Dell SRM 5.1.1.0

Upgrade Guide

5.1.1.0

June 2025
Rev. A00

Notes, cautions, and warnings

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

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

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

Contents

Tables

1

Dell SRM 5.1.1.0 Upgrade

This guide is applicable for upgrades from release 4.10.0.0 onwards only.

For upgrades of any version previous to 4.10.0.0, see SRM 4.9.0.0 Upgrade Guide at Dell Support Site.

For details about verifying the health of the system, see Dell SRM Administrator Guide at Dell Support Site.

For details about determining the configuration size, see the Dell SRM Performance and Scalability Guidelines at Dell Support Site.

Upgrade Paths

Following are the valid upgrade paths to SRM 5.1.1.0:

- From **Release 4.10.0.0**
  - 4.10.0.0 > 5.1.1.0
  - 4.10.0.0 > 4.10.0.1 > 5.1.1.0
  - 4.10.0.0 > 4.10.0.2 > 5.1.1.0
  - 4.10.0.0 > 4.10.0.3 > 5.1.1.0
- From **Release 5.0.0.0**
  - 5.0.0.0 > 5.1.1.0
- From **Release 5.0.1.0**
  - 5.0.1.0 > 5.1.1.0
- From **Release 5.0.2.0**
  - 5.0.2.0 > 5.1.1.0
  - 5.0.2.0 > 5.0.2.1 > 5.1.1.0
  - 5.0.2.0 > 5.0.2.2 > 5.1.1.0
- From **Release 5.1.0.0**
  - 5.1.0.0 > 5.1.1.0

NOTE:

- For vApp based and SLES-based binary SRM deployments, SRM 5.1.1.0 is supported only on SLES 15 SP4.
- For SLES-based binary SRM deployments, contact the Administrator for the OS upgrade.
- For versions prior to SRM 5.x.x.x upgrading the Operating System from SLES 12 SP5 to SLES 15 SP4 is mandatory.
- SUSE Linux Enterprise 15 guest operating system option is not available in Hardware version 13 (ESXi 6.5) and earlier.

For more information, see Upgrade Operating System for vApp to SLES 15 SP4.

2

Pre-Requisites for Dell SRM 5.1.1.0 Upgrade

To successfully upgrade to Dell SRM 5.1.1.0, ensure to gather the required pre-requisites that are mentioned in this chapter.

Topics:

Required Tools and Credentials

Describes the tools and credentials required for SRM upgrade.

List of necessary tools:

- WinSCP or equivalent
- Putty/SSH
- Remote Desktop

Gather the necessary credentials:

- root/administrator credentials for the servers.
- Access to vCenter to take snapshots and validate vApp properties.

MySQL

This section describes the requirements for the latest version of MySQL.

MySQL's latest version requires the following ncurses and VC++ versions:

- ncurses-libs-6.2-10.20210508.el9.x86_64
- ncurses-compat-libs-6.2-10.20210508.el9.x86_64

For Windows:

Microsoft Visual C++ 2019 redistributable package is required for the latest version of MySQL.

Pre-Upgrade Health Check Utility Script

This section provides information about the pre-upgrade Health Check Utility script to be used before the upgrade for all vApps and binary-based SRM servers.

For more information about scripts, see the following documents in Dell Support Site:

- Dell SRM Distributed Pre-Upgrade-Health-Check Utility
- Dell SRM and Storage M&R AIO Pre Upgrade Health Check Utility

Verify environment status

Before starting the upgrade process, verify and document the environment status. It helps you to evaluate the success of the upgrade.

Check Custom vApp Configuration

Do not install any external packages or software, either by using manual SSH or any other means on SRM vApp servers.

If any custom/additional packages or software is already installed on SRM vApp servers, then do not attempt the System upgrade.

The support executives must examine the compatibility of the custom configuration before proceeding to the Operating System upgrade.

Check /etc/sudoers File on Each vApp VM

Steps

1. Run - `tail /etc/sudoers`.
2. The last lines must be:

```
#includedir /etc/sudoers.d   # added by MnR platform
```

3. If the above line is missing, the upgrade of Operating System Components fails. Download and run the vApp update patch.zip on all vApp servers. For more information, see KB 000061512. It prepares the vApp servers for the Operating System upgrade. If the upgrade is already completed, then running this patch file fixes the vApp and updates the Operating System upgrade components on each server.

Check vApp Options for Dell SRM VMs

Steps

1. Select the VM, click **Configure** tab on vSphere client and select **vApp options**.
2. Verify that **vApp options are enabled** message is displayed.

   ⓘ **NOTE:** If your Dell SRM VMs installations are geographically distributed in different locations, the deployment must still meet the network latency limits that are described in the Dell SRM Performance and Scalability Guidelines at Dell Support Site.

Check Server Reachability

Steps

1. Log in to the Dell SRM UI and go to the **Administration** > **CONFIG**.
2. Click **Settings** > **Configure Servers**.
3. Check that the connection is established for all the servers of the SRM setup.

Verify Reports

About this task

On the SRM Frontend UI, verify the following:

Steps

1. Look for blank reports and graphs. Determine if collection errors cause any blank reports. Resolve any issues and document them for later follow-up.
2. Look for broken links and resolve any issues or document them for later follow-up.
3. Validate that topology is working. Resolve any issues.
4. Review the existing backends and database.

   Check the following reports:

   - **Report Library** > **System Health** > **Summary** > **Logical Summary** > **Backends** > **Components** > **Backends**
   - **Report Library** > **System Health** > **Summary** > **Logical Summary** > **Backends** > **Components** > **Databases instances**
   - Check backend thresholds to verify that there is space to accommodate new sizing.
   - Add more additional backends and databases as required.
5. Ensure that there is 5 GB available on the files systems where Dell SRM is installed. Check **Report Library** > **System Health** > **Daily Dashboard** > **File Systems**.
6. Review and document any customization.

   For example:

   - Polling intervals
   - Timeout values
7. Go to administrator page and verify if all the services are running on each host by checking **SYSTEM ADMIN** > **Servers & Modules** > **Services**.

Backup the Environment

Ensure proper backup of all the servers in the environment. It includes the Frontend, Backend, and Collector hosts.

It is mandatory to upgrade SRM vApp based deployments to SLES 15 SP4 and this process is disruptive. Ensure to take snapshots of powered off VMs on SRM setup.

Before starting the upgrade, use **Discovery Center** to export all the SolutionPack devices.

If you encounter any problems during the upgrade, these snapshots allow you to quickly recover. After the upgrade is completed without any errors, you can delete these snapshots.

NOTE:

- If a VMware snapshot of each VM is not allowed, you should completely power cycle the vApps and/or VMs before starting the upgrade. Notify all users not to log in during the upgrade.
- Due to the addition of fields **Secure Vault** and **Unique Key** in the **Manage Discovery** page, the older CSV files that are used for devices will not work. To import devices in Discovery Center, use the new CSV template from the Discovery Center and move the data from old CSV files to the new template.
- The fields **Secure Vault** and **Unique Key** should not be left empty in the CSV files during import. Use the default value * for **Unique Key** and **false** for **Secure Vault**, in case the values are not available.

For more information about backup system, see the following guides in Dell Support Site:

- Dell SRM: Backing Up with VMware vSphere Data Protection Advanced 5.8
- Dell SRM: vApp Backup and Restore Using Dell EMC NetWorker.
- Dell SRM: Backing up with Dell EMC Avamar 7.1.
- Dell SRM: vApp Backup and Restore Using IBM Tivoli Storage Manager.
- Dell SRM: vApp Backup and Restore Using Symantec NetBackup.
- Dell SRM: vApp Backup and Restore using Commvault Simpana Virtual Server Protection.

The above pointers are available in the Dell SRM 4.10.0.0 Advanced Configuration Guide at Dell Support Site.

Backup Firewall

- After OS Upgrade to SLES 15 SP4, SuSEfirewall2 is replaced by Firewalld.

  All the custom firewall settings will be lost.

- Save or export any custom firewall settings. Reapply the firewall settings post Operating System Upgrade.
- Take a backup on all the vApp VMs.

Set Java Certificates

If you have previously imported your LDAP SSL certificates, Dell Technologies recommends that you allow the upgrade to overwrite the certificates.

You can import the certificates again using the new method (described in the Communication security settings section of the Dell M&R Security Configuration Guide, which is available from the Dell Support Site). The new method improves overall security as any changes to the default trust store that ships with Java and is reflected in your environment.

If you cannot import the certificates using this new method, migrate the certificates manually, but you get the benefits of the new method.

Saving the Java certificates file

About this task

If you have previously imported your LDAP SSL certificates, Dell Technologies recommends that you allow the upgrade to overwrite the certificates. After this, you can import the certificates again using the new method (described in the "Communication security settings" section of the *Dell M&R Security Configuration Guide*, which is available from the Dell Support Site). The new method survives upgrades, and improves overall security as any changes to the default trust store that ships with Java and is reflected in your environment.

If you not able to import the certificates using this new method, migrate the certificates manually , but you will get the benefits of the new procedure. To manually migrate the certificates, save the certificates file before the upgrade, and restore them after the upgrade.

Steps

1. To save the certificates file before the upgrade, go to this directory: `${APG INSTALL DIRECTORY}/Java/Sun-JRE/<Java version>/lib/security`.
   For example, `cd /opt/APG/Java/Sun-JRE/<Java version>/lib/security`.
2. Copy the `cacerts` file to a safe place. (Do not use the Java installation directory as the new installation deletes and replaces it .)
   For example, `cp cacerts /var/tmp/cacerts`.

Import Java Certificates

If you are upgrading from 3.7.x or later, use the new method to import certificates into the trust store for use in LDAP, device discovery, or other secure communication. If you are leveraging SSL communications and have previously imported certificates into the product to enable this, you must perform a one-time operation to reimport them using this new method. Once you have done this, the import will persist across future upgrades.

About this task

ⓘ **NOTE:** If you have already imported the certificates using this method, do not import them again.

Steps

1. Check to see if there are any certificate files at `<APG_HOME>/Java/Sun-JRE/<version>/customcerts`. If there are any certificates, your certificates will be automatically migrated during the update, and you can skip the next step.
2. If there are no certificate files at `<APG_HOME>/Java/Sun-JRE/<version>/customcerts`, then any certificates you previously added manually will not persist across the upgrade to SRM 5.1.1.0 You should perform a one-time reimport of the certificates file as described in the Importing custom certificates into the JRE section of the Dell M&R Security Configuration Guide at Dell Support Site.

Backup Alert Definitions

Take backup of the modified or customized alert definitions.

About this task

To take backup of alert definitions which might have been modified or customized, follow these steps:

ⓘ **NOTE:** If the customization to the alert definitions is done using only threshold values, then back-up of alert definitions is not required as threshold values are retained after upgrade.

Copying the alert definitions does not copy the alerting contexts. To add alerting context, right-click the wanted alert definition in the table and select Configure Options.

Steps

1. Go to **Admin** > **Config** > **Alerts** > **Manage Alert Definitions**.
2. Select the folder which contains alert definitions that you want to backup and click **Export Selected Definitions**. To take a backup of all available alerts, select **Alert definitions** and then click **Export All Definitions**.
3. To export alerting-contexts.xml, in versions earlier to SRM 4.3, keep a copy of the alerting-contexts.xml from `/opt/APG/Backends/Alerting-Backend/conf` directory.
4. To export alerting-contexts.xml, in SRM 4.3.x and later versions, go to **Alerting Frontend UI**.
5. Under **Local Manager**, click **Alert Definitions**.
6. In the left pane, click **Export** button.

   A ZIP file which contains both alerting.xml and alerting-contexts.xml is downloaded.

Delete Backup Schedules and Scheduled Reports from DPA Server

Remove backup schedules and scheduled reports from the Data Protection Advisor server before the upgrade.

Steps

1. If Avamar is discovered:
   a. Go to **Reports** > **Report Jobs** > **Schedule Report**, and delete the following reports:
      - W4N-Avamar All Jobs Report
      - W4N-Avamar Client Configuration Report
      - W4N-Avamar Restore Details Configuration Report
      - W4N-Avamar Server Configuration Report

   b. Go to **Admin** > **System** > **Manage Schedules**, and delete the following schedule:
      - Avamar-1HourInterval
2. If NetBackup is discovered:
   a. Go to **Reports** > **Report Jobs** > **Schedule Report**, and delete the following reports:
      - W4N-NetBackup All Jobs Report
      - W4N-NetBackup Client Configuration Report
      - W4N-NetBackup Disk Volume Configuration Report
      - W4N-NetBackup Disk Volume Status Report
      - W4N-NetBackup Restore Details
      - W4N-NetBackup Server Configuration Report
      - W4N-NetBackup Storage Unit Configuration Report

   b. Go to **Admin** > **System** > **Manage Schedules**, and delete the following schedule:
      - NBU-1HourInterval

Boot Space Clean Up

If the SRM setup is being upgraded from SRM 4.3.1 to SRM 4.9.x.x or 4.10.x.x and then to SRM 5.1.x.x, you must remove `/boot/initrd-3.0X` file in all the vApp VMs from the boot directory before starting the OS Upgrade to SLES 15 SP4.

3

Upgrade Operating System for vApp to SLES 15 SP4

For versions prior to SRM 5.x.x.x, upgrading the Operating System from SLES 12 SP5 to SLES 15 SP4 is mandatory.

Topics:

- Upgrade Operating System Using an ISO Image
- MySQL Database Check

Upgrade Operating System Using an ISO Image

Perform the below summary of steps for a successful Operating System upgrade to SLES 15 SP4 using ISO image.

- Download ISO Image from Dell Online Support Website
- Configure ISO Image for Each SRM VMs
- Upgrade Operating System Using ISO Image on SRM Setup
- Operating System Upgrade on FrontEnd VM Using ISO Image

Download ISO Image from Dell Online Support Website

This section provides details on ISO image deployment from the Dell Online Support Website.

Prerequisites

Gather the following information:

- vCenter location where you plan to upload the ISO image.
- Data Store to be used for ISO should be accessible by all SRM VMs (vApp based).

Steps

1. Download the ISO image (`SLES15sp4_OS-5110-ISOimage.zip`) from the Dell Online Support Website.
2. Extract `SLES15sp4_OS-5110-ISOimage.zip` to get the ISO image.
3. Open vCenter Client and connect to the vCenter Server that manages the VMware environment.
4. Select the Datastore to which the ISO image must be uploaded.

   See the VMWare Link for further guidance.

Configure ISO Image for Each SRM VMs

Perform the following reconfiguration for SRM VMs (vApp based)

Steps

1. Log in to the vCenter Client and select the VMs.
2. Power off the VM.
3. Right-click the VMs and click **Edit Settings**.
4. In the **Virtual Hardware** tab, click on **ADD NEW DEVICE**, point the **CD/DVD Drive 2** setting to **DataStore ISO File.**
5. Expand the **CD/DVD Drive 2** option to display the **CD/DVD Media** location, then click **Browse**.
6. Go to the data store in which the ISO image is stored and then select the ISO image.
7. Click **OK** to close the Browse window.

8. Select **Connect At Power On** option for **CD/DVD Drive 2**.
9. Click **OK** on the **Edit Settings** pane to close the window and reconfigure the VMs settings.
10. Check the **Recent Tasks** pane of the vCenter Client to confirm that the VMs are reconfigured successfully.
11. Power on the VM.

Upgrade Operating System Using ISO Image on SRM Setup

To perform Operating System upgrade for SRM deployment using ISO image, follow these steps.

Prerequisites

- Download the ISO Image and upload it to a Datastore. For more information, see Download ISO Image from Dell Online Support Website.
- For SRM VMs, gather the following information:
  - IP address and root login credentials
  - Access to vCenter to take snapshots and validate vApp properties
- From the Dell Online Support Website, download the `SLES15sp4_OS_Upgrade-Scripts-5110.zip` file that contains the scripts for Operating System upgrade.
- Confirm that the snapshot of SRM VMs has been taken before starting Operating System upgrade to SLES 15 SP4.
- To run the upgrade process using the ISO approach, it is mandatory that the CD drive of each SRM VM point to the ISO location on the vCenter server.

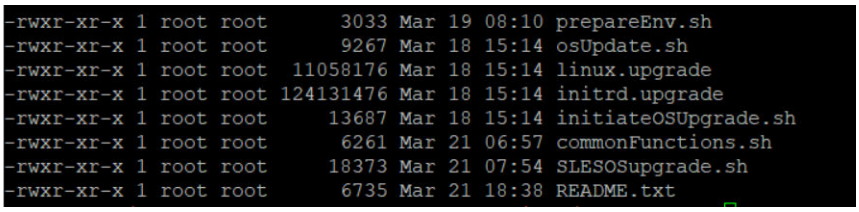
> **NOTE:** The following order should be followed for Operating System upgrades:
> - All remote VMs
> - Frontend VM

Steps

1. In vCenter UI/vSphere client, access each VM setting and ensure that the ISO file is available and connected as a CD/DVD Drive for all the vApp VMs in SRM setup.
2. Log in to the Frontend appliance.
3. Go to the directory where `SLES15sp4_OS_Upgrade-Scripts-5110.zip` is copied on the VM.
4. Run the following command to extract the file:

   ```
   unzip SLES15sp4_OS_Upgrade-Scripts-5110.zip
   ```

5. Go to the **OSUpgrade** directory and list the contents to check on the scripts. The following scripts must be present:

   ```
   -rwxr-xr-x 1 root root      3033 Mar 19 08:10 prepareEnv.sh
   -rwxr-xr-x 1 root root      9267 Mar 18 15:14 osUpdate.sh
   -rwxr-xr-x 1 root root  11058176 Mar 18 15:14 linux.upgrade
   -rwxr-xr-x 1 root root 124131476 Mar 18 15:14 initrd.upgrade
   -rwxr-xr-x 1 root root     13687 Mar 18 15:14 initiateOSUpgrade.sh
   -rwxr-xr-x 1 root root      6261 Mar 21 06:57 commonFunctions.sh
   -rwxr-xr-x 1 root root     18373 Mar 21 07:54 SLESOSupgrade.sh
   -rwxr-xr-x 1 root root      6735 Mar 21 18:38 README.txt
   ```

   Go through the **README** file for the Operating System upgrade script to know more details about the script.

6. Run the following command to create a list of vApp Remote Servers:

   ```
   SLESOSupgrade.sh -u remoteServer
   ```

7. Once the script is started, a CSV list of vApp based VMs will be created in `/opt/ADG/osupdate/SRMVMList.csv`.
8. Rerun the following command to start Operating System upgrade on the remote servers:

   SLESOSupgrade.sh -u remoteServer

9. Provide the root password for all the remote servers when prompted after which the script initiates Operating System upgrade on the SRM VMs.
10. Once the upgrade is initiated on all the VM (except the FE), use the following command to monitor the progress of upgrades on the VMs:

    ```
    SLESOSupgrade.sh -s status
    ```

    The output is a tabular format that displays the Server name and the corresponding OS version.

If the Corresponding OS version is "-", still servers OS upgrade is not completed.

11. The Operating System upgrade to SLES15 SP4 is an offline upgrade and hence to further monitor the Operating System upgrade, login to the vSphere Client console for the SRM VMs.

    The Operating System upgrade is configured to go ahead automatically and does not require any user intervention.
12. Once the Operating System upgrade to SUSE 15 SP4 is done, a login prompt is displayed on the console.

Operating System Upgrade on FrontEnd VM Using ISO Image

Prerequisites

1. To check the status of all the VMs, use the following command on the Frontend VM:

   ```
   SLESOSupgrade.sh -s status
   ```
2. The Operating System version for all the vApp VMs should be displayed as 15.4.

Steps

1. After all the VMs are upgraded, the Frontend VM must be upgraded using the following command:

   ```
   SLESOSupgrade.sh -u currentServer
   ```
2. The command will now check the Operating System version of all the VMs registered with this Frontend. If all remote VMs are upgraded to SLES 15 SP4, the Operating System upgrade of the Frontend VM proceeds.
3. The Operating System upgrade to SLES15 SP4 is an offline upgrade and hence to further monitor the Operating System upgrade, log in to the vSphere Client console for the Frontend VM.

   The Operating System upgrade is configured to go ahead automatically and does not require any user intervention.

MySQL Database Check

After OS Upgrade to SLES 15 SP4, run below command to repair any database failures on Primary Backend and Additional Backends.

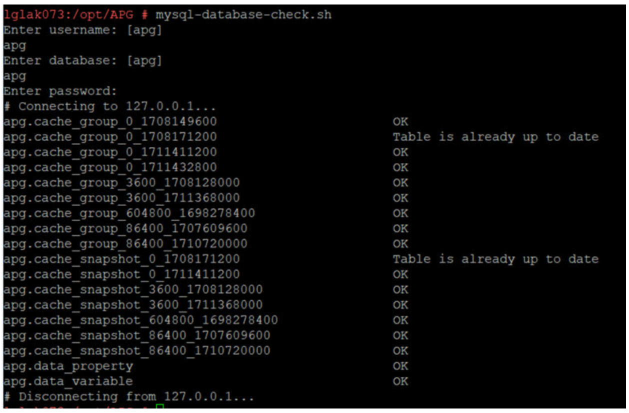
On Primary Backend, provide 'apg' database details:

```
/opt/APG/bin/mysql-database-check.sh
```

On Additional Backends, provide 'apg1', apg2', 'apg3' and 'apg4' details:

```
/opt/APG/bin/mysql-database-check.sh
```

Example



```
lglak073:/opt/APG # mysql-database-check.sh
Enter username: [apg]
apg
Enter database: [apg]
apg
Enter password:
# Connecting to 127.0.0.1...
apg.cache_group_0_1708149600                       OK
apg.cache_group_0_1708171200                       Table is already up to date
apg.cache_group_0_1711411200                       OK
apg.cache_group_0_1711432800                       OK
apg.cache_group_3600_1708128000                    OK
apg.cache_group_3600_1711368000                    OK
apg.cache_group_604800_1698278400                  OK
apg.cache_group_86400_1707609600                   OK
apg.cache_group_86400_1710720000                   OK
apg.cache_snapshot_0_1708171200                    Table is already up to date
apg.cache_snapshot_0_1711411200                    OK
apg.cache_snapshot_3600_1708128000                 OK
apg.cache_snapshot_3600_1711368000                 OK
apg.cache_snapshot_604800_1698278400               OK
apg.cache_snapshot_86400_1707609600                OK
apg.cache_snapshot_86400_1710720000                OK
apg.data_property                                  OK
apg.data_variable                                  OK
# Disconnecting from 127.0.0.1...
```

Upgrade to Dell SRM 5.1.1.0

You can upgrade to Dell SRM 5.1.1.0 by using the new update platform or system upgrade wizard.

Topics:

Upgrade to SRM 5.1.1.0 using the new update platform

As the Online Update Server is deprecated, the online update feature in SRM is now supported using the scheduled task **cup-online-update-check.task**.

Prerequisites

Before enabling and running the **cup-online-update-check.task**, ensure the following:

- **Dell Technologies Connectivity UI** is configured.
- A successful server connection is established.

Steps

1. Access Scheduled Tasks:

   Go to **SRM Admin** > **Config** > **Settings** > **Scheduled Tasks**.
2. Locate the Task:

   Search for the task named *CupOnlineUpdate*.
3. Enable the Task:

   Enable the *cup-online-update-check.task* task.
4. Run the Task:

   Run the task. The task begins downloading the relevant update bundle artifacts from the CUP Server into the SRM.
5. Verify Task Completion:

   Upon task completion, check the **task status** to ensure that it has run successfully.
6. Check for Updates:

   - Go to **SRM Admin** > **Config** > **Update System** > **System Update**.
   - Confirm that the **Update UI** displays the latest available SRM version for upgrade.
7. Proceed with the Upgrade:

   Click **Go to Maintenance Mode** in the Update UI to initiate the SRM upgrade process.

   NOTE:

   - Availability:

     This feature is available starting from SRM 5.0.2.0.
   - Disable After Completion:

     To prevent the task from running automatically in the future, disable the task after its successful run.
   - Compatibility:

This feature is compatible only with setups having same Operating System. Supported environments include:

- Only vApp
- Only Windows Binaries
- Only Linux Binaries

Upgrade to SRM 5.1.1.0 Using System Upgrade Wizard

Steps

1. Download the core update file for each of the deployed architectures from the Dell Online Support Website. The vApp file also contains the appliance update file for vApp deployments.

Option	Description
Linux (vApp)	`SRM_5.1.1.0_vApp_Update_UI.zip`
Linux (binary only)	`SRM_5.1.1.0_Linux_64-bit_Update_File.zip`
Windows	`SRM_5.1.1.0_Windows_64-bit_Update_File.zip`

2. From the SRM Admin UI, click **CONFIG** > **Update system** > **System Update**.

   ⓘ **NOTE:** Dell Technologies recommends using Chrome or Firefox browsers as IE does not update the progress bars.

3. For the Linux and/or Windows deployments, click **Browse** and select the update file.
4. Click **Upload Content**.
5. The system displays a message about ensuring that there is a minimum of 5 GB disk space on the servers. Click **OK**.

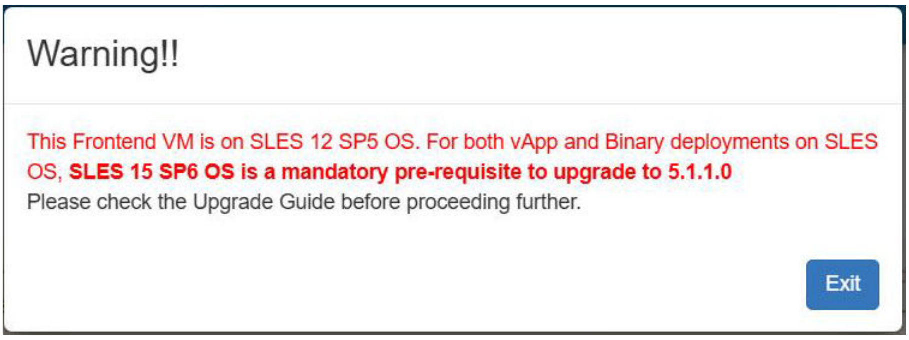
   The system upgrade files are uploaded to Administration and nondisruptively distributed to all the servers in the deployment. This process may take several minutes.

   ⓘ **NOTE:** Before proceeding with the upgrade process, it is recommended to run the `Pre-Upgrade-Health-Check-Utility-Script` from the Dell Support Site. The SRM UI also displays a dialogue box notifying the users to run the `Pre-Upgrade-Health-Check-Utility-Script` before upgrade.

6. When you are ready to proceed with the upgrade, click **Go to maintenance mode**.
   Maintenance mode begins, the Frontend becomes unavailable, and you are redirected to the Platform Upgrade page.

   ⓘ **NOTE:**

   - For vApp based SRM if the Operating System is not SLES 15 SP4, then system prompts a warning message to exit the upgrade process. Ensure to upgrade the Operating System to SLES 15 SP4 for all servers before proceeding for upgrade process.

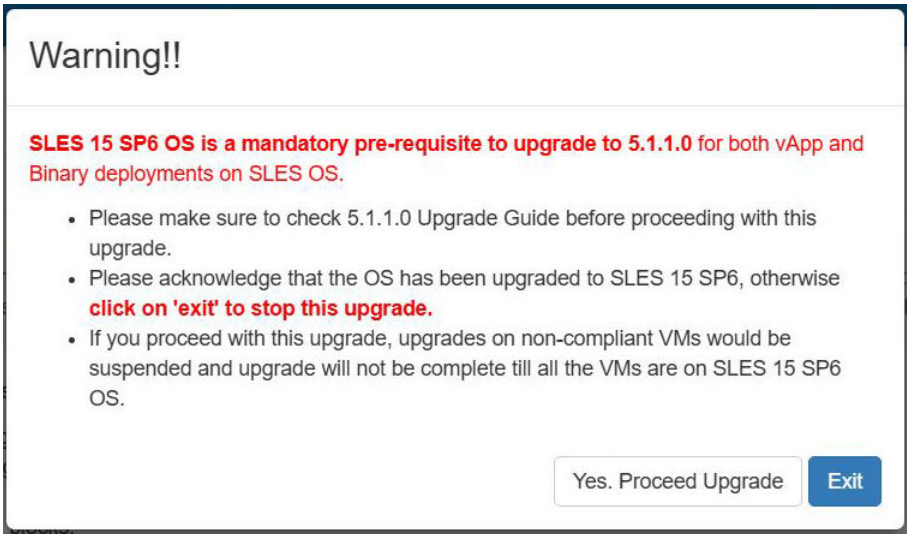


Warning!!

This Frontend VM is on SLES 12 SP5 OS. For both vApp and Binary deployments on SLES OS, **SLES 15 SP6 OS is a mandatory pre-requisite to upgrade to 5.1.1.0**

Please check the Upgrade Guide before proceeding further.

7. For versions prior to SRM 5.1.1.0, before beginning the upgrade, the system prompts for a confirmation from the user that all servers with SLES 12 SP5 (both vApp and binary) are upgraded to SLES 15 SP4.



Warning!!

SLES 15 SP6 OS is a mandatory pre-requisite to upgrade to 5.1.1.0 for both vApp and Binary deployments on SLES OS.

- Please make sure to check 5.1.1.0 Upgrade Guide before proceeding with this upgrade.
- Please acknowledge that the OS has been upgraded to SLES 15 SP6, otherwise **click on 'exit' to stop this upgrade.**
- If you proceed with this upgrade, upgrades on non-compliant VMs would be suspended and upgrade will not be complete till all the VMs are on SLES 15 SP6 OS.

8. Click **Yes, Proceed Upgrade** after confirming that all the servers with SLES12 SP5 (both vApp and binary based) are upgraded to SLES15 SP4.

   NOTE: If you click the **Yes, Proceed Upgrade** option without upgrading all SLES12 SP5 based servers to SLES15 SP4, such upgrades on noncompliant vApp based servers gets suspended and overall upgrade of the setup cannot be completed. This results in an unsupported configuration from which the system must be recovered. See Troubleshooting Process for SLES15 SP4 before attempting the upgrade again.
9. If all the servers are not upgraded to SLES15 SP4, then click the **Exit** button to stop the update manager.
10. Check the status of the Tomcat service, and if required start the Tomcat service and navigate back to the admin UI. From putty connect to SRM vApp's Frontend server, run the command manage-modules.sh service start tomcat.
11. Once the validation checks are completed, click **Launch upgrade**.
    The upgrade begins. After several minutes, the **Upgrade status** displays. When the upgrade is complete, the system displays a green check mark next to each node and a success message at the top of the window.
12. Click **Exit**.
13. Click **OK**.

    The system restarts the Frontend, and redirects you to the Solution Packs UI on the Administration Page. All the SRM servers are rebooted.
14. Verify that all the services are running on each host by checking **SYSTEM ADMIN** > **Servers & Modules** > **Services**.

Upgrade the embedded ESE version to the latest on Linux

Steps

1. **If ESE is not installed on the previous SRM release, do the following to install ESE:**
   a. Log in as **root** user to the Frontend appliance using Putty.
   b. Go to `<APG_Install_DIR>/Tools/ESE-Manager/<ESE_Version>/` and run the following command with root credentials.

      ```
      sh ese_manual_install.sh
      ```
2. **If ESE is installed on the previous SRM release, upgrade ESE:**
   a. Log in as **root** user to the Frontend appliance using Putty.
   b. Go to `<APG_Install_DIR>/Tools/ESE-Manager/<ESE_Version>/` and run the following command with root credentials.

      ```
      sh ese_upgrade.sh
      ```

3. To confirm if ESE is listening on port **9443**, type the following command:

```
SuSE: netstat -ntlp | grep 9443
RHEL: lsof -i -P -n | grep 9443
```

4. After upgrading ESE, on the **SRM Admin UI** page go to **CONFIG** > **Settings** > **Dell Technologies Connectivity** and click **Test Server Connectivity** icon giving the new AccessKey/PIN.
   a. Generate new AccessKey/PIN at Dell Product Support.
   b. Enter the generated AccessKey/PIN and click **Save**.
5. On the **SRM Admin UI** page, go to **CONFIG** > **Settings** > **Dell Technologies Connectivity** and click **Test Server Connectivity** icon to verify that connection to Dell server is successful.

   The ✓ icon indicates that connectivity to the server has been established.

   The icon indicates that connectivity to the server failed.
6. After successful connection, to confirm the version of ESE installed, use the following command

   curl -k -H $'x-dell-auth-key: Afor!@#akhdqwihqiu34344_y9yfqiwiwuefi56w3AABweuf' https://localhost:9443/ese/status

Upgrade the embedded ESE version to the latest on Windows

Steps

1. **If ESE is not installed on the previous SRM release, do the following to install ESE**:
   a. On Frontend VM, open the command prompt in Admin mode.
   b. Go to `<APG_Install_DIR>\Tools\ESE-Manager\<ESE_Version>\` and run the command `ese_manual_install.bat` as administrator.
2. **If ESE is already installed on the previous SRM release, upgrade ESE:**
   a. On Frontend VM, open the Command Prompt in Admin mode.
   b. Go to the location where `<APG_Install_DIR>\Tools\ESE-Manager\<ESE_Version>\` is installed and run the `ese_upgrade.bat` command as administrator.
3. To confirm if ESE is listening on port **9443**, type the following command:

```
netstat -aon | findstr 9443
```

4. After upgrading ESE, on the **SRM Admin UI** page go to **CONFIG** > **Settings** > **Dell Technologies Connectivity** and click **Test Server Connectivity** icon to verify that connection to Dell server is successful.

   The ✓ icon indicates that connectivity to the server has been established.

   The icon indicates that connectivity to the server failed.

Upgrade the embedded ESE version to the latest on vApp

Steps

1. **If ESE is not installed on the previous SRM release, do the following to install ESE:**
   a. Log in as **root** user to the Frontend appliance using Putty.
   b. Go to `<APG_Install_DIR>/Tools/ESE-Manager/<ESE_Version>/` and run the following command with root credentials.

      `sh ese_manual_install.sh`

2. **If ESE is installed on previous SRM release, upgrade ESE:**
   a. Log in as **root** user to the Frontend appliance using Putty.
   b. Go to `<APG_Install_DIR>/Tools/ESE-Manager/<ESE_Version>/` and run the following command with root credentials.

      ```
      sh ese_upgrade.sh
      ```

3. To confirm if ESE is listening on port **9443**, type the following command:

   ```
   sudo lsof -i -P -n | grep 9443
   ```

4. After upgrading ESE, on the **SRM Admin UI** page go to **CONFIG** > **Settings** > **Dell Technologies Connectivity** icon giving the new AccessKey/PIN.
   a. Generate new AccessKey/PIN at Dell Product Support.
   b. Key in newly generated AccessKey/PIN and click **Save**.
5. On the **SRM Admin UI** page, go to **CONFIG** > **Settings** > **Dell Technologies Connectivity** and click **Test Server Connectivity** icon to verify that connection to Dell server is successful.

   The ✓ icon indicates that connectivity to the server has been established.

   The 📉 icon indicates that connectivity to the server failed.
6. After successful connection, to confirm the version of ESE installed, use the following command:

   ```
   curl -k -H $'x-dell-auth-key: Afor!@#akhdqwihqiu34344_y9yfqiwiwuefi56w3AABweuf' https://
   localhost:9443/ese/status
   ```

5

Upgrade the SolutionPacks

After you upgrade to the latest version of Dell SRM, you must upgrade the installed SolutionPacks and other Components.

> **NOTE:** For the 4.9.0.0 upgrade, the snapshot metrics related to the following SolutionPacks turn inactive, as the snapshot retention group is modified for these SolutionPacks:
>
> - Dell Unity
> - Dell PowerMax
> - Dell PowerStore
> - NetApp FAS
> - Pure Storage
> - IBM FlashSystem
>
> For the 4.10.0.0 upgrade, the snapshot metrics related to the following SolutionPacks turn inactive, as the snapshot retention group is modified for these SolutionPacks:
>
> - HPE Nimble
> - IBM XIV
> - IBM DS
> - Dell EMC XtremIO
> - Dell PowerVault
> - Dell PowerFlex

Post upgrade, it is recommended to clean up the snapshot related inactive metrics after 24 hours.

> **NOTE:** In SRM 4.8 Release, PowerFlex devices were identified as Block type devices. From SRM 4.9 onwards, PowerFlex 4.x devices are identified as Unified devices. Due to this, a couple of new metrics are added and old metrics are turned inactive within 14 days. Until old metrics are turned inactive, few global reports continue to display data for both Block and Unified types. However, after the old metrics turn inactive, reports are displayed only for Unified type.

Topics:

Upgrade all SolutionPacks and other components

Prerequisites

Synchronize the packages and upgrade Solution Packs.

Steps

1. Synchronize the packages across the servers:
   a. On the SRM Administration page, click **CONFIG** > **Settings** > **Show Advanced** > **Manage Packages**.
   b. Click **Synchronization**.
   c. From the drop-down menu, select **retrieve the latest packages**.
   Wait for the synchronization to complete before proceeding.

   > **NOTE:** When you upgrade the SolutionPack for Dell RecoverPoint, the polling interval set during the SolutionPack installation is lost since the polling intervals for capacity and performance data collection are separated.

2. Avoid duplicate alert definitions: If you want to preserve the customized alert definitions, complete the following two optional steps before proceeding:

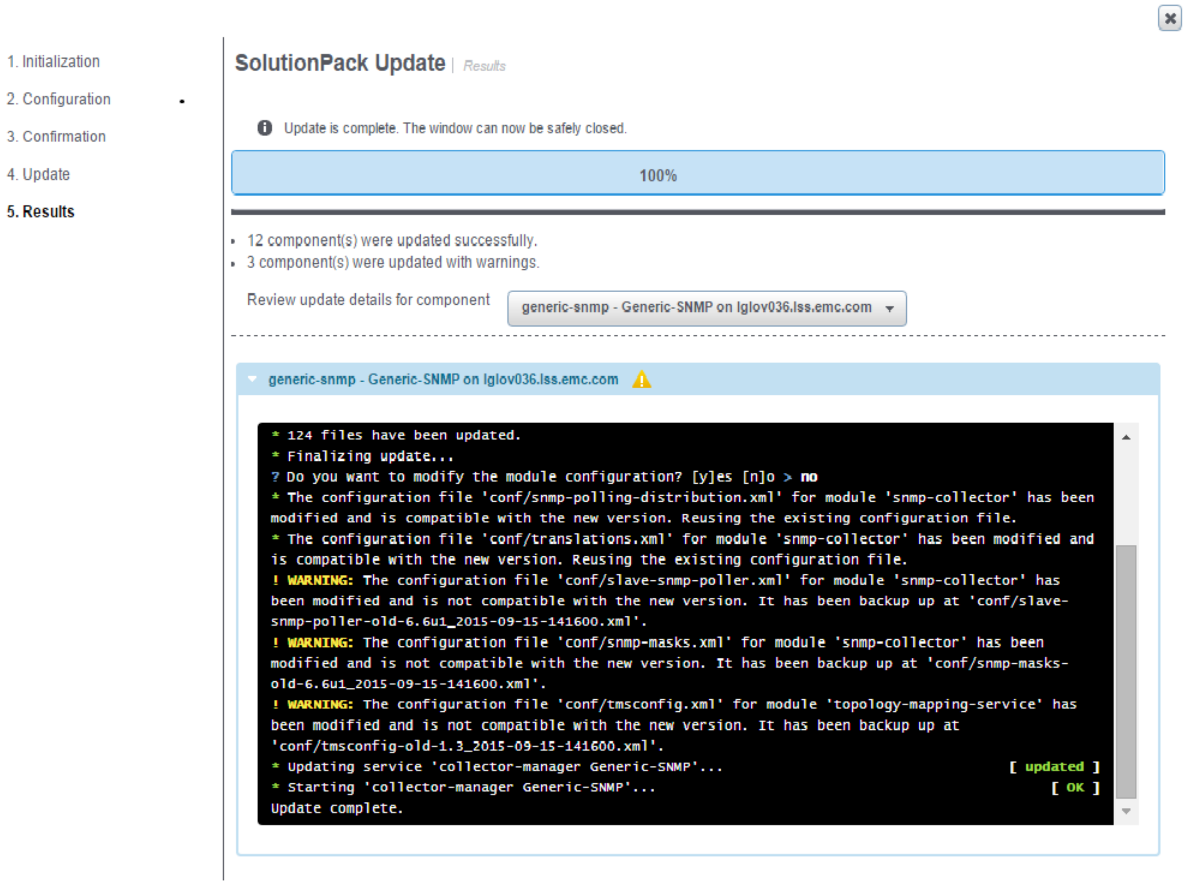
   a. Optional: Back up alert definitions for all SolutionPacks by exporting Alert definitions from the Alerting Frontend. To backup the definitions for an individual SolutionPack, click the SolutionPack folder name and export from there.
   b. Optional: Back up the `alerting-contexts.xml` file by browsing **Configuration** > **Alerts** > **Manage Alert Defnitions** from Administration. The `alerting-contexts.xml` file is located under **Configuration Files**. Copy the entries from the file that correspond to the alert definitions that you want to back up.
3. On the SRM Administration UI, click on **CONFIG** > **Solution Packs** > **Installed Solution Packs**.
4. Click the **Update All Components** button in the upper right corner of the page.

   NOTE: If the **Update All Components** button is disabled, the system has all the latest SolutionPacks, and you can skip the remaining steps.

   The **Initialization** window opens and lists the following details:
   - Number of components from SolutionPacks that is updated to the latest version.
   - Number of components that contain new features that require configuration.
5. To open the **Configuration** window, click **Next**. The left pane lists each of the components that include new features that you must configure. The right pane displays the configuration details for the component with the new features that are selected in yellow. To ensure that the configuration details for the components and SolutionPacks are correct, carefully review the selections, and modify any configuration that is not set correctly. When you have finished configuring a component, click **Next** to move onto the next component. The following SolutionPack entries must be modified while reviewing the configuration:
   - For the SolutionPack for Dell PowerScale, select an existing Frontend web service or add a new service.
   - For the SolutionPack for Dell EMC ScaleIO, select an existing Frontend web service or add a new service.
   - For the Configuration Compliance SolutionPack, ensure the **Compliance Backend Instance** field value is the same as Instance Name of Compliance Backend in the previous version. Previous name can be found from **Administration** > **CONFIG** > **Configuration Compliance** > **Compliance-Backend under Properties: Instance Name**. Typically the instance name is Generic-Compliance.
6. After you have configured every component on the list, click **Next**.
7. The **Confirmation** window opens and lists all the components that are updated. Confirm that all the components are listed correctly, and then click **Update**.
8. The **Update** window opens and displays the progress of each update, and the percentage complete of the overall update. Do not close the browser window during this step.

   The update process detects if any manual edits were made to the SolutionPack files. If a manually edited file is compatible with the new version of the SolutionPack, it is reused and the system displays a message, stating that if a manually edited file is not compatible with the new version of the SolutionPack, the system backs up the file to display a warning message. The warning message indicates the name and location of the incompatible file. The backed-up files are saved in their current directory with the following format: `<file-name>-old-<version>_<date>.<ext>`

   Messages about the following incompatible files can be ignored:
   - tmsconfig.xml
   - snmp-masks.xml
   - slave-snmp-poller.xml
   - emc-vmax-mapping.xml
   - vnxalerts-block-deviceid-<ID>-laststarttime.xml
   - vnxalerts-file-deviceid-<ID>-laststarttime.xml



Update is complete. The window can now be safely closed.

- 12 component(s) were updated successfully.
- 3 component(s) were updated with warnings.

Review update details for component: generic-snmp - Generic-SNMP on lglov036.lss.emc.com

generic-snmp - Generic-SNMP on lglov036.lss.emc.com

```
* 124 files have been updated.
* Finalizing update...
? Do you want to modify the module configuration? [y]es [n]o > no
* The configuration file 'conf/snmp-polling-distribution.xml' for module 'snmp-collector' has been
modified and is compatible with the new version. Reusing the existing configuration file.
* The configuration file 'conf/translations.xml' for module 'snmp-collector' has been modified and
is compatible with the new version. Reusing the existing configuration file.
! WARNING: The configuration file 'conf/slave-snmp-poller.xml' for module 'snmp-collector' has
been modified and is not compatible with the new version. It has been backup up at 'conf/slave-
snmp-poller-old-6.6u1_2015-09-15-141600.xml'.
! WARNING: The configuration file 'conf/snmp-masks.xml' for module 'snmp-collector' has been
modified and is not compatible with the new version. It has been backup up at 'conf/snmp-masks-
old-6.6u1_2015-09-15-141600.xml'.
! WARNING: The configuration file 'conf/tmsconfig.xml' for module 'topology-mapping-service' has
been modified and is not compatible with the new version. It has been backup up at
'conf/tmsconfig-old-1.3_2015-09-15-141600.xml'.
* Updating service 'collector-manager Generic-SNMP'...                                [ updated ]
* Starting 'collector-manager Generic-SNMP'...                                             [ OK ]
Update complete.
```

9. The **Results** window opens. Use the drop-down list to check the status of each component. Any manually edited files that the system takes back up are displayed under **Updated with warnings**.
10. Verify that all the services are running on each host by checking **System Admin** > **Servers & Modules** > **Services** from Administration.
11. Restart the Tomcat service:
    a. Putty in to the Dell SRM Frontend server.
    b. Go to the `cd /opt/APG/bin` directory.
    c. Run the following command: `./manage-modules.sh service restart tomcat` for UNIX or `manage-modules.cmd service restart tomcat` for Windows
12. In Windows deployments, the Java module is updated during the upgrade, but the old version of Java is not removed. Dell Technologies recommends that you remove the older version of Java. Only the latest Java version folder should be kept. Remove the Java files as described in this message:

```
Some files were left behind after the update of Java...
Please manually remove directory <version number> from the path 'C:\Program
Files\APG\Java\Sun-JRE\<version number>’
```

NOTE: Please check in the Release Notes if any new module or solution pack is added/introduced in this current release or the recent releases after your base SRM versions. If yes, then

- For any new module of the respective Solution pack, follow the Solution Pack Installation process.
- For any new Solution pack, follow the Solution Pack Installation process.

6

Post-Upgrade Tasks

After you upgrade to the latest version of Dell SRM, you must complete the required additional tasks.

Topics:

LUN performance metrics collection is disabled by default for Dell VMAX/PowerMax SP

In SRM 4.9.0.0 release, LUN performance feature is supported in Dell VMAX/PowerMax SolutionPack for PowerMaxOS 10.0 array.

About this task

LUN performance metrics collection is disabled by default.

To enable LUN performance metrics collection:

Steps

1. Go to `/opt/APG/Collecting/Collector-Manager/emc-vmax-hypermax/conf` on the Collector VMs where emc-vmax-hypermax, or Dell VMAX/PowerMax Solution Pack is installed.

2. Open the `collecting.xml` file and search for the line with text `Unisphere-LUN-PERF` and edit as below:

   ```
   <collector enabled="false" name="Unisphere-LUN-PERF"
   next="VMAX_PTF_LUN_PURPOSE" config="Stream-Collector/emc-vmax-hypermax/conf/
   streamcollector-lun-perf-unisphere.xml" />
   ```

   To

   ```
   <collector enabled="true" name="Unisphere-LUN-PERF"
   next="VMAX_PTF_LUN_PURPOSE" config="Stream-Collector/emc-vmax-hypermax/conf/
   streamcollector-lun-perf-unisphere.xml" />
   ```

3. Restart collector manager services for the emc-vmax-hypermax Solution Pack (Dell VMAX/PowerMax).

   NOTE: Before enabling the LUN Performance collection, see Dell SRM Performance and Scalability Guidelines for changes in the collector configurations.

Check the Status of Remote Host Services

The remote host services should start automatically after an upgrade. Check the status of the services and restart them manually if they are not running.

Steps

1. Check that all services have started on each of the hosts:
   a. From SRM Admin UI, go to **SYSTEM ADMIN** > **Servers & Modules** > **Servers**.
   b. For each host, click the hostname.
   c. Verify that the status for each service is **Started**.

      If a service did not start automatically, restart the service manually.
2. Click the name of the service.
3. Click **Start**.
   If successful, the **Service Status** changes to **Started**. If the service does not start, review the log to determine the cause. The issue may be a misconfigured option. Reconfiguring the SolutionPack settings and manually starting the service again can resolve this issue.

Verifying and configuring the user process limits for vApp and Linux binary platforms

Verify and configure the user process limits for the apg user account on all VMs to a maximum of 512000.

Prerequisites

Ensure that you log in with root privileges.

Set user process limit in vApp installation using script. Follow the instructions in the KB 000184212 to run the script and set the user process limit.

Follow the steps below to change the limit on vApp/Binary.

Steps

1. Edit the security file:

   `vi /etc/security/limits.conf.`
2. Update the following lines for apg user to change limits from 65534 to 512000.

   ```
   apg hard nofile 512000
   apg soft nofile 512000
   ```

```
apg hard nproc 512000
apg soft nproc 512000
```

3. Save the file.
4. To verify the changes, type the following command:

   ```
   su apg -c 'ulimit -n -u'
   open files (-n) 512000
   max user processes (-u) 512000'
   ```

5. To restart the services, type the following commands from the `/opt/APG/bin` directory of the installation:

   ```
   /opt/APG/bin/manage-modules.sh service stop auto
   /opt/APG/bin/manage-modules.sh service start auto
   /opt/APG/bin/manage-modules.sh service status all
   ```

Security Hardening on SRM vApps

There are standard STIG hardening rules that are supported by default on SRM vApp.

For more information, see the Dell SRM Security Hardening Guide at Dell Support Site.

Import or change any custom firewall settings.

Reset the password for the Compliance Backend module

If the MySQL password is changed before upgrading to this SRM version, the Compliance Backend module becomes inaccessible during the upgrade because the MySQL password reverts to its default value.

About this task

To retain the changed password as in preupgrade level, follow these steps:

Steps

1. Log in to the Primary Backend.
2. Run the following command:
   a. Linux: **`<APG_HOME>/bin/launch-update-backend-passwords.sh -c <path to Host configuaration file>`**
   b. Windows: **`<APG_HOME>/bin/launch-update-backend-passwords.cmd -c <pathto Host configuaration file>Username: apg|rootNew Password: <Provide with same password as given in Pre-upgrade level>`**
   c. Host Configuration File: This file has the following format: **`frontend=<FQDN>:linux-x64|windows-x64 primarybackend=<FQDN>:linux-x64|windows-x64 additionalbackend_1=<FQDN>:linux-x64|windows-x64 collector_1=<FQDN>:linux-x64|windows-x64`**

Results

For further details, check the Changing MySQL passwords section in the Dell M&R Security Configuration Guide available at Dell Support Site.

Create softlink for mysql-client dependent library

About this task

After upgrading to 5.1.1.0 from earlier versions, if the libtinfo shared library is missing, the `mysql-client.sh` command gives the following error message: The errors can be seen on the VM console for primary backend/ additional backends.

```
/opt/APG/bin/../Databases/MySQL/Default/bin/ mysql: error while
loading shared libraries: libtinfo.so.6: cannot open
```

To resolve this issue:

Steps

Create a softlink using the following command:

```
sudo ln -s /lib64/libncurses.so.x.x /lib64/libtinfo.so.x
```

Example: RHEL 9

```
sudo ln -s /lib64/libncurses.so.6 /lib64/libtinfo.so.6
```

Find and Fix Broken Links in Reports

The Broken Links Detection Tool scans the entire report tree and identifies all report links that cannot be resolved. It fixes links if possible and provides best guess suggestions for resolving others.

About this task

Reasons for broken links

As reports are moved, removed, updated, or disabled in the report tree, links to those reports from other reports must be changed. The old links no longer work. Also, pregenerated reports and reports in the **My Reports** node, such as pinned reports, scheduled reports, and favorite reports are based on links that might be broken when reports are moved, removed, or disabled. Changed UIDs result in breaking links to reports that were linked or hooked to the original UIDs. SolutionPack upgrades that include moved or updated reports can impact links. For this reason, whenever a SolutionPack upgrade occurs, the upgrade process schedules the Broken Links Detection Tool to run after a timed waiting period. If you are sequencing multiple SolutionPack upgrades closely together, the waiting period is moved out with each upgrade, so that the Broken Links Detection Tool runs only once after all the upgrades seem to be finished. You can run the Broken Links Detection Tool on demand at any time.

Fixing broken links

The tool fixes many broken lines during its execution. These links are known with 100% certainty to be remapped to other locations. The tool does not show the automatically fixed links. If you are interested in viewing them, you can change the logging level of the daily Tomcat log file. For suggested fixes that do not rate a 100% confidence, the tool presents you with the pathname of the broken link, a suggested path for fixing the link that is based on certain assumptions, and a confidence percentage for how accurate the suggestion might be. You can select whether you want to apply the suggested fix, and the tool applies the fix. If you believe that the suggestion is incorrect, or if there is no suggestion that is provided, you must manually fix the link. The following procedure describes how to run the tool and how to resolve the detected broken links that were not fixed automatically by the tool.

Steps

1. On **APG** page, click **Profile** 👤 > **User Settings**.
2. Click **Custom Reports** tab.
3. In the **Broken Links Detection** section, click **Open Tool**.
   This button launches the Broken Links Detection task. The task runs on the entire report tree. The dialog box that opens shows the results of the run.

   The dialog box shows the following information for each broken link detected:

   Table 1. Broken links description

Column	Description
Type	The type of link that is broken. Examples are: Custom reports, Favorites, Pinned, Scheduled, Pregenerated.
Name/Location	The report containing the broken link.

Table 1. Broken links description (continued)

Column	Description
Link will now point to...	The report path of the proposed new link.
Confidence	Percentage of confidence that the new link is correct. ● When Confidence is 100%, the tool fixes the link automatically and it is not listed here. The 100% confidence rating occurs when changes match those that are recorded in the mapping files that are installed with the tool. ● When Confidence is not 100%, the value is based on how many components in the broken URL were mapped to known new values or new values that are similar to the original. ● The lowest level confidence suggestions are based on similar node names to the original path, and similar depths of levels in the hierarchy. Check the suggestion carefully to ensure it is correct, and if not, fix the link manually. ● A 0 level confidence rating indicates that the tool could not find any similar report path to suggest. The old and new report path names are too different from each other to be matched. A manual fix is required.

4. Analyze the suggestion in each row.
5. To accept a suggestion, click the box in the first column.
6. Click **Apply Fixes**.
7. When a suggestion is not correct or when there is no suggestion at all, manually fix the link as follows:
    a. Click the **Go To** icon in the **Name/Location** column.
    b. Use any of the following suggestions to manually correct the link path:
        - For Scheduled Reports, Pinned Reports, and Favorites, it is easiest to re-create the link using the User Interface, and delete the outdated report.
        - Correct a link manually: Click **Modifications** > **Edit Reports**, and change either the incorrect UID or the incorrect report path in the report definition. There are various places in a report definition where a link to another report might occur. Save the change, and return to Browse Mode.
        - If there are many reports linking to the same report path, and that report path is not being found, causing many failures for the same reason, consider the following approach: Revert to the previous version, add a UID to the report that is not being found, then upgrade, add the same UID into the report definitions in the new location, and run the tool again. Analyze whether this advanced approach is better than correcting each link manually.
8. Rerun the Link Detection Tool.
9. Repeat these steps until all broken links are fixed.

View Fixed Links in Tomcat Logs

If the logging level is set to `FINE` or `FINEST`, fixed links are logged in the daily Tomcat log file.

About this task

By default, the logging level does not produce information about fixed links, so change the logging level. More log entries increase I/O activity and can impact performance.

The log file name is `catalina.<date stamp>.log` at the Frontend server here:

```
/opt/APG/Web-Servers/Tomcat/Default/logs
```

The configuration file for changing the log level is:

```
/opt/APG/Web-Servers/Tomcat/Default/conf/logging.properties
```

You can change the logging level and access the log files on the web portal.

Steps

1. From Administration, go to **SYSTEM ADMIN** > **Server & Modules** > **Modules**.
2. In **Logical Overview** table, search for **Tomcat**.

    In case of multiple tomcat instances, select the instance on the frontend VM from the search result.
3. To change the logging level:
    a. Expand the **Configuration Files** blue bar.

b. Locate the `conf/logging.properties` file and click the **Edit** icon on the row.

c. Add the following line to the end of the file:

```
com.emc.mnr.links.level=ALL
```

d. To enable FINEST logs, locate this existing line:

```
1catalina.com.watch4net.apg.logging.jul.handler.RotateFileHandler.level
= FINE
```

e. Change `FINE` to `FINEST`.

f. Save the file.

g. Restart Tomcat.

h. Rerun the Detect and Fix Links tool to start capturing the additional log entries.

4. To view the log entries:

   a. Expand the **Log Files** blue bar.

   b. Download or view a `catalina.<date stamp>.log` file.

Deprecated or Deleted Alert Definitions

The deprecated or deleted alert definitions in this release are still present under Alert definitions. These deprecated alert definitions are present in a different folder with the same old folder structure.

ⓘ **NOTE:** This is for information only and no user action is required.

Install Preconfigured Alerts for all SolutionPacks

Some SolutionPacks have alerting components that are not installed during the upgrade, and they must be installed in the same way that they would be for a fresh SolutionPack installation.

Steps

1. From SRM Administration UI, go to **CONFIG** > **SolutionPacks**.
2. Go to the Browse and Install SolutionPacks and select one for which the SolutionPack block must be installed.
3. Click **Install**.
4. Enter an instance name for the component that is being installed.
5. Assign a server for the related components. In a typical four server deployment, the recommended server is selected automatically.
6. Click **Next**.
7. Click **Install**.
8. When the installation is complete, click **OK**.

Next steps

ⓘ **NOTE:** VPLEX threshold-based alerts are disabled by default. To manually enable threshold-based alerts, go to **CONFIG** > **Alerts** > **Manage Alert Definitions** > **Dell VPLEX Alert Definitions**. (SNMP-based alerts are enabled by default.)

Restore Timeout Values

Customized timeout values are overwritten with a default value during the upgrade, and the system backs up the XML files that contained customized values.

Steps

1. On Linux, run the following command on each server to find the files with values that changed:

   ```
   find / -name *old*(year of upgrade)* -print
   ```

2. On Windows, use Windows Explorer on each server to locate the files.

   After the upgrade, you must manually compare the old files to the new files and restore the values appropriately.

   ⓘ **NOTE:** You can configure the idle time out value using the `com.watch4net.webservice.idle.timeout` property. The default value for idle time out is 15 minutes.

Edit New Actions Scripts

It states that the Frontend Server where the Actions directory exists may require to be modified to reflect to the Primary Backend Server .

Steps

In the conf file replace 127.0.0.1 with the primary backend IP address or FQDN:

Table 2. Conf file path in Linux and Windows

Option	Description
Linux	`/opt/APG/Custom/WebApps-Resources/Default/actions/event-mgmt/linux/conf`
Windows	`Program Files\APG\Custom\WebApps-Resources\Default\actions\event-mgmt\windows\conf.cmd`

Review SolutionPack Block Configuration for Frontend Access

Dell Technologies recommends reviewing the Frontend web service access configuration for some SolutionPack blocks. It is required to ensure correct settings for communication between the SolutionPack block and Tomcat server (http or https, depending on the configuration, for secure site use https and for other http).

About this task

Perform a review of settings for the following SolutionPack blocks:

- generic-chargeback
- generic-usage-intelligence
- esrs-query-config
- compliance

ⓘ **NOTE:** Repeat the following procedure for each of the SolutionPack blocks mentioned previously.

Steps

1. From SRM Administration UI, go to **CONFIG** > **Settings** > **Central Configuration Repository**.

2. Type `frontend` in the **Search** field.
3. Click the row that corresponds to the SolutionPack block that you must reconfigure.
4. Click the checkbox for the component that you must reconfigure.
5. Verify that the value in the **Tomcat port** field is **58443** (for https) or **58080** (for http), depending on the configuration.
6. Select either **HTTP** or **HTTPS** in the **Tomcat Communication Protocol** drop-down list, depending on the configuration.
7. Click **Update**.

Install the Compliance Rules Module

See the following procedure if the Compliance Rule module is not installed.

Steps

1. From Administration, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Click **Configuration Compliance**.
3. Click **Install**.
4. Ensure that the Compliance Rules module is autopopulated with the appliance where the compliance backend is installed.
5. Click **Next**.
6. From the **Web-Service Gateway** drop-down list, select **Gateway on *<Primary Backend Host>***.
7. Click **Install**.
8. Click **OK**.

   ⓘ **NOTE:** For all the policies which contain the **Default Zoning must be Disabled** rule and if the rule is in enabled state in the policy, rerun the policy. Go to the SRM Administration UI **CONFIG** > **Configuration Compliance** > **Policy & Rules Management**, right click on the appropriate policy and click on **Run Now**.

Cisco MDS/Nexus Switch Discovery

In previous versions of Dell SRM, Cisco MDS/Nexus switches were discovered through SNMP Device Discovery and the Generic-SNMP collector. Beginning with ViPR SRM 4.0, the SolutionPack for Cisco MDS/Nexus includes a dedicated SNMP Data Collection Manager that allows you to discover Cisco MDS/Nexus switches using Discovery Center. The advantage of using Discovery Center is that you can discover all the switches in a fabric by entering the IP address of just one switch in the fabric. In addition, topology and performance polling interval configurations only apply to devices discovered using Discovery Center. If you prefer to continue with SNMP device discovery, you can skip this section.

ⓘ **NOTE:** All Cisco MDS/Nexus switches should be discovered with the same method. Do not trigger discovery from both Discovery Center and SNMP Device Discovery. When a switch is discovered from both Discovery Center and SNMP Device Discovery the switch is polled twice, wasting collector resources. If Cisco MDS has been moved to the Cisco MDS/Nexus SP, then skip this section.

Export Cisco MDS/Nexus Switches

Export the Cisco MDS/Nexus switch details from SNMP Device Discovery.

Steps

1. From the SRM Administration UI, go to **DISCOVERY** > **SNMP Discovery Device** > **Snmp-Discovery** > **Devices**.
2. Select all of the Cisco MDS/Nexus switches from the device list.
3. From the **Actions** drop-down list, select **Export seed file**, and click **Execute Action**.

Results

The system saves a file that is named `agents.csv` to the local machine. The exported seed file consists of both the switch details and credentials. The same exported seed file must use for importing the switch details and credentials into the respective tables using the Discovery Groups tab in Discovery Center. This seed file will not be imported into the devices UI.

Install the SNMP Data Collector

The SNMP Data Collector allows you to discover Cisco MDS/Nexus switches using Discovery Center.

Steps

1. From the SRM Admin UI, go to **DISCOVERY>SolutionsPacks> Browse & Install SolutionPacks**.
2. Select the SolutionPack for Cisco MDS/Nexus in the **Browse and Install SolutionPacks** window.
3. Click **Install**.
4. From the **SNMP Data Collection** drop-down list, select the server where you want to install the component.

   ⓘ **NOTE:** Multiple SNMP Data Collectors can be installed on different Collector Servers. Dell Technologies recommends installing at least one Cisco SNMP Data Collector per data center.

5. Click **Next**.
   The window displays SNMP data collection details. For more information, see the SolutionPack for Cisco MDS/Nexus chapter of the *Dell SRM SolutionPack Guide*.
6. Click **Install**.

   If you are using passive host discovery, you may need to modify the regex expressions. See the Passive host discovery configuration options section of the *Dell SRM SolutionPack Guide*.

Import Switch Details into Discovery Center

After you have installed one or more SNMP Data Collectors, you can use the seed file that you exported to add the switches to Discovery Center.

Steps

1. From the SRM Administration UI, go to **CONFIG** > **Settings** > **Manage Discovery Backends**.
2. Click the Primary Backend, and then click **Register**.
3. Select the server that lists Cisco MDS/Nexus as a discoverable device type, and click **Register**.
4. From the SRM Admin UI, go to **DISCOVERY> Discovery Center> Manage Discovery** and click on **Cisco MDS/Nexus**
5. Click the **Discoverable Groups** tab.
6. Click **Add new discovery group**, provide a friendly name, and click **OK**.
7. Click the discovery group that you just created.
8. In the **Credentials** section, click **Register**.
9. Browse to the seed file (`agents.csv`), select it, and click **OK**.

   ⓘ **NOTE:** If there were previous entries in the **Credentials** section, select the merge option.

10. In the **Switch Details** section, click **Import**.
11. Browse to the seed file (`agents.csv`), select it, and click **OK**.

    ⓘ **NOTE:** If there were previous entries in the Switch Details section, select the merge option.

12. Click **Save**.
13. Click the **Collected Cisco MDS/Nexus** tab, and click **Discover**.
14. Click the **Discovery Results** tab, select the discovery group that you created, and verify that all of the devices were successfully discovered.
15. Select all of the devices, and click **Import to Collected Cisco MDS/Nexus...**.
16. Click the **Collected Cisco MDS/Nexus** tab, click **Save**, and then click **OK**.

Results

If you have installed multiple Cisco MDS/Nexus Data Collectors, the Cisco MDS/Nexus switches are distributed across the collectors. In a multiple Collectors per data center configuration, after the switches have been assigned to a Cisco MDS Collector, you must manually reassign the switch assignment to the data collector.

Delete Switches from SNMP Device Discovery

After you have imported the devices into Discovery Center, remove them from SNMP Device Discovery to prevent the devices from being polled twice.

Steps

1. From the SRM Administration UI, go to **DISCOVERY** > **SNMP Device Discovery** > **Snmp-Discovery** > **Devices**, and select the Cisco MDS/Nexus switches from the device list.
2. From the **Actions** drop-down list, select **Delete**.
3. Click **Execute Action**, and then click **OK**.
4. Click **Dashboard** in the left pane.
5. Under **Device Distribution**, click **Distribute all...**.
6. Click **Send the generated configurations...**.

Update Capabilities

For devices discovered through the Cisco MDS collector in Discovery Center, SRM 4.1 introduced a new capability that is called CISCO-DEVICE-ALIAS ([DALIAS]) that enables the discovery of Device Aliases that participate in an Active ZoneSet. SRM 4.3 introduced a new capability that is called CISCO-PORT-CHANNEL-MEMBERS([PCNLMEM]) that enables discovery of port channel members.

About this task

To start polling the new capability after upgrading to Dell SRM 5.1.1.0, complete the following procedure:

Steps

1. From the SRM Admin UI, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery** click the Cisco MDS/Nexus Solution Pack and then click the row for a Cisco switch.
   The **Edit Cisco MDS/Nexus** window opens.
2. Click **Test and Rediscover**.
3. After the Test and Rediscover function completes, click **OK**.
4. Repeat these steps for the switches that are discovered in the Discovery Center.
5. To trigger polling, click **Save**.

Brocade Switch Discovery

Beginning with ViPR SRM 4.2, you can discover Brocade switches by using Discovery Center. The advantage of using Discovery Center is that you can discover the switches in a fabric by entering the IP address of one switch in the fabric. In addition, topology and performance polling interval configurations only apply to devices discovered using Discovery Center. If you prefer to go to SNMP device discovery, you can skip this section.

ⓘ **NOTE:** Do not trigger SNMP-based switch discovery from both Discovery Center and SNMP Device Discovery. When a switch is discovered from both Discovery Center and SNMP Device Discovery the switch is polled twice, wasting collector resources.

ⓘ **NOTE:** If the Brocade switches have been moved to the Brocade SP, then skip this section.

Export Brocade Switches

Export the Brocade switch details from SNMP Device Discovery.

Steps

1. From the SRM Admin UI, go to **DISCOVERY** > **SNMP Device Discovery** > **Snmp- Discovery** > **Devices**.
2. Select Brocade switches.

3. From the **Actions** drop-down list, select **Export seed file**, and click **Execute Action**.

Results

The system saves a file that is named `agents.csv` to the local machine. The exported seed file consists of both the switch details and credentials. The same exported seed file must be used for importing the switch details and credentials into the respective tables using the Discovery Groups tab in Discovery Center. This seed file will not be imported into the devices UI.

Import Switch Details into Discovery Center

After you have installed one or more SNMP Data Collectors, you can use the seed file that you exported to add the switches to Discovery Center.

Steps

1. From the SRM Admin UI, go to **CONFIG** > **Settings** > **Manage Discovery Backends**.
2. Click the Primary Backend, and then click **Register**.
3. Select the server that lists Brocade FC Switch as a discoverable device type, and click **Register**.
4. From the SRM Admin UI, go to **DISCOVERY> Discovery Center>Manage Discovery** and click on **Brocade**.
5. Click the **Discovery Inventory Types** tab.
6. Click **Add new discovery group**, provide a friendly name, and click **OK**.
7. Click the discovery group that you just created.
8. In the **SNMP Credentials** section, click **Import**.
9. Browse to the seed file (`agents.csv`), select it, and click **OK**.

   ⓘ **NOTE:** If there were previous entries in the SNMP Credentials section, select the merge option.

10. In the **Switch Details** section, click **Import**.
11. Browse to the seed file (`agents.csv`), select it, and click **OK**.

    ⓘ **NOTE:** If there were previous entries in the Switch Details section, select the merge option.

12. Click **Save**.
13. Click the **Collected Brocade FC Switch** tab, and click **Discover**.
14. Click the **Discovery Results** tab, select the discovery group that you created, and verify that all of the devices were successfully discovered.
15. Click **Import to Collected Brocade FC Switch...**.
16. Click the **Collected Brocade FC Switch** tab, click **Save**, and then click **OK**.

Results

If you have installed multiple Brocades Data Collectors, the Brocade switches are distributed across the collectors. In multiple Collectors per data center configuration, after the switches have been assigned to a Brocade Collector, you must manually reassign the switch assignment to the data collector.

Delete Switches from SNMP Device Discovery

After you have imported the devices into Discovery Center, remove them from SNMP Device Discovery to prevent the devices from being polled twice.

Steps

1. From the SRM Admin UI, go to **DISCOVERY** > **SNMP Device Discovery** > **Snmp- Discovery** > **Devices**, and select the Brocade switches from the device list.
2. From the **Actions** drop-down list, select **Delete**.
3. Click **Execute Action**, and then click **OK**.
4. Click **Dashboard** in the left-most pane.
5. Under **Device Distribution**, click **Distribute all...**.

6. Click **Send the generated configurations...**.

DPA Scheduled Reports not Available after Upgrade

If DPA scheduled reports are not available after the upgrade, delete the following custom report templates and times from the DPA server, and then restart the DPA collector.

Steps

1. If Avamar is discovered:
   a. Go to **Reports** > **Report Templates** > **Custom Report Templates**, and delete the following templates:
      - Avamar W4N Custom Backup All Jobs
      - Avamar W4N Custom Backup Restore Details

   b. Go to **Admin** > **System** > **Manage Time Periods**, and delete the following period:
      - AvamarLasthouroffsetby15mins

   c. Go to **Admin** > **System** > **Manage Time Periods** > **Create Time Period** > **Edit Times**, and delete the following times:
      - Avamar15Minsago
      - Avamar1Hourand15Minsago
2. If NetBackup is discovered:
   a. Go to **Reports** > **Report Templates** > **Custom Report Templates**, and delete the following templates:
      - NetBackup W4N Custom Backup All Jobs
      - NetBackup W4N Custom Backup Restore Details

   b. Go to **Admin** > **System** > **Manage Time Periods**, and delete the following period:
      - NetBackupLasthouroffsetby15mins

   c. Go to **Admin** > **System** > **Manage Time Periods** > **Create Time Period** > **Edit Times**, and delete the following times:
      - NetBackup15Minsago
      - NetBackup1Hourand15Minsago
3. Restart the DPA Collector in Dell SRM.

Create an Events Database for the SolutionPack for Data Protection Advisor

An events database must be manually created before the SolutionPack for Dell Data Protection Advisor can be installed.

Prerequisites

The Events SolutionPackBlock must be installed before creating the events database. For more information about installing the Events SolutionPackBlock, see Installing new alerting components on page 37.

Steps

1. Putty in to the Primary Backend server using the command line.
2. Go to the following location:

   `/opt/APG/bin/`
3. Run the following command:

   `./mysql-client.sh`
4. Type the Username: `apg`, database: `events`.

   Type the default password is `watch4net`
5. Change to show tables; and look for `generic_backup table`
   a. Show the generic_backup fields with desc generic_backup; and compare the fields that are shown in step 6. Note any differences and then proceed with step 6 to replace the generic_backup table.
6. Create the generic_backup table in the events database:

NOTE: If you copy and paste this script, carriage return characters may exist at the end of each line in the pasted version. Use a text editor such as Notepad to remove these characters before the script run.

```
CREATE DATABASE IF NOT EXISTS events; GRANT ALL PRIVILEGES ON events.* TO
apg@'localhost' IDENTIFIED BY 'watch4net';GRANT FILE ON *.* TO apg@'localhost'
IDENTIFIED BY 'watch4net'; use events; DROP TABLE IF EXISTS generic_backup;
CREATE TABLE IF NOT EXISTS `generic_backup` ( `id` bigint(20) DEFAULT NULL,
`appjobid` varchar(256) NOT NULL DEFAULT '', `openedat` int(11) NOT NULL, `datagrp`
varchar(100) DEFAULT NULL, `prjobid` int(11) DEFAULT NULL, `bkpservr` varchar(100)
DEFAULT NULL, `bkpos` varchar(100) DEFAULT NULL, `bkprev` varchar(100) DEFAULT
NULL, `dpahost` varchar(100) DEFAULT NULL, `collhost` varchar(100) DEFAULT NULL,
`collinst` varchar(100) DEFAULT NULL, `device` varchar(100) DEFAULT NULL, `clntos`
varchar(100) DEFAULT NULL, `part` varchar(100) DEFAULT NULL, `ip` varchar(100)
DEFAULT NULL, `partdesc` varchar(100) DEFAULT NULL, `parttype` varchar(100) DEFAULT
NULL, `policy` varchar(100) DEFAULT NULL, `bkptech` varchar(100) DEFAULT NULL,
`bkptype` varchar(100) DEFAULT NULL, `retlevel` varchar(100) DEFAULT NULL, `state`
varchar(100) DEFAULT NULL, `mediasvr` varchar(100) DEFAULT NULL, `path` varchar(100)
DEFAULT NULL, `lwatermk` varchar(100) DEFAULT NULL, `hwatermk` varchar(100) DEFAULT
NULL, `stuid` varchar(100) DEFAULT NULL, `stutype` varchar(100) DEFAULT NULL,
`capacity` varchar(100) DEFAULT NULL, `userdefined1` varchar(100) DEFAULT NULL,
`userdefined2` varchar(100) DEFAULT NULL, `userdefined3` varchar(100) DEFAULT NULL,
`userdefined4` varchar(100) DEFAULT NULL, `userdefined5` varchar(100) DEFAULT NULL,
`userdefined6` varchar(100) DEFAULT NULL, `userdefined7` varchar(100) DEFAULT NULL,
`userdefined8` varchar(100) DEFAULT NULL, `userdefined9` varchar(100) DEFAULT NULL,
`userdefined10` varchar(100) DEFAULT NULL, `userdefined11` varchar(100) DEFAULT NULL,
`userdefined12` varchar(100) DEFAULT NULL, `userdefined13` varchar(100) DEFAULT NULL,
`userdefined14` varchar(100) DEFAULT NULL, `userdefined15` varchar(100) DEFAULT NULL,
`systemdefined1` varchar(100) DEFAULT NULL, `systemdefined2` varchar(100) DEFAULT
NULL, `systemdefined3` varchar(100) DEFAULT NULL, `systemdefined4` varchar(100)
DEFAULT NULL, `systemdefined5` varchar(100) DEFAULT NULL, PRIMARY KEY (`appjobid`,
`openedat`) ) ENGINE=MyISAM DEFAULT CHARSET=utf8;
```

7. See the following steps only if you are upgrading from ViPR SRM 4.0 to ViPR SRM 4.1.1:
   a. From Dell SRM, go to **Administration** > **SolutionPacks** > **Storage** > **Dell Data Protection Advisor**.
   b. Click the pencil icon for the **Data collection** component.
   c. In **Events server hostname or IP address**, change localhost to the Primary Backend.
   d. Click **Reconfigure**.
8. From Dell SRM **Administration**, go to **SYSTEM ADMIN** > **Servers & Modules** > **Modules** > **Logical Overview** > **Collecting** > **Events** and restart the **Event-Processing-Manager :: emc-dpa -** ***server_name*** collector.
9. From Dell SRM **Physical Overview**, select PBE **>Modules** > **Event- Processing Event-Processing-Manager :: emc-dpa** .

Update the SNMP Collections

Learn how to update the SNMP collections and synchronize the configuration. It would be needed only when the devices are not moved to the discovery center for the solution packs Brocade/Cisco/DataDomain.

About this task

This procedure is required only if the SNMP Discovery is still being used and the SAN has not been migrated to the new Cisco and/or Brocade SolutionPacks. SAN discovery stops if this step is not completed when using the SNMP Discovery.

Steps

1. Log in to the device discovery web interface at `https://<Frontend IP address>:58443/device-discovery`.

   (On the Administration Dashboard, Device Discovery has been renamed SNMP Device Discovery.)
2. Click **Collectors** in the left-most pane.
3. On the **Collectors** page, click the checkbox for each collector.
4. Click the **Delete** icon.
5. Click **New Collector**.
6. Retain the values for Network interface and Collector Port unless you have changed the port configuration.

7. The Collector IP Address must be the address of the Generic-SNMP collector's IP address where the collection for the SNMP-based discovery is located.
8. On the collectors, click **Send configurations to the 1 selected collector(s)**.
9. Verify that all the new capabilities are shown correctly against the collector.
10. On the Dashboard, click **Discover capabilities from all the approved devices** to ensure that the SNMP masks have gone into effect after the update.
11. On the Dashboard, examine the Device Distribution section. If any collectors are not synchronized, this section contains a warning such as 1 collector(s) configuration not synchronized.
12. If any of the collectors are not synchronized, click the **Distribute all approved devices...** button.
13. Click **Send the generated configurations on all available collectors**.

    After you confirm that the collector configurations are synchronized, go through the UI and review the Reports, SolutionPacks, and other features. One way to check that the health of the system is to view the reports in the System Health SolutionPack.

    In order for new data to display in the UI, three polling cycles must pass and the import-properties-Default task must have run.

Virus Scanning Software in Windows Deployments

Running virus-scanning software on directories containing MySQL data and temporary tables can cause issues, both in terms of the performance of MySQL and the virus-scanning software misidentifying the contents of the files as containing spam.

After installing MySQL Server, Dell Technologies recommends that you disable virus scanning on the main APG directory. In addition, by default, MySQL creates temporary files in the standard Windows temporary directory. To prevent scanning the temporary files, configure a separate temporary directory for MySQL temporary files and add the directory to the virus scanning exclusion list. To do this, add a configuration option for the `tmpdir` parameter to the `my.ini` configuration file.

Review Report Customization

After an upgrade, you must decide whether to use a saved reportpack or the new one.

Report customization is maintained during the upgrade (under My Reports), but you must decide whether to use the saved reportpack or the new one. New metrics to a report are not merged with the old report, so you must manually add any new metrics to the old reports.

Validate the Environment

After upgrading the system, verify the operational status.

Steps

1. Look for blank reports and graphs.

   Determine whether blank reports collection errors cause blank reports. Resolve issues or document them for later follow-up.
2. Look for broken links. Resolve issues or document them for later follow-up.
3. Verify that all tasks are successfully completed (except automatic updates and Dell Technologies Connectivity).
4. Validate that topology is working. Resolve any issues.
5. Verify or edit polling periods.

Verify vApp Linux Operating System is Upgraded

After the upgrade, verify that the vApp Linux Operating System has been upgraded.

Steps

Ensure that the Operating System kernel version is 5.14.21-150400.24.153-default. If the SRM 5.1.1.0 vApp Operating System does not show the Operating System kernel version as 5.14.21-150400.24.153-default, then the Linux Operating System is not upgraded. Check the `/etc/sudoers` file and the last line in this file should be #includedir /etc/sudoers.d # added by MnR platform." If missing, add this line and save. Run the following command to complete the Operating System update.

```
#includedir /etc/sudoers.d   # added by MnR platform
```

NOTE: This must be checked on each of the SRM Linux Servers.

```
/opt/APG/bin/launch-vapp-update.sh
```

NOTE: Run this command on each of the Linux server where the Linux Operating System was not upgraded.

Reconfiguring Dell PowerVault Frontend Web Service

After the upgrade, reconfigure the Dell PowerVault Frontend Web Service.

Steps

1. In SRM Admin UI, go to **CONFIG** > **Installed Solution Packs**.
2. Click **Dell PowerVault**.
3. Click the **Reconfigure given answers** ✎ icon for block 'collect'.
4. In the **Frontend Web service** field, you can either use the existing service or add a new service.
5. Click **Reconfigure**.

Reconfiguring Pure Storage Frontend Web Service

After the upgrade, reconfigure the Pure Storage Frontend Web Service.

Steps

1. In SRM Admin UI, go to **CONFIG** > **Installed Solution Packs**.
2. Click **Pure Storage**.
3. Click the **Reconfigure given answers** ✎ icon for block 'collect'.
4. In the **Frontend Web service** field, you can either use the existing service or add a new service.
5. Click **Reconfigure**.

Reconfiguring Kubernetes

Reconfigure the collect block and modify the alert consolidation and topology-related settings based on the service's installation location in your setup.

For alerting support, install the newly added blocks alerts and alert consolidation.

Deleting the ISO Image from Data Store Location

About this task

After the Operating System upgrade on all the vApp VM (including Frontend) is completed, it is mandatory to remove the ISO image deployed for this upgrade. To do so, follow the below steps for each vApp VM.

Steps

1. Log in to the vCenter Client and select the VM.
2. Shut down the VM.
3. Right click on the VM and click **Edit Settings**.
4. In the **Virtual Hardware** tab, Delete the **CD/DVD Drive 2**.
5. Click **OK** on the **Edit Settings** pane to close the window and reconfigure the VMs settings.
6. Check the **Recent Task** pane of the vCenter client and confirm that VMs are reconfigured successfully.
7. Power on the VM.

   After the above steps are run successfully on all the vApp VMs, go to ISO image uploaded in the Datastore location and delete it.

Limitations and Known Issues

The following are the limitations and known issues.

- After the upgrade, on the **Report Library** > **Recoverpoint** > **Inventory** > **Consistency Groups** report, the Transfer Status column shows that stale data until older metrics become inactive.
- After you update the generic-rsc block, the CPU Utilization % for Linux Hosts may increase rapidly into the thousands. The system starts to display the correct CPU Utilization % when you update the SolutionPack for Physical Hosts. The higher CPU Utilization values are visible in the reports for few days because the report settings show data that is collected over 2 weeks.
- Units (such as GB and TB) may not display in Capacity charts and Bandwidth charts. To resolve this issue, use SSH to log in to the Dell SRM Frontend and run the following command: `/opt/APG/bin/manage-modules.sh service restart tomcat`
- After the upgrade, the Path Details and Storage Connectivity report for Dell Data Domain is blank.
- For XMS V2 API, the logic to identify metrics has been changed to reduce inactive metrics due to change in xmsip. It would have implications on all existing metrics post upgrade where all XtremIO metrics go inactive and the historical data is not displayed in default reports. New reports have been added for users to access inactive metrics that are related to capacities for array and volume. These reports are hidden by default and are available at **Report Library>Dell EMC XtremIO>Capacity**. This scenario is applicable only for Dell EMC XtremIO SolutionPack.
- Alert config changes for Port link down results in duplicate alerts. The alerts are missing for some hosts where the part name is same, this impacts the upgrade. The old alerts become inactive, and new alerts are generated based on the fix. To overcome this issue, manually acknowledge the old alerts.
- In upgraded setup, Scheduled Report to a remote location using FTP option does not work as `FW_TRUSTED_NETS` in the file `/etc/sysconfig/SuSEfirewall2` is missing because of firewall changes in SLES 15 SP4. Remote Transfer using FTP to work, Run the following commands in the path `/etc/firewalld/zones` :
  1. `firewall-cmd --permanent --zone=trusted --add-source=<ip-of-ftp>`
  2. `firewall-cmd --reload`

  Once the command is run, a success message is displayed and a `trusted.xml` file is generated.

7

Troubleshooting

Topics:

Enhanced Upgrade Log

If there is an upgrade failure, the following can be done to troubleshoot:

- The enhanced SRM upgrade UI provides details of the log messages to be reviewed.

SRM APG UI Loading Issue

In vApp, after OS Upgrade to SLES 15 SP4, SuSEfirewall2 is replaced by Firewalld. To enable the ports, follow the below steps.

Steps

1. Log in to the SRM appliance using root credentials.
2. Run the below command:

   ```
   /usr/APG_Source/conf/open-new-ports.sh
   ```
3. Scripts add all the required ports to the firewall.
4. Now the SRM APG UI page is loaded, the login prompt is shown.

Troubleshooting Procedure for SLES 15 SP4 OS Upgrade

This procedure is applicable only while upgrading from versions older than SRM 5.1.1.0.

The following lists the troubleshooting scenarios which you may come across during the upgrade.

Topics

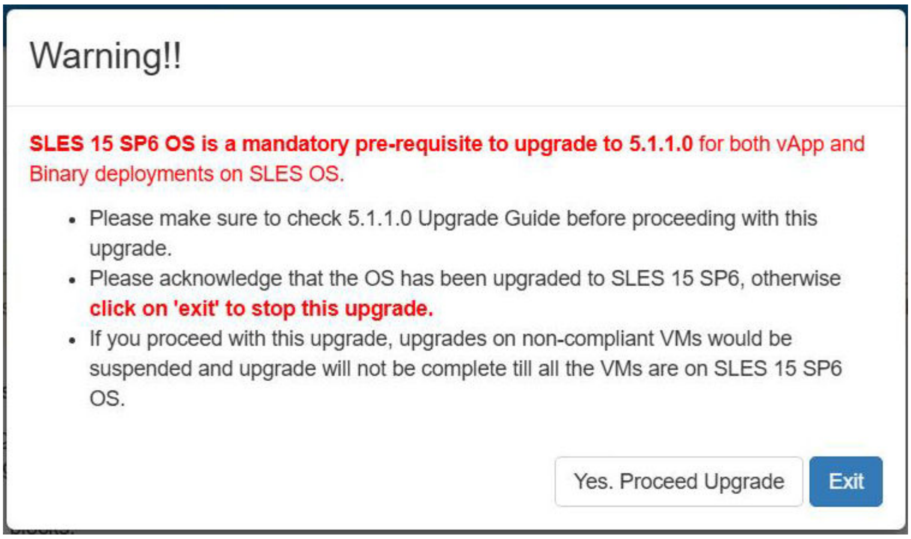
- Resume the Upgrade on SRM Setup.
- OS Upgrade Initiation Failed.
- Failed to Establish Connection.
- VMutils Manager Packages.
- Failed to start D-Bus System Message
- Passive STIG Rules
- Unmapping CD/DVD Drive
- Wrong Password during OS Upgrade Script

Resume the Upgrade on SRM Setup

This section provides detailed steps to resume the upgrade procedure on SRM setup.

About this task

Before launching SRM upgrade from the UI using the **Launch Upgrade** button, the system prompts for the following confirmation.



Warning!!

SLES 15 SP6 OS is a mandatory pre-requisite to upgrade to 5.1.1.0 for both vApp and Binary deployments on SLES OS.

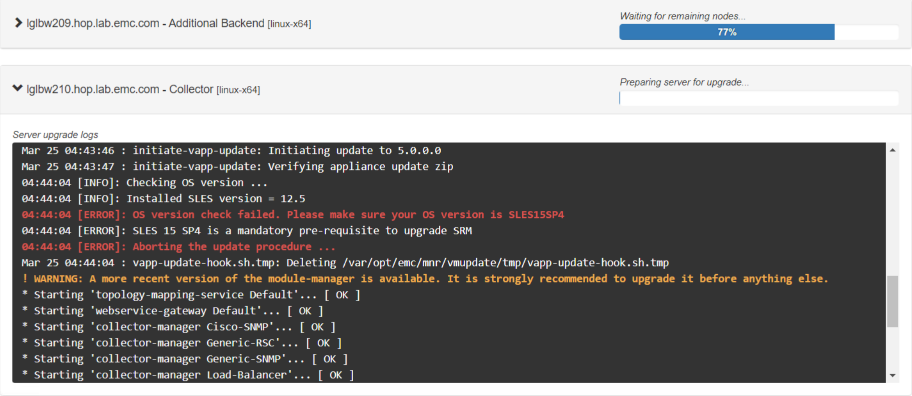
- Please make sure to check 5.1.1.0 Upgrade Guide before proceeding with this upgrade.
- Please acknowledge that the OS has been upgraded to SLES 15 SP6, otherwise **click on 'exit' to stop this upgrade.**
- If you proceed with this upgrade, upgrades on non-compliant VMs would be suspended and upgrade will not be complete till all the VMs are on SLES 15 SP6 OS.

The prompt displays that all the SLES12 SP5 based servers (both vApp and binary) associated with the SRM Frontend must be upgraded to SLES15 SP4 (Operating System upgrade). User must confirm and proceed ahead with the SRM upgrade.

If a user skips the Operating System upgrades to SLES15 SP4 for a few servers(non- compliant servers) proceeds ahead to upgrade instead of Exit, then the setup would go into an unsupported configuration , and overall upgrade of the SRM setup is not completed as well.

For binary-based SLES 12 servers (except Frontend), the SRM Upgrades would go through although they would still qualify as unsupported configuration, since this SRM version requires SLES15 SP4 Operating System as a prerequisite.

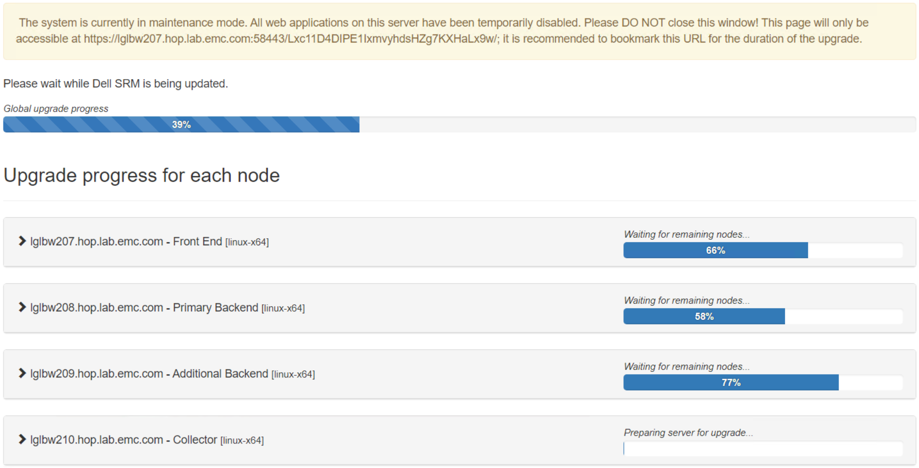
On the non-compliant servers, the following error is shown:



lglbw209.hop.lab.emc.com - Additional Backend [linux-x64]
Waiting for remaining nodes...
77%
lglbw210.hop.lab.emc.com - Collector [linux-x64]
Preparing server for upgrade...
Server upgrade logs

```
Mar 25 04:43:46 : initiate-vapp-update: Initiating update to 5.0.0.0
Mar 25 04:43:47 : initiate-vapp-update: Verifying appliance update zip
04:44:04 [INFO]: Checking OS version ...
04:44:04 [INFO]: Installed SLES version = 12.5
04:44:04 [ERROR]: OS version check failed. Please make sure your OS version is SLES15SP4
04:44:04 [ERROR]: SLES 15 SP4 is a mandatory pre-requisite to upgrade SRM
04:44:04 [ERROR]: Aborting the update procedure ...
Mar 25 04:44:04 : vapp-update-hook.sh.tmp: Deleting /var/opt/emc/mnr/vmupdate/tmp/vapp-update-hook.sh.tmp
! WARNING: A more recent version of the module-manager is available. It is strongly recommended to upgrade it before anything else.
* Starting 'topology-mapping-service Default'... [ OK ]
* Starting 'webservice-gateway Default'... [ OK ]
* Starting 'collector-manager Cisco-SNMP'... [ OK ]
* Starting 'collector-manager Generic-RSC'... [ OK ]
* Starting 'collector-manager Generic-SNMP'... [ OK ]
* Starting 'collector-manager Load-Balancer'... [ OK ]
```

The overall upgrade of the SRM setup(containing such non- compliant servers) is aborted, and a prompt is displayed as shown in the below screenshot.



The system is currently in maintenance mode. All web applications on this server have been temporarily disabled. Please DO NOT close this window! This page will only be accessible at https://lglbw207.hop.lab.emc.com:58443/Lxc11D4DIPE1IxmvyhdsHZg7KXHaLx9w/; it is recommended to bookmark this URL for the duration of the upgrade.

Please wait while Dell SRM is being updated.

Global upgrade progress

39%

Upgrade progress for each node

- lglbw207.hop.lab.emc.com - Front End [linux-x64] — *Waiting for remaining nodes...* 66%
- lglbw208.hop.lab.emc.com - Primary Backend [linux-x64] — *Waiting for remaining nodes...* 58%
- lglbw209.hop.lab.emc.com - Additional Backend [linux-x64] — *Waiting for remaining nodes...* 77%
- lglbw210.hop.lab.emc.com - Collector [linux-x64] — *Preparing server for upgrade...*

Follow the below procedure to troubleshoot the SRM setup, to resume the SRM upgrade process.

Steps

1. Run Operating System upgrades to SLES 15 SP4 for all the noncompliant servers (both vApp and Binary). For vApp based servers, follow the methods provided earlier in this Guide. For binary SLES 12 servers, contact the Administrator for Operating System upgrades.
2. Ensure that all the servers with SLES12 SP5 Operating System must be upgraded to SLES15 SP4 Operating System.
3. If the overall Upgrade did not finish on the UI, log in to the Frontend VM with root credentials.
4. Find out the Update manager process, and kill the same.

   On Linux machines, find the process number and then use the kill command.

   ```
   ps -ef | grep -i update
   ```

   ```
   kill -9 <process number>
   ```

   On windows FE, kill the process with the image name as `java.exe`.

5. Restart all services on the Frontend including Tomcat.

   To perform this task, go to the following directories.

   - Linux command: `cd /opt/APG/bin`
   - Windows command: `cd Program Files/APG/bin`

6. To restart the services, use the following commands.
   - Linux command: `manage-modules.sh service restart all`
   - Windows command: `manage-modules.cmd service restart all`

7. Log in to the Primary Backend, Additional Backend using root/administrator credentials. Perform the above steps to restart all services.
8. Log in to the SRM UI and then restart all services across the collector servers. Restart the services.

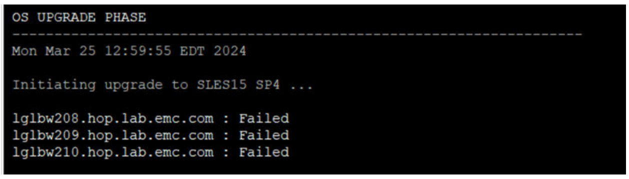
   ⓘ **NOTE:** Following the above steps, restart the SRM setup again. Now ensure to follow the below steps to restart the upgrade process.

9. Log in to the SRM Admin UI. On the admin UI page, go to **SYSTEM ADMIN** > **System Operations** > **Update System** to launch SRM upgrade.

OS Upgrade Initiation Failed

ISO is not attached

When one or multiple Remote Servers OS Upgrade Initiation Failed, the following error is shown.

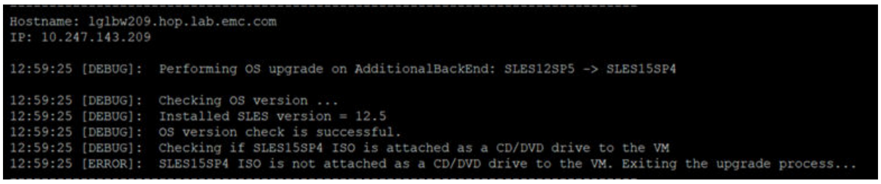


```
OS UPGRADE PHASE
--------------------------------------------------------------------
Mon Mar 25 12:59:55 EDT 2024

Initiating upgrade to SLES15 SP4 ...

lglbw208.hop.lab.emc.com : Failed
lglbw209.hop.lab.emc.com : Failed
lglbw210.hop.lab.emc.com : Failed
```

Follow the below procedure to troubleshoot the Remote Servers OS Upgrade Initiation.

Steps

1. Log in to the Frontend Appliance and navigate to /opt/ADG/osupdate/logs directory.
2. Check the osUpgradeInitiation.log for below error for all the servers.



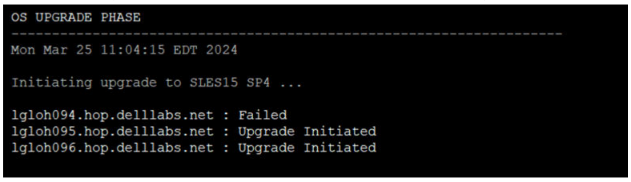
```
Hostname: lglbw209.hop.lab.emc.com
IP: 10.247.143.209

12:59:25 [DEBUG]:  Performing OS upgrade on AdditionalBackEnd: SLES12SP5 -> SLES15SP4

12:59:25 [DEBUG]:  Checking OS version ...
12:59:25 [DEBUG]:  Installed SLES version = 12.5
12:59:25 [DEBUG]:  OS version check is successful.
12:59:25 [DEBUG]:  Checking if SLES15SP4 ISO is attached as a CD/DVD drive to the VM
12:59:25 [ERROR]:  SLES15SP4 ISO is not attached as a CD/DVD drive to the VM. Exiting the upgrade process...
```

3. ISO Image is not attached to the VM, then follow the steps that are mentioned in Configure ISO Image for Each SRM VMs
4. After ISO Image attachment, rerun the below command.

   `SLESOSupgrade.sh -u remoteServer`
5. The script will initiate the Operating System upgrade on the Failed Servers.

ISO is attached

When one or multiple Remote Servers OS Upgrade Initiation Failed, the following error is shown.



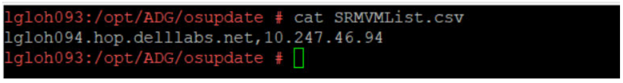
```
OS UPGRADE PHASE
------------------------------------------------------------------
Mon Mar 25 11:04:15 EDT 2024

Initiating upgrade to SLES15 SP4 ...

lgloh094.hop.delllabs.net : Failed
lgloh095.hop.delllabs.net : Upgrade Initiated
lgloh096.hop.delllabs.net : Upgrade Initiated
```

Follow the below procedure to retrigger the OS upgrade on the Failed Servers and complete the OS upgrade process.

Steps

1. Log in to the Frontend Appliance and navigate to `/opt/ADG/osupdate/` directory
2. Edit the `SRMVMList.csv` file to include only the OS Upgrade Initiation Failed Servers and Save the file.

   Example



```
lgloh093:/opt/ADG/osupdate # cat SRMVMList.csv
lgloh094.hop.delllabs.net,10.247.46.94
lgloh093:/opt/ADG/osupdate #
```

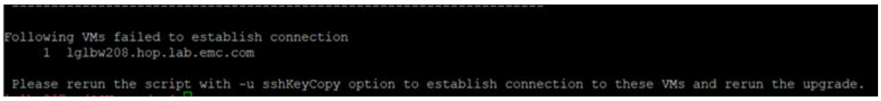
3. Navigate to the OSUpgrade directory where the OS Upgrade scripts are copied. Rerun the below command to trigger OS Upgrade on Failed Servers:

   `SLESOSupgrade.sh -u remoteServer`
4. The script will initiate the Operating System upgrade on the Failed Servers.
5. To monitor the progress of upgrades on all the VMs, include all the Servers in the `/opt/ADG/osupdate/SRMVMList.csv` file . Run the below command.

   `SLESOSupgrade.sh -s status`

Failed to Establish Connection

When one or multiple Remote Servers failed to establish the connection, the following error is shown.



```
Following VMs failed to establish connection
    1  lglbw208.hop.lab.emc.com

 Please rerun the script with -u sshKeyCopy option to establish connection to these VMs and rerun the upgrade.
```

Follow the below procedure to troubleshoot the failed to establish connection.

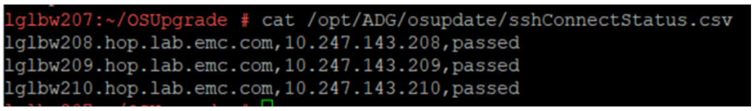
Steps

1. Log in to the Frontend Appliance and navigate to the OSUpgrade directory where the OS Upgrade scripts are copied.

   Run the below command to provide the correct password so that connection is established with the servers.

   ```
   SLESOSupgrade.sh -u sshKeyCopy
   ```
2. Once the script is triggered, provide the password for the VM's. Connection establishment must be successful.
3. To check Connection establishment status, run below command.

   ```
   cat /opt/ADG/osupdate/sshConnectStatus.csv
   ```
4. All the server's status should be passed as below, if status is failed for any of the servers, you must rerun the above steps.

   ```
   lglbw207:~/OSUpgrade # cat /opt/ADG/osupdate/sshConnectStatus.csv
   lglbw208.hop.lab.emc.com,10.247.143.208,passed
   lglbw209.hop.lab.emc.com,10.247.143.209,passed
   lglbw210.hop.lab.emc.com,10.247.143.210,passed
   ```
5. Rerun the below command to trigger the OS Upgrade on the remote servers.

   ```
   SLESOSupgrade.sh -u remoteServer
   ```
6. The script will initiate the Operating System upgrade on the remote Servers .
7. To monitor the progress of upgrades on all the VMs, include all the Servers in the `/opt/ADG/osupdate/SRMVMList.csv` file. Run the below command.

   ```
   SLESOSupgrade.sh -s status
   ```

VMutils Manager Packages

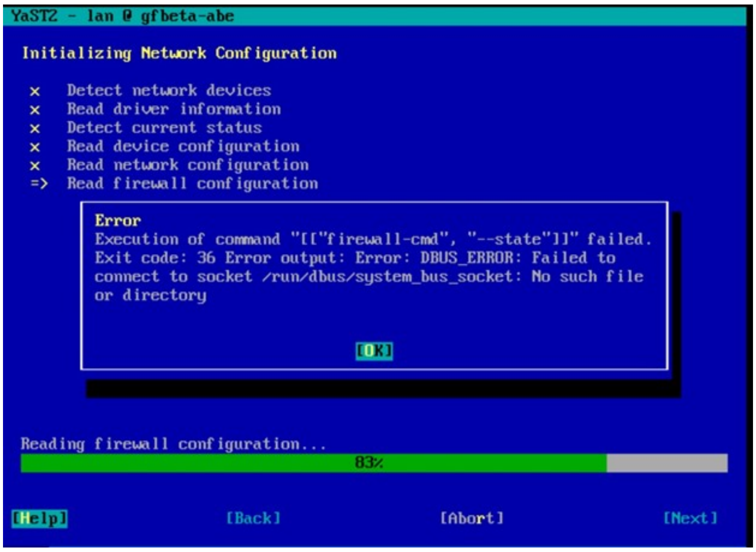
`tcpdump` and `net-snmp` packages configured or installed before the upgrade to SRM 5.1.1.0 using `vmutils-manager.sh` will not work after the upgrade to SRM 5.1.1.0. To resolve the issue, follow the steps below on all the vApp VMs.

Steps

1. Log in to the appliance using root credentials.
2. Run `vmutils-manager.sh` and reinstall the `tcpdump` and `net-snmp` packages.

Failed to start D-Bus System Message

During OS Upgrade from SLES 12 SP5 to SLES 15 SP4, if you get into the issue as below:



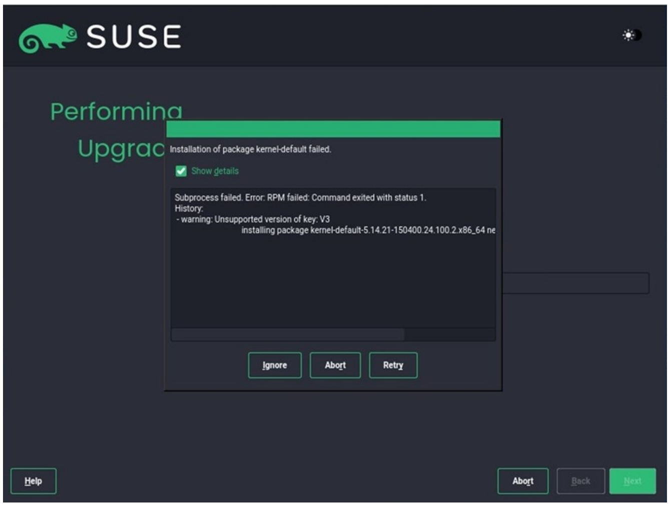
```
YaST2 - lan @ gfbeta-abe

Initializing Network Configuration

 ×   Detect network devices
 ×   Read driver information
 ×   Detect current status
 ×   Read device configuration
 ×   Read network configuration
 =>  Read firewall configuration

         Error
         Execution of command "[["firewall-cmd", "--state"]]" failed.
         Exit code: 36 Error output: Error: DBUS_ERROR: Failed to
         connect to socket /run/dbus/system_bus_socket: No such file
         or directory

                                 [OK]

Reading firewall configuration...
                                    83%
```

Steps

1. Revert the snapshot of the VM.
2. To resolve the d-bus system issue, apply the steps that are mentioned in the KB on the VM where it is observed.
3. Rerun the OS Upgrade procedure.

Unsupported V3 key

During OS Upgrade from SLES 12 SP5 to SLES 15 SP4, if you get below warning message:



Installation of package kernel-default failed.

☑ Show details

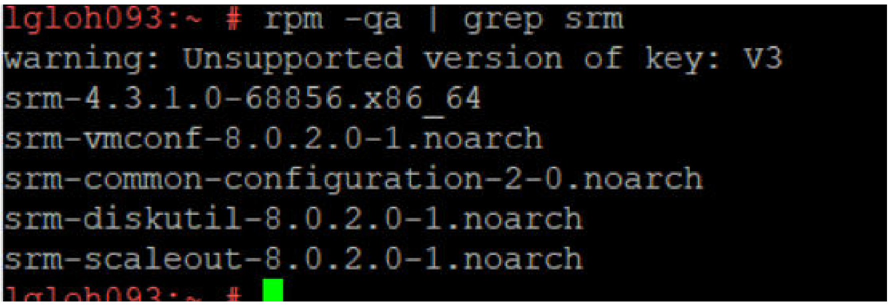
```
Subprocess failed. Error: RPM failed: Command exited with status 1.
History:
 - warning: Unsupported version of key: V3
                    installing package kernel-default-5.14.21-150400.24.100.2.x86_64 ne
```

Steps

1. Revert the snapshot of the VM.
2. To resolve the unsupported V3 key warning, apply the steps that are mentioned in the KB on the VM where it is observed.
3. Rerun the OS Upgrade procedure.

After the OS Upgrade to SRM 5.x.x.x, there might be a warning message when OS-related commands are run, which can be ignored. The warning message is as follows.

```
warning: Unsupported version of key: V3
```



```
lgloh093:~ # rpm -qa | grep srm
warning: Unsupported version of key: V3
srm-4.3.1.0-68856.x86_64
srm-vmconf-8.0.2.0-1.noarch
srm-common-configuration-2-0.noarch
srm-diskutil-8.0.2.0-1.noarch
srm-scaleout-8.0.2.0-1.noarch
lgloh093:~ #
```

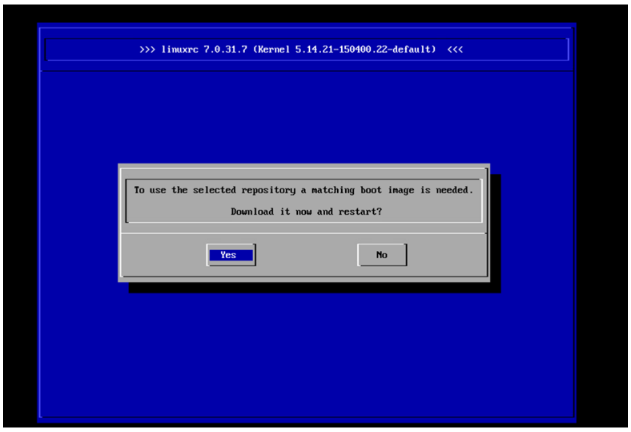
For more information, refer SUSE Support KBA 000019712 .

Passive STIG Rules

SRM recommends disabling the Passive STIG rules that are enabled as SRM 5.1.1.0 is not supported with STIG implementation.

Unmapping CD/DVD Drive

During upgrade to SLES 15 SP4, the following error is displayed if SLES 12 SP4 ISO is still connected to appliance CD/DVD Drive.



```
>>> linuxrc 7.0.31.7 (Kernel 5.14.21-150400.22-default) <<<

To use the selected repository a matching boot image is needed.
Download it now and restart?
```

Follow the procedure below to troubleshoot the issue.

Steps

1. Revert all the VM's to the previous snapshot.
2. Power-off the VM.
3. Right click on the VM and click **Edit Settings**.
4. In the **Virtual Hardware** tab, point the **CD/DVD Drive** setting where SLES 12 SP4 ISO is mapped, to **Client Drive**.
5. Click **OK** on the Edit Settings pane to close the window and reconfigure the VMs settings.
6. Check the **Recent Task** pane of the vCenter client and confirm that VMs are reconfigured successfully.
7. Power on the VM.
8. Retry the steps in Upgrade Operating System for vApp to SLES 15 SP4.

Wrong Password during OS Upgrade Script

During OS Upgrade, the root password for the remote servers is asked. By default, six attempts are used for root user module as this is the security hardening that is implemented in SRM 5.1.1.0 for the root user.

8

Documentation Feedback

Dell Technologies strives to provide accurate and comprehensive documentation and welcomes your suggestions and comments. You can provide feedback in the following ways:

- Online feedback form — **Rate this content** feedback form is present in each topic of the product documentation web pages. Rate the documentation or provide your suggestions using this feedback form.
- Email—Send your feedback to SRM Doc Feedback. Include the document title, release number, chapter title, and section title of the text corresponding to the feedback.

To get answers to your queries related to Dell SRM through email, chat, or call, go to Dell Technologies Technical Support page.