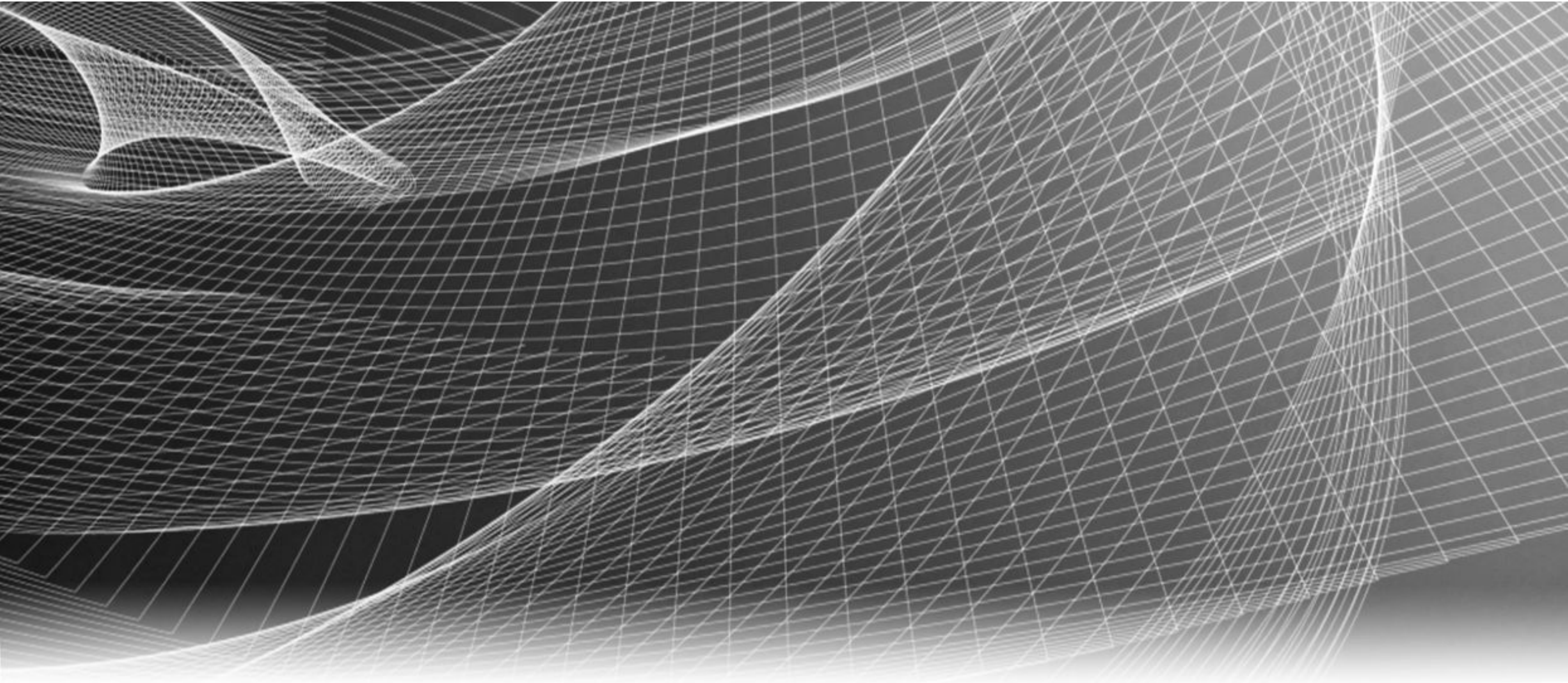


EMC® ViPR SRM

Version 3.7

Upgrading to ViPR SRM 3.7 using the System Upgrade UI

P/N 302-002-431

REV 01

Published October, 2015

EMC 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. EMC Corporation 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 EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to EMC Online Support (https://support.emc.com).

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** 5

Overview 6
Required tools 6
Required credentials 6
Verifying and documenting the current status of the environment 6
Backing up the environment 7
Saving the Java certificates file 7
Updating WinRM URL prefixes 8
Updating the Centralized Management module 8
Upgrading the system 10
Restoring the Java certificates file 13

Chapter 2 **Upgrading the SolutionPacks** 15

Upgrading all SolutionPacks and other components 16

Chapter 3 **Post-Upgrade Tasks** 19

Checking the status of remote host services 20
Reconfiguring a SolutionPack 20
Increasing the heap size for the Tomcat service 20
Chargeback Reports 21
Restoring timeout values 21
Editing new actions scripts 21
Deleting old alert definitions 22
Deleting old data from the SolutionPack for EMC Atmos 22
Checks for the SolutionPack for Physical Hosts 23
Compliance changes 23
Installing the Compliance Rules module 23
Updating the SNMP collections 24
Installing new alerting components 25
Deleting backup schedules from the DPA server 26
Virus scanning software in Windows deployments 26
Reviewing report customizations 26
Validating the environment 26

CHAPTER 1

Upgrading the System

This chapter includes the following topics:

- Overview 6
- Required tools 6
- Required credentials 6
- Verifying and documenting the current status of the environment 6
- Backing up the environment 7
- Saving the Java certificates file 7
- Updating WinRM URL prefixes 8
- Updating the Centralized Management module 8
- Upgrading the system 10
- Restoring the Java certificates file 13

Overview

This guide applies to binary-only installations of 3.6.x and mixed/vApp installations of version 3.6.4 or higher.

If you are upgrading a binary-only installation of 3.5.x, refer to *EMC VIPR SRM: Upgrading version 3.5.x to 3.7*.

If you are upgrading a vApp or mixed deployment of 3.6.3 or lower, refer to *EMC VIPR SRM: Upgrading version 3.5.x to 3.7* or *EMC ViPR SRM: Upgrading version 3.6.1, 3.6.2, or 3.6.3 to 3.7*.

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 admin 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 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 assess the success of the upgrade.

Before you begin

Refer to *Manage ViPR SRM System Health* 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 end-to-end topology is working. Resolve any issues.
4. Review the existing backend and databases. Check **Report Library** › **EMC M&R Health** › **Module Performance** › **Backends** and **Report Library** › **EMC M&R Health** › **Module Performance** › **Databases**.
   - Check backend thresholds to verify that you have room to accommodate new sizing
   - Add additional backends and databases as required.
   - Refer to the *Watch4net Database Split* v1.2 document for help if you need to manually move data to redistribute the metrics.
5. Review and document any customizations.

   For example:

   - Polling intervals
   - Timeout values

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.

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 NetBackup*
- *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.

Saving the Java certificates file

The certificates file provided with the Java installation is overwritten during the upgrade. If you deployed LDAP over SSL and have certificates stored in this file (such as for an

LDAP server configuration), save the certificates file before the upgrade, and restore the file after the upgrade.

Procedure

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 because it will be deleted and replaced by the new installation.)

   For example, `cp cacerts /var/tmp/cacerts`.

After you finish

If the certificate is lost and you set up LDAP over SSL as a custom solution, then you will need to follow the same custom steps to set it up again.

Updating WinRM URL prefixes

Prior to ViPR SRM version 3.7, if you discovered Windows hosts using Custom WinRM URL prefixes, you had to add the custom URL prefix to module.properties of Generic-RSC Collector Manager. After upgrading to 3.7, these changes are no longer applicable.

Procedure

1. To resolve this issue, enter the custom WinRM URL prefix along with the host credentials.

Updating the Centralized Management module

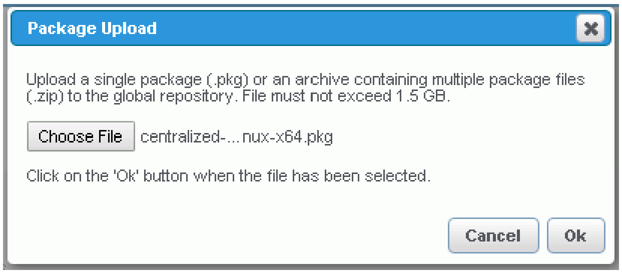
To get the new System Upgrade interface in Centralized Management to upgrade all of the servers from a single UI, you must update the Centralized Management module to the latest version.

Procedure

1. Download the Centralized Management package from support.emc.com.

Option	Description
Linux	`centralized-management-2.5u1-linux-x64.pkg`
Windows	`centralized-management-2.5u1-windows-x64.pkg`

2. From Centralized Management, click **Packages Management** on the left-hand pane.
3. On the **Packages Listing** page, click the **Upload** button.
4. Click **Browse**, and select the Centralized Management package file.
5. Click **OK**.



Upload a single package (.pkg) or an archive containing multiple package files (.zip) to the global repository. File must not exceed 1.5 GB.

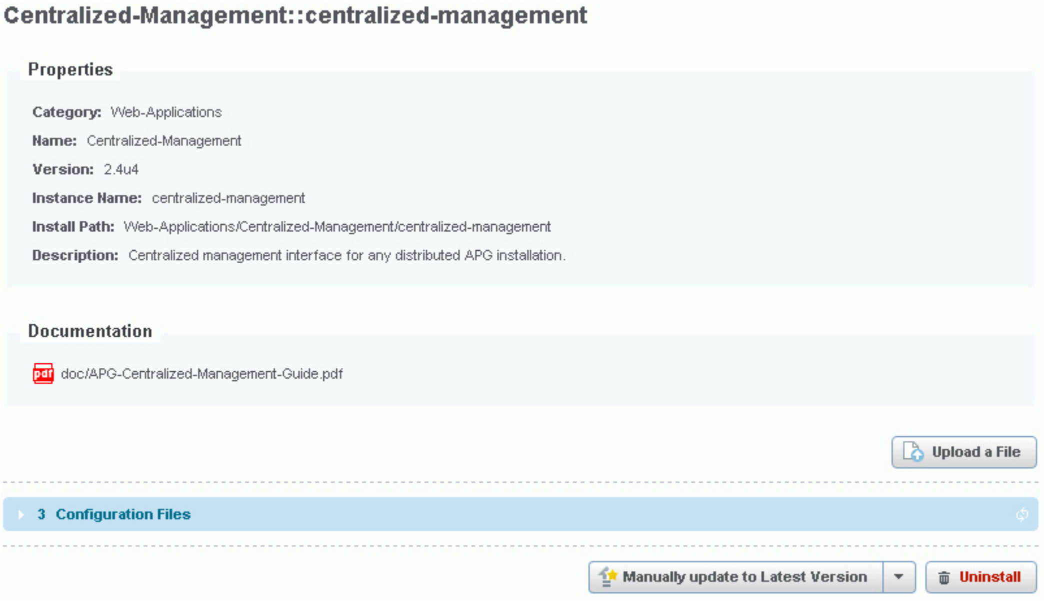
centralized-...nux-x64.pkg

Click on the 'Ok' button when the file has been selected.

6. **Click Continue.**

   The package is uploaded to the server.

7. On the left-hand pane, navigate to **Physical Overview** › **Front End** › **Modules** › **Web-Applications** › **Centralized Management**.
8. Click **Manually Update to Latest Version.**



Centralized-Management::centralized-management

Properties

Category: Web-Applications

Name: Centralized-Management

Version: 2.4u4

Instance Name: centralized-management

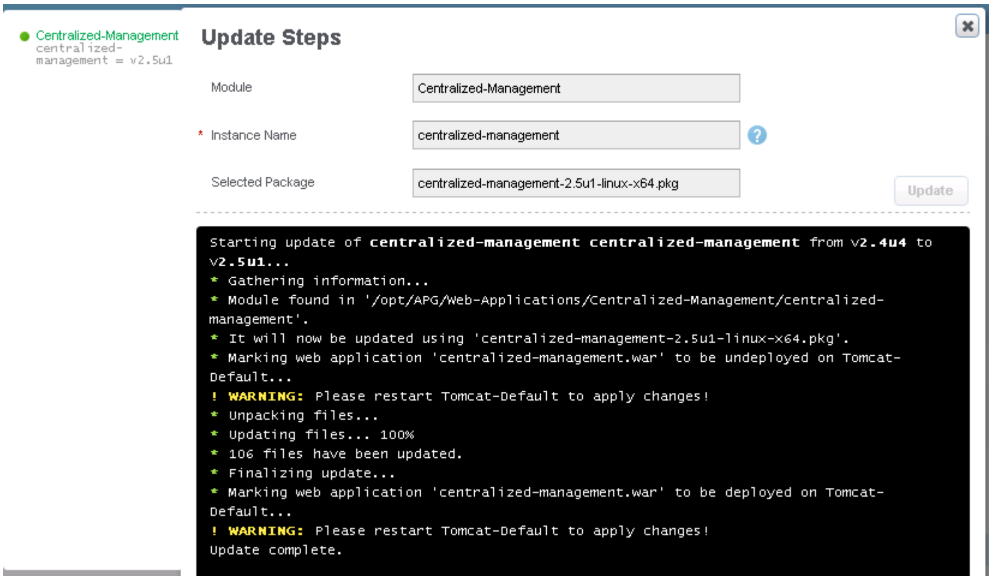
Install Path: Web-Applications/Centralized-Management/centralized-management

Description: Centralized management interface for any distributed APG installation.

Documentation

doc/APG-Centralized-Management-Guide.pdf

9. Click **Update.**



Update Steps

Module: Centralized-Management

* Instance Name: centralized-management

Selected Package: centralized-management-2.5u1-linux-x64.pkg

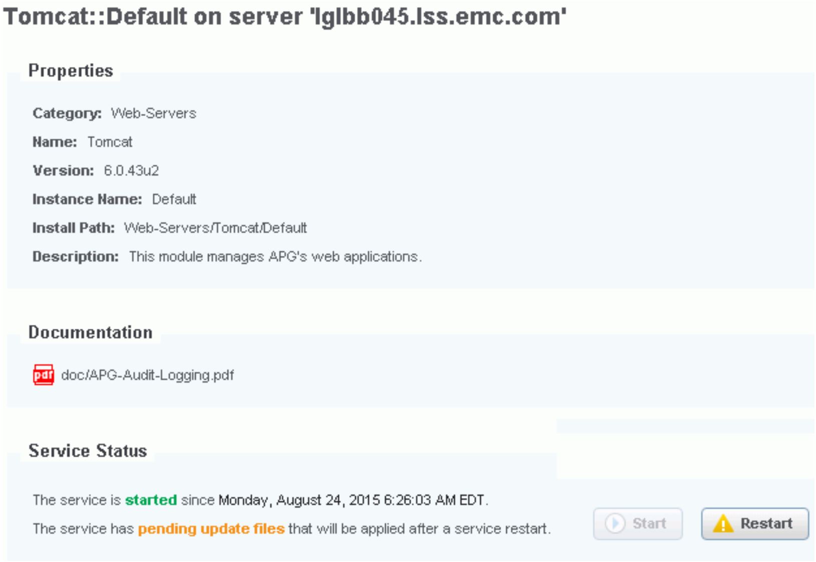
```
Starting update of centralized-management centralized-management from v2.4u4 to
v2.5u1...
* Gathering information...
* Module found in '/opt/APG/Web-Applications/Centralized-Management/centralized-
management'.
* It will now be updated using 'centralized-management-2.5u1-linux-x64.pkg'.
* Marking web application 'centralized-management.war' to be undeployed on Tomcat-
Default...
! WARNING: Please restart Tomcat-Default to apply changes!
* Unpacking files...
* Updating files... 100%
* 106 files have been updated.
* Finalizing update...
* Marking web application 'centralized-management.war' to be deployed on Tomcat-
Default...
! WARNING: Please restart Tomcat-Default to apply changes!
Update complete.
```

10. Restart the tomcat service.

    a. From Centralized Management, navigate to **Physical Overview › Front End**.

    b. On the **Services** tab, click the Tomcat module.

    c. Click **Restart**.



Tomcat::Default on server 'lglbb045.lss.emc.com'

Properties

Category: Web-Servers

Name: Tomcat

Version: 6.0.43u2

Instance Name: Default

Install Path: Web-Servers/Tomcat/Default

Description: This module manages APG's web applications.

Documentation

doc/APG-Audit-Logging.pdf

Service Status

The service is **started** since Monday, August 24, 2015 6:26:03 AM EDT.

The service has **pending update files** that will be applied after a service restart.

Upgrading the system

Learn how to upgrade the system with the System Upgrade wizard.

Before you begin

If you have enabled Online Update, the files have automatically been staged, and you can skip steps 1, 3, and 4. For information about enabling and configuring Online Update, refer to the “Online Update overview” section of the *EMC ViPR SRM Administrator’s Guide*.

Procedure

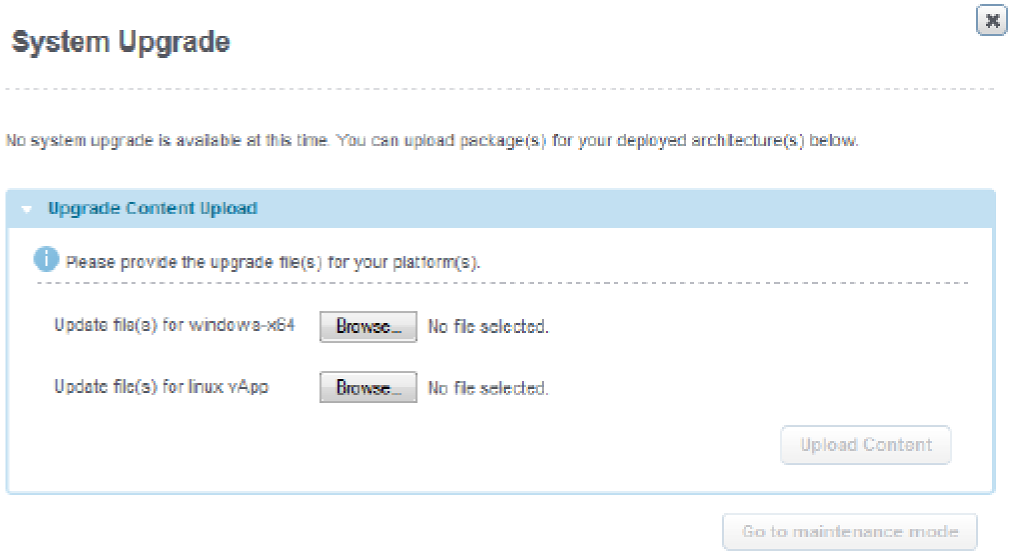
1. Download the core update file for each of your deployed architectures from support.emc.com. The vApp file also contains the appliance update file for vApp deployments.

Option	Description
Linux (vApp)	`ViPR_SRM_3.7.0.0_vApp_Update_UI.zip`
Linux (binary only)	`ViPR_SRM_3.7.0.0_Linux_64-bit_Update_File.zip`
Windows	`ViPR_SRM_3.7.0.0_Windows_64-bit_Update_File.zip`

2. 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.

3. For your Linux and/or Windows deployments, click **Browse** and select the core update file.



System Upgrade

No system upgrade is available at this time. You can upload package(s) for your deployed architecture(s) below.

Upgrade Content Upload

Please provide the upgrade file(s) for your platform(s).

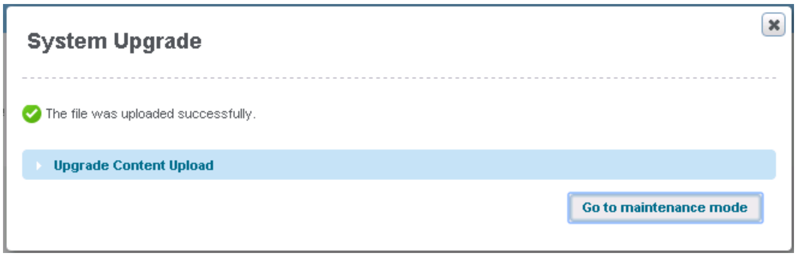
Update file(s) for windows-x64 No file selected.

Update file(s) for linux vApp No file selected.

4. Click **Upload Content.**
5. 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.

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



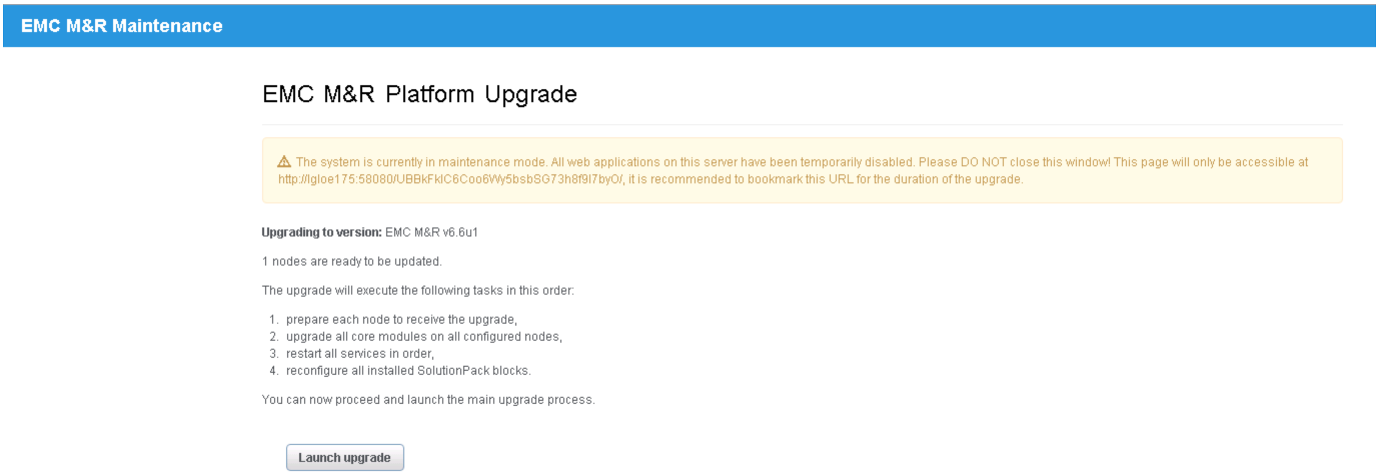
System Upgrade

The file was uploaded successfully.

Upgrade Content Upload

Maintenance mode begins, the front end becomes unavailable, and 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.

7. When the system has completed the validation checks, click **Launch upgrade**.



EMC M&R Maintenance

EMC M&R Platform Upgrade

⚠ 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://lgloe175:58080/UBBkFklC6Coo6Wy5bsbSG73h8f9l7byO/, it is recommended to bookmark this URL for the duration of the upgrade.

Upgrading to version: EMC M&R v6.6u1

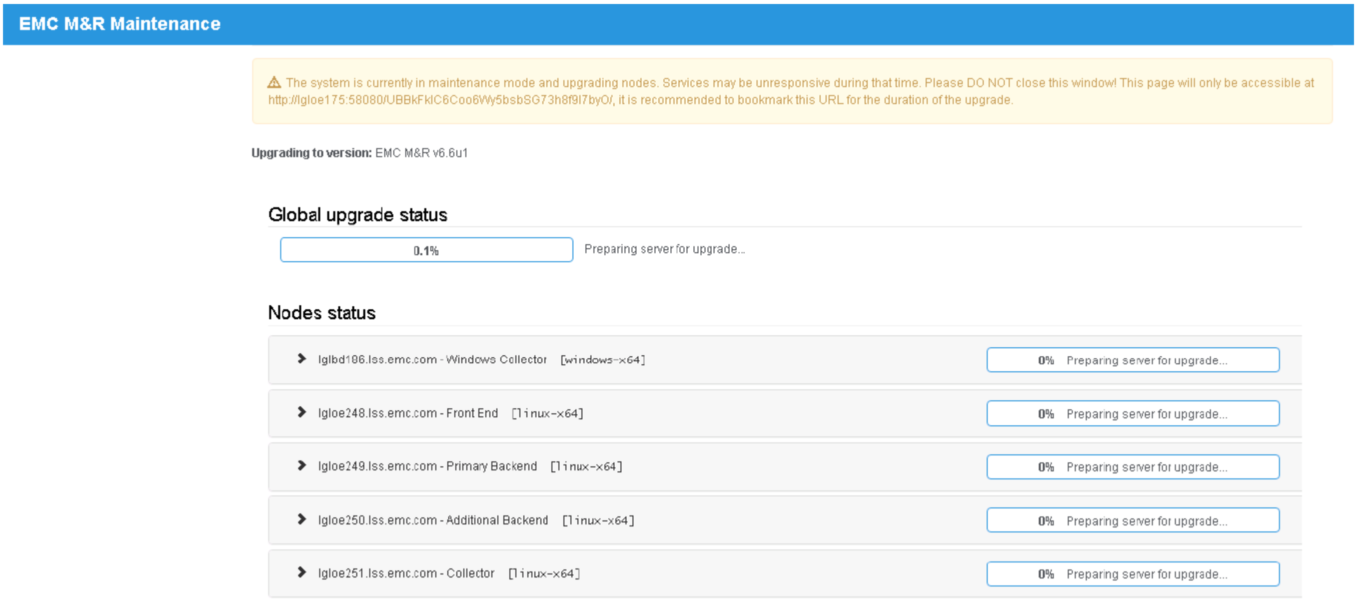
1 nodes are ready to be updated.

The upgrade 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 upgrade process.

The upgrade begins. After several minutes, the **Upgrade status** displays.



EMC M&R Maintenance

⚠ The system is currently in maintenance mode and upgrading nodes. Services may be unresponsive during that time. Please DO NOT close this window! This page will only be accessible at http://lgloe175:58080/UBBkFklC6Coo6Wy5bsbSG73h8f9l7byO/, it is recommended to bookmark this URL for the duration of the upgrade.

Upgrading to version: EMC M&R v6.6u1

Global upgrade status

0.1% Preparing server for upgrade...

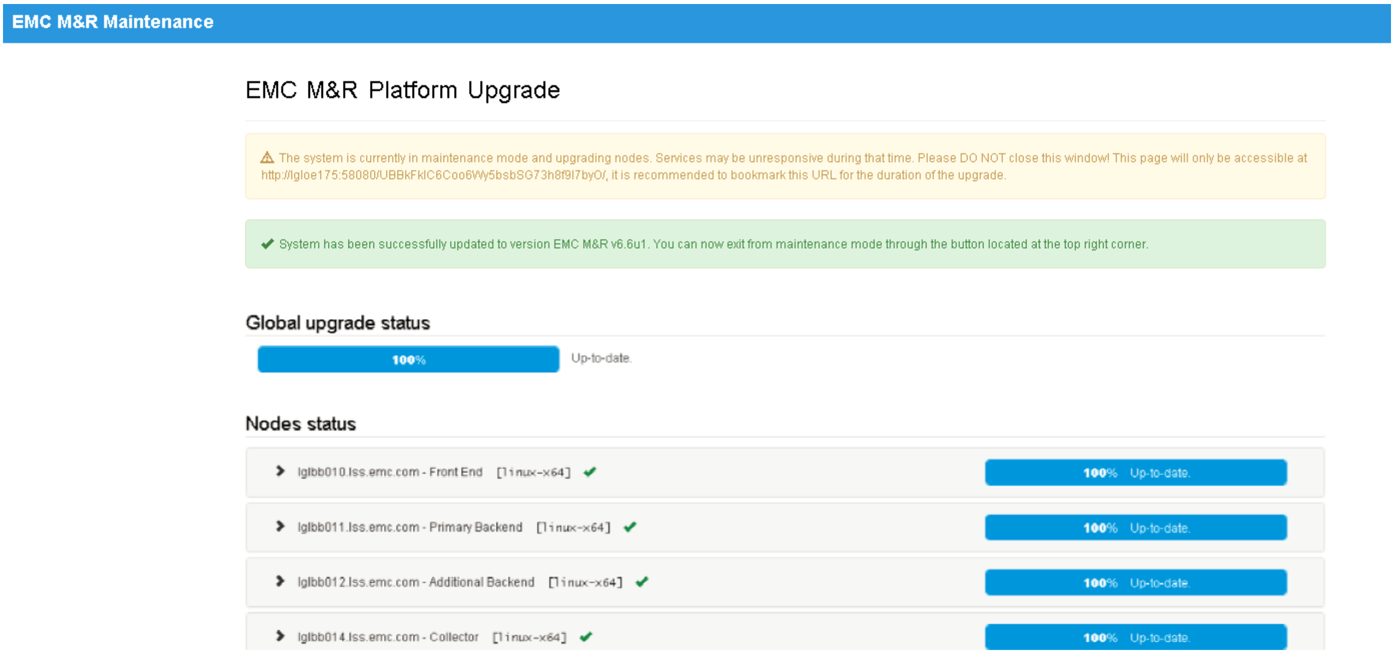
Nodes status

lglbd186.lss.emc.com - Windows Collector [windows-x64]	0% Preparing server for upgrade...
lgloe248.lss.emc.com - Front End [linux-x64]	0% Preparing server for upgrade...
lgloe249.lss.emc.com - Primary Backend [linux-x64]	0% Preparing server for upgrade...
lgloe250.lss.emc.com - Additional Backend [linux-x64]	0% Preparing server for upgrade...
lgloe251.lss.emc.com - Collector [linux-x64]	0% Preparing server for upgrade...

Note

You may need to manually refresh your browser to see the **Upgrade status** page.

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.



EMC M&R Maintenance

EMC M&R Platform Upgrade

⚠ The system is currently in maintenance mode and upgrading nodes. Services may be unresponsive during that time. Please DO NOT close this window! This page will only be accessible at http://lgloe175:58080/UBBkFklC6Coo6Wy5bsbSG73h8f9l7byO/, it is recommended to bookmark this URL for the duration of the upgrade.

✓ System has been successfully updated to version EMC M&R v6.6u1. You can now exit from maintenance mode through the button located at the top right corner.

Global upgrade status

100% Up-to-date.

Nodes status

- lglbb010.lss.emc.com - Front End [linux-x64] ✓ 100% Up-to-date.
- lglbb011.lss.emc.com - Primary Backend [linux-x64] ✓ 100% Up-to-date.
- lglbb012.lss.emc.com - Additional Backend [linux-x64] ✓ 100% Up-to-date.
- lglbb014.lss.emc.com - Collector [linux-x64] ✓ 100% Up-to-date.

8. Click **Exit**.
9. Click **OK**.

   The system restarts the front end, and it is now available to users.

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.

Restoring the Java certificates file

Restore the cacerts file that you saved before upgrading the software.

Procedure

1. Go to the directory where the upgraded version of Java was installed: `${APG INSTALL DIRECTORY}/Java/Sun-JRE/<new Java version>/lib/security`

   For example, `cd /opt/APG/Java/Sun-JRE/<new Java version>/lib/security`
2. Save the current certificates file.

   For example, `cp cacerts cacerts.bak`

3. Restore the original cacerts file containing your certificates.

   For example,
   ```
   cp /var/tmp/cacerts cacerts
   ```

4. Restart the tomcat service.

   For example,
   ```
   ${APG INSTALL DIRECTORY}/bin/manage-modules.sh
   service restart tomcat Default
   ```

CHAPTER 2

Upgrading the SolutionPacks

This chapter includes the following topics:

- Upgrading all SolutionPacks and other components 16

Upgrading all SolutionPacks and other components

You can upgrade all of your installed SolutionPacks and other components with a single click.

Before you begin

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 admin guide.

For information about load-balancing in a scaled-out deployment, refer to the *Configuring Load Balancing for ViPR SRM* article on community.emc.com.

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.

Procedure

1. From Centralized Management, click **SolutionPacks** on the left-hand pane.
2. Click the **Update All Components** button in the top-right corner of the page.

   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.

3. Click **Next**.

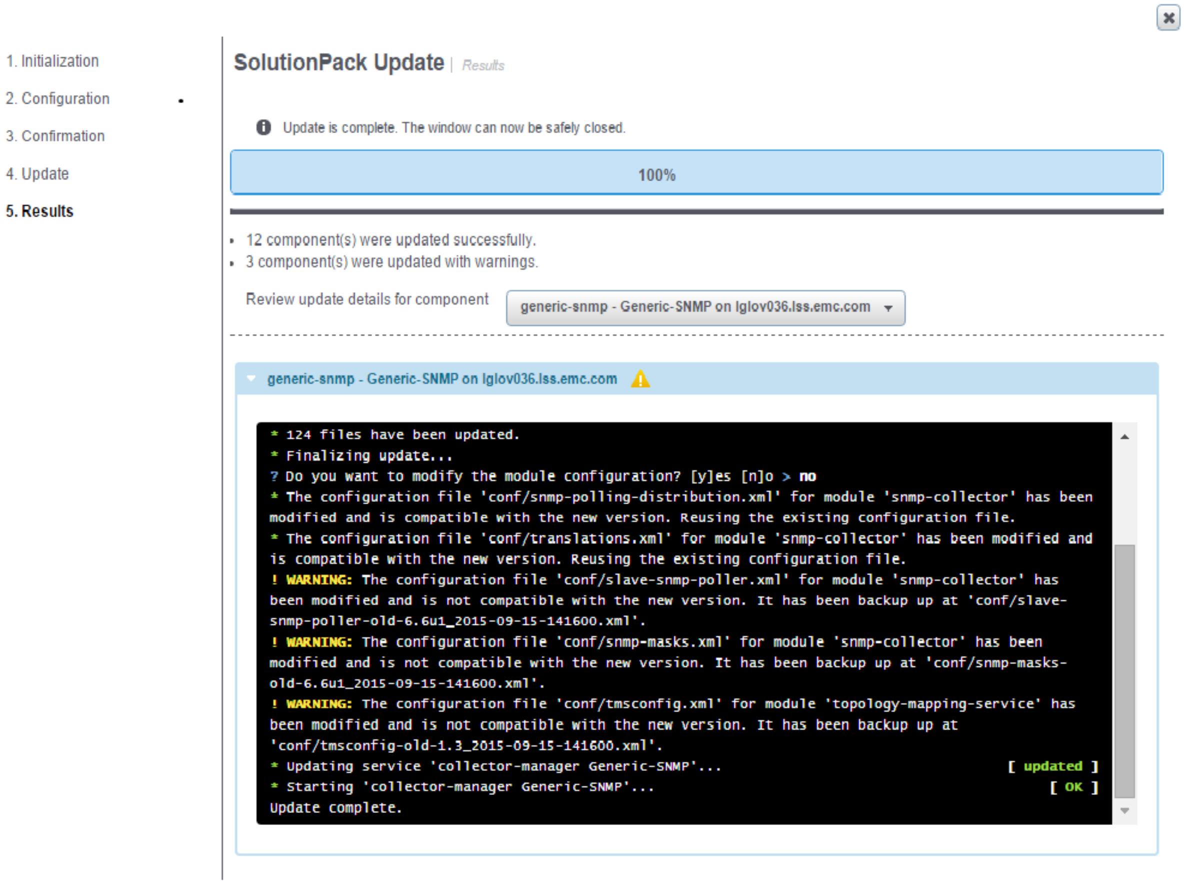
   The **Configuration** window opens. The left-hand pane lists each of the components that include new features that you need to configure. The right-hand pane displays the configuration details for the component with the new features highlighted in yellow. Carefully review the selections to make sure 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. After you have configured every component on the list, click **Next**.

4. 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**.
5. 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



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.
```

6. 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.”

CHAPTER 3

Post-Upgrade Tasks

This chapter includes the following topics:

- Checking the status of remote host services 20
- Increasing the heap size for the Tomcat service 20
- Chargeback Reports 21
- Restoring timeout values 21
- Editing new actions scripts 21
- Deleting old alert definitions 22
- Deleting old data from the SolutionPack for EMC Atmos 22
- Checks for the SolutionPack for Physical Hosts 23
- Compliance changes 23
- Installing the Compliance Rules module 23
- Updating the SNMP collections 24
- Installing new alerting components 25
- Deleting backup schedules from the DPA server 26
- Virus scanning software in Windows deployments 26
- Reviewing report customizations 26
- Validating the environment 26

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. On the **Services** tab, select **All** from the **Show entries** drop-down menu.
4. 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.

Reconfiguring a SolutionPack

Learn how to reconfigure a SolutionPack.

Procedure

1. Navigate to **Centralized Management**.
2. Click the **SolutionPacks** node on the left-hand panel to display the installed SolutionPacks.
3. Click the SolutionPack to access its SolutionPackBlocks.
4. Locate the instance that you want to reconfigure. For SolutionPackBlocks that are a component of a SolutionPack, select the SolutionPack, and then locate the instance on the **Properties** page.
5. Click the **Pencil** icon next to the SolutionPackBlock.
6. Click **Reconfigure**.

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**.
7. Log in to the frontend server.
8. Enter the following command from the bin directory of the EMC M&R platform installation:

Option	Description
Unix	`./manage-modules.sh service start tomcat Default`
Windows	`manage-modules.cmd service start tomcat Default`

Chargeback Reports

When you upgrade from a previous version to ViPR SRM 3.7, the SolutionPack for Block Chargeback is not installed by default and the old chargeback reports reference a broken link. You need to install the SolutionPack for Block Chargeback to obtain chargeback reports and resolve this link.

The reports are empty immediately after the SolutionPack is installed. They start displaying data only after the chargeback preprocessor task completes successfully and data has had sufficient time to propagate through the environment. The chargeback preprocessor task runs using the schedule selected during installation. You can also run the task manually. For instructions, see the SolutionPack for Block Chargeback chapter in the *SolutionPack Installation Guide*.

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 to find the files with values that changed:
   ```
   find / -name *old*2015* -print
   ```
2. On Windows, use Windows Explorer 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

After upgrading a multiple virtual machine setup (vApp) or performing a manual installation or upgrade of multiple servers, you must 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`

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

Deleting old alert definitions

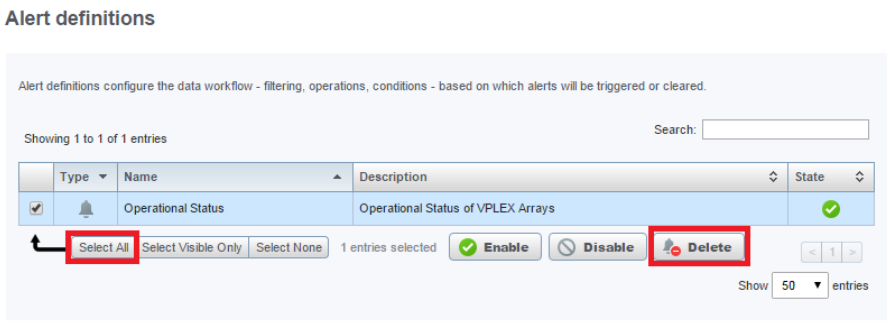
Any alert customizations completed prior to 3.7 must be re-created under the new alerts folder. After validating that customized alerts are working in the new alerts folder, the old folders can be deleted.

Procedure

1. Click **Administration** › **Modules** › **Alerting**. The **Alerting** page opens.
2. Click **Alert Definitions**.
3. Delete the alerts from the old alerts folders. The following table shows the old and new names of the alerts folders that changed.

SolutionPack Name	Old Alerts Folder Name	New Alerts Folder Name
Brocade FC Switch	Brocade FC Switch	Brocade FC Switch Alert Definitions
Cisco MDS/Nexus Switch	Cisco MDS Nexus	Cisco MDS Nexus Alert Definitions
EMC VPLEX	EMC-VPLEX	EMC VPLEX Alert Definitions
IBM SAN Volume Controller/Storwize	IBM-SVC definitions	IBM SAN Volume Controller Storwize Alert Definitions
NetApp Filer	NetApp Filer Definitions	NetApp Filer Alert Definitions
Physical Hosts	Physical Hosts	Physical Hosts Alert Definitions

4. In each alert folder, select the alerts and click **Delete**.



Alert definitions

Alert definitions configure the data workflow - filtering, operations, conditions - based on which alerts will be triggered or cleared.

Showing 1 to 1 of 1 entries

Search:

	Type	Name	Description	State
☑	🔔	Operational Status	Operational Status of VPLEX Arrays	✓

1 entries selected

Show 50 entries

5. Repeat these steps to delete all of the alerts under the old alert folders.

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. Edit the filter 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**.

Checks for the SolutionPack for Physical Hosts

After upgrading ViPR SRM to 3.7 from a version lower than 3.6, any host with uppercase "hostname" will be listed twice in Physical Host reports (both uppercase and lowercase). With default vstatus configuration, these double entries will show up in reports for 14 days, after which only lowercase entries will be seen. The "inactive" metrics generated through uppercase hostnames will remain in the database until they are cleaned up from the database.

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`.

Compliance changes

Configuration changes related to zoning, LUN masking, and mapping are disabled in version 3.7. EMC can enable these events upon request.

User-defined scopes for hosts with upper case letters in their filters will not work in version 3.7 because the scopes are case sensitive. For example, if you have defined a scope such as device="HOST011", after you upgrade to version 3.7 the scope will not work because the host name was changed to lower case (host011). If any of your scopes have devices with uppercase letters, change them to lower case letters and save the scope.

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**.

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.

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	Alert Consolidation, Pre-configured alerts
EMC Isilon	Alert Consolidation, Pre-configured alerts
EMC ScaleIO	Alert Consolidation, Pre-configured alerts
EMC ViPR	Alert Consolidation, Pre-configured alerts
EMC VPLEX	Alert Consolidation, Pre-configured alerts
Hitachi Device Manager	Alert Consolidation, Pre-configured alerts
HP 3PAR StoreServ	Alert
HP StorageWorks P9000	Alert Consolidation, Pre-configured alerts
IBM DS	Alert Consolidation, Pre-configured alerts
IBM SAN Volume Controller/Storwize	Pre-configured alerts
IBM XIV	Alert Consolidation, Pre-configured alerts

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.)

Deleting backup schedules from the DPA server

ViPR SRM 3.7 includes custom reports, so you should remove backup schedules from the DPA server after the upgrade.

Procedure

1. Log in to the DPA server.
2. Navigate to **Reports** › **Schedule Reports**.
3. Delete W4N-Avamar Reports.
4. Delete W4N-Netbackup Reports.
5. Restart the DPA Collector in ViPR SRM.

   All of the backup technology reports are created automatically.

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.

Engage EMC Support if you need assistance to help resolve any observed issues subsequent to the upgrade.

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. Look for broken links. Resolve issues or document them for later follow up.
3. Verify that all tasks are completing successfully (with the possible exception of automatic updates and ESRS).

4. Validate that End-to-End 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.

5. Verify or edit polling periods.