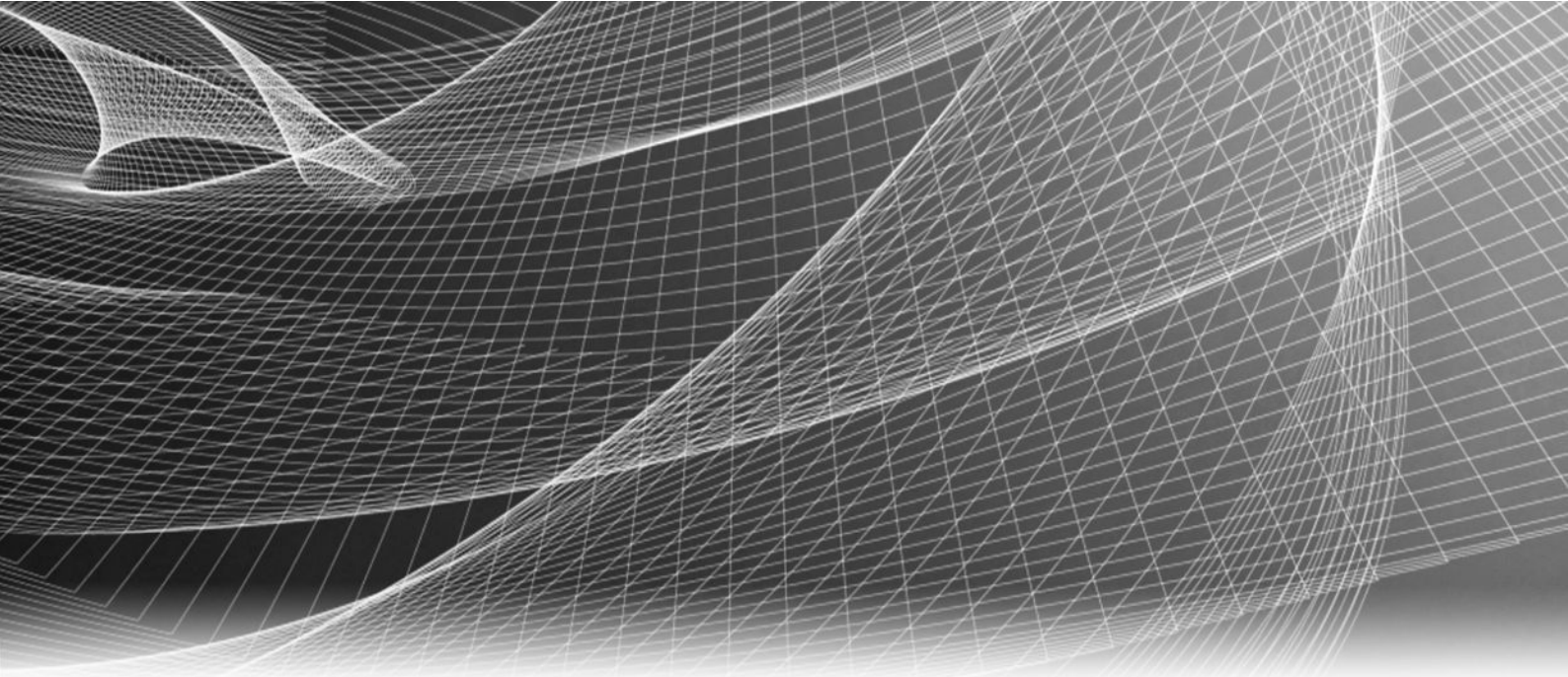




EMC[®] Storage Resource Management Suite

Version 3.0

Installation and Configuration Guide

PN 302-000-506

REV 02

Copyright © 2013 EMC Corporation. All rights reserved. Published in USA.

Published December, 2013

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>). For documentation on EMC Data Domain products, go to the EMC Data Domain Support Portal (<https://my.datadomain.com>).

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

CONTENTS

Tables		7
Chapter 1	Installation Workflow	9
	Core software	10
	Storage Resource Management Suite SolutionPacks	10
Chapter 2	Virtual Appliance Installation	11
	Virtual Appliance installation overview	12
	Four VM vApp installation option	12
	One VM vApp installation option	12
	Deploying an appliance	13
	Starting the appliance	14
	ISO image mounted on vApp startup	15
	Verifying the appliance deployment	15
	Logging in to the User Interface	15
	Passwords	15
	Expanding disk space	16
	Virtual Machine components	16
Chapter 3	Standard Installation	21
	Standard installation options	22
	Installing core software on UNIX	22
	Installing core software on Windows Server	23
	Virtual Machine components	24
Chapter 4	Configuration	27
	Starting the core software services from the command line	28
	Starting the core software services on Windows	28
	Verifying if the core software services are running	29
	Troubleshooting service start-up problems on UNIX	29
	Troubleshooting service start-up problems on Windows	30
	Logging in to the User Interface	30
	Connecting to Centralized Management	30
	Confirming settings for the first time	31
	Installing core suite licensing	31
	Adding licenses	31
	Verifying core software licenses from Centralized Management	32
	Configuring the user process limits for the Linux installation	32
Chapter 5	Infrastructure Preparation for Discovery and Data Collection	35
	Host preparation for discovery and data collection	36
	Windows Host configuration for discovery and data collection	36
	UNIX and Linux host configuration for discovery and data collection	42
	Configuring ESX hosts to collect PowerPath metrics	44

	Configuring hosts to collect PowerPath metrics.....	44
	Installing EMC Host Interface on Windows Server.....	44
	Switch configuration for discovery and data collection.....	47
	Brocade switch configuration.....	47
	Cisco switch configuration.....	48
	Storage system preparation for discovery and data collection.....	51
	Preparing EMC Centera.....	51
	Preparing Converged Infrastructure.....	52
	Preparing EMC Data Domain.....	52
	Preparing EMC Isilon.....	52
	Preparing EMC VMAX.....	52
	Preparing EMC VNX.....	56
	Preparing EMC VPLEX.....	58
	Preparing Hitachi Device Manager.....	58
	Preparing HP 3PAR StoreServ.....	58
	Preparing HP EVA.....	59
	Preparing IBM DS.....	59
	Preparing IBM XIV.....	59
	Preparing NetApp Filer.....	60
	Preparing VI VirtualWisdom.....	60
Chapter 6	SolutionPack Installation	63
	Connecting to Centralized Management.....	64
	Installing a SolutionPack.....	64
	Configuration during SolutionPack installation.....	65
	Post-installation configuration of SolutionPacks.....	82
	Post-installation configuration details.....	86
	Configuring Solutions Enabler client access for VMAX.....	86
	Enabling passive host discovery through Brocade FC SolutionPack.....	90
	Enabling passive host discovery through Generic-SNMP.....	90
	Post-install configuration for SolutionPack for Physical Hosts.....	91
	Configuring compliance-frontend.xml.....	92
Chapter 7	Migration for Multiple Hosts	95
	Migration workflow.....	96
	Migration for multiple hosts with installed SolutionPacks.....	96
	Migrating core software on a UNIX server.....	99
	Migrating core software on a Windows server.....	99
	Identifying which modules to update.....	100
	Module update order for multiple hosts.....	100
	Updating modules.....	103
	Recommendations for answering module update questions.....	104
	manage-modules.sh update command.....	105
	Updating all core software services from the command line.....	106
	Starting the core software services from the command line.....	106
	Logging in to Centralized Management.....	107
	Confirming settings for the first time.....	107
	Retrieving the list of modules from remote host servers using Centralized Management.....	108
	Updating modules from Centralized Management.....	108
	Recommendations for answering module update questions.....	109
	Installing the generic-rsc package.....	110
	Installing the generic-topology package.....	110

	Installing the Maps-Service package.....	111
	Updating the SolutionPackBlocks.....	111
	Controlling services from Centralized Management.....	112
	Default ReportPack migration.....	112
	Exporting a ReportPack.....	113
	Updating the Default ReportPack.....	113
	Deleting a ReportPack.....	114
	Installing a SolutionPack.....	114
	Post-migration tasks.....	115
	Installing SolutionPack for Storage Compliance.....	115
	Creating and configuring storage compliance schema.....	117
	Configuring alert consolidation features in a migration scenario.....	118
	Reviewing reports.....	122
Chapter 8	Migration for Single Host	123
	Migration workflow.....	124
	Migration for single host with installed SolutionPacks.....	124
	Migrating core software on a UNIX server.....	126
	Migrating core software on a Windows server.....	126
	Identifying which modules to update.....	127
	Module update order for single hosts.....	128
	Updating modules.....	129
	Recommendations for answering module update questions.....	130
	Updating all core software services from the command line.....	131
	Starting the core software services from the command line.....	132
	Logging in to Centralized Management.....	132
	Confirming settings for the first time.....	133
	Updating modules from Centralized Management.....	133
	Recommendations for answering module update questions.....	133
	Installing the generic-rsc package.....	135
	Installing the generic-topology package.....	135
	Installing the Maps-Service package.....	136
	Updating the SolutionPackBlocks.....	136
	Controlling services from Centralized Management.....	137
	Default ReportPack migration.....	137
	Exporting a ReportPack.....	138
	Updating the Default ReportPack.....	138
	Deleting a ReportPack.....	139
	Reviewing reports.....	139
Chapter 9	Suite Software Uninstallation	141
	Overview.....	142
	Stopping core software services on a UNIX server.....	142
	Uninstalling core software from a UNIX server.....	142
	Stopping core software services on a Windows server.....	142
	Uninstalling core software from a Windows server.....	143
	Uninstalling a SolutionPack.....	143
Chapter 10	Suite Software Updates	145
	Updating standard installations.....	146
	Updating the core software installation.....	146
	Installing a SolutionPack Center Update.....	152
	Updating an existing SolutionPack.....	154

TABLES

1	Installed components.....	17
2	Installed components.....	24
3	SolutionPack configuration details.....	65
4	Group A: Core modules for CLI update.....	101
5	Group B: Launch the update from Centralized Management › Logical Overview.....	102
6	Group A: Core modules for CLI update.....	128
7	Group B: Core modules to update from Centralized Management.....	129
8	Group A: Core modules for CLI update.....	148
9	Group B: Launch the update from Centralized Management › Logical Overview.....	148

CHAPTER 1

Installation Workflow

This chapter includes the following topics:

- ◆ [Core software](#)..... 10
- ◆ [Storage Resource Management Suite SolutionPacks](#)..... 10

Core software

The core software platform provides a reporting solution built on a scalable architecture of distributed backends, frontends, collectors and databases.

Installing the core software platform establishes the foundation for the suite, providing common capabilities, functions and user interfaces available to all suite users, regardless of the specific installed SolutionPacks.

You can install suite software as a Virtual Appliance in a VMWare environment or using a standard binary installation:

- ◆ The Virtual Appliance installation enables you to deploy the suite software as an appliance in a supported VMWare environment.
- ◆ Alternatively, you can perform a standard, or binary, installation of the suite software on physical or virtual servers.

Storage Resource Management Suite SolutionPacks

The suite includes a number of storage infrastructure-related SolutionPacks to support EMC and third-party storage infrastructure components.

Refer to the following documents for details on SolutionPacks supported with Storage Resource Management Suite:

- ◆ *EMC Storage Resource Management Suite Support Matrix*
- ◆ *EMC Storage Resource Management Suite Release Notes*

CHAPTER 2

Virtual Appliance Installation

This chapter includes the following topics:

♦ Virtual Appliance installation overview	12
♦ Deploying an appliance	13
♦ Starting the appliance	14
♦ Verifying the appliance deployment	15
♦ Logging in to the User Interface	15
♦ Expanding disk space	16
♦ Virtual Machine components	16

Virtual Appliance installation overview

You can deploy the suite in a supported VMWare environment.

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.

Storage Resource Management Suite vApps are distributed using Open Virtualization Format (OVF) files. Depending on your environment requirements, two types of OVF installations are available to install the suite core software:

- ◆ Four VM vApp installation - Distributes core software components across four VMs (Frontend, Primary Backend, Additional Backend, and Collector). The VMs 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 VMs using the one VM vApp installation.
- ◆ One VM vApp installation - Has the potential to install any of the core software components in a single VM. This can be used to install a single, consolidated VM with all components for evaluation purposes, or to add additional Backend and 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 Storage Resource Management Suite 3.0 release.

Four VM vApp installation option

Use this procedure to install the four VM vApp.

The four VM vApp installation deploys four VMs:

- ◆ Frontend VM - This VM hosts the web portal and centralized management applications and controls licensing.
- ◆ Primary Backend VM - This VM hosts the primary database, back end components, load balancer/arbitrator and modules which support capacity, alerting and topology. You can have only one instance of the Primary Backend in your environment.
- ◆ Additional Backend VM - This VM includes back end components and timeseries databases and is used to scale out back end processing.
- ◆ Collector VM - This VM hosts collectors used to discover, collect and process data from supported hosts, switches and storage devices.

One VM vApp installation option

Use this option to install a vApp which includes all core software components or to extend a four VM vApp environment to include additional vApps.

This installation provides a specific appliance as a single virtual machine, including:

- ◆ Frontend VM - This appliance hosts the web portal and centralized management applications and controls licensing.

- ◆ Primary Backend VM - This VM hosts the primary database, back end components, load balancer/arbitrator and modules which support capacity, alerting and topology. You can have only one instance of the Primary Backend in your environment.
- ◆ Additional Backend VM - This VM includes back end components and timeseries databases.
- ◆ Collector VM - This VM hosts collectors used to discover, collect and process data from supported hosts, switches and storage devices.

In addition, the one VM vApp installation provides the following specialized installation options:

- ◆ All-In-One Appliance - This vApp is intended for a small site or to conduct proof of concept activities with the suite software and installs Frontend, Backend and Collector core software components on a single virtual machine.
- ◆ Minimal Installation - Installs the minimal base software components required for the core software, enabling a custom installation options on a single virtual machine.

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.

ISO image mounted on vApp startup

A ISO image used for deployment is included in the vApp and must be present first startup.

When the vApp is first started, a mounted ISO image provides required information needed during deployment.

You can safely leave the ISO image mounted and it will be persisted in subsequent restarts.

If you manually remove the ISO image after initial startup, it will not re-mount when the system restarts.

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.

Logging in to the User Interface

Log in to continue to view reports or to test user access by specifying operator credentials.

Procedure

1. Point your browser to the URL.

For example, `http://<Frontend-hostname>:58080/APG`

2. Log in.

- a. Type the login credentials.

The default username is **admin** and the default password is **changeme**.

- b. Click **Sign In**.

After you finish

Note

You are automatically logged off after four hours.

Passwords

Use passwords to control access to the appliance.

The default usernames and passwords are:

Environment	Username and password
Web-based console accessed via a browser	admin/changeme Make sure you change this password.
Linux guest OS appliance console accessed via SSH or vSphere	root/Changeme1!

If you set the appliance console password while you were deploying the OVF, the password you entered is the default password.

Passwords must conform to the following requirements.

Note

These requirements do not apply to the Linux passwords.

- ◆ Be a minimum of eight characters and a maximum of 40 characters in length
- ◆ 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 !
- ◆ May not contain the single quote character (') because it is a delimiter for the password string

Expanding disk space

Add a virtual machine disk to a running system for use by suite virtual machines.

Procedure

1. From the vSphere Console, add a new disk to a virtual machine.
2. Select **Edit Settings** on the virtual machine.
3. Click **Add**.
4. Select **Hard Disk**, then click **Next**.
5. Select **Create a new virtual disk**, then click **Next**.
6. Specify the disk size, the provisioning type, and the location of the disk, then click **Next**.
7. Specify the virtual device node (the default value should be OK), then click **Next**.
8. Review the options, and then click **Finish**.
9. Access a Linux login prompt. You can access a login prompt through the vSphere Console or using an SSH tool such as PuTTY.
10. Log in to Linux.
11. At the system prompt, type the command `expand_disk.pl`.

Virtual Machine components

Each host type includes specific components and modules that serve distinct logical purposes in the core software architecture.

This section provides a list of key installed components for each host or installation type.

Table 1 Installed components

Host type	Installed components
Frontend host	• APG-Diagnostic-Tools • APG-Frontend • APG-Property-Store • APG-Web-Service • Administration-Tool • Alerting-Frontend • Centralized-Management • Compliance-Frontend • Device-Discovery • Formulas • Frontend-Search • Frontend-Report-Generator • JDBC-Drivers • License-Manager • Maps-Service • MIB-Browser • Module-Manager • SolutionPack modules • Sun-JRE • Task-Scheduler • Tomcat • WebApps-Resources • Webservice-Gateway
Primary Backend host	• Administration-Tool • Alert-Consolidation • Alerting-Backend • APG-Diagnostic-Tools • APG-Backend • Collector-Manager • Event-Key-Modifier • Event-Log-Processor • Event-Processing-Manager • Event-Property-Tagger • FailOver-Filter • Generic-Event-Listener • Generic-Event-Writer

Table 1 Installed components (continued)

Host type	Installed components
	• Generic-Live-Writer • Generic-Topology • JDBC-Drivers • Load-Balancer • Load-Balancer-Arbiter • MySQL • Trap-Receiver • Sun-JRE • License-Manager • Module-Manager • MySQL-Maintenance-Tool • Task-Scheduler • Topology • Topology-Service • Webservice-Gateway
Additional Backend host	• APG-Backend(s) • JDBC-Drivers • MySQL • Sun-JRE • License-Manager • Module-Manager • MySQL-Maintenance-Tool • Webservice-Gateway
Collector host	• APG-Diagnostic-Tools • Device-Discovery • Generic-RSC • Generic-SNMP • JDBC-Drivers • License-Manager • Module-Manager • Sun-JRE • Tomcat • Topology-Mapping-Service • WebApps-Resources • Webservice-Gateway

Table 1 Installed components (continued)

Host type	Installed components
Minimal installation (all host types)	• Sun-JRE • License-Manager • Module-Manager • Webservice-Gateway

CHAPTER 3

Standard Installation

This chapter includes the following topics:

♦ Standard installation options	22
♦ Installing core software on UNIX	22
♦ Installing core software on Windows Server	23
♦ Virtual Machine components	24

Standard installation options

You have several available options when performing a standard, or binary, installation of the core software.

There are three types of hosts that make up the core software infrastructure:

- ◆ 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 your configuration. Additional Backend hosts do not include the main database and exclude a subset of modules.

The components that collectively differentiate the host types are called modules. The core software installation binary supports the following installation options.

Default (UNIX) or Recommended Modules (Windows) installation

Use this option to install all modules available in the core software binary installation package. You can use this option on a single host, enabling it to serve as a Frontend, Backend, and Collector host. You can further customize this host by manually adding or removing specific modules.

Host-specific installations

For a host which requires a specific set of modules to perform its intended function (Frontend, Backend or Collector host), you can use the same core software binary installation and select the specific installation type.

Minimal (UNIX) or Base Installation (Windows)

Use this option to install the minimal modules required for any host type. You can further customize this host by manually adding specific modules.

Installing core software on UNIX

You can install the core software on supported UNIX hosts. This procedure specifically uses the Linux installation procedure as an example.

Before you begin

- ◆ When installing core software on a UNIX server, you must assign executable permissions to the installation script.
- ◆ Make sure 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 the location where the core software is located.
3. Change the permissions of the installer so you can run it.

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

```
chmod +x productname-setup-linux-x86_64-v63.sh
```

- Run the installer from the directory.

For example:

```
./productname-setup-linux-x86_64-v63.sh
```

- Read and accept the End User License Agreement. Use the **space bar** to scroll through the agreement. Press **y** to accept it.
- Press **Enter** to accept the default installation directory of `/opt/APG`. Or, enter another location and press **y**.
- Press **Enter** to accept the default user account name of **apg** or enter another name.
- Press **Enter** to accept the default location of service scripts of `/etc/init.d` or enter another location.
- Press **Enter** to accept the default base directory of `/etc` for runlevels scripts or type another location.
- Depending on the host purpose, select one of the following:

Option	Description
Default	Installs all recommended modules available in the binary installation package. You can use this option on a single host, enabling it to serve as a Frontend, Backend and Collector host. You can further customize this host by manually adding or removing 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. You can further customize this host by manually adding specific modules.

Installing core software on Windows Server

You can install the core software on supported Windows Server hosts.

Before you begin

- Make sure 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

- Locate the installation package.
- Double-click the setup file. For example: `productname-setup-win64-v63.exe`
- Click **Next** in the **Welcome** screen.
- Read and accept the End User License Agreement. Click **I Agree**.
- Select the Destination Folder:
 - Change the drive to a Windows non-root drive.
 - Maintain the default folder structure (`Program Files\APG`).
 - Click **Next**.
- Depending on the host purpose, select one of the following:

Option	Description
Recommended Modules	Installs all recommended modules available in the binary installation package. You can use this option on a single host, enabling it to serve as a Frontend, Backend and Collector host. You can further customize this host by manually adding or removing 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. You can further customize this host by manually adding specific modules.

7. Click **Install**.
8. On completion, click **Next**.
9. Click **Finish** to close the installer.

Virtual Machine components

Each host type includes specific components and modules that serve distinct logical purposes in the core software architecture.

This section provides a list of key installed components for each host or installation type.

Table 2 Installed components

Host type	Installed components
Frontend host	• APG-Diagnostic-Tools • APG-Frontend • APG-Property-Store • APG-Web-Service • Administration-Tool • Alerting-Frontend • Centralized-Management • Compliance-Frontend • Device-Discovery • Formulas • Frontend-Search • Frontend-Report-Generator • JDBC-Drivers • License-Manager • Maps-Service • MIB-Browser

Table 2 Installed components (continued)

Host type	Installed components
	• Module-Manager • SolutionPack modules • Sun-JRE • Task-Scheduler • Tomcat • WebApps-Resources • Webservice-Gateway
Primary Backend host	• Administration-Tool • Alert-Consolidation • Alerting-Backend • APG-Diagnostic-Tools • APG-Backend • Collector-Manager • Event-Key-Modifier • Event-Log-Processor • Event-Processing-Manager • Event-Property-Tagger • FailOver-Filter • Generic-Event-Listener • Generic-Event-Writer • Generic-Live-Writer • Generic-Topology • JDBC-Drivers • Load-Balancer • Load-Balancer-Arbiter • MySQL • Trap-Receiver • Sun-JRE • License-Manager • Module-Manager • MySQL-Maintenance-Tool • Task-Scheduler • Topology • Topology-Service • Webservice-Gateway

Table 2 Installed components (continued)

Host type	Installed components
Additional Backend host	• APG-Backend(s) • JDBC-Drivers • MySQL • Sun-JRE • License-Manager • Module-Manager • MySQL-Maintenance-Tool • Webservice-Gateway
Collector host	• APG-Diagnostic-Tools • Device-Discovery • Generic-RSC • Generic-SNMP • JDBC-Drivers • License-Manager • Module-Manager • Sun-JRE • Tomcat • Topology-Mapping-Service • WebApps-Resources • Webservice-Gateway
Minimal installation (all host types)	• Sun-JRE • License-Manager • Module-Manager • Webservice-Gateway

CHAPTER 4

Configuration

This chapter includes the following topics:

◆ Starting the core software services from the command line	28
◆ Starting the core software services on Windows	28
◆ Verifying if the core software services are running	29
◆ Logging in to the User Interface	30
◆ Connecting to Centralized Management	30
◆ Confirming settings for the first time	31
◆ Installing core suite licensing	31
◆ Configuring the user process limits for the Linux installation	32

Starting the core software services from the command line

After installing core software, you must start all required services.

Before you begin

- ◆ Before starting core software services, ensure the library search path is correct on the server hosting core software. This requirement applies to the libaio package on Linux.
- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the core software application uses instead of root.

Procedure

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

Operating system	Command
UNIX	<code>./manage-modules.sh service start all</code>
Windows	<code>manage-modules.cmd service start all</code>

Results

A list of services appears. For 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 core software services on Windows

After installing core software 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.

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 core software services are running

Verify the core software services are running by obtaining the status.

Before you begin

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

Procedure

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

Operating system	Command
UNIX	<code>./manage-modules.sh service status all</code>
Windows	<code>manage-modules.cmd service status all</code>

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

Results

```
* 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

Make sure you have logged in with root or APG privileges to check the log files.

Procedure

- ◆ Check these logs in the `/opt/APG/` directory to troubleshoot start-up problems:

```
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

Make sure you have logged in with system administrator credentials to check the log files.

Procedure

- ◆ Check these logs in the C:\Program Files\APG directory to troubleshoot start-up problems:

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

Logging in to the User Interface

Log in to continue to view reports or to test user access by specifying operator credentials.

Procedure

1. Point your browser to the URL.

For example, `http://<Frontend-hostname>:58080/APG`

2. Log in.

- a. Type the login credentials.

The default username is **admin** and the default password is **changeme**.

- b. Click **Sign In**.

After you finish

Note

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 core software.

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 core software is running.

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

For 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.

Confirming settings for the first time

After you first log in with administrator credentials for core software, you must confirm the configuration settings for the server.

Procedure

- ◆ Click **Save** to accept the predefined values for the server.
- Fields that are blank must remain blank.

Installing core suite licensing

When you install a suite, add a license for the suite. Licenses for specific SolutionPacks are contained in the suite license. We recommend that you immediately install a permanent suite license. After 30 days the initial bootstrap license expires.

There are two type of licenses:

- ◆ Permanent--Permanent licenses do not expire.
- ◆ Temporary--Temporary licenses have expiration dates. When temporary licenses expire, the module license checks fail and the modules stop working. If the frontend module fails, you cannot access the product.

Adding licenses

You must upload a license file whenever you install a new SolutionPack or ReportPack. The license enables views and reports to display.

Before you begin

- ◆ Obtain the required license file by creating a Service Request on EMC Online Support.

Procedure

1. Log in to the host with administrator credentials.
For example, `http://Frontend-hostname:58080/APG`
2. Click **Administration**.
3. In the **Centralized Management** pane, select **Licenses**.
4. In the Physical Overview tree, select **Licenses Management**.
5. In the **Licenses Listing** pane, click **Upload**.
6. In the **License Upload** dialog box, browse to your license file. Click **OK**.

Licenses in a .zip file are extracted and appear in the **Licenses Listing** pane.

7. When **License Upload Complete** appears, click **OK**, then click **Continue**.
8. If you have remote servers in a distributed environment, click **Synchronize** to add the licenses to the remote servers.

Deleting licenses from core software

You can select and delete specific licenses or delete all existing licenses from the core software server.

Procedure

1. Log in to with administrator credentials.
For example, `http://Frontend-hostname:58080/APG`
2. Click **Administration**.
3. In the **Centralized Management** pane, select **Licenses**.
4. In the Physical Overview tree, select **Licenses Management**.
5. In the **Licenses Listing** pane, select one or more license checkboxes.
6. Click **Delete**.
7. If you have remote servers in a distributed environment, click **Synchronize** to remove the licenses from the remote servers.

Verifying core software licenses from Centralized Management

Verify whether core software licenses are valid or expired for all servers in your environment from Centralized Management. The local and remote servers listed in this view are registered with Centralized Management.

Procedure

1. Log in with administrator credentials.
For example, `http://Frontend-hostname:58080/centralized-management`
2. Select **Licenses Management**.
3. In the **Licenses Listing** pane, read the **Expiration** column.

The *EMC Watch4net Centralized Management Guide* provides information about using Centralized Management and server registration.

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 core software 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'
```


CHAPTER 5

Infrastructure Preparation for Discovery and Data Collection

This chapter includes the following topics:

- ◆ [Host preparation for discovery and data collection](#) 36
- ◆ [Switch configuration for discovery and data collection](#) 47
- ◆ [Storage system preparation for discovery and data collection](#) 51

Host preparation for discovery and data collection

You need to configure hosts to support resource discovery and data collection.

- ◆ [Windows Host configuration for discovery and data collection on page 36](#)
- ◆ [UNIX and Linux host configuration for discovery and data collection on page 42](#)
- ◆ [Configuring ESX hosts to collect PowerPath metrics on page 44](#)
- ◆ [Installing host agent software on Windows hosts](#)

Windows Host configuration for discovery and data collection

In order to discover windows hosts and collect data from these hosts you have to configure various parameters.

- ◆ [Considerations for hostname and IP address on page 36](#)
- ◆ [Considerations for SNIA libraries and HBA drivers on page 36](#)
- ◆ [Configure WinRM for Windows host discovery on page 39](#)
- ◆ [Create a WinRM HTTPS listener on page 37](#)

Considerations for hostname and IP address

You have to follow these guidelines to ensure a successful host discovery and data collection.

- ◆ The host names are in Domain Name Server (DNS) format with fully qualified domain name (FQDN).
- ◆ IP addresses are registered with the appropriate domain name servers and resolve for a reverse DNS lookup.
- ◆ Hostname labels can contain only the lowercase ASCII letters a through z, the digits 0 through 9, and the hyphen (-). No other symbols, punctuation characters, or white spaces are permitted.

Note

If SRM Suite encounters a host name with an underscore, users may be prevented from logging in.

Considerations for SNIA libraries and HBA drivers

In order to discover SNIA-qualified HBA-related information for all the host platforms you should ensure the right versions of SNIA library, drivers and firmware are in place.

- ◆ Ensure you have EMC-supported host bus adapter (HBA) drivers and firmware. *EMC Storage Resource Management Suite Support Matrix* provides information for the supported SNIA compliant version of the HBA driver.
- ◆ The vendor-specific SNIA libraries must be installed on the target host.
- ◆ The HBA model number and part number should be verified before updating the hosts with SNIA libraries for HBA.
- ◆ You can install the SNIA library as part of HBA driver installation package or install the latest version of HBAnywhere (for Emulex installations) or SAN Surfer (for Qlogic installation).

To discover an HP-UX host with a multi-port Fibre Channel card, the package CommonIO bundle 0812(Dec 2008) or later should be present on the host to obtain the updated FC-SNIA file set.

Creating a WinRM HTTPS listener

You have to create a WinRM HTTPS listener to enable a handshake between the server and client for a successful discovery and data collection of Windows hosts. WinRM HTTPS requires a local computer server authentication certificate with a CN matching the host name, that is not expired, revoked, or self-signed to be installed.

You need to perform these steps only if you need a HTTPS listener, else, you can directly configure WinRM for HTTP.

Procedure

1. [Generate a .pfx certificate on page 37](#)
2. [Exporting the .pfx certificate on page 37](#)
3. [Importing the .pfx certificate on page 38](#)
4. [Generate a .cer file on page 38](#)
5. [Import the .cer file on page 38](#)

Generating a .pfx certificate

You can generate the required certificate using any certificate generator. This procedure demonstrates generating a certificate using Makecert.

Procedure

1. From the command prompt, run the command `C:\>makecert.exe -ss MY -sr LocalMachine -n "CN=<hostname>" -sky exchange -pe -a sha1 -eku.`
2. On a Windows host, click **Start > Run**.
3. Type `mmc` and click **OK**.

The Console window appears.

4. Click **File > Add/Remove Snap-in**.
5. Select **Certificates** under **Available snap-ins** and click **Add**.
6. Select **Computer account**.
7. Click **Finish**.
8. Click **OK** in the **Add or Remove snap-ins** window.

This creates a certificate under the personal store.

Exporting the .pfx certificate

You have to export the .pfx certificate created by Makecert in order to import it on to other hosts, if required.

Procedure

1. On a Windows host, click **Start > Run**.
2. Type `mmc` and click **OK**.
3. In the Console window, click **Certificates (local Computer) > Personal > Certificates**.
4. Double-click **Certificates**.
5. Under **Details**, click **Copy to File**.

6. In the **Certificate Export Wizard** select **Yes, export the private key.** and click **Next.**
7. Select **Include all certificates in the certification path if possible** and click **Next.**
8. Type a password for the private key.
This password is used when you import this certificate on other hosts.
9. Type a filename and save the `.pfx` file.

Importing the .pfx certificate

You have to import the `.pfx` if you want to use the same certificate on multiple hosts.

Before you begin

The `.pfx` certificate must be copied on the host where it is to be imported.

Procedure

1. On a Windows host, click **Start > Run.**
2. Type `mmc` and click **OK.**
3. In the Console window, click **Certificates (Local Computer) > Personal > Certificates**
4. Right-click and select **All Tasks > Import.**
5. In the browse window, select the `.pfx` certificate and click **OK.**

Generating a .cer file

The `.cer` file is created from a `.pfx` certificate with only a public key, which is used along with the private key for a successful handshake between the client and server.

Procedure

1. Go to **Start > Run > mmc > Certificates (Local Computer) > Personal > Certificates**
2. Double-click **Certificates.**
3. Under **Details**, click **Copy to File.**
4. Select **No, do not export the private keys.**
5. Selecting the **Encoding type** and click **Next.**
6. Type a file name and click **Save.**

Importing a .cer file

You have to import the `.cer` file on the collector host to enable a successful handshake between the server and the client.

Procedure

1. Copy the `.cer` file on the collector host.
2. Log in to the collector.
3. Run the command `/opt/APG/Java/Sun-JRE/6.0u45/bin/keytool -import -file <Public_Certificate_File> -keystore /opt/APG/Java/Sun-JRE/6.0u45/lib/security/cacerts -alias <Name>`

A sample output returned by the command:

```
Owner: CN=linbgm071
Issuer: CN=Root Agency
Serial number: 522200243f029a894c741bcb83d58a5d
Valid from: Tue Dec 10 11:59:03 EST 2013 until: Sat Dec 31
18:59:59 EST 2039
Certificate fingerprints:
MD5: 99:2A:6E:DC:CD:D7:7E:7D:07:C3:E2:8A:8F:E1:BB:DD
```

```

SHA1:
17:29:F4:45:99:AE:DC:C5:08:C6:73:D4:CF:A6:BE:7E:79:48:50:76
Signature algorithm name: SHA1withRSA
Version: 3
Extensions:
#1: ObjectId: 2.5.29.1 Criticality=false
#2: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
serverAuth
]
Trust this certificate? [no]: yes

```

Configuring WinRM for Windows host discovery

In order to discover remote Windows hosts and collect performance data, you have to configure Windows Remote Management (WinRM) service that is used by the remote shell collector.

Before you begin

Ensure the server authentication certificate is placed in the location `Console Root/Certificates/Personal`

This procedure requires that you obtain the `SRMSuiteHostConfig-3.0.0.ps1` script to support the WinRM configuration. Contact EMC Customer Support to obtain the required script.

Procedure

1. Run the Host-configuration powershell script on the target host to set the prerequisite: `C:\Users\administrator.PLUGIN\Desktop> .`

```
\SRMSuiteHostConfig-3.0.0.ps1 -verify -authType Basic
```

This verifies the existing settings on Host - script and prints status message for various configurations

An example snippet on how the script is used:

```

#####
linbgb109.plugin.SRM1.com : STATUS-OK :WinRM service already
started
linbgb109.plugin.SRM1.com : STATUS-ERROR :No Listener present for
WSMAN on the h
ost. Please create a listener using the command - winrm create
winrm/config/list
ener?Address=*&Transport=HTTP
linbgb109.plugin.SRM1.com : STATUS-OK : A firewall exception rule
with Name: Windows Remote Management(Http-In), Program: System,
LocalPort:5985 present already and is enabled.
linbgb109.plugin.SRM1.com : STATUS-ERROR : Basic Authentication
mode is set to false. Please run the script with "-set " option OR
set it to true using the command - winrm set winrm/config/Service/
Auth @{Basic ="true"}
linbgb109.plugin.SRM1.com : STATUS-OK : AllowUnencrypted is set to
true already.
-----
linbgb109.plugin.SRM1.com : Not ready for successful WSMAN
discovery from SRM Suite.
Please verify the settings.
-----
#####

```

2. To enable or set any incorrect settings, run script with "-set " option: `c:\Users\administrator.PLUGIN\Desktop> .\SRMSuiteHostConfig-3.0.0.ps1 -set -authType Basic`

An example snippet on how the script is used prompting for user inputs for various settings:

```
linbgb109.plugin.SRM1.com : STATUS-OK :WinRM service already
started
Are you sure that you want to create a listener for accepting
WSMAN requests on
this host?(yes/no): yes
Creating Listener for WSMAN
Listener for WSMAN created successfully
linbgb109.plugin.SRM1.com : STATUS-OK : A firewall exception rule
with Name: Windows Remote Management(Http-In), Program: System,
LocalPort:5985 present already and is enabled.
Are you sure that you want to set Basic authentication mode to
true on this host? (yes/no): yes
Setting Basic Authentication mode on the host...
linbgb109.plugin.SRM1.com : STATUS-OK : Basic Authentication mode
is set to true successfully.
linbgb109.plugin.SRM1.com : STATUS-OK : AllowUnencrypted is
already set to true on the host
#####
#####
```

3. To verify the new settings, run the script with "-verify " option: **C:\Users**

```
\administrator.PLUGIN\Desktop> .\SRMSuiteHostConfig-3.0.0.ps1 -
verify -authType Basic
```

An example snippet verifying the WSMAN configuration settings on the host.

```
#####
linbgb109.plugin.SRM1.com : STATUS-OK :WinRM service already
started
linbgb109.plugin.SRM1.com : STATUS-OK : Listener for accepting
WSMAN requests is present already.
linbgb109.plugin.SRM1.com : STATUS-OK : A firewall exception rule
with Name: Windows Remote Management(Http-In), Program: System,
LocalPort:5985 present already and is enabled.
linbgb109.plugin.SRM1.com : STATUS-OK : Basic Authentication mode
is set to true already.
linbgb109.plugin.SRM1.com : STATUS-OK : AllowUnencrypted is set to
true already.
-----
linbgb109.plugin.SRM1.com : WSMAN Prerequisite check completed for
successful discovery...
-----
#####
```

4. Provide the Thumbprint and CN (certificate host name) details in the server authentication certificate when you run the script: **C:\Users**

```
\administrator.PLUGIN\Desktop> .\SRMSuiteHostConfig-3.0.0.ps1 -set
-authType Basic -ssl -thumbprint
aaa0ffd0ceac6165e33f480bc98a56573cade9e9
```

An example snippet on how the script is used.

```
#####
#####

linbgb109.plugin.SRM1.com : STATUS-OK :WinRM service already
started
linbgb109.plugin.SRM1.com : STATUS-OK :Certificate with
Thumbprint: aaa0ffd0ceac6165e33f480bc98a56573cade9e9
and Hostname: linbgb109.plugin.srm1.com has been configured to
listen on port 5986
linbgb109.plugin.SRM1.com : STATUS-OK : A firewall exception rule
with Name: Windows Remote Management(Http-In), Program: System,
LocalPort:5986 present already and is enabled.
linbgb109.plugin.SRM1.com : STATUS-OK : Basic Auth mode is already
set to true on the host
```

```
linbgbl09.plugin.SRM1.com : STATUS-OK : AllowUnencrypted is
already set to true on the host
#####
#####
```

Configuring group policy

Use a group policy if you do not want to manually set the configuration on each and every host (either manually or using a script). The group policy lets you apply a set of configurations across a set of hosts. You have to configure the group policy so that it can be applied across hosts as required.

Procedure

1. Right-click **Computer** and select **Manage**.
2. Go to **Features > Group Policy Management > Forest Domain name > Domains > Domain Name > Default Domain Policy**.
3. Right-click **Default Domain Policy** and select **Edit**.

The group policy editor appears.

4. Select **Default Domain Policy > Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management**.
5. Modify the following parameters as required:
 - Allow automatic configuration of listeners
 - Allow basic authentication
 - Allow CredSSP authentication
 - Allow encrypted traffic
 - Disallow Kerberos authentication
 - Disallow Negotiate authentication
 - specify channel binding token hardening level
 - Turn on http compatibility listener
 - Turn on https compatibility listener

Configuring firewall port exception using group policy

You have to configure firewall port exception using group policy if you are not using default ports.

Procedure

1. Click **Computer**.
2. Go to **Computer Configurations > Policies > Windows Settings > Windows Firewall with Advanced Security > Inbound Rules**
3. Create a new inbound rule

This enables the WinRM communication.

Updating group policy

If you update the group policy on a domain controller, the changes are reflected on the computers that are part of the domain in approximately 90-120 minutes. Use this procedure to force update the group policy on the member computers.

Procedure

1. You can use any of the options for force update of group policy:

Option	Comment
Run the command <code>gpupdate /force</code> on all the member computers. This command results in a fetch operation for the group policy	This command has to be run on all the hosts and hence maybe cumbersome.
Change the Group Policy Refresh Interval in the Group Policy Management editor under Computer Configuration > Administrative Templates > System > Group Policy	Minimum possible time is 7 minutes. Reducing refresh interval is not recommended as it increases the load o the network.

UNIX and Linux host configuration for discovery and data collection

In order to discover Linux and UNIX hosts and collect data from these hosts you have to configure sudo as many discovery and data collection commands require root privileges. You have to generate a valid public and private key pair for the SSH key based authentication method of discovering UNIX hosts.

- ◆ [Configuring sudo for host discovery on page 42](#)
- ◆ [Generating a public and private key pair for SSH key based authentication on page 43](#)

Configuring sudo for host discovery

In order to discover Linux and UNIX hosts you must configure sudo to elevate the user privileges to root privileges for select commands.

Procedure

1. Include the path of sudo command in the environment variable \$PATH for the sudo user.
The variable \$PATH can be set either in `/etc/environment` or `/etc/default/login` or any other OS specific file.
2. Include the paths of OS commands in the environment variable \$PATH for sudo user.
3. Verify that the \$PATH is correct.
 - a. Log in as sudo user
 - b. Type **which sudo**.
4. Ensure that the sudoers file is available.
By default, the sudoers file is available in `/etc` or `/opt/sfw/etc/` or `/usr/local/etc/sudoers`.
5. Ensure that the sudo user has root privilege to run the following commands on a given host:

- `inq`
- `powermt`
- `sar`
- `mpstat`
- `vxdisk` (Solaris)
- `dmidecode` (Linux)
- `vgs` (Linux)
- `lvdisplay` (Linux)
- `vgdisplay` (HP-UX)
- `pvs` (Linux)

Generating a public and private key pair for SSH key based authentication

While using the SSH key based authentication to discover UNIX hosts, you can choose any key generation tool to generate a valid public and private key pair.

Before you begin

You must have a public key present on all the UNIX hosts that are to be discovered using the private key.

These steps describe the procedure to generate a public and private key pair for UNIX hosts using the `ssh-keygen` tool.

Procedure

1. For UNIX hosts that are not part of SRM Suite, generate a public and private key pair using the command `ssh-keygen -t rsa -f <location_of_the_private_key/name_of_private_key_file> -N ""`.

For example: `ssh-keygen -t rsa -f /root/.ssh/id_rsa -N ""`

2. Ensure that the public and private key pair that is generated has the following permissions:

- `chmod 600 /root/.ssh/id_rsa`
- `chmod 644 /root/.ssh/id_rsa.pub`

The private key file is `id_rsa`.

The public key file is `id_rsa.pub`.

3. To make the key pair functional, append the public key to `<users home directory>/ .ssh/authorized_keys` in the target UNIX host using the command `cat <location_of_the_private_key/name_of_private_key_file> >> <users home directory>/ .ssh/authorized_keys`

For example: `cat /root/.ssh/id_rsa.pub >> /root/.ssh/authorized_keys`

4. Place the generated private key in the RSC conf folder `/opt/APG/Collecting/Remote-Shell-Collector/<instance_of_collector>/conf`
5. Change the owner by running the command `chown apg:apg <private_key_file>`
6. Click **Administration**.
7. Under **Centralized Management**, click **SolutionPacks > Independent SolutionPackBlocks** and select the required instance.

The **SolutionPack Reconfiguration** dialog box appears.

8. Select the **Authentication type** as **Public key based**.
9. Type the location of the private key `/opt/APG/Collecting/Remote-Shell-Collector/<instance_of_collector>/conf/<name_of_private_key>`
10. Click **Reconfigure**.
11. Verify the changes in `host-definiton.xml` file located in the `<APG>/Collecting /Remote-Shell-Collector/<Instance_of_collector>/conf` directory.

Configuring ESX hosts to collect PowerPath metrics

Provides information about configuring ESX host to collect PowerPath metrics.

Before you begin

Ensure that PowerPath/VE remote CLI (rpowermt) is installed on the host and enable performance collection by running the `rpowermt set perfmon={on [interval=<#seconds>] | off} host=HOST_FQDN` command.

The *EMC Storage Resource Management Suite Support Matrix* provides more information on supported PowerPath versions.

To collect PowerPath metrics, do the following:

Procedure

1. Create lockbox.
2. Update host username and password in the lockbox.

Note

The PowerPath/VE for VMware vSphere Installation and Administration Guide provides detailed description of performing the above steps.

Configuring hosts to collect PowerPath metrics

Provides information about configuring host to collect PowerPath metrics.

To collect PowerPath metrics, do the following:

Procedure

1. Install PowerPath CLI (powermt) on the host.
2. Enable performance collection by running the `powermt set perfmon={on [interval=<#seconds>] | off}` command.

Note

The *EMC Storage Resource Management Suite Support Matrix* provides more information on supported PowerPath versions.

Installing EMC Host Interface on Windows Server

The EMC Host Interface is host agent software which enables Storage Resource Management Suite to collect data from supported hosts without requiring host credentials.

The EMC Host Interface software is installed as a Windows service on supported Windows hosts to enable data collection between the host and SRM Suite.

The installer automatically installs a prerequisite (Microsoft Visual C++ 2005 Service Pack 1 Redistributable) before installing the EMC Host Interface software.

You can choose local or LDAP authentication when installing EMC Host Interface. For both local and LDAP authentication, local database files are protected and encrypted using the RSA Common Security Toolkit.

Local authentication

The local authentication option installs a database on the local host which maintains authentication with a username and password.

LDAP authentication

The LDAP authentication option configures authentication using an LDAP server providing centralized control of authentication credentials.

Installing EMC Host Interface with local authentication

Install the EMC Host Interface from the command line using the LOCAL authentication option.

Before you begin

Consult the *EMC Storage Resource Management Suite Support Matrix* for information on supported Windows host operating systems on which you can install EMC Host Interface software.

This procedure describes the commands and parameters used to install the EMC Host Interface on a single server. You can also run the installer using remote push technology that supports MSI/EXE and use the parameters and push technology options to control the installation.

Procedure

1. Download the EMC Host Interface executable (`emc_host_interface-version-platform`) to a temporary location on the local host.
2. Open a command prompt and navigate to the temporary location.
3. Construct the executable syntax from the command line using the following security parameters.

Option	Description
SECURITY	LOCAL - database maintained on local machine
USER	Username for authentication. Default: admin
LBPASS	Password to be given to LOCAL user, min length 8, max length 40, alpha number mix required, mixed case required. Default: #1Password

4. Do one of the following:
 - Establish local authentication using the default credentials (admin/#1Password) as shown in the following example: `C:/temp/Emc-host-interface.exe`
 - Specify local authentication and provide your own credentials as shown in the following example: `C:/temp/Emc-host-interface.exe SECURITY=LOCAL USER=myaccount LBPASS=$4Secret`

Results

You can use these credentials when accessing the host using the SolutionPack for Physical Hosts.

After you finish

Verify installation by accessing the log file in: `install_dir\log\installation.log`

Troubleshoot runtime issues by accessing the log file in: `install_dir\log\cimomlog.txt`

Installing EMC Host Interface with LDAP authentication

Install the EMC Host Interface and configure LDAP authentication using the command line.

Before you begin

Consult the *EMC Storage Resource Management Suite Support Matrix* for information on supported Windows host operating systems on which you can install EMC Host Interface software.

This procedure describes the commands and parameters used to install the EMC Host Interface on a single server. You can also run the installer using remote push technology that supports MSI/EXE and use the parameters and push technology options to control the installation.

Procedure

1. Download the EMC Host Interface executable (`emc_host_interface-version-platform`) to a temporary location on the local host.
2. Open a command prompt and navigate to the temporary location.
3. Construct the executable syntax from the command line using the following security parameters.

Option	Description
SECURITY	LDAP - Use provided LDAP Authority
USER	Represents LDAP user to be given access rights.
LBPASS	Password to be given to secure lockbox store holding LDAP configuration information, min length 8, max length 40, alpha number mix required, mixed case required. Default: #1Password
PORT	Port number of the LDAP service. Default: 389
SERVER	Hostname or IP Address of the LDAP server to use for authentication. There is no default value.
DOMAIN	Distinguished Name (DN) of the privileged account used to perform operations, such as searching users and groups, on the LDAP directory. There is no default value.
BINDPASS	Password of the privileged account for accessing LDAP server. There is no default value.
USERSEARCH	DN of the node at which to begin user searches.
GROUPSEARCH	DN of the node at which to begin group searches. There is no default value.
CONFIGNAME	Name of this LDAP configuration/authority, when logging with agent pack use <code>CONFIGNAME/USER</code> . There is no default value.

4. Establish LDAP authentication as shown in the following example:

```
Emc-host-interface.exe SECURITY=LDAP USER=myldapuser LBPASS=
$4Secret PORT=389 SERVER=ldap.company.com DOMAIN="uid=admin,
ou=Administrators,ou=TopologyManagement,o=netscaperoot"
BINDPASS=Password USERSEARCH="ou=People,dc=emc,dc=localdomain"
GROUPSEARCH="ou=Groups,dc=emc,dc=localdomain"
CONFIGNAME="company.localdomain"
```

Results

You can use these credentials when accessing the host using the SolutionPack for Physical Hosts. For example, use credentials:

Username: *company.localdomain\myldapuser*

Password: *ldap_user_password*

After you finish

Verify installation by accessing the log file in: *install_dir\log\installation.log*

Troubleshoot runtime issues by accessing the log file in: *install_dir\log\cimomlog.txt*

Switch configuration for discovery and data collection

You need to configure switches to support switch discovery, data collection, and alert consolidation.

- ◆ [Brocade switch configuration on page 47](#)
- ◆ [Cisco switch configuration on page 48](#)

Brocade switch configuration

You need to configure Brocade switches and the SMI agents to support switch discovery, data collection and alert consolidation.

- ◆ [Configuring Brocade SMI Agents on page 47](#)
- ◆ [Configuring Brocade switches for alert consolidation on page 48](#)

Configuring Brocade SMI Agents

You have to install and configure the Brocade SMI Agent in order to enable zoning discovery.

Procedure

1. Install CMCNE with one of the following options an option of either an integrated Brocade SMI Agent (SAN with Brocade SMI Agent) or just the Brocade SMI Agent only (headless installation).

Option	Description
integrated Brocade SMI Agent (SAN with Brocade SMI Agent)	The Brocade SMI agent is integrated with CMCNE, BNA, CMDCE, DCFM and gets installed when you install any of these products.
Brocade SMI Agent only (headless installation)	You can use this option if you do not want to install CMCNE, BNA, CMDCE, or DCFM.

The CMCNE or CMDCE and/or Brocade SMI Agent documentation provides details on installation and configuration instructions.

Configuring Brocade switches for alert consolidation

Use this procedure to configure forwarding of alert traps (SNMP v1) from Brocade switches to the suite.

Procedure

1. Log into the Brocade FC switch as the administrator.
2. Type `snmpConfig --set snmpv1`, and press **Enter**.
3. Type the following details, when prompted:

Option	Input
Community	[public]
Trap recipient's IP address	The SRM Suite trap recipient IP which, in a single vApp installation is the SRM Suite IP, and in a distributed environment, is the suite's Backend IP.
Trap recipient severity level	(0..5)
Trap recipient port	2041, which is the SRM Suite trap listening port.

4. If you have multiple Brocade FC switches in your storage environment, repeat this procedure on each switch.

Cisco switch configuration

You need to configure Cisco switches to support discovery, data collection, and alert consolidation.

SRM Suite supports two modes of SNMP communications for Cisco switches: the less secure SNMPv1/v2 mode and more secure SNMPv3 mode. You have to perform the following procedures as part of Cisco switch configuration:

- ◆ [Pre-configuration tasks on page 48](#)
- ◆ [Configure switches for SNMPv1 and SNMPv2 on page 49](#)
- ◆ [Configure switches for SNMPv3 on page 49](#)
- ◆ [Configure Cisco switches for alert consolidation on page 50](#)

Performing pre-configuration tasks

Before you discover a Cisco switch in SRM Suite you need to perform the following checks.

All switches in the Cisco fabric must have the same SNMP credentials for use with SRM Suite. For example, if the SNMPv1/v2 community setting private is used, all Cisco switches in the fabric should have the SNMPv1/v2 private community name set with a role of network-admin. For an SNMPv3 user, the same SNMPv3 credentials with the role of network-admin should be set on every switch in the fabric.

Procedure

1. Ensure all hardware, including the switch model, and software is listed as supported in the *EMC Storage Resource Management Suite Support Matrix*.

2. Verify the TCP/IP connectivity to the switches to be discovered. Test by issuing a `ping` command to these switches.
3. Determine if SNMP traps are enabled. Log in to the switch and run the command `show snmp trap`.
4. Run the command `snmp-server enable traps` to enable SNMP traps.

```
SWDevCisco8-9216i# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWDevCisco8-9216i (config)# snmp-server enable traps
```
5. Display the traps that are enabled. Execute the `show snmp trap` command. The values in the `Enabled` column should be `Yes`.

Configuring switches for SNMPv1 and SNMPv2

You have to configure Cisco switches for SNMPv1 or SNMPv2 to enable discovery, data collection, and alert consolidation for the switches. The SNMPv1 or SNMPv2 information you provide when performing discovery is necessary for SRM Suite to contact the switch to obtain information.

Before you begin

Ensure that the Cisco switches have an SNMPv1 community name that has read only privileges set on every switch in the fabric. The SNMP community selected must have a network-operator role.

SRM Suite collects data from the switch using the same SNMP community name. It uses the SNMP port for communication. The default port set is port 161.

Note

The Cisco documentation provides information on configuring Cisco switches for SNMPv1 and SNMPv2 management.

Procedure

1. Log into the switch as an administrator.
2. To configure the `snmp-server` community string with read-only privileges, run the following commands:

```
Cisco8-9216i# config terminal
Cisco8-9216i(config)# snmp-server community eccuser ro
```

You have to type configuration commands, one per line and end with **CNTL/Z**.

3. To verify if the SNMPv1 community string exists, run the command `show snmp community`.

A sample output of the command:

Community	Group/Access
eccuser	network-operator

Configuring switches for SNMPv3

You have to configure Cisco switches for SNMPv3 to enable discovery, data collection, and alert consolidation for the switches. The SNMPv3 information you provide when

performing discovery is necessary for SRM Suite to contact the switch to obtain information.

SRM Suite collects data from the switch using SNMPv3 secure credentials. SRM Suite uses the SNMP port for communication. SRM Suite supports SNMPv3 with all the combinations of Auth (MD5, SHA) and Priv (AES, DES, NONE).

Note

Create the same SNMPv3 users with the same authentication and privacy passwords on all physical switches in the fabric. The Cisco documentation provides information on creating SNMPv3 users on Cisco switches.

This procedure provides an example of creating an SNMPv3 user called ECCuser with a network-operator role, SHA authorization, and AES128 authentication.

Procedure

1. Log into the switch as an administrator.

```
Cisco8-9216i# config terminal
```

Enter configuration commands, one per line. End with **CNTL/Z**.

```
Cisco8-9216i (config)#snmp-server user ECCuser network-  
operator auth sha <SHA-password> priv aes-128 <AES-password>
```

2. Run the snmp-server user commands as follows:

```
config terminal
```

```
snmp-server user ECCuser network-operator auth sha <SHA-  
password> priv aes-128 <AES-password>
```

You have to type configuration commands, one per line and end with **CNTL/Z**.

3. To verify the new user creation run the command `show snmp user`.

A sample output of the command:

SNMP USERS			
User	Auth	Priv(enforce)	Groups
admin	md5	no	network-admin
ECCuser	sha	aes-128(no)	network-operator
NOTIFICATION TARGET USERS (configured for sending V3 Inform)			
User	Auth	Priv	
SWDevCisco8-9216i#			

Configuring Cisco switches for alert consolidation

Use this procedure to configure forwarding of alert traps (SNMP v1) from Cisco FC switches to the suite.

Procedure

1. Log into the Cisco FC switch as the administrator.
2. To enter the global configuration mode, at the terminal prompt, type # **config**, and press **Enter**.

Cisco documentation provides more information on the global configuration mode.

3. Type `snmp-server host <trap_recipient IP> traps <SNMP trap version> <Community String> udp-port <trap listening port >`, and press **Enter**.

In the command syntax:

Syntax element	Input
<i><trap_recipient IP></i>	In a single vApp installation is the SRM Suite IP, and in a distributed environment, is the suite's Backend host IP.
<i><SNMP trap version></i>	version 1
<i><Community String></i>	public
<i><trap listening port ></i>	2041 , which is the SRM Suite trap listening port.

Example: `snmp-server host 10.247.24.190 traps version 1 public udp-port 2041`

4. If you have multiple Cisco FC switches in your storage environment, repeat this procedure on each switch.

Storage system preparation for discovery and data collection

You need to prepare storage systems for discovery and data collection. In some cases, you may have to perform some additional configuration on the storage systems.

The following information enables you to prepare supported storage systems for discovery, data collection and alert consolidation.

Preparing EMC Centera

Identify the information required to support resource discovery and data collection before installing the SolutionPack for EMC Centera.

You enable discovery and data collection for EMC Centera by installing a supported version of Centera CLI software on the SRM Suite Collector host.

Procedure

1. Identify the SRM Suite Collector host on which you will install the EMC Centera Viewer CLI software.
2. Install a supported version of the EMC Centera Viewer CLI on the Collector host.
The EMC Centera Viewer CLI is currently supported on Microsoft Windows Server 2008 R2. For the specific version of Centera CLI software required and supported Collector host operating systems, refer to the *EMC Storage Resource Management Suite Support Matrix*.
3. Identify the username (monitor role) and password.
4. Record this information for use when you install the SolutionPack.

Results

During installation of the SolutionPack for EMC Centera, you will be asked to provide the location of the `CenteraViewer.jar` file.

Preparing Converged Infrastructure

Identify the information required to support resource discovery and data collection before installing the SolutionPack for Converged Infrastructure.

SRM Suite communicates with Unified Infrastructure Manager using credentials with access to the UIM host.

Procedure

1. Identify the user account credentials used to access the UIM host.
2. Record this information for use when you install the SolutionPack.

Preparing EMC Data Domain

Identify the information required to support resource discovery and data collection before installing the SolutionPack for EMC Data Domain.

The SRM Suite Collector host communicates with EMC Data Domain using SNMP. You must enable a supported version of SNMP on any Data Domain systems that you want Storage Resource Management Suite to poll. For details on the supported versions of SNMP used with Data Domain, refer to the *EMC Storage Resource Management Suite Support Matrix*.

Procedure

1. On the Data Domain system, use the following command to view the SNMP configuration:

```
# snmp show config
```

2. Use the following command to add the SRM Suite SNMP Collector host: `# snmp add ro-community public hosts collector_host`.

Preparing EMC Isilon

Identify the information required to support resource discovery and data collection before installing the SolutionPack for EMC Isilon.

SRM Suite uses SNMP to access EMC Isilon.

Procedure

1. Ensure that SNMP Read-Only is activated on the EMC Isilon array.

Preparing EMC VMAX

Identify the information required to support resource discovery and data collection before installing the SolutionPack for EMC VMAX and perform the necessary pre-configuration.

SRM Suite requires EMC Solutions Enabler to communicate with VMAX arrays. There are two supported scenarios.

Solutions Enabler proxy scenario (recommended)

In this scenario, you install Solutions Enabler on the SRM Suite Collector host designated to collect data from VMAX.

You configure Solutions Enabler to communicate over TCP/IP with a Solutions Enabler instance on the remote SYMAPI server (Array Provider).

You should add two additional gatekeepers to the host that is already monitoring the Symmetrix array.

Local Solutions Enabler scenario

In this scenario, you install the SRM Suite Collector software on an existing SYMAPI server (which already has Solutions Enabler installed). Collection processing is performed on the SYMAPI server and passed to the SRM Suite Collector host.

You must add two additional gatekeepers to the host, resulting in a total of eight gatekeepers.

Solutions Enabler proxy scenario

The Solutions Enabler proxy scenario supports resource discovery and data collection for EMC VMAX.

In this scenario, no SRM Suite software is installed on the SYMAPI server. Instead, a client host and server host proxy relationship is configured. This is the preferred configuration for monitoring VMAX arrays.

- ◆ Client host - You install Solutions Enabler on the SRM Suite Collector host designated to collect data from VMAX. The client host has no direct connectivity to the array.
- ◆ Server host - Solutions Enabler already exists on the SYMAPI server with connectivity and gatekeeper access to the array.

The client host is then configured for proxy communicate with the server host over TCP/IP (port 2707). In this scenario, map two additional gatekeeper devices to your SYMAPI server.

Configuring Solutions Enabler proxy support

Configure support for the Solutions Enabler proxy scenario.

Before you begin

- ◆ Install a supported version of EMC Solutions Enabler on the SRM Suite Collector host. Refer to the *EMC Storage Resource Management Suite Support Matrix* for supported versions used with SRM Suite.
- ◆ In a proxy configuration, you must maintain the same Solutions Enabler family version. A mixed 32-bit and 64-bit Solution Enabler is supported in a proxy configuration.
- ◆ Map two additional gatekeeper devices for SRM Suite and present them to your SYMAPI server.
- ◆ Ensure the `storsrvd` daemon is running on the Server host. You can confirm this by issuing the `stordemon list` command on the Server host.

This procedure is applicable for Solutions Enabler or the Solutions Enabler installed with the EMC SMI-S Provider.

Procedure

1. On the client host on which you installed Solutions Enabler, navigate to the `netcnfg` file.

On Linux, the file is located at: `/var/symapi/config/netcnfg`.

On Windows the file is located at: `.. \Program Files\EMC\SYMAPI\config`

2. Edit the file to add the remote host to which Solutions Enabler will communicate. Add a line similar to to the last line in the following example:

```
# This is a sample config -- where WWW.XXX.YYY.ZZZ is a valid IP
address.          #
# Please use this format for your
host.              #
#
```

```

#
# SYMAPI_SERVER - TCPIP node001 WWW.XXX.YYY.ZZZ 2707
- #
# SYMAPI_SECURE - TCPIP node001 WWW.XXX.YYY.ZZZ 2707
SECURE #

SYMAPI_SERVER - TCPIP hostname IP-address 2707 NONSECURE

```

Select **NONSECURE** when the server side is configured for **NONSECURE**, or **ANY** on the `deamons_options` file in the `SECURITY_LEVEL` section.

3. Set the following System environment variables on the client host:

- `SYMCLI_CONNECT=SYMAPI_SERVER`
- `SYMCLI_CONNECT_TYPE=REMOTE`

Option	Description
Windows	The environment variables are shown with the set command at the command prompt. To establish persistent variables use Computer > Properties > Advanced system settings . Select Environment Variables > New to create the two variables as shown above.
Linux	Use the env command to show the environment variables. To establish persistent variables use export to create the two variables as shown above.

4. On the SYMAPI server host, ensure that the `SERVER` license key is registered by reviewing the `symapi\config\symapi_licenses.dat` file. If it is not there, use the `symlmf` utility to add the license key.

You can also control the Solutions Enabler licenses from the array.

Verifying the Solutions Enabler proxy configuration

Verify proxy configuration success and , if necessary, identify and resolve any configuration issues.

Procedure

1. From the SYMAPI server host, type **sympd list** to display a list of devices that are visible to the host. Note the results.
2. On the client host, type **sympd list**.
 - If the results match, the configuration is complete.
 - If the command issued from the client returns a message such as `no devices found`, continue to the next step.
3. To isolate the issue:
 - a. Verify that the same command works on the host with the FC connection to the Symmetrix array.
 - b. Verify that the environment variables for Solutions Enabler are set using the **symcli -def** command.
 - c. Verify that the `netcfg` file has been edited using the `symcfg -services list` command.

- d. Verify the arrays you intend to monitor using the `symcfg list` command.
- e. Verify that six gatekeepers are provisioned from each Symmetrix array using the `sympd list` command.

Local Solutions Enabler scenario

The local Solutions Enabler scenario supports resource discovery and data collection for EMC VMAX.

In this scenario, you install only the SRM Suite Collector software directly on the existing SYMAPI Solutions Enabler server.

- ◆ The Solutions Enabler proxy scenario is the preferred configuration.
- ◆ Implementing this scenario includes the advantages of reduced network calls and a more secure configuration. However, the Collector software installed on the SYMAPI server will require processing cycles from that server.
- ◆ This scenario requires two additional gatekeeper devices be mapped to your Collector host.

Configuring VMAX arrays for consolidation of availability alerts

Use this procedure to configure forwarding of availability alert traps (SNMP v1) from VMAX arrays to the suite.

VMAX performance alerts are collected using the discovery data collection configuration.

Procedure

1. Log into Solutions Enabler on the array provider host as an administrator.
2. Navigate to the `daemon_options` file in the `C:\Program Files\EMC\SYMAPI\config\` directory.
3. In the parameter section `SNMP_TRAP_CLIENT_REGISTRATION`:
 - a. Uncomment the line `storevntd:SNMP_TRAP_CLIENT_REGISTRATION`
 - b. Add the SRM Suite trap recipient IP to the trap filter. The trap recipient IP is the Backend host IP.

The syntax is `<IP>,<port>,<filter>,<state>`, where `<filter>` is the filtering level for trap forwarding defined in the `FCMGMT-MIB` file.

Example: `10.31.90.148, 2041,10,ACTIVE`
4. In the parameter section `LOG_EVENT_TARGETS`, uncomment the line `storevntd:LOG_EVENT_TARGETS = snmp file.`
5. To identify the arrays from which traps should be forwarded to the suite, type `symcfg list`, and press **Enter**.
6. For each array that should forward alert traps to SRM Suite:
 - a. Type `symcfg list`, and press **Enter**.
 - b. In the parameter section `LOG_SYMMETRIX_EVENTS`, specify the appropriate event categories in the format:

`sid=<SYM serial number>, <event category 1>, <event category 2>\`

Example: `SID=000194900854, disk, device, device pool, director, srdf consistency group, srdafa session, srdf link, srdf system, service processor, environmental,`

```
diagnostic, checksum, status, events, array subsystem,
groups, optimizer, thresh_critical=3, thresh_major=2,
thresh_warning=1, thresh_info=0 ;\
```

7. To reload the changes to the `daemon_options` file, type **stordaeomon action storevntd -cmd reload**, and press **Enter**.
8. Ensure that the storevntd Event Daemon is running on the provider host.
9. If you have multiple VMAX array provider hosts in your storage environment, repeat this procedure on each array provider host.

Preparing EMC VNX

Identify the information required to support resource discovery and data collection before installing the SolutionPack for EMC VNX and perform the necessary pre-configuration.

SRM Suite uses Navisphere Secure CLI (NavisecCLI) installed on the suite Collector host to access the VNX arrays.

EMC recommends matching Naviseccli versions with Block Operating Environment versions of VNX systems configured in the Collector. For information on compatible Block OE and Naviseccli versions, refer to the *VNX OE for Block Release Notes* and the *Unisphere Host Agent/CLI and Utilities Release Notes* on EMC Online Support.

For block and unified data collection, you must enable statistics logging on the array. To enable statistics logging, refer to Unisphere documentation.

Configuring simple authentication

You can configure simple authentication with VNX arrays using the default SRM Suite account.

In order to poll and collect performance statistics from a VNX array, administrator privileges are required for the user account used to access the arrays.

Note

The preferred method for secure polling and collection of data from VNX arrays is to configure authentication using a Unisphere security file. Refer to [Unisphere security file authentication on page 56](#).

Procedure

1. Configure the default SRM Suite account (apg) with administrator privileges to access the VNX array as described in the Unisphere documentation.
2. Validate access to the VNX array by running the following block command:

```
naviseccli -h (host) -user username -password password -scope 0
getagent
```

Unisphere security file authentication

A Unisphere security file is the preferred method to provide secure polling and data collection from VNX arrays.

By default, the SRM Suite Collector runs using the local system account which is a special Windows user with no environment. The preferred secure method is to create a Unisphere security file, an encrypted file stored on the Collector host.

When you create a security file, the username you use to log in to the current host is automatically stored in the security file, or you can specify an alternative username for the security file in the `-AddUserSecurity` request using the optional `-user` switch. If

you omit the `-user` switch, the security file uses your current username. You can also target the security file at a specific storage system using the `-ip` option.

You can store the security file on the Collector host and edit parser XML files to include this path which will provide the required authentication to access the arrays.

Note the following:

- ◆ By default, the security file is stored in your default home directory. With NavisecCLI, you can specify an alternative file path using the optional `-secfilepath` switch.
- ◆ Once the security file exists, you can edit XML configuration files that are used to poll and collect data to use the path to the security file on the Collector host. The security file handles authentication.
- ◆ For details on configuring a security file on a host, refer to the Unisphere documentation.

Configuring security file authentication

Configure the Unisphere security file authentication on SRM Suite Collector hosts that will collect data from VNX arrays.

Utilize the security file to configure array access from the Collector host.

Procedure

1. On the SRM Suite Collector host designated for collecting VNX data, create the folder:

```
...\APG\Collecting\Text-Collector\context
```

2. Using NavisecCLI, store the security file into that directory as shown in the following example:

```
naviseccli -AddUserSecurity -User username -Password password -
Scope 1 -secfilepath D:\Program Files\APG\Collecting\Text-Collector
\context
```

3. Edit parser-*.xml configuration files to include this path when communicating with VNX arrays:

```
naviseccli -secfilepath D:\Program Files\APG\Collecting
\Text-Collector\context -h <IP> ...
```

Configuring VNX arrays for consolidation of file alerts

Configure forwarding of VNX file alerts to SRM Suite.

Note

Consolidation of VNX block alerts does not require separate configuration.

Procedure

1. Log into Control Station as the root user.
2. Open the `nas_mcd.cfg` configuration file in the `/nas/sys/` directory.
3. Enable the XML-API service by uncommenting the following entry:

```
daemon "XML API Server"
    executable      "/nas/sbin/start_xml_api_server"
    optional        yes
    canexit         yes
    autorestart     yes
    ioaccess        no
```

4. Type **# service nas start**, and press **Enter** to restart the XML-API service.
5. If you have multiple VNX arrays in your storage environment, repeat this procedure on each VNX array.

Preparing EMC VPLEX

Identify the information required to support resource discovery and data collection before installing the SolutionPack for EMC VPLEX and perform the necessary pre-configuration.

SRM Suite utilizes SSH to communicate to VPLEX arrays. In addition, you must enable perpetual monitors and configure the maximum amount of SSH sessions.

Procedure

1. Enable perpetual monitors on the VPLEX arrays.
 - a. Log in to the VPLEX management server using the user credentials for the service account.
 - b. From the vplexcli prompt, type: **report create-monitors**.
2. Configure the maximum number of SSH sessions to 20.
 - a. Log in to the VPLEX management server using the user credentials for the service account.
 - b. Type the following commands:


```
cd /etc/ssh
sudo cp sshd_config sshd_config.original
sudo vi sshd_config
```
 - c. At the end of the configuration file, add the following line to configure the `MaxSessions` setting:


```
MaxSessions 20
```
 - d. Type: **sudo /etc/init.d/sshd restart**

Preparing Hitachi Device Manager

Identify the information required to support resource discovery and data collection before installing the SolutionPack for Hitachi Device Manager.

SRM Suite communicates with the Hitachi Device Manager to poll information for HDS arrays.

Procedure

1. Identify account credentials with administrator privileges on the Hitachi Device Manager system.
2. Record the IP address/hostname for SSH and CIMOM communication.

Preparing HP 3PAR StoreServ

Identify the information required to support resource discovery and data collection before installing the SolutionPack for HP 3PAR StoreServ.

SRM Suite communicates with the HP 3PAR StoreServ array using an account with read-only privileges on the array.

Procedure

1. Identify an account with read-only privileges for the HP 3PAR StoreServ array.
2. Ensure that the array can be accessed on port 22 using SSH.
3. Record this information for use when you install the SolutionPack.

Preparing HP EVA

Identify the information required to support resource discovery and data collection before installing the SolutionPack for HP EVA.

SRM Suite communicates with the HP EVA Element Manager to poll information for HP EVA arrays.

Procedure

1. Identify account credentials with administrator privileges on the HP EVA Element Manager system.
2. Record the IP address/hostname for SSH and CIMOM communication.

Preparing IBM DS

Identify the information required to support resource discovery and data collection before installing the SolutionPack for IBM DS.

SRM Suite communicates with the IBM CIM/SMI-S provider that queries the storage array.

- ◆ For details on supported IBM DS models, refer to the *EMC Storage Resource Management Suite Support Matrix*.
- ◆ For details on installing and enabling provider support on IBM DS models, refer to the appropriate IBM documentation.

Procedure

1. Depending on your IBM DS model, do one of the following:
 - IBM DS 3K/4K/5K models - Manually install and configure the IBM CIM/SMI-S provider on a management server.
 - IBM DS 6K/8K models, the CIM/SMI-S provider is built into the Hardware Management Console (HMC).

Note

Ensure that the CIM agent is enabled, as it was disabled by default in earlier releases (e.g., prior to Release 4, Bundle 62.0.175.0).

2. Identify the CIM username and password used to access the array.
3. Record this information for use when you install the SolutionPack.

Preparing IBM XIV

Identify the information required to support resource discovery and data collection before installing the SolutionPack for IBM XIV.

SRM Suite communicates with IBM XIV using the CIM agent.

Procedure

1. Ensure CIM agent is installed.

Starting with IBM XIV Storage System V10.1.0, the CIM agent is pre-installed on the administrative module. The embedded CIM agent is automatically enabled and pre-configured.

2. Identify the access credentials.
3. Record this information for use when you install the SolutionPack.

Preparing NetApp Filer

Identify the information required to support resource discovery and data collection before installing the SolutionPack for NetApp Filer.

SRM Suite communicates with NetApp Filer arrays using the NetApp CLI over SSH.

Procedure

1. Identify the username, password and NetApp Filer Mode (the default is 7-Mode).
2. Record this information for use when you install the SolutionPack.

Preparing VI VirtualWisdom

Identify the information required to support resource discovery and data collection before installing the SolutionPack for VI VirtualWisdom and perform any necessary pre-configuration.

SRM Suite collects VirtualWisdom data using proxy software installed on the VirtualWisdom Portal Server. Download and install the proxy software on the VirtualWisdom Portal Server

Procedure

1. Obtain the proxy installation package using Virtual Instruments customer credentials from their SFDC portal, or from [ftp.virtualinstruments.com](ftp://ftp.virtualinstruments.com). The package is located in the CURRENT directory.
2. Copy the installation package to the VirtualWisdom server.
3. Unzip the package into a suitable temporary directory.
4. Stop the VirtualWisdom service.
5. Open a command prompt.

Note

You may need to run as Administrator to allow files to be copied.

6. Navigate to the temporary directory where the proxy is unzipped and run the `install.bat` script.
7. Enter the VirtualWisdom installation path.
8. Restart the VirtualWisdom service.

Results

You do not need to perform any additional configuration of the proxy which runs as part of the standard VirtualWisdom.

After you finish

Create a VirtualWisdom user account dedicated for access by the SolutionPack for VI VirtualWisdom. When you install the SolutionPack, you will provide these credentials

which are then stored on the Collector host in: `APG/Collecting/XML-Collector/vi-virtualwisdom/conf/VI-proxyRequest.xml`.

Connecting to multiple VirtualWisdom Portal Servers

If you have more than one VirtualWisdom Portal Server, you can combine data from multiple Portal Servers. The data will populate the same reports.

Before you begin

Install and configure the proxy software on each VirtualWisdom Portal Server.

Use this configuration to collect the same metrics from all Portal Servers using the same frequency (poll cycle) and credentials. Each host will be polled in the sequence you specify in the configuration file.

Procedure

1. On the Collector host, navigate to `APG/Collecting/XML-Collector/vi-virtualwisdom` and open the `VI-collector.xml` file.
2. Add one or more Portal Server hosts to the configuration file by typing the additional host IP addresses.

```
<input>http://(host):8080/Proxy</input>
```

```
    <host>ip_address</host>
```

```
    <host>ip_address</host>
```

```
    <parameter name="connect-type">
```

```
        <value>any</value>
```

```
    </parameter>
```

3. If the VirtualWisdom WebServices port numbers are different for each Portal Server host, you can remove the port number from the `<input>` line and append the unique port numbers to the host address. For example:

```
<input>http://(host)/Proxy</input>
```

```
    <host>ip_address:port</host>
```

```
    <host>ip_address:port</host>
```

```
    <parameter name="connect-type">
```

```
        <value>any</value>
```

```
    </parameter>
```

4. Restart the VirtualWisdom collector.

CHAPTER 6

SolutionPack Installation

This chapter includes the following topics:

◆	Connecting to Centralized Management	64
◆	Installing a SolutionPack	64
◆	Configuration during SolutionPack installation	65
◆	Post-installation configuration of SolutionPacks	82
◆	Post-installation configuration details	86

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 core software.

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 core software is running.

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

For 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.

Installing a SolutionPack

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

Before you begin

- ◆ Core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Core modules are modules that are not installed by a SolutionPack. Examples of core modules include webapps, module-manager, license-manager, java, mysql, backend, tools, and so forth. Update these core modules: **Databases, Backends, Frontends, Miscellaneous** (except Blocks). Since the recommended module update order varies, refer to the Module Update Order section for the multiple hosts or single host deployments. Also, the *EMC Watch4net Centralized Management Guide* provides more information.

Procedure

1. Log in and select **Administration**.
2. Select **Centralized Management** in the Administration tree.
3. Select **SolutionPacks** in the tree.
4. Select **SolutionPack Center**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.

6. Read the summary information and click **Install**.
7. 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, Reports, and Events** list boxes.
 - c. Click **Next**.
8. 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.
9. Select the maximize arrow next to each component to view the installation process.

When the installation successfully completes, green checkmarks appear.
10. After installation is complete, select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

After you finish

Install the SolutionPack for EMC Watch4net Health if you have not already done so. This is available from **Centralized Management** > **SolutionPack Center**.

Configuration during SolutionPack installation

This topic describes any required or suggested configuration for each Storage Resource Management Suite SolutionPack during installation.

Note

This information supplements the field-level assistance already provided in the SolutionPack installer user interface for the SolutionPacks included in Storage Resource Management Suite. As such, some fields which are self-explanatory or do not require additional configuration details are omitted.

Table 3 SolutionPack configuration details

SolutionPack	Configuration Details
SolutionPack for Brocade FC Switch	In the Select the components to install window: • In Alert Consolidation, select the Primary Backend host. • In Pre-configured alerts, select the Primary Backend host. • In SMI Data Collection, select the Collector host. • In Reports, select the Frontend host. • In SNMP Masks, select the Frontend host. In the Pre-configured alerts window: • In Alerting Web-Service Instance, select the Primary Backend host. • In Recipient for email alerts, provide an email address.

Table 3 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	• Select Enable the Brocade FC Switch Port Link Utilization Alert if desired. In the SMI Data Collection window: • Select Activate the APG Failover-Filter if desired. • In Hostname or IP address to send data, type the Primary Backend host. The default port is 2020. • In Topology Service hostname or IP address, type the Primary Backend host. • In Please select the Gateway, select the Primary Backend host and gateway port: <i>primary_backend: 48443</i>. If this gateway is not included in the selected list, click Add new gateway to create a new gateway with this setting. • In SMI Provider IP Address or Host Name, type the Brocade SMI-S Provider host. • Provide access credentials. • In Port, if using a non-default port, include the port number in the address. The default ports are 5988 for non-SSL and 5989 for SSL.
SolutionPack for Cisco MDS/Nexus	In the Select the components to install window: • In Alert Consolidation, select the Primary Backend host. • In Pre-configured alerts, select the Primary Backend host. • In Reports, select the Frontend host. • In SNMP Masks, select the Frontend host. In the Pre-configured alerts window: • In Alerting Web-Service Instance, select the Primary Backend host. • Select Enable the Cisco Switch Port Link Utilization Alert if desired. In the Reports window: • In Administration Web-Service Instance, select the Frontend host.
SolutionPack for Cisco UCS	In the Select the components to install window: • In Pre-configured alerts, select the Primary Backend host. • In Data Collection, select the Collector host. • In Events, select the Backend host. • In Reports, select the Frontend host. In the Pre-configured alerts window:

Table 3 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	• In Alerting Web-Service Instance, select the Primary Backend host. • In Recipient for email alerts, provide an email address. In the Data Collection window: • Select Activate the APG Failover-Filter if desired. • In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. • Leave Enable alerting on data collected checked. • In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010. • In UCS type, select UCS Manager (Blade Chassis) or UCS C-Series (Server). • In Hostname or IP address type the UCS management host. This is the server's management port. • In Username and Password, type the credentials for the management server. • In Communication port, type the port number for the management server. • Select the Enable events collection checkbox. • In Event server hostname or IP address, select the Backend host on which the events server is running. The default port is 52004. • Select Use advanced settings to configure polling settings. In the Events window: • Type the database information for the events database running on the Backend host. • The default Database port is 53306 and the default Event server port number is 52004. In the Reports window: • In Administration Web-Service Instance, select the Frontend host.
SolutionPack for Converged Infrastructure	In the Select the components to install window: • In Topology Collector, select the Collector host. • In Reports, select the Frontend host. In the Data Collection window: • Select Activate the APG Failover-Filter if desired. • In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020.

Table 3 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	• Leave Enable alerting on data collected checked. • In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010. • In UIM/P hostname or IP address, type the UIM/P host. • In Username and Password, type the required credentials for the UIM/P host. • In UIM/O hostname or IP address, type the UIM/O host. • In Username and Password, type the required credentials for the UIM/O host. • Select Use advanced settings to configure polling settings. • Click the plus (+) sign to add additional UIM devices. In the Reports window: • In Administration Web-Service Instance, select the Frontend host.
SolutionPack for EMC Centera	In the Select the components to install window: • In EMC Centera Collector, select the Collector host. • In Reports, select the Frontend host. In the Data Collection window: • Select Activate the APG Failover-Filter if desired. • In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. • Leave Enable alerting on data collected checked. • In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010. • In Hostname or IP address of the management node, type the Centera Viewer CLI host. • In Centera friendly name, type the name. • In Centera username (monitor role) and Password, type the credentials for the management server. The default is system/manager. • In Path to the Centera Viewer jar file (CenteraViewer.jar), type the path to the .jar file you configured as described in Preparing EMC Centera on page 51. • Select Use advanced settings to configure polling settings. • Click the plus (+) sign to add additional Centera devices. In the Reports window:

Table 3 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	In Administration Web-Service Instance, select the Frontend host.
SolutionPack for EMC Data Domain	In the Select the components to install window: - In Reports, select the Frontend host. - In SNMP Masks, select the Frontend host. In the Reports window: - In Administration Web-Service Instance, select the Frontend host.
SolutionPack for EMC Data Protection Advisor	In the Select the components to install window: - In Data Collection, select the Collector host. - In Events, select the Backend host. - In Reports, select the Frontend host. In the Data Collection window: - Select Activate the APG Failover-Filter if desired. - In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. - Leave Enable alerting on data collected checked. - In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010. - Select Enable alert collection from DPA. - In DPA appliance Host name or IP, type the host information for the DPA appliance. - In Please select the Credentials, provide the credentials for the DPA appliance. - If this is the first instance of SRM polling from the DPA instance, select Advanced Settings and Enable scheduling of DPA reports. If you do not select these options, there are no DPA reports for SRM to collect. - The Polling performance intervals are set by default. These are configurable. - Click the plus (+) sign to add additional DPA appliances. In the Events window: - Type the database information for the events database running on the Backend host. - The default Database port is 53306 and the default Network Port is 22020. - The Network port option is set by default, unless you configured a different port in the Data Collection window, Event server

Table 3 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	port. If you changed it there you must put the same port number in Network port. In the Reports window: • In Administration Web-Service Instance, select the Frontend host.
SolutionPack for EMC Isilon	In the Select the components to install window: • In Reports, select the Frontend host. • In SNMP Masks, select the Frontend host. In the Reports window: • In Administration Web-Service Instance, select the Frontend host.
SolutionPack for EMC VMAX	In the Select the components to install window: • In Alert Consolidation, select the Primary Backend host. • In Pre-configured alerts, select the Primary Backend host. • In Data Collection, select the Collector host. • In Reports, select the Frontend host. In the Pre-configured alerts window: • In Alerting Web-Service Instance, select the Primary Backend host. • Select the EMC VMAX Front-End Director Utilization Alert and Enable the EMC VMAX Front-End Director Port Utilization Alert checkboxes. In the Data collection window: • Select Activate the APG Failover-Filter if desired. • In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. • Leave Enable alerting on data collected checked. • In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010. • In APG WebService hostname or IP address, select the Frontend host and provide the port number (default 58080) and credentials to access the Frontend Web portal. • Leave Enable Topology Backend on data collected checked. • In Topology Backend hostname or IP address, select the Primary Backend host. • In Please select the Gateway, select the Primary Backend host and gateway port: <code>primary_backend:48443</code>. If this gateway is

Table 3 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	not included in the selected list, click Add new gateway to create a new gateway with this setting. • Leave Configure Unisphere performance collection checked. • In Unisphere hostname or IP address, select the host on which Unisphere for VMAX is running and change the default Unisphere network port, Username and Password if different. • Click the plus (+) sign to add additional Unisphere hosts. • If Solutions Enabler was installed in the default location, leave the Solutions Enabler bin directory empty. If installed in another location, type the path to the bin directory. • In Connection type, select Remote if you are using the Solutions Enabler proxy scenario or Local if you are using a local Solutions Enabler scenario. Refer to Preparing EMC VMAX on page 52 • In SYMAPI Connection name, type the connection name. The default is SYMAPI_SERVER. To view the name that is configured, use the <code>symcfg services list</code> command. • In the VMAX array configuration section of the Data collection window, you add the serial number of each array from which you want to collect data. Run the <code>symcfg list</code> command to view a list of arrays. You should only add arrays with an attachment of Local. • In Array Full Serial Number, type the Symmetrix SID and click the plus (+) icon to add additional SIDs. Note EMC recommends not to exceed six medium-sized (30K-40K devices) VMAX arrays for each VMAX collector. • Select Use advanced settings to configure polling settings. In the Reports window: • In Administration Web-Service Instance, select the Frontend host.
SolutionPack for EMC VNX	In the Select the components to install window: • In Alert Consolidation, select the Primary Backend host. • In Pre-configured alerts, select the Primary Backend host. • In Data Collection, select the Collector host. • In Events, select the Backend host. • In Reports, select the Frontend host. In the Pre-configured alerts window:

Table 3 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	• In Alerting Web-Service Instance, select the Primary Backend host. • Select the EMC VNX Block SP Utilization Alert and Enable the EMC VNX Block Dirty Pages Utilization Alert checkboxes. In the Data collection window: • Select Activate the APG Failover-Filter if desired. • In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. • Leave Enable alerting on data collected checked. • In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010. • In APG WebService hostname or IP address, select the Frontend host and provide the port number (default 58080) and credentials to access the Frontend Web portal. • Leave Enable Topology Backend on data collected checked. • In Topology Service hostname or IP address, select the Primary Backend host. • In Please select the Gateway, select the Primary Backend host and gateway port: <i>primary_backend</i>: 48443. If this gateway is not included in the selected list, click Add new gateway to create a new gateway with this setting. • In Event server hostname or IP address, select the Backend host on which the Events Listener is installed. The default port is 52001. • In Alert Event server hostname or IP address, select the Primary Backend host. The default port is 2040. • In Naviseccli Path, type the path if using a non-default path, or leave blank if you are using the default path. • In VNX type, select Block, File or Unified. • In Unique friendly name for the VNX system, type the name. • In SP A IP, type the IP address of the SPA. • In SP B IP, type the IP address of the SPB. • In Use Naviseccli security file, select this checkbox if you are using the security file. • In User Scope, select LDAP, Global or Local. • In Naviseccli Username and Naviseccli Password, type the Naviseccli credentials for the block storage systems. • In Primary control station IP, type the IP address of the primary control station.

Table 3 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	• In Secondary control station IP, type the IP address of the secondary control station. • In VNX File username and VNX File password, type the credentials for the file storage system. • Use the plus (+) icon to add more VNX arrays. • Select Use advanced settings to configure polling settings. In the Reports window: • In Administration Web-Service Instance, select the Frontend host.
SolutionPack for EMC VPLEX	In the Select the components to install window: • In Data Collection, select the Collector host. • In Reports, select the Frontend host. In the Data collection window: • Select Activate the APG Failover-Filter if desired. • In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. • Leave Enable alerting on data collected checked. • In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010. • In VPLEX type, select Geo/Metro or Local. • Provide cluster host and authentication details for VPLEX systems. • Use the plus (+) icon to add more VPEX systems. In the Reports window: • In Administration Web-Service Instance, select the Frontend host.
SolutionPack for EMC Watch4net Health	Install this SolutionPack on all core softwarehosts in your environment. In the Select the components to install window: • In Data Collection, select the Collector host. • In Reports, select the Frontend host. In the Data collection window: • Select Activate the APG Failover-Filter if desired. • In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. • Leave Enable alerting on data collected checked. • In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010.

Table 3 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	In the Reports window: In Administration Web-Service Instance, select the Frontend host.
SolutionPack for Hitachi Device Manager	In the Select the components to install window: - In Data Collection, select the Collector host. - In Reports, select the Frontend host. In the Data Collection window: - Select Activate the APG Failover-Filter if desired. - In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. - Leave Enable alerting on data collected checked. - In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010. - In Hitachi Device Manager, type the Hitachi Device Manager CIM server host. - In Username and Password, type the required credentials. - Optionally, select the Enable Secure Connection (SSL) checkbox. - If using a secure connection, the default port is 5989. If using a non-secure connection, the default is 5988. - Select the Do you want to configure advanced settings to configure polling and collection threads settings. - Click the plus (+) sign to add Hitachi Device Manager hosts. In the Reports window: - In Administration Web-Service Instance, select the Frontend host.
SolutionPack for HP 3PAR StoreServ	In the Select the components to install window: - In Data Collection, select the Collector host. - In Reports, select the Frontend host. In the Data Collection window: - Select Activate the APG Failover-Filter if desired. - In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. - Leave Enable alerting on data collected checked. - In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010. - In Array Name, type the HP 3PAR StoreServ array. - In Username and Password, type the required credentials.

Table 3 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	• Select the Do you want to configure advanced settings to configure polling and collection threads settings. • Click the plus (+) sign to add more arrays. In the Reports window: • In Administration Web-Service Instance, select the Frontend host.
SolutionPack for HP EVA	In the Select the components to install window: • In Data Collection, select the Collector host. • In Reports, select the Frontend host. In the Data Collection window: • Select Activate the APG Failover-Filter if desired. • In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. • Leave Enable alerting on data collected checked. • In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010. • In HP EVA specific configuration, select the host information and access credentials to communicate with the HP EVA Element Manager host. • Select Use advanced settings to configure polling settings. In the Reports window: • In Administration Web-Service Instance, select the Frontend host.
SolutionPack for IBM DS	In the Select the components to install window: • In Data Collection, select the Collector host. • In Reports, select the Frontend host. In the Data Collection window: • Select Activate the APG Failover-Filter if desired. • In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. • Leave Enable alerting on data collected checked. • In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010. • In IBM DS Model, select the appropriate model. • Type the IBM DS host information and access credentials to communicate with the IBM CIM/SMI-S provider on a management server.

Table 3 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	- If using a secure connection, the default port is 5989. If using a non-secure connection, the default is 5988. - Select Use advanced settings to configure polling settings. In the Reports window: - In Administration Web-Service Instance, select the Frontend host.
SolutionPack for IBM XIV	In the Select the components to install window: - In Data Collection, select the Collector host. - In Reports, select the Frontend host. In the Data Collection window: - Select Activate the APG Failover-Filter if desired. - In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. - Leave Enable alerting on data collected checked. - In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010. - Type the host information and access credentials to communicate with the IBM XIV. - If using a secure connection, the default port is 5989. If using a non-secure connection, the default is 5988. - Click the plus (+) sign to add more arrays. In the Reports window: - In Administration Web-Service Instance, select the Frontend host.
SolutionPack for Microsoft Hyper-V	In the Select the components to install window: - In Data Collection, select the Collector host. - In Reports, select the Frontend host. In the Data Collection window: - Select Activate the APG Failover-Filter if desired. - In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. - Leave Enable alerting on data collected checked. - In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010. - Type the host information and access credentials to communicate with the Hyper-V. - Click the plus (+) sign to add more Hyper-V hosts.

Table 3 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	In the Reports window: • In Administration Web-Service Instance, select the Frontend host.
SolutionPack for NetApp Filer	In the Select the components to install window: • In Data Collection, select the Collector host. • In Reports, select the Frontend host. In the Data Collection window: • Select Activate the APG Failover-Filter if desired. • In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. • Leave Enable alerting on data collected checked. • In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010. • In NetApp Filer Mode, leave the default, 7-Mode or select C-Mode. • Type the NetApp Filer host information and access credentials to communicate with the NetApp Filer CLI. In the Reports window: • In Administration Web-Service Instance, select the Frontend host.
SolutionPack for Oracle Database	In the Select the components to install window: • In Data Collection, select the Collector host. • In Reports, select the Frontend host. In the Data Collection window: • Select Activate the APG Failover-Filter if desired. • In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. • Leave Enable alerting on data collected checked. • In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010. • In Choose configuration mode, select Simple, RAC Instance, or Advanced. • In Database port, type the port number. The default is 1521. • In Database service name, type the database SID. • Type the access credentials to communicate with the Oracle database. • Click the plus (+) sign to add more Oracle databases.

Table 3 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	- Optionally select the Enable property import for server enrichment checkbox. - In the Backend configuration section, type the host information and credentials for the Backend host. - Select Configure collector advanced settings to configure polling settings. In the Reports window: - In Administration Web-Service Instance, select the Frontend host.
SolutionPack for Physical Hosts	In the Select the components to install window: - In generic-host-alertconsolidation, select the Primary Backend host. - In Pre-configured alerts, select the Primary Backend host. - In Reports, select the Frontend host. - In Scripts, select the Collector host. In the Pre-configured alerts window: - In Alerting Web-Service Instance, select the Primary Backend host. - Select Enable the Host PowerPath Alerts if desired. - In Recipient for email alerts, provide an email address. In the Reports window: - In Administration Web-Service Instance, select the Frontend host. In the Scripts window: - Select Collect performance metrics if desired. - Select Collect performance metrics for PowerPath LUNs if desired. - Select Use advanced settings to configure polling settings.
SolutionPack for EMC Host Interface	In the Select the components to install window: - In Data Collection, select the Collector host. In the Data Collection window: - Select Activate the APG Failover-Filter if desired. - In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. - Leave Enable alerting on data collected checked. - In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010.

Table 3 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	• Leave Enable Topology Backend on data collected checked. • In Topology Service hostname or IP address, type the Primary Backend host. • In Please select the Gateway, select the Primary Backend host and gateway port: <i>primary_backend:48443</i>. If this gateway is not included in the selected list, click Add new gateway to create a new gateway with this setting. • In Host running Host Provider (IP or hostname), type a host on which the EMC Host Interface is installed. • In Please select the Credentials, select the user name configured when the EMC Host Interface was installed. • Optionally, select the Enable Secure Connection (SSL) checkbox. • If using a secure connection, the default port is 5989. If using a non-secure connection, the default is 5988. • Select the Do you want to configure advanced settings to configure polling and collection threads settings. Note For performance reasons, change the Topology polling interval from its default 900 (15 minutes) to 21600 (6 hours). • Click the plus (+) sign to add more hosts.
SolutionPack for RecoverPoint	In the Select the components to install window: • In EMC RecoverPoint Collector, select the Collector host. • In Reports, select the Frontend host. In the Data Collection window: • Select Activate the APG Failover-Filter if desired. • In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. • Leave Enable alerting on data collected checked. • In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010. • In RecoverPoint FQDN hostname, type the fully-qualified domain name of the RecoverPoint host. • In Please select the Credentials, select the user name to access the RecoverPoint host. • Select Do you want to configure advanced settings to configure polling settings. • Click the plus (+) sign to add more hosts. In the Reports window:

Table 3 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	In Administration Web-Service Instance, select the Frontend host.
SolutionPack for Storage Compliance	Note the following: - If you are installing the on a Windows host, stop the process jucheck.exe. This is a Java JRE update validator and uses the same port as the SolutionPack. - Do not install multiple instances of the Storage Compliance Backend, as the same port would be used for each installation. This will lead to service startup failure. - Alerting backend service should be available during installation; otherwise alerting definition will not be created. The SolutionPack for Storage Compliance creates alerting definition for notifying mentioned users with email alerts for breaches/violations. - Though the Compliance service comes up immediately, do not run ESM rules as the SolutionPack installation also populates the database with ESM data, for ESM rule validation, which takes some time to get the database populated (approximately 15-20 minutes). In the Select the components to install window: - In Compliance Notifications, select the Primary Backend host. - In Compliance Backend, select the Primary Backend host. - In Compliance Reports, select the Frontend host. In the Compliance Notifications window: - In Alerting Web-Service Instance, select the Primary Backend host. In the Compliance Backend window: - In the APG WebService (WS) Details section, select the Frontend host and provide the port number (default 58080) and credentials to access the Frontend Web portal. - In the Breach Notification Details section, select the Primary Backend host. In the Reports window: - In Administration Web-Service Instance, select the Frontend host.
SolutionPack for VI VirtualWisdom	In the Select the components to install window: - In Data Collection, select the Collector host. - In Reports, select the Frontend host. In the Data Collection window: - Select Activate the APG Failover-Filter if desired.

Table 3 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	• In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. • Leave Enable alerting on data collected checked. • In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010. • In VirtualWisdom Server Name, type the VirtualWisdom Portal Server host. • In VirtualWisdom Server Port, type the port for the webservice proxy. The default is 8080. The value is configured in the <code>virtualwisdom.properties</code> file in the VirtualWisdom installation directory on the VirtualWisdom Portal Server. • In VirtualWisdom Username and Password, type the credentials used for authentication with the proxy. • Select Enable advanced settings to configure polling and collection threads settings. In the Reports window: • In Administration Web-Service Instance, select the Frontend host.
SolutionPack for VMware vCenter	In the Select the components to install window: • In Alert Consolidation, select the Primary Backend host. • In Pre-configured alerts, select the Primary Backend host. • In Data Collection, select the Collector host. • In Events, select the Backend host. • In Reports, select the Frontend host. • In Scripts, select the Collector host. In the Pre-configured alerts window: • In Alerting Web-Service Instance, select the Primary Backend host. • Select Enable the Host PowerPath Alerts if desired. • In Recipient for email alerts, provide an email address. In the Data collection window: • Select Activate the APG Failover-Filter if desired. • In Hostname or IP address to send data, type the Primary Backend host. the default port is 2020. • Leave Enable alerting on data collected checked. • In Alerting Backend the hostname or IP address, select the Primary Backend host. The default port is 2010.

Table 3 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	- In Topology Service hostname or IP address, type the Primary Backend host. - In Please select the Gateway, select the Primary Backend host and gateway port: <i>primary_backend: 48443</i>. If this gateway is not included in the selected list, click Add new gateway to create a new gateway with this setting. - In VMWare vCenter Hostname or IP address, type the vCenter service host and the Username and Password used to poll vCenter. - Select Do you want to configure advanced settings to configure polling and collection thread settings, a backend data group, and a re-synch interval. - Click the plus (+) sign to add more hosts. In the Events window: - Type the database information for the events database running on the Backend host. - The default Database port is 53306. - In VMWare vCenter Hostname or IP address, type the vCenter service host and the Username and Password used to poll vCenter. - Click the plus (+) sign to add more hosts. In the Reports window: - In Administration Web-Service Instance, select the Frontend host.

Post-installation configuration of SolutionPacks

This topic describes any required or suggested configuration for each Storage Resource Management Suite SolutionPack after installation.

SolutionPack Configuration Details

SolutionPack	Configuration Details
SolutionPack for Brocade FC Switch	You do not need to perform any additional configuration.
SolutionPack for Cisco MDS/Nexus	You do not need to perform any additional configuration.
SolutionPack for Cisco UCS	You do not need to perform any additional configuration.
SolutionPack for Converged Infrastructure	You do not need to perform any additional configuration.

SolutionPack	Configuration Details
SolutionPack for EMC Centera	You do not need to perform any additional configuration.
SolutionPack for EMC Data Domain	You do not need to perform any additional configuration.
SolutionPack for EMC Data Protection Advisor	To enable object discovery, data collection, and events reporting, log in to the MySQL console of the suite virtual appliance and type mysql> source /opt/APG/Event-Processing/Generic-Live-Writer/emc-dpa/conf/create_table_dpa_events.sql to enable database events. Edit your Web-Application configuration file, APG.xml. Go to the conf/Catalina/localhost/APG.xml file and add the following line to the ResourceLink tag within the emc-dpa section: <pre><ResourceLink name="jdbc/FLOW-DPA-LIVE:{ mapping=FLOW-DPA.xml, table=dpa_events }" global="jdbc/FLOW-EVENTS" type="javax.sql.DataSource"/></pre> Type manage-modules.sh service restart all to restart all services. After some collection cycles, data will be available in the SolutionPack.
SolutionPack for EMC Isilon	To establish polling of the Isilon arrays, you need to add the arrays to an SNMP Collector using the Device Discovery page in the Frontend user interface. To add agents (SNMP devices) to your installation, navigate to http://Frontend-Host:58080/device-discovery .
SolutionPack for EMC VMAX	Refer to Configuring Solutions Enabler client access for VMAX on page 86 for detailed procedures for configuring a secure host and user-based authorization solution. After installing or updating a SolutionPack, new data will not be available for three polling cycles. The data is available to the UI every hour with the Property Store task. This task can be run earlier, if desired, by selecting the Property Store task found on the Frontend host.
SolutionPack for EMC VNX	To enable events reporting, edit your Web-Application configuration file (APG.xml), by uncommenting the emc-vnx section (uncomment the ResourceLink tag). You will then need to restart the Tomcat service in order to make the change effective. The Tomcat Catalina APG.xml file is located in: /APG/Web-Servers/Tomcat/Default/conf/Catalina/localhost After installing or updating a SolutionPack, new data will not be available for three polling cycles. The data is available to the UI every hour with the Property Store task. This task can be run earlier, if desired, by selecting the Property Store task found on the Frontend host.
SolutionPack for EMC VPLEX	You do not need to perform any additional configuration.

SolutionPack	Configuration Details
SolutionPack for EMC Watch4net Health	You do not need to perform any additional configuration.
SolutionPack for Hitachi Device Manager	You do not need to perform any additional configuration.
SolutionPack for HP 3PAR StoreServ	Depending on the numbers of Storage elements managed, you may need to edit the <code>unix-services.properties</code> file to increase the Heap Memory to a suitable level. The file is located at: <code>/APG/Collecting/Collector-Manager/your_instance/conf/unix-services.properties</code>
SolutionPack for HP EVA	You do not need to perform any additional configuration.
SolutionPack for IBM DS	You do not need to perform any additional configuration.
SolutionPack for IBM XIV	You do not need to perform any additional configuration.
SolutionPack for Microsoft Hyper-V	You do not need to perform any additional configuration.
SolutionPack for NetApp Filer	You do not need to perform any additional configuration.
SolutionPack for Oracle Database	After the Collector-Manager has been running for 30 seconds or more, review the <code>Collecting-0.0.log</code> file to determine if any operational issues exist. To access the log file: 1. Expand the <code>Log Files</code> section of the Collector-Manager. 2. Open the <code>collecting-0.0.log</code>. 3. Verify that the Collector-Manager started without <code>Severe</code> errors. To verify, look for conditions marked as <code>Severe</code> and troubleshoot the indicated problem. Note the following: • You may see a severe error: <code>Failed to load properties for name [/cache.ccf]</code>. This error is a normal condition that occurs at start-up time and can be ignored. • Look for the <code>collect done</code> line, which confirms that data is being collected: <pre>'Oracle-Perf' collect done: 549 new raw values collected in 3 seconds 537 ms using 25 SQL queries</pre>
SolutionPack for Physical Hosts	You do not need to perform any additional configuration.
SolutionPack for EMC Host Interface	You do not need to perform any additional configuration.
SolutionPack for RecoverPoint	You do not need to perform any additional configuration.
SolutionPack for Storage Compliance	After installing the SolutionPack you have to restart the following services: To restart the tomcat service: 1. Go to <code>/OPT/APG/bin</code>

SolutionPack	Configuration Details
	2. Run the command <code>./manage-modules.sh service restart tomcat instance-name</code> To restart the backend service: 1. Navigate to Administration > Centralized Management > Physical View and select the host on which the backend is installed. 2. Select backend. The backend service details view appears. 3. Click Restart. If you reset the web service password, then you have to reconfigure the Storage Compliance SolutionPack as follows: 1. Navigate to Administration > Centralized Management > SolutionPacks > Storage Compliance. 2. Click  to reconfigure the Compliance Backend SolutionPackBlock instance. 3. Type the new password in the web service details section. 4. Click Reconfigure. 5. Restart the tomcat service.
SolutionPack for VI VirtualWisdom	You do not need to perform any additional configuration.
SolutionPack for VMware vCenter	• To enable PowerPath LUN or Path performance data collection on Linux, navigate to <code>APG/Collecting /Remote-Shell-Collector/<Instance Name>/scripts directory</code> 1. Edit <code>LunMappingDetection.pl</code> script. 2. Set <code>want_powerpath_lun_performance=1</code> Note By default, the <code>want_powerpath_lun_performance</code> flag is set to 0 • To enable PowerPath LUN or Path performance data collection on Windows, navigate to <code>C:\Program Files\APG\Collecting \Remote-Shell-Collector\<Instance Name> \scripts\windows directory</code>. 1. Edit <code>LunMappingDetection.ps1</code> script. 2. Set <code>powerPathPerformanceCollection=enabled</code>. Note By default, the <code>powerPathPerformanceCollection</code> flag is set to disabled. • To enable events reporting,

SolutionPack	Configuration Details
	1. Edit your Web-Application configuration file (<code>APG.xml</code>), by uncommenting the <code>vmware-vcenter</code> section (uncomment the <code>ResourceLink</code> tag). 2. Restart the Tomcat service in order to make the change effective.

Documentation Resources

For SolutionPacks which have no additional configuration required, you can refer to the *EMC Storage Resource Management Suite User and Administration Guide* and online help for information on using SolutionPacks.

Post-installation configuration details

This topic provides detailed post-installation configuration information for a specific SolutionPacks.

In some cases you may need to perform more extensive configuration tasks related to a SolutionPack that cannot be effectively covered in the checklist provided in [Post-installation configuration of SolutionPacks on page 82](#).

Configuring Solutions Enabler client access for VMAX

Symmetrix Authorization using `symauth` provides a secure host and user-based authorization solution. Use this procedure in environments in which Symmetrix Authorization is enabled.

Before you begin

Ensure that you have configured an appropriate Solutions Enabler scenario as described in [Preparing EMC VMAX on page 52](#)

For more detailed information about Solutions Enabler, refer to the following documents:

- ◆ *EMC Solutions Enabler Symmetrix Array Management Product Guide*
- ◆ *EMC Solutions Enabler Symmetrix Security Configuration Guide*

The following configuration procedures are specific to a Solutions Enabler proxy configuration. However, you can also use these procedures for a local Solutions Enabler configuration in which the SRM Suite Collector software is installed directly on the existing SYMAPI Solutions Enabler server. The term "client" refers to the host where the Collector software has been installed.

Procedure

1. Validate if Symmetrix Authorization is enabled by running the `symauth list` command on the host that has direct FC connectivity to the arrays to be managed.
2. Check the status displayed in the the `Authorization Control` section to determine the required action:

Option	Description
Disabled	Symmetrix Authorization is not configured.

Option	Description
Enabled	Symmetrix Authorization is configured. In this case, you must configure the apg user and SRM Suite hosts that will be issuing commands. Continue to step 3.

3. If Symmetrix Authorization is enabled, use the following procedures to complete the configuration:
 - a. [Configuring host access on page 87](#)
 - b. [Adding client hosts to existing SYMAUTH configuration on page 87](#)
 - c. [Enabling client authorization on page 88](#)
 - d. [Validating Symmetrix access controls on page 89](#)

Configuring host access

Enable the SRM Suite apg account to access the local Solutions Enabler resources and logs.

This procedure provides an example of configuring access on a host using the Linux operating system.

Procedure

1. Log in to the Solutions Enabler client host.
2. Navigate to `/var/symapi`
3. Grant the `apg` user write access to the following Solutions Enabler directories and contents:
 - a. `chown -R apg <SYMAPI_HOME>/config`
 - b. `chown -R apg <SYMAPI_HOME>/db`
4. Repeat steps 1-3 for each VMAX Collector server.
5. Grant the `apg` user authorization for the Solutions Enabler storapid daemon by navigating to `<SYMAPI_HOME>/config/daemon_users` and adding the following line to the `storapid[Base Daemon]` section of the file:


```
apg storapid <all>
```
6. Save and exit the `daemon_users` file.
7. Set a password for the `apg` user.
8. Repeat steps 5-7 for each VMAX collector server.
9. Log out and log in as the `apg` user and run `symauth show -username` to determine the fully-qualified account name.
10. Make note of the value displayed in `your current username`. For example:


```
H:system_name\apg
```
11. Repeat steps 9-11 for each VMAX Collector server.

Adding client hosts to existing SYMAUTH configuration

Enable the `apg` user with read-only monitoring access for VMAX arrays using Solutions Enabler User Authorization.

Before you begin

Complete the procedure described in [Configuring host access on page 87](#).

You must be logged in as Root or Administrator.

Perform the following procedure for each VMAX you want to enable SRM Suite to access.

Procedure

1. Run the `symauth -sid <SID> list` command to determine if User Authorization Control is enabled on the local client system.
 - If User Authorization Control is disabled (Disabled) for the specific VMAX, proceed to [Enabling client authorization on page 88](#).
 - If User Authorization Control is enabled (Enabled) and in use (Enforced) for the specific VMAX, continue with this procedure.
2. Ensure that you are logged in with an existing privileged account (e.g., root or administrator).
3. Use the `find / -name auth.txt` command to find the `auth.txt` file.
4. Navigate to the folder with the `auth.txt` file.
5. Edit the file to include a line based on the results obtained from performing the procedure described in [Configuring host access on page 87](#). For example:


```
assign user H:system_name\apg to role Monitor;
```
6. Save the file.
7. Use the `symauth -sid <SID> -f auth.txt` command to commit changes to the User Authorization User-to-Role map.
8. Repeat this procedure for each VMAX array.

Enabling client authorization

Use this procedure when User Authorization Control is disabled (Disabled) for the specific VMAX and you want to restrict the `apg` user to a monitoring role without limiting other accounts in the environment.

Before you begin

You determined that User Authorization Control is disabled by performing the task described in [Adding client hosts to existing SYMAUTH configuration on page 87](#).

You are logged in to the client host with local root or administrator credentials.

Procedure

1. Create an `auth.txt` file with the following contents:


```
assign user * to role Admin;

set enforcement enforce;

assign user H:system_name\apg to role Monitor;
```
2. Repeat step 1 for each VMAX Collector server.
3. Use the `symauth -sid <SID> -f auth.txt` command to commit changes to the User Authorization User-to-Role map.
4. Repeat step 3 for each VMAX array.
5. Use the `symauth -sid <SID> enable` command to enable User Authorization Control for a specific VMAX array.
6. Repeat step 5 for each VMAX array.

7. Use the `symauth list` command to validate that User Authorization Control is enabled and enforced.

```

S Y M M E T R I X   A U T H O R I Z A T I O N   S T A T U S

Symmetrix ID: 000195700363

Authorization Control           : Enabled

Time Enabled                   : Mon Aug  5 12:51:08 2013
Time Disabled                   : Thu Aug  1 15:54:23 2013
Time Updated                    : Mon Aug  5 12:51:08 2013

Enforcement Mode               : Enforce
Server Policy                   : Trust clients

```

Validating Symmetrix access controls

Validate that the Symmetrix Access Control (SymACL) security feature is enabled and in use on VMAX systems.

Before you begin

You are logged in to the client host with local root or administrator credentials.

Procedure

1. Run the `symacl list` command for each VMAX array. Status information is displayed.

```

S Y M M E T R I X   A C C E S S   C O N T R O L   S T A T U S

Symmetrix ID: 000195700363

Access   Session
Control  Locked   Time Last Updated
-----
N/A      N/A      N/A

Symmetrix ID: 000195700932

Access   Session
Control  Locked   Time Last Updated
-----
N/A      N/A      N/A

```

- If the Access Control field indicates N/A, SymACL is not enabled on this VMAX system.
 - If the Access Control field indicates Enabled, continue this procedure to secure SRM Suite client systems from a host system in the existing `SymACL AdminGrp` for each VMAX system.
2. Create a SymACL access group appropriate to contain the SRM Suite client systems (e.g., SRMGRP)
 3. Add each client system's unique identifier to the access group.
 4. Repeat for each SRM Suite client host system.
 5. Grant BASE access rights to the access group just created for all devices (ALL_DEVS).
 6. Repeat this procedure for each VMAX system monitored by SRM Suite.

Enabling passive host discovery through Brocade FC SolutionPack

You have to enable passive host discovery when you want to see end to end topology from hosts to array and identify chargeback on SAN enabled hosts, without active host discovery.

You can passively resolve hosts, discovered through the SolutionPack for Brocade FC Switch, from zoning records.

The zone naming patterns supported in SRM Suite are:

`z_%h%`

`z_%h%_*`

`z_%h%_ *_*`

`%h%_*`

If you want to add a new host zone naming pattern, then you have to add the corresponding regular expression to the configuration file `vhf-mds-zone-dns.xml` located in `/opt/APG/Collecting/Variable-Handling-Filter/brocade-fc-switch/conf` directory.

Procedure

1. Click **Administration**.
2. Click **Centralized Management**.
3. Click **SolutionPacks**.
4. Click **Brocade FC Switch** SolutionPack.
5. Click  to reconfigure the **SMI Data Collection** SolutionPackBlock instance.
6. Select **Enable Passive Host Discovery** checkbox.
7. Click **Reconfigure**.

Enabling passive host discovery through Generic-SNMP

You have to enable passive host discovery when you want to see end to end topology from hosts to array and identify chargeback on SAN enabled hosts, without active host discovery.

You need to reconfigure Generic-SNMP independent solution pack to enable passive host discovery through the SolutionPack for Cisco MDS/Nexus.

The zone naming patterns supported in SRM Suite are:

`z_%h%`

`z_%h%_*`

`z_%h%_ *_*`

`%h%_*`

If you want to add a new host zone naming pattern, then you have to add the corresponding regular expression to the configuration file `vhf-mds-zone-dns.xml` located in `/opt/APG/Collecting/Variable-Handling-Filter/Generic-SNMP/conf` directory:

Procedure

1. Click **Administration**.

2. Click **Centralized Management**.
3. Click **SolutionPacks**.
4. Under **Independent SolutionPack Blocks**, click  to reconfigure the **Generic-SNMP** SolutionPackBlock instance.
5. Select **Enable Passive Host Discovery** checkbox.
6. Click **Reconfigure**.

Post-install configuration for SolutionPack for Physical Hosts

In order to discover hosts and collect data you have to perform the following configuration on the collector after installing the SolutionPack for Physical Hosts

1. [Add hosts for discovery and data collection on page 91](#)
2. [Configure remote shell collector on page 91](#)

Adding hosts for discovery and data collection

In order to discover hosts and collect data from the hosts you have to add the hosts through the Discovery Center.

Procedure

1. Click **Administration**.
2. Click **Centralized Management** > **Discovery Center**.
3. Click **Host Configuration**.
4. Click **Add new device....**
5. Provide these details for the host:

Option	Description
Server	Specify the server on which the host has to be discovered.
Instance	Specify the instance Generic-RSC on which the host has to be discovered.
Host name or IP address	Type the host name or the IP address of the host.
Specify the OS type	Type the operating system. Available values are: AIX, HPUX, LINUX, Solaris, and Windows.
Authentication type	Available values: <code>Password based</code>: Type in the username and password <code>Public key based</code>: Type in the username and location of the private key.
Custom Port	Provide the network port if you enable this.

Configuring remote shell collector

If you have a scale-out environment, you have to configure the collectors so that data can be forwarded to Linux VMs which are receiving data into APG `backend/Topology Service`. These configuration changes will enable you to view topology maps and IO connectivity on a multiple VM SRM Suite instance. You do not require this configuration

for standalone Windows binary installer or if Windows host is discovered natively from Linux VM from vApp SRM Suite instance.

Before you begin

You have the SolutionPack for Physical Hosts installed.

Procedure

1. Click **Administration**.
2. Click **Centralized Management**.
3. Click **SolutionPacks**.
4. Under **Independent SolutionPack Blocks**, click  to reconfigure the **Generic-RSC** SolutionPackBlock instance.
5. Provide the following details under Generic-RSC.

Option	Description
Push INQ	Select this checkbox to push inq on the target host.
Hostname or IP address to send data to	The hostname or IP address of the host to which the collected data is to be sent.
Alerting Backend hostname or IP address	The Alerting Backend hostname or IP address of the host where the data is to be sent, for alerting on real time data.
Topology Service hostname or IP address	The Topology Service hostname or IP address from where the data can be queried from, for data collection and property tagging.

6. Click **Reconfigure**.

Configuring compliance-frontend.xml

To enable storage compliance features, you have to edit the compliance-frontend.xml by replacing `localhost` with primary backend VM name in a multiple VM environment. Also, if you have installed multiple databases, you have to edit the xml file to connect these databases.

Before you begin

SolutionPack for Storage Compliance must be installed.

Procedure

1. Log in to the host using **Putty**.
2. Change the directory path to `/opt/APG/Web-Servers/Tomcat/Default/conf/Catalina/localhost/` and edit the `compliance-frontend.xml` file to make changes to `localhost` and replace it with the name of the primary backend VM (same location where compliance backend is installed) in the following three entries:

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

```

        factory="org.apache.naming.factory.BeanFactory"
            user="admin" pass="changeme"
        url="service:jmx:rmi:///jndi/rmi://localhost:52755/jmxrmi" />
    • <Resource name="manager/CompliancePolicyTemplateManager"
        auth="Container"

        type="com.emc.srm.base.compliance.jmx.ComplianceManagerFactory"

        factory="org.apache.naming.factory.BeanFactory"
            user="admin" pass="changeme"
        url="service:jmx:rmi:///jndi/rmi://localhost:52755/jmxrmi" />

```

3. If you have installed multiple databases, you have to edit the compliance-frontend.xml file located in the /opt/APG/Web-Servers/Tomcat/Default/conf/Catalina/localhost/ directory to connect all the databases.

```

<!-- Gives access to the timeseries database. -->
<ResourceLink name="jdbc/APG-DB:{ cachegrp=DB }" global="jdbc/APG-DB" type="javax.sql.DataSource"/>
<ResourceLink name="jdbc/APG-DB4:{ cachegrp=DB }" global="jdbc/APG-DB4" type="javax.sql.DataSource"/>
<ResourceLink name="jdbc/APG-DB3:{ cachegrp=DB }" global="jdbc/APG-DB3" type="javax.sql.DataSource"/>
<ResourceLink name="jdbc/APG-DB2:{ cachegrp=DB }" global="jdbc/APG-DB2" type="javax.sql.DataSource"/>
<ResourceLink name="jdbc/APG-DB1:{ cachegrp=DB }" global="jdbc/APG-DB1" type="javax.sql.DataSource"/>

```


CHAPTER 7

Migration for Multiple Hosts

This chapter includes the following topics:

◆ Migration workflow.....	96
◆ Migrating core software on a UNIX server.....	99
◆ Migrating core software on a Windows server.....	99
◆ Identifying which modules to update.....	100
◆ Module update order for multiple hosts.....	100
◆ Updating modules	103
◆ Updating all core software services from the command line.....	106
◆ Starting the core software services from the command line.....	106
◆ Logging in to Centralized Management.....	107
◆ Confirming settings for the first time.....	107
◆ Retrieving the list of modules from remote host servers using Centralized Management.....	108
◆ Updating modules from Centralized Management.....	108
◆ Installing the generic-rsc package.....	110
◆ Installing the generic-topology package.....	110
◆ Installing the Maps-Service package.....	111
◆ Updating the SolutionPackBlocks.....	111
◆ Controlling services from Centralized Management.....	112
◆ Default ReportPack migration.....	112
◆ Installing a SolutionPack.....	114
◆ Post-migration tasks.....	115
◆ Reviewing reports.....	122

Migration workflow

If you have existing core software installed, you need to migrate to the latest software version.

Depending on your existing core software version, do one of the following procedures.

If you have:	Perform:
Legacy core software such as version 6.1 or 6.1ux.	1. Migrate to version 6.2 as described in the <i>EMC Watch4net Migration Guide</i> available from EMC Online Support. Note You must migrate any older Watch4net releases to version 6.2.x before using the procedures in this guide to migrate to version 6.3. The Migration Guides for each release describe how to update from one version to the next. 2. Migrate from version 6.2 to version 6.3.
Core software version 6.2 or 6.2ux.	Migrate to version 6.3: ◆ Migration for multiple hosts with installed SolutionPacks on page 96 ◆ Migration for single host with installed SolutionPacks on page 124

Migration for multiple hosts with installed SolutionPacks

In this migration scenario, version 6.2.x software is already installed on multiple hosts and you wish to migrate to version 6.3.x.

Prerequisites

- ◆ Ensure each host server to be migrated meets system requirements for version 6.3.x.
- ◆ Identify the server hosting Centralized Management. Use this server to launch the setup script or executable first (*productname-setup-linux-x86_64-v63.sh* or *productname-setup-win64-v63.exe*).
- ◆ Ensure each host server is listed in the **Physical Overview** section of the Centralized Management server.
- ◆ Version 6.2.x must be installed and running on all host servers.
- ◆ Version 6.3.x software installs with temporary licenses for each feature. Ensure you obtain permanent licenses for any SolutionPacks you plan to use for longer than 30 days.
- ◆ Ensure each host server has 2 GB free disk space.
- ◆ Ensure you have a login with root or system administrator privileges.
- ◆ Back up the existing installation before starting the migration tasks.
- ◆ Review the workflow before starting and refer back to it as needed during the migration process.

Workflow

Migration for multiple hosts consists of two phases:

- ◆ Updating the host server designated for Centralized Management
- ◆ Updating the remote servers from the Centralized Management server

You will use CLI commands to migrate specific core modules on the server designated for Centralized Management. Then log into Centralized Management and retrieve all module packages from the remote host servers. After this step, you can update most modules on the remote host servers from the Logical Overview and SolutionPack nodes in Centralized Management. A small number of core module updates require you to log into the remote servers and issue CLI commands. It is very important to follow the recommended order of module updates.

1. Log into the server designated for Centralized Management and run the setup script or executable. This step copies version 6.3.x modules into the Module Repository folder in the existing APG directory path. [Migrating core software on a UNIX server on page 99](#) or [Migrating core software on a Windows server on page 99](#)
2. If you have host servers using different architectures (Windows versus Linux for example), choose one server with an architecture different from the Centralized Management server and run the setup script or executable there as well. Run the script on only one host server per type of architecture.
3. On the server designated for Centralized Management, issue the `manage-modules list installed` command to determine which modules require updating. The Status column identifies modules available for update. [Identifying which modules to update on page 100](#)
4. Review the order in which modules must be updated. [Module update order for multiple hosts on page 100](#)
5. Use the `manage-modules update <module name>` CLI command to update a subset of core modules before proceeding to update modules in Centralized Management. [Updating modules on page 103](#)
6. Update services. [Updating all core software services from the command line on page 106](#)
7. Start services. [Starting the core software services from the command line on page 28](#)
8. Log on to the server designated for Centralized Management. [Logging in to Centralized Management on page 107](#)
9. If you added or updated servers, confirm the settings.
10. Retrieve module packages from remote host servers in order to update them from the Centralized Management server. [Retrieving the list of modules from remote host servers using Centralized Management on page 108](#)
11. Update a second subset of core modules from Centralized Management. Ensure you follow the recommended update order and restart any services that are stopped by the update process.

Note

After you retrieve modules from the remote servers, you may find another set of modules similar to the ones you updated earlier with CLI commands. After you retrieve modules from the remote servers, launch all updates from Centralized Management in the correct order. For `module-manager`, `java`, and `webservice-gateway` modules, you must also log in to the remote host servers and complete the update process using CLI commands. [Module update order for multiple hosts on page 100](#)

[Updating modules from Centralized Management on page 108](#)

12. Install new package files to enable topology features. [Installing the generic-rsc package on page 110](#), [Installing the generic-topology package on page 110](#) and [Installing the Maps-Service package on page 111](#)
13. Update Independent SolutionPackBlocks followed by SolutionPackBlocks.

Note

After this step, there will still be a small number of modules (Collectors and Event Processors) that are marked as available for update with the yellow star icon. Do not update these modules.

14. Ensure that all services stopped during the update process have restarted. [Controlling services from Centralized Management on page 112](#)
 15. Update the default ReportPack to ensure the latest SolutionPack template is in use. [Updating the Default ReportPack on page 113](#)
 16. Install new SolutionPacks to add new features available in version 6.3. [Installing a SolutionPack on page 64](#)
-

Note

Some SolutionPacks require additional steps such as creation of database schemas or updates to the APG.xml file. Check the SolutionPack documentation for details.

17. Review reports. [Reviewing reports on page 122](#)

Conventions for defaults

During the migration, the multiple choice questions show the default answer with an uppercase letter (for example, Y/n means Yes is the default answer). Press **Enter** to accept the default. Press **Enter** to accept the default. If you enter **A** for All, the all actions will be performed. If you enter **N** for None, none of the actions will be performed.

Default directory paths are:

Operating system	Default installation directory
UNIX	/opt/APG/
Windows	C:\Program Files\APG\

Operating system	Default module repository directory
UNIX	<INSTALL_DIR>/Tools/Module-Repository
Windows	<INSTALL_DIR>\Tools\Module-Repository

Note

Install the 6.3 core software into the same directory where the 6.2 core software exists. If you do not specify the same directory, the setup script or executable may overwrite the services configurations since the setup script or executable does not detect the existing 6.2 installation.

Migrating core software on a UNIX server

Perform this procedure on a single host where version 6.2.x software is already installed. Typically, the host has core software with installed SolutionPacks. During the procedure, you must assign executable permissions to the setup script.

Before you begin

- ◆ Make sure you have a login with root privileges to run the setup script.
- ◆ Download the installation package to a directory on the server, such as `/temp`.

Procedure

1. Locate the installation package.
2. Change the permissions of the setup script so you can run it.

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

```
chmod +x productname-setup-linux-x86_64-v63.sh
```

3. Run the setup script from the directory.

For example:

```
./productname-setup-linux-x86_64-v63.sh
```

4. Read and accept the End User License Agreement. Use the **space bar** to scroll through the agreement. Press **y** and **Enter** to accept it.
5. Press **Enter** to accept the default installation directory of `/opt/APG`.

Or, if your existing core software resides in another location, specify the other location and press **Enter**.

6. Press **y** and **Enter** to install the new packages in the `/opt/APG/Tools/Module-Repository` directory.

After you finish

Identify which modules to update.

Migrating core software on a Windows server

Perform this procedure on a single host where version 6.2.x software is already installed. Typically, the host has core software with installed SolutionPacks. During the procedure, you must assign executable permissions to the setup executable.

Before you begin

- ◆ Make sure you have a login with system administrator privileges to run the setup executable.
- ◆ Download the installation package to a folder on the server, such as `\temp`.

Procedure

1. Locate the installation package.
2. Double-click the setup executable.

For example: `productname-setup-win64-v63.exe`

3. Click **Next** in the **Welcome** screen.
4. Read and accept the End User License Agreement. Click **I Agree**.

5. Press **Enter** to accept the default installation directory of `C:\Program Files\APG`.

Or, if your existing core software resides in another location, specify the other location and press **OK**.

6. Press **OK** to install the new packages in the `C:\Program Files\APG\Tools\Module-Repository` directory.

After you finish

Identify which modules to update.

Identifying which modules to update

After you update a core software installation, run the `manage-modules.sh list installed` command to view the installed modules and to determine which modules to update. Update the modules with the status of `can be updated`.

Procedure

- ◆ Type the command for your operating system from the core software installation directory:

Operating system	Command
UNIX	<code><INSTALL_DIR>/bin/manage-modules.sh list installed</code>
Windows	<code><INSTALL_DIR>\bin\manage-modules.cmd list installed</code>

When you view the output, record the identifier value of each module that needs to be updated. You will need to specify the identifier later when you update the module.

This sample output indicates to update the Module-Manager first, then to update the Alerting-Backend and the Alerting-Frontend modules to version 3.5. For other lines, pay attention to the status recommendations.

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

Identifier Revision OS-Arch	Instance Status	:Category	Module Name	Version
-----	-----	-----	-----	-----
* alerting-backend r4123 linux-x64	Default can be updated to v3.5	:Backends	Alerting-Backend	v3.1u2
* alerting-frontend r4123 linux-x64	alerting-frontend can be updated to v3.5	:Web-Applications	Alerting-Frontend	v3.1u2

Module update order for multiple hosts

Update modules in a specific order to avoid issues involving software dependencies and redundant files. Modules that are available for update are marked with a yellow star icon in Centralized Management. If a Module-Manager update is available, always update this module first. Refer to the release notes or the workflow for your deployment scenario for additional recommendations.

Depending on your installed SolutionPacks, the list of modules needing to be updated will vary. When updating modules in a multiple host deployment, follow these recommendations:

- ◆ Update a subset of core modules (Group A) on the Centralized Management server first using the CLI command, `manage-modules.sh update` or `manage-modules.cmd update`.
- ◆ After updating the last core module in Group A, update the services and then start the services.
- ◆ After retrieving modules from the remote host servers, launch the update of a second subset of modules (Group B) from **Centralized Management > Logical Overview**. A few modules require an additional manual CLI update step on the remote host servers.
- ◆ Update Independent SolutionPackBlocks.
- ◆ Update SolutionPackBlocks.

Note

Do not update any other modules, even if they display in **Centralized Management > Logical Overview** with the yellow star update icon.

Table 4 Group A: Core modules for CLI update

Update these core modules using CLI commands.
module-manager
java
license-manager
mysql (optional, but recommended)
jdbc-drivers
tomcat
WebApps, includes one or more of these modules if marked for update: • alerting-frontend • centralized-management • device-discovery • frontend • frontend-ws • mib-browser • ip-sla-probes • transaction-collector-gui
webapps-resources
webservice-gateway

Table 5 Group B: Launch the update from Centralized Management › Logical Overview

Core module update order	Node in Logical Overview	Notes
module-manager	Miscellaneous	Launch from Logical Overview to send the module update to the remote host server. You must also issue the CLI command, <code>(manage-modules.sh update module-manager or manage-modules.cmd update module-manager)</code> on the remote host to apply the update.
java	Miscellaneous	Launch from Logical Overview to send the module update to the remote host server. You must also issue the CLI command, <code>(manage-modules.sh update java or manage-modules.cmd update java)</code> on the remote host to apply the update. Ensure all services are restarted after updating java. <code>(manage-modules.sh service start all or manage-modules.cmd service start all</code>
license-manager	Miscellaneous	
mysql	Databases	
jdbc-drivers	Databases	
tomcat	Miscellaneous	The update stops the service. If the display indicates the service failed to stop, retry the update.
alerting-frontend	Frontends	
centralized-management	Frontends	
device-discovery	Frontends	
frontend	Frontends	
frontend-ws	Frontends	
mib-browser	Frontends	
ip-sla-probes	Frontends	
transaction-collector-gui	Frontends	
webapps-resources	Miscellaneous	
webservice-gateway	Miscellaneous	Launch from Logical Overview to send the module update to the remote host server. You must also issue the CLI command, <code>(manage-modules.sh update webservice-gateway or manage-modules.cmd update</code>

Table 5 Group B: Launch the update from Centralized Management › Logical Overview (continued)

Core module update order	Node in Logical Overview	Notes
		webservice-gateway) on the remote host to apply the update.
alerting-backend	Backends	
apg-backend	Backends	
apg-property-store	Databases	
administration-tool	Miscellaneous	
diagnostic-tools	Miscellaneous	
frontend-report-generator	Miscellaneous	
frontend-search	Miscellaneous	
task-scheduler	Miscellaneous	
topology-cli	Miscellaneous	

When updating multiple modules, update first by Category and then by Module Name.

The Frontend and SNMP module families are not used in all deployments.

Since modules belonging to the Frontend family have logical interdependencies, the modules must be updated to the same version or problems may occur.

Modules belonging to the SNMP family also have logical interdependencies and must be updated to the same version.

You can view the Category and Module Name values by using the `manage-modules.sh list installed` command or by viewing the nodes in **Centralized Management › Logical Overview**.

Updating modules

Run the `manage-modules.sh update <identifier>` command to update the modules and their managers. Some modules may request information from you during an update. For example, you may be prompted for a module instance name if there are multiple instances, whether you want to continue the update, and whether you want to keep the original copy of a file that is updated.

Before you begin

- ◆ Obtain the identifier by using the `manage-modules.sh list installed` command.
- ◆ Make sure you have a login with root or system administrator privileges to update modules.

Update the manager of the module first before updating the module. Use the same command and substitute the appropriate identifier.

Procedure

1. Type the command for your operating system from the core software installation directory:

Operating system	Command
UNIX	<code><INSTALL_DIR>/bin/manage-modules.sh update <module_identifier> [<module_instance>]</code>
Windows	<code><INSTALL_DIR>\bin\manage-modules.cmd update <module_identifier> [<module_instance>]</code>

2. Answer any questions.

Recommendations for answering module update questions

During the module update process, there will be questions asked about saving, deleting, or overwriting existing files.

Usually, you should answer no ([n]o) when asked to delete files. You can then compare the old and new files later if there is a problem with the update. However there are exceptions to this recommendation.

centralized-managment module

When updating an older version of the centralized-management module to version 2.2 or higher, you may delete `conf/servers.xml` when prompted during the update process.

```
Starting update of centralized-management centralized-management from
v2.1u2 to v2.2...
* Gathering information...
* Module found in '/opt/APG/Web-Applications/Centralized-Management/
centralized-management'.
* It will now be updated using 'centralized-management-2.2-linux-
x64.pkg'.
* Undeploying web application '/opt/APG/Web-Applications/Centralized-
Management/centralized-management/webapp/mgmt.war' from Tomcat-
Default...
* Unpacking files...
* Configuration file 'conf/servers.xml', which has not changed since
its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Updating files... 100%
* 81 files have been updated.
* Finalizing update...
* Deploying web application '/opt/APG/Web-Applications/Centralized-
Management/centralized-management/webapp/mgmt.war' on Tomcat-
Default...
? Task file online-update-check.task added by module centralized-
management centralized-management. Enable it? [y]es, [n]o, [A]ll,
[N]one > y
```

webapps-resources

You may delete the property-mapping values when updating to webapps-resources version 1.3 or higher.

```
Starting update of webapps-resources Default from v1.2u1 to v1.3...
* Gathering information...
* Module found in '/opt/APG/Custom/WebApps-Resources/Default'.
* It will now be updated using 'webapps-resources-1.3-linux-x64.pkg'.
* Unpacking files...
* Configuration file 'property-mapping/FLOW-TF-SRCADDR.xml', which
has not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-DATA.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-PROTO.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-DSTADDR.xml', which
```

```

has not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-APPLI.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Updating files... 100%
* 530 files have been updated.
* Finalizing update...

```

frontend-report-generator

When prompted to replace the v6.2u3 version with the v6.3 version of the `daily_health_report`, enter `[y]es`. When prompted to keep the old version as a backup, enter `[y]es`.

```

The task file scheduled-reports/user1/daily_health_report.task is
already installed in the task scheduler but with different content.
Replace the current task which is enabled by the updated one? [y]es
[n]o [A]ll [N]one > y

```

manage-modules.sh update command

Use the `manage-modules.sh update` command to update modules and their managers. Type the command for your operating system from the `bin` directory of your core software installation directory.

Description

The `manage-modules.sh update` command updates installed modules and their managers. For UNIX, specify `manage-modules.sh update`. For Windows, specify `manage-modules.cmd update`.

Update the manager of the module first before updating the module.

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

Syntax

```

manage-modules.sh update <module_identifier>
[ <module_instance> ]

```

Options

module_identifier

The identifier value of the installed module or manager.

module_instance

The unique name of the module or manager. 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 update or the command will prompt you for the instance name.

The identifier and instance values form a unique key to refer to the module or manager.

In this Linux example, the following commands update the manager, Collector-Manager, and a corresponding module, XML-Collector.

```

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

```

In this Windows example, the following commands update the Tomcat Web server and a corresponding module, MIB-Browser.

```
<INSTALL_DIR>\bin\manage-modules.cmd update tomcat
<INSTALL_DIR>\bin\manage-modules.cmd update mib-browser
```

In this Linux example, the following commands update specific instances.

```
./manage-modules.sh update tomcat instance3
./manage-modules.sh update mib-browser mymib_browser2
```

Updating all core software services from the command line

After migrating core software, you must update all required services.

Before you begin

- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the core software application uses instead of root.

Procedure

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

Operating system	Command
UNIX	<code>./manage-modules.sh service update all</code>
Windows	<code>manage-modules.cmd service update all</code>

Results

A list of services appears. For example:

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

Starting the core software services from the command line

After installing core software, you must start all required services.

Before you begin

- ◆ Before starting core software services, ensure the library search path is correct on the server hosting core software. This requirement applies to the libaio package on Linux.
- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the core software application uses instead of root.

Procedure

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

Operating system	Command
UNIX	<code>./manage-modules.sh service start all</code>
Windows	<code>manage-modules.cmd service start all</code>

Results

A list of services appears. For 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 ]
```

Logging in to Centralized Management

Log in to Centralized Management to perform operations affect all servers.

Procedure

1. Point your browser to the URL.

For example, `http://<Frontend-hostname>:58080/centralized-management`

2. Log in.

- a. Type the login credentials.

The default username is **admin** and the default password is **changeme**.

- b. Click **Sign In**.

After you finish**Note**

You are automatically logged off after four hours.

Confirming settings for the first time

After you first log in with administrator credentials for core software, you must confirm the configuration settings for the server.

Procedure

- ◆ Click **Save** to accept the predefined values for the server.

Fields that are blank must remain blank.

Retrieving the list of modules from remote host servers using Centralized Management

If you have remote servers in a distributed environment, during migration, you need to copy the list of modules in use on remote host servers into the Centralized Management server.

Before you begin

- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the core software application uses instead of root.
- ◆ Make sure the Centralized Management server has remote access to the remote servers and that their webservice-gateway service is running.

Procedure

1. Navigate to **Centralized Management > Packages Management**.
2. In **Packages Listing**, select **Synchronization**.
3. Select the checkbox for **Retrieve the latest packages from the remote servers** and click **OK**.

Updating modules from Centralized Management

Use Centralized Management as one of the methods to update a module.

Before you begin

- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the core software application uses instead of root.
- ◆ Check the required update order for your scenario.

Procedure

1. Navigate to **Centralized Management**.
2. Select **Logical Overview**.
In the pane, notice that the nodes are listed in the **Logical Group** column.
3. Scroll through the pane in the required update order for your scenario to locate nodes with modules that are marked with the yellow star icon.
4. Update each module marked with the yellow star icon.
 - a. Click the **yellow star icon**.
 - b. Click **Update to Latest Version**.
 - c. Click **Update**.
If you are prompted for information, press **Enter** to select the default value or type another value appropriate for your deployment.
 - d. Close the window when the update process is finished.
 - e. Repeat for each module marked with the yellow star icon.
After each module is updated, the yellow star icon disappears.

Recommendations for answering module update questions

During the module update process, there will be questions asked about saving, deleting, or overwriting existing files.

Usually, you should answer no ([n]o) when asked to delete files. You can then compare the old and new files later if there is a problem with the update. However there are exceptions to this recommendation.

centralized-managment module

When updating an older version of the centralized-management module to version 2.2 or higher, you may delete `conf/servers.xml` when prompted during the update process.

```
Starting update of centralized-management centralized-management from
v2.1u2 to v2.2...
* Gathering information...
* Module found in '/opt/APG/Web-Applications/Centralized-Management/
centralized-management'.
* It will now be updated using 'centralized-management-2.2-linux-
x64.pkg'.
* Undeploying web application '/opt/APG/Web-Applications/Centralized-
Management/centralized-management/webapp/mgmt.war' from Tomcat-
Default...
* Unpacking files...
* Configuration file 'conf/servers.xml', which has not changed since
its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Updating files... 100%
* 81 files have been updated.
* Finalizing update...
* Deploying web application '/opt/APG/Web-Applications/Centralized-
Management/centralized-management/webapp/mgmt.war' on Tomcat-
Default...
? Task file online-update-check.task added by module centralized-
management centralized-management. Enable it? [y]es, [n]o, [A]ll,
[N]one > y
```

webapps-resources

You may delete the property-mapping values when updating to webapps-resources version 1.3 or higher.

```
Starting update of webapps-resources Default from v1.2u1 to v1.3...
* Gathering information...
* Module found in '/opt/APG/Custom/WebApps-Resources/Default'.
* It will now be updated using 'webapps-resources-1.3-linux-x64.pkg'.
* Unpacking files...
* Configuration file 'property-mapping/FLOW-TF-SRCADDR.xml', which
has not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-DATA.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-PROTO.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-DSTADDR.xml', which
has not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-APPLI.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Updating files... 100%
* 530 files have been updated.
* Finalizing update...
```

frontend-report-generator

When prompted to replace the v6.2u3 version with the v6.3 version of the `daily_health_report`, enter [y]es. When prompted to keep the old version as a backup, enter [y]es.

```
The task file scheduled-reports/user1/daily_health_report.task is
already installed in the task scheduler but with different content.
Replace the current task which is enabled by the updated one? [y]es
[n]o [A]ll [N]one > y
```

Installing the generic-rsc package

Manually install the `generic-rsc` package when migrating from 6.2.x to the 6.3.x core software release.

Procedure

1. Navigate to **Centralized Management**.
2. Expand **Physical Overview** and select the server where the collector host is installed.
3. Select the **SolutionPacks and Modules** tab.
4. Click **Install** to access **Packages Installation**.
5. Select the **Block** category and select the **generic-rsc** package.
6. Click **Launch** to access the **Installation Steps** window.
7. Accept the default values and click **Install** for each component:
 - Topology-Mapping-Service
 - Collector-Manager
 - FailOver-Filter
 - Inline-Calculation-Filter
 - Variable-Handling-Filter
 - Property-Tagging-Filter
 - Remote-Shell-Collector
 - generic-rsc

If you are prompted for information, press **Enter** to select the default value or type another value appropriate for your deployment.

The component status turns green.

8. Click **Back** to return to **Packages Installation** to continue installing more packages or close the **Installation Steps** window.

Installing the generic-topology package

Manually install the `generic-topology` package when migrating from 6.2.x to the 6.3.x core software release.

Procedure

1. Navigate to **Centralized Management**.
2. Expand **Physical Overview** and select the server where the Backend modules are installed.
3. Select the **SolutionPacks and Modules** tab.

4. Click **Install** to access **Packages Installation**.
5. Select the **Block** category and select the **generic-topology** package.
6. Click **Launch** to access the **Installation Steps** window.
7. Accept the default values and click **Install** for each component:
 - Topology-Service
 - generic-topology

If you are prompted for information, press **Enter** to select the default value or type another value appropriate for your deployment.

The component status turns green.
8. Click **Back** to return to **Packages Installation** to continue installing more packages or close the **Installation Steps** window.

Installing the Maps-Service package

Manually install the `Maps-Service` package when migrating from 6.2.x to the 6.3.x core software release.

Procedure

1. Navigate to **Centralized Management**.
2. Expand **Physical Overview** and select the server where the Frontend modules are installed.
3. Select the **SolutionPacks and Modules** tab.
4. Click **Install** to access **Packages Installation**.
5. Select the **Tools** category and select the **Maps-Service** package.
6. Click **Launch** to access the **Installation Steps** window.
7. Accept the default values and click **Install**.

If you are prompted for information, press **Enter** to select the default value or type another value appropriate for your deployment.

The component status turns green.
8. Click **Back** to return to **Packages Installation** to continue installing more packages or close the **Installation Steps** window.

Updating the SolutionPackBlocks

After installing a software update or migrating from an older release, you must update SolutionPackBlocks in order to use the latest module configurations and report templates. This block update may trigger the update of an associated module.

Before you begin

- ◆ Be sure you have updated core modules (except for blocks, collectors, and event processors) in all of the servers before you update SolutionPackBlocks.

Procedure

1. Click the **SolutionPacks** node on the left panel to access **Installed SolutionPacks**.

Two panes appear: Independent SolutionPackBlocks and SolutionPacks. Update the Independent SolutionPackBlocks first before you update the SolutionPackBlocks that belong to the SolutionPacks.

- Do the following to locate the block that you want to update:

In the pane for	Perform:
Independent SolutionPackBlocks	Locate the block.
SolutionPacks	- Select the specific SolutionPack. - Locate the block in the Properties page.

- Click the **yellow star icon**.

The **SolutionPack Update** page appears.

- Carefully review the settings on this page and make changes as needed.

Most values are from the existing SolutionPack but some may be default values for the new SolutionPack.

- Click **Update**.

The update process begins. The **SolutionPack Update** page provides information on the progress of the update.

- Select the maximize arrow next to view the update progress.

When the update successfully completes, a green checkmark appears above this information.

Controlling services from Centralized Management

You can start, stop, or restart services from the Centralized Management.

Before you begin

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

Procedure

- Log in and select **Administration > Centralized Management**.
- Select the server in **Physical Overview**.
- In the **Services** tab, select the module.
- Click one of the following buttons.

Operation	Description
Start	Starts the service.
Stop	Stops the service.
Restart	Restarts the service.

Read the status message.

Default ReportPack migration

Update the Default ReportPack to ensure you use the latest SolutionPack template.

Update the Default ReportPack from the Administration menu after logging in to the User Interface URL, for example, `http://<Frontend-hostname>:58080/APG`

The Default ReportPack contains the default reports. To access all of the new report features available in a software release, update the Default ReportPack during the migration process.

1. Back up the existing Default ReportPack by exporting the `.arp` file.
2. Upload the Default ReportPack.
3. Delete the old ReportPack.

Note

Scheduled reports, pre-generated reports and template restrictions are lost when you delete the old Default ReportPack. The online help describes methods for exporting ReportPack templates so you can save them.

Exporting a ReportPack

You can export a ReportPack to back up the `<ReportPack>.arp` file or for use in another system.

Procedure

1. Click **Administration**.
2. Under **ReportPacks**, click **List / Import ReportPacks**.
3. Select the ReportPack.
4. Click **Export** to download the `<ReportPack>.arp` file that contains the required information and templates.
5. Click **Save** to navigate to the download location.

Updating the Default ReportPack

Update your existing Default ReportPack by replacing it completely with a new Default ReportPack.

Before you begin

- ◆ Ensure you have a login with root, APG, or system administrator privileges to perform this task. The user `apg` is the account that the core software application uses instead of root.
- ◆ Locate the new `Default ReportPack.arp` file. The file is located on the server in `<INSTALL_DIR>/Web-Servers/Tomcat/Default/webapps/APG`. If you are accessing the server remotely, you will need to download the `.arp` file to your local directory first.

Procedure

1. Log in and select **Administration > ReportPacks** to access **ReportPacks Management**.
Available ReportPacks are listed in a pane.
2. Rename the existing Default ReportPack to distinguish between the existing one and the new one.
 - a. Select **Default ReportPack** in the pane.
 - b. Type **(original 6.2)** in the **Name** field.
The **Name** field value reads: Default ReportPack (original 6.2)
 - c. Click **Save**.

You are returned to **ReportPacks Management**.

3. Click **Upload a ReportPack**.
4. Select the `Default ReportPack.arp` file from your local directory.
5. Click **Save**.

After you finish

If you are satisfied with the resulting reports, you can delete the old Default ReportPack.

Note

Scheduled reports, pre-generated reports and template restrictions will be lost if you remove it.

Deleting a ReportPack

When a ReportPack is no longer needed, you can remove it and its report templates.

Procedure

1. Click **Administration**.
2. Under **ReportPacks**, click **List / Import ReportPacks**.
3. Select the ReportPack.
4. Click **Delete** to remove the ReportPack and its templates.
5. Click **Ok** at the warning message.

Installing a SolutionPack

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

Before you begin

- ◆ Core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Core modules are modules that are not installed by a SolutionPack. Examples of core modules include webapps, module-manager, license-manager, java, mysql, backend, tools, and so forth. Update these core modules: **Databases, Backends, Frontends, Miscellaneous** (except Blocks). Since the recommended module update order varies, refer to the Module Update Order section for the multiple hosts or single host deployments. Also, the *EMC Watch4net Centralized Management Guide* provides more information.

Procedure

1. Log in and select **Administration**.
2. Select **Centralized Management** in the Administration tree.
3. Select **SolutionPacks** in the tree.
4. Select **SolutionPack Center**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. 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, Reports, and Events** list boxes.
 - c. Click **Next**.
8. 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.
9. Select the maximize arrow next to each component to view the installation process.

When the installation successfully completes, green checkmarks appear.
10. After installation is complete, select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

After you finish

Install the SolutionPack for EMC Watch4net Health if you have not already done so. This is available from **Centralized Management** > **SolutionPack Center**.

Post-migration tasks

You must manually install and configure components which support storage compliance and alert consolidation.

Post-migration tasks include:

- ◆ [Installing SolutionPack for Storage Compliance on page 115](#)
- ◆ [Creating and configuring storage compliance schema on page 117](#)
- ◆ [Configuring alert consolidation features in a migration scenario on page 118](#)

Installing SolutionPack for Storage Compliance

To enable storage compliance features, you must install SolutionPack for Storage Compliance.

Before you begin

You must have obtained the license for storage compliance, if you are migrating to a higher version of the Suite.

Procedure

1. Log in to the host using **Putty**.
2. Change the directory path to `/opt/APG/bin/`.
3. Type the `./manage-modules.sh install compliance-frontend-1.0-linux-x64.pkg` command to update the Frontend.
4. Start the `tomcat` service.
5. Log in to the core softwareUI and select **Administration**.
6. If you are migrating from a lower to a higher version of the suite, then upload the storage compliance license file.

If it is a fresh installation there is no need to upload the license file separately. It is taken care of by default.

7. Select **Centralized Management** in the **Administration** tree.
8. Select **SolutionPacks** in the tree.
9. Select **SolutionPack Center**.
10. Select the SolutionPack for Storage Compliance in the **Browse and Install SolutionPacks** screen.
11. Read the summary information and click **Install**.
12. Select the components to install.
 - a. Type the instance name.
 - b. For Compliance Notifications, Backend, and Reports, select the appropriate VMs. For example, Frontend VM, Primary Backend VM, or Collector VM for each of the modules to be installed.
 - c. Click **Next**.
13. 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.
14. Select the maximize arrow next to each component to view the installation process.

Note

Review the information in install screen and make changes as necessary. It is preferable to preserve the default settings. Answer the questions during installation. The recommended answer when a delete question asked is to say no, by typing **n**.

When the installation successfully completes, a green checkmark appears.

15. Change the directory path to `/opt/APG/Web-Servers/Tomcat/Default/conf/Catalina/localhost/` and edit the `compliance-frontend.xml` file to make changes to `localhost` and replace it with the name of the primary backend VM (same location where compliance backend is installed) in the following three entries:
 - ```
<Resource name="manager/ComplianceManager" auth="Container"
 type="com.emc.srm.base.compliance.jmx.ComplianceManagerFactory"
 factory="org.apache.naming.factory.BeanFactory"
 user="admin" pass="changeme"
 url="service:jmx:rmi:///jndi/rmi://localhost:52755/jmxrmi" />
```
  - ```
<Resource name="manager/ComplianceESMManager" auth="Container"
  type="com.emc.srm.base.compliance.jmx.ComplianceManagerFactory"
  factory="org.apache.naming.factory.BeanFactory"
    user="admin" pass="changeme"
  url="service:jmx:rmi:///jndi/rmi://localhost:52755/jmxrmi" />
```
 - ```
<Resource name="manager/CompliancePolicyTemplateManager"
 auth="Container"
 type="com.emc.srm.base.compliance.jmx.ComplianceManagerFactory"
 factory="org.apache.naming.factory.BeanFactory"
 user="admin" pass="changeme"
 url="service:jmx:rmi:///jndi/rmi://localhost:52755/jmxrmi" />
```

16. If you have installed multiple databases, you have to edit the `compliance-frontend.xml` file located in the `/opt/APG/Web-Servers/Tomcat/Default/conf/Catalina/localhost/` directory to connect all the databases.
17. Restart tomcat service.
18. After installation is complete, select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.  
Proceed to [creating and configuring compliance schema on page 117](#).

## Creating and configuring storage compliance schema

After installing SolutionPack for Storage Compliance, the storage compliance schema must be created and configured to work with the appliance.

### Before you begin

You must have installed the SolutionPack for Storage Compliance as described in the [installing SolutionPack for Storage Compliance on page 115](#) procedure.

You must create the database instance for compliance and configure the front host to work with the compliance schema.

### Procedure

1. **Note**  
Use Putty for Unix and Remote Desktop or an equivalent software for Windows.  
Log in to appliance using **Putty** or an equivalent software.
2. Change the directory path to point to `/opt/APG/Backend/Compliance-Backend` for Unix or `.. \APG\Backend\Compliance-Backend` for Windows.
3. Type and run the command `ls` for Unix or `dir` for Windows command to list the database instance name.
4. Note down the folder name listed.  
This is the default schema name.  
For example, `generic-compliance`.
5. Type and run the command `mysql-client.sh` to start the mysql client.
6. Specify these details when prompted:
  - username: root
  - database: apg
  - password: watch4net
 The `sql>` prompt appears.
7. Type and run the command `source /opt/APG/Backends/Compliance-Backend/<Instance Name>/ddl/compliance-schema.sql`. This command is applicable for both Unix and Windows.  
The `<instance name>` is the name of the folder noted in step#4.
8. Type and run the command `exit` for Unix and `quit` for Windows to exit the sql client and go back to the default prompt.
9. From the default prompt, change the directory path to point to `/opt/APG/bin/` for Unix or `.. \APG\bin\` for Windows.

10. Type and run the command `./manage-modules.sh service start compliance-backend <Instance Name>` command to start the compliance backend service.

The <instance name> is the name of the folder noted in step#4.

Proceed to configure the frontend to communicate with the compliance schema.

11. Edit the `/opt/APG/Web-Servers/Tomcat/Default/conf/Server.xml` file for Unix or `.. \APG\Web-Servers\Tomcat\Default\conf\Server.xml` file for Windows. Include this information with appropriate hostname url in the `url="jdbc:mysql:// path:`

```
<!--Defines the connections to the Flow Compliance Breach.-->
<Resource name="jdbc/FLOW-COMPLIANCE" auth="Container"
 type="javax.sql.DataSource" maxActive="10"
maxIdle="10"
 validationQuery="SELECT 1" testOnBorrow="false"
testWhileIdle="true"
 timeBetweenEvictionRunsMillis="10000"
validationQueryTimeout="5"
 minEvictableIdleTimeMillis="60000"
maxWait="10000" username="apg"
 password="watch4net"
driverClassName="com.mysql.jdbc.Driver"
 removeAbandoned="true"
removeAbandonedTimeout="60" logAbandoned="true"
 url="jdbc:mysql://<HOST_NAME_URL>:53306/
compliance?autoReconnect=true&tinyInt1isBit=false" />
```

12. Save and exit.

13. Edit the `/opt/APG/Web-Servers/Tomcat/Default/conf/Catalina/<localhost>/APG.xml` file for Unix or `.. \APG\Web-Servers\Tomcat\Default\conf\Catalina\localhost\APG.xml` file for Windows. Include this information with appropriate hostname url in the `url="jdbc:mysql:// path:`

```
<!--Defines the connections to the Compliance schema.-->
<ResourceLink name="jdbc/FLOW-COMPLIANCE-BREACH:
{ mapping=FLOW-COMPLIANCE-BREACH.xml,
 table=breach }" global="jdbc/FLOW-COMPLIANCE"
 type="javax.sql.DataSource" />
```

14. Save and exit.

15. Restart the tomcat server.

16. Log into the appliance to verify the Storage Compliance is installed and displayed in the UI.

## Configuring alert consolidation features in a migration scenario

Alert consolidation is a new core component that you must manually install and configure when migrating from SRM Suite 2.0.x to SRM Suite 3.0. You must perform some manual configuration in order to enable alert consolidation and update some existing SolutionPacks to use the feature.

Configuration includes:

- ◆ [Installing the alert consolidation package on page 119](#)
- ◆ [Updating existing SolutionPacks to use alert consolidation on page 119](#)
- ◆ [Enabling alert consolidation of email and trap notifications on page 120](#)

## Installing the alert consolidation package

Install the alert consolidation package, configure the `apg.xml` file and update the database schema to support the feature.

### Before you begin

This procedure requires that you obtain a table creation script to update the MySQL database to support alert consolidation. Contact EMC Customer Support to obtain the required script.

### Procedure

1. Log in to the host where the Alert Consolidation block is installed (typically the Primary Backend) using Putty.
2. Change the directory path to `/opt/APG/bin/`.
3. Type `manage-modules.sh install alert-consolidation-3.0.pkg` to update the Backend.
4. Edit the `/opt/APG/Web-Servers/Tomcat/Default/conf/Catalina/localhost/APG.xml` file for Unix or `.. \APG\Web-Servers\Tomcat\Default\conf\Catalina\localhost\APG.xml` file for Windows. Update the generic events schema section of the `apg.xml` file to include the line `mapping=FLOW-GENERIC-EVENT.xml`:  

```
<!-- Generic event schema -->
<ResourceLink name="jdbc/FLOW-EVENTS-GENERIC:{ mapping=FLOW-
GENERIC-EVENT.xml, table=genericevents_live }" global="jdbc/FLOW-
EVENTS" type="javax.sql.DataSource" />
```
5. Save the `apg.xml` file.
6. Restart the tomcat service.
7. Login into the Primary Backend host as root user.
8. Execute the mysql-client script: `./mysql-client.sh`
9. Provide the username, password and database. The default is root, watch4net, apg
10. At the `mysql` prompt, paste the table creation script provided by EMC Customer Support and press **Enter**.
11. Verify that Query OK, 0 rows affected, 1 warning displays when the script is completed indicating a successful result.

## Updating existing SolutionPacks to use alert consolidation

Update any applicable existing SolutionPacks to use alert consolidation.

### Before you begin

Ensure that you have installed and configured the Alert-Consolidation package.

If they are currently installed, update the following SolutionPacks to use the new alert consolidation feature. This will update missing blocks, events and pre-configured alerts.

### Procedure

1. Re-install the SolutionPack for EMC VMAX and restart the Alert-Consolidation service.
2. Re-install the SolutionPack for Brocade FC Switch and restart the Alert-Consolidation service.
3. Re-install the SolutionPack for Cisco MDS/Nexus and restart the Alert-Consolidation service.

4. Re-install the SolutionPack for EMC VNX and restart the Alert-Consolidation service.
5. Verify the alert components are installed and configured by logging in to the SRM Suite user interface and navigating to **Operations > Alerts**.

## Enabling alert consolidation of email and trap notifications

When migrating from SRM Suite 2.0.x to SRM Suite 3.0, you must update the `alerting.xml` configuration file to make email and traps available in the Alerting-Frontend application.

### Procedure

1. Navigate to the `alerting.xml` located in `/opt/APG/Backends/Alerting-Backend/Default/conf`.

2. Add the following adapter under the adapter list entries:

```
<adapter-list enabled="true" name="Alert Consolidation Adapter">
 <class>com.watch4net.alerting.adapter.EventAdapter</class>
 <param-list name="value-field"></param-list>
 <param-list name="properties-field">id,name,openedat,count,eventstate,source,parttype,part,event
name,parttypedisplayname,partdisplayname,eventdisplayname,fullmsg,d
evtype,device,sourceip,sourcedomainname,sourceeventtype,value,activ
e,timestamp,closedat,duration,lastchangedat,isroot,isproblem,acknow
ledged,eventtype,category,eventtext,severity,impact,certainty,inmai
ntenance,troubleticketid,owner,systemdefined1,systemdefined2,system
defined3,systemdefined4,systemdefined5,userdefined1,userdefined2,us
erdefined3,userdefined4,userdefined5,userdefined6,userdefined7,user
defined8,userdefined9,userdefined10,userdefined11,userdefined12,use
rdefined13,userdefined14,userdefined15,userdefined16,userdefined17,
userdefined18,userdefined19,userdefined20,enterprise,generic</
param-list>
 <param-list name="timestamps-field"></param-list>
 <param-list name="port">2012</param-list>
</adapter-list>
```

3. Add trap and email definitions under the definition list entries:

```
<definition-list enabled="false" name="Alert Consolidation Trap
Notification">
 <description>Alert notification definition for sending
SNMP traps</description>
 <entry-point-list>1385100547216</entry-point-list>
</definition-list>

 <definition-list enabled="true" name="Alert Consolidation
Email Notification">
 <description>Alert notification definition for sending
emails</description>
 <entry-point-list>85854716679323</entry-point-list>
</definition-list>
```

4. Add trap and email entry points under the entry point list entries:

```
<entry-point-list id="1385100547216">
 <name>Trap notification severity check</name>

 <class>com.watch4net.alerting.operation.FilteredEntryPoint</class>
 <filter>adapterName=='Alert Consolidation Adapter' &
(severity=='1' | severity=='2' | severity=='3' | severity=='4')</
filter>
 <description>Trap notification entry point</description>
 <action-list to="entry" from="output">1385101374510</
action-list>
</entry-point-list>

<entry-point-list id="85854716679323">
 <name>Email notification severity check</name>
```

```
<class>com.watch4net.alerting.operation.FilteredEntryPoint</class>
 <filter>adapterName=='Alert Consolidation Adapter' &
(severity=='1' | severity=='2' | severity=='3')</filter>
 <description>Email notification entry point</description>
 <action-list to="entry" from="output">1385101505613</
action-list>
</entry-point-list>
```

5. Add trap and email actions under the action list entries:

```
<action-list id="1385101374510">
 <name>Alert consolidation notification trap</name>
 <class>com.watch4net.alerting.action.SNMPTrapAction</class>
 <description>Send trap for alert consolidation</
description>
 <param-list name="port">162</param-list>
 <param-list name="community">public</param-list>
 <param-list name="generic">6</param-list>
 <param-list name="specific">1</param-list>
 <param-list name="trap-
content">PROP.'fullmsg',PROP.'device',PROP.'devtype',PROP.'severity
',PROP.'source',PROP.'sourceip',PROP.'parttype',PROP.'part',PROP.'c
ategory'</param-list>
</action-list>

<action-list id="1385101505613">
 <name>Alert consolidation notification email</name>
 <class>com.watch4net.alerting.action.MailAction</class>
 <description>Send email for alert consolidation</
description>
 <param-list name="subject">Sev-PROP.'severity'
PROP.'category' alert received for PROP.'devtype'-PROP.'device'</
param-list>
 <param-list name="message">An alert has been received with
the following attributes:

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

This is an auto-generated email. To change the notification
settings, consult the site administrator.</param-list>
</action-list>
```

6. Save the alerting.xml file.

7. Navigate to /opt/apg/bin.

8. Type **manage-modules.sh service restart alerting-backend Default**.

9. Verify the feature configuration:

- a. Log in to the Alerting user interface.
- b. Select **Local Manager > Alert Definitions**.
- c. Expand **Alert Definitions**.
- d. Verify that the **Alert Consolidation Email Notification** and **Alert Consolidation Trap Notification** nodes are included.

## 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 8

## Migration for Single Host

This chapter includes the following topics:

◆ Migration workflow.....	124
◆ Migrating core software on a UNIX server.....	126
◆ Migrating core software on a Windows server.....	126
◆ Identifying which modules to update.....	127
◆ Module update order for single hosts.....	128
◆ Updating modules .....	129
◆ Updating all core software services from the command line.....	131
◆ Starting the core software services from the command line.....	132
◆ Logging in to Centralized Management.....	132
◆ Confirming settings for the first time.....	133
◆ Updating modules from Centralized Management.....	133
◆ Installing the generic-rsc package.....	135
◆ Installing the generic-topology package.....	135
◆ Installing the Maps-Service package.....	136
◆ Updating the SolutionPackBlocks.....	136
◆ Controlling services from Centralized Management.....	137
◆ Default ReportPack migration.....	137
◆ Reviewing reports.....	139

## Migration workflow

If you have existing core software installed, you need to migrate to the latest software version.

Depending on your existing core software version, do one of the following procedures.

If you have:	Perform:
Legacy core software such as version 6.1 or 6.1ux.	1. Migrate to version 6.2 as described in the <i>EMC Watch4net Migration Guide</i> available from EMC Online Support.          <b>Note</b>   You must migrate any older Watch4net releases to version 6.2.x before using the procedures in this guide to migrate to version 6.3. The Migration Guides for each release describe how to update from one version to the next.          2. Migrate from version 6.2 to version 6.3.
Core software version 6.2 or 6.2ux.	Migrate to version 6.3:       ◆ <a href="#">Migration for multiple hosts with installed SolutionPacks on page 96</a>     ◆ <a href="#">Migration for single host with installed SolutionPacks on page 124</a>

## Migration for single host with installed SolutionPacks

In this migration scenario, version 6.2.x software is already installed and you wish to migrate to version 6.3.x on the same host. Launch the setup script or executable to copy the latest version of modules into the existing APG module repository.

### Prerequisites

- ◆ Ensure the host server meets system requirements for version 6.3.x.
- ◆ Version 6.2.x must be installed and running before migrating to version 6.3.x.
- ◆ Version 6.3.x software installs with temporary licenses for each feature. Ensure you obtain permanent licenses for any SolutionPacks you plan to use for longer than 30 days.
- ◆ Ensure the host server has 2 GB free disk space.
- ◆ Ensure you have a login with root or system administrator privileges.
- ◆ Back up the existing installation before starting the migration tasks.
- ◆ Review this workflow before starting. The specific procedures mentioned in the workflow follow this topic in the chapter.

### Workflow

You will use CLI commands to migrate specific core modules on the server designated for Centralized Management. Then log into Centralized Management and update remaining modules from the Logical Overview and SolutionPack nodes. It is very important to follow the recommended order of module updates.

1. Log in to the host server with root or administrator credentials and run the setup script or executable to copy the new module packages into the existing APG directory

path. For example, `productname-setup-linux-x86_64-v63.sh` or `productname-setup-win64-v63.exe`.

2. Issue the `manage-modules list installed` command to determine which modules require updating. The Status column identifies modules available for update.
3. Review the order in which modules must be updated. [Module update order for single hosts on page 128](#)
4. Use the `manage-modules update <module name>` CLI command to update a subset of core modules before logging in to Centralized Management.
5. Update services.
6. Start services.
7. Log in to Centralized Management.
8. If you updated the server, you may be prompted to confirm the server settings.
9. Update a second subset of core modules from Centralized Management. Ensure you follow the recommended update order and restart any services that are stopped by the update process.
10. Install new package files to enable topology features.
11. Update Independent SolutionPacks followed by SolutionPacks.

---

#### Note

After this step, there will still be a small number of modules that are marked as available for update with the yellow star icon. Do not update these modules.

---

12. Ensure that all services stopped during the update process have restarted.
13. Update the default ReportPack to ensure the latest SolutionPack template is in use.
14. Install new SolutionPacks to add new features available in version 6.3.

---

#### Note

Some SolutionPacks require additional steps such as creation of database schemas or updates to the `APG.xml` file. Check the SolutionPack documentation for details.

---

15. Review reports.

#### Conventions for defaults

During the migration, the multiple choice questions show the default answer with an uppercase letter (for example, **Y/n** means Yes is the default answer). Press **Enter** to accept the default. If you enter **A** for All, the all actions will be performed. If you enter **N** for None, none of the actions will be performed.

Default directory paths are:

Operating system	Default installation directory
UNIX	/opt/APG/
Windows	C:\Program Files\APG\

Operating system	Default module repository directory
UNIX	<INSTALL_DIR>/Tools/Module-Repository

Operating system	Default module repository directory
Windows	<INSTALL_DIR>\Tools\Module-Repository

#### Note

Install the 6.3.x software into the directory where 6.2.x software is installed. If you do not specify the same directory, the setup script or executable may overwrite the services configurations because the setup script or executable does not detect the existing 6.2.x installation.

## Migrating core software on a UNIX server

Perform this procedure on a single host where version 6.2.x software is already installed. Typically, the host has core software with installed SolutionPacks. During the procedure, you must assign executable permissions to the setup script.

#### Before you begin

- ◆ Make sure you have a login with root privileges to run the setup script.
- ◆ Download the installation package to a directory on the server, such as /temp.

#### Procedure

1. Locate the installation package.
2. Change the permissions of the setup script so you can run it.  
For example, for the Linux 64-bit executable, type:  

```
chmod +x productname-setup-linux-x86_64-v63.sh
```
3. Run the setup script from the directory.  
For example:  

```
./productname-setup-linux-x86_64-v63.sh
```
4. Read and accept the End User License Agreement. Use the **space bar** to scroll through the agreement. Press **y** and **Enter** to accept it.
5. Press **Enter** to accept the default installation directory of /opt/APG.  
Or, if your existing core software resides in another location, specify the other location and press **Enter**.
6. Press **y** and **Enter** to install the new packages in the /opt/APG/Tools/Module-Repository directory.

#### After you finish

Identify which modules to update.

## Migrating core software on a Windows server

Perform this procedure on a single host where version 6.2.x software is already installed. Typically, the host has core software with installed SolutionPacks. During the procedure, you must assign executable permissions to the setup executable.

#### Before you begin

- ◆ Make sure you have a login with system administrator privileges to run the setup executable.

- ◆ Download the installation package to a folder on the server, such as `\temp`.

### Procedure

1. Locate the installation package.
2. Double-click the setup executable.  
For example: `productname-setup-win64-v63.exe`
3. Click **Next** in the **Welcome** screen.
4. Read and accept the End User License Agreement. Click **I Agree**.
5. Press **Enter** to accept the default installation directory of `C:\Program Files\APG`.  
Or, if your existing core software resides in another location, specify the other location and press **OK**.
6. Press **OK** to install the new packages in the `C:\Program Files\APG\Tools\Module-Repository` directory.

### After you finish

Identify which modules to update.

## Identifying which modules to update

After you update a core software installation, run the `manage-modules.sh list installed` command to view the installed modules and to determine which modules to update. Update the modules with the status of `can be updated`.

### Procedure

- ◆ Type the command for your operating system from the core software installation directory:

Operating system	Command
<b>UNIX</b>	<code>&lt;INSTALL_DIR&gt;/bin/manage-modules.sh list installed</code>
<b>Windows</b>	<code>&lt;INSTALL_DIR&gt;\bin\manage-modules.cmd list installed</code>

When you view the output, record the identifier value of each module that needs to be updated. You will need to specify the identifier later when you update the module.

This sample output indicates to update the Module-Manager first, then to update the Alerting-Backend and the Alerting-Frontend modules to version 3.5. For other lines, pay attention to the status recommendations.

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

Identifier Revision OS-Arch	Instance Status	:Category	Module Name	Version
-----	-----	-----	-----	-----
* alerting-backend	Default	:Backends	Alerting-Backend	v3.1u2
r4123 linux-x64	can be updated to	v3.5		
* alerting-frontend	alerting-frontend	:Web-Applications	Alerting-Frontend	v3.1u2

r4123      linux-x64    can be updated to v3.5

## Module update order for single hosts

Update modules in a specific order to avoid issues involving software dependencies and redundant files. Modules that are available for update are marked with a yellow star icon in Centralized Management. If a Module-Manager update is available, always update this module first. Refer to the release notes or the workflow for your deployment scenario for additional recommendations.

Depending on your installed SolutionPacks, the list of modules needing to be updated will vary. When updating modules in a single host deployment, follow these guidelines:

- ◆ Update a subset of core modules (Group A) using the CLI command, `manage-modules.sh update` or `manage-modules.cmd update`.
- ◆ After updating the last core module in Group A, update the services and then start the services.
- ◆ Update a second subset of modules (Group B) after logging in to **Centralized Management** › **Logical Overview**.
- ◆ Update Independent SolutionPackBlocks.
- ◆ Update SolutionPackBlocks.

---

### Note

Do not update any other modules, even if they display in **Centralized Management** › **Logical Overview** with the yellow star update icon.

---

**Table 6** Group A: Core modules for CLI update

Update these core modules for a single host using CLI commands
module-manager
java
license-manager
mysql (optional, but recommended)
jdbc-drivers
tomcat
WebApps, includes one or more of these modules if marked for update:     • alerting-frontend    • centralized-management    • device-discovery    • frontend    • frontend-ws    • mib-browser    • ip-sla-probes    • transaction-collector-gui

**Table 6** Group A: Core modules for CLI update (continued)

Update these core modules for a single host using CLI commands
webapps-resources
webservice-gateway

**Table 7** Group B: Core modules to update from Centralized Management

Core module update order	Node in Logical Overview
alerting-backend	Backends
apg-backend	Backends
apg-property-store	Databases
administration-tool	Miscellaneous
diagnostic-tools	Miscellaneous
frontend-report-generator	Miscellaneous
frontend-search	Miscellaneous
task-scheduler	Miscellaneous
topology-cli	Miscellaneous

When updating modules, update first by Category and then by Module Name.

The Frontend and SNMP module families are not used in all deployments.

Since modules belonging to the Frontend family have logical interdependencies, the modules must be updated to the same version or problems may occur.

Modules belonging to the SNMP family also have logical interdependencies and must be updated to the same version.

View the Category and Module Name values by using the `manage-modules.sh list installed` command or by viewing the nodes in **Centralized Management > Logical Overview**.

## Updating modules

Run the `manage-modules.sh update <identifier>` command to update the modules and their managers. Some modules may request information from you during an update. For example, you may be prompted for a module instance name if there are multiple instances, whether you want to continue the update, and whether you want to keep the original copy of a file that is updated.

### Before you begin

- ◆ Obtain the identifier by using the `manage-modules.sh list installed` command.
- ◆ Make sure you have a login with root or system administrator privileges to update modules.

Update the manager of the module first before updating the module. Use the same command and substitute the appropriate identifier.

## Procedure

1. Type the command for your operating system from the core software installation directory:

Operating system	Command
<b>UNIX</b>	<code>&lt;INSTALL_DIR&gt;/bin/manage-modules.sh update &lt;module_identifier&gt; [&lt;module_instance&gt;]</code>
<b>Windows</b>	<code>&lt;INSTALL_DIR&gt;\bin\manage-modules.cmd update &lt;module_identifier&gt; [&lt;module_instance&gt;]</code>

2. Answer any questions.

## Recommendations for answering module update questions

During the module update process, there will be questions asked about saving, deleting, or overwriting existing files.

Usually, you should answer no ([n]o) when asked to delete files. You can then compare the old and new files later if there is a problem with the update. However there are exceptions to this recommendation.

### centralized-managment module

When updating an older version of the centralized-management module to version 2.2 or higher, you may delete `conf/servers.xml` when prompted during the update process.

```
Starting update of centralized-management centralized-management from
v2.1u2 to v2.2...
* Gathering information...
* Module found in '/opt/APG/Web-Applications/Centralized-Management/
centralized-management'.
* It will now be updated using 'centralized-management-2.2-linux-
x64.pkg'.
* Undeploying web application '/opt/APG/Web-Applications/Centralized-
Management/centralized-management/webapp/mgmt.war' from Tomcat-
Default...
* Unpacking files...
* Configuration file 'conf/servers.xml', which has not changed since
its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Updating files... 100%
* 81 files have been updated.
* Finalizing update...
* Deploying web application '/opt/APG/Web-Applications/Centralized-
Management/centralized-management/webapp/mgmt.war' on Tomcat-
Default...
? Task file online-update-check.task added by module centralized-
management centralized-management. Enable it? [y]es, [n]o, [A]ll,
[N]one > y
```

### webapps-resources

You may delete the property-mapping values when updating to webapps-resources version 1.3 or higher.

```
Starting update of webapps-resources Default from v1.2u1 to v1.3...
* Gathering information...
* Module found in '/opt/APG/Custom/WebApps-Resources/Default'.
* It will now be updated using 'webapps-resources-1.3-linux-x64.pkg'.
* Unpacking files...
* Configuration file 'property-mapping/FLOW-TF-SRCADDR.xml', which
has not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-DATA.xml', which has
not changed since its installation, is about to be removed.
```

```
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-PROTO.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-DSTADDR.xml', which
has not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-APPLI.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Updating files... 100%
* 530 files have been updated.
* Finalizing update...
```

### frontend-report-generator

When prompted to replace the v6.2u3 version with the v6.3 version of the `daily_health_report`, enter `[y]es`. When prompted to keep the old version as a backup, enter `[y]es`.

The task file `scheduled-reports/user1/daily_health_report.task` is already installed in the task scheduler but with different content. Replace the current task which is enabled by the updated one? `[y]es [n]o [A]ll [N]one > y`

## Updating all core software services from the command line

After migrating core software, you must update all required services.

### Before you begin

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

### Procedure

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

Operating system	Command
UNIX	<code>./manage-modules.sh service update all</code>
Windows	<code>manage-modules.cmd service update all</code>

### Results

A list of services appears. For example:

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

## Starting the core software services from the command line

After installing core software, you must start all required services.

### Before you begin

- ◆ Before starting core software services, ensure the library search path is correct on the server hosting core software. This requirement applies to the libaio package on Linux.
- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the core software application uses instead of root.

### Procedure

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

Operating system	Command
UNIX	<code>./manage-modules.sh service start all</code>
Windows	<code>manage-modules.cmd service start all</code>

### Results

A list of services appears. For 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]
```

## Logging in to Centralized Management

Log in to Centralized Management to perform operations affect all servers.

### Procedure

1. Point your browser to the URL.

For example, `http://<Frontend-hostname>:58080/centralized-management`

2. Log in.

- a. Type the login credentials.

The default username is **admin** and the default password is **changeme**.

- b. Click **Sign In**.

### After you finish

---

#### Note

You are automatically logged off after four hours.

---

## Confirming settings for the first time

After you first log in with administrator credentials for core software, you must confirm the configuration settings for the server.

### Procedure

- ◆ Click **Save** to accept the predefined values for the server.
- Fields that are blank must remain blank.

## Updating modules from Centralized Management

Use Centralized Management as one of the methods to update a module.

### Before you begin

- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the core software application uses instead of root.
- ◆ Check the required update order for your scenario.

### Procedure

1. Navigate to **Centralized Management**.
2. Select **Logical Overview**.

In the pane, notice that the nodes are listed in the **Logical Group** column.

3. Scroll through the pane in the required update order for your scenario to locate nodes with modules that are marked with the yellow star icon.
4. Update each module marked with the yellow star icon.
  - a. Click the **yellow star icon**.
  - b. Click **Update to Latest Version**.
  - c. Click **Update**.

If you are prompted for information, press **Enter** to select the default value or type another value appropriate for your deployment.

- d. Close the window when the update process is finished.
- e. Repeat for each module marked with the yellow star icon.

After each module is updated, the yellow star icon disappears.

## Recommendations for answering module update questions

During the module update process, there will be questions asked about saving, deleting, or overwriting existing files.

Usually, you should answer no ([n]o) when asked to delete files. You can then compare the old and new files later if there is a problem with the update. However there are exceptions to this recommendation.

**centralized-managment module**

When updating an older version of the centralized-management module to version 2.2 or higher, you may delete `conf/servers.xml` when prompted during the update process.

```
Starting update of centralized-management centralized-management from
v2.1u2 to v2.2...
* Gathering information...
* Module found in '/opt/APG/Web-Applications/Centralized-Management/
centralized-management'.
* It will now be updated using 'centralized-management-2.2-linux-
x64.pkg'.
* Undeploying web application '/opt/APG/Web-Applications/Centralized-
Management/centralized-management/webapp/mgmt.war' from Tomcat-
Default...
* Unpacking files...
* Configuration file 'conf/servers.xml', which has not changed since
its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Updating files... 100%
* 81 files have been updated.
* Finalizing update...
* Deploying web application '/opt/APG/Web-Applications/Centralized-
Management/centralized-management/webapp/mgmt.war' on Tomcat-
Default...
? Task file online-update-check.task added by module centralized-
management centralized-management. Enable it? [y]es, [n]o, [A]ll,
[N]one > y
```

**webapps-resources**

You may delete the property-mapping values when updating to webapps-resources version 1.3 or higher.

```
Starting update of webapps-resources Default from v1.2u1 to v1.3...
* Gathering information...
* Module found in '/opt/APG/Custom/WebApps-Resources/Default'.
* It will now be updated using 'webapps-resources-1.3-linux-x64.pkg'.
* Unpacking files...
* Configuration file 'property-mapping/FLOW-TF-SRCADDR.xml', which
has not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-DATA.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-PROTO.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-DSTADDR.xml', which
has not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-APPLI.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Updating files... 100%
* 530 files have been updated.
* Finalizing update...
```

**frontend-report-generator**

When prompted to replace the v6.2u3 version with the v6.3 version of the `daily_health_report`, enter `[y]es`. When prompted to keep the old version as a backup, enter `[y]es`.

```
The task file scheduled-reports/user1/daily_health_report.task is
already installed in the task scheduler but with different content.
Replace the current task which is enabled by the updated one? [y]es
[n]o [A]ll [N]one > y
```

## Installing the generic-rsc package

Manually install the `generic-rsc` package when migrating from 6.2.x to the 6.3.x core software release.

### Procedure

1. Navigate to **Centralized Management**.
2. Expand **Physical Overview** and select the server where the collector host is installed.
3. Select the **SolutionPacks and Modules** tab.
4. Click **Install** to access **Packages Installation**.
5. Select the **Block** category and select the **generic-rsc** package.
6. Click **Launch** to access the **Installation Steps** window.
7. Accept the default values and click **Install** for each component:
  - Topology-Mapping-Service
  - Collector-Manager
  - FailOver-Filter
  - Inline-Calculation-Filter
  - Variable-Handling-Filter
  - Property-Tagging-Filter
  - Remote-Shell-Collector
  - generic-rsc

If you are prompted for information, press **Enter** to select the default value or type another value appropriate for your deployment.

The component status turns green.

8. Click **Back** to return to **Packages Installation** to continue installing more packages or close the **Installation Steps** window.

## Installing the generic-topology package

Manually install the `generic-topology` package when migrating from 6.2.x to the 6.3.x core software release.

### Procedure

1. Navigate to **Centralized Management**.
2. Expand **Physical Overview** and select the server where the Backend modules are installed.
3. Select the **SolutionPacks and Modules** tab.
4. Click **Install** to access **Packages Installation**.
5. Select the **Block** category and select the **generic-topology** package.
6. Click **Launch** to access the **Installation Steps** window.
7. Accept the default values and click **Install** for each component:
  - Topology-Service

- generic-topology

If you are prompted for information, press **Enter** to select the default value or type another value appropriate for your deployment.

The component status turns green.

8. Click **Back** to return to **Packages Installation** to continue installing more packages or close the **Installation Steps** window.

## Installing the Maps-Service package

Manually install the `Maps-Service` package when migrating from 6.2.x to the 6.3.x core software release.

### Procedure

1. Navigate to **Centralized Management**.
2. Expand **Physical Overview** and select the server where the Frontend modules are installed.
3. Select the **SolutionPacks and Modules** tab.
4. Click **Install** to access **Packages Installation**.
5. Select the **Tools** category and select the **Maps-Service** package.
6. Click **Launch** to access the **Installation Steps** window.
7. Accept the default values and click **Install**.

If you are prompted for information, press **Enter** to select the default value or type another value appropriate for your deployment.

The component status turns green.

8. Click **Back** to return to **Packages Installation** to continue installing more packages or close the **Installation Steps** window.

## Updating the SolutionPackBlocks

After installing a software update or migrating from an older release, you must update SolutionPackBlocks in order to use the latest module configurations and report templates. This block update may trigger the update of an associated module.

### Before you begin

- ◆ Be sure you have updated core modules (except for blocks, collectors, and event processors) in all of the servers before you update SolutionPackBlocks.

### Procedure

1. Click the **SolutionPacks** node on the left panel to access **Installed SolutionPacks**.

Two panes appear: Independent SolutionPackBlocks and SolutionPacks. Update the Independent SolutionPackBlocks first before you update the SolutionPackBlocks that belong to the SolutionPacks.

2. Do the following to locate the block that you want to update:

In the pane for	Perform:
Independent SolutionPackBlocks	Locate the block.

In the pane for	Perform:
<b>SolutionPacks</b>	a. Select the specific SolutionPack. b. Locate the block in the <b>Properties</b> page.

3. Click the **yellow star icon**.

The **SolutionPack Update** page appears.

4. Carefully review the settings on this page and make changes as needed.

Most values are from the existing SolutionPack but some may be default values for the new SolutionPack.

5. Click **Update**.

The update process begins. The **SolutionPack Update** page provides information on the progress of the update.

6. Select the maximize arrow next to view the update progress.

When the update successfully completes, a green checkmark appears above this information.

## Controlling services from Centralized Management

You can start, stop, or restart services from the Centralized Management.

### Before you begin

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

### Procedure

1. Log in and select **Administration > Centralized Management**.
2. Select the server in **Physical Overview**.
3. In the **Services** tab, select the module.
4. Click one of the following buttons.

Operation	Description
<b>Start</b>	Starts the service.
<b>Stop</b>	Stops the service.
<b>Restart</b>	Restarts the service.

Read the status message.

## Default ReportPack migration

Update the Default ReportPack to ensure you use the latest SolutionPack template.

Update the Default ReportPack from the Administration menu after logging in to the User Interface URL, for example, `http://<Frontend-hostname>:58080/APG`

The Default ReportPack contains the default reports. To access all of the new report features available in a software release, update the Default ReportPack during the migration process.

1. Back up the existing Default ReportPack by exporting the `.arp` file.
2. Upload the Default ReportPack.
3. Delete the old ReportPack.

---

#### Note

Scheduled reports, pre-generated reports and template restrictions are lost when you delete the old Default ReportPack. The online help describes methods for exporting ReportPack templates so you can save them.

---

## Exporting a ReportPack

You can export a ReportPack to back up the `<ReportPack>.arp` file or for use in another system.

#### Procedure

1. Click **Administration**.
2. Under **ReportPacks**, click **List / Import ReportPacks**.
3. Select the ReportPack.
4. Click **Export** to download the `<ReportPack>.arp` file that contains the required information and templates.
5. Click **Save** to navigate to the download location.

## Updating the Default ReportPack

Update your existing Default ReportPack by replacing it completely with a new Default ReportPack.

#### Before you begin

- ◆ Ensure you have a login with root, APG, or system administrator privileges to perform this task. The user `apg` is the account that the core software application uses instead of root.
- ◆ Locate the new `Default ReportPack.arp` file. The file is located on the server in `<INSTALL_DIR>/Web-Servers/Tomcat/Default/webapps/APG`. If you are accessing the server remotely, you will need to download the `.arp` file to your local directory first.

#### Procedure

1. Log in and select **Administration > ReportPacks** to access **ReportPacks Management**. Available ReportPacks are listed in a pane.
2. Rename the existing Default ReportPack to distinguish between the existing one and the new one.
  - a. Select **Default ReportPack** in the pane.
  - b. Type **(original 6.2)** in the **Name** field.  
The **Name** field value reads: Default ReportPack (original 6.2)
  - c. Click **Save**.

You are returned to **ReportPacks Management**.

3. Click **Upload a ReportPack**.
4. Select the `Default ReportPack.arp` file from your local directory.
5. Click **Save**.

#### After you finish

If you are satisfied with the resulting reports , you can delete the old Default ReportPack.

---

#### Note

Scheduled reports, pre-generated reports and template restrictions will be lost if you remove it.

---

## Deleting a ReportPack

When a ReportPack is no longer needed, you can remove it and its report templates.

#### Procedure

1. Click **Administration**.
2. Under **ReportPacks**, click **List / Import ReportPacks**.
3. Select the ReportPack.
4. Click **Delete** to remove the ReportPack and its templates.
5. Click **Ok** at the warning message.

## 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 9

## Suite Software Uninstallation

This chapter includes the following topics:

◆ Overview.....	142
◆ Stopping core software services on a UNIX server.....	142
◆ Uninstalling core software from a UNIX server.....	142
◆ Stopping core software services on a Windows server.....	142
◆ Uninstalling core software from a Windows server.....	143
◆ Uninstalling a SolutionPack.....	143

## Overview

You can uninstall a SolutionPack and uninstall core software from a UNIX or Windows server.

Stop the core software services before uninstalling core software.

## Stopping core software services on a UNIX server

Use the `manage-modules.sh service stop` command to stop a specific core software service or to stop all core software services on a UNIX server.

### Before you begin

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

### Procedure

- ◆ Type `manage-modules.sh service stop <service_name>` from the `bin` directory of the installation to stop a specific core software service.

This example shows how to stop all core software services:

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

## Uninstalling core software from a UNIX server

Use the `manage-modules.sh service remove all` command to uninstall all core software 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 core software services.
2. Type `rm -rf /opt/APG` to remove the installation directory.

## Stopping core software services on a Windows server

Use this procedure to stop core software services from the Windows desktop.

### Before you begin

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

### Procedure

1. From the application desktop, select **Start > Administrative Tools > Services**.
2. Right-click each service and click **Stop**, in order:
  - APG MySQL
  - APG Backend
  - APG Alerting Backend

- APG Collector Manager
- APG Tomcat
- APG Task Scheduler
- APG Webservice Gateway

## Uninstalling core software from a Windows server

Use the `manage-modules.cmd service remove all` command to remove all core software 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 core software services.
2. Use the **Windows Control Panel** to uninstall core software.
  - 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 core software 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 10

## Suite Software Updates

This chapter includes the following topics:

- ◆ [Updating standard installations](#)..... 146

## Updating standard installations

Follow the procedures in this section to update the full core software installation, to update SolutionPack files before installing the SolutionPack for the first time, or to update an existing installed SolutionPack.

### Update core software

- ◆ [Updating the core software installation on page 146](#)

### Update SolutionPack software for your core software installation

- ◆ [Module update order for multiple hosts on page 100](#)
- ◆ [Updating modules on page 103](#)
- ◆ [Installing a SolutionPack Center Update on page 152](#)

### Update a SolutionPack that is already installed

- ◆ [Module update order for multiple hosts on page 100](#)
- ◆ [Updating modules on page 103](#)
- ◆ [Updating an existing SolutionPack on page 154](#)

## Updating the core software installation

Run the installer to update the core software installation. After the installer detects an existing installation, it copies the newer installation into the module repository, which is in `<INSTALL_DIR>/Tools/Module-Repository`.

### Before you begin

- ◆ Ensure that the installation update is downloaded from EMC Online Support to the installation directory, such as `/INSTALL_DIR`
- ◆ Ensure you have a login with root or system administrator privileges to perform this task.

### Procedure

1. Go to the installation directory.
2. Change the permissions of the installer so you can run it.

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

```
chmod +x setup-linux-x86_64-v63u1.sh
```

3. Run the installer for your operating system from the installation directory:

Operating system	Command
UNIX	<code>setup-linux-x86_64-&lt;version_number&gt;.sh</code>
Windows	<code>setup-win64-&lt;version_number&gt;.exe</code>

4. Answer any questions.
5. After the installation update is complete, identify the modules to update.

[Identifying which modules to update on page 100](#)

6. Update the modules.

## Updating modules on page 103

### Identifying which modules to update

After you update a core software installation, run the `manage-modules.sh list installed` command to view the installed modules and to determine which modules to update. Update the modules with the status of `can be updated`.

#### Procedure

- ◆ Type the command for your operating system from the core software installation directory:

Operating system	Command
<b>UNIX</b>	<code>&lt;INSTALL_DIR&gt;/bin/manage-modules.sh list installed</code>
<b>Windows</b>	<code>&lt;INSTALL_DIR&gt;\bin\manage-modules.cmd list installed</code>

When you view the output, record the identifier value of each module that needs to be updated. You will need to specify the identifier later when you update the module.

This sample output indicates to update the Module-Manager first, then to update the Alerting-Backend and the Alerting-Frontend modules to version 3.5. For other lines, pay attention to the status recommendations.

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

Identifier Revision OS-Arch	Instance Status	:Category	Module Name	Version
-----	-----	-----	-----	-----
* alerting-backend r4123 linux-x64	Default can be updated to v3.5	:Backends	Alerting-Backend	v3.1u2
* alerting-frontend r4123 linux-x64	alerting-frontend can be updated to v3.5	:Web-Applications	Alerting-Frontend	v3.1u2

### Module update order for multiple hosts

Update modules in a specific order to avoid issues involving software dependencies and redundant files. Modules that are available for update are marked with a yellow star icon in Centralized Management. If a Module-Manager update is available, always update this module first. Refer to the release notes or the workflow for your deployment scenario for additional recommendations.

Depending on your installed SolutionPacks, the list of modules needing to be updated will vary. When updating modules in a multiple host deployment, follow these recommendations:

- ◆ Update a subset of core modules (Group A) on the Centralized Management server first using the CLI command, `manage-modules.sh update` or `manage-modules.cmd update`.
- ◆ After updating the last core module in Group A, update the services and then start the services.

- ◆ After retrieving modules from the remote host servers, launch the update of a second subset of modules (Group B) from **Centralized Management > Logical Overview**. A few modules require an additional manual CLI update step on the remote host servers.
- ◆ Update Independent SolutionPackBlocks.
- ◆ Update SolutionPackBlocks.

---

**Note**

Do not update any other modules, even if they display in **Centralized Management > Logical Overview** with the yellow star update icon.

---

**Table 8** Group A: Core modules for CLI update

Update these core modules using CLI commands.
module-manager
java
license-manager
mysql (optional, but recommended)
jdbc-drivers
tomcat
WebApps, includes one or more of these modules if marked for update:      • alerting-frontend     • centralized-management     • device-discovery     • frontend     • frontend-ws     • mib-browser     • ip-sla-probes     • transaction-collector-gui
webapps-resources
webservice-gateway

**Table 9** Group B: Launch the update from Centralized Management > Logical Overview

Core module update order	Node in Logical Overview	Notes
module-manager	Miscellaneous	Launch from Logical Overview to send the module update to the remote host server. You must also issue the CLI command, ( <code>manage-modules.sh update module-manager</code> or <code>manage-modules.cmd update</code> )

**Table 9** Group B: Launch the update from Centralized Management › Logical Overview (continued)

Core module update order	Node in Logical Overview	Notes
		module-manager) on the remote host to apply the update.
java	Miscellaneous	Launch from Logical Overview to send the module update to the remote host server. You must also issue the CLI command, (manage-modules.sh update java or manage-modules.cmd update java) on the remote host to apply the update. Ensure all services are restarted after updating java. (manage-modules.sh service start all or manage-modules.cmd service start all
license-manager	Miscellaneous	
mysql	Databases	
jdbc-drivers	Databases	
tomcat	Miscellaneous	The update stops the service. If the display indicates the service failed to stop, retry the update.
alerting-frontend	Frontends	
centralized-management	Frontends	
device-discovery	Frontends	
frontend	Frontends	
frontend-ws	Frontends	
mib-browser	Frontends	
ip-sla-probes	Frontends	
transaction-collector-gui	Frontends	
webapps-resources	Miscellaneous	
webservice-gateway	Miscellaneous	Launch from Logical Overview to send the module update to the remote host server. You must also issue the CLI command, (manage-modules.sh update webservice-gateway or manage-modules.cmd update webservice-gateway) on the remote host to apply the update.
alerting-backend	Backends	
apg-backend	Backends	

**Table 9** Group B: Launch the update from Centralized Management › Logical Overview (continued)

Core module update order	Node in Logical Overview	Notes
apg-property-store	Databases	
administration-tool	Miscellaneous	
diagnostic-tools	Miscellaneous	
frontend-report-generator	Miscellaneous	
frontend-search	Miscellaneous	
task-scheduler	Miscellaneous	
topology-cli	Miscellaneous	

When updating multiple modules, update first by Category and then by Module Name.

The Frontend and SNMP module families are not used in all deployments.

Since modules belonging to the Frontend family have logical interdependencies, the modules must be updated to the same version or problems may occur.

Modules belonging to the SNMP family also have logical interdependencies and must be updated to the same version.

You can view the Category and Module Name values by using the `manage-modules.sh list installed` command or by viewing the nodes in **Centralized Management › Logical Overview**.

## Updating modules

Run the `manage-modules.sh update <identifier>` command to update the modules and their managers. Some modules may request information from you during an update. For example, you may be prompted for a module instance name if there are multiple instances, whether you want to continue the update, and whether you want to keep the original copy of a file that is updated.

### Before you begin

- ◆ Obtain the identifier by using the `manage-modules.sh list installed` command.
- ◆ Make sure you have a login with root or system administrator privileges to update modules.

Update the manager of the module first before updating the module. Use the same command and substitute the appropriate identifier.

### Procedure

1. Type the command for your operating system from the core software installation directory:

Operating system	Command
UNIX	<code>&lt;INSTALL_DIR&gt;/bin/manage-modules.sh update &lt;module_identifier&gt; [&lt;module_instance&gt;]</code>

Operating system	Command
Windows	<code>&lt;INSTALL_DIR&gt;\bin\manage-modules.cmd update &lt;module_identifier&gt; [&lt;module_instance&gt;]</code>

2. Answer any questions.

## manage-modules.sh update command

Use the `manage-modules.sh update` command to update modules and their managers. Type the command for your operating system from the `bin` directory of your core software installation directory.

### Description

The `manage-modules.sh update` command updates installed modules and their managers. For UNIX, specify `manage-modules.sh update`. For Windows, specify `manage-modules.cmd update`.

Update the manager of the module first before updating the module.

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

### Syntax

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

### Options

#### module\_identifier

The identifier value of the installed module or manager.

#### module\_instance

The unique name of the module or manager. 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 update or the command will prompt you for the instance name.

The identifier and instance values form a unique key to refer to the module or manager.

In this Linux example, the following commands update the manager, Collector-Manager, and a corresponding module, XML-Collector.

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

In this Windows example, the following commands update the Tomcat Web server and a corresponding module, MIB-Browser.

```
<INSTALL_DIR>\bin\manage-modules.cmd update tomcat
<INSTALL_DIR>\bin\manage-modules.cmd update mib-browser
```

In this Linux example, the following commands update specific instances.

```
./manage-modules.sh update tomcat instance3
./manage-modules.sh update mib-browser mymib_browser2
```

## Installing a SolutionPack Center Update

Periodically, updates of the SolutionPacks are available in a .zip file called SolutionPackCenter Update on EMC Online Support. This .zip file contains a README file that describes the changes made to each SolutionPack and individual `<solution>.pkg` files for installing each update.

### Before you begin

- ◆ Install the required license file to enable your SolutionPack.
- ◆ Ensure any Domain Managers that supply data to the SolutionPack are installed and configured.
- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the core software application uses instead of root.
- ◆ Update the core modules in all servers before you update or install a SolutionPack after upgrading your base installation.

Core modules are modules that are not installed by a SolutionPackBlock. Examples of core modules include webapps, module-manager, license-manager, java, mysql, backend, tools, and so forth. Update these core modules: **Databases, Backends, Frontends, Miscellaneous** (except Blocks). Since the recommended module update order varies, refer to the Module Update Order section for the multiple hosts or single host deployments. Also, the *EMC Watch4net Centralized Management Guide* provides more information.

Examples of modules that are installed with SolutionPackBlocks include collector-manager, event-processing-manager, and collector or event components.

### Procedure

1. Locate the Watch4net downloads area on EMC Online Support.
  - a. Go to `https://support.emc.com`.
  - b. Click **Support by Product**.
  - c. Type **watch4net** in the **Find a Product** field, and then click the arrow next to it.
  - d. Click **Downloads**.

The **Downloads for Watch4net** page appears.

2. Download the latest SolutionPackCenter Update to a local directory.  
For example: SolutionPackCenter Update `<month> <year>`
3. Browse to **Administration > Centralized-Management > Packages Management** and click **Upload**.
4. Browse to the SolutionPackCenter Update .zip file and click **OK**.

### After you finish

Update the SolutionPackBlocks after installing the SolutionPack update: [Updating the SolutionPackBlocks on page 111](#).

Browse to **Administration > Centralized Management > SolutionPacks > SolutionPack Center** and install the SolutionPack.

You can confirm the SolutionPack version number by browsing **SolutionPacks** in the left panel.

## Updating the SolutionPackBlocks

After installing a software update or migrating from an older release, you must update SolutionPackBlocks in order to use the latest module configurations and report templates. This block update may trigger the update of an associated module.

### Before you begin

- ◆ Be sure you have updated core modules (except for blocks, collectors, and event processors) in all of the servers before you update SolutionPackBlocks.

### Procedure

1. Click the **SolutionPacks** node on the left panel to access **Installed SolutionPacks**.

Two panes appear: Independent SolutionPackBlocks and SolutionPacks. Update the Independent SolutionPackBlocks first before you update the SolutionPackBlocks that belong to the SolutionPacks.

2. Do the following to locate the block that you want to update:

In the pane for	Perform:
Independent SolutionPackBlocks	Locate the block.
SolutionPacks	a. Select the specific SolutionPack.     b. Locate the block in the <b>Properties</b> page.

3. Click the **yellow star icon**.

The **SolutionPack Update** page appears.

4. Carefully review the settings on this page and make changes as needed.

Most values are from the existing SolutionPack but some may be default values for the new SolutionPack.

5. Click **Update**.

The update process begins. The **SolutionPack Update** page provides information on the progress of the update.

6. Select the maximize arrow next to view the update progress.

When the update successfully completes, a green checkmark appears above this information.

## Reconfiguring a SolutionPack in Centralized Management

You can reconfigure a SolutionPack by modifying its settings in Centralized Management.

### Procedure

1. Navigate to **Centralized Management**.
2. Click the **SolutionPacks** node on the left panel to display the existing installed SolutionPacks.
3. Depending on whether the SolutionPackBlock is an independent block or component of a SolutionPacks, do the following to locate the instance that you want to reconfigure:

In the pane for	Perform:
SolutionPacks	a. Select the SolutionPack.

In the pane for	Perform:
	b. Locate the instance in the <b>Properties</b> page.
<b>Independent SolutionPackBlocks</b>	Locate the instance.

- Click the **Pencil** icon next to the instance for the SolutionPackBlock.
- In the **SolutionPack Reconfiguration** screen for each SolutionPackBlock, change one or more settings and click **Reconfigure**.

## Updating an existing SolutionPack

Periodically, updates of the SolutionPacks are available in a .zip file called SolutionPackCenter Update on EMC Online Support. This .zip file contains a README file that describes the changes made to each SolutionPack and individual `<solution>.pkg` files for installing each update.

### Before you begin

- Download the SolutionPack from EMC Online Support to a local directory.
- Upload the SolutionPack to the server where the core software is running.
- Update the core modules in all of the servers before you update an existing SolutionPack.

The modules used by a SolutionPack are updated with the latest version in the module repository during this process. This may override customizations made to .xml files and reports.

Core modules are modules that are not installed by a SolutionPackBlock. Examples of core modules include webapps, module-manager, license-manager, java, mysql, backend, tools, and so forth. Update these core modules: **Databases, Backends, Frontends, Miscellaneous** (except Blocks). Since the recommended module update order varies, refer to the Module Update Order section for the multiple hosts or single host deployments. Also, the *EMC Watch4net Centralized Management Guide* provides more information.

Examples of modules that are installed with SolutionPackBlocks include collector-manager, event-processing-manager, and collector or event components.

### Procedure

- Log in with administrator credentials for core software.
- Browse to **Administration > Centralized Management > Packages Management**.
- Click **SolutionPacks** on the left panel to display the existing installed SolutionPacks.
- Select the SolutionPack to update.

A **Properties** page appears for the selected SolutionPack, which includes all related SolutionPackBlocks.

- Select the SolutionPackBlock to update by clicking on its yellow star icon.

The **SolutionPack Update** page appears.

- Carefully review the settings on this page and make changes as needed.

Most values are from the existing SolutionPack but some may be default values for the new SolutionPack.

- Click **Update**.

The **SolutionPack Update** page provides information on the progress of the update. When the update successfully completes, a green checkmark appears above this information.

8. Click **SolutionPacks** on the panel to list the existing installed SolutionPacks.

The updated SolutionPack with its new version and updated SolutionPackBlock appear in this list.

