EMC® M&R

Version 6.5u1

Installation and Configuration Guide

P/N 302-001-500

REV 01

EMC²

Copyright © 2012-2015 EMC Corporation. All rights reserved. Published in USA.

Published January, 2015

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

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC², EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

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

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

CONTENTS

Figures 7

Tables 9

Chapter 1 System Requirements for EMC M&R 11

Revision history 12
Operating system requirements 12
Database requirements for EMC M&R 12
Browser requirements 13
Supported mobile devices 13

Chapter 2 Installation 15

Explanation of name changes 16
Options for standard installation 16
Installing EMC M&R platform on UNIX 17
Installing EMC M&R platform on Windows Server 18

Chapter 3 Configuration 19

Starting the EMC M&R platform services from the command line 20
Starting the EMC M&R platform services on Windows 20
Verifying if the EMC M&R platform services are running 21
- Troubleshooting service start-up problems on UNIX 22
- Troubleshooting service start-up problems on Windows 22

Configuring the user process limits for the Linux installation 23
Logging in to the User Interface 23
Connecting to Centralized Management 24
Confirm configuration settings and register remote servers 24
Licensing Operations 25
- Trial licenses 25
- License duration 25
- License purchase 25

Log in with administrator credentials 26
View license information 26
Upload a new license file 26
Delete licenses 27
Synchronize licenses on multiple hosts 27
Troubleshooting licensing problems 28
Permanent license stops working after host reconfiguration 28
Users are locked out 28
- Install license file from the command line 29
- Restart Tomcat service 29
- Reinstall license file and delete trial licenses after lockout 30

Module does not start or has no license 30
Where to find the latest SolutionPack software 31
Installing a SolutionPack 31
Reviewing reports 32

Chapter 4 EMC M&R Platform Update 33

Planning the upgrade 34
Preparing the environment for the upgrade 34
EMC M&R upgrade workflow 35
Mixed operating system deployments 35
Preparing for an update in a Linux environment 36
Updating module-manager for Linux operating systems 37
Updating core modules in a Linux environment 37
Preparing for an update in a Windows environment 38
Updating module-manager for Windows 38
Updating core modules in a Windows environment 39
Update all components 40
Checking the status of remote host services 41
Removing an obsolete Default ReportPack 41
Validating the environment 42
Update SolutionPacks and other components 42
Update all SolutionPacks and other components 42
Update all SolutionPacks 43
Update all other components 44
Update individual SolutionPacks or other components 45

Chapter 5 Uninstallation 47

Overview 48
Stopping EMC M&R platform services on a UNIX server 48
Uninstalling EMC M&R platform from a UNIX server 48
Stopping EMC M&R platform services on a Windows server 48
Uninstalling EMC M&R platform from a Windows server 49
Uninstalling a SolutionPack 49

Chapter 6 Troubleshooting 51

Troubleshooting service start-up problems on UNIX 52
Troubleshooting service start-up problems on Windows 52
SSL certificates 52
SSL certificate error examples 53
Troubleshooting an SSL certificate error: Accepting the exception 53
Installing a self-signed SSL certificate from an Internet Explorer browser 54
Importing an SSL certificate into your truststore 54
Exporting an SSL certificate from an Internet Explorer browser 55

Appendix A Available Modules 57

Available modules 58

Appendix B Automated Online Update of EMC M&R Software 61

Online Update overview 62
Configuring server settings for online updates 62
Enabling the online update task 62
Running the online update task manually 63
Online Update Status 63
Downloading a major update 64
Online Update History 64

Disabling the online update task 64

Appendix C Virtual Appliance Installation 67

Virtual Appliance installation for EMC M&R 68
Deploying an appliance 68
Starting the appliance 70
Verifying the appliance deployment 70
Log onto the appliance 70
Passwords 70
Installing a SolutionPack 71
Reviewing reports 72

Appendix D Restoring Modules to their Previous Version 73

Restoring modules workflow 74
Listing restorable modules 74
Restoring modules 75
manage-modules.sh restore command 76
Starting the EMC M&R platform services from the command line 77
Starting the EMC M&R platform services on Windows 78

FIGURES

1 Online Update Status 63
2 Online Update Status with a major version update detected 64

TABLES

1 Supported operating systems 12
2 Supported relational database management systems 12
3 Supported browsers 13
4 Supported mobile devices 13
5 Version 6.5u1 available modules 58
6 Default usernames and passwords 70

CHAPTER 1

System Requirements for EMC M&R

This chapter includes the following topics:

- Revision history 12
- Operating system requirements 12
- Database requirements for EMC M&R 12
- Browser requirements 13
- Supported mobile devices 13

Revision history

Use this table to review the revisions made to this document.

Revision	Date	Description
01	January 2015	GA release of EMC M&R 6.5u1

Operating system requirements

The following operating systems are supported for production.

Table 1 Supported operating systems

Operating system	Version
Red Hat Enterprise Linux	• 5, 64-bit • 6, 64-bit
CentOS Linux	• 5, 64-bit • 6, 64-bit
SUSE Linux Enterprise Server (SLES)	11, 64-bit
Microsoft Windows	• Server 2008 R2 • Server 2012 • Server 2012 R2

Note

vApp installations require VMware. Hyper-V, or any other virtual environment, is not supported for vApp installations.

Database requirements for EMC M&R

EMC M&R supports these relational database management systems.

Table 2 Supported relational database management systems

Relational database management systems	Version	Notes
MySQL	5.5	EMC M&R ships with MySQL 5.5. Existing customers may continue to use MySQL 5.0 in their EMC M&R installations.
Oracle Database Enterprise Edition	10G or later	Ensure that the EMC M&R server and its operating system satisfy the database engine requirements. Consult the Oracle website for more information.

Table 2 Supported relational database management systems (continued)

Relational database management systems	Version	Notes
		For a distributed EMC M&R scenario, the server with the EMC M&R back-end components must satisfy the database engine requirements.
Datastore	N/A	Datastore is an internal database.

Browser requirements

For the following browsers, support varies.

Table 3 Supported browsers

Browser	Version	Operating system	Notes
Google Chrome	Latest	Windows, Linux	Full support
Internet Explorer	8	Windows	Minimal Browse mode
Internet Explorer	9, 10, 11	Windows	Full support
Mozilla Firefox	Latest	Windows, Linux	Full support
Apple Safari	Latest	Mac OS X and iOS	Full support

Minimal Browse mode is for report viewing and browsing. It can display tables, including interactive tables, and graphs that are not interactive. Topology maps are not supported.

Full support includes report viewing and browsing, plus support for interactive tables and graphs, topology maps, and administration tasks (user management, enrichment GUI, alerting GUI, and so on).

Supported mobile devices

To manage the application and view reports, you can use any of the supported mobile devices.

Table 4 Supported mobile devices

Device	Version	Operating system	Notes
Apple iPhone	Latest	Mac iOS	Using EMC M&R iPhone client from AppStore
Apple iPad	Latest	Mac iOS	Using EMC M&R iPad client from AppStore

CHAPTER 2

Installation

This chapter includes the following topics:

- Explanation of name changes 16
- Options for standard installation 16
- Installing EMC M&R platform on UNIX 17
- Installing EMC M&R platform on Windows Server 18

Explanation of name changes

The procedures in this guide are applicable when installing or upgrading EMC products based on EMC M&R version 6.5u1 software artifacts.

EMC M&R may be used instead of **EMC Watch4net** in EMC product suites that use version 6.5u1 as their underlying monitoring and reporting platform. The procedures in this guide are applicable for installations and upgrades of version 6.5u1 software or higher. Install setup file names may vary depending upon which products are licensed. For example,

- Watch4net download filenames may have this syntax: `setup-linux-x86_65u1-v64.sh` or `setup-win65u1-v64.exe`
- Product suite download filenames may have this syntax: `EMC_MnR_6.5.1_Linux_64-bit_Setup_File.sh` or `EMC_MnR_6.5.1_Linux_64-bit_Setup_File.exe`.

Options for standard installation

You have several options when you perform a binary installation of the EMC M&R platform.

The EMC M&R platform infrastructure consists of three types of hosts:

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

Note

You can have only one Primary Backend host. You can add Additional Backend hosts to scale out a deployment.

The EMC M&R platform binary installation package supports the following installation options.

Default (UNIX) or Recommended Modules (Windows) installation
To install all of the modules in the EMC M&R platform binary installation package, use this option.

You can use this option on a single host and enable it to serve as a Frontend, Backend, and Collector host. You can customize this host further by manually adding or removing specific modules.

Host-specific installations
To install software only on a specific host (Frontend, Backend or Collector host), use the same EMC M&R platform binary installation package and select the type of host to install.

Minimal (UNIX) or Base Installation (Windows)
To install the minimum modules required for any host type, use this option. You can customize this host by manually adding specific modules.

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 package to a directory on the server, such as `/temp`.

Procedure

1. Locate the installation package.
2. Navigate to where the EMC M&R platform is located.
3. Change the permissions of the installer.

   For example, for the Linux 64-bit executable, type:

   ```
   chmod +x EMC_MnR_6.5.1_Linux_64-bit_Setup_File.sh
   ```

4. Run the installer from the directory.

   Example:

   ```
   ./EMC_MnR_6.5.1_Linux_64-bit_Setup_File.sh
   ```

5. Read and accept the End User License Agreement.
6. Accept the default installation directory of `/opt/APG` or type another location.
7. Accept the default user account name of **`apg`** or type another name.
8. Accept the default location of service scripts of `/etc/init.d` or type another location.
9. Accept the default base directory of `/etc` for runlevel scripts or type another base directory.
10. 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.
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.

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 package to a folder on the server, such as `\temp`.

Procedure

1. Locate the installation package.
2. Double-click the setup file, for example: `EMC_MnR_6.5.1_Windows_64-bit_Setup_File.exe`
3. Click **Next** on the **Welcome** screen.
4. Read and accept the End User License Agreement. Click **I Agree**.
5. 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**.
6. 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.

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

CHAPTER 3

Configuration

This chapter includes the following topics:

- Starting the EMC M&R platform services from the command line 20
- Starting the EMC M&R platform services on Windows 20
- Verifying if the EMC M&R platform services are running 21
- Configuring the user process limits for the Linux installation 23
- Logging in to the User Interface 23
- Connecting to Centralized Management 24
- Confirm configuration settings and register remote servers 24
- Licensing Operations 25
- Log in with administrator credentials 26
- View license information 26
- Upload a new license file 26
- Delete licenses 27
- Synchronize licenses on multiple hosts 27
- Troubleshooting licensing problems 28
- Permanent license stops working after host reconfiguration 28
- Users are locked out 28
- Module does not start or has no license 30
- Where to find the latest SolutionPack software 31
- Installing a SolutionPack 31
- Reviewing reports 32

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`
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

Verifying if the EMC M&R platform services are running

Verify the EMC M&R platform 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 EMC M&R platform application uses instead of root.

Procedure

1. Type the command for your operating system from the `bin` directory of the EMC M&R platform 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.

Results

Note

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

Example:

```
* Checking 'topology-mapping-service Default'... [ running ]
* Checking 'webservice-gateway Default'... [ running ]
```

```
* Checking 'mysql Default'... [ running ]
* Checking 'alerting-backend Default'... [ running ]
* Checking 'backend Default'... [ running ]
* Checking 'collector-manager Default'... [ running ]
* Checking 'collector-manager Generic-SNMP'... [ running ]
* Checking 'collector-manager Load-Balancer'... [ running ]
* Checking 'collector-manager emc smarts'... [ running ]
* Checking 'event-processing-manager emc smarts'... [ running ]
* Checking 'tomcat Default'... [ running ]
* Checking 'task-scheduler Default'... [ running ]
```

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 or APG privileges to check the log files.

Procedure

- Look for log files in these `/opt/APG/` directory paths.

  The list of available log files will vary depending upon choices made during installation. (Collector, Backend, Frontend, Default, or Minimal installations will generate different sets of log files.)

  ```
  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 upon choices made during installation. (Collector, Backend, Frontend, Default, or Minimal installations will generate different sets of log files.)

  ```
  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
  ```

Configuring the user process limits for the Linux installation

Increase the user process limits for the user account to a maximum of 65534. This modification enables services to open 65534 files and 65534 processes when needed.

Before you begin

- Make sure you have a login with root privileges.
- The EMC M&R platform installed on a server running Red Hat Enterprise Linux 6, CentOS Linux 6, or SUSE Linux Enterprise Server (SLES) 11.
- The name specified for the user account during the installation.

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  65534
   apg   soft  nofile  65534
   apg   hard  nproc   65534
   apg   soft  nproc   65534
   ```

3. Save the file.
4. Type the following commands from the `bin` directory of the installation to restart the services:

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

5. Type the following command to verify the changes:

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

Logging in to the User Interface

Log in to view reports or test user access.

Procedure

1. Open a browser, and then type the URL.

   Example: `http://<Frontend-hostname>:58080/APG`

2. Log in.
   a. Type the login credentials.

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

   b. Click **Sign In**.

After you finish

You are automatically logged off after four hours.

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 **`http://<serverIP:port>/centralized-management`**.

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

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

   Example:

   ```
   http://myHost.emc.com:58080/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.

Confirm configuration settings and register remote servers

Confirm configuration settings for the Frontend server after you first log in. In a multi-host environment, you must also register remote servers with the Frontend server and confirm those configuration settings too.

Before you begin

After you first log in with administrator credentials for core software, you must confirm the configuration settings for the Frontend server. If you install additional servers after installing the Frontend server (for example, collectors, backend server, and so forth), you must register each of them on the Frontend server.

Procedure

1. In the **Servers Configuration** window, click **Save** to accept the predefined values for the Frontend server. Fields that are blank must remain blank.
2. To register additional servers, log into **Centralized Management** and click **Configuration** › **Register a Server**.
3. Complete the fields and click **Save**.

   For detailed information about the entries, click **Documentation** and view the *Centralized Management Guide* or check the online help available from the User Interface.

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 26 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:

   ```
   http://frontend-hostname:58080/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 in ViPR SRM using the following URL:

   `http://frontend-hostname:58080/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 27.

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:

   `http://frontend-hostname:58080/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:

   ```
   http://frontend-hostname:58080/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:

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 26.

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 29
3. Restart the Tomcat service. See Restart Tomcat service on page 29.
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 30.

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:

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 ViPR SRM 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:

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:

   ```
   http://frontend-hostname:58080/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:

   ```
   http://frontend-hostname:58080/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.

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** › **License Management**. If the license is not listed, obtain one by completing a Support Request (SR) form, which you can find on the EMC support website http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation.
- Look for additional SolutionPack-specific installation instructions on the EMC Community Network (ECN) or the EMC Support website. For example, more detailed information may be found in *Service Assurance Suite SolutionPack Articles* available from the EMC support website or from the EMC Community Network. Many SolutionPacks have read me files embedded in the software. You can find these after you install the SolutionPack by navigating to **Centralized Management** › **SolutionPacks**. Expand the tree and click on the SolutionPack to open the Properties page where the document is listed.

Procedure

1. Log in and select **Administration**.
2. Select **Centralized Management** in the Administration tree.
3. Select **SOLUTIONPACK CENTER**.
4. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
5. Read the summary information and click **Install**.
6. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.

7. For each list box you select, a screen appears.
   a. Click **Next** after you complete each screen.
   b. Click **Install** after you complete the last screen.

   The installation process begins.
8. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.

After you finish

After the installation is complete, select **Centralized Management** › **SolutionPack** to verify the installed SolutionPack.

Reviewing reports

After you install a new release or migrate to a new release, check the reports to ensure that the data appears properly.

Before you begin

If the collector configuration changed, you can manually run the scheduled tasks in **Administration** › **Centralized-Management** › **Scheduled Tasks** › **Database** to speed up the report generation process. Wait at least two polling cycles before manually running the scheduled tasks.

To view your report:

Procedure

1. Navigate to **User Interface › SolutionPacks** or **User Interface › ReportPacks** depending upon which features you have installed.
2. Click the SolutionPack or ReportPack you want to view.

Results

It may take several polling cycles to display all relevant information.

CHAPTER 4

EMC M&R Platform Update

This chapter includes the following topics:

- Planning the upgrade 34
- Preparing the environment for the upgrade 34
- EMC M&R upgrade workflow 35
- Preparing for an update in a Linux environment 36
- Preparing for an update in a Windows environment 38
- Update all components 40
- Checking the status of remote host services 41
- Removing an obsolete Default ReportPack 41
- Validating the environment 42
- Update SolutionPacks and other components 42
- Update all SolutionPacks and other components 42
- Update all SolutionPacks 43
- Update all other components 44
- Update individual SolutionPacks or other components 45

Planning the upgrade

The procedures needed to upgrade to EMC M&R platform version 6.5.x vary depending upon the version you have installed.

In earlier versions of Watch4net documentation, the term, "migration" described how to move from one "point" release to the next. (For example, from 6.2 to 6.3.) The terms, "upgrade" or "update," described how to move from one software update bundle to the next. (For example, 6.3u1 to 6.3u2.)

In these procedures, a single term, "upgrade," describes all migration or update activities.

If you have:	Task:
Watch4net version 6.1.x	1. Migrate to version 6.2.x as described in the *EMC Watch4net Migration Guide* available from EMC Online Support. 2. Migrate from version 6.2.x to version 6.3.x as described in the *The EMC Watch4net Version 6.3 Installation and Configuration Guide*. 3. EMC M&R upgrade workflow on page 35
Watch4net version 6.2.x	1. Migrate to version 6.3.x as described in the *EMC M&R (Watch4net) Installation and Configuration Guide*. 2. EMC M&R upgrade workflow on page 35
EMC M&R (Watch4net) version 6.3.x	1. EMC M&R upgrade workflow on page 35
EMC M&R 6.4.x and higher versions	1. EMC M&R upgrade workflow on page 35

Preparing the environment for the upgrade

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

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

- Use your current backup software to perform backups of the EMC M&R environment before starting the upgrade .
- Look for blank reports and graphs. Determine if blank reports are cause by collection errors. Resolve any issues or document them for later follow up.
- Look for broken links. Resolve any issues or document them for later follow up
- Validate that End-to-End topology is working. Resolve any issues.
- Rename your old Default ReportPack if you are using a legacy default reportpack. A newer version of the Default ReportPack template may be installed during the upgrade, and you will need to delete the old one after checking your reports. Rename the existing Default ReportPack to make it easier to distinguish between the old and new versions. To rename it, click **Administration** › **ReportPacks** and edit the name of

the default ReportPack (for example, `Default ReportPack (olderversion)`). Click **Save**.

- Use the ViPR SRM Deployment Planner to determine sizing based on the set of Service Assurance Suite SolutionPacks you want to install.
  - 1. Download the ViPR SRM Deployment Planner from support.emc.com/downloads/34247_ViPR-SRM
    2. For additional details about determining configuration size, refer to *EMC Service Assurance Suite SolutionPack Performance and Scalability Guidelines* available on the EMC Support online website.
- Review the existing backend and databases. Check **Report Library** › **EMC M&R (Watch4net) Health** › **Module Performance** › **Databases**
  - Check backend thresholds to verify that you have room to accommodate new sizing
  - Add additional backends and databases as required (The metric count should not exceed 1 million.)
  - Refer to the *Watch4net Database Split* v1.2 document for help if you need to manually move data to redistribute the metrics.

EMC M&R upgrade workflow

You can upgrade the EMC M&R platform in a Linux, Windows, or mixed operating system environment. Ensure you back up all servers before starting the upgrade process.

Ensure new software is downloaded to all EMC M&R servers

If you have enabled Online Update for your system, the automatic update process has already downloaded and distributed new EMC M&R modules to each server. You do still have to run the launch-update script to upgrade the modules. Automated Online Update of EMC M&R Software on page 61 provides information about configuring your deployment to use the online update feature.

Upgrade workflow

1. Update module-manager on each server. Updating module-manager for Linux operating systems on page 37 or Updating module-manager for Windows on page 38
2. Update core modules by running the update script on each server. Preparing for an update in a Linux environment on page 36 or Preparing for an update in a Windows environment on page 38
3. Update all components on page 40
4. Verifying if the EMC M&R platform services are running on page 21
5. Removing an obsolete Default ReportPack on page 41

Mixed operating system deployments

To update a mixed-operating system deployment (non-vApp Linux and Windows), you must perform the steps for single operating system deployments separately, once on each platform.

One server must be the server that is hosting Centralized Management. For example, a Linux deployment with one Windows collector would required updating the Linux machine hosting Centralized Management and updating the Windows machine where the collector is running.

Preparing for an update in a Linux environment

Before you can update the EMC M&R platform in your Linux environment, you must complete certain tasks and run the setup script.

Before you begin

- 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 install binary files from your product page on the EMC support website. (For example, for Service Assurance Suite downloads, `EMC_MnR_6.5.1_Linux_64-bit_Setup_File.sh`. For Watch4net downloads, `setup-linux-x86_65u1-v64.sh`.) http://support.emc.com.

Note

If you have enabled Online Update for your system, the automatic update process has already downloaded and distributed the modules to each server. You can skip this binary file install process. Automated Online Update of EMC M&R Software on page 61 provides information about enabling and configuring Online Update.

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_6.5.1_Linux_64-bit_Setup_File.sh`
4. Run the setup script for your product. For example, `./EMC_MnR_6.5.1_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.

Results

Your system is now prepared for an update.

After you finish

Run the setup script on each Linux server that you want to upgrade.

Before starting core software services, ensure the library search path is correct on the server hosting the core software. This requirement applies to the `libaio` package on Linux. To verify the path:

1. Log in as root and run the following command: `ldconfig -v | grep -i libaio`

Output similar to the following should display:

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

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

Updating module-manager for Linux operating systems

Ensure the latest version of the `module-manager` module is installed before running the `launch-update` script.

The `launch-update` script is delivered through the module-manager, so update the module-manager module first.

Procedure

1. Type the command to update `module-manager` from the EMC M&R `/bin` directory.

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

   Example:

   ```
   ./opt/APG/bin/manage-modules.sh update module-manager
   ```

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 where the EMC M&R software is deployed. Core modules must be updated prior to any others, and they must be updated from the command line using the `launch-update` script. If the script fails for any reason, re-run it to resume the update.

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.

The system does not check files that were not were not included with the SolutionPacks.

Note

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

Procedure

1. Navigate to `<install directory>/Tools/Module-Manager/1.7/bin`.
2. Change the permissions for the `launch-update.sh` script:

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

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

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

4. 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.

5. To see the list of modules that were updated, issue this command: `./manage-modules.sh list installed`

   All modules except block-type modules are updated by the script. Block-type modules will be updated later from Centralized Management.

Preparing for an update in a Windows environment

Before you can update the EMC M&R platform in your Windows environment, you must complete certain tasks and run the setup executable.

Before you begin

- 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 install binary setup script from the EMC support website. (For example, for Service Assurance Suite downloads, `EMC_MnR_6.5.1_Windows_64-bit_Setup_File.exe`. For Watch4net downloads, `setup-win64-v65u1.exe`.) http://support.emc.com.
- Place the Windows installation binary setup script in a temporary folder on every server that you plan to upgrade.

Note

If you have enabled Online Update for your system, the automatic update process has already downloaded and distributed the modules to each server. You can skip ths binary file install process. Automated Online Update of EMC M&R Software on page 61 provides information about enabling and configuring Online Update.

Procedure

1. Locate the setup executable file for your product.
2. Double-click the executable file for your product. For example, `EMC_MnR_6.5.1_Windows_64-bit_Setup_File.exe`.
3. Click **Next**.
4. Read and accept the End User License Agreement. Click **I Agree**.
5. Press **Enter** to accept the default installation folder of `C:\Program Files\APG`, or specify a different directory.
6. Press **OK** to install the new packages in the `C:\Program Files\APG\Tools\Module-Repository` directory.

   Your system is now prepared for update.

After you finish

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

Updating module-manager for Windows

Ensure the latest version of the `module-manager` module is installed before running the `launch-update` script.

The `launch-update` script is delivered through the module-manager, so update the module-manager module first.

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`

   Use Windows Task Manager to verify that all of the APG services have stopped. Wait a few minutes for the services to stop, and then manually stop any services that are in the "Stopping" state.

2. Type the command to update `module-manager` from the EMC M&R `bin`.

   `<INSTALL_DIR>\bin\manage-modules.cmd update module-manager`

   Example:

   ```
   c:\Program Files\APG\bin\manage-modules.cmd update module-manager
   ```

Updating core modules in a Windows environment

Update EMC M&R foundation (core modules) using the `launch-update` script.

During this step, you will update the core modules on all of the servers where the EMC M&R software is deployed. Core modules must be updated prior to any others, and they must be updated from the command line using the `launch-update` script. If the script fails for any reason, re-run it to resume the update.

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.

The system does not check files that were not were not included with the SolutionPacks.

Note

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

Procedure

1. Navigate to `<install directory>\Tools\Module-Manager\1.7\bin`.
2. Run `launch-update.cmd`
3. 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.

4. To see the list of modules that were updated, issue this command from the `c:\Program Files\APG\bin` path: `manage-modules.cmd list installed`

   All modules except block-type modules are updated by the script. Block-type modules will be updated later from Centralized Management.

After you finish

You must manually remove the older version of Java after a Windows upgrade.

Deleting old Java files after Windows update

When upgrading from older versions of EMC M&R, there is an error on startup due to a file in the previous Java version folder not getting deleted 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 be 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 7.0u67 from the path 'C:\Program
Files\APG\Java\Sun-JRE\7.0u67’
```

Update all components

Update SolutionPacks and all other components to the latest software version.

Procedure

1. Navigate to the Installed SolutionPacks page: `http://<Frontend IP address>:58080/centralized-management/#/sp`
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. 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.

Checking the status of remote host services

The remote host services should start automatically after an upgrade. Check the services status and restart them manually if not running.

Before you begin

Check that all services have started on each of the hosts. Navigate to **Centralized Management › Host Services**. Select **Show all entries**. Verify that the status for each service is **Started**.

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

Procedure

1. Navigate to **Centralized Management › Physical Overview**.
2. Select the Frontend server or the server where Centralized Management is running. Click **Services**.

   Locate the stopped service and click its name to open the **Service Status** for the instance.
3. Click **Start**.

   If successful, the **Service Status** changes to **Started**. If the service does not start, review the log to determine the cause. The issue may be a misconfigured option that can be resolved by reconfiguring the SolutionPack settings and manually starting the service again.

Removing an obsolete Default ReportPack

After an upgrade, you may see duplicate nodes in the navigation tree. Delete the obsolete Default ReportPack to remove the duplicate nodes.

When you install or update the Report block of any SolutionPack, a generic-report module installs a default ReportPack template. This process does not remove or update an existing default ReportPack, and you may see duplicate node entries in the navigation tree as a result.

Procedure

1. Check the new reports after installing or updating a SolutionPack. Ensure any scheduled reports or pre-generated reports are set up to use the new Default ReportPack template before deleting the old one.

   You can find the list of scheduled reports and pre-generated reports by accessing Scheduled Reports in the User Interface or by viewing **Physical Overview › Tasks › report-scheduling** or **Centralized Management › Scheduled Tasks › report-scheduling**.
2. In the **User Interface**, select **Administration**.
3. Expand **ReportPacks**.
4. Expand the **Default ReportPack** and click the date to access the current default ReportPack.
5. If you see two **Default ReportPacks** in the pane, select the older one for deletion.

   Newer default ReportPacks show a version number associated with the release, for example, 3.5.0.0.

6. Click **Delete**.
7. Click **Save**.

Validating the environment

After upgrading your system, verify the operational status.

Before you begin

Procedure

1. Look for blank reports and graphs.

   Determine whether blank reports are caused by collection errors. Resolve issues or document them for later follow up.
2. Look for broken links. Resolve issues or document them for later follow up.
3. Validate that End-to-End topology is working. Resolve any issues.

Update SolutionPacks and other components

Learn how 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.

Refer to the *Automate the Download of Updates* article for details about Online Update.

The product provides several options for updating SolutionPacks and other components:

- Update all of the SolutionPacks and other components with a single click
- Update all of the SolutionPacks with a single click
- Update all of the other components with a single click
- Update individual SolutionPacks or other components

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.

Update all SolutionPacks and other components

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

Procedure

1. Navigate to the SolutionPacks page: `http://<Frontend IP address>:58080/centralized-management/#/sp`
2. Click the **Update All Components** button in the top-right corner of the page.

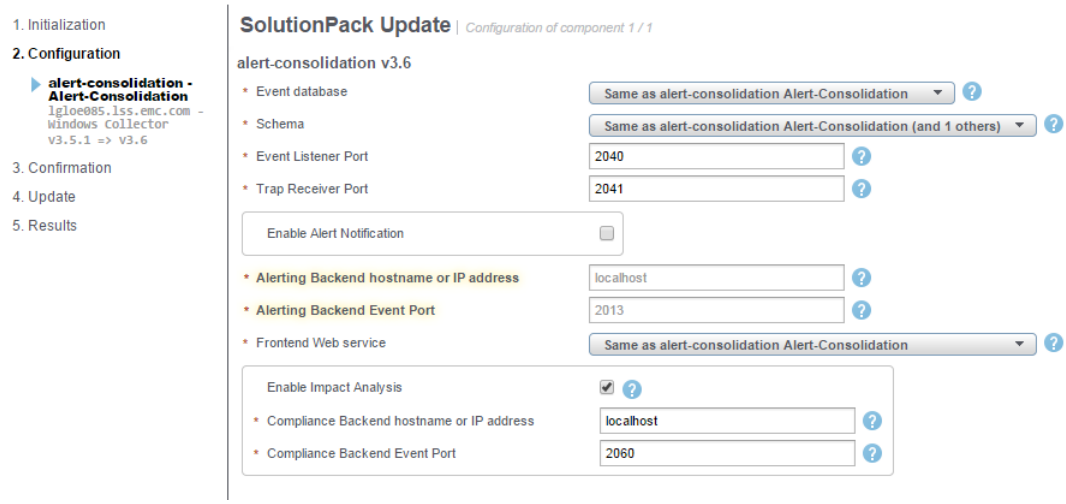
   The **Initialization** window opens and lists the following details:

   - 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.



4. 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**.
5. 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.
6. Review the update details for each component.

Update all SolutionPacks

You can update all of your installed SolutionPacks with a single click.

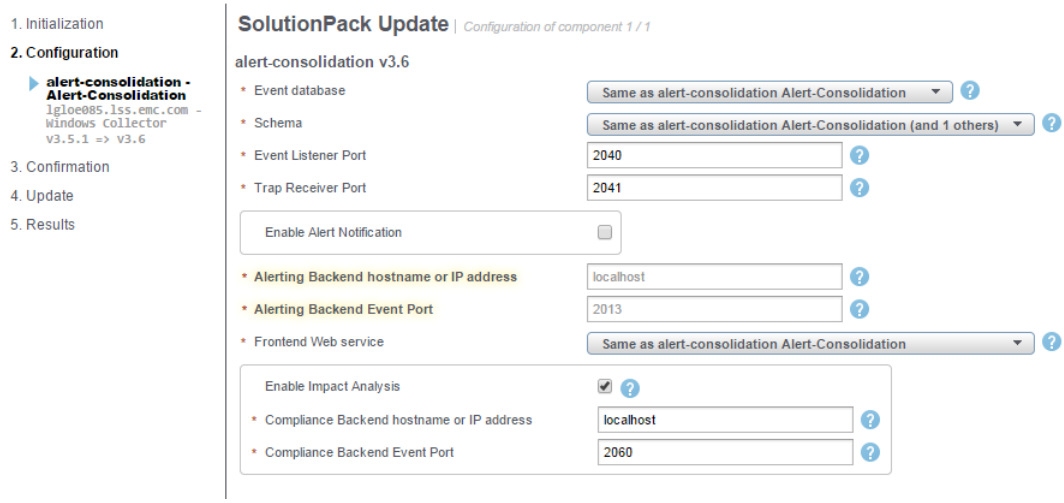
Procedure

1. Navigate to the SolutionPacks page: `http://<Frontend IP address>:58080/centralized-management/#/sp`
2. Click the **Select All** button located below the SolutionPacks table, and then click the **Update** button.

   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.



4. 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**.
5. 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.
6. Review the update details for each component.

Update all other components

You can update all of your other installed components with a single click.

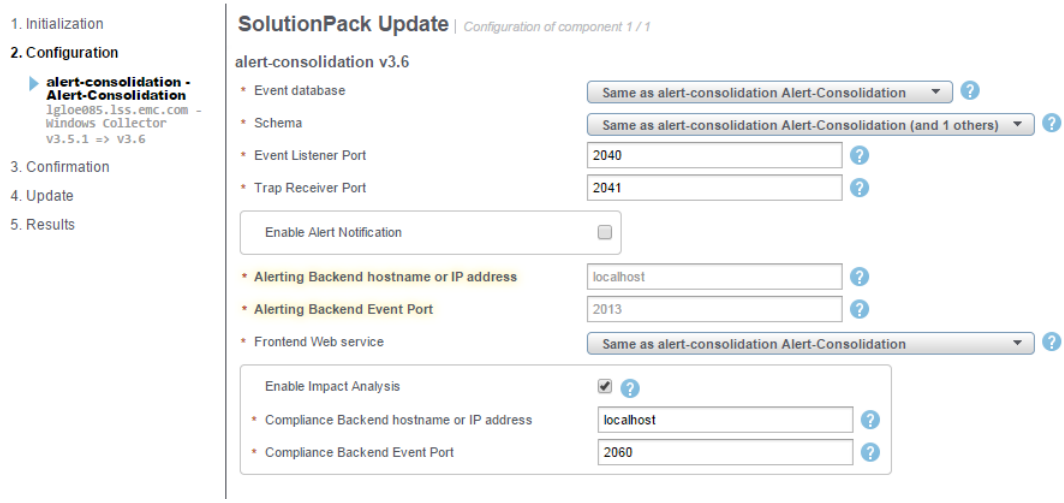
Procedure

1. Navigate to the SolutionPacks page: `http://<Frontend IP address>:58080/centralized-management/#/sp`
2. Click the **Select All** button located below the Other Components table, and then click the **Update** button.

   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.



4. 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**.
5. 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.
6. Review the update details for each component.

Update individual SolutionPacks or other components

You can easily update individual SolutionPacks or other components.

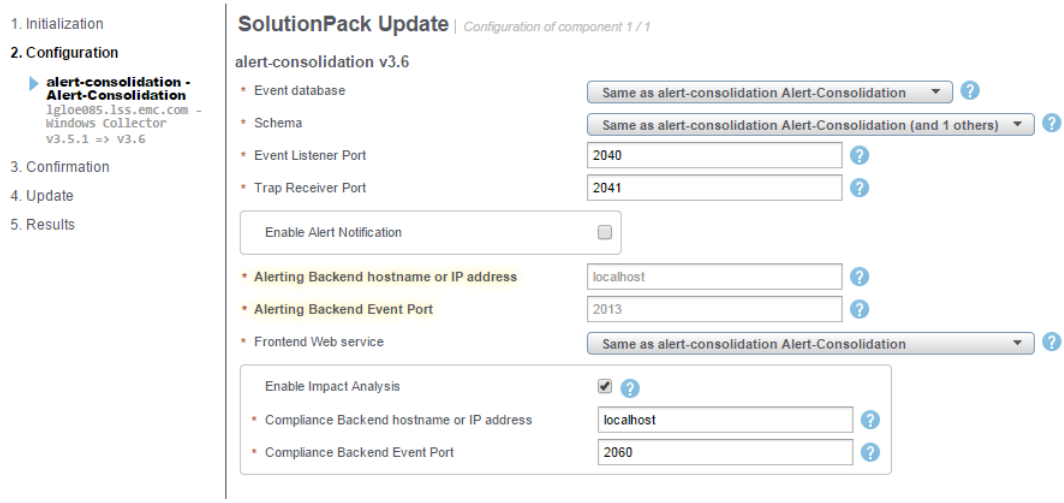
Procedure

1. Navigate to the SolutionPacks page: `http://<Frontend IP address>:58080/centralized-management/#/sp`
2. In the SolutionPacks table or the Other Components table, click the update icon for the SolutionPack or component 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.



4. 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**.
5. 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.
6. Review the update details for each component.

CHAPTER 5

Uninstallation

This chapter includes the following topics:

- Overview 48
- Stopping EMC M&R platform services on a UNIX server 48
- Uninstalling EMC M&R platform from a UNIX server 48
- Stopping EMC M&R platform services on a Windows server 48
- Uninstalling EMC M&R platform from a Windows server 49
- Uninstalling a SolutionPack 49

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 6

Troubleshooting

This chapter includes the following topics:

- Troubleshooting service start-up problems on UNIX 52
- Troubleshooting service start-up problems on Windows 52
- SSL certificates 52

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 or APG privileges to check the log files.

Procedure

- Look for log files in these `/opt/APG/` directory paths.

  The list of available log files will vary depending upon choices made during installation. (Collector, Backend, Frontend, Default, or Minimal installations will generate different sets of log files.)

```
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 upon choices made during installation. (Collector, Backend, Frontend, Default, or Minimal installations will generate different sets of log files.)

```
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
```

SSL certificates

Generally, EMC products are distributed with a self-signed SSL certificate. If you receive an SSL certificate error or a blank pane when you are attempting to access content served by a data source, resolve the issue by doing one of the following procedures.

SSL certificate error examples on page 53 provides a list of sample errors.

Temporary resolution

Accept the certificate exception temporarily: Troubleshooting an SSL certificate error: Accepting the exception on page 53.

Permanent resolution

Add an SSL certificate to your truststore to permanently prevent the exceptions from appearing.

You can:	Perform:
Install the self-signed SSL certificate that is provided with the EMC product using an Internet Explorer browser.	Installing a self-signed SSL certificate from an Internet Explorer browser on page 54
Install the self-signed SSL certificate that is provided with the EMC product using a Chrome or Firefox browser.	1. Export the self-signed SSL certificate to save it to the export location: Exporting an SSL certificate from an Internet Explorer browser on page 55 2. Importing an SSL certificate into your truststore on page 54
Import an exported SSL certificate that you or another administrator prepared.	Importing an SSL certificate into your truststore on page 54

If you need to prepare an SSL certificate to share with other users, use: Exporting an SSL certificate from an Internet Explorer browser on page 55.

SSL certificate error examples

The SSL certificate error or a blank pane appears because the certificate is self-signed and it is not added as an exception or into the truststore yet. For example, if you are attempting to access content served by a data source, a blank pane appears when you select views under **SolutionPacks**.

Chrome error examples

```
This site's security certificate is not trusted!
```

Or, a blank pane.

Firefox error example

```
This Connection is Untrusted
```

Internet Explorer error examples

```
There is a problem with this website's security certificate.
```

```
Content was blocked because it was not signed by a valid security
certificate.
```

Troubleshooting an SSL certificate error: Accepting the exception

An SSL certificate error appears in your browser.

To resolve this issue,

Procedure

- Accept the exception.

  Steps may vary for your browser. For example, for Internet Explorer, click **Continue to this website (not recommended)**.

This temporary solution causes the exception to be ignored for the current browser session, but the exception reappears if you open another browser tab or window.

Installing a self-signed SSL certificate from an Internet Explorer browser

Install the self-signed SSL certificate that is provided with the EMC product to prevent certificate exception errors.

The following procedure is for Internet Explorer version 9.0. The steps may vary slightly depending on your browser version.

Procedure

1. Click **Continue to this website (not recommended)** in the browser window.
2. Click the red **Certificate Error** indicator next to the address bar.
3. In the **Untrusted Certificate** window, select **View certificates**.
4. In the **Certificate** dialog box, in the **General** tab, click **Install Certificate**.
5. Follow the instructions in the **Certificate Import Wizard**.
   a. Select the **Place all certificates in the following store** setting to add the certificate to your truststore.
6. In the **Certificate** dialog box, in the **General** tab, click **OK**.

After you finish

Refresh the browser window.

Importing an SSL certificate into your truststore

Import an SSL certificate into your truststore to prevent certificate exception errors.

Procedure

- Import the certificate using one of the following procedures:
  - Importing an SSL certificate in Chrome on page 54
  - Importing an SSL certificate in Firefox on page 55
  - Importing an SSL certificate in Internet Explorer on page 55

Importing an SSL certificate in Chrome

For Chrome, use this procedure to import the certificate into your truststore.

The following procedure is for Chrome version 28.0.1500.95. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Settings** › **Show advanced settings**.
2. Scroll down and select **HTTP/SSL** › **Manage Certificates**.
3. In the **Trusted Root Certification Authorities** tab, click **Import**.
4. Follow the instructions in the **Certificate Import Wizard** to import the certificate.
5. Click **OK** in **Internet options**.
6. Refresh the browser window.

Importing an SSL certificate in Firefox

For Firefox, use this procedure to import the certificate into your truststore.

The following procedure is for Firefox version 23.0. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Firefox** › **Options** › **Options**.
2. Click **Advanced**.
3. In the **Certificates** tab, click **View Certificates**.
4. Click **Import**.
5. Locate the certificate file and click **Open**.
6. Click **Save**.
7. Click **OK** in **Certificate Manager**.
8. Refresh the browser window.

Importing an SSL certificate in Internet Explorer

For Internet Explorer, use this procedure to import the certificate into your truststore.

The following procedure is for Internet Explorer version 9.0. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Tools** › **Internet options**.
2. In the **Content** tab, click **Certificates**.
3. Select the **Trusted Root Certification Authorities** tab.
4. Click **Import**.
5. Follow the instructions in the **Certificate Import Wizard** to import the certificate.
6. Click **OK** in **Internet options**.
7. Refresh the browser window.

Exporting an SSL certificate from an Internet Explorer browser

Use this procedure to export a self-signed SSL certificate, so that you can either import the resulting exported certificate into your truststore or share it with other users.

The following procedure is for Internet Explorer version 10.0. The steps may vary slightly depending on your browser version.

Procedure

1. Access the host for which you want to export the SSL certificate from the browser.

   For example: `https://<myHostname>.emc.com`
2. Select **Continue to this website (not recommended)** in the **There is a problem with this website's security certificate** window.
3. Click the red **Certificate Error** indicator next to the address bar.
4. In the **Untrusted Certificate** window, select **View certificates**.
5. In the **Certificate** dialog box, select the **Details** tab and ensure that the Show field is set to All. Click **Copy to File**.

6. In the **Certificate Export Wizard**,
   a. Click **Next** in the **Welcome** screen.
   b. Click **Next** to accept the default DER encoded binary X.509 setting in the **Export File Format** screen.
   c. Browse to the location where you want to save the certificate.
   d. Specify the certificate file name and click **Save**.
   e. In the **File name** field, ensure that the location and the certificate file name are correct. Click **Next**.
   f. Click **Finish**.
   g. Click **OK** when `The export was successful` appears.
7. In the **Certificate** dialog box, click **OK** in the **Details** tab.
8. Share the resulting exported SSL certificate with other users to use.

APPENDIX A

Available Modules

This appendix includes the following topics:

- Available modules 58

Available modules

Each type of installation (Default, Minimal, Frontend, Backend, or Collector) installs a set of core modules. These module installations then trigger additional modules to be installed. For the full list of modules that are installed, issue the `manage-modules.sh list installed` or `manage-modules.cmd list installed` command from the `/bin` folder in your installation path.

Table 5 Version 6.5u1 available modules

Module Name	Version	Install type
Administration-Tool	v1.3u1	Default / Frontend / Backend
alert-consolidation	v3.6	Default / Backend
Alerting-Backend	v3.8u1	Default / Backend
Alerting-Frontend	v3.8u1	Default / Frontend
APG-Backend	v5.8	Default / Backend
Centralized-Management	v2.4u1	Default / Frontend
Collector-Manager (emc-watch4net-health)	5.6	Default / Frontend
Compliance-Backend (generic-compliance)	v3.5u1???	Default / Backend
Device-Discovery	v3.4u1	Default / Frontend
APG-Diagnostic-Tools	v6.0	Default / Frontend / Backend / Collector
APG-Frontend	v6.5u1	Default / Frontend
Frontend-Report-Generator	v6.5u1	Default / Frontend
Frontend-Search	v6.5u1	Default / Frontend
Frontend-WS	v6.5u1	Default / Frontend
generic-rsc	v3.6.1	Default / Collector
generic-snmp	v3.6.1	Default / Collector
generic-topology	v3.6.1	Default / Backend
License-Manager	v5.4	Default / Minimal / Frontend / Backend / Collector
load-balancer-arbiter	v3.6.1	Default / Backend
Maps-Service	v2.0	Default / Frontend
Mib-Browser	v6.5u1	Default / Frontend
Module-Manager	v1.7u1	Default / Minimal / Frontend / Backend / Collector
MySQL	v5.5.36	Default / Backend / Database
MySQL-Maintenance-Tool	v1.4	Default / Backend

Table 5 Version 6.5u1 available modules (continued)

Module Name	Version	Install type
APG-Property-Store	v2.0	Default / Frontend / Database
Task-Scheduler	v1.6u1	Default / Backend
Tomcat	6.0.43	Default / Frontend
Topology	v1.7	Default / Backend
Topology-Service	v1.2u1	Default / Backend
Webservice-Gateway	v2.0	Default / Minimal / Frontend / Backend / Collector

APPENDIX B

Automated Online Update of EMC M&R Software

This chapter includes the following topics:

- Online Update overview 62
- Configuring server settings for online updates 62
- Enabling the online update task 62
- Running the online update task manually 63
- Online Update Status 63
- Online Update History 64
- Disabling the online update task 64

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. By default, online update uses the EMC Online Support username and password specified under **Configuration** › **EMC Support**. If you want to use different credentials, click **Override Support Credentials**. These credentials are used only for online update.
6. 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.
7. 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.

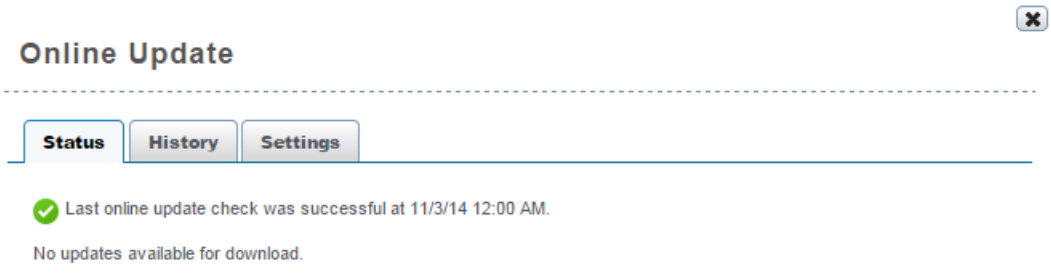
Procedure

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 1 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 2 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**.

APPENDIX C

Virtual Appliance Installation

This appendix includes the following topics:

- Virtual Appliance installation for EMC M&R 68
- Deploying an appliance 68
- Starting the appliance 70
- Verifying the appliance deployment 70
- Log onto the appliance 70
- Installing a SolutionPack 71
- Reviewing reports 72

Virtual Appliance installation for EMC M&R

You can deploy EMC M&R as a virtual appliance (vApp) in a vSphere or vCloud environment, as an alternative to the standard installation.

A virtual appliance (vApp) is a software solution composed of one or more virtual solutions that is packaged by an appliance vendor and can be deployed, managed, and maintained as a unit.

vApps are distributed using Open Virtualization Format (OVF) files. Depending on your environment requirements, two types of OVF installations are available to install the EMC M&R platform:

- Four VM vApp installation - Distributes EMC M&R platform components across four VMs (Frontend, Primary Backend, Additional Backend, Collector). The appliances in this installation are pre-configured to communicate with each other, offering an out-of-the-box configuration that can function in smaller environments. You can further scale and extend the environment by installing additional virtual appliances using the one VM vApp installation.
- One VM vApp installation - Has the potential to install any of the EMC M&R platform components in a single VM. This can be used to either install a single, consolidated VM with all components for evaluation purposes, or to add additional Backend or Collector appliances to extend or scale the environment created using the four VM vApp installation.

Note

The vApp deployment should be used only for new installations. If you need to upgrade an existing installation, use the standard binary setup script or executable to migrate to a newer release. The vApp deployment support was not available prior to the EMC M&R 6.3 release.

Deploying an appliance

You can deploy an appliance from an OVF file using a vSphere Client.

Before you begin

- An administrator login with root privileges
- vCenter location where you are deploying the appliance
- Data store you can use for deployment
- Static IP address to assign to your appliance
- Gateway
- Netmask
- DNS Servers

Procedure

1. Open vSphere Client and connect to the vCenter Server that manages your VMware environment.
2. From the **File** menu, select **Deploy OVF Template**.
3. In the **Source** step, browse to the location of the `YourOVFfile.ovf` file.

   Example file path: `/opt/ovf/YourOVFfile_OVFxx.ovf`

Example URL: `http://myHost.emc.com/ovf/snapshot/92/YourOVFfile_OVFxx.ovf`

4. Click **Next**.

   To minimize the deployment time, deploy the appliance within the same local area network (LAN) shared by your VMware ESX/ESXi servers. The deployment time is approximately 5 to 15 minutes. Deployment across a WAN can take 2 hours or more.

5. In the **OVF Template Details** step, review the details of the loaded .ovf file and click **Next**.
6. In the **End User License Agreement** step, review the license agreement. Click **Accept** and then click **Next** to continue.
7. In the **Name and Location** step:
   a. Type a **`Name`** for the appliance.
   b. Specify an **`Inventory Location`** for the appliance within your VMware environment.
   c. Click **Next**.
8. In the **Host/Cluster** step, select a host or cluster where the appliance will run and click **Next**.
9. In the **Resource Pool** step, select a resource pool associated with the host or cluster where the appliance will run and click **Next**.

   Note

   This step is required only if the host or cluster contains a predefined resource pool.

10. In the **Datastore** step, select a datastore to hold the appliance images and click **Next**.
11. In the **Disk Format** step, select the storage space provisioning method and click **Next**.

Option	Description
Thin provisioned format	On-demand expansion of available storage, used for newer data store file systems.
Thick provisioned format	Appliance storage that is allocated immediately and reserved as a block.

   Note

   The **Thin provisioned format** option is recommended when the vApp is deployed in a high performance environment.

12. In the **Network Mapping** step, select a destination network that has an IP Pool associated with it and click **Next**.
13. Provide the values of the properties as defined in the Virtual Appliance Properties table and click **Next**.
14. In the **Ready to Complete** step, review the list of properties for the appliance and click **Finish**.

    A status bar appears in the vSphere Client showing the deployment progress.

15. After deployment is complete, click **Close** in the **Deployment Completed Successfully** dialog box.

Starting the appliance

Start the appliance using vSphere after deployment. The appliance may take up to 20 minutes to start the first time. You can monitor the progress on the vSphere console.

Procedure

1. In the vSphere Client, right-click the appliance name.
2. Select **Power** › **Power On**.

   The status appears in the **Recent Tasks** bar.

Verifying the appliance deployment

After deploying the appliance, verify that it is working.

Procedure

1. In the vSphere client, navigate to the **VMs and Templates** view.
2. From the configured resource pool, find the resource pool you selected for the appliance.

   The new appliance is listed under the resource pool.
3. In the console, log in to the appliance with the credentials you defined during the deployment.
4. Verify the services.

Log onto the appliance

Using a browser, you can access the appliance to view and manage your applications as well as develop applications.

Procedure

1. Open a web browser.
2. Browse to the appliance at `http://<Frontend-hostname>:58080/APG`.

   hostname is the fully qualified domain name of your host.

   A security-related dialog box may appear asking you to accept a security certificate from EMC. Accept the certificate or allow a security exception for and continue. To eliminate this message from appearing, install a Certificate Authority-signed SSL certificate.
3. Enter the default username and password.

Passwords

Use passwords to control access to the appliance.

Table 6 Default usernames and passwords

Environment	Username and password
Web-based console accessed in a browser	**`admin`**/**`changeme`** Ensure that you change this password.

Table 6 Default usernames and passwords (continued)

Environment	Username and password
Linux guest OS appliance console accessed through SSH or vSphere	`root/Changeme1!`

If you set the appliance console password while you deployed the OVF, the password that you entered is the default password.

Passwords must conform to the following requirements.:

- Be at least eight characters and no more than 40 characters
- Contain at least one numeric character
- Contain at least one uppercase and one lowercase character
- Contain at least one non-alphanumeric character such as # or !
- Cannot contain the single quote character (') because it is a delimiter for the password string

Note

These requirements do not apply to the Linux passwords.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** › **License Management**. If the license is not listed, obtain one by completing a Support Request (SR) form, which you can find on the EMC support website http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation.
- Look for additional SolutionPack-specific installation instructions on the EMC Community Network (ECN) or the EMC Support website. For example, more detailed information may be found in *Service Assurance Suite SolutionPack Articles* available from the EMC support website or from the EMC Community Network. Many SolutionPacks have read me files embedded in the software. You can find these after you install the SolutionPack by navigating to **Centralized Management** › **SolutionPacks**. Expand the tree and click on the SolutionPack to open the Properties page where the document is listed.

Procedure

1. Log in and select **Administration**.
2. Select **Centralized Management** in the Administration tree.
3. Select **SOLUTIONPACK CENTER**.
4. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
5. Read the summary information and click **Install**.

6. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
7. For each list box you select, a screen appears.
   a. Click **Next** after you complete each screen.
   b. Click **Install** after you complete the last screen.

   The installation process begins.
8. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.

After you finish

After the installation is complete, select **Centralized Management** › **SolutionPack** to verify the installed SolutionPack.

Reviewing reports

After you install a new release or migrate to a new release, check the reports to ensure that the data appears properly.

Before you begin

If the collector configuration changed, you can manually run the scheduled tasks in **Administration** › **Centralized-Management** › **Scheduled Tasks** › **Database** to speed up the report generation process. Wait at least two polling cycles before manually running the scheduled tasks.

To view your report:

Procedure

1. Navigate to **User Interface › SolutionPacks** or **User Interface › ReportPacks** depending upon which features you have installed.
2. Click the SolutionPack or ReportPack you want to view.

Results

It may take several polling cycles to display all relevant information.

APPENDIX D

Restoring Modules to their Previous Version

This appendix includes the following topics:

- Restoring modules workflow 74
- Listing restorable modules 74
- Restoring modules 75
- Starting the EMC M&R platform services from the command line 77
- Starting the EMC M&R platform services on Windows 78

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 6.5.x version of Module Manager is fully compatible with version 6.4.x 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 74
2. Restoring modules on page 75
3. Start the EMC M&R platform services: Starting the EMC M&R platform services from the command line on page 20 or Starting the EMC M&R platform services on Windows on page 20

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
   -------------------------- ----------------------- -------
--------------------
 * variable-handling-filter  Generic-SNMP            v1.8u3
11/26/13 9:00:30 AM
 * property-tagging-filter   Generic-SNMP            v2.5u1
11/26/13 8:57:46 AM
 * frontend-report-generator Default                 v6.2u3
11/26/13 8:38:01 AM
 * collector-manager         emc-smarts              v5.3u2
11/26/13 8:31:29 AM
 * event-processing-manager  emc-smarts              v1.2u3
11/26/13 8:32:29 AM
```

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>]`
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 6.5.x to 6.4.x. 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 6.5.x to 6.4.x. 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 6.4.

```
./manage-modules.sh restore frontend-ws apg-ws 6.4
./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`
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