EMC® ViPR SRM

Version 4.0.1

Upgrading version 3.6.1, 3.6.2, or 3.6.3 to 4.0.1

P/N 302-003-314

REV 04

EMC²

Published November 2016

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 8
Checks for the SolutionPack for Physical Hosts 8
Deleting backup schedules and scheduled reports from the DPA server 9
Prepare for the upgrade 9
- Updating Linux components for vApp VMs 9
- Staging components on vApp VMs 10
- Staging components on non-vApp Linux servers 11
- Staging components on Windows servers 12
- Staging components in mixed deployments 12

Upgrade core modules 12
- Upgrading the core modules on Linux servers 12
- Upgrading the core modules on Windows 13

Rebooting the vApp 14
Restoring the Java certificates file 15

Chapter 2 Upgrading the SolutionPacks 17

Upgrading all SolutionPacks and other components 18

Chapter 3 Post-Upgrade Tasks 23

Checking the status of remote host services 24
Increasing the heap size for the Tomcat service 24
Fixing broken links 24
Chargeback Reports 25
Restoring timeout values 26
Editing new actions scripts 26
Deleting old alert definitions 26
Deleting old data from the SolutionPack for EMC Atmos 27
Compliance changes 28
Installing the Compliance Rules module 28
Cisco MDS/Nexus switch discovery 28
- Exporting Cisco MDS/Nexus switches 29
- Installing the SNMP Data Collector 29
- Importing switch details into Discovery Center 30
- Deleting switches from SNMP Device Discovery 31

Updating the SNMP collections 31
Installing new alerting components 32
Deleting report templates and times from the DPA server 33
Creating an events database for the SolutionPack for DPA 33
Backend-tools 35
- Installing the backend-tools 36
- Using the backend-tools 39

Virus scanning software in Windows deployments 40
Reviewing report customizations 40

Validating the environment..... 40
Reinstalling the SolutionPack for EMC Isilon pre-configured alerts..... 40
Limitations and known issues..... 41

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 8
- Checks for the SolutionPack for Physical Hosts 8
- Deleting backup schedules and scheduled reports from the DPA server 9
- Prepare for the upgrade 9
- Upgrade core modules 12
- Rebooting the vApp 14
- Restoring the Java certificates file 15

Overview

This guide describes the process for upgrading an existing 3.6.1, 3.6.2, or 3.6.3 installation. These instructions apply to vApp installations and mixed environments.

If you are upgrading from 3.6.4 or higher, or you are upgrading a binary-only deployment, refer to *Upgrading to ViPR SRM 4.0 using the System Upgrade UI*.

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 *EMC ViPR SRM Administrator's 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's 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.

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.

Saving the Java certificates file

The certificates file provided with the Java installation is overwritten during the upgrade. If you have custom certificates stored in this file (such as for an LDAP server configuration), those certificates will also be overwritten. Starting in version 3.7, ViPR SRM provided a new means for importing those certificates so they are not lost during the upgrade.

If you have previously imported your LDAP SSL certificates, EMC recommends that you allow the upgrade to overwrite the certificates. Once this is done, you can import the certificates again using the new method (described in the "Enabling LDAP over SSL" section of the EMC M&R Platform Security Guide, which is available from the SRM 4.0 Documentation Index). The new method not only survives upgrades, but also improves overall security as any changes to the default trust store that ships with Java will be reflected in your environment.

If you are unable to import the certificates using this new method, you may manually migrate the certificates, but you will not gain the benefits of the new procedure. To manually migrate the certificates, you must 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`.

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

Prepare for the upgrade

Prepare your environment for the upgrade by staging all of the updated modules in Module Manager. If your deployment is a vApp installation, this process also upgrades all of the operating system software that is managed by EMC.

Updating Linux components for vApp VMs

If you have enabled Online Update for your system, the automatic update process has already downloaded and distributed the modules to each VM, and you can skip steps 1

through 5. 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. 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 <Version Number) vApp Update for <Version Number>** file.
4. Validate that the checksum matches by clicking the “Checksum” link on the download page, and then using a local utility such as md5sum to generate the checksum.
5. Using a tool such as SCP, upload the `ViPR_SRM_<version_number>_vApp_Update.zip` file to a temporary directory on every ViPR SRM VM in the system (in any order).
6. Log in to each VM host as root.
7. Extract the ZIP file:

```
#unzip ViPR_SRM_<version_number>_vApp_Update.zip
```

8. Navigate to the `applianceUpdate` directory in the folder where you extracted the ZIP file.
9. Run the applianceUpdate script:

```
./applianceUpdate
```

Note

You can install simultaneously on multiple VMs by using tools like putty-nd, which allows you to run the same command on multiple window sessions.

Note

On the hosts, a firewall modification takes place. This modification may result in error messages after the modified firewall is reloaded but before the upgrade script completes. These error messages (such as `FATAL: Could not load /lib/modules/3.0.101-0.35-default/modules.dep: No such file or directory` and other errors related to iptables) can safely be ignored

Staging components on vApp VMs

Stage the ViPR SRM components on all of the VMs deployed using the vApp installer.

Procedure

1. Log in as root to each vApp VM.

2. Navigate to the `/usr/APG_Source` directory and run the post install script:

```
./post_install.sh
```

3. Answer the questions as directed. For example, accept the EULA and use the defaults for the installation directory and the package installation.

Results

The new packages are installed in the `/opt/APG/Tools/Module-Repository` directory.

After you finish

If you have an installation without any other Linux or Windows servers, your system is now prepared for update, and you can skip to Upgrade core modules. If you have any additional Linux servers deployed using the 1 VM vApp, run the steps above on each of the deployments.

If you have any non-vApp Linux deployments included in your environment, locate each system and perform the steps described in Staging components on non-Vapp Linux servers.

If you have any Windows deployments included in your environment, locate each system and perform the steps described in Staging components on Windows servers.

Staging components on non-vApp Linux servers

If you have enabled Online Update for your system, the automatic update process has already downloaded and distributed the modules to each server, and you can skip this section. 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. 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 <Version Number> Linux Deployment** file.
4. Using a tool such as SCP, upload the file to a temporary directory on every server that you plan to upgrade.
5. Log in to the server as root.
6. Navigate to the temporary directory and make the setup script executable:

```
chmod +x ViPR_SRM_<version_number>_Linux_x86_64.sh
```

7. Run the setup script:

```
./ViPR_SRM_<version_number>_Linux_x86_64.sh
```

8. Answers the questions as directed. For example, accept the EULA and use the defaults for the installation directory and the package installation.

Staging components on Windows servers

If you have enabled Online Update for your system, the automatic update process has already downloaded and distributed the modules to each server, and you can skip this section. 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. 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 <Version Number> Windows Deployment** file.
4. Place the file in a temporary location on every server.
5. Double-click the setup executable.
6. Click **Next**.
7. Read and accept the End User License Agreement. Click **I Agree**.
8. Press Enter to accept the default installation directory of `C:\Program Files\APG`, or specify a different location.
9. Click **OK** to install the new packages in the `C:\Program Files\APG\Tools\Module-Repository` directory.

Staging components in mixed deployments

Procedure

1. To update a mixed operating system deployment (non-vApp Linux and Windows), you must perform the steps for single operating system deployments separately on each platform on all servers. For example, a Linux deployment with one Windows collector would require following the non-vApp Linux steps for the machine hosting Centralized Management and the Windows steps for the Windows collector.

Upgrade core modules

Update the core modules on all of the ViPR SRM servers. These modules must be updated prior to any others, and they must be updated from the command line using the launch-update script.

Upgrading the core modules on Linux servers

Run the launch-update script on all of the Linux servers (in any order).

Procedure

1. The launch-update script is delivered through the module-manager, so update the module-manager module by typing the following command from the `/opt/APG/bin` directory:

```
./manage-modules.sh update module-manager
```

2. Navigate to the `/opt/APG/Tools/Module-Manager/<version>/bin` directory.
3. Launch the script from `/opt/APG/Tools/Module-Manager/<version>/bin`:

```
./launch-update.sh
```

You can run this script on multiple servers at the same time.

On the frontend server, you will see a message about frontend search being deleted. EMC recommends that you select "yes."

4. At the prompt, review the SolutionPacks that will be reconfigured.
5. At the `proceed?` prompt, hit Enter. The script starts updating modules. Let the script run uninterrupted.

Once completed, the script lists which modules and SolutionPacks were updated and reconfigured successfully. All modules except some block type modules are updated at this point. The remaining block type modules are updated later through the UI.

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.

Upgrading the core modules on Windows

Run the launch-update script on all of the Windows servers (in any order).

Procedure

1. Stop all of the services by typing the following command from the `C:\Program Files\APG\bin` directory:

```
manage-modules.cmd service stop all
```

2. Use Windows Task Manager to verify that all of the APG services have stopped. Manually stop any services that are stuck in the "Stopping" state for more than a few minutes.
3. The launch-update script is delivered through the module-manager, so update the module-manager module by typing the following command from the `C:\Program Files\APG\bin` directory:

```
manage-modules.cmd update module-manager
```

4. Launch the script from C:\Program Files\APG\Tools\Module-Manager\1.9\bin

```
launch-update.cmd
```

5. At the prompt, review the modules that will be updated and the SolutionPacks that will be reconfigured.
6. At the `proceed?` prompt, hit Enter. The script starts updating modules. Let the script run uninterrupted.

   Once completed, the script lists which modules and SolutionPacks were updated and reconfigured successfully. All modules except some block type modules are updated at this point. The remaining block type modules are updated later through the UI.
7. To review the list of installed modules and their update status, run the following command:

   ```
   manage-modules.cmd list installed
   ```

   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.
8. After the launch-update script runs, the Windows collector indicates successful update of the Java module, but the older 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>'
   ```

Rebooting the vApp

For vApp deployments, the upgrade includes a Linux kernal update that requires a reboot at this point.

Procedure

1. Power off the VMs through the vCenter using the Power Off the vApp folder.
2. Power the VMs back on through the vCenter by using the Power On the vApp folder.
3. To reboot a VM that is not in the vApp folder (such as a deployment of a 1 VM vApp), enter the following command:

   ```
   shutdown –r now
   ```

   In complex configurations, manually reboot the hosts in the following order:

   a. All additional backends

   b. Primary backend

c. Frontend

d. All collectors

Restoring the Java certificates file

If you have previously saved the certificates file, you now have two choices.

You may either restore the file manually, or follow the directions in the "Importing custom certificates into the JRE" section of the *EMC M&R Security Configuration Guide*, which is available from the SRM 4.0 Documentation Index. This allows you to import the certificates using the mechanism introduced in 3.7. EMC recommends this, but if you are unable to follow that procedure, you may restore the certificates file using the following steps.

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 18

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.

Procedure

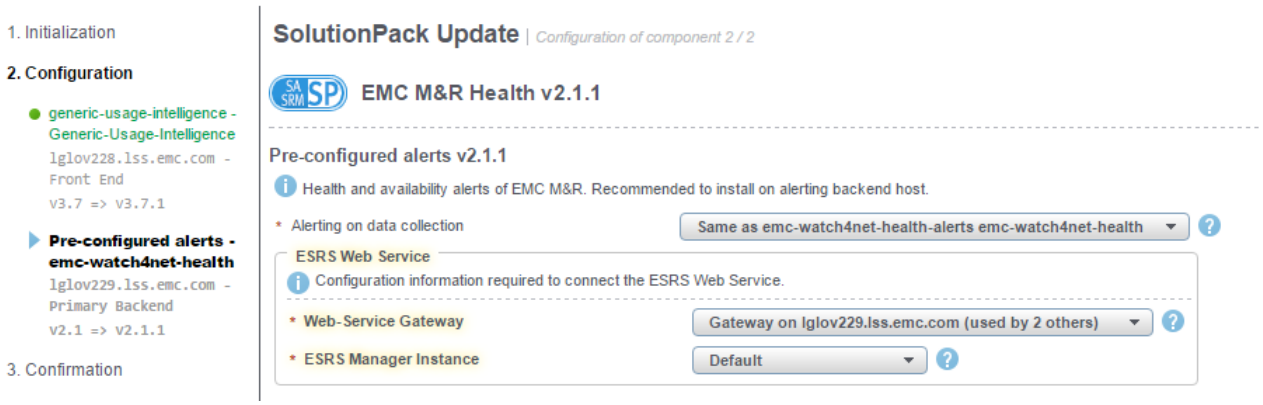
1. From Centralized Management, click **SolutionPacks** on the left-hand pane.
2. Click the **Update All Components** button in the top-right corner of the page.

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

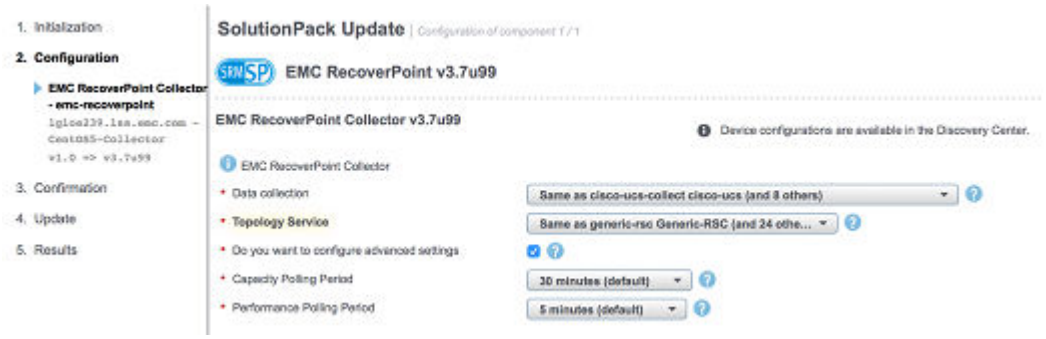
   - Number of components from SolutionPacks that will be updated to the latest version.
   - Number of components that contain new features that require configuration.

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. You must edit some SolutionPack entries while reviewing the configuration:

   - For the SolutionPack for EMC M&R Health, select the Front End hostname for the Web-Service Gateway.



   - For the SolutionPack for EMC RecoverPoint, select an existing topology service or add a new one.

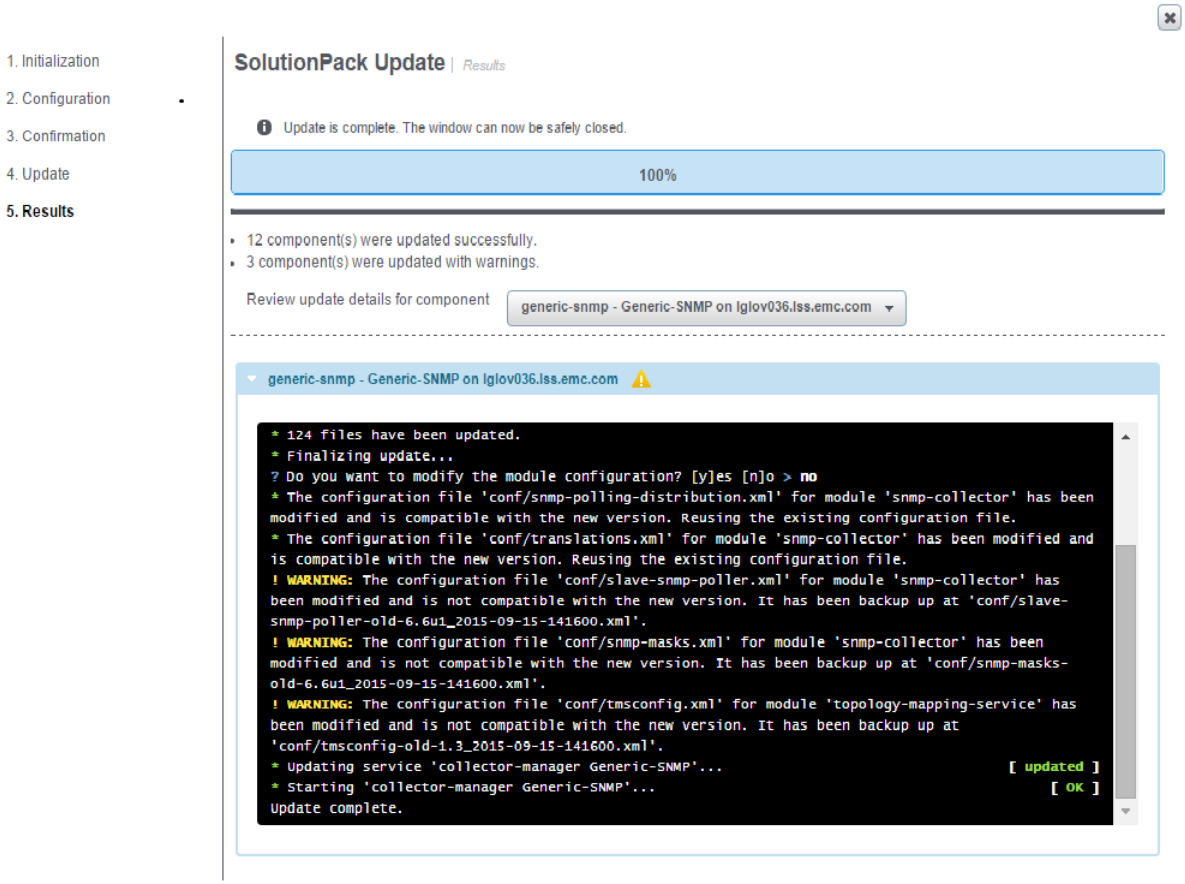


4. The **Confirmation** window opens and lists all of the components that will be updated. Confirm that all of the components are correctly listed, and then click **Update**.
5. The **Update** window opens and displays the progress of each update and the percentage complete of the overall update. Do 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
- vnxalerts-block-deviceid-<ID>-laststarttime.xml
- vnxalerts-file-deviceid-<ID>-laststarttime.xml



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."
7. 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.

8. 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`

9. 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 24
- Increasing the heap size for the Tomcat service 24
- Fixing broken links 24
- Chargeback Reports 25
- Restoring timeout values 26
- Editing new actions scripts 26
- Deleting old alert definitions 26
- Deleting old data from the SolutionPack for EMC Atmos 27
- Compliance changes 28
- Installing the Compliance Rules module 28
- Cisco MDS/Nexus switch discovery 28
- Updating the SNMP collections 31
- Installing new alerting components 32
- Deleting report templates and times from the DPA server 33
- Creating an events database for the SolutionPack for DPA 33
- Backend-tools 35
- Virus scanning software in Windows deployments 40
- Reviewing report customizations 40
- Validating the environment 40
- Reinstalling the SolutionPack for EMC Isilon pre-configured alerts 40
- Limitations and known issues 41

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.

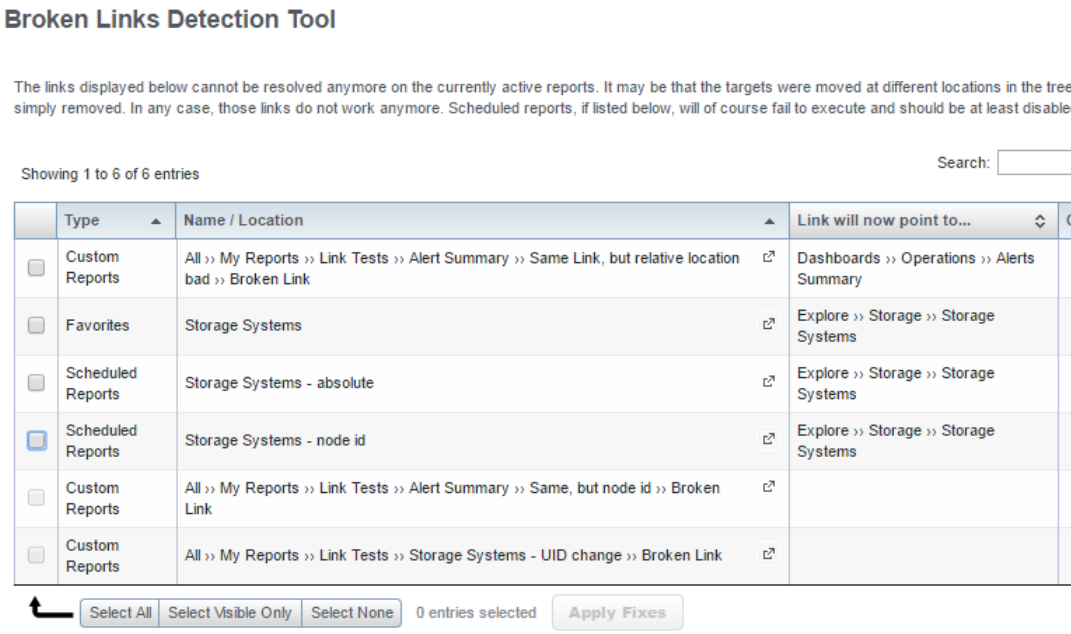
The following types of links are potentially affected:

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

Procedure

1. Click the **Settings** button.
2. Click the **Custom Reports** tab.
3. Click **Open Tool**.

   The system displays a potential match for each 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.

Chargeback Reports

SolutionPack for Block Chargeback is not installed by default and the old chargeback reports reference a broken link. If you are upgrading from 3.6.x, you need to install the SolutionPack for Block Chargeback to obtain chargeback reports and resolve this link. If you are upgrading from 3.7.x and you already installed the SolutionPack, you can skip this step.

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 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`

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.

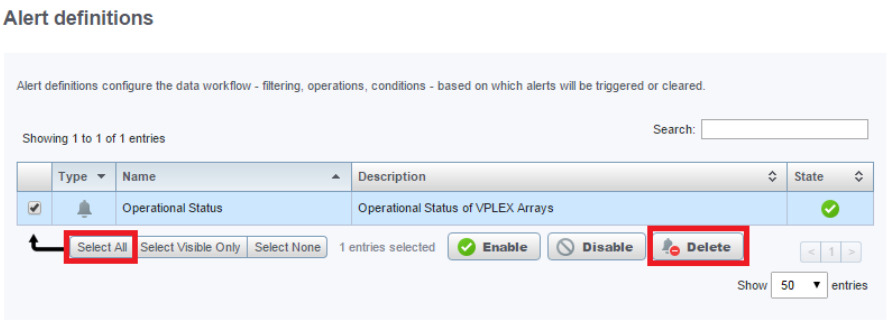
Procedure

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 Isilon	EMC Isilon	EMC Isilon Alert Definitions
EMC ViPR Controller	EMC ViPR	EMC ViPR Alert Definitions

SolutionPack Name	Old Alerts Folder Name	New Alerts Folder Name
EMC VMAX	EMC VMAX Definitions	EMC VMAX Alert Definitions
EMC VNX	EMC VNX	EMC VNX Alert Definitions
EMC VPLEX	EMC-VPLEX	EMC VPLEX Alert Definitions
EMC XtremIO	EMC XtremIO Definitions	EMC XtremIO Alert Group Definitions
Hitachi Device Manager	Hitachi Device Manager	Hitachi Device Manager Alert Definitions
HP 3PAR StoreServ	HP 3PAR definitions	HP 3PAR Alert Definitions
HP StorageWorks P9000	HP StorageWorks P9000	HP StorageWorks P9000 Alert Definitions
IBM SAN Volume Controller/Storwize	IBM-SVC definitions	IBM SAN Volume Controller Storwize Alert Definitions
IBM XIV	IBM XIV Definitions	IBM XIV Alert Definitions
NetApp Filer	NetApp Filer Definitions	NetApp Filer Alert Definitions
Physical Hosts	Physical Hosts Definitions	Physical Hosts Alert Definitions
VMware vCenter	VMware vCenter definitions	VMware vCenter Alert Definitions

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



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**.

Compliance changes

Configuration changes related to zoning, LUN masking, and mapping are disabled in version 3.7 and higher. 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 and higher because the scopes are case sensitive. For example, if you have defined a scope such as device="HOST011", after you upgrade, 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**.

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 4.0.1 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 4.0.1 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 **Devices 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 Devices** 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 devices**.
16. Click the **Collected Devices** tab, click **Save**, and then click **Accept**.

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 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	Pre-configured alerts
EMC ScaleIO	Alert Consolidation, Pre-configured alerts
EMC VPLEX	Alert Consolidation, Pre-configured alerts
IBM DS (if upgrading from 3.6.x)	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.)

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 4.0.1:
   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.

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.

```
<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.

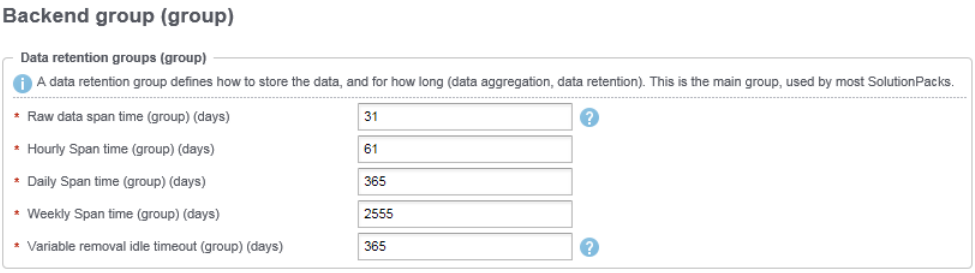
Selecting each backend group shows the raw data span time for each group. Each data retention group can be changed in the **Data retention groups** table and then applied to all the backend servers.

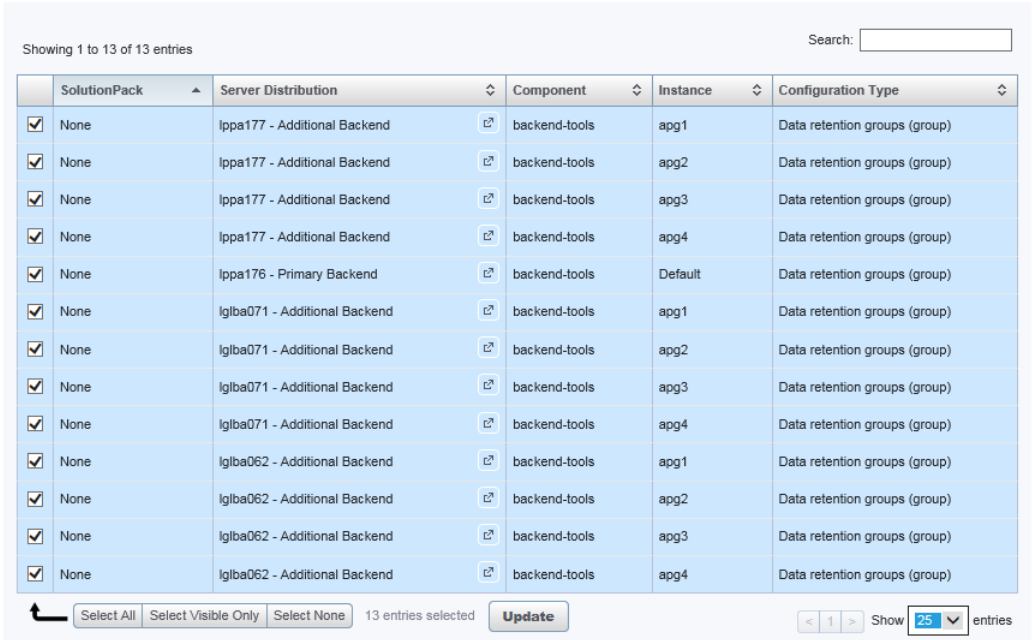
Note

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**.





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.

Reinstalling the SolutionPack for EMC Isilon pre-configured alerts

EMC Isilon alert definitions have been simplified and consolidated in the SolutionPack for EMC Isilon 4.0.1. Due to the name changes of these alert definitions, upgrading to ViPR SRM 4.0.1 results in two sets of alert definitions being listed. To remove the earlier alert definitions, remove and reinstall the EMC Isilon pre-configured alerts component. Custom EMC Isilon alert definitions will be preserved.

Procedure

1. Navigate to **Centralized Management**.
2. Click **SolutionPacks** > **Storage** > **EMC Isilon**.
3. Remove the **Pre-configured alerts** block using the trash can icon.
4. Click **SOLUTIONPACK CENTER**.
5. Select **EMC Isilon** from the **Browse and Install SolutionPacks** window.
6. Click **Install**.
7. Ensure that the **Pre-configured alerts** component is selected and click **Next**.
8. Click **Install**.

   The following alert definitions are now listed:

   - CPU and Memory
   - Disk
   - Fan
   - Node
   - Power Supply
   - Quota
   - Snapshot
   - Battery Failure
   - Miscellaneous Event
   - Process Failure
   - Sensor Event

Limitations and known issues

- After the upgrade, device names, N/A, or PROP.'fqdn' may display in the Platform group filter for reports related to alerts. These filters are removed when another occurrence of the same alert is generated or after 7 days (whichever happens first).
- If you upgraded from 3.6.x, on the **Oracle Database** > **Inventory** page, the system will display two entries for a single standalone Oracle instance with different component/sub-component counts.
- After upgrading generic-reports, the alerts tables under **Dashboards** and **Operations** are empty until you restart Tomcat.
- After the upgrade, the alert counts displayed in topology map tooltips for Isilon devices report only new alerts and do not report any alerts that were triggered before the upgrade.
- The storage system type for Data Domain was changed from Unified to File in SRM 4.0. If you upgraded the SolutionPack for EMC Data Domain from 3.7 or 3.7.1 to 4.0, the system will display duplicate summary tables for one day until the property `sstype=Unified` becomes inactive.
- For the SolutionPack for EMC Isilon, node pool metrics are inactive after upgrade for systems with more than one node pool.

- If you upgraded from 3.6.x, for the SolutionPack for EMC VMAX, duplicate microcode versions may display in the in the Enginuity/Microcode columns for up to 14 days.
- Group Filters: If you upgraded from 3.6.3 or 3.6.4, the predefined filters for Customer and Business Unit that appear at the top of many reports show a pipe symbol (|) after the default filter value. The value appears as Default| rather than Default.
- After the upgrade, the Memory Utilization fields in the following EMC Data Domain reports are blank:
  - **Summary**
  - **Performance** > **List of Data Domains**
  - **Top 10**