex OS Gateway on Windows:

```plaintext
os.patching.is.upload.needed=true
os.patching.patch.script.source.path=C:\\temp\\patch_script
os.patching.verification.script.source.path=C:\\temp\\verification_script
```

d. Restart the VxFlex OS Gateway service.
   For example, in ESXi:
   ```bash
   systemctl stop scaleio-gateway.service
   systemctl start scaleio-gateway.service
   ```

e. Copy the `patch_script` and `verification_script` files to the relevant folder on the gateway host.

f. In the Security settings of the files, allow read, write and execute permissions.

2. In your browser, navigate to the IP address of the VxFlex OS Gateway, and log in.
3. Click the Maintain tab.
4. Enter the IP address and login credentials for the Master MDM, and for LIA.
5. At the bottom right of the screen, click Retrieve system topology.
   The system topology is displayed.
6. Click System Logs & Analysis, and select the Run Script on Hosts option.
   The Run script on hosts dialog box is displayed.
7. Enter the MDM password again.
8. For Running script on options, select one from the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entire System</td>
<td>Run the script on all MDM and SDS nodes in the system.</td>
</tr>
<tr>
<td></td>
<td>If you choose this option, you can also choose whether</td>
</tr>
<tr>
<td></td>
<td>to run the script at the same time on SDSs that belong</td>
</tr>
<tr>
<td></td>
<td>to different Protection Domains. To do so, select the</td>
</tr>
<tr>
<td></td>
<td>check box for In parallel on different Protection</td>
</tr>
<tr>
<td></td>
<td>Domains.</td>
</tr>
<tr>
<td>Protection</td>
<td>Run the script on MDM and SDS nodes in a single</td>
</tr>
<tr>
<td>Domain</td>
<td>Protection Domain. Select the required Protection</td>
</tr>
<tr>
<td></td>
<td>Domain from the drop-down list.</td>
</tr>
<tr>
<td>Fault Set</td>
<td>Run the script on MDM and SDS nodes in a single Fault</td>
</tr>
<tr>
<td></td>
<td>Set. Select the required Fault Set from the drop-down</td>
</tr>
<tr>
<td>SDS</td>
<td>Run the script on a single SDS. Select the required</td>
</tr>
<tr>
<td></td>
<td>SDS from the drop-down list.</td>
</tr>
</tbody>
</table>

9. For Running configuration, select the Stop process on script failure option, if desired.
   If problems occur, see the troubleshooting notes following these steps.
10. In the **Script time-out** box, enter the number of minutes that should elapse before the VxFlex OS Installer stops waiting for a response about the running script, and prints a timeout message.

11. In the **Verification script** box, select one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run a verification script after the script.</td>
<td>Select Run</td>
</tr>
<tr>
<td>If a reboot is performed, the verification script is executed after the reboot.</td>
<td></td>
</tr>
<tr>
<td>Do not run a verification script after the script</td>
<td>Select Do not run</td>
</tr>
</tbody>
</table>

12. In the **Post script action** box, select one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot the server after execution of the script</td>
<td>Select Reboot</td>
</tr>
<tr>
<td>Do not reboot the server after execution of the script</td>
<td>Select Do not reboot</td>
</tr>
</tbody>
</table>

13. Click **Run Script on Hosts**.

14. Click the **Monitor** tab, - validate state starts.

   During this phase, the system verifies certificates and builds an execution phase for the nodes list.

15. Click **Start** - the execute phase starts.

16. When the execute phase is complete, click **Mark operation completed**.

   Troubleshooting notes:
   If a failure in executing the patch_script occurs, it may be due to one of the following reasons. Rectify the problem and then try again.
   - Script timeout
   - Script file permissions
   - Syntax error in the script
   - Degraded capacity, or MDM cluster in degraded state
   - An SDS is already in Maintenance Mode

**Results**

Upgrade of the CentOS operating system on all SVMs except for the VxFlex OS Gateway is now complete. Upgrade the VxFlex OS Gateway using the steps described in "Deploy and replace the VxFlex OS Gateway SVM operating system using the VxFlex OS plug-in" in the Upgrade VxFlex OS Guide.
Operating System Patching