EMC® Service Assurance Suite

Version 9.5

Installation and Configuration Guide for EMC M&R

302-003-644

REV 02

EMC²

Copyright © 2015-2017 Dell Inc. or its subsidiaries All rights reserved.

Published December 2017

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

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

Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

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

CONTENTS

Figures 7

Tables 9

Chapter 1 **Installing Using the Binary Installer** 11
Installation options for a standard installation 12
General requirements 12
Linux requirements 12
Installing EMC M&R platform on UNIX 13
Configuring the user process limits for a Linux installation 14
Installing EMC M&R platform on Windows Server 15
Configuring virus-scanning software 15
Logging in to the user interface 16
Set default navigation style 16
Connecting to Centralized Management 17
Confirming settings for the first time 17
Installing the health collectors 17
Installing a SolutionPack 19
Verifying that the services are running 19
Troubleshooting service start-up problems on UNIX 19
Troubleshooting service start-up problems on Windows 19

Chapter 2 **Using the Binary Installer to Scaleout the Environment** 21
Installation options for a standard installation 22
General requirements 22
Linux requirements 23
Server requirements 23
Installing the basic binary deployment with four hosts 23
Configuring the hosts 24
Installing and configuring the Primary Backend hosts 24
Installing and configuring the Additional Backend hosts 25
Installing and configuring the Frontend host 28
Installing and starting the collector 32
Configuring the load balancer arbiter 32
Configuring Load Balancer Connectors, generic-snmp, and generic-rsc 34
Logging in to the user interface 35
Set default navigation style 35
Connecting to Centralized Management 36
Confirming settings for the first time 36
Installing the health collectors 36
Installing a SolutionPack 38
Editing new actions scripts 38
Verifying that the services are running 38
Troubleshooting service start-up problems on UNIX 38
Troubleshooting service start-up problems on Windows 39

Chapter 3 **Installing and Configuring Elastic Search with M&R 6.8u2** 41

Overview 42
Installing and configuring Elastic Search 42

Chapter 4 Licensing 45
Licensing Operations 46
Trial licenses 46
License duration 46
License purchase 46
Log in with administrator credentials 47
View license information 47
Upload a new license file 48
Delete licenses 48
Synchronize licenses on multiple hosts 49
Troubleshooting licensing problems 49
Permanent license stops working after host reconfiguration 49
Users are locked out 50
Module does not start or has no license 52

Chapter 5 Upgrading from 6.5u4 onwards to 6.8u2 53
Overview 54
Required tools 54
Required credentials 54
Verifying and documenting the current status of the environment 54
Saving the Java certificates file 55
Importing Java certificates 56
Checks for the SolutionPack for Physical Hosts 56
Updating WinRM URL prefixes 56
Deleting backup schedules and scheduled reports from the DPA server 57
Updating the Centralized Management module 58
Upgrading the system 60
Restoring the Java certificates file 63

Chapter 6 Upgrading through CLI 65
Preparing for the upgrade of binary installations in Linux deployments 66
Updating core modules in a Linux environment 67
Preparing for the upgrade of binary installations in Windows deployments 68
Updating core modules in a Windows environment 69

Chapter 7 Post Upgrade Tasks 71
Performing the post upgrade tasks 72

Chapter 8 Updating SolutionPacks and Other Components 73
Overview 74
Upgrading all SolutionPacks and other components 74
Updating SolutionPacks and other components 76
Adding new components 78
Updating components distributed in package (.pkg) files 78

Chapter 9 Automating the Download of Updates 79
Online Update overview 80

Configuring server settings for online updates..... 80
Enabling the online update task..... 80
Running the online update task manually.....81
Online Update Status..... 81
Online Update History..... 83
Disabling the online update task.....83

Chapter 10 Uninstallation 85
Overview..... 86
Stopping EMC M&R platform services on a UNIX server..... 86
Uninstalling EMC M&R platform from a UNIX server..... 86
Stopping EMC M&R platform services on a Windows server..... 86
Uninstalling EMC M&R platform from a Windows server.....87
Uninstalling a SolutionPack.....87

Chapter 11 Reverting HTTPS Mode to HTTP Mode for M&R 6.8u2 Installation 89
How to revert HTTPS mode to HTTP mode for M&R 6.8u2 installation.....90

Appendix A Telnet and Socket Interface Ports 91
Telnet and socket interface ports for each backend.....92

Appendix B SolutionPack Ports 93
SolutionPack Port Details.....94

Appendix C SolutionPack Reconfiguration Fields 97
SolutionPack Reconfiguration Fields..... 98

Appendix D Restoring Modules to their Previous Version 101
Restoring modules workflow.....102
Listing restorable modules..... 102
Restoring modules..... 103
manage-modules.sh restore command.....104
Starting the EMC M&R platform services from the command line.....105
Starting the EMC M&R platform services on Windows.....106

FIGURES

1 SolutionPack update incompatible file messages..... 76
2 Online Update Status..... 81
3 Online Update Status with a major version update detected..... 82

TABLES

1 Installation Options..... 12
2 Installation Options..... 22
3 Required Server Resources..... 23
4 Host-id commands..... 50
5 Install license commands..... 51
6 Restart tomcat commands..... 51
7 SolutionPack Reconfiguration Fields..... 98

CHAPTER 1

Installing Using the Binary Installer

This chapter includes the following topics:

- Installation options for a standard installation 12
- General requirements 12
- Linux requirements 12
- Installing EMC M&R platform on UNIX 13
- Installing EMC M&R platform on Windows Server 15
- Logging in to the user interface 16
- Connecting to Centralized Management 17
- Confirming settings for the first time 17
- Installing the health collectors 17
- Installing a SolutionPack 19
- Verifying that the services are running 19

Installation options for a standard installation

Learn how to install the platform using a binary installation package.

The platform infrastructure consists of the following types of hosts:

- Frontend host
- Backend host
- Collector host
- All-In-One (recommended for POCs and testing only)

The MySQL version included with the product is 5.7.17 MySQL Community Server (GPL). The Elastic Search version included with the product is 5.2.

Table 1 Installation Options

	Default
Linux Installation Options	[D]efault
Windows Installation Options	Default Modules

General requirements

These requirements are for a minimal deployment. In a production environment, the requirements will vary depending on the provisioned load, and you must include careful planning and sizing before beginning the deployment.

The environment must meet the following requirements:

- 64 bit operating system (Linux or Windows)
- 32 GB RAM
- 600 GB hard disk
- 4 CPUs
- Forward and Reverse IP and DNS lookups must work on each server

Note

The following sections use Linux commands and directories as examples. For Windows, use `.cmd` instead of `.sh`, and `/` instead of `\` for directories.

Linux requirements

The environment must meet the following requirements. Make adjustments to the host before continuing.

- `/tmp` folder larger than 2.5 GB
- SWAP file should be at least equal to the RAM size
- On CentOs or RedHat-like Linux, the SELinux should be disabled or reconfigured Refer to *EMC M&R Installation and Configuration Guide* for OS support.

- The graphical desktop environment is not required
- On some Linux distributions:
  - MySQL server requires libaio1, libaio-dev, or libaio to start
  - The installation process requires unzip
  - On system restart the apg services may not start

Installing EMC M&R platform on UNIX

You can install the EMC M&R platform on supported UNIX hosts. This procedure specifically uses the Linux installation procedure as an example.

Before you begin

- When you install EMC M&R platform on a UNIX server, assign executable permissions to the installation script.
- Ensure that you have a login with root privileges to run the installer.
- Download the installation file from https://support.emc.com, and place it in a temporary location on the server.

Procedure

1. Log in to the server as root.
2. Change the permissions of the installer.

   For example:

   ```
   chmod +x <file_name>.sh
   ```

3. Run the installer from the directory.

   For example:

   ```
   ./<file_name>.sh
   ```

4. Read and accept the End User License Agreement.
5. Accept the default installation directory of `/opt/APG` or type another location.
6. Accept the default user account name of **apg** or type another name.
7. Accept the default location of service scripts of `/etc/init.d` or type another location.
8. Accept the default base directory of `/etc` for runlevel scripts or type another base directory.
9. Depending on the host purpose, select one of the following options:

Option	Description
Default	Installs recommended modules available in the binary installation package. You can use this option on a single host, which enables it to serve as a Frontend, Backend and Collector host. To customize this host further, manually add or remove specific modules.
Frontend	Installs web services and front end applications.
Backend	Installs the database and backend services.

Option	Description
Collector	Installs base modules to perform data collection and enrichment.
Minimal	Installs the minimal modules required for any host type. To customize this host further, manually add specific modules. You may also use this option to install and configure additional Backend Hosts.

Configuring the user process limits for a Linux installation

Increase the user process limits for the apg user account to a maximum of 65536. This modification enables services to open 65536 files and 65536 processes when needed. This step is required for proper functioning of the core software.

Before you begin

- Make sure you have a login with root privileges.
- The core software installed on a server running Red Hat Enterprise Linux 6/7, CentOS Linux 6/7, or any other supported Linux operating systems.

Procedure

1. Open the `/etc/security/limits.conf` file.
2. Add the following lines for the user.

   In this example, the user is `apg`.

   ```
   apg   hard  nofile  65536
   apg   soft  nofile  65536
   apg   hard  nproc   65536
   apg   soft  nproc   65536
   ```

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

   ```
   su apg -c 'ulimit -n -u'
   ```

   Following is the output:

   ```
   open files                      (-n) 65536
   max user processes              (-u) 65536
   ```

5. In the `opt/APG/bin/apg.properties` file, edit the hostname to a FQDN host name.
6. To restart the services, type the following commands from the `bin` directory of the installation:

   ```
   ./manage-modules.sh service stop all
   ```

   ```
   ./manage-modules.sh service start all
   ```

Installing EMC M&R platform on Windows Server

You can install the EMC M&R platform on supported Windows Server hosts.

Before you begin

- Ensure that you have a login with system administrator privileges to run the installer.
- Download the installation file from https://support.emc.com, and place it in a temporary location on the server.

Procedure

1. Double-click the .exe file.
2. Click **Next** on the **Welcome** screen.
3. Read and accept the End User License Agreement. Click **I Agree**.
4. Select the Destination Folder:
   a. Change the drive to a Windows non-root drive.
   b. Maintain the default folder structure (`Program Files\APG`).
   c. Click **Next**.
5. Depending on the host purpose, select one of the following options:

Option	Description
Recommended Modules	Installs all recommended modules available in the binary installation package. You can use this option on a single host, which enables it to serve as a Frontend, Backend and Collector host. To customize this host further, manually add or remove specific modules.
Frontend Modules	Installs web services and front end applications.
Backend Modules	Installs the database and backend services.
Collector Modules	Installs base modules to perform data collection and enrichment.
Base Installation	Installs the minimal modules required for any host type. To customize this host further, manually add specific modules. You may also use this option to install and configure Additional Backend Hosts.

6. Click **Install**.
7. When the installation is complete, click **Next**.
8. To close the installer, click **Finish**.

Configuring virus-scanning software

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 directory used to store your MySQL table data (such as `C:\Program Files\APG\Databases\MySQL\Default\data`). 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.

Logging in to the user interface

Log in to the user interface to use and edit reports, manage users, and customize the interface to meet your needs

Procedure

1. Open a browser and type the following URL:

   `https://<Frontend-hostname>:58443/APG`

   Note

   M&R 6.8u2 is installed by default in the HTTPS mode. To revert to HTTP mode for M&R 6.8u2 installation, refer to Reverting HTTPS Mode to HTTP Mode for M&R 6.8u2 Installation on page 89. It is recommended to use HTTPS mode.

2. Type the login credentials.

   The default username is `admin`. The default password is `changeme`.

3. Click **Sign In**.

   Note

   You are automatically logged off after four hours.

Set default navigation style

The navigation style controls the look and feel of the left navigation column in the reporting interface.

This procedure sets the global default navigation style. Users can override the global default style for their user account on **Profile** > **View Profile** > **Preferences**.

Procedure

1. Click **Administration** > **Portal**.
2. Click the **Default Display** tab.
3. In **Navigation Style**, make a selection.

   Use tree navigation: The navigation column is a hierarchical tree of report names.

4. Click **Save**.

   Note

   For the default navigation style, the Use tree navigation setting is recommended for the SolutionPacks for the 9.5 release. For procedure to change the preferences from icon based to tree based, refer to the dedicated SolutionPack articles.

Connecting to Centralized Management

Connect to the server so that you can access Centralized Management to install and administer SolutionPacks.

Centralized Management is one of the multiple web applications available in EMC M&R platform.

Procedure

1. Open a browser.
2. Type **`https://<serverIP:port>/centralized-management`**.

   The *serverIP* is the fully qualified hostname or IP address of the server where the EMC M&R platform frontend runs.

   The *port* is the port number of the server.

   Example:

   ```
   https://myHost.emc.com:58443/centralized-management
   ```

3. Log in.
   a. Default username is **`admin`**.
   b. Default password is **`changeme`**.
   c. Click **Sign In**.

After you finish

You are automatically logged off after four hours.

Confirming settings for the first time

After you first log in with administrator credentials for EMC M&R platform, you must confirm the configuration settings for the server.

Procedure

- Upon first login, the Server Configuration page opens automatically. Modify the references to localhost in the WS Gateway URL to the DNS name of the server.
- To accept the predefined values for the server, click **Save**.

  Blank fields must remain blank.

Installing the health collectors

Learn how to install the health collectors. Each server should have a health collector to monitor and report its state.

Before you begin

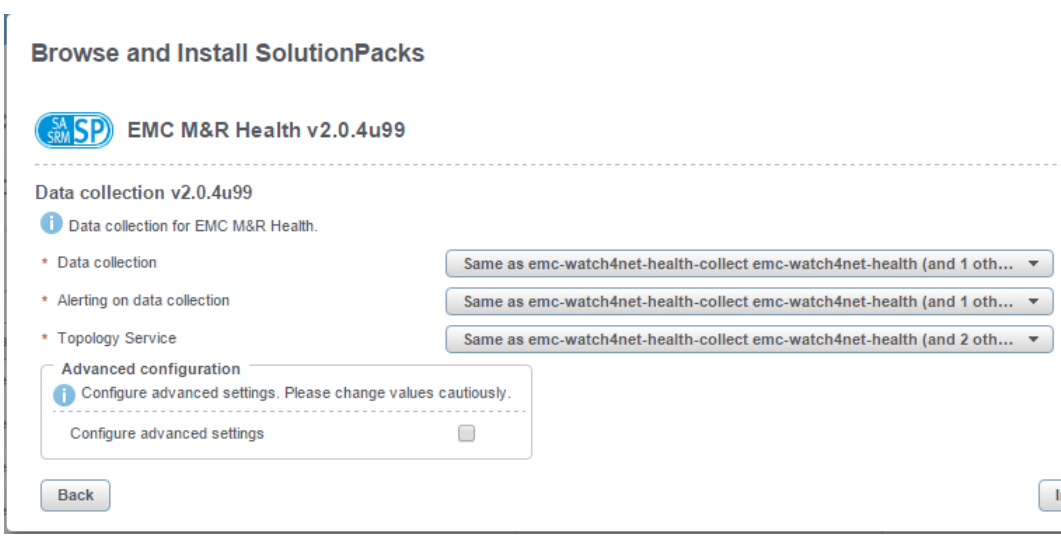
The Health Collector on the primary backend must point to the local LBA and its port. In this installation, the port is 2020.

The first installation of the SolutionPack will install the Health Reports on the frontend server.

Procedure

1. Log in to the Centralized Management UI.
2. Open SolutionPack Center and select EMC M&R Health.
3. Click **Install**.
4. On the Select the **Components to Install** window:
   a. Install Pre-configured alerts and the Events block where the primary backend is located.
   b. Install the Data collection block on every host by repeating the installation procedure for each host.
   c. Install Reports on the frontend.

5. On the **Data Collection** window:
   a. Data collection is the local LBC on port 2020.
   b. Alerting is on the primary backend.
   c. Topology host and gateway is on the primary backend



Installing a SolutionPack

To install the SolutionPack, use the SolutionPack portal, see *Service Assurance Suite SolutionPack Articles* for more information.

The entire list of SolutionPacks are mentioned in *Service Assurance Suite SolutionPack Articles* guide.

Verifying that the services are running

Verify that the services are running on each host by obtaining the status.

Before you begin

Ensure that you have a login with root, APG, or system administrator privileges. The user apg is the account that the application uses instead of root.

Procedure

1. Type the command for your operating system from the `bin` directory of the installation:

Operating system	Command
UNIX	`manage-modules.sh service status all`
Windows	`manage-modules.cmd service status all`

2. Verify that each service has a status of running in the output.

Troubleshooting service start-up problems on UNIX

Check the log files when services do not start.

Before you begin

Ensure that you have logged in with root to check the log files.

Procedure

- The default path is `/opt/APG/`.

  The list of available log files will vary depending on the type of server (Frontend, Backend, or Collector).

```
Databases/MySQL/Default/data/[SERVER NAME].err
Backends/Alerting-Backend/Default/logs/alerting-0-0.log
Backends/APG-Backend/Default/logs/cache-0-0.log
Collecting/Collector-Manager/Default/logs/collecting-0-0.log
Web-Servers/Tomcat/Default/logs/service.log
Tools/Task-Scheduler/Default/logs/scheduler-0-0.log
Tools/Webservice-Gateway/Default/logs/gateway-0-0.log
```

Troubleshooting service start-up problems on Windows

Check the log files when services do not start.

Before you begin

Ensure that you have logged in with system administrator credentials to check the log files.

Procedure

- Look for log files in these `C:\Program Files\APG` directory paths.

  The list of available log files will vary depending on the type of server (Frontend, Backend, or Collector).

```
Databases\MySQL\Default\data\[SERVER NAME].err.
Backends\Alerting-Backend\Default\logs\alerting-0-0.log
Backends\APG-Backend\Default\logs\cache-0-0.log
Collecting\Collector-Manager\Default\logs\collecting-0-0.log
Web-Servers\Tomcat\Default\logs\service.log
Tools\Task-Scheduler\Default\logs\scheduler-0-0.log
Tools\Webservice-Gateway\Default\logs\gateway-0-0.log
```

CHAPTER 2

Using the Binary Installer to Scaleout the Environment

This chapter includes the following topics:

- Installation options for a standard installation 22
- General requirements 22
- Linux requirements 23
- Server requirements 23
- Installing the basic binary deployment with four hosts 23
- Configuring the hosts 24
- Installing and configuring the Primary Backend hosts 24
- Installing and configuring the Additional Backend hosts 25
- Installing and configuring the Frontend host 28
- Installing and starting the collector 32
- Configuring the load balancer arbiter 32
- Configuring Load Balancer Connectors, generic-snmp, and generic-rsc 34
- Logging in to the user interface 35
- Connecting to Centralized Management 36
- Confirming settings for the first time 36
- Installing the health collectors 36
- Installing a SolutionPack 38
- Editing new actions scripts 38
- Verifying that the services are running 38

Installation options for a standard installation

Learn how to install the platform using a binary installation package.

The platform infrastructure consists of the following types of hosts:

- Frontend host
- Backend hosts (Primary Backend and Additional Backend)
- Collector host

You can only have one Primary Backend host. You can add Additional Backend hosts with up to four Time-Series databases on each Additional Backend host.

The MySQL version included with the product is 5.7.17 MySQL Community Server (GPL).

Table 2 Installation Options

	Frontend	**Primary Backend**	**Additional Backend**	**Collector**
Linux Installation Options	[f]rontend	[b]ackend	[m]inimal	[c]ollector
Windows Installation Options	Frontend Modules	Backend Modules	Base Installation (with none of the modules selected)	Collector Modules

General requirements

These requirements are for a minimal deployment. In a production environment, the requirements will vary depending on the provisioned load, and you must include careful planning and sizing before beginning the deployment.

The environment must meet the following requirements:

- 64 bit operating system (Linux or Windows)
- 16 to 24 GB RAM for each host
- Frontend – 16 GB RAM, 320 GB disk storage
- Backends – 24 GB RAM, disk storage is determined by the sizing
- Additional backend –16 GB RAM, disk storage is determined by the sizing
- Collectors – 16 GB RAM, 130+ GB disk storage
- 4 CPUs per host
- Forward and Reverse IP and DNS lookups must work on each server

Note

The following sections use Linux commands and directories as examples. For Windows, use `.cmd` instead of `.sh`, and `/` instead of `\` for directories.

Linux requirements

The environment must meet the following requirements. Make adjustments to the host before continuing.

- `/tmp` folder larger than 2.5 GB
- SWAP file should be at least equal to the RAM size
- On CentOs or RedHat-like Linux, the SELinux should be disabled or reconfigured Refer to *EMC M&R Installation and Configuration Guide* for OS support.
- The graphical desktop environment is not required
- On some Linux distributions:
  - MySQL server requires libaio1, libaio-dev, or libaio to start
  - The installation process requires unzip
  - On system restart the apg services may not start

Server requirements

The environment must meet certain server requirements.

The environment must meet the following requirements:

- Each server should have a health collector to monitor and report its state
- The Load Balancer Arbiter should be installed on the primary backend
- The Load Balancer Connector should be installed on each of the collector hosts

Table 3 Required Server Resources

Type of Server	RAM (GB)	HDD (GB)
Backend default installation with Load Balancer Arbiter	24	150
Additional backend with 4 backend instances	16	150
Frontend	16	150
Collector	16	150

Installing the basic binary deployment with four hosts

Install the system components on four hosts to establish the basic four host solution.

Install the product using the binary installation package as described in Installing Using the Binary Installer on page 11.

Procedure

- Install the software for the following types of hosts:
  - 1 frontend host

- 2 backend hosts
- 1 collector host

Configuring the hosts

You must configure the hosts in a particular order.

Configure the four hosts in the following order:

Procedure

1. Select one of the backend hosts to be the primary backend.
2. Select the other backend host to be the additional backend.
3. Select a host to be the frontend.
4. Select a host to be the collector.

Installing and configuring the Primary Backend hosts

Learn how to install and configure the Primary Backend hosts.

Before you begin

- Identify the host you want to configure as the Primary Backend host.
- Identify the hosts you want to configure as the Frontend, Collectors, and Additional Backends.
- Minimum System Requirements:
  - CPU: 4
  - Memory: 24 GB
  - Disk Space: 150 GB HDD

Procedure

1. Start the installation as described in Installing EMC M&R platform on UNIX on page 13.
2. When you are prompted to select the installation type, choose the "backend" option and complete the installation.
3. Configure the user process limits as described in Configuring the user process limits for a Linux installation on page 14.
4. Set the Maximum Java Heap Size in the `/opt/APG/Backends/Topology-Service/Default/conf/unix-service.properties` file to 6144 MB.
5. Reconfigure the topology service to commit the change.

   ```
   /opt/APG/bin/manage-modules.sh service update topology-service
   ```

   ```
   /opt/APG/bin/manage-modules.sh service start topology-service
   ```

6. Allow remote access to the databases.

   On the primary backend, replace *<FQDN-New-Server>* with localhost, Collectors, Backends and Frontend hosts Fully Qualified Domain names:

   ```
   <APG>/bin/mysql-command-runner.sh -c <APG>/Tools/MySQL-
   Maintenance-Tool/Default/conf/mysql-root-mysql.xml -Q "GRANT
   ```

```
ALL PRIVILEGES ON \`compliance\`.* TO 'apg'@'<FQDN-New-
Server>' IDENTIFIED BY 'watch4net';"
<APG>/bin/mysql-command-runner.sh -c <APG>/Tools/MySQL-
Maintenance-Tool/Default/conf/mysql-root-mysql.xml -Q "GRANT
ALL PRIVILEGES ON \`apg\`.* TO 'apg'@'<FQDN-New-Server>'
IDENTIFIED BY 'watch4net';"
<APG>/bin/mysql-command-runner.sh -c <APG>/Tools/MySQL-
Maintenance-Tool/Default/conf/mysql-root-mysql.xml -Q "GRANT
ALL PRIVILEGES ON \`events\`.* TO 'apg'@'<FQDN-New-Server>'
IDENTIFIED BY 'watch4net';"
<APG>/bin/mysql-command-runner.sh -c <APG>/Tools/MySQL-
Maintenance-Tool/Default/conf/mysql-root-mysql.xml -Q "GRANT
ALL PRIVILEGES ON \`master\`.* TO 'apg'@'<FQDN-New-Server>'
IDENTIFIED BY 'watch4net';"
<APG>/bin/mysql-command-runner.sh -c <APG>/Tools/MySQL-
Maintenance-Tool/Default/conf/mysql-root-mysql.xml -Q "GRANT
ALL PRIVILEGES ON \`topology\`.* TO 'apg'@'<FQDN-New-Server>'
IDENTIFIED BY 'watch4net';"
```

7. Start the backend services:

Option	Description
Linux	manage-module.sh service start all
Windows	manage-module.cmd service start all

8. Verify that all of the services are running:

Option	Description
Linux	manage-module.sh service status all
Windows	manage-module.cmd service status all

Installing and configuring the Additional Backend hosts

Learn how to install and configure the additional backend host. This step is optional. To configure an additional backend host, choose the **Minimal** option when installing the software.

Before you begin

- Identify the host you want to configure as the Additional Backend host.
- Identify the hosts you want to configure as the Frontend, Collectors, and Additional Backends.
- Minimum System Requirements:
  - 64-bit Operating System
  - CPU: 4
  - Memory: 16 GB
  - Disk Space: 150 GB HDD

Procedure

1. Start the installation as described in Installing EMC M&R platform on UNIX on page 13.
2. When you are prompted to select the installation type, choose the "minimal" option and complete the installation.

3. Configure the user process limits as described in Configuring the user process limits for a Linux installation on page 14.

   At this stage, you will have a host with minimal components installed. Customize this host further by manually adding the modules required for additional backend.

4. Install the MySQL module:

```
/opt/APG/bin/manage-modules.sh install mysql <Instance-Name>
```

   Answer "no" when asked to install the databases packaged with the application.

5. Start the MySQL process:

```
/opt/APG/bin/manage-modules.sh service start mysql
```

6. Install the maintenance tool for each new backend by running the following command for each apg database. Answer **yes** to each question.

```
/opt/APG/bin/manage-modules.sh install mysql-maintenance-
tool apg[1..n]
```

7. Create four new databases with the names apg1, apg2, apg3, and apg4 by running the following command four times (replacing the [1..n] with a number):

```
/opt/APG/bin/mysql-command-runner-apg[1..n].sh -
c /opt/APG/Tools/MySQLMaintenance-Tool/apg[1..n]/conf/
mysql-root-mysql.xml -Q "create database apg[1..n]";
```

   Note

   EMC recommends keeping the default APG timeseries database.

8. Register the apg databases to the APG Backend server by running the following command for each apg database. Answer **Yes** to each question.

```
/opt/APG/bin/manage-modules.sh install backend apg[1..n]
```

   Note

   The MySQL Storage Adapter uses in-memory temporary tables. You should set the max_heap_table_size in …/APG/Databases/MySQL/Default/my.cnf (Unix) or my.ini (Windows) to at least 128M (depending on your installation size) to avoid errors.

9. Allow remote access to the new databases. Each database must be configured to be accessible from other hosts. Repeat the following command replacing <HostName> with each collector, frontend, primary backend and localhost:

```
/opt/APG/bin/mysql-command-runner.sh -c /opt/APG/Tools/MySQL-
Maintenance-
Tool/<apg[1..n]>/conf/mysql-root-mysql.xml -Q "GRANT ALL
PRIVILEGES ON *.* TO 'apg'@'<HostName>' IDENTIFIED BY
PASSWORD'*FA71926E39A02D4DA4843003DF34BEADE3920AF3'"
```

The <HOST NAME> must be the DNS name resolved from the nslookup <CLIENT IP> command executed from the Additional Backend host.

10. Find all of the XML files in the `/opt/APG/Backends/APG-Backend/apg[1..n]` folders that contains JDBS connection URLs.

    For example: …`localhost:53306/apg`

11. Update the URLs to include the correct APG database numbers.

    For example: …`localhost:53306/apg[1..n]`

    To complete this step with a script (for Linux), run this command:

```
find /opt/APG/Backends/APG-Backend/apg[1..n] -name '*.xml' |
xargs
sed -i "s|jdbc:mysql://localhost:53306/apg|\\0[1..n]|"
```

12. Set the Telnet interface port for each new apg database.

    The Telnet interface port for each new apg database must be different. The default port is 2001. To change the port numbers, edit the following file and set the port numbers to 2[1..n]01: `/opt/APG/Backends/APG-Backend/apg[1..n]/conf/telnetinterface.xml`

    Refer to Telnet and Socket Interface Ports on page 91 for guidelines.

13. Set the socket interface port for each new apg database.

    The socket interface port for each new apg database must be different. The default port is 2000. To change the port numbers, edit the following files and set the port numbers to 2[1..n]00:`/opt/APG/Backends/APG-Backend/apg[1..n]/conf/Negotiating-socket-interface.xml`

14. Point the MySQL maintenance tools to the new local databases.

    Edit the following files and replace "apg" with the correct name, for example, "apg1."`/opt/APG/Tools/MySQL-Maintenance-Tool/apg[1..n]/conf/mysql.xml`
    `/opt/APG/Tools/MySQL-Maintenance-Tool/apg[1..n]/conf/mysql-root-apg.xml`

    For example:

```
<url>jdbc:mysql://localhost:53306/apg1?autoReconnect=true</
url>
<!-- The username for database access. -->
<username>apg</username>
<!-- The password for database access. -->
<password>watch4net</password>
```

    To complete this step with a script (for Linux), run the following command:
    `find /opt/APG/Tools/MySQL-Maintenance-Tool/apg[1..n] -name '*.xml' | xargs sed -i "s|jdbc:mysql://localhost:53306/apg|\\0[1..n]|"`

15. Start the backend services:

Option	Description
Linux	manage-modules.sh service start all
Windows	manage-modules.cmd service start all

16. Verify that all the services are running:

Option	Description
Linux	manage-modules.sh service status all
Windows	manage-modules.cmd service status all

17. To complete the configuration of additional backends, reconfigure the Load Balancer Arbiter (LBA) as described in Configuring the load balancer arbiter on page 32 and add an entry for each of the apg backends.

    After the installation, you can reconfigure the backends and ports from **Centralized Management** > **SolutionPacks** > **Other Components**.

Installing and configuring the Frontend host

Learn how to install and configure the frontend host.

Before you begin

- Ensure that you have the details of the Backend host, Additional Backend hosts, and Collector hosts.
- Minimum System Requirements:
  - 64-bit Operating System
  - CPU: 4
  - Memory: 16 GB
  - Disk Space: 150 GB HDD

Procedure

1. Start the installation as described in Installing EMC M&R platform on UNIX on page 13.
2. When you are prompted to select the installation type, choose the "frontend" option and complete the installation.
3. Configure the user process limits as described in Configuring the user process limits for a Linux installation on page 14.
4. Set the connections that point to a local MySQL server to point to the primary backend. In the following files, locate all of the strings like `localhost:53306`, and replace the string `localhost` with the primary backend DNS name (it must be resolvable):
   - `/opt/APG/Web-Servers/Tomcat/Default/conf/server.xml`
   - `/opt/APG/Tools/Frontend-Report-Generator/Default/conf/report-generation-config.xml`
   - `/opt/APG/Tools/Administration-Tool/Default/conf/master-accessor-service-conf.xml`
   - `/opt/APG/Tools/WhatIf-Scenario-CLI/Default/conf/whatif-scenario-cli-conf.xml`

5. Set non-MySQL localhost connections to point to the new primary backend:
   a. Locate and replace the hostname in the strings `localhost:48443` in the following file:

      `/opt/APG/Web-Servers/Tomcat/Default/conf/Catalina/localhost/APG.xml`

   b. Locate and replace the hostname in the strings `localhost:52569` in the following file:

      `/opt/APG/Web-Servers/Tomcat/Default/conf/Catalina/localhost/alerting-frontend.xml`

   c. Locate and replace the hostname in the strings `localhost:52569` in the following file:

      `/opt/APG/Tools/Frontend-Report-Generator/Default/conf/report-generation-config.xml`

6. Increase the maximum memory that the Tomcat server can use by locating `memory.max=` in the `/opt/APG/Web-Servers/Tomcat/Default/conf/unix-service.properties` file and setting it to `memory.max=8192`.
7. Update the Tomcat service to apply the new memory settings:

```
#/opt/APG/bin/manage-modules.sh service update tomcat Default
```

8. Restart the Tomcat service and the webservice-gateway:

```
#/opt/APG/bin/manage-modules.sh service start tomcat Default
#/opt/APG/bin/manage-modules service.sh restart webservice-gateway Default
```

9. Execute the following command to check the list of database accessors that are in the frontend:

   `/opt/APG/bin/manage-resources.sh list`

   Wait for few minutes for the resources to be available.
10. Using a web browser, log in to Centralized Management on the frontend at `https://<frontend-host>:58443/centralized-management`.
    - User Name = admin
    - Password = changeme

    At the first login, the Servers Configuration page opens. Register the frontend host by updating the WS Gateway URL. Replace localhost with the FQDN of the frontend host and click **Save**.
11. Go to **Configuration** > **Servers**, and then click **Register a Server**. Register all of the APG servers that are up and running.

    Use the following settings:
    - Server HostName – the DNS name of the server
    - Gateway URL – `https://<server DNS name>:48443/`
    - User Name – admin

- Password – changeme

12. Click **Save**.
13. Once you have registered all of the servers, verify that they display in **Centralized Management** > **Physical Overview** without any error messages.
14. ResourceLinks for the timeseries database are now stored in the master database. To give access to the timeseries database on the primary backend and the additional backend, update the resources using the **manage-resources.sh** command:

```
#/opt/APG/bin/manage-modules.sh service restart all
#/opt/APG/bin/manage-resources.sh list (this will list all
the resources)
#/opt/APG/bin/manage-resources.sh get "dba/APG-DB"
```

a. Check the details of dba/APG-DB and update the connection URL to point to the primary backend host:

```
/opt/APG/bin/manage-resources.sh update dba/APG-DB '{
  "type": "jdbc",
  "datasource":   {
    "maxActive": "10",
    "maxIdle": "10",
    "validationQuery": "SELECT 1",
    "testOnBorrow": "false",
    "testWhileIdle": "true",
    "validationQueryTimeout": "5",
    "timeBetweenEvictionRunsMillis": "10000",
    "minEvictableIdleTimeMillis": "60000",
    "maxWait": "10000",
    "removeAbandoned": "true",
    "removeAbandonedTimeout": "60",
    "logAbandoned": "true",
    "driverClassName": "com.mysql.jdbc.Driver",
    "username": "apg",
    "password":
"{6230FED930DD59BEB1095D6801AA74E2FC23B2C8B76AFF6447D5C49B84
C4001FDF5B6441DF7CD5CB2B19D4A927C63934}",
    "url": "jdbc:mysql://<FQDN-Primary-Backend>:53306/apg?
autoReconnect=true&connectTimeout=20000&maxReconnects=2"
  },
  "settings": {"cachegrp": "DB"}
}'
```

b. Update the management resource for the data management tool to communicate with the backend:

```
/opt/APG/bin/manage-resources.sh update mgmt/APG-DB '{
  "type": "webservice",
  "connection":   {
    "disableSSLValidation": true,
    "url": "https://<FQDN-Primary-Backend>:48443/Backends/
APG-Backend/apg",
    "user": "admin",
    "password":
"{68951D237EABAFD17BD2F90B2029E51B9078C3968D27791E745EB38C2F
8E4B7B6351D632200618220667E25792D7E8894330B34886D638E3C3B938
56C94998B9}"
```

```
    }
  }'
```

c. Update all of the remaining resources in the same way.

15. Create resources for each of the newly added APG databases on the Additional Backend with resources names such as dba/APG-DB[1..n] and mgmt./APG-DB[1..n]. Perform this operation every time a new additional backend host is added to the environment to scale-out backends.

    For example, to create a Database resource:

```
manage-resources.sh create dba/APG-DB[1..n] '{
    "type": "jdbc",
     "datasource":   {
     "maxActive": "10",
     "maxIdle": "10",
     "validationQuery": "SELECT 1",
     "testOnBorrow": "false",
     "testWhileIdle": "true",
     "validationQueryTimeout": "5",
     "timeBetweenEvictionRunsMillis": "10000",
     "minEvictableIdleTimeMillis": "60000",
     "maxWait": "10000",
     "removeAbandoned": "true",
     "removeAbandonedTimeout": "60",
     "logAbandoned": "true",
     "driverClassName": "com.mysql.jdbc.Driver",
     "username": "apg",
     "password":
"{6230FED930DD59BEB1095D6801AA74E2FC23B2C8B76AFF6447D5C49B84C4
001FDF5B6441DF7CD5CB2B19D4A927C63934}",
     "url": "jdbc:mysql://<FQDN-Additional-Backend>:53306/
apg[1..n]?
autoReconnect=true&connectTimeout=20000&maxReconnects=2"
   },
   "settings": {"cachegrp": "DB"}
 }'
```

To create a Management Resource:

```
manage-resources.sh update mgmt/APG-DB[1..n] '{
  "type": "webservice",
  "connection":   {
    "disableSSLValidation": true,
    "url": "https://<FQDN-Additional-Backend>:48443/Backends/
APG-Backend/apg[1..n]",
    "user": "admin",
    "password":
"{68951D237EABAFD17BD2F90B2029E51B9078C3968D27791E745EB38C2F8E
4B7B6351D632200618220667E25792D7E8894330B34886D638E3C3B93856C9
4998B9}"
  }
}'
```

Installing and starting the collector

Learn how to install and start the collector.

Procedure

1. Start the installation as described in Installing EMC M&R platform on UNIX on page 13.
2. When you are prompted to select the installation type, choose the "collector" option and complete the installation.
3. Configure the user process limits as described in Configuring the user process limits for a Linux installation on page 14.
4. Start the collector service:

   ```
   manage-modules service start all
   ```

Configuring the load balancer arbiter

Learn how to configure the load balancer arbiter from Centralized Management. Complete these steps every time a new backend host is added to the environment to scaleout backends.

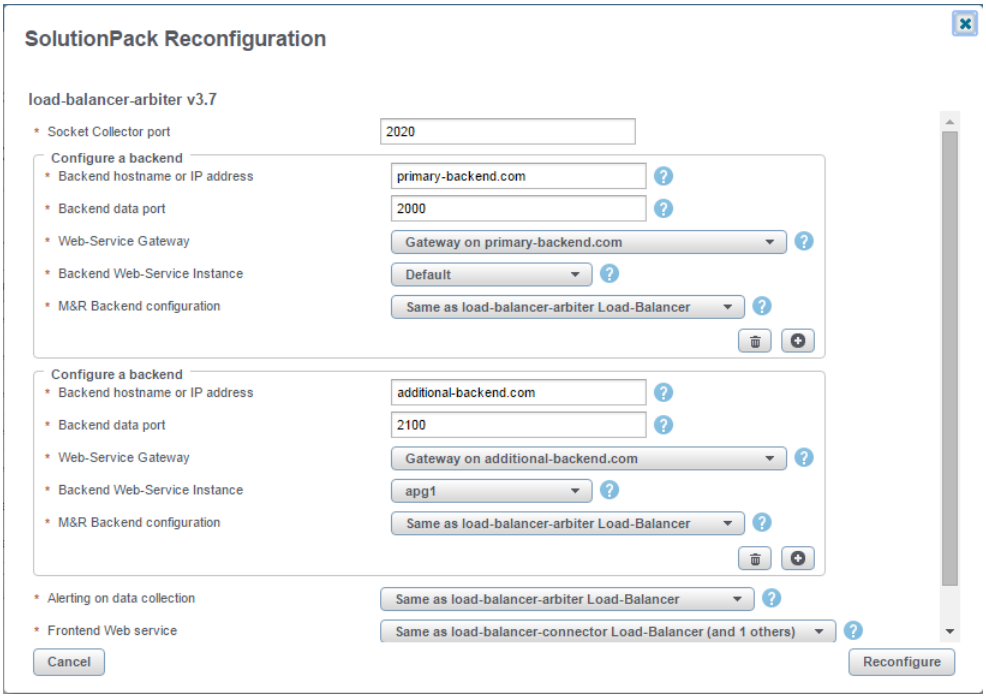
Before you begin

- The connection must point to the FQDN of the primary backend or additional backend host.
- The listening port must be 2020.

Procedure

1. Log in to Centralized Management at `https://<frontend-host>:58443/centralized-management`.
2. Navigate to **SolutionPacks** > **Other Components**.
3. Locate the load-balancer-arbiter component and click the **Reconfigure** button.
4. Click on the drop down against Arbiter configuration and select Add a new arbiter configuration
   a. Update the backend hostname with the DNS name of primary backend host.
   b. Change the Web-Service Gateway to the primary backend host.
   c. Update the backend database hostname with the DNS name of primary backend host.
5. Add a configuration for all the apg backends installed on the additional backend host. Complete this step whenever a new additional backend host is added to the environment to scale out backends.

   For example:



SolutionPack Reconfiguration Fields describes the values that you should enter for each field on the SolutionPack Reconfiguration page.

6. Click the + button and add an entry for each of the backend instances (apg1, apg2, apg3 and apg4) created on the additional backend host.
7. Provide the appropriate backend data port, web-service gateway, backend instance name, and DB connection details for each of the instances.
8. Modify the Alerting data collection section and provide the primary backend DNS name for Alerting Backend hostname.
9. Modify the Frontend Web service section and provide the frontend DNS name for Tomcat hostname.
10. Once everything is updated, click **Reconfigure**.
11. After you have setup the arbiter, check the logs under `/opt/APG/Collecting/Collector-Manager/Load-Balancer/logs` to see if all of the APG backend instances were correctly installed.

    For example:

```
# cat /opt/APG/Collecting/Collector-Manager/Load-Balancer/
logscollecting-0-0.log | grep "LoadFactorDecision::isReady"
INFO -- [2014-06-05 12:28:44 EDT] --
LoadFactorDecision::isReady(): Starting decision with current
load factor of:
INFO -- [2014-06-05 12:28:44 EDT] --
LoadFactorDecision::isReady(): Backend1 0.0/750000.0 (0.0)
INFO -- [2014-06-05 12:28:44 EDT] --
LoadFactorDecision::isReady(): Backend2 0.0/750000.0 (0.0)
INFO -- [2014-06-05 12:28:44 EDT] --
LoadFactorDecision::isReady(): Backend3 0.0/750000.0 (0.0)
INFO -- [2014-06-05 12:28:44 EDT] --
LoadFactorDecision::isReady(): Backend4 0.0/750000.0 (0.0)
INFO -- [2014-06-05 12:28:44 EDT] --
LoadFactorDecision::isReady(): Backend0 595.0/750000.0
(7.933333333333333E-4)
```

Configuring Load Balancer Connectors, generic-snmp, and generic-rsc

Learn how to configure Load Balancer Connectors (LBCs). Complete these steps every time a new collector host is added to the environment to scale-out collectors.

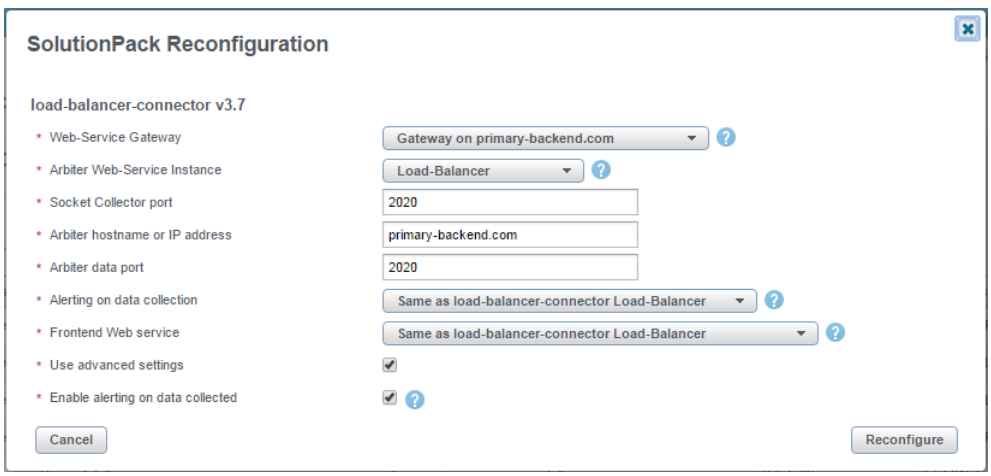
Before you begin

- The Load Balancer Arbiter is installed on the primary backend with the listener port of 2020.
- The LBCs are installed on all of the collector hosts.
- The LBC listens on port 2020 local on that collector server and communicates with the Load Balancer Arbiter on the primary backend also using port 2020.

Procedure

1. During the installation of the LBC, when the script asks for the `Web-Service gateway hostname or IP address [localhost]`, enter the DNS of the primary backend server where the arbiter is installed.
2. The collector server has the LBC installed by default, but you must reconfigured it to point it to the primary backend and its arbiter:
   a. In **Centralized Management** > **SolutionPacks** > **Other Components**, filter on the collector name, and click the **Reconfigure** button for the load-balancer-connector.
   b. Update all of the host names and gateway URLs so they point to the primary backend.
   c. Update the Alerting Backend hostname to Primary Backend host and 2010 port.
   d. Update the Frontend Web Service to point to the Frontend host.

      For example:



   e. generic-rsc is installed by default on the collector host. Click the **Reconfigure** button and update the Frontend Web Service to point to frontend host. Update the Topology service question by changing the host name and gateway to point to the primary backend host.

f. Click the **Reconfigure** button for generic-snmp. Update the Frontend Web service to point to frontend host. Update the Topology service question by changing the host name and gateway to point to primary backend host

Logging in to the user interface

Log in to the user interface to use and edit reports, manage users, and customize the interface to meet your needs

Procedure

1. Open a browser and type the following URL:

   `https://<Frontend-hostname>:58443/APG`

   Note

   M&R 6.8u2 is installed by default in the HTTPS mode. To revert to HTTP mode for M&R 6.8u2 installation, refer to Reverting HTTPS Mode to HTTP Mode for M&R 6.8u2 Installation on page 89. It is recommended to use HTTPS mode.

2. Type the login credentials.

   The default username is **`admin`**. The default password is **`changeme`**.

3. Click **Sign In**.

   Note

   You are automatically logged off after four hours.

Set default navigation style

The navigation style controls the look and feel of the left navigation column in the reporting interface.

This procedure sets the global default navigation style. Users can override the global default style for their user account on **Profile** > **View Profile** > **Preferences**.

Procedure

1. Click **Administration** > **Portal**.
2. Click the **Default Display** tab.
3. In **Navigation Style**, make a selection.

   Use tree navigation: The navigation column is a hierarchical tree of report names.

4. Click **Save**.

   Note

   For the default navigation style, the Use tree navigation setting is recommended for the SolutionPacks for the 9.5 release. For procedure to change the preferences from icon based to tree based, refer to the dedicated SolutionPack articles.

Connecting to Centralized Management

Connect to the server so that you can access Centralized Management to install and administer SolutionPacks.

Centralized Management is one of the multiple web applications available in EMC M&R platform.

Procedure

1. Open a browser.
2. Type **`https://<serverIP:port>/centralized-management`**.

   The *serverIP* is the fully qualified hostname or IP address of the server where the EMC M&R platform frontend runs.

   The *port* is the port number of the server.

   Example:

   ```
   https://myHost.emc.com:58443/centralized-management
   ```

3. Log in.
   a. Default username is **`admin`**.
   b. Default password is **`changeme`**.
   c. Click **Sign In**.

After you finish

You are automatically logged off after four hours.

Confirming settings for the first time

After you first log in with administrator credentials for EMC M&R platform, you must confirm the configuration settings for the server.

Procedure

- Upon first login, the Server Configuration page opens automatically. Modify the references to localhost in the WS Gateway URL to the DNS name of the server.
- To accept the predefined values for the server, click **Save**.

  Blank fields must remain blank.

Installing the health collectors

Learn how to install the health collectors. Each server should have a health collector to monitor and report its state.

Before you begin

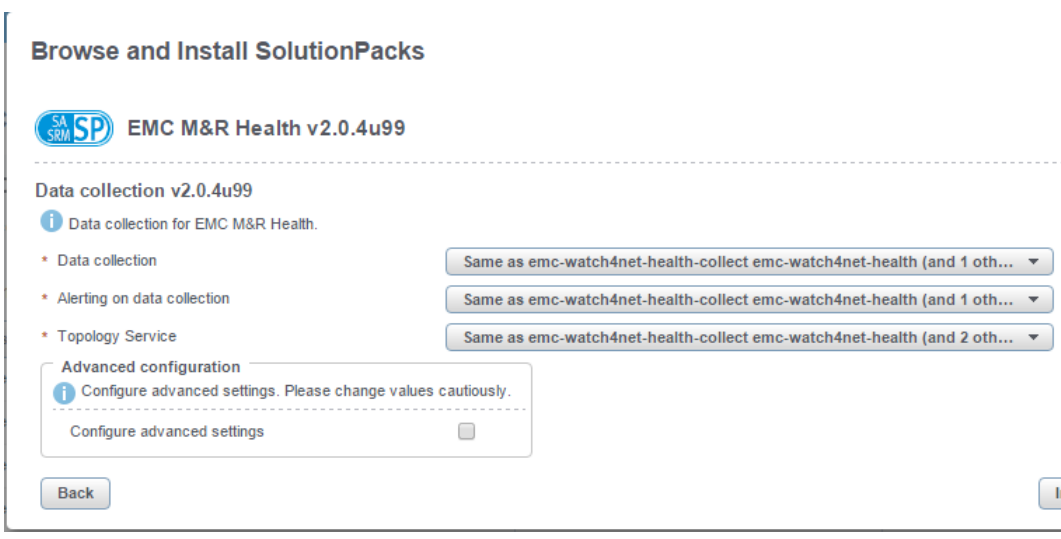
The Health Collector on the primary backend must point to the local LBA and its port. In this installation, the port is 2020.

The first installation of the SolutionPack will install the Health Reports on the frontend server.

Procedure

1. Log in to the Centralized Management UI.
2. Open SolutionPack Center and select EMC M&R Health.
3. Click **Install**.
4. On the Select the **Components to Install** window:
   a. Install Pre-configured alerts and the Events block where the primary backend is located.
   b. Install the Data collection block on every host by repeating the installation procedure for each host.
   c. Install Reports on the frontend.

5. On the **Data Collection** window:
   a. Data collection is the local LBC on port 2020.
   b. Alerting is on the primary backend.
   c. Topology host and gateway is on the primary backend



Installing a SolutionPack

To install the SolutionPack, use the SolutionPack portal, see *Service Assurance Suite SolutionPack Articles* for more information.

The entire list of SolutionPacks are mentioned in *Service Assurance Suite SolutionPack Articles* guide.

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`

Verifying that the services are running

Verify that the services are running on each host by obtaining the status.

Before you begin

Ensure that you have a login with root, APG, or system administrator privileges. The user apg is the account that the application uses instead of root.

Procedure

1. Type the command for your operating system from the `bin` directory of the installation:

Operating system	Command
UNIX	`manage-modules.sh service status all`
Windows	`manage-modules.cmd service status all`

2. Verify that each service has a status of running in the output.

Troubleshooting service start-up problems on UNIX

Check the log files when services do not start.

Before you begin

Ensure that you have logged in with root to check the log files.

Procedure

- The default path is `/opt/APG/`.

The list of available log files will vary depending on the type of server (Frontend, Backend, or Collector).

```
Databases/MySQL/Default/data/[SERVER NAME].err
Backends/Alerting-Backend/Default/logs/alerting-0-0.log
Backends/APG-Backend/Default/logs/cache-0-0.log
Collecting/Collector-Manager/Default/logs/collecting-0-0.log
Web-Servers/Tomcat/Default/logs/service.log
Tools/Task-Scheduler/Default/logs/scheduler-0-0.log
Tools/Webservice-Gateway/Default/logs/gateway-0-0.log
```

Troubleshooting service start-up problems on Windows

Check the log files when services do not start.

Before you begin

Ensure that you have logged in with system administrator credentials to check the log files.

Procedure

- Look for log files in these `C:\Program Files\APG` directory paths.

  The list of available log files will vary depending on the type of server (Frontend, Backend, or Collector).

```
Databases\MySQL\Default\data\[SERVER NAME].err.
Backends\Alerting-Backend\Default\logs\alerting-0-0.log
Backends\APG-Backend\Default\logs\cache-0-0.log
Collecting\Collector-Manager\Default\logs\collecting-0-0.log
Web-Servers\Tomcat\Default\logs\service.log
Tools\Task-Scheduler\Default\logs\scheduler-0-0.log
Tools\Webservice-Gateway\Default\logs\gateway-0-0.log
```

CHAPTER 3

Installing and Configuring Elastic Search with M&R 6.8u2

This chapter includes the following topics:

- Overview 42
- Installing and configuring Elastic Search 42

Overview

With the M&R 6.8u2 release, Elastic Search has been introduced as a new backend technology.

Installing Elastic Search on M&R platform is specific to some of the SolutionPacks. For installation, configuration, and upgrade instructions for each SolutionPack, refer to the *Service Assurance Suite SolutionPack Articles* guide.

Installing and configuring Elastic Search

To install and configure Elastic Search with M&R 6.8u2, complete the following steps:

Before you begin

- Perform M&R 6.8u2 installation successfully.
- Configure the Primary Backend hosts before Elastic Search configuration.

Procedure

1. Navigate to the `/opt/APG/bin/` directory.
2. Open the /etc/sysctl.conf file.
3. Add the following line:

   ```
   vm.max_map_count=262144
   ```

4. In the `/etc/security/limits.conf` file, add the following lines for the user.

   In this example, the user is `apg`.

   ```
   apg   hard  nofile  65536
   apg   soft  nofile  65536
   apg   hard  nproc   65536
   apg   soft  nproc   65536
   ```

5. Save the file.
6. To install the Elastic Search cluster package, type the following command:

   ```
   ./manage-modules.sh install elasticsearch-cluster
   ```

   When you are prompted for the IP address, provide the M&R host IP address. In the **more entries** option, select `no` unless Elastic Search needs to be configured in the cluster mode.

7. To verify the changes, type the following command:

   ```
   su apg -c 'ulimit -n -u'
   ```

   Following is the output:

   ```
   open files                      (-n) 65536
   max user processes              (-u) 65536
   ```

8. In the `/opt/APG/Databases/Elasticsearch/Default/conf/elasticsearch.yml` file, add the following entry:

```
bootstrap.seccomp: false
script.max_compilations_per_minute: 120
```

9. Restart Elastic Search server.

   Ensure that Elastic Search server is running.

CHAPTER 4

Licensing

This chapter includes the following topics:

- Licensing Operations 46
- Log in with administrator credentials 47
- View license information 47
- Upload a new license file 48
- Delete licenses 48
- Synchronize licenses on multiple hosts 49
- Troubleshooting licensing problems 49

Licensing Operations

Use Centralized Management user interface to perform licensing management operations.

These operations include uploading, verifying, deleting, and synchronizing licenses.

Trial licenses

Your software can include all trial licenses or a combination of permanent and trial licenses.

Licenses that you purchase are permanent. Other software comes with trial licenses.

Trial licenses let you test features in the UI and perform some initial configurations before full purchase. Trial licenses typically last for 30 days after the installation time. You cannot copy or regenerate a trial license in the product.

If all of your licenses are trial licenses, including the core software license that includes the Web Portal feature, the software can lock out all users from accessing the UI when the trial expires.

License duration

Permanent licenses do not expire. Trial licenses have expiration dates, typically 30 days after the installation date.

When trial licenses expire, module license checks fail and the modules stop working. If the Web Portal module fails, you cannot access the product.

Because the License Management UI operates behind the Web Portal module, you must upload your permanent license file or extended trials before the 30-day license for the core features expires. Otherwise, the UI locks and you cannot upload the license file.

License purchase

To convert a feature from a trial license into a permanently licensed feature, you need to purchase a license.

To initiate the purchase of a license for a SolutionPack, visit EMC Online Support using the following URL:

```
https://support.emc.com/servicecenter/createSR/
```

On the page that appears, submit a service request to EMC. Include the SolutionPack name that you want to purchase.

When all purchasing transactions are complete, EMC sends you instructions for downloading a regenerated license file for your site that includes the newly purchased software license. Download the file to a local server, and then follow instructions in Upload a new license file on page 48 to upload the new license file.

Note

Until the license is purchased and the new license file is obtained and uploaded, the SolutionPack is inoperable, unless the 30-day trial license is still in effect.

Log in with administrator credentials

You must have administrator credentials to perform license management operations.

Procedure

1. Access EMC M&R platform software by typing the following URL in a web browser:

   ```
   https://frontend-hostname:58443/centralized-management
   ```

   where *frontend-hostname* is the server where the frontend module is installed.

   The login page opens.
2. Log in with a user account that has administrator credentials.

   The Centralized Management UI opens to the Physical Overview page.
3. In the navigation tree in the left pane, click **Licenses Management**.

   The **Licenses Listing** page opens. Notice the **Upload** and **Synchronize** operational commands at the top of the page.

View license information

You can view license information in two ways. One method displays licenses by host. The other one shows a centralized view of all licenses.

Procedure

1. Log in with administrator credentials.
2. To view active licenses on a physical host, navigate to **Administration** > **Centralized Management** > **Physical Overview** > ***host-name***.
3. Click the **Licenses** tab.

   The Licenses tab displays active licenses on that host. It also indicates whether licenses are permanent or trial, the expiration date for trials, and additional license properties, if applicable.
4. To view a consolidated list of licenses for all hosts, and to perform license management operations, in the navigation tree in the left pane, click **Licenses Management**.

   The **Licenses Listing** page opens showing all licenses on all servers.
   Notice the ELMS permanent license, showing all features included in the license and the license serial number. Also notice the **Upload** and **Synchronize** commands at the top of the page.

   This table displays Information for ELMS licenses related to product name for the license, SWID (software ID), and serial numbers.

Upload a new license file

To add a new license to your system, such as a newly purchased SolutionPack license, upload a new license file.

Before you begin

1. Purchase the required licenses.
2. Download the new license file to a local server, as directed by EMC during the purchase process.

When you upload a license file, the new file affects all servers capable of using the licenses.

Procedure

1. Log in to the Centralized Management UI using the following URL:

   ```
   https://frontend-hostname:58443/centralized-management
   ```

2. In the navigation pane, select **Licenses Management**.
3. Click **Upload** at the top of the page.

   The License Upload dialog appears.
4. Click **Browse** and locate the new license file that you downloaded.
5. Click **OK**.

   The system extracts the licenses and displays them in the table on the Licenses Listing pane.
6. When the **License Upload Complete** dialog appears, click **OK**, and then click **Continue**.

   The new license automatically affects all servers capable of using the license.
7. Delete the trial licenses that correspond to newly licensed features, if any.

   To delete a trial license, see Delete licenses on page 48.

Delete licenses

You can select and delete specific licenses or delete all licenses. A delete action affects all servers that use the license.

After you install a permanent license, delete the trial licenses that are covered by the permanent license.

Procedure

1. Log in to the Centralized Management UI using the following URL:

   ```
   https://frontend-hostname:58443/centralized-management
   ```

2. In the navigation pane, select **Licenses Management**.
3. In the **Licenses Listing** table, select one or more license check boxes.

4. Click **Delete**.

   The **Delete** command appears below the table. It is dimmed until you select at least one license.

   The system deletes the selected license from all available servers.

Synchronize licenses on multiple hosts

The **Synchronize** action ensures that all remote hosts have licenses based on those available on the Centralized Management host.

Certain situations might cause licenses to become out of sync. For example, if a remote host is unavailable when you perform an upload or a delete operation, those operations would not be propagated to the offline server. Another example is if you add a new server to your configuration, the new server would need licensing information.

Procedure

1. Log in to the Centralized Management UI using the following URL:

   ```
   https://frontend-hostname:58443/centralized-management
   ```

2. In the navigation pane, select **Licenses Management**.
3. Click **Synchronize** at the top of the page.

   The system synchronizes the licenses on all remote hosts.

Troubleshooting licensing problems

You can resolve common licensing problems.

Permanent license stops working after host reconfiguration

If you change the configuration of a host, for example, by adding interfaces, removing interfaces, or changing the operating system, your permanent license might stop working. If your license does not work, obtain a new host ID and request a new permanent license.

Before you begin

Ensure that you have a login with root, APG, or system administrator privileges to perform this task. The user `apg` is the account that the application uses instead of root.

Procedure

1. Log in to the operating system command line on the host server.
2. To obtain the new host ID, run one of the following operating system commands:

Table 4 Host-id commands

Operating system	Command
UNIX	`/opt/APG/bin/manage-licenses.sh host-id`
Windows	`C:\Program Files\APG\bin\manage-licenses.cmd host-id`

The command output is the new host ID.

3. Copy the host ID information to the clipboard or to a text file.
4. To obtain the new license, go to the EMC support site using the following URL:

```
https://support.emc.com/servicecenter/createSR/
```

The **Create a Service Request** page opens.

5. Submit a service request to EMC, asking for a new permanent license file for a new host. Paste the new host ID into the request.
6. When EMC sends you the new license file, follow the procedure in Upload a new license file on page 48.

Users are locked out

If the license for the core software features expires, the system locks users out of the UI.

To recover from this scenario:

1. Obtain a license file with permanent licenses.
2. Install the new license file from the command line. Install license file from the command line on page 50
3. Restart the Tomcat service. See Restart Tomcat service on page 51.
4. Log in and perform the following tasks:
   a. Reinstall the new license file from the Centralized Management UI.
   b. Delete the expired trial licenses.

   See Reinstall license file and delete trial licenses after lockout on page 51.

Install license file from the command line

You can install a license file from the command line if you are locked out of the UI. Always use the UI unless you are locked out.

Before you begin

- Ensure that you have an OS account with root, APG, or system administrator privileges. The application uses the `apg` account, rather than root.
- Acquire a new license file from EMC and download it to a local server. To request a new license file, create a Service Request on EMC Online Support.

Procedure

1. Log in to the server where the core software is installed.
2. Copy the new, valid license file to this same server. The file is a `.zip` file.

3. At the OS command line, navigate to the `bin` directory.
4. Install the license file using one of the following commands appropriate to your OS:

Table 5 Install license commands

Operating System	Command
UNIX	`./manage-licenses.sh install download_path/license.zip`
Windows	`manage-licenses.cmd install download_path\license.zip`

Note

The command installs the license file on this server only.

Restart Tomcat service

If the Web Portal license expires, you might need to restart the Tomcat service.

Before you begin

1. Install the new license file using operating system commands.
2. Ensure that the library search path is correct on the server that is the host for the core software. This requirement applies to the `libstdc` package on a Solaris server and the `libaio` package on a LINUX server.

It is only necessary to restart the Tomcat service when the license for a web application, such as the Web Portal, expires.

Procedure

1. Log in to the server where the core software is installed.
2. At the OS command line, navigate to the `bin` directory.
3. Run one of the following commands appropriate to the OS:

Table 6 Restart tomcat commands

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

The command output starts like this:

```
* Starting 'tomcat Default'... [ OK ]
```

Reinstall license file and delete trial licenses after lockout

After you install a permanent license file on the command line, you need to reinstall that file using the Centralized Management UI to make the license visible in the UI and

available for distribution to other remote servers. You also need to delete the expired trial licenses.

Procedure

1. Open a browser and log in to Centralized Management using the following URL:

   ```
   https://frontend-hostname:58443/centralized-management
   ```

2. In the navigation pane, select **Licenses Management**.
3. Click **Upload** at the top of the page.

   The License Upload dialog appears.
4. Click **Browse** and locate the new license file.
5. Click **OK**.

   The system extracts the licenses and displays them in the table on the Licenses Listing pane.
6. When the **License Upload Complete** dialog appears, click **OK**, and then click **Continue**.

   The new license automatically affects all servers capable of using the license.
7. In the License Listing table, select all expired trial licenses by clicking the appropriate check boxes.
8. Click **Delete.**

   The **Delete** command appears at the bottom of the page, below the table of licenses.

   The delete action automatically affects all available servers.

Module does not start or has no license

If a component reports that it has no license or does not start, verify the licenses on the physical host.

Procedure

1. Log in to the Centralized Management UI using the following URL:

   ```
   https://frontend-hostname:58443/centralized-management
   ```

2. Navigate to **Physical hosts** > ***host-name*** > **Licenses**.

   The page shows all licenses active on this local host.
3. Inspect the **Expiration** column for the termination date of each license.

CHAPTER 5

Upgrading from 6.5u4 onwards to 6.8u2

This chapter includes the following topics:

- Overview 54
- Required tools 54
- Required credentials 54
- Verifying and documenting the current status of the environment 54
- Saving the Java certificates file 55
- Importing Java certificates 56
- Checks for the SolutionPack for Physical Hosts 56
- Updating WinRM URL prefixes 56
- Deleting backup schedules and scheduled reports from the DPA server 57
- Updating the Centralized Management module 58
- Upgrading the system 60
- Restoring the Java certificates file 63

Overview

The Service Assurance Suite 9.5 release supports EMC M&R 6.8u2. This chapter applies to binary-only installations of 6.5u4, 6.6u1, or 6.7u1 upgrading to 6.8u2.

Note

Upgrading from 6.5u4 to 6.8u2 using the Centralized Management GUI is a two-step process. In this case, you need to upgrade first from 6.5u4 to 6.7u1, and then to 6.8u2. For more information, refer to Updating the Centralized Management module on page 58. However, if you are upgrading using the CLI, you can directly upgrade from 6.5u4 to 6.8u2.

If you want to update a single SolutionPack to receive the benefit of a required fix or feature, refer to Updating SolutionPacks and Other Components on page 73.

Ensure your environment meets the operating system support requirements described in the *EMC M&R 6.8u2 Release Notes*.

- 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. The article, *How to Set Up SAM, EMC M&R, and the SolutionPack for EMC Smarts* provide more information.

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 servers
- ESX server credentials (if appropriate)

Verifying and documenting the current status of the environment

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

Before you begin

Refer to the *EMC Service Assurance Suite SolutionPack Performance and Scalability Guidelines* for details about determining configuration size.

Note

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

Procedure

1. Look for blank reports and graphs. Determine if there are any blank reports caused by collection errors. Resolve any issues or document them for later follow up.
2. Look for broken links and resolve any issues or document them for later follow up.
3. Validate that end-to-end topology is working. Resolve any issues.
4. Review the existing backend and databases. Check **Report Library** > **EMC M&R Health** > **Stress** > **Components** > **Backends** and **Report Library** > **EMC M&R Health** > **Stress** > **Components** > **Databases**.
   - Check backend thresholds to verify that you have room to accommodate new sizing
   - Add additional backends and databases as required.
   - Refer to the *Watch4net Database Split* v1.2 document for help if you need to manually move data to redistribute the metrics.
5. Review and document any customizations.

   For example:
   - Polling intervals
   - Timeout values

After you finish

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

Saving the Java certificates file

If you are upgrading from EMC M&R 6.5u4, 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 6.6u1, the EMC M&R platform software provides 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 "Importing custom certificates into the JRE" section of the *EMC M&R Security Configuration Guide*. 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`.

Importing Java certificates

If you are upgrading from EMC M&R 6.6u1/6.7u1, you may make use of a new method for importing certificates into the trust store for use in LDAP, device discovery, or other secure communication. If you are leveraging SSL communications and have previously imported certificates into the product to enable this, you may need to perform a one-time operation to re-import them using this new method. Once you have done this, the import will persist across future upgrades.

Note

If you have already imported the certificates using this method, you do not need to import them again. This procedure will validate that you have done so.

Procedure

1. Check to see if there are any certificate files located at `<APG_HOME>/Java/Sun-JRE/<version>/customcerts`. If so, your certificates will be automatically migrated during the update, and you can skip the next step.
2. If there are not any certificate files in this location, then any certificates you previously added manually will not persist across the upgrade to EMC M&R 6.8u2. You should perform a one-time re-import of the certificates file as described in the "Importing custom certificates into the JRE" section of the *EMC M&R Security Configuration Guide*. For moving self-signed certificate to CA certificate, refer to "Configuring HTTPS with certificates signed by a certificate authority" section of the *EMC M&R Security Configuration Guide*.

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`.

Updating WinRM URL prefixes

Prior to release of EMC M&R 6.6u1, if you discovered Windows hosts using Custom WinRM URL prefixes, you had to add the custom URL prefix to module.properties of

Generic-RSC Collector Manager. These changes are no longer applicable after the upgrade.

Procedure

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

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

Updating the Centralized Management module

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

Note

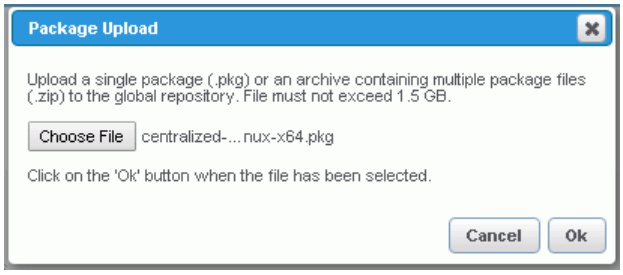
This section is only required if you are upgrading a binary-only installation of EMC M&R 6.5u4.

Procedure

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

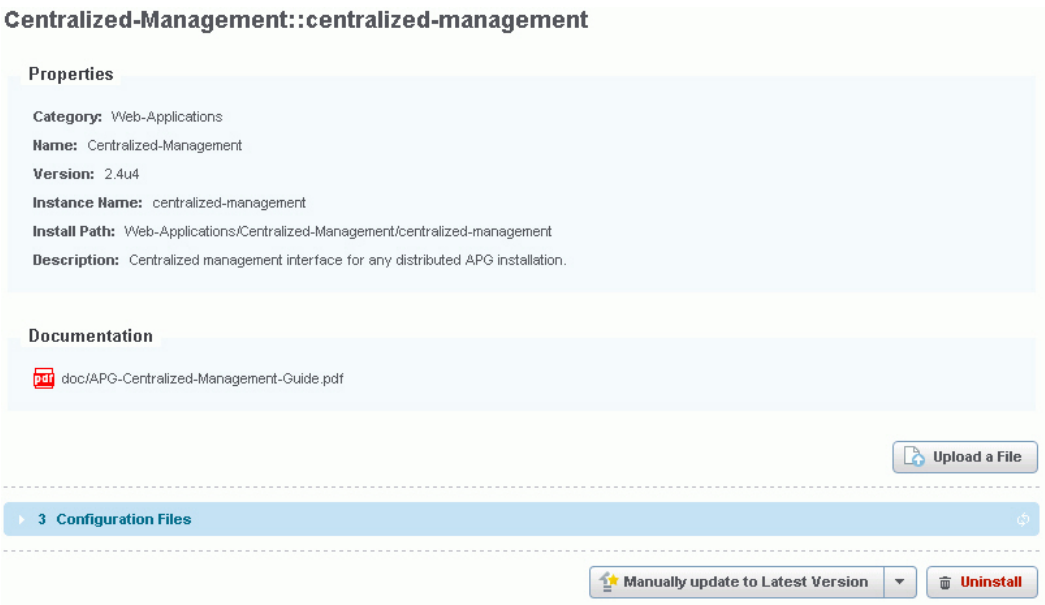
Option	Description
Linux	`centralized-management-<version number>-linux-x64.pkg`
Windows	`centralized-management-<version number>-windows-x64.pkg`

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

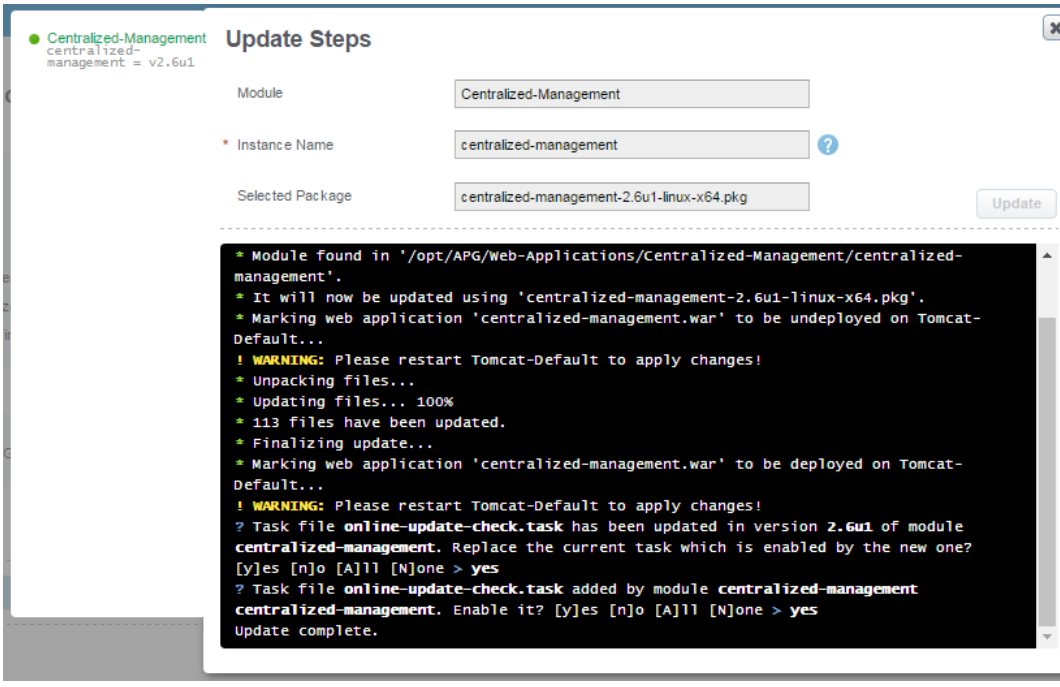


6. **Click Continue**.

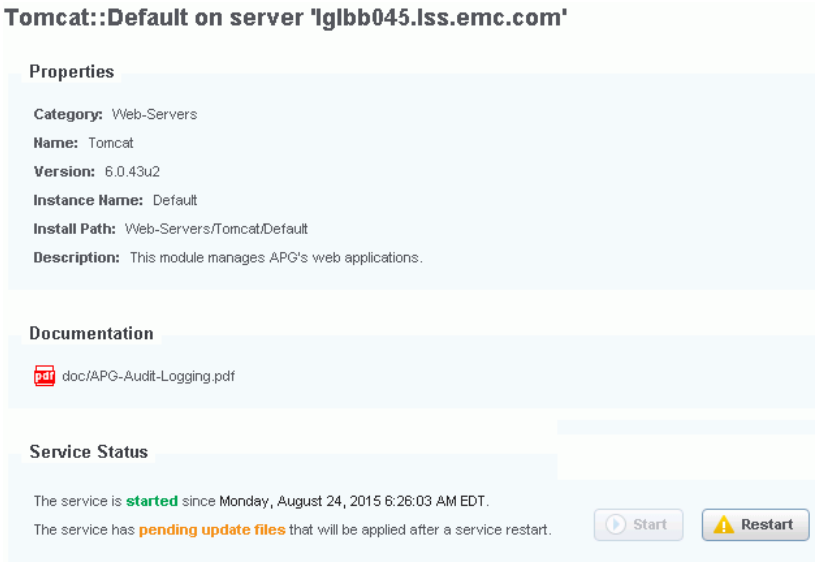
   The package is uploaded to the server.
7. On the left-hand pane, navigate to **Physical Overview** > **Front End** > **Modules** > **Web-Applications** > **Centralized Management**.
8. Click **Manually Update to Latest Version**.



9. Click **Update**. Answer yes to both of the questions about online-update-check.task.



10. Restart the tomcat service.
    a. From Centralized Management, navigate to **Physical Overview** > **Front End**.
    b. On the **Services** tab, click the Tomcat module.
    c. Click **Restart**.



Upgrading the system

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

Before you begin

If you have enabled Online Update, the files have automatically been staged, and you can skip steps 1, 3, and 4. For information about enabling and configuring Online Update, refer to Automating the Download of Updates on page 79.

Procedure

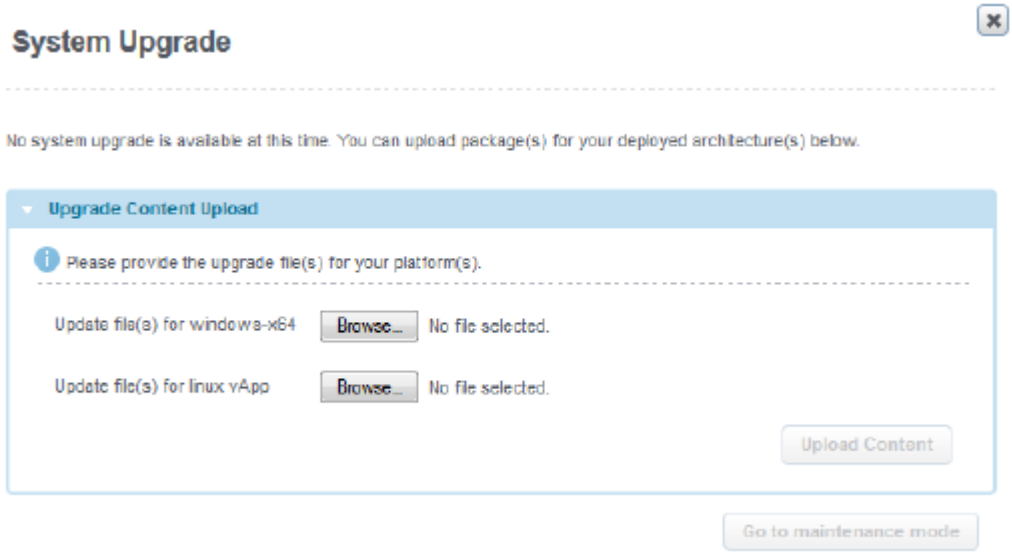
1. Download the core update file for each of your deployed architectures from support.emc.com.

Option	Description
Linux (binary only)	`EMC_MnR_6.8.2_Linux_64-bit_Update_File.zip`
Windows	`EMC_MnR_6.8.2_Windows_64-bit_Update_File.zip`

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

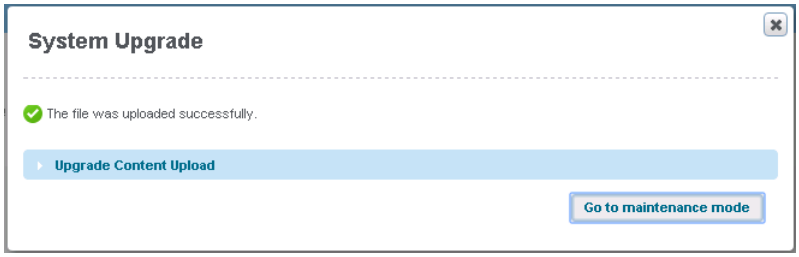
   If an upgrade package is currently being downloaded via Online Update, wait until the download is complete before proceeding to the next step.

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

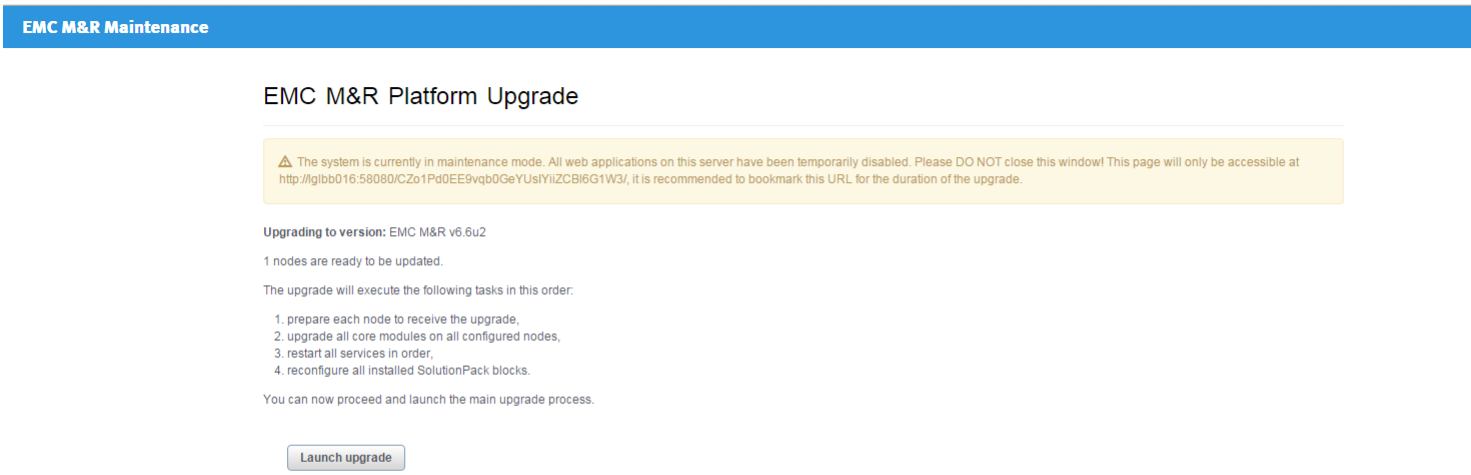


4. Click **Upload Content**.
5. The system displays a message about ensuring that there is minimum of 5 GB disk space on the servers. Click **OK**.

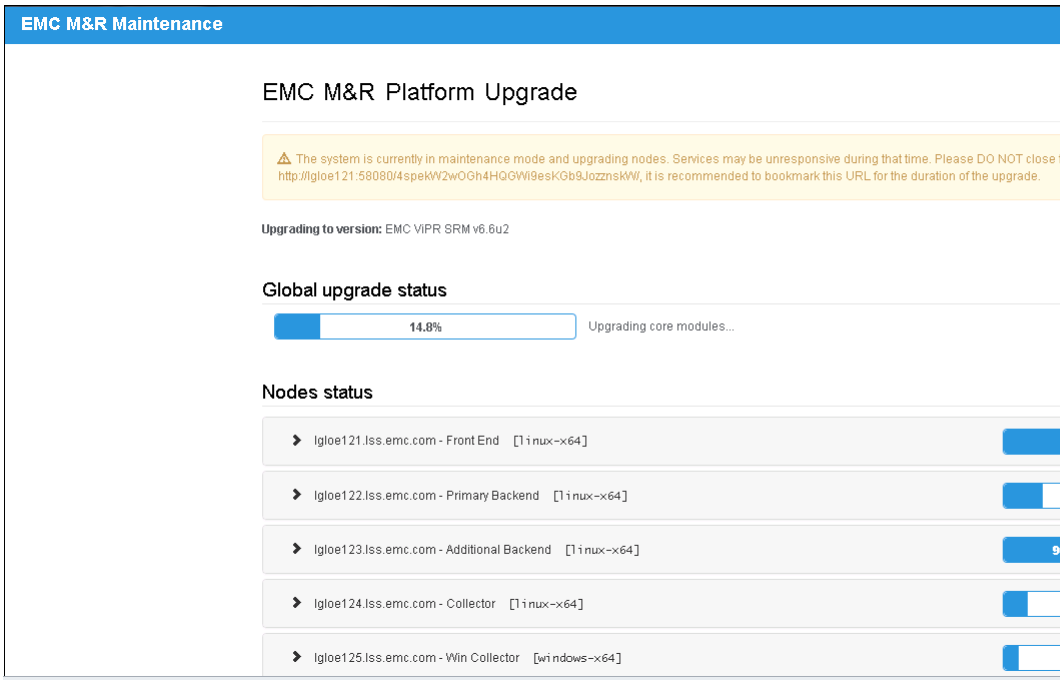
   The system upgrade files are uploaded to Centralized Management and non-disruptively distributed to all of the servers in the deployment. This process may take several minutes.
6. When you are ready to proceed with the upgrade, click **Go to maintenance mode**.



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



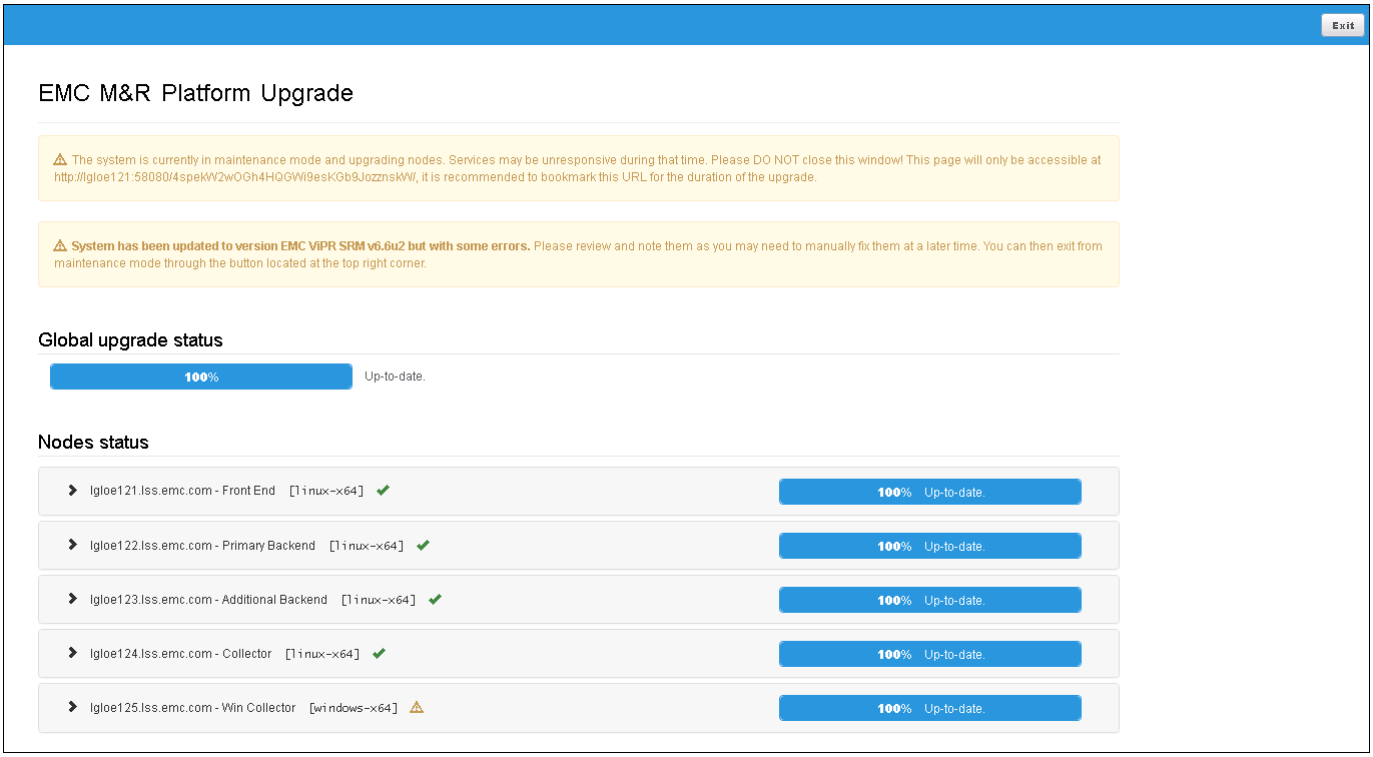
The upgrade begins. After several minutes, the **Upgrade status** displays.



Note

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

When the upgrade is complete, the system displays a green check mark next to each node and a success message at the top of the window.



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

   The system restarts the front end, and it is now available to users.
10. 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.

11. In Windows deployments, the Java module is updated during the upgrade, but the old version of Java is not removed. EMC recommends that you remove the older version of Java. Only the latest Java version folder should be kept. Remove the Java files as described in this message:

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

Restoring the Java certificates file

If you are upgrading from EMC M&R 6.5u4, and you 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. This allows importing these certificates using the new mechanism. 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 6

Upgrading through CLI

This chapter includes the following topics:

- Preparing for the upgrade of binary installations in Linux deployments 66
- Preparing for the upgrade of binary installations in Windows deployments 68

Preparing for the upgrade of binary installations in Linux deployments

Before you can upgrade the EMC M&R platform in your Linux environment, you must run the setup script on each server.

Before you begin

Note

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 *Automate the Download of Updates*.

- Identify the servers that you plan to upgrade and back up all necessary files.
- Ensure that a login with root credentials is available.
- If you have not enabled Online Update, download the Linux setup script (`<product name>_<version number>_Linux_x86_64.sh`) from your product page on the EMC support website.

Procedure

1. Use a tool such as SCP to upload the setup script to a temporary directory on every server that you plan to upgrade.
2. Log in to the server as `root`.
3. Navigate to the temporary directory and make the setup script executable. For example:

   ```
   chmod +x EMC_MnR_6.8.2_Linux_64-bit_Setup_File.sh
   ```

4. Run the setup script for your product. For example:

   ```
   ./EMC_MnR_6.8.2_Linux_64-bit_Setup_File.sh
   ```

5. Answer the questions as directed. For example, accept the EULA and use the defaults for the installation directory and the package installation. A warning message may display when modules are updated. For example,

```
 " WARNING message will be provided for those module which
has an update"

For example
Identifier                          Instance              :
Category         Module Name                         Version
Revision OS-Arch   Status
   ---------------------------------- ----------------------
- ---------------- ------------------------------------
------- -------- --------- ---------------------------
 * active-cache                        Alert-
Consolidation    : Event-Processing Active-
Cache                        v1.1    r31744   linux-x64
 * active-cache                        emc-
smarts             : Event-Processing Active-
Cache                        v1.1    r31744   linux-x64
 ! administration-tool
Default                : Tools            Administration-
Tool                 v1.3u1  r53752   linux-x64 can be
updated to v1.4u1
```

```
 ! alert-consolidation                Alert-
Consolidation    : Block            alert-
consolidation                 v3.6.1  r11870            can
be updated to v4.0
 ! alerting-backend
Default                : Backends         Alerting-
Backend                   v3.8u1  r54289   linux-x

 Warning: if a newer version of the module-manager is
available, please make sure it gets updated before any other
module.
```

Results

Your system is now prepared for update.

After you finish

Repeat these steps for each Linux server you want to upgrade.

If you are upgrading from 6.5.1, delete these SolutionPack packages from **Centralized Management** > **Packages Management** before continuing the update process:

- SolutionPack for Nokia Siemens Network (NSN GGSN)
- SolutionPack for Cisco CUCM version 1.1 (cisco-voip-cucm version 1.1).

Updating core modules in a Linux environment

Update core modules using the `launch-update` script.

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

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 `<install directory>/Tools/Module-Manager/1.8u1/bin` directory.
3. Change the permissions for the `launch-update.sh` script:

   ```
   chmod u+x launch-update.sh
   ```

4. Run `./launch-update.sh`

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

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

5. Review the modules that will be updated and the SolutionPacks that will be reconfigured. At the `Proceed?` prompt, press **`Enter`** to launch the update.

   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 block-type modules are updated by the script. 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.

Deleting old Java files after Windows update

You must remove old Java files after running the `launch-update` script.

Before you begin

After the `launch-update` script runs, the Windows collector indicates successful update of the Java module, but the older version of Java may not have been removed. If the old version remains, you must manually remove the Java directory as described in this message:

```
Some files were left behind after the update of Java...
Please manually remove directory 8.0u25 from the path 'C:\Program
Files\APG\Java\Sun-JRE\8.0u25'
```

Preparing for the upgrade of binary installations in Windows deployments

Before you can upgrade the EMC M&R platform in your Windows environment, you must run the setup executable on each server.

Before you begin

Note

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 *Automate the Download of Updates*.

- Identify the servers that you plan to upgrade and back up all necessary files.
- Ensure that login credentials with System Administrator permissions are available.
- If you have not enabled Online Update, download the Windows executable, for example, `EMC_MnR_6.8.2_Windows_64-bit_Setup_File.exe`, from your product page on the EMC support website. http://support.emc.com.
- Place the Windows installation binary setup script in a temporary folder on every server that you plan to upgrade.

Procedure

1. Double-click the executable file.
2. Click **Next**.
3. Read and accept the End User License Agreement. Click **I Agree**.
4. Press **Enter** to accept the default installation folder of `C:\Program Files\APG`, or specify a different directory.

5. Press **OK** to install the new packages in the `C:\Program Files\APG\Tools\Module-Repository` directory. A warning message may display when modules are updated. For example,

```
 " WARNING message will be provided for those module which
has an update"

For example
Identifier                          Instance              :
Category         Module Name                        Version
Revision OS-Arch   Status
   ------------------------------------ ----------------------
- ---------------- ------------------------------------
------- -------- --------- ---------------------------
 * active-cache                        Alert-
Consolidation    : Event-Processing Active-
Cache                        v1.1    r31744   linux-x64
 * active-cache                        emc-
smarts             : Event-Processing Active-
Cache                        v1.1    r31744   linux-x64
 ! administration-tool
Default                : Tools            Administration-
Tool                 v1.3u1  r53752   linux-x64 can be
updated to v1.4u1
 ! alert-consolidation                Alert-
Consolidation    : Block            alert-
consolidation                 v3.6.1  r11870            can
be updated to v4.0
 ! alerting-backend
Default                : Backends         Alerting-
Backend                    v3.8u1  r54289   linux-x

 Warning: if a newer version of the module-manager is
available, please make sure it gets updated before any other
module.
```

Your system is now prepared for update.

After you finish

Repeat these steps for each Windows server you want to upgrade.

If you are upgrading from 6.5.1, delete these SolutionPack packages from **Centralized Management** > **Packages Management** before continuing the update process:

- SolutionPack for Nokia Siemens Network (NSN GGSN)
- SolutionPack for Cisco CUCM version 1.1 (cisco-voip-cucm version 1.1).

Updating core modules in a Windows environment

Update core modules using the `launch-update` script.

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

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 `<install directory>\Tools\Module-Manager\1.8u1\bin` by running `launch-update.cmd`.
5. Review the modules that will be updated and the SolutionPacks that will be reconfigured.
6. At the `Proceed?` prompt, press **`Enter`** to launch the update.

   The script starts updating modules. Let the script run uninterrupted. Once completed, the script lists which modules and SolutionPacks were updated and reconfigured successfully.

7. To review the list of installed modules and their update status, type this command from the `C:\Program Files\APG\bin` directory:

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

   At this stage of the upgrade, only a few block-type modules should need to be updated. These will be updated later through the UI.

After you finish

After the launch-update script runs, the Windows collector indicates successful update of the Java module. If you are upgrading from EMC M&R 6.5u1, the older version of Java is not removed. You must manually remove the older version of Java after a Windows upgrade.

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.

CHAPTER 7

Post Upgrade Tasks

This chapter includes the following topics:

- Performing the post upgrade tasks 72

Performing the post upgrade tasks

After upgrading to 6.8u2, switch to the HTTPS mode.

The *SSL setup for SAM and EMC M&R* section in the *Service Assurance Suite SolutionPack Articles* guide provides information on how to switch to the HTTPS mode.

Note

When you upgrade to M&R 6.8u2, it is upgraded by default to the HTTP mode.

CHAPTER 8

Updating SolutionPacks and Other Components

This chapter includes the following topics:

- Overview 74
- Upgrading all SolutionPacks and other components 74
- Updating SolutionPacks and other components 76
- Adding new components 78
- Updating components distributed in package (.pkg) files 78

Overview

Use these procedures to update SolutionPacks and other components that Online Update has downloaded from the EMC Update server to the Module Repository on the Centralized Management (CM) server. You can update SolutionPacks separately from the process of upgrading the system to the latest version.

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 system does not check files that were not were not included with the SolutionPack.

Upgrading all SolutionPacks and other components

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

Before you begin

If you want to update a single SolutionPack to receive the benefit of a required fix or feature, refer to Updating SolutionPacks and other components on page 76. For installation, configuration, and upgrade instructions for each SolutionPack, referto the dedicated SolutionPack articles.

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.

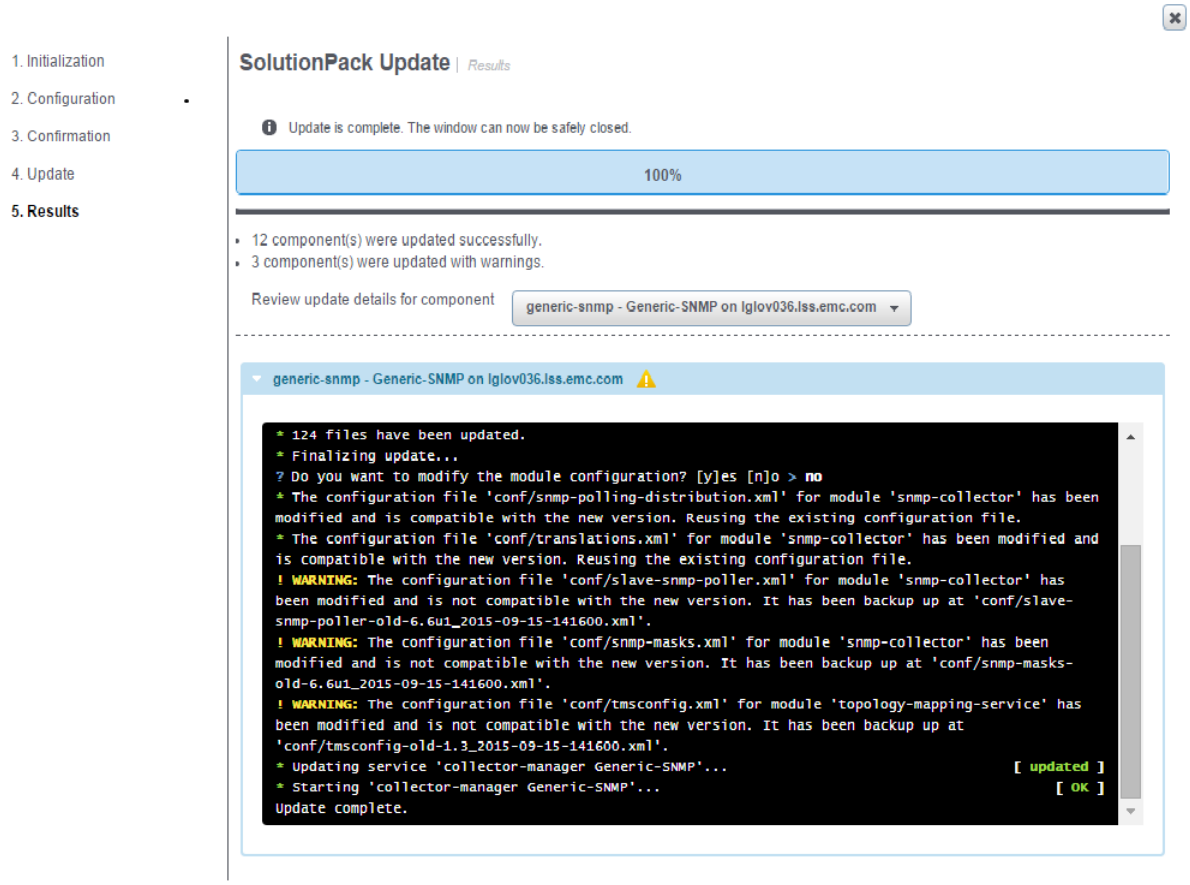
4. After you have configured every component on the list, click **Next**.
5. The **Confirmation** window opens and lists all of the components that will be updated. Confirm that all of the components are correctly listed, and then click **Update**.
6. The **Update** window opens and displays the progress 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

Figure 1 SolutionPack update incompatible file messages



7. 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.”

Updating SolutionPacks and other components

Learn how to update installed SolutionPacks and other components.

Procedure

1. Navigate to the installed SolutionPacks page: `https://<Frontend IP address>:58443/centralized-management/#/sp`
2. Depending on which SolutionPacks or components you want to update, click the appropriate button:

Option	Description
Update all of the installed SolutionPacks and other components	Click the **Update All Component**s button in the top-right corner of the page.
Update all of the installed SolutionPacks	Click the **Select All** button located below the SolutionPacks table, and then click the `Update` button.

Option	Description
Update all of the installed other components	Click the **Select All** button located below the Other Components table, and then click the **Update** button.
Update individual SolutionPacks or other components	In the SolutionPacks table or the Other Components table, click the update icon for the SolutionPacks or other components that you want to update.

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

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

3. Click **Next**.

   The **Configuration** window opens. The left-hand pane lists each of the components that include new features that you need to configure. The right-hand pane displays the configuration details for the component with the new features highlighted in yellow. Carefully review the selections to make sure the configuration details for the components and SolutionPacks are correct, and modify any configuration that are not set correctly. When you have finished configuring a component, click **Next** to move onto the next component. After you have configured every component on the list, click **Next**.

4. The **Confirmation** window opens and lists all of the components that will be updated. Confirm that all of the components are correctly listed, and then click **Update**.

   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. When the installation is complete, the **Results** page opens.

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 an incompatible tmsconfig file can safely be ignored. Similar warnings while updating generic-snmp about incompatible files for module 'snmp-collector' can also safely be ignored.

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.”

Adding new components

Procedure

1. Navigate to the installed SolutionPacks page: `https://<Frontend IP address>:58443/centralized-management/#/sp`
2. In the **Other Components** section of the page, click **Add Component**.

   The **Browse and Install Other Components** page opens.
3. Click the component that you want to install.
4. Specify the server where you want to install the new component, and click **Next**.
5. If necessary, specify additional configuration settings.
6. Click **Install**.

Updating components distributed in package (.pkg) files

Use this procedure to update EMC M&R software when a component is distributed as a .pkg or .zip file containing multiple package files.

Before you begin

- A login with administrative privileges.
- The `<EMC MnR component>.pkg` file you downloaded from EMC Online Support to a directory, such as `/temp`.

Procedure

1. From Centralized Management, click **Packages Management**.
2. On the **Packages Listing** page, click the **Upload** button.
3. Click **Browse**, and select the package file to be uploaded.
4. Click **OK** and then **Continue**.

   The package is uploaded to the server where you can install it.

CHAPTER 9

Automating the Download of Updates

This chapter includes the following topics:

- Online Update overview 80

Online Update overview

Online Update automatically downloads the latest versions of the SolutionPacks and EMC M&R components from the EMC Update server to the Module Repository on the Centralized Management (CM) server.

In a multi-server environment, the downloaded modules are distributed to all of the remote servers managed by the CM server.

Configuring server settings for online updates

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Click **Configuration** > **Online Update** .
4. Ensure that you are on the **Settings** tab.
5. Check the **Enabled** checkbox.
6. Type your EMC Online Support username and password.
7. Click the icon to test connectivity to the update server.

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

   The icon indicates that connectivity to the server failed.
8. Click **Save**.

Enabling the online update task

Enable the Online Update task to download the latest updates from the EMC Update server automatically.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. On the **Physical Overview** page, click the ***<host_name>*** **- Front End** where the Online Update task needs to run.
4. Click **Tasks**.
5. Type `OnlineUpdate` in the **Search** bar.
6. Click the **OnlineUpdate** scheduled task.
7. Click **Enable**.

   Note

   By default, this task is set to run once everyday at 12AM. You can customize the task schedule by editing the configuration file.

Running the online update task manually

At any time, you can run the Online Update task manually to access the available updates.

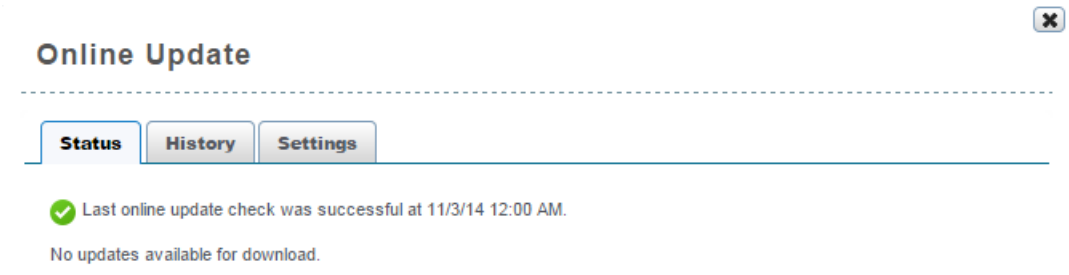
Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. On the **Physical Overview** page, click the ***<host_name>*** **- Front End** where the Online Update task needs to run.
4. Click **Tasks**.
5. Type `OnlineUpdate` in the **Search** bar.
6. Click the **OnlineUpdate** scheduled task.
7. Click **Run Now**.

Online Update Status

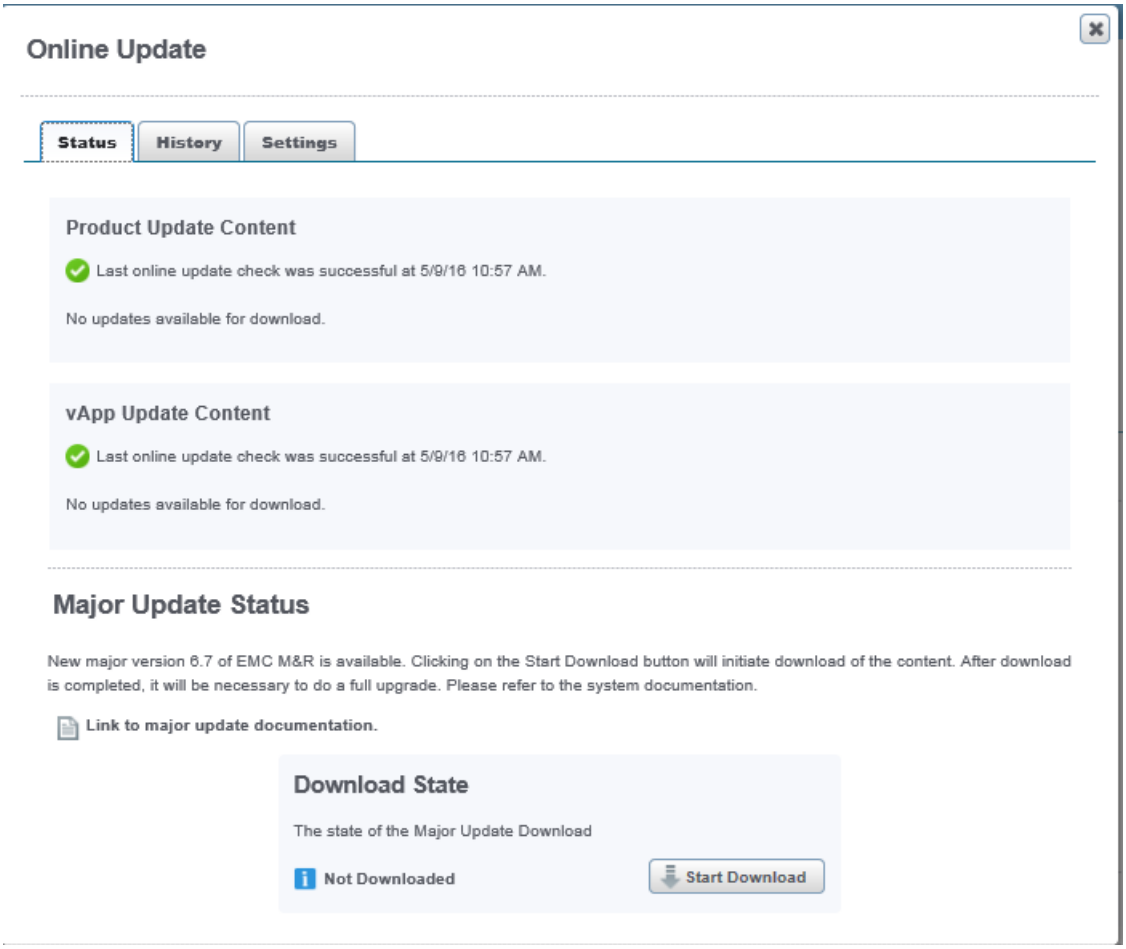
The Online Update Status tab indicates whether or not the last online update check was successful, provides the date and time of the last successful check, and lists any updates that are available for download.

Figure 2 Online Update Status



If a major update of the EMC M&R platform is detected, the Status tab includes a Major Update Status section that describes the version that is available, provides a link to the upgrade documentation, and includes a Start Download button.

Figure 3 Online Update Status with a major version update detected



Downloading a major update

You can use Online Update to download a major version of the EMC M&R platform. You should only download a major version if you intend to immediately complete the full upgrade process.

Procedure

1. Click **Administration**.
2. Click **Centralized Management**.
3. Click **Configuration** > **Online Update**.
4. Click the **Status** tab.
5. Click **Start Download**. When the download is finished, the Download State will change from "Not Downloaded" to "Complete."
6. Complete the upgrade process as described in the upgrade documentation.

Online Update History

The Online Update History tab provides a download history with the names of the components, the version numbers, and the date and time of the downloads.

The History tab also allows you to search the download history for a particular component name or version number.

Disabling the online update task

You can disable the Online Update task if you prefer to manually download the updates from the EMC Update server.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. On the **Physical Overview** page, click the ***<host_name>*** **- Front End** where the Online Update task needs to run.
4. Click **Tasks**.
5. Type `OnlineUpdate` in the **Search** bar.
6. Click the **OnlineUpdate** scheduled task.
7. Click **Disable**.

CHAPTER 10

Uninstallation

This chapter includes the following topics:

- Overview 86
- Stopping EMC M&R platform services on a UNIX server 86
- Uninstalling EMC M&R platform from a UNIX server 86
- Stopping EMC M&R platform services on a Windows server 86
- Uninstalling EMC M&R platform from a Windows server 87
- Uninstalling a SolutionPack 87

Overview

You can uninstall a SolutionPack and uninstall EMC M&R platform from a UNIX or Windows server.

Stop the EMC M&R platform services before uninstalling EMC M&R platform.

Stopping EMC M&R platform services on a UNIX server

Use the `manage-modules.sh service stop` command to stop a specific EMC M&R platform service or to stop all EMC M&R platform services on a UNIX server.

Before you begin

Make sure you have logged in with root or APG privileges.

Note

The list of services varies depending upon which type of installation was performed, for example, vApp, collector, backend, frontend, and so forth.

Procedure

- Type **`manage-modules.sh service stop <service_name>`** from the `bin` directory of the installation to stop a specific EMC M&R platform service.

  This example shows how to stop all EMC M&R platform services:

  ```
  ./manage-modules.sh service stop all
  ```

Uninstalling EMC M&R platform from a UNIX server

Use the `manage-modules.sh service remove all` command to uninstall all EMC M&R platform services.

Before you begin

Make sure you have a login with root privileges.

Procedure

1. Type **`manage-modules.sh service remove all`** from the `/opt/APG/bin` directory to uninstall all EMC M&R platform services.

2. Type **`rm -rf /opt/APG`** to remove the installation directory.

Stopping EMC M&R platform services on a Windows server

Use this procedure to stop EMC M&R platform services from the Windows desktop.

Before you begin

Make sure you have logged in with system administrator credentials to manage services.

Note

The list of services varies depending upon which type of installation was performed, for example, vApp, collector, backend, frontend, and so forth.

Procedure

1. Type **`manage-modules.cmd service stop <service_name>`** from the `bin` directory of the installation to stop a specific EMC M&R platform service.

   This example shows how to stop all EMC M&R platform services:

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

Uninstalling EMC M&R platform from a Windows server

Use the `manage-modules.cmd service remove all` command to remove all EMC M&R platform services from a Windows server.

Before you begin

Make sure you have logged in with system administrator credentials.

Procedure

1. Type **`manage-modules.cmd service remove all`** from the `C:\Program Files\APG\bin` folder to uninstall all EMC M&R platform services.

2. Use the **Windows Control Panel** to uninstall EMC M&R platform.

   a. Click **Start** > **Control Panel** > **Programs**.

   b. Click **Uninstall a program**.

   c. Select the **Watch4net Solutions APG** and click **Uninstall**.

Uninstalling a SolutionPack

If you no longer want to view the reports of a certain SolutionPack, you can uninstall that SolutionPack from the server.

Procedure

1. Log in with administrator credentials for EMC M&R platform and select **Administration**.
2. Select **Centralized Management** in the Administration tree.
3. Select **SolutionPacks** in the tree.
4. Select the SolutionPack that you want to uninstall in the **Installed SolutionPacks** screen.
5. In the **Properties** area, click **Trashcan** icon for each instance of the SolutionPackBlock and click **Remove**.

CHAPTER 11

Reverting HTTPS Mode to HTTP Mode for M&R 6.8u2 Installation

This chapter includes the following topics:

- How to revert HTTPS mode to HTTP mode for M&R 6.8u2 installation.....90

How to revert HTTPS mode to HTTP mode for M&R 6.8u2 installation

If you want to access M&R 6.8u2 in the HTTP mode, complete the following steps:

Note

When you install M&R 6.8u2, it is installed by default in the HTTPS mode.

Procedure

1. In the `/opt/APG/Web-Servers/Tomcat/Default/conf/server.xml` file, do the following:
   a. Locate and remove the entry `redirectPort="58443"`.
   Before removing the entry `redirectPort="58443"`, it appears as follows:

```
<Connector port="58080" protocol="HTTP/1.1"
 connectionTimeout="20000"
 compression="2048"/>
 redirectPort="58443" URIEncoding="UTF-8" />
```

   After removing the entry `redirectPort="58443"`, it must appear as follows:

```
<Connector port="58080" protocol="HTTP/1.1"
 connectionTimeout="20000"
 compression="2048"
 URIEncoding="UTF-8" />
```

   b. Comment out the following line:

```
<Valve
className="com.watch4net.apg.v2.gui.tomcat.ForceSSL" />
```

2. Restart the tomcat service.
3. Clear the browser cache, and then log in using HTTP.

APPENDIX A

Telnet and Socket Interface Ports

This appendix includes the following topics:

- Telnet and socket interface ports for each backend 92

Telnet and socket interface ports for each backend

The telnet and socket interface for each backend must be different on that backend host. These ports are open in the Linux firewall setting by default.

Backend Host	Backend	socket interface	telnet interface
Primary Backend (PBE)	DB	2000	2001
Additional Backend #1 (ABE)	DB1	2100	2101
	DB2	2200	2201
	DB3	2300	2301
	DB4	2400	2401
Additional Backend #2 (ABE)	DB-*hostname*-1	2100	2101
	DB-*hostname*-2	2200	2201
	DB-*hostname*-3	2300	2301
	DB-*hostname*-4	2400	2401
Additional Backend #3 (ABE)	DB-*hostname*-1	2100	2101
	DB-*hostname*-2	2200	2201
	DB-*hostname*-3	2300	2301
	DB-*hostname*-4	2400	2401
Additional Backend #4 (ABE)	DB-*hostname*-1	2100	2101
	DB-*hostname*-2	2200	2201
	DB-*hostname*-3	2300	2301
	DB-*hostname*-4	2400	2401
Additional Backend #5 (ABE)	DB-*hostname*-1	2100	2101
	DB-*hostname*-2	2200	2201
	DB-*hostname*-3	2300	2301
	DB-*hostname*-4	2400	2401
Additional Backend #6 (ABE)	DB-*hostname*-1	2100	2101
	DB-*hostname*-2	2200	2201
	DB-*hostname*-3	2300	2301
	DB-*hostname*-4	2400	2401

APPENDIX B

SolutionPack Ports

This appendix includes the following topics:

- SolutionPack Port Details 94

SolutionPack Port Details

The following ports need to be open in the firewall for SolutionPack access.

Port name	Port number	Description
http	58080	Used for accessing SAS Web portal.
ESRS	58443	Secures access of M&R frontend portal. It will periodically check on port 58443 that SAS install is up and running.
LDAP	389	Used for LDAP authentication.
SSHd	22	Used by text collector.
https	443	SSL connection to vCenter for Vmware VMs/ESX/ESXi's discovery using Vmware APIs.
SNMP	161	SNMP V1/V2/V3
		Standard SNMP Polling for discovering network switches or routers.
Load-Balancer Arbiter	2020	Load Balancer connector(LBC) running on Collector hosts will communicate with Load Balancer Arbiter(LBA) running on Primary Backend host for latest Load Factor/ Balancing information.
Backend-1	2101	TCP Socket connector ports for pushing data to additional Backend DBs. This is in case of a 4-VM vApp.
Backend-2	2201	TCP Socket connector ports for pushing data to additional Backend DBs. This is in case of a 4-VM vApp.
Backend-3	2301	TCP Socket connector ports for pushing data to additional Backend DBs. This is in case of a 4-VM vApp.
Backend-4	2401	TCP Socket connector ports for pushing data to additional Backend DBs. This is in case of a 4-VM vApp.

Port name	Port number	Description
Backend Mgmt	2001	TCP Socket control interface for Backend
Alerting-Backend	2010	Raw data sent from Collector to alerting backend
Topology Service	48443	Topology Mapping Service(TMS)service running on Collector will send data to Topology Service running on Backend Host.
Topology Service	48443	Frontend web application will communicate with Topology Service (TS) running on Primary Backend.
Topology Service	58083	58083 is just internal port for Web service gateway to communicate with Topology Service. However, in all-in-one deployments, where secure communication between components is not required, this could be used instead of 48443 by both TMS, or the frontend.
Event Processing Manager (Alert Consolidation)	2040	Alerts collected for VNX will be posted through this port.
Generic Event Listener(Alert Consolidation)	2042	User action events such as - Acknowledge/ Unacknowledged or Assigned/unassigned, triggered from Alerting Dashboard, Situation to Watch or any other relevant Alerting view would be sent to Primary Backends' port 2042.
Web-Service gateway	48443	To connect/register from Frontend to administer remote W4N servers.
		Also, Maps Service on Frontend communicates to Topology Service running on Primary Backend via this port.
SNMP Collector-1	2008	Administer remote SNMP Collector
SNMP Collector-2	2108	Administer remote SNMP Collector
SNMP Collector-3	2208	Administer remote SNMP Collector

Port name	Port number	Description
SNMP Collector-4	2308	Administer remote SNMP Collector
JMX	52569	Alert Manager configuration
MySQL	53306	MySQL Database Access
Event Processing	52001	Listens for incoming requests for event processing
Tomcat-listener	58005	Tomcat listens for incoming requests on this port
Event Processing	52004	TCP port used by the collector to send events to event processor on Primary backend
Event Processing	52007	TCP port to send Cisco UCS events to event processor on Primary backend
Alert Event Processing	2060	Alerting sends the event to Compliance for Impact Analysis. This is specifically for the Binary Installs where Compliance Backend can be installed independently.
Elastic Search	9200, 9300	Elastis Search
SolutionPack for Alcatel-Lucent	5620	SolutionPack for Alcatel-Lucent
JMS port for Alcatel-Lucent SolutionPack	1099	JMS port for Alcatel-Lucent SolutionPack
SolutionPack for Traffic Flows	NetFlow: 2055, 9555, 9556, or 9996	SolutionPack for Traffic Flows
	sFlow: 6343	
SolutionPack for EMC Smarts	15672	SolutionPack for EMC Smarts
Smarts broker	426	Smarts broker
SolutionPack for EMC Network Configuration Manager	5435	SolutionPack for EMC Network Configuration Manager
SolutionPack for Cisco Unified Communications Manager	52006	SolutionPack for Cisco Unified Communications Manager

APPENDIX C

SolutionPack Reconfiguration Fields

This appendix includes the following topics:

- SolutionPack Reconfiguration Fields 98

SolutionPack Reconfiguration Fields

You can change the settings for the SolutionPack from the SolutionPack Reconfiguration page.

Table 7 SolutionPack Reconfiguration Fields

Field	Description
Socket Collector port	On this TCP port on the Primary Backend, the Arbiter is accepting the remote connections from all LBCs.
APG Backend hostname or IP address	The hostname of the server where the apg database and its backend service are running. In this deployment, the possible options are backend and backend2. Do not use "localhost" for the default apg on the primary backend.
APG Backend data port	Each apg has a backend and each backend has its own TCP port to receive raw data. The port must be unique only inside the server. Refer to Installing and configuring the Additional Backend hosts on page 25. In this installation, the ports are 2000, 2100, 2200, 2300 and 2400.
Web-Service Gateway	Each APG server has a Web-Service Gateway. This hostname must point to the APG server with the backend service.
Backend Web-Service Instance	The backend instance name. In this deployment, the possible values are: • Default (the default backend instance name from primary backend) • apg1 • apg2 • apg3 • apg4
Backend database type	MySQL by default.
Backend database hostname or IP address	The hostname where the MySQL database is running. By default, it is same as the APG Backend hostname.
Backend database port number	The port on which MySQL is accepting remote TCP connections. By default, it is 53306 .
Backend Database name	The database name used in MySQL. For example, apg, apg1, apg2.

Table 7 SolutionPack Reconfiguration Fields (continued)

Field	Description
Backend database username	The user configured in MySQL. The default is "apg"
Backend database password	The default password for the MySQL user is "watch4net"

APPENDIX D

Restoring Modules to their Previous Version

This appendix includes the following topics:

- Restoring modules workflow 102
- Listing restorable modules 102
- Restoring modules 103
- Starting the EMC M&R platform services from the command line 105
- Starting the EMC M&R platform services on Windows 106

Restoring modules workflow

If you need to, you can revert to the previous version of EMC M&R platform after an update. If the software is installed on multiple servers, you need to perform the restore process on each server.

Restoring the modules does not restore them to their exact state prior to an upgrade. The reason is that during the update process, some modules may modify their data files to work for newer version. Once the data files are modified, they cannot revert to their previous state.

The Module-Manager cannot be restored to its previous version. The 6.8u2 or higher version of Module Manager is fully compatible with version 6.7u2 and can be used in its place.

Make sure you have a login with root or system administrator privileges to restore modules.

For single host or multiple host deployments:

1. Listing restorable modules on page 102
2. Restoring modules on page 103
3. Start the EMC M&R platform services: Starting the EMC M&R platform services from the command line on page 105 or Starting the EMC M&R platform services on Windows on page 106

Listing restorable modules

Use the `manage-modules.sh list restorable` command to list all modules that can be restored.

Before you begin

Make sure you have a login with root or system administrator privileges to restore modules.

Procedure

- Type the command for your operating system from the EMC M&R platform installation directory:

Operating system	Command
UNIX	`<INSTALL_DIR>/bin/manage-modules.sh list restorable [--match="<module>"]`
Windows	`<INSTALL_DIR>\bin\manage-modules.cmd list restorable [--match="<module>"]`

To determine if the module has more than one version to restore, specify the `--match` option. For example:

```
/opt/APG/bin/manage-modules.sh list restorable --
match="frontend"
```

When you view the output, record the order in which the modules display. You will need to use the order later when you restore the modules.

This partial Linux sample output indicates modules that can be restored.

```
Available Restore Points:

   Identifier                 Instance       Version
Date
   -------------------------- -------------- -------
-------------------
* availability-filter         Generic-RSC    1.8u1   9/8/17
7:49:39 PM
* xml-collector               emc-ncm        1.13    9/8/17
7:59:35 PM
* inline-calculation-filter   Generic-SNMP   6.3u1   9/8/17
7:54:26 PM
* failover-filter             emc-ncm        5.2     9/8/17
7:53:15 PM
* frontend                    APG            6.7u1   9/8/17
8:00:02 PM
```

Restoring modules

Restore modules to their previous version.

Before you begin

- Identify all modules that can be restored by using the `manage-modules.sh list restorable` command.
- Make sure you have a login with root or system administrator privileges to restore modules.

Restore the modules in the order in which they displayed, starting from first to last. To avoid dependency issues, restore the main components or managers before their sub-components. For example, restore the Event Processing Manager before its sub-component, Event Property Tagger. Refer to the Module Manager documentation for more complete information about module rollback. This document is in the documentation directory of the installation path (for example, `/opt/APG/Doc`).

Procedure

1. Type the command for your operating system from the EMC M&R platform installation directory:

Operating system	Command
UNIX	`<INSTALL_DIR>/bin/manage-modules.sh restore <module_identifier> [<module_instance>]`

Operating system	Command
Windows	`<INSTALL_DIR>\bin\manage-modules.cmd restore <module_identifier> [<module_instance>]`

2. Answer any questions.

   This Linux sample output shows that the administration-tool module has been restored to its previous version.

```
opt/APG/manage-modules.sh restore administration-tool
Starting restoration of administration-tool Default v1.0u2...
 * Gathering information...
 * Issuing a rollback will overwrite all existing files -
except the data ones - and replace them with their previous
versions, including configuration files.
 * The module 'Administration-Tool' will now be restored in
'/opt/APG/Tools/Administration-Tool/Default'.
 ! WARNING: The targeted directory already exists. This will
overwrite existing files in this directory.
 ? Continue? [y]es, [n]o > y
 * Restoring files...
Restoration complete.
```

manage-modules.sh restore command

Use the `manage-modules.sh restore` command to revert modules to their previous version after an update. Type the command for your operating system from the `bin` directory of your EMC M&R platform installation directory.

Description

The `manage-modules.sh restore` command enables you to revert to the previous version of EMC M&R platform after an update. For UNIX, specify `manage-modules.sh restore`. For Window, specify `manage-modules.cmd restore`.

To look up the identifier and module instance name, use the `manage-modules.sh list restorable` command.

Syntax

```
manage-modules.sh restore <module_identifier>
[ <module_instance> ] [ <version> ]
```

Options

module_identifier

The identifier value of the installed module.

module_instance

The unique name of the module. Omit this value if only one instance is installed since the command will use it as the default. If multiple instances exist, specify the instance you want to restore.
The identifier and instance values form a unique key to refer to the module.

version

The version number to which the module should be restored. Omit this value if only one previous version exists.

In this Linux example, the following command restores the Collector-Manager from 6.8u2 to 6.7u1. Since only one previous version exists, the `version` option is omitted.

```
<INSTALL_DIR>/bin/manage-modules.sh update collector-manager
```

In this Windows example, the following command restores the variable-handling-filter from 6.8u2 to 6.7u1. Since only one previous version exists, the `version` option is omitted.

```
<INSTALL_DIR>\bin\manage-modules.cmd restore variable-handling-
filter generic-snmp
```

In this Linux example, the following command restores the frontend-ws to version 6.7u1.

```
./manage-modules.sh restore frontend-ws apg-ws 6.7
./manage-modules.sh update mib-browser mymib_browser2
```

Starting the EMC M&R platform services from the command line

After you install EMC M&R platform, start required services.

Before you begin

- Before you start EMC M&R platform services, ensure the library search path is correct on the server that hosts EMC M&R platform. This requirement applies to the libaio package on Linux.
- Ensure that you have a login with root, APG, or system administrator privileges. The user apg is the account that the EMC M&R platform application uses instead of root.

Procedure

- Type the command for your operating system from the `bin` directory of the installation:

Operating system	Command
UNIX	`./manage-modules.sh service start all`

Operating system	Command
Windows	`manage-modules.cmd service start all`

Results

The platform displays a list of services.

Note

The list of available services will vary depending upon choices (Collector, Backend, Frontend, Default, or Minimal) made during installation.

Example:

```
* Starting 'topology-mapping-service Default'... [ OK ]
* Starting 'webservice-gateway Default'... [ OK ]
* Starting 'mysql Default'... [ OK ]
* Starting 'alerting-backend Default'... [ OK ]
* Starting 'backend Default'... [ OK ]
* Starting 'collector-manager Default'... [ OK ]
* Starting 'collector-manager Generic-SNMP'... [ OK ]
* Starting 'collector-manager Load-Balancer'... [ OK ]
* Starting 'collector-manager emc smarts'... [ OK ]
* Starting 'event-processing-manager emc smarts'... [ OK ]
* Starting 'tomcat Default'... [ OK ]
* Starting 'task-scheduler Default'... [ OK ]
```

Starting the EMC M&R platform services on Windows

After installing EMC M&R platform on Windows, you can start all required services from a Windows desktop.

Before you begin

Make sure you have logged in with system administrator credentials to manage services.

Note

The list of available services will vary depending upon choices (Collector, Backend, Frontend, Default, or Minimal) made during installation.

Procedure

1. From the application server's desktop, select **Start** > **Administrative Tools** > **Services**.
2. Right-click each service and click **Start**, in this order:
   - APG Topology Mapping Service
   - APG Topology Service
   - APG Webservice Gateway
   - APG MySQL
   - APG Alerting Backend
   - APG Backend

- APG Collector Manager (Generic RSC)
- APG Collector Manager (Generic-SNMP)
- APG Collector Manager (Load-Balancer)
- APG Event Processing Manager (Alert-Consolidation)
- APG Tomcat
- APG Task Scheduler