

EMC ViPR SRM: Upgrading version 3.0.x to 3.5.1

ABSTRACT

This white paper explains how to upgrade EMC ViPR SRM from version 3.0.x to 3.5.1.

September 2014

Rev. 2

Copyright © 2014 EMC Corporation. All Rights Reserved.

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 listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

VMware and are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other trademarks used herein are the property of their respective owners.

Part Number H13403

TABLE OF CONTENTS

EXECUTIVE SUMMARY	4
PREPARING YOUR ENVIRONMENT FOR UPDATE	4
Verify and document the current status of the environment	4
vApp Deployments	4
Single Operating System Deployments (non-vApp Linux)	7
Single Operating System Deployments (Windows)	8
Mixed Operating System Deployments	9
UPDATING CORE MODULES USING THE LAUNCH-UPDATE SCRIPT	9
Running the launch-update script on all of the servers	9
UPDATING SOLUTIONPACKBLOCKS	12
Prerequisites	13
Synchronize your deployment	14
Install the Load-Balancer-Connector	14
Update the Health SolutionPack	14
Updating Independent SolutionPackBlocks	15
Updating Blocks in SolutionPacks	18
CHECKING THE STATUS OF REMOTE HOST SERVICES	21
DELETING THE OLD VERSION OF THE DEFAULT REPORTPACK	21
POST UPGRADE ALERTING CHANGES	22
UPGRADING THE WHATIF_SCENARIOS TABLE	24
ADDING BLOCKS FOR ALERTS	25
UPDATING THE SNMP COLLECTIONS	26
CONFIGURING VIRUS-SCANNING SOFTWARE (WINDOWS)	26
VALIDATING THE ENVIRONMENT	26
Verify the post-upgrade operational status	26
APPENDIX A	27
How to Export a Report Definition	27
APPENDIX B	30
Updating and reconfiguring the Storage Compliance SolutionPackBlocks	30
Installing the Storage Compliance frontend module	30

Executive summary

This document describes the process for upgrading an existing 3.0.x installation of ViPR SRM to 3.5.1. These instructions apply to standard installations, vApp installations, and installations across multiple platforms.

IMPORTANT: Please read this entire document before starting the upgrade process to avoid experiencing a problem or a missed prerequisite during the upgrade.

This upgrade process may take between 4 and 8 hours.

Preparing your environment for update

This section describes how to 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.

Use your current backup software to perform backups of the ViPR SRM environment before starting the upgrade.

Refer to the ViPR SRM support matrix on support.emc.com for an up-to-date list of supported web browsers.

Verify and document 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.

- 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.
- Look for broken links — Resolve any issues or document them for later follow up.
- Validate that End-to-End topology is working — Resolve any issues.
- Using the data in the ViPR SRM UI, run the ViPR SRM Deployment Planner to determine sizing with the targeted ViPR SRM version.
 - Download the ViPR SRM Deployment Planner from support.emc.com/downloads/34247_ViPR-SRM
 - For additional details about determining configuration size, refer to *ViPR SRM Performance and Scalability Guidelines* at support.emc.com/products/34247_ViPR-SRM/Documentation
- Review the existing backend and databases — Check **Report Library > EMC Watch4net Health > Modules Performance > Backends** and **Report Library > EMC Watch4net Health > Modules Performance > Databases**
 - Check backend thresholds to verify that you have room to accommodate the new sizing.
 - Add additional backends and databases as required. (The metric count should not exceed 1 million.)
 - This may require the manual movement of data to redistribute the metrics. Refer to the Watch4net Database Split v1.2 document for these steps.

Note: Engage EMC Support to resolve any observed issues prior to proceeding with the upgrade. This will aid in understanding the success of the upgrade.

vApp Deployments

Prerequisites

Ensure that the following prerequisites are met:

- Gather the names of all of the ViPR SRM VMs in the system.
- Take snapshots of all of the ViPR SRM VMs in your deployment.
- Ensure that a login with root credentials is available. The default account is `root/Changeme1!`. If the defaults have been changed, ensure that you know the new credentials.
- Download the ViPR SRM 3.5SP1 vApp Update file (`ViPR_SRM_3.5.1_vApp_Update.zip`) from support.emc.com.

- 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.
- Any changes made to the firewall configuration by editing `etc/sysconfig/SuSEfirewall2.d/services/apg` will be overwritten by the default firewall configuration applied during the upgrade. Make sure you save a copy of this file so you can compare and reapply them after the upgrade by running the `/usr/sbin/enable_firewall_port.sh` script, which will preserve the configuration across future upgrades. Run `enable_firewall_port.sh` for instructions on how to use the script. Refer to *EMC ViPR SRM Security Configuring Guide* on support.emc.com for additional details.

Update Linux Components

To update the Linux components, complete the following steps for every ViPR SRM VM in the system:

1. Upload the `ViPR_SRM_3.5.1_vApp_Update.zip` file to a temporary directory on the VM using a tool such as SCP.
2. Log in to the VM host as root.
3. Extract the ZIP file.
4. Navigate to the `applianceUpdate` directory and make the `applianceUpdate` script executable:
`chmod +x applianceUpdate`
5. Run the `applianceUpdate` script:
`./applianceUpdate`

```
lg1bd185:/tmp # cd applianceUpdate/
lg1bd185:/tmp/applianceUpdate # chmod +x applianceUpdate
lg1bd185:/tmp/applianceUpdate # ./applianceUpdate
05:43:38 [INFO]: Updating FrontEnd appliance to version: 3.5.1.0.114
05:43:38 [INFO]: Preparing for update ...
05:43:39 [INFO]: Checking SLES for an update.
05:43:40 [INFO]: No new update found for SLES.
05:43:40 [INFO]: Checking packages for an update ...
34 packages to upgrade.
05:43:40 [INFO]: Updating existing packages. This may take some time. Please wait ...
05:44:24 [INFO]: Update of existing packages completed ...
05:44:24 [INFO]: Checking patterns for an update
3 new packages to install.
05:44:25 [INFO]: New update found. Installing pattern: SRM-update. Please wait ...
05:44:36 [INFO]: Update of existing packages for Pattern Install completed ...
05:44:36 [INFO]: Update complete.
Not running on a Primary Backend, skipping
Cleaning up /tmp/fix-load-balancer
We are not an Additional Backend Appliance, exiting!
No Ports to add for Frontend Appliance

#-----
#                               EMC Installation Manager
#-----
Copyright (c) [1997-2014] EMC Corporation. All Rights Reserved.

This software contains the intellectual property of EMC Corporation or is
licensed to EMC Corporation from third parties. Use of this software and the
intellectual property contained therein is expressly limited to the terms and
conditions of the License Agreement under which it is provided by or on behalf
of EMC.
```

Note: The output of the script will be different for the primary and additional backend host. Additional steps are required for the load balancer configuration (on the primary backend host) and the installation of the task-scheduler (on the additional backend host).

Important: On the primary backend host, 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/3.0.101-0.8-default/modules.dep: No such file or directory* and other errors related to iptables) can safely be ignored.

Important: The upgrade to ViPR SRM 3.5.1 in vApp deployments includes a Linux kernel update which requires a reboot before updates can proceed. Reboot the vApp before moving to the next step.

To reboot the vApp:

1. Login to each server and enter the following command from the command prompt:
`shutdown -h now`
2. Power the VMs back on through the vCenter by using the Power On the vApp folder.

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
```

The proper order for manually rebooting hosts in a complex configuration is:

1. Primary backend
2. All additional backends
3. Frontend
4. All collectors

Stage ViPR SRM Components on all ViPR SRM VMs deployed using the vApp installer

To stage the ViPR SRM components on all of the ViPR SRM VMs deployed using the vApp installer:

1. Log in as root to each VM.
2. Navigate to the `/usr/APG_Source` directory and run the post install script:
`./post_install.sh`
3. Answers the questions as directed. For example, accept the EULA and use the defaults for the installation directory and the package installation.

```
If Customer has a currently enforceable, written and separately signed software license agreement directly with EMC
or the Distributor from whom Customer obtained this Software, then by clicking on the "Agree" or "Accept" or sim
ilar button at the end of this Agreement, or proceeding with the installation, downloading, use or reproduction of
this Software, or authorizing any other person to do so, you are representing that you are (i) authorized to bind
the Customer; and (ii) agreeing on behalf of the Customer that the terms of such written, signed agreement shall

Do you accept EULA [y/N] ? y
Enter the new or current installation directory [/opt/APG]:
Install new packages in /opt/APG/Tools/Module-Repository [Y/n] ?
Copying new packages to /opt/APG/Tools/Module-Repository.....
..... done

! WARNING: A more recent version of the module-manager is available. It is strongly recommended to upgrade it bef
ore anything else.
Installed Modules:

  Identifier              Instance              : Category  Module Name              Versi
on Revision OS-Arch   Status
-----
! apg-self-monitoring-collector   emc-watch4net-health : Collecting APG-Self-Monitoring-Collector   v1.4
r45755   linux-x64 can be updated to v1.5
! availability-filter             Generic-SNMP         : Collecting Availability-Filter              v1.3u
1 r41349   linux-x64 can be updated to v1.4
! availability-filter             netapp-filer         : Collecting Availability-Filter              v1.3u
1 r41349   linux-x64 can be updated to v1.4
* brocade-fc-switch-collect       brocade-fc-switch    : Block    brocade-fc-switch-collect v3.0.
1 r4690
! collector-manager               Generic-RSC          : Collecting Collector-Manager                v5.4
r45610   linux-x64 can be updated to v5.5u1
! collector-manager               Generic-SNMP         : Collecting Collector-Manager                v5.4
r45610   linux-x64 can be updated to v5.5u1
! collector-manager               brocade-fc-switch    : Collecting Collector-Manager                v5.4
```

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

If you have an installation without any other Linux or Windows servers, your system is now prepared for update, and you can skip to the [Updating core modules using the launch update script](#) section. 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 Windows deployments included in your environment, locate each system and perform the steps described in the [Single Operating System Deployments \(Windows\)](#) section.

If you have any non-vApp Linux deployments included in your environment, locate each system and perform the steps described in the [Single Operating System Deployments \(non-vApp Linux\)](#) section.

Single Operating System Deployments (non-vApp Linux)

Pre-Requisites

Ensure that the following pre-requisites are met:

- Identify the servers that you plan to upgrade
- Ensure that a login with root credentials is available
- Download the ViPR SRM 3.5SP1 Linux Deployment file (ViPR_SRM_3.5.1_Linux_x86_64.tgz) from support.emc.com

Procedure

1. Using a tool such as SCP, upload the file to a temporary directory on every server that you plan to upgrade.
2. Log in to the server as root.
3. Extract the ViPR_SRM_3.5.1_Linux_x86_64.tgz file:


```
tar zxvf ViPR_SRM_3.5.1_Linux_x86_64.tgz
or
gunzip -c newViPR_SRM_3.5.1_Linux_x86_64.tgz |tar xvf -
```
4. Navigate to the temporary directory and make the setup script executable:


```
chmod +x EMC_MnR_6.4.1_Linux_64-bit_Setup_File.sh
```
5. Run the setup script:


```
./EMC_MnR_6.4.1_Linux_64-bit_Setup_File.sh
```
6. Answers the questions as directed. For example, accept the EULA and use the defaults for the installation directory and the package installation.

```
Do you accept EULA [y/N] ? y
Enter the new or current installation directory [/opt/APG]:
Install new packages in /opt/APG/Tools/Module-Repository [Y/n] ? y
Copying new packages to /opt/APG/Tools/Module-Repository..... done
.....

! WARNING: A more recent version of the module-manager is available. It is strongly recommended to upgrade it before anything else.
Installed Modules:
```

Identifier	Instance	Category	Module Name	Version	Revision	OS-Arch	Status
! administration-tool	Default	: Tools	Administration-Tool	v1.1u4	r44610	linux-x64	can be updated to v1.2u1
! alert-consolidation	Alert-Consolidation	: Block	alert-consolidation	v3.1.1	r4729	linux-x64	can be updated to v3.5.1
! alerting-backend	Default	: Backends	Alerting-Backend	v3.6u1	r48357	linux-x64	can be updated to v3.7u1
! alerting-frontend	alerting-frontend	: Web-Applications	Alerting-Frontend	v3.6u4	r50287	linux-x64	can be updated to v3.7u1
! apg-self-monitoring-collector	emc-watch4net-health	: Collecting	APG-Self-Monitoring-Collector	v1.4	r45755	linux-x64	can be updated to v1.5
! availability-filter	Generic-SNMP	: Collecting	Availability-Filter	v1.3u1	r41349	linux-x64	can be updated to v1.4
! backend	Default	: Backends	APG-Backend	v5.6u1	r47899	linux-x64	can be updated to v5.7

Your system is now prepared for update.

Note: For non-vApp Linux deployments, before starting core software services, ensure the library search path is correct on the server hosting the core software. This requirement applies to the libaio package on Linux. To verify the path:

1. Log in as root and the run the following command:

```
ldconfig -v | grep -i libaio
```

Output similar to the following should display at the end of the messages generated by the script:

```
libaio.so.1.0.0 -> libaio.so.1.0.0
libaio.so.1 -> libaio.so.1.0.1
```

For example:

```
lg1ba182:/usr/APG_Source # ldconfig -v | grep -i libaio
ldconfig: Can't stat /usr/X11R6/lib64/Xaw3d: No such file or directory
ldconfig: Can't stat /usr/lib64/Xaw3d: No such file or directory
ldconfig: Can't stat /usr/X11R6/lib/Xaw3d: No such file or directory
ldconfig: Can't stat /usr/lib/Xaw3d: No such file or directory
ldconfig: Can't stat /opt/kde3/lib: No such file or directory
ldconfig: Can't stat /opt/kde3/lib64: No such file or directory
ldconfig: Path `/lib' given more than once
ldconfig: Path `/lib64' given more than once
ldconfig: Path `/usr/lib' given more than once
ldconfig: Path `/usr/lib64' given more than once
libaio.so.1 -> libaio.so.1.0.1
lg1ba182:/usr/APG_Source #
```

If no output (or incorrect output) is returned, install the latest libaio package from the OS vendor.

Single Operating System Deployments (Windows)

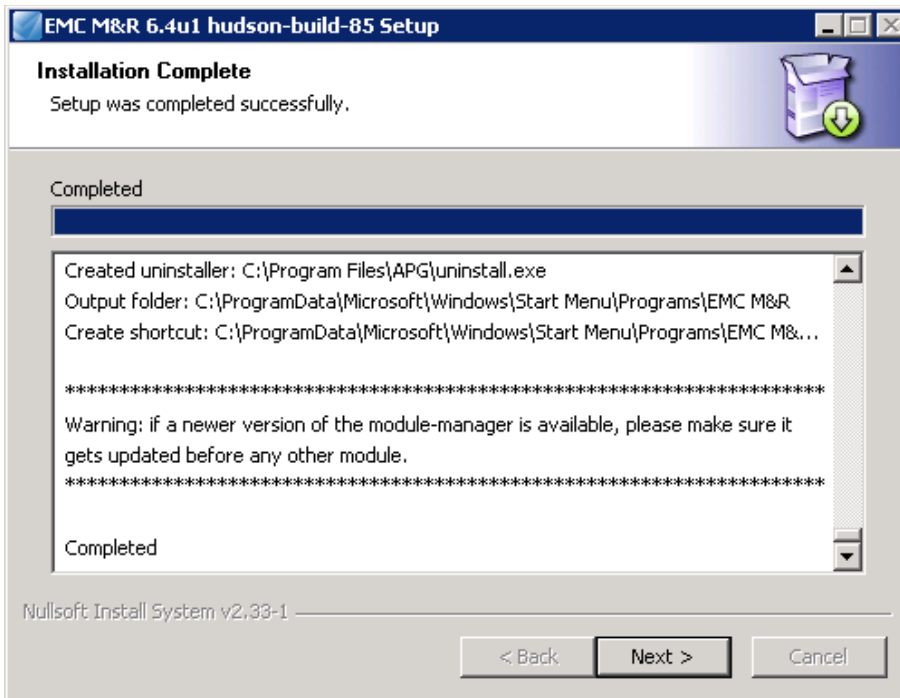
Pre-Requisites

Ensure that the following pre-requisites are met:

- Identify the servers that you plan to upgrade
- Ensure that login credentials with System Administrator permissions are available
- Download the ViPR SRM 3.5SP1 Windows Deployment file (ViPR_SRM_3.5.1_Win64.zip) from support.emc.com, and place the install binary in a temporary location on every server
- Place the install binary in a temporary location on every server

Procedure

1. Extract the zip file to temporary location.
2. Double-click the EMC_MnR_6.4.1_Windows_64-bit_Setup_File executable.
3. Click **Next**.
4. Read and accept the End User License Agreement. Click **I Agree**.
5. Press **Enter** to accept the default installation directory of C:\Program Files\APG, or specify a different location.
6. Press **OK** to install the new packages in the C:\Program Files\APG\Tools\Module-Repository directory.



Your system is now prepared for update.

Mixed Operating System Deployments

To update a mixed-operating system deployment (non-vApp Linux and Windows), you must perform the steps for single operating system deployments separately, once on each platform. One server must be the server that is hosting Centralized Management.

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.

Updating core modules using the launch-update script

During this step, you will update the core modules on all of the ViPR SRM servers. These are modules that must be updated prior to any others, and they must be updated from the command line using the launch-update script.

Running the launch-update script on all of the servers

Linux

Important: Run the launch-update script on collector hosts before running it on the primary backend host. This will maintain the synchronization between the topology service and topology mapping service.

Important: Any manual collection customizations or configurations changes made directly in the XML files will be overwritten. Any report customizations to the Report Library reports will be lost. Make sure you backup and merge your changes. For instructions on how to backup and import the changes, refer to kb000185065 on the EMC Support website or see Appendix A for a copy of the kb articles.

To run the launch-update script on all of the Linux servers:

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
```

```

lg1bdi89:/usr/APG_Source # cd /opt/APG/bin/
lg1bdi89:/opt/APG/bin # ./manage-modules.sh update module-manager
! WARNING: A more recent version of the module-manager is available. It is strongly recommended to upgrade it before anything else.
Required dependencies, in processing order:
[1] java '6.0u45' v6.0u45
[2] U module-manager '1.5u2' v1.5u2 => v1.6u1
> 1 not modified, 1 to update
> 9.6 MB space required / 111.3 GB available
? Enter the step to modify, 'yes' to accept them, or 'no' to cancel the operation [yes] > yes

Starting update of module-manager 1.5u2 from v1.5u2 to v1.6u1...
* Gathering information...
* Module found in '/opt/APG/Tools/Module-Manager/1.5u2'.
* It will now be updated using 'module-manager-1.6u1-linux-x64.pkg'.
* Unpacking files...
* Updating files... 100%
* 51 files have been updated.
* Finalizing update...
Update complete.
lg1bdi89:/opt/APG/bin #

```

2. Navigate to the /opt/APG/Tools/Module-Manager/1.6u1/bin directory.
3. Change the permissions for the script:


```
chmod u+x launch-update.sh
```
4. Launch the script from /opt/APG/Tools/Module-Manager/1.6u1/bin by running:


```
./launch-update.sh
```
5. At the prompt, review the modules that will be updated and the SolutionPacks that will be reconfigured.

```

lg1bdi88:/opt/APG/Tools/Module-Manager/1.6u1/bin # ./launch-update.sh
14 modules are about to be updated:
* jdbc-drivers Default (2.1 => 2.2)
* license-manager Default (5.2u2 => 5.3u1)
* webservice-gateway Default (1.2 => 1.3u1)
* apg-self-monitoring-collector emc-watch4net-health (1.4 => 1.5)
* backend apg1 (5.6u1 => 5.7u1)
* backend apg2 (5.6u1 => 5.7u1)
* backend apg3 (5.6u1 => 5.7u1)
* backend apg4 (5.6u1 => 5.7u1)
* collector-manager emc-watch4net-health (5.4 => 5.5u1)
* failover-filter emc-watch4net-health (5.1 => 5.1u1)
* mysql Default (5.5u1 => 5.5u2)
* property-tagging-filter emc-watch4net-health (2.6u1 => 2.7u1)
* task-scheduler Default (1.4u1 => 1.5u1)
* java 6.0u45 (6.0u45 => 7.0u67)

1 SolutionPackBlocks will be reconfigured:
* emc-watch4net-health-collect emc-watch4net-health (1.0)

IMPORTANT: Any manual collection customizations or configurations changes made directly in the XML files of currently installed SolutionPacks will be overwritten. Any report customizations to the currently installed SolutionPacks will be overwritten. Make sure you backup and merge your changes. Reports can be exported and imported back or simply copied in the MyReports section. Article kb000185065 (https://support.emc.com/kb/185065) on the EMC Support website explains the export feature.

Proceed? (yes/no) [y] >

```

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. To review the list of installed modules and their update status, run the following command. (At this stage of the upgrade, there should only be a few modules that still need to be updated. These will be handled later in this upgrade procedure.)

```
manage-modules.sh list installed
```

All modules except some block type modules will have been updated successfully. These block type modules are updated later through the UI.

IMPORTANT: If you are updating a vApp VM from ViPR SRM 3.0:

Run the following command on the additional backend host to ensure that the backend ports are not blocked:

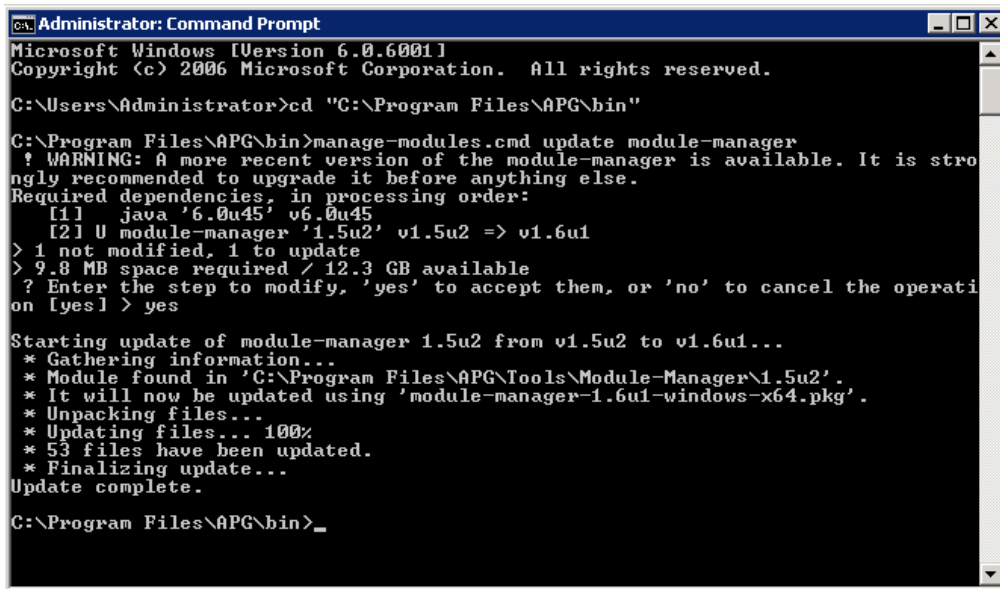
```
enable_firewall_port.sh TCP 2100 2101 2200 2201 2300 2301 2400 2401
```

The script is located in the /usr/sbin directory.

Windows

To run the launch-update script on all of the Windows servers:

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. Verify that all of the services have stopped by typing the following command from the C:\Program Files\APG\bin directory:
`manage-modules.cmd service status all`
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`



```
C:\Users\Administrator>cd "C:\Program Files\APG\bin"
C:\Program Files\APG\bin>manage-modules.cmd update module-manager
! WARNING: A more recent version of the module-manager is available. It is strongly recommended to upgrade it before anything else.
Required dependencies, in processing order:
    [1] java '6.0u45' v6.0u45
    [2] U module-manager '1.5u2' v1.5u2 => v1.6u1
> 1 not modified, 1 to update
> 9.8 MB space required / 12.3 GB available
? Enter the step to modify, 'yes' to accept them, or 'no' to cancel the operation [yes] > yes

Starting update of module-manager 1.5u2 from v1.5u2 to v1.6u1...
* Gathering information...
* Module found in 'C:\Program Files\APG\Tools\Module-Manager\1.5u2'.
* It will now be updated using 'module-manager-1.6u1-windows-x64.pkg'.
* Unpacking files...
* Updating files... 100%
* 53 files have been updated.
* Finalizing update...
Update complete.

C:\Program Files\APG\bin>
```

4. Launch the script from C:\Program Files\APG\Tools\Module-Manager\1.6u1\bin by running:
`launch-update.cmd`

- At the prompt, review the modules that will be updated and the SolutionPacks that will be reconfigured.

```
Administrator: Command Prompt - launch-update.cmd
C:\Program Files\APG\Tools\Module-Manager\1.6u1>cd bin
C:\Program Files\APG\Tools\Module-Manager\1.6u1\bin>launch-update.cmd
25 modules are about to be updated:
* jdbc-drivers Default <2.1 => 2.2>
* license-manager Default <5.2u2 => 5.3u1>
* webservice-gateway Default <1.2 => 1.3u1>
* app-self-monitoring-collector emc-watch4net-health <1.4 => 1.5>
* availability-filter Generic-SNMP <1.3u1 => 1.4>
* collector-manager Generic-RSC <5.4 => 5.5u1>
* collector-manager Generic-SNMP <5.4 => 5.5u1>
* collector-manager emc-centera <5.4 => 5.5u1>
* collector-manager emc-watch4net-health <5.4 => 5.5u1>
* failover-filter Generic-RSC <5.1 => 5.1u1>
* failover-filter Generic-SNMP <5.1 => 5.1u1>
* failover-filter emc-centera <5.1 => 5.1u1>
* failover-filter emc-watch4net-health <5.1 => 5.1u1>
* property-tagging-filter Generic-RSC <2.6u1 => 2.7u1>
* property-tagging-filter Generic-SNMP <2.6u1 => 2.7u1>
* property-tagging-filter emc-centera <2.6u1 => 2.7u1>
* property-tagging-filter emc-watch4net-health <2.6u1 => 2.7u1>
* remote-shell-collector Generic-RSC <1.3u4 => 1.4>
* snmp-collector Generic-SNMP <6.3u1 => 6.4u1>
* text-collector emc-centera <1.10u1 => 1.11>
* topology-mapping-service Default <1.0u2 => 1.1u1>
* variable-handling-filter Generic-RSC <1.9u1 => 1.12>
* variable-handling-filter Generic-SNMP <1.9u1 => 1.12>
* variable-handling-filter emc-centera <1.9u1 => 1.12>
* java 6.0u45 <6.0u45 => 7.0u67>

4 SolutionPackBlocks will be reconfigured:
* emc-centera-collect emc-centera <1.3>
* emc-watch4net-health-collect emc-watch4net-health <1.0>
* generic-rsc Generic-RSC <3.1.2>
* generic-snmp Generic-SNMP <3.1.1>

IMPORTANT: Any manual collection customizations or configurations changes made d
irectly in the XML files of currently installed SolutionPacks will be overwritte
n. Any report customizations to the currently installed SolutionPacks will be ov
erwritten. Make sure you backup and merge your changes. Reports can be exported
and imported back or simply copied in the MyReports section. Article kb000185065
(https://support.emc.com/kb/185065) on the EMC Support website explains the exp
ort feature.

Proceed? <yes/no> [y] > _
```

- 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.
- To review the list of installed modules and their update status, run the following command. (At this stage of the upgrade, there should only be a few modules that still need to be updated. These will be handled later in this upgrade procedure.)
`./manage-modules.cmd list installed`
- 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 6.0u45 from path 'C:\Program Files\APG\Java\Sun-JRE'
```

All modules except some block type modules will have been updated successfully. These block type modules are updated later through the UI.

Updating SolutionPackBlocks

In this section, you will update all of the installed SolutionPackBlocks to their latest versions.

IMPORTANT: Any manual collection customizations or configurations changes made directly in the XML files will be overwritten. Any report customizations to the Report Library reports will be lost. Make sure you backup and merge your changes. For instructions on how to backup and import the changes, refer to kb000185065 on the EMC Support website or see Appendix A for a copy of the kb articles.

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

Prerequisites

Rename your old Default ReportPack

When the reports block for a SolutionPack is updated, ViPR SRM installs a generic-reports module and adds the latest version of the Default ReportPack to the frontend. The result is that two Default ReportPacks (an old version and a new version) are displayed. If there are no issues with the new version of the Default ReportPack, you can delete the old one. Renaming the old Default ReportPack will help you identify the Default ReportPack that can be deleted.

1. Login to `http://<Frontend IP address>:58080/APG/`.
2. Click **Administration**, and then click **ReportPacks** on the left-hand pane to access ReportPacks Management. The available ReportPacks are listed in the right-hand pane.
3. Rename the existing Default ReportPack to distinguish between the existing one and the new one.
 - a. Select **Default ReportPack** in the pane.
 - b. Rename the file you will replace. For example, type “old” in the Name field.
 - c. Click **Save**. You are returned to ReportPacks Management.

Administration >> ReportPacks >> Default ReportPack(older)

ReportPack Modification: Default ReportPack(older) | Administration

This section allows the creation and modification of ReportPacks.

ReportPack Information

i This information is for administration purposes only. It will not be displayed in the user interface.

Name	Default ReportPack(older)
Version	3.1.1.0
Description	The default ReportPack, included with any Watch4net install.

Delete

Export

Save

Synchronize your deployment

Note: If you are running a system with only one server, you do not need to synchronize your deployment, and you can skip to the [Updating Independent SolutionPackBlocks](#) section.

Depending on how your system is deployed and what steps you took previously, it is possible the Centralized Management UI will not have all the latest data about which packages are deployed and available. For this reason, you must first synchronize all modules and their available versions.

To synchronize all of the modules and their available versions:

1. Log in to the Centralized Management web interface:
`http://<Frontend IP address>:58080/centralized-management`
The default username is `admin`, and the default password is `changeme`.
2. Navigate to Packages Management on the left-hand panel of the home screen.
3. In the Packages listing section of the right-hand pane, click **Synchronization**.
4. Select the "Retrieve the latest packages from the remote servers" checkbox and click **OK**.

Install the Load-Balancer-Connector

Note: The Load-Balancer-Connector (LBC) does not need to be installed in AIO (All-In-One) environments or in environments where you have previously installed it.

Before completing these steps, validate the load-balancer configuration by reviewing the settings described in the "Configuring Load Balancing for ViPR SRM" article on community.emc.com.

To install the LBC, complete the following steps on each collector host:

1. From the Centralized Management UI, select the collector host under **Physical Overview** in the left-hand pane.
2. Select the **SolutionPacks & Modules** tab.
3. Click **Install**. The Packages Installation window opens.
4. In the Categories section, click the **Block** checkbox.
5. In the Packages section, click the **load-balancer-connector v3.5.1** checkbox.
6. Click **Launch**.
7. Accept the defaults (and specify an instance name for each module) to install the Collector Manager, FailOver-Filter, Load-Balancer, and Load-Balancer-Connector.

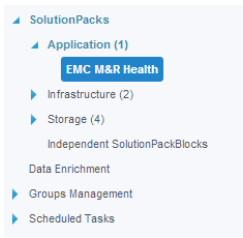
Note: Do not change the default instance names for the LBC.

Note: Ensure that the firewall ports on all of the backends are opened up in listening mode.

Update the Health SolutionPack

Navigate to **SolutionPacks > Application > EMC Watch4net Health** and update the report SolutionPackBlock. This installs the generic reports module (as a dependency) and also uploads the latest version of the Default ReportPack.

Note: All of the new SolutionPackBlock modules are already staged in your system. Applying the updates requires two steps. First, update the Independent SolutionPackBlocks, and then update the SolutionPackBlocks that are part of SolutionPacks.



Instance	SolutionPackBlock	Version	SolutionPack(s) Version	Server Distribution
emc-watch4net-health	Data collection	1.0	1.3	lgbd180.iss.emc.com - Front End
emc-watch4net-health	Data collection	1.0	1.3	lgbd181.iss.emc.com - Primary Backend
emc-watch4net-health	Data collection	1.0	1.3	lgbd183.iss.emc.com - Collector
emc-watch4net-health	Reports	1.3	1.3	lgbd180.iss.emc.com - Front End
emc-watch4net-health	Data collection	1.4.1	1.4.1	lgbd182.iss.emc.com - Additional Backend

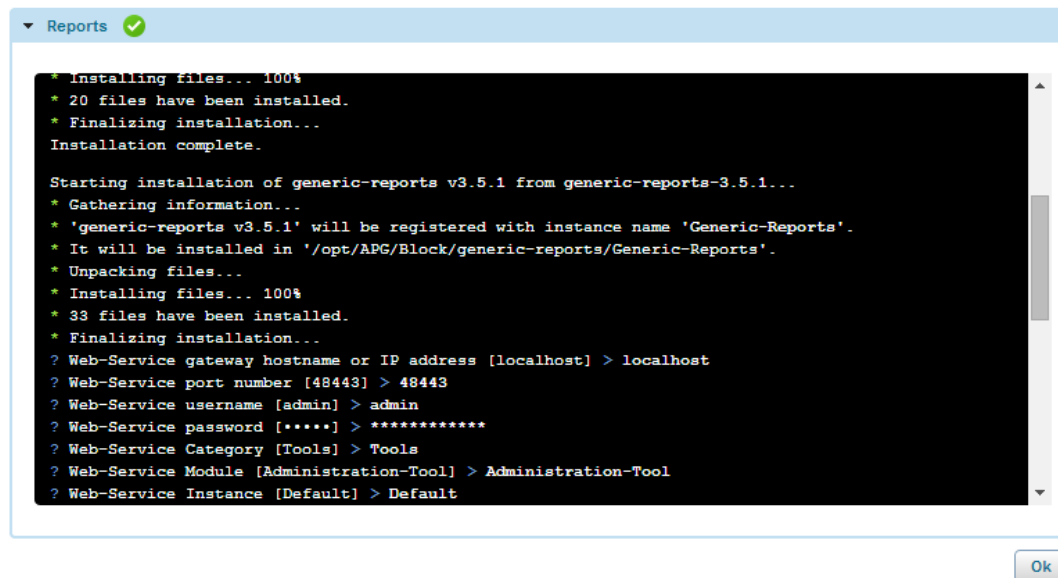
Showing 1 to 5 of 5 entries

First Previous 1 Next Last

SolutionPack Update

EMC M&R Health v1.4.1

Updating



Updating Independent SolutionPackBlocks

Important: While updating all independent and data collection SolutionPackBlocks, check the property store configuration. Wherever it is set to "localhost," change it to the frontend hostname.

Important: While updating independent and data collection SolutionPackBlocks that are installed on the collector hosts, ensure that the "Hostname or IP address to send data to" field in the data collection section is set to localhost:2020.

Note: If you are upgrading a vApp AIO (All-In-One) environment, which has only the default database configuration (one Backend and one Timeseries database), when updating the Load-Balancer in the Independent SolutionPackBlocks (load-balancer-arbiter), the reconfiguration UI will show five databases configured. Only the Default APG backend and Database are installed. Remove all the additional APG Backend configurations by clicking the Trash icon and reconfiguring.

To update Independent SolutionPackBlocks:

1. In the ViPR SRM Centralized Management UI, navigate to **SolutionPacks > Independent SolutionPackBlocks** on the left-hand pane.

← → ↻ | lgld185-58080/centralized-management/#/sp/orphans

Welcome admin (logged as admin) C.M. - EMC M&R Wednesday, August 13, 2014

ONLINE UPDATE SOLUTIONPACK CENTER USER SETTINGS CONFIGURATION DOCUMENTATION

Your Company Logo

- Packages Management
- Licenses Management
- Audit Logs
- Discovery Center
 - Host Agent specific configuration
 - Host configuration
 - Netapp Configuration
 - VIPR Configuration
 - VMAX
 - VMware vCenter (vmware-vcenter)
 - VMware vCenter (vmware-vcenter)
 - VNX
 - VPLEX
- Central Configuration Repository
- SolutionPacks
 - Application (2)
 - Infrastructure (3)
 - Storage (11)
 - Independent SolutionPacksBlock

Independent SolutionPacksBlocks

List of all the installed SolutionPacksBlocks not owned by any SolutionPack. SolutionPacksBlocks will be reconfigurable if the package is available remotely.

Show 10 entries Search:

Instance	SolutionPackBlock	Version	Server Distribution
Alert-Consolidation	alert-consolidation	3.1.1	lgld186.lss.emc.com - Primary Backend
Generic-RSC	generic-rsc	3.1.2	lgld189.lss.emc.com - Collector
Generic-RSC	generic-rsc	3.1.2	lgld198.lss.emc.com - Windows Collector
Generic-SNMP	generic-snmp	3.1.1	lgld189.lss.emc.com - Collector
Generic-SNMP	generic-snmp	3.1.1	lgld198.lss.emc.com - Windows Collector
Generic-Topology	generic-topology	3.1.1	lgld186.lss.emc.com - Primary Backend
Load-Balancer	load-balancer-arbiter	3.1.1	lgld186.lss.emc.com - Primary Backend

Showing 1 to 7 of 7 entries

First Previous 1 Next Last

- Each installed Independent SolutionPackBlock that must be updated will display a yellow star. Click the star to begin the update.

Independent SolutionPacksBlocks

Independent SolutionPacksBlocks

List of all the installed SolutionPacksBlocks not owned by any SolutionPack. SolutionPacksBlocks will be reconfigurable if the package is available remotely.

Show 10 entries Search:

Instance	SolutionPackBlock	Version	Server Distribution
Alert-Consolidation	alert-consolidation	3.1.1	lgld186.lss.emc.com - Primary Backend
Generic-RSC	generic-rsc	3.1.2	lgld189.lss.emc.com - Collector
Generic-RSC	generic-rsc	3.1.2	lgld198.lss.emc.com - Windows Collector
Generic-SNMP	generic-snmp	3.1.1	lgld189.lss.emc.com - Collector
Generic-SNMP	generic-snmp	3.1.1	lgld198.lss.emc.com - Windows Collector
Generic-Topology	generic-topology	3.1.1	lgld186.lss.emc.com - Primary Backend
Load-Balancer	load-balancer-arbiter	3.1.1	lgld186.lss.emc.com - Primary Backend

Showing 1 to 7 of 7 entries

First Previous 1 Next Last

- Carefully review all settings on the Update page, and then click **Update**.

SolutionPack Update

alert-consolidation v3.5.1

- Database Type: MySQL ?
- Database hostname or IP address: lgld186.lss.emc.com ?
- Database port: 53306 ?
- Database username: app ?
- Database password: ?
- Alert Consolidation schema: events ?
- Alert Retention period: 30 ?
- Event Listener Port: 2040 ?
- Trap Receiver Port: 2041 ?

Enable Alert Notification ☐

Frontend Web service

Configure the Frontend Web service. Please indicate where the frontend Web service is running. This is typically your frontend server.

The progress of the update will be displayed in the update page. You can maximize this page to monitor the progress of the update. Once the update completes, a green checkmark will be displayed at the top of the page.

SolutionPack Update

Updating

alert-consolidation ✓

```
? Alert Consolidation schema [events] > events
? Alert Retention period [30] > 30
? Event Listener Port [2040] > 2040
? Trap Receiver Port [2041] > 2041
? Enable Alert Notification [yes [no] > yes
? Alerting Backend hostname or IP address [lgld186.lss.emc.com] > lgld186.lss.emc.com
? Alerting Backend Event Port [2012] > 2012
? Tomcat hostname or IP address [localhost] > localhost
? Tomcat port [58080] > 58080
[1] HTTP
[2] HTTPS
? Tomcat communication protocol > 1
? Username [ws-user] > ws-user
? Password [.....] > .....
? Frontend Web service instance name [APG-WS] > APG-WS
? Enable Impact Analysis [yes [no] > no
* Stopping 'event-processing-manager Alert-Consolidation'... [ OK ]
* Starting 'event-processing-manager Alert-Consolidation'... [ OK ]
Update complete.
```

Ok

Repeat this process for each Independent SolutionPackBlock that can be updated before moving on to the next section.

Updating Blocks in SolutionPacks

Important: If you have installed or plan to install the Storage Compliance SolutionPack, follow the procedure in Appendix B before updating the Storage Compliance SolutionPack update.

Important: While updating independent and data collection SolutionPackBlocks that are installed on the collector hosts, ensure that the "Hostname or IP address to send data to" field in the data collection section is set to localhost:2020.

Note: The SolutionPacks for Isilon and NetApp require additional steps that are provided at the end of this section. Some of the steps need to be completed before updating these SolutionPacks, so refer to the additional steps before continuing.

To update Blocks in SolutionPacks:

1. In the ViPR SRM Centralized Management UI, navigate to **SolutionPacks** on the left hand panel. Make sure you are in the **SolutionPacks** section of the right-hand pane.

Welcome admin (logged as admin) C.M. - EMC M&R Wednesday, August 13, 2014

ONLINE UPDATE SOLUTIONPACK CENTER USER SETTINGS CONFIGURATION DOCUMENTATION

Installed SolutionPacks

SolutionPacks

List of all the available SolutionPacks with at least one SolutionPackBlock installed. SolutionPackBlocks shared between multiple SolutionPacks will be list as installed in all of them.

Show 10 entries Search:

Name	Family	Installed SolutionPackBlocks	Description
Brocade FC Switch	Storage	5	Easily understand Brocade FC Switch performance and availability metrics and alerts with the SolutionPack for Brocade FC Switch.
Cisco MDS/Nexus Switch	Storage	4	Easily understand Cisco MDS/Nexus Switch performance and availability metrics with the SolutionPack for Cisco MDS/Nexus Switch.
EMC Host Interface	Infrastructure	1	Obtain a global view of the performance of your physical host devices, as well as, the internal and external storage infrastructure associated to them with this SolutionPack through EMC Host Interface.
EMC M&R Health	Application	6	Monitor the health of your EMC M&R infrastructure with the SolutionPack for EMC M&R Health.
EMC ViPR	Storage	3	Maximize utilization of your EMC ViPR Software-Defined Storage Platform with the SolutionPack for EMC ViPR.
EMC VMAX	Storage	4	Identify issues quickly using real-time troubleshooting, trending and capacity planning reports with the SolutionPack for EMC VMAX.
EMC VNX	Storage	5	Gain a clear understanding of EMC VNX performance and availability metrics with the SolutionPack for EMC VNX.
EMC VPLEX	Storage	2	Gain insight regarding the health of your hardware and software based VPLEX platform with the SolutionPack for EMC VPLEX.
EMC XtremIO	Storage	2	Maximize utilization of your EMC XtremIO flash arrays with the SolutionPack for EMC XtremIO.
IBM SAN Volume Controller/Storwize	Storage	2	Maximize utilization of your IBM SAN Volume Controller (SVC) / Storwize environments with the SolutionPack for IBM SVC / Storwize.

Showing 1 to 10 of 16 entries

2. Each SolutionPack containing a SolutionPackBlock that can be updated will have a yellow star. Click the star to open the individual SolutionPack page.

https://support.emc.com

Show 10 entries Search:

Instance	SolutionPackBlock	Version	SolutionPack(s) Version	Server Distribution
emc-vmax	Alert Consolidation	3.0	3.0.2	lgld186.iss.emc.com - Primary Backend
emc-vmax	Data collection	3.0.2	3.0.2	lgld189.iss.emc.com - Collector
emc-vmax	Pre-configured alerts	3.0.2	3.0.2	lgld186.iss.emc.com - Primary Backend
emc-vmax	Reports	3.0.2	3.0.2	lgld185.iss.emc.com - Front End

Showing 1 to 4 of 4 entries

- For each SolutionPackBlock that requires update, click the yellow star and review the settings on the Update page
- Click **Update**. The progress of the update will be displayed in the update page. You can maximize this page to monitor the progress of the update. Once the update completes, a green checkmark will be displayed at the top of the page.



SolutionPack Update

EMC VMAX v3.5.1

Updating

▼

Reports

✓

```

[?] Install one new file with unknown name
? Which option should be applied? > 2
Installation complete.

Starting update of emc-vmax-reports emc-vmax from v3.0.2 to v3.5.1...
* Gathering information...
* Module found in '/opt/APG/Block/emc-vmax-reports/emc-vmax'.
* It will now be updated using 'emc-vmax-reports-3.5.1.pkg'.
* Unpacking files...
* Updating files... 100%
* 5 files have been updated.
* Finalizing update...
? Web-Service gateway hostname or IP address [localhost] > localhost
? Web-Service port number [48443] > 48443
? Web-Service username [admin] > admin
? Web-Service password [*****] > *****
? Web-Service Category [Tools] > Tools
? Web-Service Module [Administration-Tool] > Administration-Tool
? Web-Service Instance [Default] > Default
Update complete.

```

Ok

- Repeat this process for each SolutionPackBlock in each SolutionPack to be updated.
- Validate that all SolutionPackBlocks are updated by inspecting all of the rows in the SolutionPackBlock table.

Additional steps for the SolutionPack for EMC Isilon

The SolutionPack for EMC Isilon is not compatible with previous versions, so historical data will be lost. Complete the following steps to enable data collection with ViPR SRM 3.5.1.

To disable SNMP polling:

- Log in to `http://<Frontend IP address>:58080/centralized-management`
- Navigate to SolutionPacks > Storage > EMC Isilon.
- Click the warning icon next to Isilon SNMP Masks and delete the module.



4. Click the trash icon in the Reports row to delete the Reports block.
5. Log in to [http:// <Frontend IP address>:58080/device-discovery](http://<Frontend IP address>:58080/device-discovery).
6. Navigate to **Devices**.
7. Select the Isilon array and click the trash icon to delete the array.
8. Repeat for all Isilon arrays.

To install the new collector and switch from SNMP collection to collection via restful API, click **SOLUTIONPACK CENTER**, select EMC Isilon, and install the SolutionPack.

Note: In order for new data to display in the UI, three polling cycles must pass and the property-Store task must have run.

Additional steps for the SolutionPack for NetApp

Before updating the SolutionPack for NetApp to 3.5.1, delete the old metrics associated with NetApp Cluster-Mode:

1. Navigate to Administration > Modules > Management of Database Metrics.
2. Enter the filter expression as `mode=='Cluster-Mode' & source=='Netapp-v8-cli'`
3. Click **Query**.
4. Select all the metrics and delete them.

Checking the status of remote host services

Review that all of the 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:

1. Click the name of the service.
2. Click **Start**. If successful, the Service Status will change 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.

To reconfigure a SolutionPack:

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**.

Deleting the old version of the Default ReportPack

After the SolutionPack updates are complete, review your new reports. If you are satisfied, you can delete the old Default ReportPack. This will remove previously scheduled reports, template restrictions, and pre-generated reports.

Note: Some elements of the navigation in the left-hand pane will be duplicated until you delete the old ReportPack. (The new reports are the second set of reports in the tree.)

1. Login to <http://<Frontend IP address>:58080/APG/>.
2. Click **Administration**, and then click **ReportPacks** on the left-hand pane to access ReportPacks Management. The available ReportPacks are listed in the right-hand pane.
3. Delete the older version of Default ReportPack.
 - a. Select **Default ReportPack(old)** in the pane.
 - b. Delete this file.

ReportPack Modification: Default ReportPack(older) | Administration

This section allows the creation and modification of ReportPacks.

ReportPack Information

i This information is for administration purposes only. It will not be displayed in the user interface.

Name	Default ReportPack(older)
Version	3.1.1.0
Description	The default ReportPack, included with any Watch4net install.

Delete

Export

Save

Post upgrade alerting changes

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

Actions are in the following paths.

Linux: /opt/APG/Custom/WebApps-Resources/Default/actions/event-mgmt/linux

- o ack-event
- o releaseowner-event
- o takeowner-event
- o unack-event

Windows: Program Files\APG\Custom\WebApps-Resources\Default\actions\event-mgmt\windows

- o ack-event.cmd
- o releaseowner-event.cmd
- o takeowner-event.cmd
- o unack-event.cmd

For each file, replace 127.0.0.1 with the primary backend hostname. For example:

```
..\..\..\..\Tools/Generic-Event-Sender/Default/bin/send-event.cmd -h 127.0.0.1 -p 2042 -def
Source="%W4N_SOURCE%" -def Name="%W4N_EVENTNAME%" -def owner="%W4N_USER%" -def acknowledged="Yes" -def
ConsoleAction="Ack" -def eventtype="%W4N_EVENTTYPE%"
```

Alert-Consolidation configuration

1. Navigate to **Administration > Modules > Alerting** and click **Adapters** in the left-hand pane.
2. Click the Alert Consolidation Adapter row, and then click **Edit**.
3. In the Properties field, replace the following three attributes, and then click **Save**:
 - name with Name
 - openedat with OpenedAt
 - source with Source
4. Expand the **Alert definitions** node in the left-hand pane, and then click **Alert Consolidation Email Notification**.
5. Hover the mouse over the Mail circle, and then click the edit icon.
6. In the Message field, replace `PROP.'source'` with `PROP.'Source'`
7. In the Subject field, replace the existing content with the following:

```
Sev-PROP.'severity' PROP.'category' alert received for PROP.'devtype'-PROP.'device' is now  
PROP.'eventstate'
```
8. Click **OK**, and then click **Save**. If you have not previously added an alert notification definition, the New Definition window opens. If you have configured all of the parameters for this alert, click **Save and Enable**. If you have not configured all of the parameters, click **Save and Disable**.
9. Expand the **Alert definitions** node in the left-hand pane, and then click **Alert Consolidation Trap Notification**.
10. Hover the mouse over the SNMP Trap circle, and then click the edit icon.
11. In the Trap content field, replace the existing content with the following:

```
PROP.'id',PROP.'Name',PROP.'OpenedAt',PROP.'count',PROP.'eventstate',PROP.'Source',PROP.'parttype',PRO  
P.'part',PROP.'eventname',PROP.'parttypedisplayname',PROP.'partdisplayname',PROP.'eventdisplayname',PR  
OP.'fullmsg',PROP.'devtype',PROP.'device',PROP.'sourceip',PROP.'sourcedomainname',PROP.'sourceeventtyp  
e',PROP.'value',PROP.'active',PROP.'timestamp',PROP.'closedat',PROP.'duration',PROP.'lastchangedat',PR  
OP.'isroot',PROP.'isproblem',PROP.'acknowledged',PROP.'eventtype',PROP.'category',PROP.'eventtext',PRO  
P.'severity',PROP.'impact',PROP.'certainty',PROP.'inmaintenance',PROP.'troubleticketid',PROP.'owner',P  
ROP.'systemdefined1',PROP.'systemdefined2',PROP.'systemdefined3',PROP.'systemdefined4',PROP.'systemdef  
ined5',PROP.'userdefined1',PROP.'userdefined2',PROP.'userdefined3',PROP.'userdefined4',PROP.'userdefin  
ed5',PROP.'userdefined6',PROP.'userdefined7',PROP.'userdefined8',PROP.'userdefined9',PROP.'userdefined  
10',PROP.'userdefined11',PROP.'userdefined12',PROP.'userdefined13',PROP.'userdefined14',PROP.'userdefi  
ned15',PROP.'userdefined16',PROP.'userdefined17',PROP.'userdefined18',PROP.'userdefined19',PROP.'userd  
efined20'
```
12. Click **OK**, and then click **Save**. If you have not previously added an alert notification definition, the New Definition window opens. If you have configured all of the parameters for this alert, click **Save and Enable**. If you have not configured all of the parameters, click **Save and Disable**.

If you are upgrading from VIPR SRM 3.0, create two new alert templates.

To create the Default Alert email Template:

1. Click **Templates** in the left-hand pane, and then click the **Create a new element** icon in the upper-left corner of the left-hand pane.
2. Select **Action** from the Family drop-down menu.
3. Select **Mail** from the Group drop-down menu.
4. Select **Mail Action** from the Type drop-down menu.
5. Type "Default Alert email Template" in the Name field.
6. In the Subject Field, add the following content:

```
Sev-PROP.'severity' PROP.'category' alert received for PROP.'devtype'-PROP.'device' is now  
PROP.'eventstate'
```
7. In the Message field, add the following content:

```
An PROP.'eventstate' alert has been received with the following attributes:
```

```
Message: PROP.'fullmsg'  
Device: PROP.'device'  
Device Type: PROP.'devtype'  
Severity: PROP.'severity'  
Source: PROP.'Source'  
Source IP: PROP.'sourceip'  
Part Type: PROP.'parttype'  
Part: PROP.'part'  
Category: PROP.'category'
```

This is an auto-generated email. To change the notification settings, consult the site administrator.

8. Click **Create**.

To create the Default Alert Trap template:

1. Click **Templates** in the left-hand pane, and then click the **Create a new element** icon in the upper-left corner of the left-hand pane.
2. Select **Action** from the Family drop-down menu.
3. Select **SNMP Trap** from the Group drop-down menu.
4. Select **SNMP v1 Trap** from the Type drop-down menu.
5. Type "Default Alert Trap Template" in the Name field.
6. Type "2041" in the Port field.
7. Type "public" in the Community field.
8. Type "6" in the Generic ID field.
9. Type "1" in the Enterprise specific ID field.
10. In the Trap content field, add the following content:

```
PROP.'id',PROP.'Name',PROP.'OpenedAt',PROP.'count',PROP.'eventstate',PROP.'Source',PROP.'parttype',PROP.  
P.'part',PROP.'eventname',PROP.'parttypedisplayname',PROP.'partdisplayname',PROP.'eventdisplayname',PR  
OP.'fullmsg',PROP.'devtype',PROP.'device',PROP.'sourceip',PROP.'sourcedomainname',PROP.'sourceeventtyp  
e',PROP.'value',PROP.'active',PROP.'timestamp',PROP.'closedat',PROP.'duration',PROP.'lastchangedat',PR  
OP.'isroot',PROP.'isproblem',PROP.'acknowledged',PROP.'eventtype',PROP.'category',PROP.'eventtext',PRO  
P.'severity',PROP.'impact',PROP.'certainty',PROP.'inmaintenance',PROP.'troubleticketid',PROP.'owner',P  
ROP.'systemdefined1',PROP.'systemdefined2',PROP.'systemdefined3',PROP.'systemdefined4',PROP.'systemdef  
ined5',PROP.'userdefined1',PROP.'userdefined2',PROP.'userdefined3',PROP.'userdefined4',PROP.'userdefin  
ed5',PROP.'userdefined6',PROP.'userdefined7',PROP.'userdefined8',PROP.'userdefined9',PROP.'userdefined  
10',PROP.'userdefined11',PROP.'userdefined12',PROP.'userdefined13',PROP.'userdefined14',PROP.'userdefi  
ned15',PROP.'userdefined16',PROP.'userdefined17',PROP.'userdefined18',PROP.'userdefined19',PROP.'userdef  
efined20'
```

11. Click **Create**.

Upgrading the whatif_scenarios table

When you upgrade to ViPR SRM 3.5.1, you must manually upgrade the whatif_scenarios table in the MySQL database to add new columns. The what-if scenarios are used by the ScenarioBasedForecast formula. This formula extends a metric according to an extension mode and applies the what-if scenarios on the extended metric to modify its value.

If your MySQL server and frontend are not on the same host, copy the sql file from the frontend host to the host with the MySQL database:

1. Login to the frontend host and navigate to the /opt/APG/Tools/WhatIf-Scenario-CLI/Default/ddl directory.
2. Copy the WhatIfScenariosUpgrade63To64.sql file to the same path on the backend host. Create the necessary folder structure if the subfolders do not exist under the WhatIf-Scenario-CLI folder.

To upgrade the whatif_scenarios table:

1. Log in to MySQL on the backend host. For example:

Linux: /opt/APG/bin/mysql-client.sh

Windows: Program Files\APG\bin\mysql-client.cmd

2. Enter the username. (Default is apg)
3. Enter the database name. (Default is apg)
4. Enter the password (the default is watch4net). You will see the prompt "Welcome to the MySQL monitor."
5. To view the list of tables associated with the Events database, type these commands:

```
mysql> use events;
```

```
mysql> show tables;
```

6. Run the script. For example:

Linux: source /opt/APG/Tools/WhatIf-Scenario-CLI/Default/ddl/WhatIfScenariosUpgrade63To64.sql

Windows: C:\Program Files\APG\Tools\WhatIf-Scenario-CLI\Default\ddl\WhatIfScenariosUpgrade63To64.sql

The script adds the following columns to the table:

- devtype
- device
- parttype
- part

7. To verify that the columns have been added to the database, type the following command:

```
mysql> show columns from whatif_scenarios;
```

8. Login to the frontend host using root credentials.

9. Navigate to the following directory:

Linux: /opt/APG/Tools/WhatIf-Scenario-CLI/Default/conf

Windows: C:\Program Files\APG\Tools\WhatIf-Scenario-CLI\Default\conf

10. Edit the whatif-scenario-cli-conf.xml file. Replace "localhost" with the primary backend hostname.

```
<scenario-database>
<!-- Defines the connection to the master database for MySQL. -->
<datasource driverClassName="com.mysql.jdbc.Driver"
url="jdbc:mysql://localhost:53306/events?autoReconnect=true"
```

11. Save the file.

Adding blocks for alerts

EMC M&R Health SolutionPack

1. Go to **Centralized Management**, and then click **SOLUTIONPACK CENTER**.
2. Select the EMC M&R Health SolutionPack.
3. Install the Pre-configured alerts block on the alerting backend host (which is generally the primary backend host).

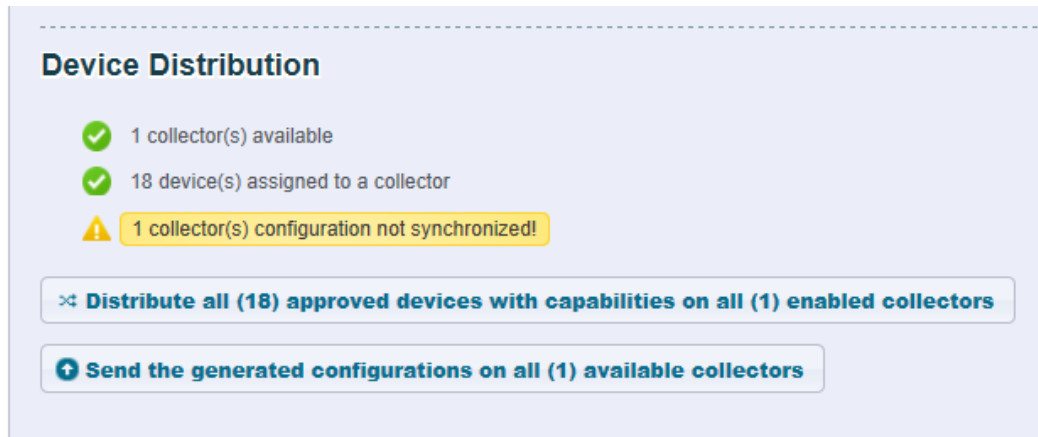
Xtreme IO SolutionPack

1. Go to **Centralized Management**, and then click **SOLUTIONPACK CENTER**.
2. Select the EMC XtremIO SolutionPack.
3. Install the Alert Consolidation block on the alerting backend host (which is generally the primary backend host).

Updating the SNMP Collections

To update the SNMP collectors and synchronize the configuration:

1. Log into the device discovery web interface at
`http://<Frontend IP address>:58080/device-discovery`
Note: On the Administration Dashboard, Device Discovery has been renamed SNMP Device Discovery.
2. 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."



3. If any of the collectors are not synchronized, click the **Distribute all approved devices...** button.
4. 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.

Note: In order for new data to display in the UI, three polling cycles must pass and the property-Store task must have run.

Configuring virus-scanning software (Windows)

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.

Validating the environment

Verify the post-upgrade operational status

- 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.
- Look for broken links — Resolve any issues or document them for later follow up.
- Validate that End-to-End topology is working — Resolve any issues.

Note: The SYMCLI version for VIPR SRM is 7.6.2.25. Connections to earlier versions of Solutions Enabler will generate a version incompatibility error when running Solutions Enabler proxy commands. The Solutions Enabler version on the server side must be updated to the latest version (from support.emc.com) by upgrading to the latest version of the EMC SMI-S Provider.

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

Appendix A

How to Export a Report Definition

Article Number:000185065 Version:3

Goal

To export an existing report's definition. This can be used to upload to another user's profile or for customizing reports while keeping the original report intact.

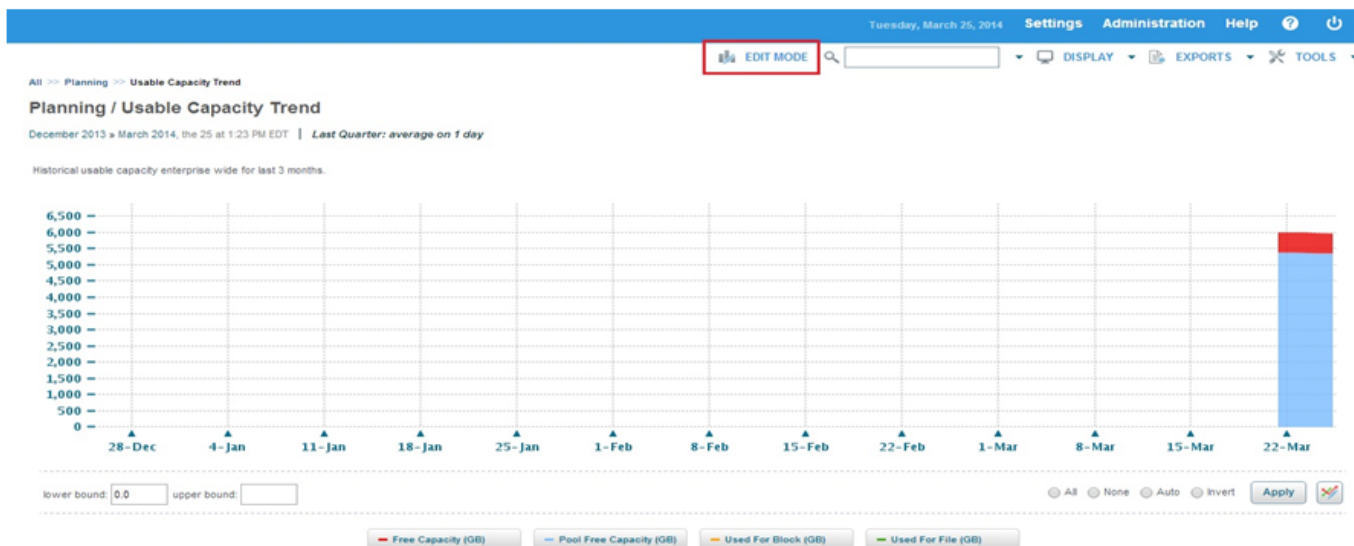
Environment

EMC SW: Watch4net

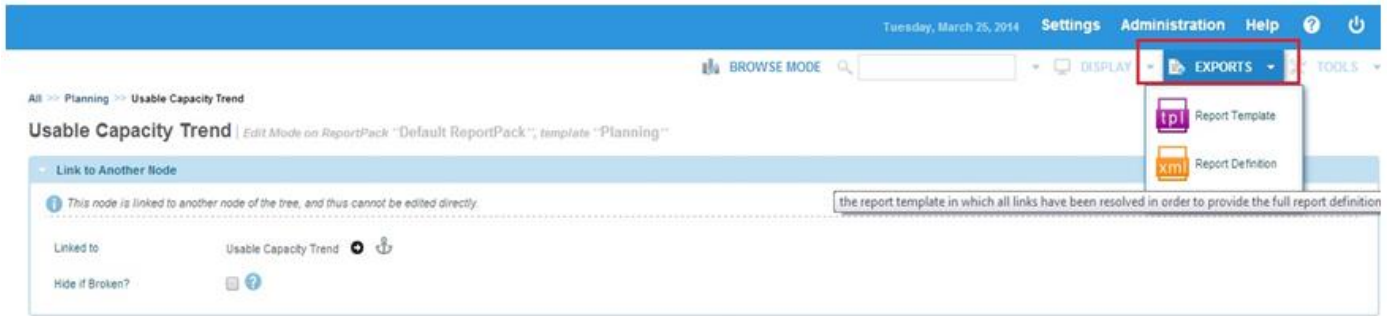
EMC SW: SRM

Resolution

1. Log into the account where the report is available.
2. Select the node or report on the left side and click on Edit Mode button.



- Click on Exports drop-down menu and select Report Definition as it will include all the relevant links in the report. This will download an xml template of the report.



How to Export and Import a report tree

Article Number:000185065 Version:3

Goal

This article explains how to export and import a report tree in Watch4Net & ViPR SRM

Issue

Created multiple custom reports in one environment and want to import the report tree into a new environment

Environment

EMC Software: Storage Resource Management Suite (SRM)

EMC Software: ViPR SRM

EMC Software: Watch4net

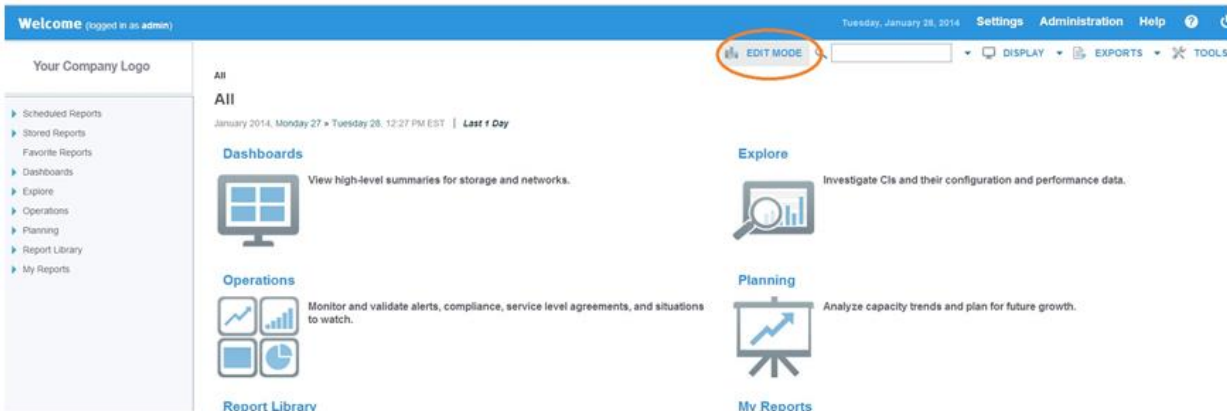
Resolution

- Start by exporting the tree you want to import in the new environment.
- Navigate to the report you want to export.
- Click on edit mode and EXPORTS -> Report Definition.

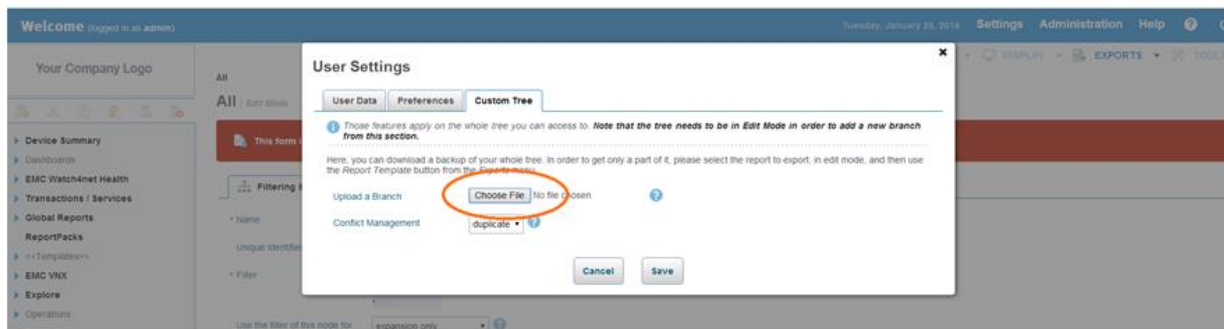


To import the report do the following:

1. Navigate where you want to import the tree and click Edit mode as highlighted below:



2. Click Settings. In the User Settings dialog, select the Custom Tree tab and click the Choose File button highlighted below:



3. Navigate to the location of the exported Report Definition file.
4. Upload the file and click Save.

Appendix B

Updating and reconfiguring the Storage Compliance SolutionPackBlocks

To update the SolutionPackBlocks in the Storage Compliance SolutionPack:

1. In the VIPR SRM Centralized Management UI, navigate to **SolutionPacks** on the left hand panel. Make sure you are in the **SolutionPacks** section of the right-hand pane. Select the Storage Compliance SolutionPack and update the following blocks:
 - Compliance Reports
 - Compliance Notifications
 - Compliance Backend
2. For the Compliance Backend SolutionPackBlock, reconfigure the SolutionPackBlock by clicking the reconfigure icon next to the SolutionPackBlock instance name.

Installing the Storage Compliance frontend module

To install the Storage Compliance frontend module:

1. Log in to <http://<Frontend IP address>:58080/centralized-management>.
2. Go to **Centralized Management**, and then click **SOLUTIONPACK CENTER**.
3. Select the **Storage Compliance** SolutionPack, and then click **Install**.
4. Install only the Compliance Frontend module.

Browse and Install SolutionPacks

SRM

SP

Storage Compliance v3.0.2u99

?

Important Note: Compliance SolutionPack contains EMC support matrix rules packaged along with it. Due to the large size of these rules, processing may take 3-5 minutes. Hence you might experience slow UI response time during this period.

Select the components to install

* Instance name

generic-compliance

?

●

Compliance Notifications

-Will not be installed-

?

⊙

●

Compliance Backend

-Will not be installed-

?

⊙

▶

Compliance Frontend

lgld164.lss.emc.com - Front End

?

✓

●

Compliance Reports

-Will not be installed-

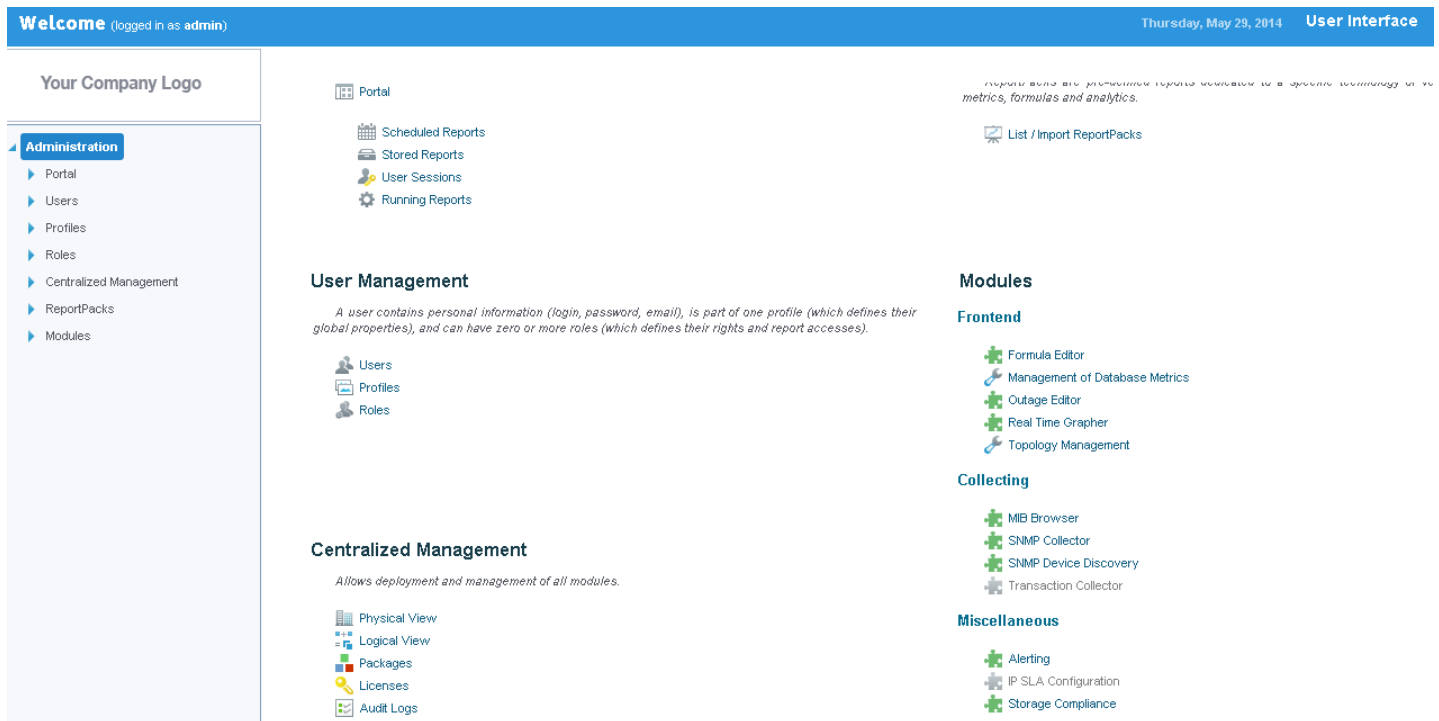
?

⊙

Back

Next

The Storage Compliance link will now be visible in Administration view.



Configuring files in Linux deployments

To update the APG configuration files on the frontend:

1. Log in to the frontend appliance as root user.
2. Navigate to the `/opt/APG/Web-Applications/Compliance-Frontend/compliance-frontend/conf/update-script` folder.
3. Make the `compliance-update.sh` script executable:

```
chmod +x compliance-update.sh
```
4. Run the `./compliance-update.sh` script. Provide passwords for the root and apg database users when prompted. The default password is `watch4net`. If you have changed the default password, provide it here.
5. Restart the Tomcat service:

```
#cd <APG-ROOT>\bin
#./manage-modules.sh service restart tomcat Default
```

Now when you click the **Storage Compliance** link in the Administration view, the compliance link will launch.

Review the Tomcat logs to ensure that the steps and edits described in this section have been completed correctly. You can also ensure that the changes are working correctly by verifying that the View Policies report is not blank:

1. Log in to `http://<Frontend IP address>:58080/APG`.
2. Navigate to **All > Operations > Compliance > Storage Compliance > View Policies**.
3. Verify that the policies configured before the update are displayed here and that this report is not blank.

You can now continue with the rest of the update steps.

Configuring files in Windows deployments

To update the APG configuration files on the frontend appliance:

1. Log in to the frontend appliance.
2. Navigate to the <APG folder>\Tools\Frontend-Report-Generator\Default\conf directory.
3. Edit the report-generation-config.xml file. Include the datasource entries below in between the <database> tag. Replace <PrimaryBackEndIP> with the host name hosting the compliance database and <APGDBPassword> with the "apg" database user password.

```
<datasource id="FLOW-COMPLIANCE-POLICY:{ mapping=FLOW-COMPLIANCE-POLICY.xml, table=policy }"
driverClassName="com.mysql.jdbc.Driver"
url="jdbc:mysql://<PrimaryBackEndIP>:53306/compliance?autoReconnect=true&tinyInttisBit=false"
username="apg" password="<APGDBPassword>" maxActive="30" maxIdle="5" validationQuery="SELECT 1"
testOnBorrow="false" testWhileIdle="true" timeBetweenEvictionRunsMillis="10000"
minEvictableIdleTimeMillis="60000" maxWait="10000" removeAbandoned="true" removeAbandonedTimeout="60"
logAbandoned="true"/>
<datasource id="FLOW-COMPLIANCE-RULE:{ mapping=FLOW-COMPLIANCE-RULE.xml, table=rule }"
driverClassName="com.mysql.jdbc.Driver" url="jdbc:mysql://
<PrimaryBackEndIP>:53306/compliance?autoReconnect=true&tinyInttisBit=false" username="apg"
password="<APGDBPassword>" maxActive="30" maxIdle="5" validationQuery="SELECT 1" testOnBorrow="false"
testWhileIdle="true" timeBetweenEvictionRunsMillis="10000" minEvictableIdleTimeMillis="60000"
maxWait="10000" removeAbandoned="true" removeAbandonedTimeout="60" logAbandoned="true"/>
<datasource id="FLOW-COMPLIANCE-CONFIGCHANGE:{ mapping=FLOW-COMPLIANCE-CONFIGCHANGE.xml,
table=config_change }" driverClassName="com.mysql.jdbc.Driver" url="jdbc:mysql://
<PrimaryBackEndIP>:53306/compliance?autoReconnect=true&tinyInttisBit=false" username="apg"
password="<APGDBPassword>" maxActive="30" maxIdle="5" validationQuery="SELECT 1" testOnBorrow="false"
testWhileIdle="true" timeBetweenEvictionRunsMillis="10000" minEvictableIdleTimeMillis="60000"
maxWait="10000" removeAbandoned="true" removeAbandonedTimeout="60" logAbandoned="true"/>
```

4. Browse to <APG-ROOT>\Web-Servers\Tomcat\Default\conf\Catalina\localhost directory and edit the APG.xml file with the following ResourceLink tags:

```
<ResourceLink name="jdbc/FLOW-COMPLIANCE-POLICY:{ mapping=FLOW-COMPLIANCE-POLICY.xml, table=policy }"
global="jdbc/FLOW-COMPLIANCE" type="javax.sql.DataSource" />
<ResourceLink name="jdbc/FLOW-COMPLIANCE-RULE:{ mapping=FLOW-COMPLIANCE-RULE.xml, table=rule }"
global="jdbc/FLOW-COMPLIANCE" type="javax.sql.DataSource" />
<ResourceLink name="jdbc/FLOW-COMPLIANCE-CONFIGCHANGE:{ mapping=FLOW-COMPLIANCE-CONFIGCHANGE.xml,
table=config_change }" global="jdbc/FLOW-COMPLIANCE" type="javax.sql.DataSource" />
```

Update the compliance-frontend.xml file on the server where Tomcat is running:

1. Navigate to the /opt/APG/Web-Servers/Tomcat/Default/conf/Catalina/localhost directory and edit the compliance-frontend.xml file.
2. There are three entries that must be changed from "localhost" to the hostname of the primary backend. For example:

```
<Resource name="manager/ComplianceManager" auth="Container"
type="com.emc.srm.base.compliance.jmx.ComplianceManagerFactory"
factory="org.apache.naming.factory.BeanFactory" user="admin" pass="changeme"
url="service:jmx:rmi:///jndi/rmi://localhost:52755/jmxrmi" />
<Resource name="manager/ComplianceESMManager" auth="Container"
type="com.emc.srm.base.compliance.jmx.ComplianceManagerFactory"
factory="org.apache.naming.factory.BeanFactory" user="admin" pass="changeme"
url="service:jmx:rmi:///jndi/rmi://localhost:52755/jmxrmi" />
<Resource name="manager/CompliancePolicyTemplateManager" auth="Container"
type="com.emc.srm.base.compliance.jmx.ComplianceManagerFactory"
factory="org.apache.naming.factory.BeanFactory" user="admin" pass="changeme"
url="service:jmx:rmi:///jndi/rmi://localhost:52755/jmxrmi" />
```

- Restart the Tomcat service:

```
#cd <APG-ROOT>\bin
#./manage-modules.sh service restart tomcat Default
```

Now when you click the **Storage Compliance** link in the Administration view, the compliance link will launch.

Review the Tomcat logs to ensure that the steps and edits described in this section have been completed correctly. You can also ensure that the changes are working correctly by verifying that the View Policies report is not blank:

- Log in to `http://<Frontend IP address>:58080/APG`.
- Navigate to **All > Operations > Compliance > Storage Compliance > View Policies**.
- Verify that the policies configured before the update are displayed here and that this report is not blank.

Creating new scopes

As part of the upgrade, you must create new scopes to validate the newly added policies.

- Log in to `http://<Frontend IP address>:58080/compliance-frontend`.
- Click **Policy and Rules Management**.
- Create new scopes as listed in the following table:

Policy	New Scope	Criteria
VPLEX Configuration	All VPLEX Clusters	devtype='VirtualStorage'
ViPR Configuration	All ViPR Virtual Data Centers	devtype='Host' & parttype ='Tenant'
Array Configuration	NetApp Array	devtype='UnifiedArray'

For example, to create a new scope named “All VPLEX Clusters” for the VPLEX Configuration policy:

- On the Policy and Management page, right-click **VPLEX Configuration** and click **Edit**.
- Click the **Scope** tab, and then click **Create Scope**.
- In the Name field, type All VPLEX Clusters.
- In the Criteria field, type `devtype='VirtualStorage'`
- Click **Save**.