EMC® ViPR SRM

Version 4.1

Upgrading to version 4.1

P/N 302-003-732

REV 04

Published February 2018

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS-IS.“ DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

CONTENTS

CHAPTER 1

Upgrading the System

This chapter includes the following topics:

Overview

Note

If you are upgrading a vApp deployment, you may need to run a script before starting the upgrade process. Refer to Knowledgebase article 000489632 for more information.

If you want to update a single SolutionPack to receive the benefit of a required fix or feature, refer to the Updating SolutionPacks and Other Components chapter of the Administration Guide.

Required tools

Ensure that you have the necessary tools.

- WinSCP or equivalent
- Putty/SSH
- Remote Desktop

Required credentials

Gather the necessary credentials.

- root/administrator credentials for all of the ViPR SRM servers
- ESX/vCenter server credentials (if appropriate)
- SMI array hosts
- Brocade SMI hosts

Verifying and documenting the current status of the environment

Verify and document the current status of the environment before starting the upgrade process. This will help you evaluate the success of the upgrade.

Before you begin

Refer to chapter 4 of the *ViPR SRM Administrator Guide* for details about verifying the health of your system.

Refer to the *ViPR SRM Performance and Scalability Guidelines* for details about determining configuration size.

Note

The Topology-Mapping-Service module, by default, is configured with 2GB max heap. For those installed on the Frontend and Backend hosts, actual maximum consumption is under 128MB. The additional memory need not be considered for sizing calculations. The Topology-Mapping-Service installed on the Collector host should have its full 2GB max heap considered.

Procedure

1. Look for blank reports and graphs. Determine if there are any blank reports caused by collection errors. Resolve any issues or 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 databases. Check **Report Library** > **EMC M&R Health** > **Logical Summary** > **Backends** > **Components** > **Backends** and **Report Library** > **EMC M&R Health** > **Logical Summary** > **Backends** > **Components** > **Databases**.
   - Check backend thresholds to verify that you have room to accommodate new sizing.
   - Add additional backends and databases as required.
5. Ensure that there is 5 GB available on the files systems where ViPR SRM is installed. Check **Report Library** > **EMC M&R Health** > **Misc. Reports** > **Daily Dashboard** > **File Systems**.
6. Review and document any customizations.

   For example:

   - Polling intervals
   - Timeout values
7. Verify that all of the services are running on each host by checking **Centralized Management** > **Phyical Overview** > **<host>** > **Services**.

After you finish

Engage EMC Support to resolve any observed issues prior to proceeding with the upgrade.

Backing up the environment

Ensure the proper backup of all of the servers in your environment. This includes all of the frontend, backend, and collector hosts.

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

If it is allowed in your environment, perform a complete shutdown of ViPR SRM and take an offline VMware snapshot of each VM before starting the upgrade. These snapshots will allow you to quickly recover if you encounter any problems during the upgrade. After the upgrade is complete 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.

Note

Notify all users not to log in during the upgrade.

Refer to the following guides for details about your backup system:

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

These guides are available from the ViPR SRM Product Documentation Index.

VMAX discovery

In previous versions of ViPR SRM, you could discover VMAX2 arrays through SYMCLI topology collection. Beginning with ViPR SRM 4.1, the SolutionPack for EMC VMAX does not support data collection for VMAX2 arrays through SYMCLI.

Procedure

1. If you are upgrading from SRM 4.0.x, change the data collection for VMAX2 arrays to SMI-S before the upgrade.
2. If you are upgrading from SRM 3.7.x, take note of your discovered VMAX2 arrays and re-discover them after the upgrade.

   Note

   If you move the data collection for existing VMAX3/All Flash arrays to the SolutionPack for EMC VMAX HYPERMAX after the upgrade, disk related information will not be collected. Refer to the "SolutionPack for EMC VMAX HYPERMAX" chapter of the SolutionPack Guide for more information.

Checks for the SolutionPack for Physical Hosts

Hosts discovered with a private/public key pair will fail if the Generic-RSC instance (directory) created under "Remote-Shell-Collector" directory is cleaned up manually from the collector appliance. A sample path to the Generic-RSC instance on a Unix Collector is `/opt/APG/Collecting/Remote-Shell-Collector/Generic-RSC`.

Deleting backup schedules and scheduled reports from the DPA server

You should remove backup schedules and scheduled reports from the DPA server before the upgrade.

Procedure

1. If Avamar is discovered:

   a. Navigate 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. Navigate to **Admin** > **System** > **Manage Schedules**, and delete the following schedule:

  - Avamar-1HourInterval

2. If NetBackup is discovered:

   a. Navigate 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. Navigate to **Admin** > **System** > **Manage Schedules**, and delete the following schedule:

  - NBU-1HourInterval

Pre-upgrade steps for the SolutionPack for IBM LPAR

Before upgrading from 3.7.x to 4.1, complete the following steps to correct the serialnb property in the database.

Procedure

1. Change the following line in the `streamcollector-config-hmc.xml` file for collecting-configurations "LPAR-Collecting" from: `<properties context-key="serialnu" propertyname="serialnb"/>` to `<properties context-key="lparsernum" propertyname="serialnb"/>`
2. Restart the IBM-LPAR collector.

Upgrading from versions prior to 4.0.1

If you are updating a vApp installation from a ViPR SRM version prior to 4.0.1, EMC recommends reviewing Knowledge Base Article 000489632 (https://support.emc.com/kb/489632) before beginning the upgrade. A defect existed in earlier versions of ViPR SRM where upgrading to a version before 4.0.1 could cause a permission problem that disrupts future vApp updates. The article describes the situation in more detail and provides a script that can repair the problem if it exists. If needed, EMC recommends running this script before upgrading to ViPR SRM 4.1 to minimize the chance of errors. If you do not run the script, the update will still succeed, but the operating system software on the vApp deployment may not be updated.

Uploading the pre-upgrade ZIP file

Note

This section is only required if you are upgrading from SRM 3.7.x.

Procedure

1. Navigate to the Support by Product page for ViPR SRM (https://support.emc.com/products/34247_ViPR-SRM).
2. Click **Downloads**.
3. Download the `ViPR_SRM_4.1.0_Update_Supplement.zip` file.
4. From Centralized Management, click **Packages Management** on the left-hand pane.
5. On the **Packages Listing** page, click the **Upload** button.
6. Click **Browse**, and select the file.
7. Click **OK**.
8. **Click Continue**.

   The file is uploaded to the server.

Upgrading the system using Online Update

Procedure

1. If you have not already enabled Online Update:

   a. From Centralized Management, click **Configuration** > **Online Update**.

   b. Ensure that you are on the **Settings** tab.

   c. Check the **Enabled** checkbox.

   d. Type your EMC Online Support username and password.

   e. Click the icon to test connectivity to the update server.

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

   The icon indicates that connectivity to the server failed.

   f. Click **Save**.

2. Run the online update task:

   a. On the **Physical Overview** page, click ***<host_name>*** **- Front End**.

   b. Click **Tasks**.

   c. Type `OnlineUpdate` in the **Search** bar.

   d. Click the **OnlineUpdate** scheduled task.

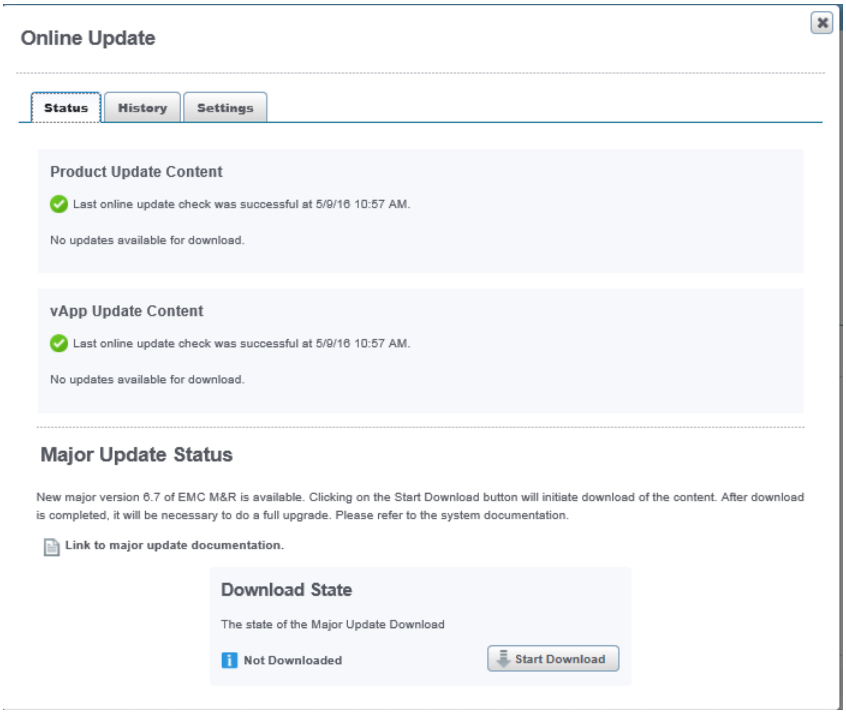
   e. Click **Run Now**.

3. Download the update:

   a. Click **Configuration** > **Online Update**.

   b. Click the **Status** tab.

   c. Click **Start Download**. When the download is finished, the Download State will change from "Not Downloaded" to "Complete."



Online Update

Product Update Content

✓ Last online update check was successful at 5/9/16 10:57 AM.

No updates available for download.

vApp Update Content

✓ Last online update check was successful at 5/9/16 10:57 AM.

No updates available for download.

Major Update Status

New major version 6.7 of EMC M&R is available. Clicking on the Start Download button will initiate download of the content. After download is completed, it will be necessary to do a full upgrade. Please refer to the system documentation.

Link to major update documentation.

Download State

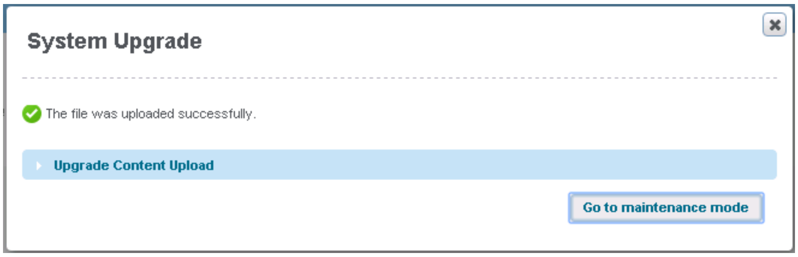
The state of the Major Update Download

Not Downloaded

4. From Centralized Management, click **Configuration** > **System Upgrade.**

   If an upgrade package is currently being downloaded via Online Update, wait until the download is complete before proceeding to the next step.

5. When you are ready to proceed with the upgrade, click **Go to maintenance mode**.

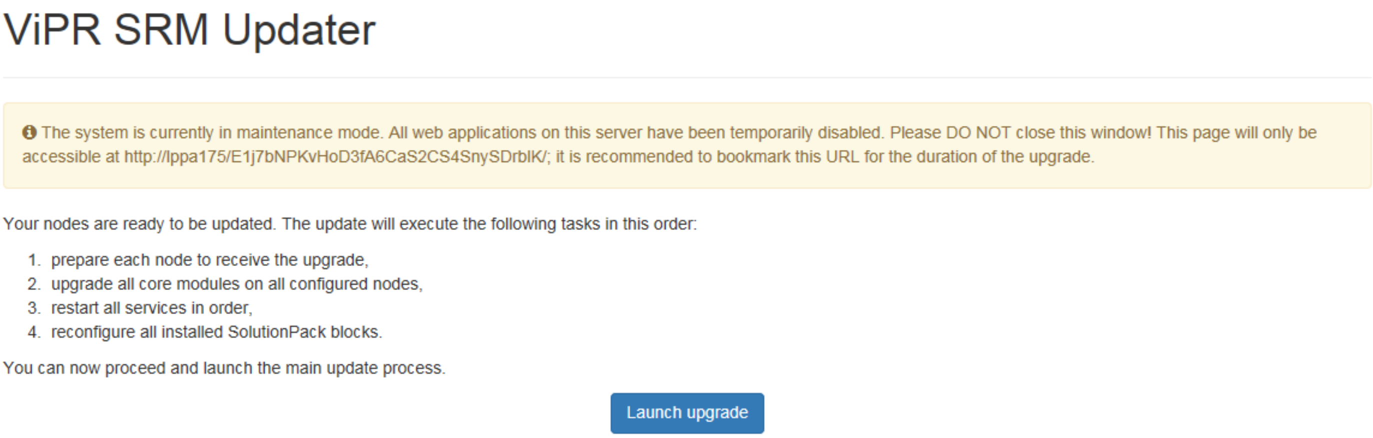


System Upgrade

✓ The file was uploaded successfully.

   Maintenance mode begins, the front end becomes unavailable, and after a short wait you are redirected to the Platform Upgrade page. Any users who try to access the front end will receive a message that it is in maintenance mode and has been temporarily disabled.

6. When the system has completed the validation checks, copy the URL from the message in the highlighted text, and then click **Launch upgrade**.



ViPR SRM Updater

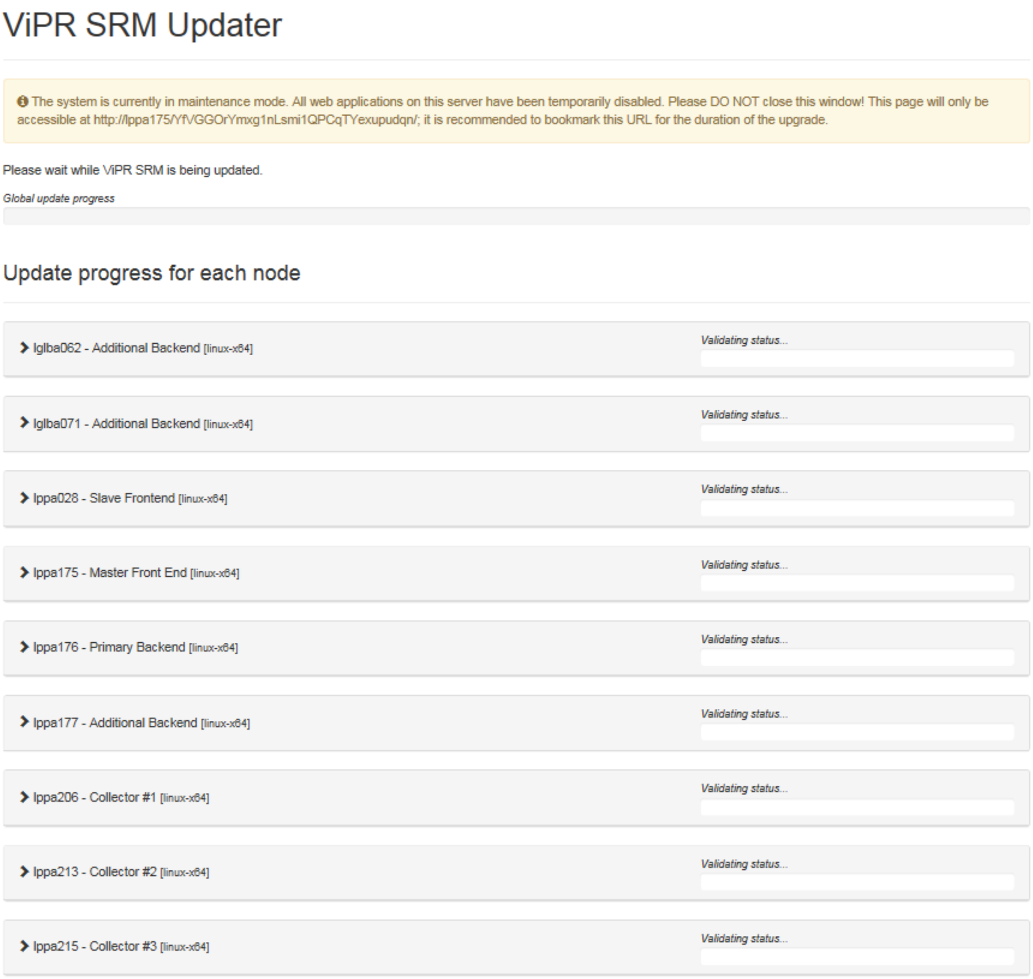
The system is currently in maintenance mode. All web applications on this server have been temporarily disabled. Please DO NOT close this window! This page will only be accessible at http://lppa175/E1j7bNPKvHoD3fA6CaS2CS4SnySDrblK/; it is recommended to bookmark this URL for the duration of the upgrade.

Your nodes are ready to be updated. The update will execute the following tasks in this order:

1. prepare each node to receive the upgrade,
2. upgrade all core modules on all configured nodes,
3. restart all services in order,
4. reconfigure all installed SolutionPack blocks.

You can now proceed and launch the main update process.

The system validates the status of the servers, prepares for the upgrade, and begins upgrading the modules.



ViPR SRM Updater

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 http://lppa175/YfVGGOrYmxg1nLsmi1QPCqTYexupudqn/; it is recommended to bookmark this URL for the duration of the upgrade.

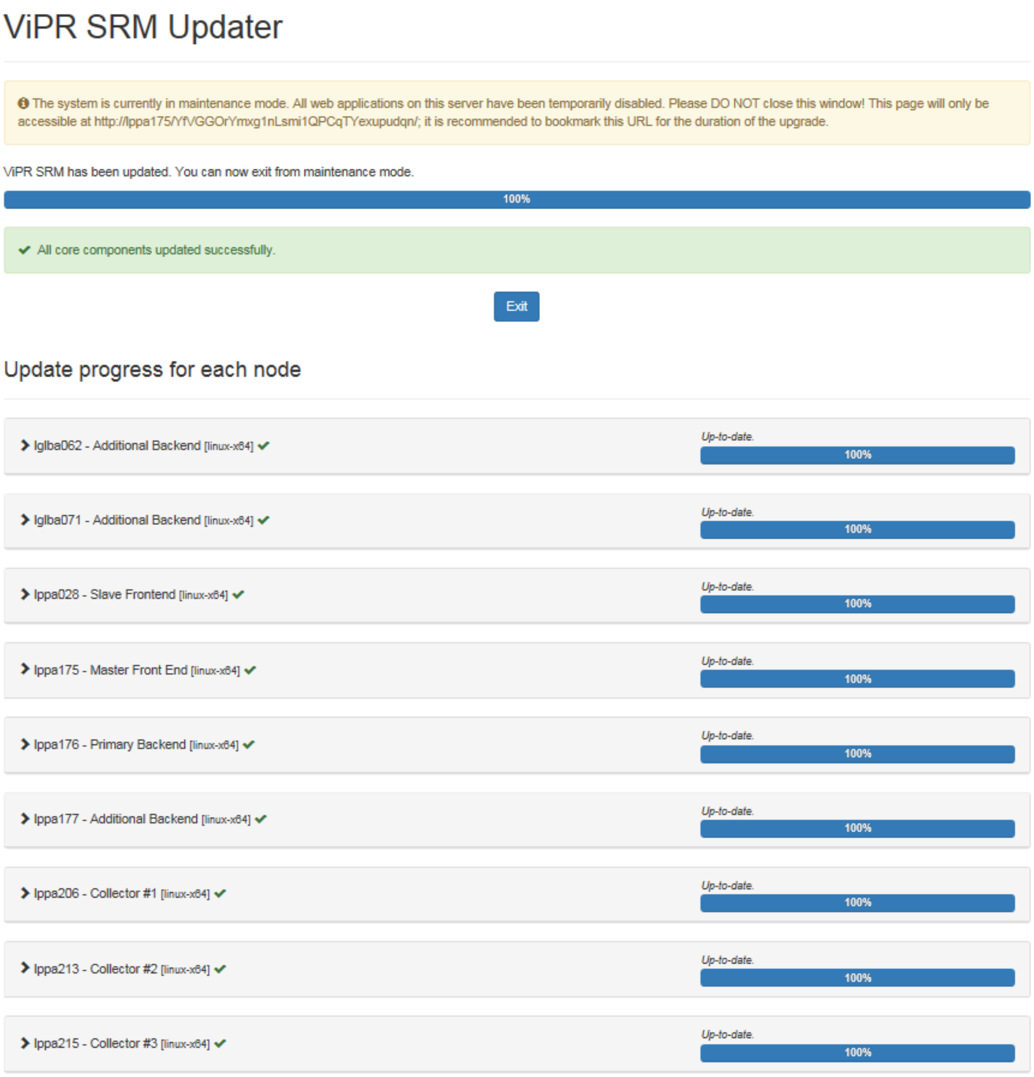
Please wait while ViPR SRM is being updated.

Global update progress

Update progress for each node

- lglba062 - Additional Backend [linux-x64] — *Validating status...*
- lglba071 - Additional Backend [linux-x64] — *Validating status...*
- lppa028 - Slave Frontend [linux-x64] — *Validating status...*
- lppa175 - Master Front End [linux-x64] — *Validating status...*
- lppa176 - Primary Backend [linux-x64] — *Validating status...*
- lppa177 - Additional Backend [linux-x64] — *Validating status...*
- lppa206 - Collector #1 [linux-x64] — *Validating status...*
- lppa213 - Collector #2 [linux-x64] — *Validating status...*
- lppa215 - Collector #3 [linux-x64] — *Validating status...*

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.



ViPR SRM Updater

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 http://lppa175/YfVGGOrYmxg1nLsmi1QPCqTYexupudqn/; it is recommended to bookmark this URL for the duration of the upgrade.

ViPR SRM has been updated. You can now exit from maintenance mode.

100%

✓ All core components updated successfully.

Exit

Update progress for each node

lglba062 - Additional Backend [linux-x64] ✓ Up-to-date. 100%

lglba071 - Additional Backend [linux-x64] ✓ Up-to-date. 100%

lppa028 - Slave Frontend [linux-x64] ✓ Up-to-date. 100%

lppa175 - Master Front End [linux-x64] ✓ Up-to-date. 100%

lppa176 - Primary Backend [linux-x64] ✓ Up-to-date. 100%

lppa177 - Additional Backend [linux-x64] ✓ Up-to-date. 100%

lppa206 - Collector #1 [linux-x64] ✓ Up-to-date. 100%

lppa213 - Collector #2 [linux-x64] ✓ Up-to-date. 100%

lppa215 - Collector #3 [linux-x64] ✓ Up-to-date. 100%

7. Click **Exit**.

   The system restarts the front end and redirects you to the SolutionPack UI.

Upgrading the system without using Online Update

Procedure

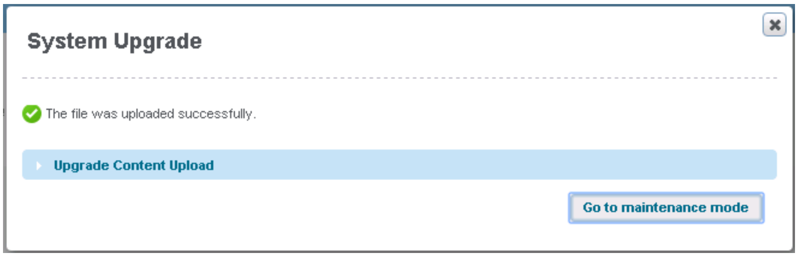
1. Navigate to the Support by Product page for ViPR SRM (https://support.emc.com/products/34247_ViPR-SRM).
2. Click **Downloads**.
3. Download the core update file for each of your deployed architectures. The vApp file also contains the appliance update file for vApp deployments.

Option	File Title	File Name
Linux (vApp)	ViPR SRM <Version Number> vApp Update for System Upgrade UI	ViPR_SRM_<version_number>_vApp_Update_UI.zip

Option	File Title	File Name
Linux (binary only)	ViPR SRM <Version Number> Linux Update	ViPR_SRM_<version_number>_Linux_64-bit_Update_File.zip
Windows	ViPR SRM <Version Number> Windows Update	ViPR_SRM_<version_number>_Windows_64-bit_Update_File.zip

4. From Centralized Management, click **Configuration** > **System Upgrade.**
5. Click the **Browse** button (or buttons for mixed environments) and provide the upgrade files for your platforms.
6. Click **Upload Content**.
7. The system displays a message about ensuring that there is minimum of 5 GB disk space on the servers. Click **OK**.

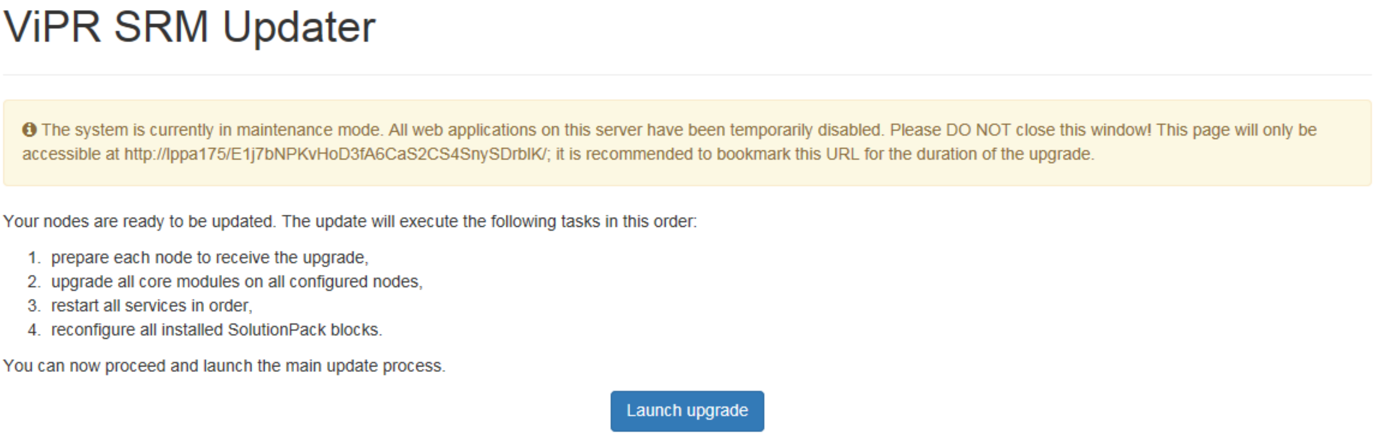
   The system upgrade files are uploaded to Centralized Management and non-disruptively distributed to all of the servers in the deployment. This process may take several minutes.
8. When you are ready to proceed with the upgrade, click **Go to maintenance mode**.

   System Upgrade

   The file was uploaded successfully.

   Maintenance mode begins, the front end becomes unavailable, and after a short wait you are redirected to the Platform Upgrade page. Any users who try to access the front end will receive a message that it is in maintenance mode and has been temporarily disabled.
9. When the system has completed the validation checks, copy the URL from the message in the highlighted text, and then click **Launch upgrade**.



ViPR SRM Updater

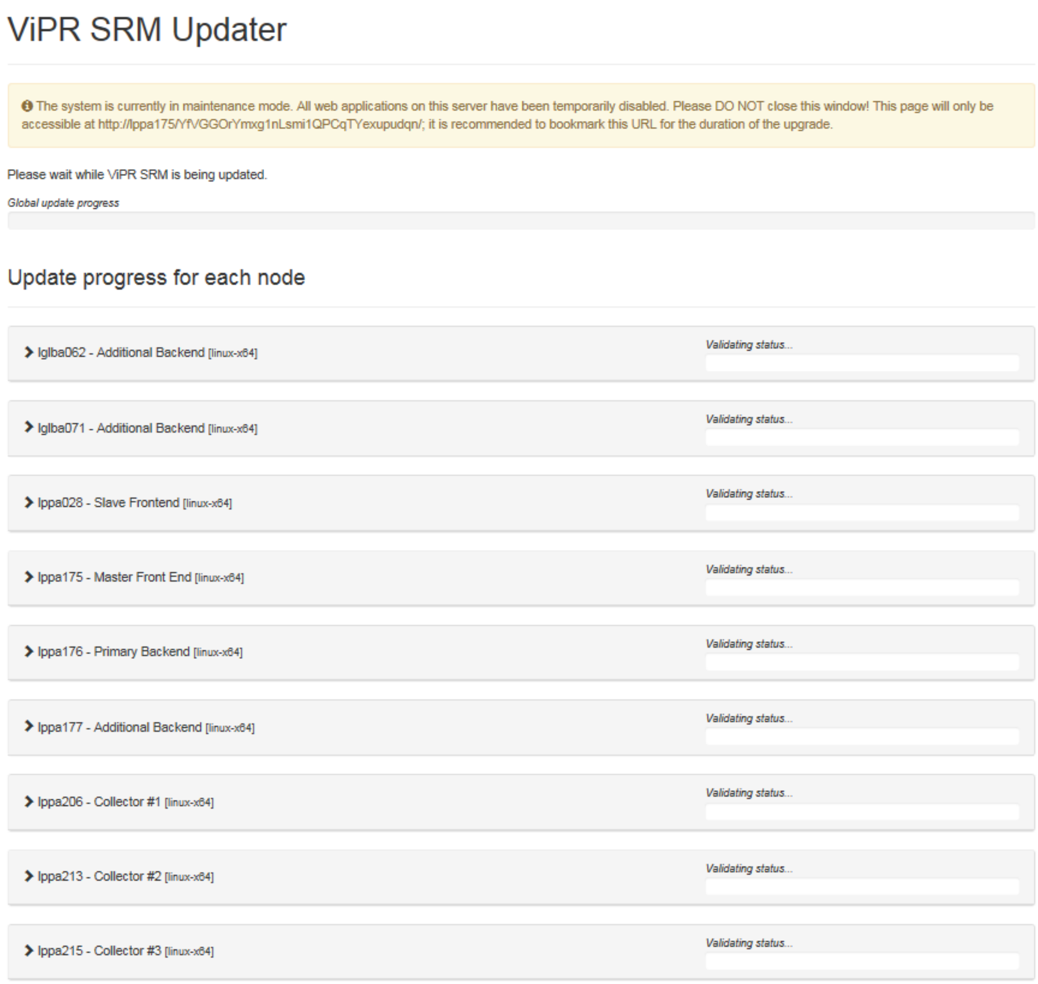
The system is currently in maintenance mode. All web applications on this server have been temporarily disabled. Please DO NOT close this window! This page will only be accessible at http://lppa175/E1j7bNPKvHoD3fA6CaS2CS4SnySDrblK/; it is recommended to bookmark this URL for the duration of the upgrade.

Your nodes are ready to be updated. The update will execute the following tasks in this order:

1. prepare each node to receive the upgrade,
2. upgrade all core modules on all configured nodes,
3. restart all services in order,
4. reconfigure all installed SolutionPack blocks.

You can now proceed and launch the main update process.

The system validates the status of the servers, prepares for the upgrade, and begins upgrading the modules.



ViPR SRM Updater

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 http://lppa175/YfVGGOrYmxg1nLsmi1QPCqTYexupudqn/; it is recommended to bookmark this URL for the duration of the upgrade.

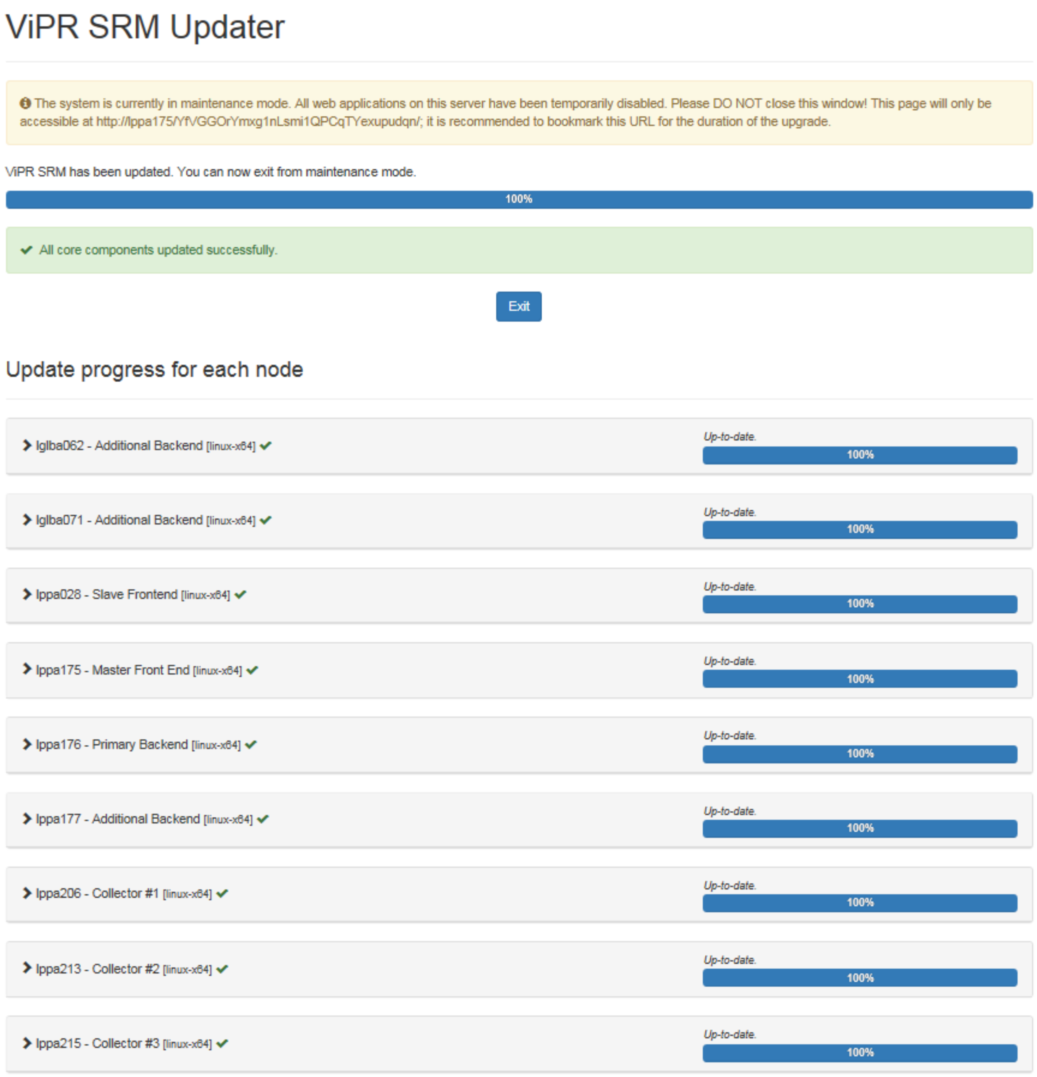
Please wait while ViPR SRM is being updated.

Global update progress

Update progress for each node

- lglba062 - Additional Backend [linux-x64] — *Validating status...*
- lglba071 - Additional Backend [linux-x64] — *Validating status...*
- lppa028 - Slave Frontend [linux-x64] — *Validating status...*
- lppa175 - Master Front End [linux-x64] — *Validating status...*
- lppa176 - Primary Backend [linux-x64] — *Validating status...*
- lppa177 - Additional Backend [linux-x64] — *Validating status...*
- lppa206 - Collector #1 [linux-x64] — *Validating status...*
- lppa213 - Collector #2 [linux-x64] — *Validating status...*
- lppa215 - Collector #3 [linux-x64] — *Validating status...*

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.



ViPR SRM Updater

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 http://lppa175/YfVGGOrYmxg1nLsmi1QPCqTYexupudqn/; it is recommended to bookmark this URL for the duration of the upgrade.

ViPR SRM has been updated. You can now exit from maintenance mode.

100%

✓ All core components updated successfully.

Update progress for each node

- lglba062 - Additional Backend [linux-x64] ✓ Up-to-date. 100%
- lglba071 - Additional Backend [linux-x64] ✓ Up-to-date. 100%
- lppa028 - Slave Frontend [linux-x64] ✓ Up-to-date. 100%
- lppa175 - Master Front End [linux-x64] ✓ Up-to-date. 100%
- lppa176 - Primary Backend [linux-x64] ✓ Up-to-date. 100%
- lppa177 - Additional Backend [linux-x64] ✓ Up-to-date. 100%
- lppa206 - Collector #1 [linux-x64] ✓ Up-to-date. 100%
- lppa213 - Collector #2 [linux-x64] ✓ Up-to-date. 100%
- lppa215 - Collector #3 [linux-x64] ✓ Up-to-date. 100%

10. Click **Exit**.

    The system restarts the front end and redirects you to the SolutionPack UI.

CHAPTER 2

Upgrading the SolutionPacks

This chapter includes the following topics:

Upgrading all SolutionPacks and other components

Before you begin

Synchronize the packages across the servers:

1. From Centralized Management, click **Packages Management** on the left-hand pane.
2. Click the **Synchronization** button.
3. Select **retrieve the latest packages from the remote servers**.
4. Wait for the synchronization to complete before proceeding.

Note

When you upgrade the SolutionPack for EMC RecoverPoint, the polling interval set during the SolutionPack installation is lost because the polling intervals for capacity and performance data collection were separated.

Note

Alert definitions have been reorganized in several SolutionPacks for SRM 4.1. Due to the name changes of these alert definitions, upgrading to ViPR SRM 4.1 results in two sets of alert definitions being listed. This issue applies to the following SolutionPacks:

- Dell SC and FS Series
- IBM SAN Volume Controller/Storwize
- Isilon
- Unity/VNX/VNXe
- VPLEX

To avoid duplicate alert definitions:

1. Remove and reinstall the pre-configured alerts component for each affected SolutionPack. If you want to preserve your customized alert definitions, complete the following two optional steps before proceeding.
2. Optional: Backup the alert definitions for all SolutionPacks by exporting "Alert definitions" from the Alerting Frontend. You can also backup the definitions for an individual SolutionPack by clicking the SolutionPack folder name and exporting from there.
3. Optional: Backup the `alerting-contexts.xml` file by navigating to **Centralized-Management** > **Logical Overview** > **Backends** > **Alerting Backend**. 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.
4. Navigate to **Centralized Management**.
5. Click **SolutionPacks** > **Storage** > **<SolutionPack Name>**.
6. Remove the **Pre-configured alerts** block using the trash can icon. This deletes all of the alert definitions for the SolutionPack.
7. Click **SOLUTIONPACK CENTER**.

8. Select **<SolutionPack Name>** from the **Browse and Install SolutionPacks** window.
9. Click **Install**.
10. Ensure that the **Pre-configured alerts** component is selected and click **Next**.
11. Click **Install**.

Procedure

1. Complete the following steps to upgrade all of the SolutionPacks and other components:
2. From Centralized Management, click **SolutionPacks** on the left-hand pane.
3. Click the **Update All Components** button in the top-right corner of the page.

   Note

   If the button is disabled, your system has all of the latest SolutionPacks, and you can skip the remaining steps in this section.

   The **Initialization** window opens and lists the following details:

   - Number of components from SolutionPacks that will be updated to the latest version.
   - Number of components that contain new features that require configuration.

4. Click **Next**. The **Configuration** window opens. The left-hand pane lists each of the components that include new features that you need to configure. The right-hand pane displays the configuration details for the component with the new features highlighted in yellow. Carefully review the selections to make sure the configuration details for the components and SolutionPacks are correct, and modify any configuration that are not set correctly. When you have finished configuring a component, click **Next** to move onto the next component. You must edit some SolutionPack entries while reviewing the configuration.

   - For the SolutionPack for EMC RecoverPoint, select an existing topology service or add a new one.
   - For the SolutionPack for Microsoft Hyper-V, select an existing topology service or add a new one.
   - For the SolutionPack for EMC ScaleIO, select an existing frontend web service or add a new one.
   - If you are upgrading from 3.7.x in a multiple-server installation, for the ESRS Web-Service Gateway, specify the instance that corresponds to the frontend.

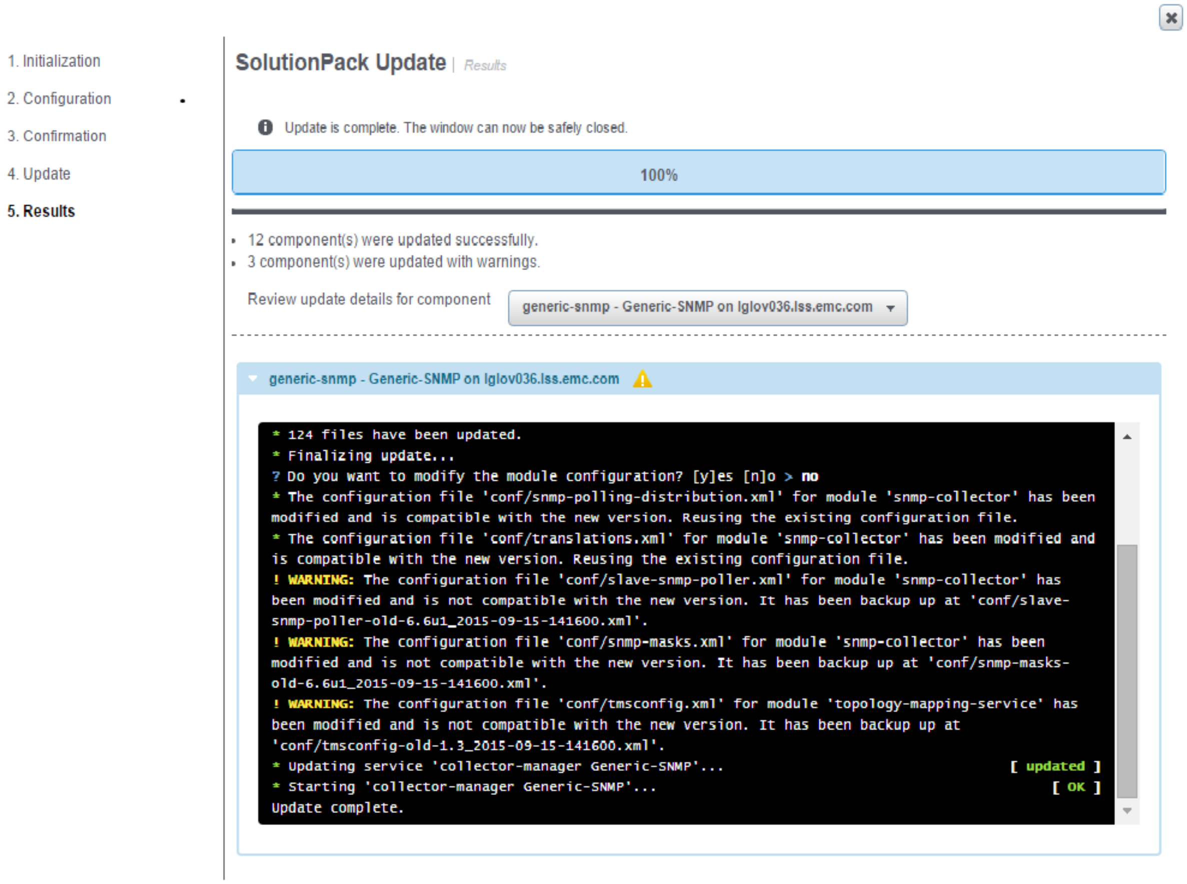
5. After you have configured every component on the list, click **Next**.
6. The **Confirmation** window opens and lists all of the components that will be updated. Confirm that all of the components are correctly listed, and then click **Update**.
7. The **Update** window opens and displays the progress 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 will be reused and the system will display a message to let you know. If a manually edited file is not compatible with the new version of the SolutionPack, the system will back up the file and display a warning message that 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 safely 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



SolutionPack Update | Results

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

100%

- 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.
```

8. The **Results** window opens. Use the drop-down menu to check the status of each component. Any manually edited files that were backed up by the system will be displayed under “Updated with warnings.”

9. Verify that all of the services are running on each host by checking **Centralized Management** > **Phyical Overview** > **<host>** > **Services**.

Note

It is normal for the Topology-Mapping Service on the primary backend, the frontend, or the additional backend to remain stopped at this point. The service will start automatically when the SolutionPack for EMC M&R Health is upgraded on these systems.

10. Restart the Tomcat service:

    a. Log in to the ViPR SRM Frontend server.

b. Navigate to the `bin` directory.

c. Run the following command:

Operating System	Command
UNIX	`./manage-modules.sh service restart tomcat`
Windows	`manage-modules.cmd service restart tomcat`

11. In Windows deployments, the Java module is updated during the upgrade, but the old version of Java is not removed. EMC 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>’
```

CHAPTER 3

Post-Upgrade Tasks

This chapter includes the following topics:

Checking 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.

Before you begin

Check that all services have started on each of the hosts:

1. Navigate to **Centralized Management** > **Physical Overview**.
2. For each host, click the host name.
3. Verify that the status for each service is **Started**.

If a service did not start automatically, restart the service manually.

Procedure

1. Click the name of the service.
2. 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 that can be resolved by reconfiguring the SolutionPack settings and manually starting the service again.

Increasing the heap size for the Tomcat service

Increase the heap size for the Tomcat service on the frontend to 8 GB.

Procedure

1. Navigate to **Centralized Management** > **Physical Overview** > **Front End**.
2. On the **Services** tab, click the Tomcat module.
3. Click **Configure service**.
4. From the **Available memory for the service** drop-down menu, select **Custom**.
5. In the **max** field, type `8`, and select **GB** from the drop down menu.
6. Click **Save**.

Fixing broken links

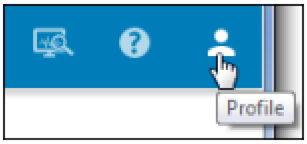
Due to changes in the report structure, some report links may be broken during the upgrade. The Link Detection Tool allows you to easily identify and potentially fix these links.

The following types of links are potentially affected:

- Links from custom reports to out-of-the-box reports
- Scheduled reports
- Favorite reports
- Pinned reports
- Pre-generated reports

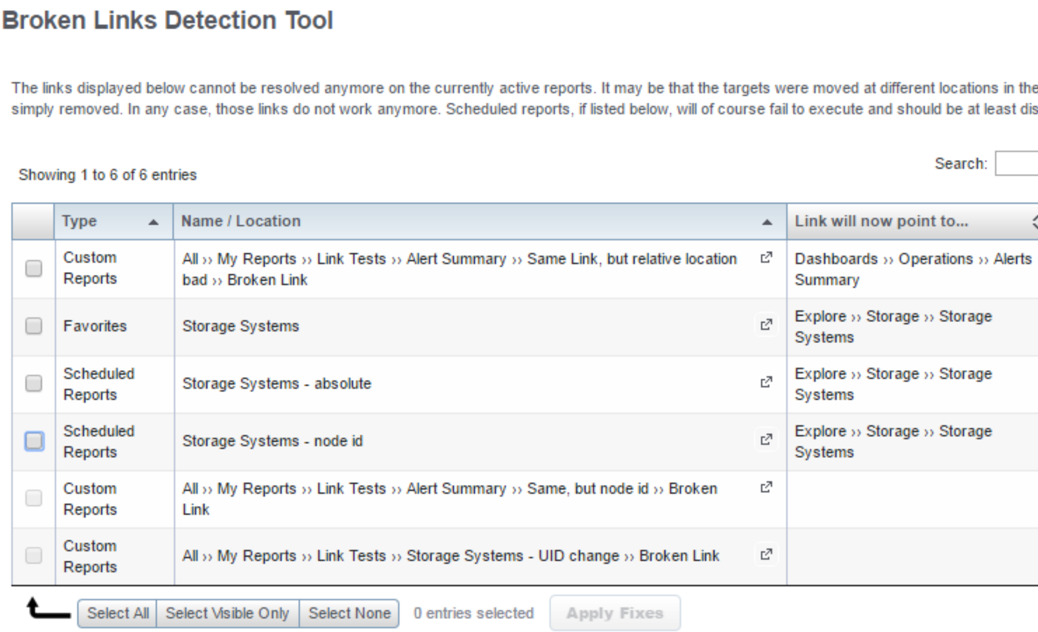
Procedure

1. From the VIPR SRM Frontend, click **Profile** > **View Profile** in the banner.



2. Click the **Custom Reports** tab.
3. Click **Open Tool**.

   The system displays a potential match for each broken link.



Broken Links Detection Tool

The links displayed below cannot be resolved anymore on the currently active reports. It may be that the targets were moved at different locations in the
simply removed. In any case, those links do not work anymore. Scheduled reports, if listed below, will of course fail to execute and should be at least dis

Showing 1 to 6 of 6 entries

Search:

	Type	Name / Location	Link will now point to...
□	Custom Reports	All ›› My Reports ›› Link Tests ›› Alert Summary ›› Same Link, but relative location bad ›› Broken Link	Dashboards ›› Operations ›› Alerts Summary
□	Favorites	Storage Systems	Explore ›› Storage ›› Storage Systems
□	Scheduled Reports	Storage Systems - absolute	Explore ›› Storage ›› Storage Systems
□	Scheduled Reports	Storage Systems - node id	Explore ›› Storage ›› Storage Systems
□	Custom Reports	All ›› My Reports ›› Link Tests ›› Alert Summary ›› Same, but node id ›› Broken Link	
□	Custom Reports	All ›› My Reports ›› Link Tests ›› Storage Systems - UID change ›› Broken Link	

4. Evaluate each of the potential matches to determine if it is correct. Select the checkbox for each correct match, and then click **Apply Fixes**.

   The system fixes the links to point to the correct target.

Installing new alerting components

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.

The following table lists the new SolutionPackBlocks that you need to install.

SolutionPack Name	New SolutionPackBlocks
EMC Centera	Alert Consolidation, Pre-configured alerts
EMC Data Domain	Alert Consolidation, Pre-configured alerts
EMC Data Protection Advisor	Events, Pre-configured alerts
EMC VPLEX	Alert Consolidation, Pre-configured alerts

SolutionPack Name	New SolutionPackBlocks
IBM DS	Alert Consolidation, Pre-configured alerts
IBM SAN Volume Controller/Storwize	Pre-configured alerts
Microsoft SQL Server	Pre-configured alerts
Oracle Database	Pre-configured alerts, ASM Data collection

Procedure

1. From **Centralized Management**, click **SolutionPack Center**.
2. Navigate to the SolutionPack for which a new Solution Pack 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**.

After you finish

Note

VPLEX threshold based alerts are disabled by default. To manually enable threshold based alerts, go to **Administration** > **Modules** > **Alerting** > **Alert Definitions** > **EMC VPLEX Alert Definitions**. (SNMP based alerts are enabled by default.)

Changing the host port for Dell SC Series devices

During the upgrade, the Dell Storage Manager Data Collector Host Port is automatically populated with the default port number 3033. You can change the port number if necessary.

Procedure

1. From **Centralized Management**, navigate to **Discovery Center** > **Inventory Management** > **SolutionPack for Dell SC Series.**.
2. Click the row for the device that you want to update.
3. Enter the correct **Dell Storage Manager Data Collector Host Port**.
4. Click **OK**.
5. Verify that the port is open from the Collector Hosts and the device.

Restoring 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.

Procedure

1. On Linux, run the following command on each server to find the files with values that changed: `find / -name *old*2016* -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 desired values accordingly.

Editing new actions scripts

Edit actions on the frontend host to send events to the machine on which the event-processing-manager of the alerting-consolidation module is configured.

Procedure

1. In the following file, replace 127.0.0.1 with the primary backend IP address:

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`

Configuring SolutionPack blocks to use SSL

If SSL was enabled before the upgrade, you must make some configuration changes after completing the upgrade.

This issue applies to the following SolutionPack blocks:

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

Note

For Compliance, if you want to use certificate validation, add the 4.1 certificate as described in Using Compliance in ViPR SRM.

Procedure

1. Navigate to **Centralized Management** > **Central Configuration Repository** > **Fronted Web service**.
2. Type `frontend` in the **Search** field.
3. Click the row that corresponds to the SolutionPack block that you need to configure.

4. Click the checkbox for the component that you need to configure.
5. Type `58443` in the **Tomcat port** field.
6. Select **HTTPS** from the **Tomcat communication protocol** drop-down menu.
7. Click **Update**.

Deleting old data from the SolutionPack for EMC Atmos

After the upgrade, historical data for the SolutionPack for EMC Atmos is not consistent with newly collected data. EMC recommends deleting the old data. If you do not delete the old data, you will see duplicate or inconsistent reports until the previous metrics turn inactive in 14 days.

Procedure

1. Navigate to **Centralized Management** > **Logical Overview** > **Collecting**.
2. Open the Collector-Manager :: emc-atmos module, and click **Stop**.
3. Navigate to **Administration** > **Modules** > **Management of Database Metrics**.
4. Right-click **Filter <Everything>**, select **Edit expression**, and enter the following text:

   ```
   source='ATMOS%'
   ```

5. Click **Query**.
6. Select all of the metrics, click **Delete**, and accept the warning that displays.
7. Click **OK**.
8. Navigate to **Centralized Management** > **Logical Overview** > **Collecting.**
9. Open the Collector-Manager :: emc-atmos module, and click **Start**.

Installing the Compliance Rules module

Procedure

1. Navigate to **Centralized Management** > **SolutionPack Center**.
2. Click **Storage Compliance**.
3. Click **Install**.
4. Ensure that the Compliance Rules module is auto populated with the appliance where the compliance backend is installed.
5. Click **Next**.
6. From the **Web-Service Gateway** drop-down menu, select **Gateway on <Primary Backend Host>**.
7. Click **Install**.
8. Click **OK**.

   Note

   Make sure to rerun all the policies which contain "Default Zoning must be Disabled" rule in enabled state or else there might be some discrepancy in number of breaches.

Cisco MDS/Nexus switch discovery

In previous versions of ViPR 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 via Discovery Center. The advantage of using Discovery Center is that you can discover all of 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.

Exporting Cisco MDS/Nexus switches

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

Procedure

1. Navigate to **SNMP Device Discovery** > **Devices**.
2. Select all of the Cisco MDS/Nexus switches.
3. From the **Actions** drop-down menu, select **Export seed file**, and click **Execute Action**.

Results

The system saves a file named `agents.csv` to the local machine. The exported seed file consists of both the switch details and credentials. The same exported seed file needs to be used for importing the switch details and credentials into the respective tables using the Discovery Groups tab in Discovery Center.

Installing the SNMP Data Collector

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

Procedure

1. Click **Administration** ⚙.
2. Click **Centralized Management**.
3. Click **SolutionPack Center**.
4. Select the SolutionPack for Cisco MDS/Nexus in the **Browse and Install SolutionPacks** window.
5. Click **Install**.
6. From the **SNMP Data Collection** drop-down menu, select the server where you want to install the component.

Note

Multiple SNMP Data Collectors can be installed on different Collector Servers. EMC recommends installing at least one Cisco SNMP Data Collector per Datacenter.

7. Click **Next**.

   The window displays SNMP data collection details. For additional information, refer to the "SolutionPack for Cisco MDS/Nexus" chapter of the *EMC ViPR SRM 4.1 SolutionPack Guide*.

8. Click **Install**.

   If you are using passive host discovery, you may need to modify the regex expressions. Refer to the "Passive host discovery configuration options" section of the *EMC ViPR SRM 4.1 SolutionPack Guide*.

Importing 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 your switches to Discovery Center.

Procedure

1. Navigate to **Discovery Center** > **Discovery Center 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. Click **Inventory Management** in the left-hand pane, and click **Cisco MDS/Nexus**.
5. Click the **Discovery 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 **Import**.
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 datacenter configuration, after the switches have been assigned to a Cisco MDS Collector, you must manually reassign the switch assignment to the data collector.

Deleting switches from SNMP Device Discovery

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

Procedure

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

Updating capabilities

For devices discovered through the Cisco MDS collector in Discovery Center, ViPR SRM 4.1 introduced a new capability called “CISCO-DEVICE-ALIAS” ([DALIAS]) that enables the discovery of Device Aliases that participate in an Active ZoneSet.

Complete the following procedure to start polling the new capability after upgrading to ViPR SRM 4.1.

Procedure

1. Navigate to **Centralized Management** > **Discovery Center** > **Inventory Management** > **Cisco MDS/Nexus** and click the row for a Cisco switch.
2. The **Add a new Cisco MDS/Nexus** window opens. Click **Test**.
3. After the Test function completes, click **OK**.
4. Repeat these steps for all of the switches that are discovered in Discovery Center.
5. Click **Save** to trigger polling.

Updating the SNMP collections

Learn how to update the SNMP collections and synchronize the configuration.

Procedure

1. Log into the device discovery web interface at `http://<Frontend IP address>:58080/device-discovery`.

(On the Administration Dashboard, Device Discovery has been renamed SNMP Device Discovery.)

2. Click **Collectors** in the left-hand pane.
3. On the **Collectors** page, click the checkbox for each collector.
4. Click the **Delete** icon.
5. Cick **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 of 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 will contain 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, navigate through the UI and review your Reports, SolutionPacks, and other features. One way to check the health of the system is to look at the reports in the EMC Watch4net 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.

Deleting report templates and times from the DPA server

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.

Procedure

1. If Avamar is discovered:

    a. Navigate 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. Navigate to **Admin** > **System** > **Manage Time Periods**, and delete the following time period:

    - AvamarLasthouroffsetby15mins

    c. Navigate to **Admin** > **System** > **Manage Time Periods** > **Create Time Period** > **Edit Times**, and delete the following times:

- Avamar15Minsago
- Avamar1Hourand15Minsago

2. If NetBackup is discovered:

   a. Navigate 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. Navigate to **Admin** > **System** > **Manage Time Periods**, and delete the following time period:

      - NetBackupLasthouroffsetby15mins

   c. Navigate to **Admin** > **System** > **Manage Time Periods** > **Create Time Period** > **Edit Times**, and delete the following times:

      - NetBackup15Minsago
      - NetBackup1Hourand15Minsago

3. Restart the DPA Collector in ViPR SRM.

Creating an events database for the SolutionPack for DPA

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

Before you begin

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

Procedure

1. Login to the Primary Backend server via the command line.
2. Navigate to the following location:

   `/opt/APG/bin/`

3. Execute the following command:

   `./mysql-client.sh`

4. Enter the apg db password.

   The default apg db password is `watch4net`

5. Execute the following command:

   `connect events;`

6. Create the following table:

```
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. Follow the steps below only if you are upgrading from ViPR SRM 4.0 to ViPR SRM 4.1:

   a. From ViPR SRM, navigate to **Administration** > **Centralized Management** > **SolutionPacks** > **Storage** > **EMC 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 ViPR SRM, navigate to **Administration** > **Centralized Management** > **Logical Overview** > **Collecting** > **Events** and restart the **Event-Processing-Manager :: emc-dpa - *server_name*** collector.
9. From ViPR SRM, navigate to **Administration** > **Centralized Management** > **Logical Overview** > **Collecting** and restart the **Collector-Manager :: emc-dpa - *server_name*** collector.

Installing the Device Configuration Wizard

After upgrading to ViPR SRM 4.1, you may want to install the Device Configuration Wizard to collect new devices in an easier way. The Device Configuration Wizard may or may not have been installed in a previous version of ViPR SRM.

Procedure

1. Check to see if the Device Configuration Wizard is already installed:

    a. Navigate to **Centralized Management** > **Logical Overview** > **Frontends**.

    b. In the **Search** field, type `Device-Configuration-Wizard`.

    If the Device Configuration Wizard module is listed, then it is already installed and you do not have to do anything. If it is not installed, and you want to install the Device Configuration Wizard, complete the following steps.

2. Navigate to **Centralized Management** > **<Front End server>** > **Packs & Modules**.
3. Click **Install**.
4. On the **Packages Installation** page, click **Web Applications**.
5. Under **Packages**, click **Device-Configuration-Wizard v4.1**, and then click **Launch**.
6. On the **Installation Steps** page, type the instance name, and then click **Install**. Close the window when the installation is complete.
7. Restart the Tomcat Service(s). If there are several Tomcat Services on the same host, you may have been asked where to install the Device Configuration Wizard. Restart the ones that you chose.

    a. On the same **Centralized Management** > **<Front End server>** > **Packs & Modules** page, type `tomcat` in the **Search** field.

    a. Click the Tomcat Service where you installed the Device Configuration Wizard.

    b. In the **Service Status** section, click **Restart**.

8. On the same Tomcat Service page, expand the **Configuration Files** section.
9. Click **Edit File** (pencil icon) for `conf/Catalina/localhost/device-config-wizard.xml`.

    Replace:

```
<ResourceLink name="dba/master" global="dba/master"
type="com.watch4net.apg.gui.datasource.DatasourceConfiguration
" />
```

with:

```
<ResourceLink name="jdbc/master" global="jdbc/master"
type="javax.sql.DataSource"/>
```

10. Restart the tomcat service again.

Backend-tools

ViPR SRM 4.0.1 includes a new module (backend-tools) that provides a user interface for configuring data-retention parameters. After you install the backend-tools, you can configure the data-retention settings through the Centralized Management user interface.

This new module is a SolutionPackBlock that is not installed by default during the upgrade to version 4.0.1. The backend-tools module is installed with new 4.0.1 deployments.

Note

Installing the backend-tools will reset data retention settings and port number to default settings.

Backend-tools takes ownership of the following files:

In the `APG/Backends/APG-Backend/<instance>/conf` directory:

- aggregates.xml
- config.xml
- mysql.xml
- socketinterface.xml
- telnetinterface.xml

In the `APG/Tools/MySQL-Maintenance-Tool<instance>/conf` directory:

- mysql.xml
- mysql-root-apg.xml
- mysql-root-mysql.xml

Installing the backend-tools

Install the backend-tools on the primary backend and additional backend servers. One backend-tools instance is installed for each APG-Backend instance.

Before you begin

- Additional backend groups cannot be configured
- The `aggregates.xml` file cannot be modified.
- `Cross-Failover-Socket-Collector` cannot be configured.
- The M&R backend cannot include custom configurations.
- You must know the MySQL password (if it is not the default).

Procedure

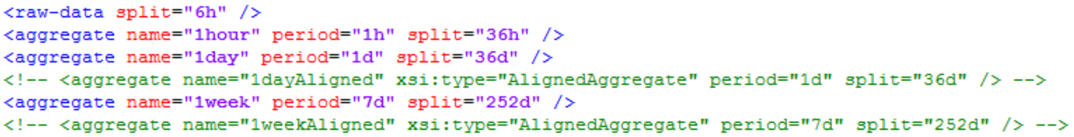
1. Gather the configured settings before installing the backend tools.

Note

The default settings for the backend-tools shown during the installation do not reflect the current configuration of the backend. If you accept the defaults, the previous settings will be lost.

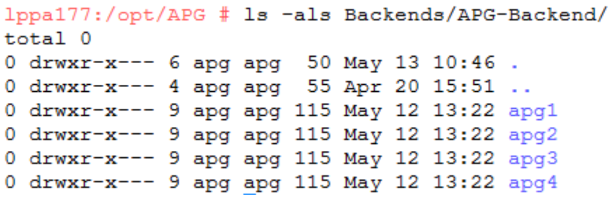
a. Review the settings in the `aggregates.xml` files. Take note of any non-default settings so you can use them when installing the backend-tools.

- On the Primary Backend, the file is located in the `/opt/APG/Backends/APG-Backend/Default/conf` directory.
- On the Additional Backends, the files are located in the `/opt/APG/Backends/APG-Backend/apg[1..4]/conf` directories. (The following example uses the default settings.)



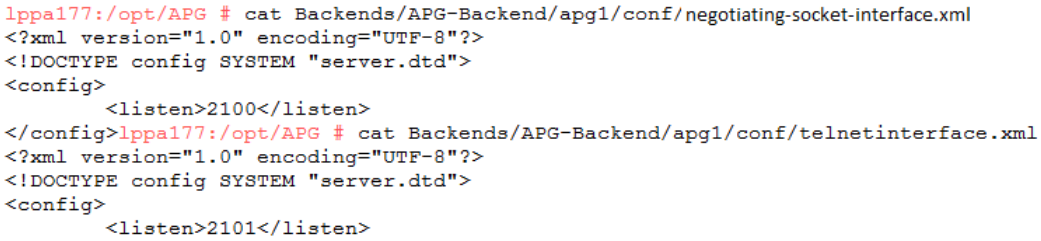
```
<raw-data split="6h" />
<aggregate name="1hour" period="1h" split="36h" />
<aggregate name="1day" period="1d" split="36d" />
<!-- <aggregate name="1dayAligned" xsi:type="AlignedAggregate" period="1d" split="36d" /> -->
<aggregate name="1week" period="7d" split="252d" />
<!-- <aggregate name="1weekAligned" xsi:type="AlignedAggregate" period="7d" split="252d" /> -->
```

b. Verify the APG-Backend instance names. (The example below is for an additional backend server.)



```
lppa177:/opt/APG # ls -als Backends/APG-Backend/
total 0
0 drwxr-x--- 6 apg apg  50 May 13 10:46 .
0 drwxr-x--- 4 apg apg  55 Apr 20 15:51 ..
0 drwxr-x--- 9 apg apg 115 May 12 13:22 apg1
0 drwxr-x--- 9 apg apg 115 May 12 13:22 apg2
0 drwxr-x--- 9 apg apg 115 May 12 13:22 apg3
0 drwxr-x--- 9 apg apg 115 May 12 13:22 apg4
```

c. Determine the socket interface and telnet interface ports for each of the database instances on each backend server.



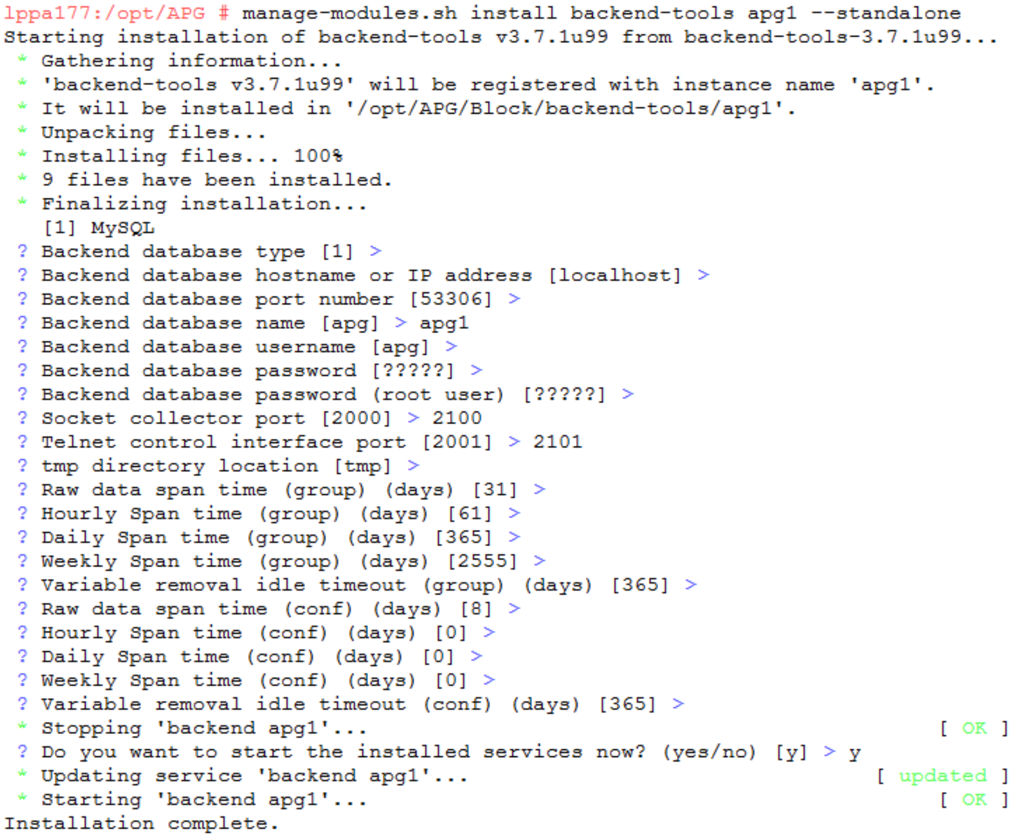
```
lppa177:/opt/APG # cat Backends/APG-Backend/apg1/conf/negotiating-socket-interface.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE config SYSTEM "server.dtd">
<config>
        <listen>2100</listen>
</config>lppa177:/opt/APG # cat Backends/APG-Backend/apg1/conf/telnetinterface.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE config SYSTEM "server.dtd">
<config>
        <listen>2101</listen>
```

Default ports:

Backend Server	Socket Interface Port	Telnet Interface Port
Primary Backend (Default)	2000	2001
Additional Backend (apg1)	2100	2101
Additional Backend (apg2)	2200	2201
Additional Backend (apg3)	2300	2301
Additional Backend (apg4)	2400	2401

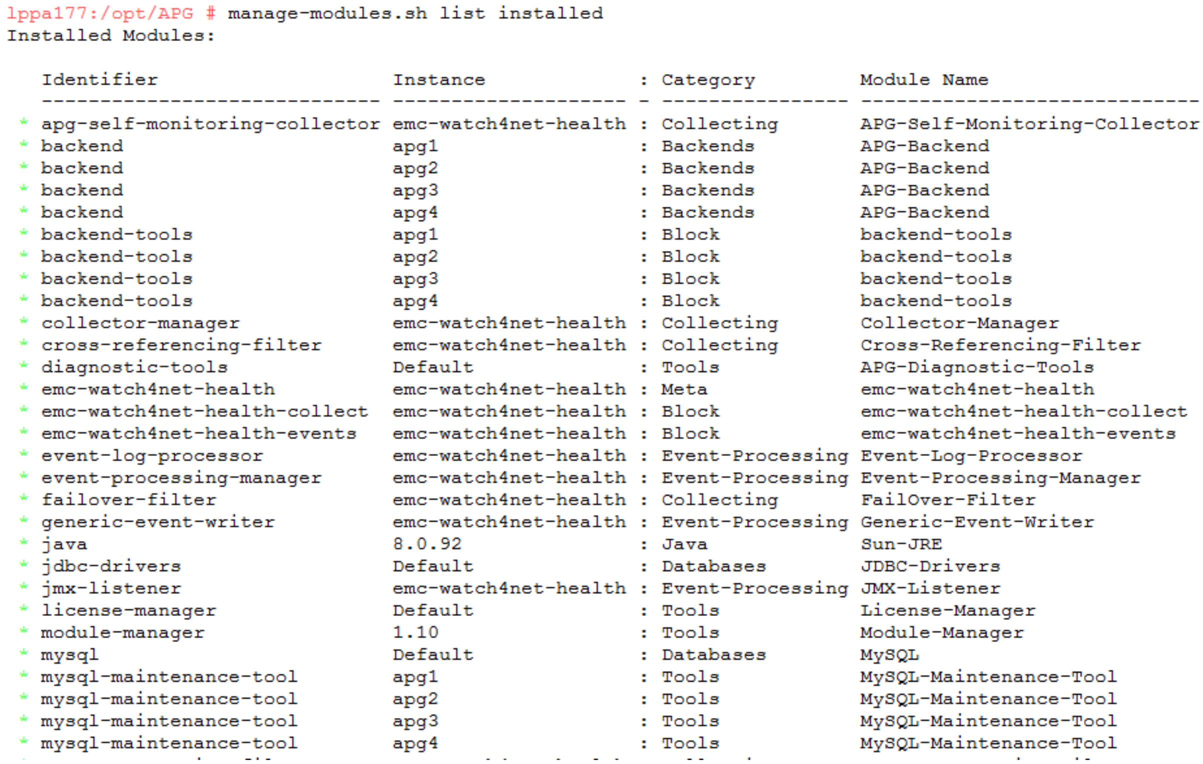
2. On each backend server, install one instance of backend-tools for each backend instance. Use the `--standalone` option to override the prerequisites.

```
/opt/APG/bin/manage-modules.sh install backend-tools apg1 --
standalone
```



```
lppa177:/opt/APG # manage-modules.sh install backend-tools apg1 --standalone
Starting installation of backend-tools v3.7.1u99 from backend-tools-3.7.1u99...
 * Gathering information...
 * 'backend-tools v3.7.1u99' will be registered with instance name 'apg1'.
 * It will be installed in '/opt/APG/Block/backend-tools/apg1'.
 * Unpacking files...
 * Installing files... 100%
 * 9 files have been installed.
 * Finalizing installation...
   [1] MySQL
 ? Backend database type [1] >
 ? Backend database hostname or IP address [localhost] >
 ? Backend database port number [53306] >
 ? Backend database name [apg] > apg1
 ? Backend database username [apg] >
 ? Backend database password [?????] >
 ? Backend database password (root user) [?????] >
 ? Socket collector port [2000] > 2100
 ? Telnet control interface port [2001] > 2101
 ? tmp directory location [tmp] >
 ? Raw data span time (group) (days) [31] >
 ? Hourly Span time (group) (days) [61] >
 ? Daily Span time (group) (days) [365] >
 ? Weekly Span time (group) (days) [2555] >
 ? Variable removal idle timeout (group) (days) [365] >
 ? Raw data span time (conf) (days) [8] >
 ? Hourly Span time (conf) (days) [0] >
 ? Daily Span time (conf) (days) [0] >
 ? Weekly Span time (conf) (days) [0] >
 ? Variable removal idle timeout (conf) (days) [365] >
 * Stopping 'backend apg1'...                                       [ OK ]
 ? Do you want to start the installed services now? (yes/no) [y] > y
 * Updating service 'backend apg1'...                          [ updated ]
 * Starting 'backend apg1'...                                       [ OK ]
Installation complete.
```

3. Verify the installed backend modules.



```
lppa177:/opt/APG # manage-modules.sh list installed
Installed Modules:

  Identifier                    Instance             : Category         Module Name
  ----------------------------- -------------------- - ---------------- -----------------------------
* apg-self-monitoring-collector emc-watch4net-health : Collecting       APG-Self-Monitoring-Collector
* backend                       apg1                 : Backends         APG-Backend
* backend                       apg2                 : Backends         APG-Backend
* backend                       apg3                 : Backends         APG-Backend
* backend                       apg4                 : Backends         APG-Backend
* backend-tools                 apg1                 : Block            backend-tools
* backend-tools                 apg2                 : Block            backend-tools
* backend-tools                 apg3                 : Block            backend-tools
* backend-tools                 apg4                 : Block            backend-tools
* collector-manager             emc-watch4net-health : Collecting       Collector-Manager
* cross-referencing-filter      emc-watch4net-health : Collecting       Cross-Referencing-Filter
* diagnostic-tools              Default              : Tools            APG-Diagnostic-Tools
* emc-watch4net-health          emc-watch4net-health : Meta             emc-watch4net-health
* emc-watch4net-health-collect  emc-watch4net-health : Block            emc-watch4net-health-collect
* emc-watch4net-health-events   emc-watch4net-health : Block            emc-watch4net-health-events
* event-log-processor           emc-watch4net-health : Event-Processing Event-Log-Processor
* event-processing-manager      emc-watch4net-health : Event-Processing Event-Processing-Manager
* failover-filter               emc-watch4net-health : Collecting       FailOver-Filter
* generic-event-writer          emc-watch4net-health : Event-Processing Generic-Event-Writer
* java                          8.0.92               : Java             Sun-JRE
* jdbc-drivers                  Default              : Databases        JDBC-Drivers
* jmx-listener                  emc-watch4net-health : Event-Processing JMX-Listener
* license-manager               Default              : Tools            License-Manager
* module-manager                1.10                 : Tools            Module-Manager
* mysql                         Default              : Databases        MySQL
* mysql-maintenance-tool        apg1                 : Tools            MySQL-Maintenance-Tool
* mysql-maintenance-tool        apg2                 : Tools            MySQL-Maintenance-Tool
* mysql-maintenance-tool        apg3                 : Tools            MySQL-Maintenance-Tool
* mysql-maintenance-tool        apg4                 : Tools            MySQL-Maintenance-Tool
```

Using the backend-tools

The backend-tools provide two new user interfaces in Centralized Management.

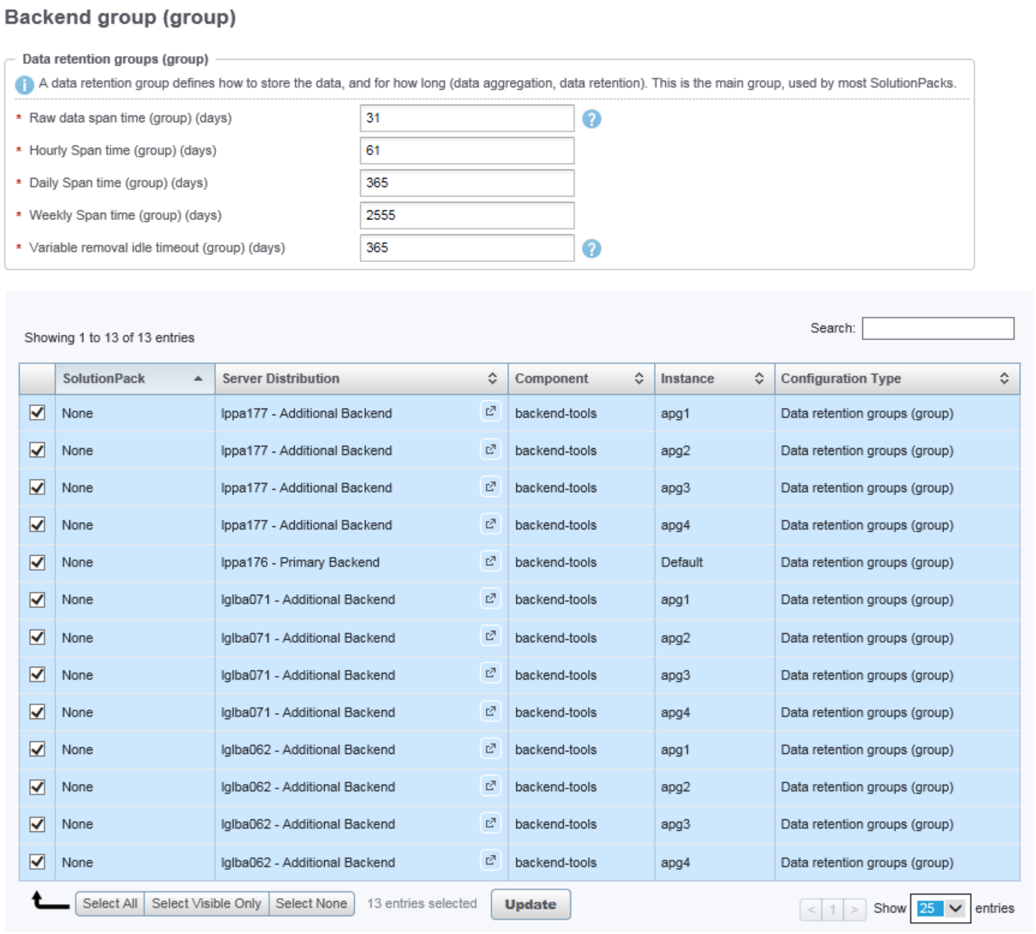
Selecting each backend group shows the raw data span time for each group. Each data retention group can be changed in the **Data retention groups** table and then applied to all the backend servers.

Note

Any change to retention settings could increase the size of the databases which could require the size of the filesystem to increase.

Procedure

1. Navigate to **Centralized Management** > **Central Configuration Repository** > **Backend group (conf)** or **Centralized Management** > **Central Configuration Repository** > **Backend group (group)**.
2. Select a backend group to view the raw data span time for that group.
3. Update the data retention settings.
4. Select the backends where you want to apply the data retention changes.
5. Click **Update**.



Backend group (group)

Data retention groups (group)

A data retention group defines how to store the data, and for how long (data aggregation, data retention). This is the main group, used by most SolutionPacks.

* Raw data span time (group) (days)	31
* Hourly Span time (group) (days)	61
* Daily Span time (group) (days)	365
* Weekly Span time (group) (days)	2555
* Variable removal idle timeout (group) (days)	365

Showing 1 to 13 of 13 entries

Search:

	SolutionPack	Server Distribution	Component	Instance	Configuration Type
☑	None	lppa177 - Additional Backend	backend-tools	apg1	Data retention groups (group)
☑	None	lppa177 - Additional Backend	backend-tools	apg2	Data retention groups (group)
☑	None	lppa177 - Additional Backend	backend-tools	apg3	Data retention groups (group)
☑	None	lppa177 - Additional Backend	backend-tools	apg4	Data retention groups (group)
☑	None	lppa176 - Primary Backend	backend-tools	Default	Data retention groups (group)
☑	None	lglba071 - Additional Backend	backend-tools	apg1	Data retention groups (group)
☑	None	lglba071 - Additional Backend	backend-tools	apg2	Data retention groups (group)
☑	None	lglba071 - Additional Backend	backend-tools	apg3	Data retention groups (group)
☑	None	lglba071 - Additional Backend	backend-tools	apg4	Data retention groups (group)
☑	None	lglba062 - Additional Backend	backend-tools	apg1	Data retention groups (group)
☑	None	lglba062 - Additional Backend	backend-tools	apg2	Data retention groups (group)
☑	None	lglba062 - Additional Backend	backend-tools	apg3	Data retention groups (group)
☑	None	lglba062 - Additional Backend	backend-tools	apg4	Data retention groups (group)

13 entries selected

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, it is recommended 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 this directory to the virus scanning exclusion list. To do this, add a configuration option for the `tmpdir` parameter to your `my.ini` configuration file.

Reviewing report customizations

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

Report customizations are maintained during the upgrade (under “My Reports”), but you will need to 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.

Validating the environment

After upgrading your system, verify the operational status.

Procedure

1. Look for blank reports and graphs.

   Determine whether blank reports are caused by collection errors. Resolve issues or document them for later follow up.

2. Verify that all tasks are completing successfully (with the possible exception of automatic updates and ESRS).
3. Validate that topology is working. Resolve any issues.

   Note

   Topology maps may temporarily contain duplicate objects after the upgrade. This duplication will resolve itself after 48 hours without any user intervention.

4. Verify or edit polling periods.

Limitations and known issues

- After the upgrade, on the **Report Library** > **Recoverpoint** > **Inventory** > **Consistency Groups** report, the Transfer Status column shows stale data until older metrics become inactive.
- If you discover more than one VPLEX cluster, and the system does not get the serialnb or device property for any of the discovered clusters, the **Report Library** > **EMC VPLEX** > **Summary** report will show a "Null" value instead of the serial number on the **Card View**. The system will correct the property serial number once the metric becomes inactive. This issue applies to any upgrade from SRM 4.0.3 or earlier to SRM 4.1.
- After you update the generic-rsc block, the CPU Utilization % for Linux Hosts may increase rapidly into the thousands. The system will start to display the correct CPU Utilization % when you update the SolutionPack for Physical Hosts. The higher CPU Utilization values will be visible in the reports for few days because the report settings show data 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 ViPR SRM frontend and run the following command: `/opt/APG/bin/manage-modules.sh service restart tomcat`
- After the upgrade, the Path Details & Storage Connectivity report for EMC Data Domain is blank.
- If you upgraded from 3.7, the Memory Utilization fields in the following EMC Data Domain reports are blank:
  - **Summary**
  - **Performance** > **List of Data Domains**
  - **Top 10**