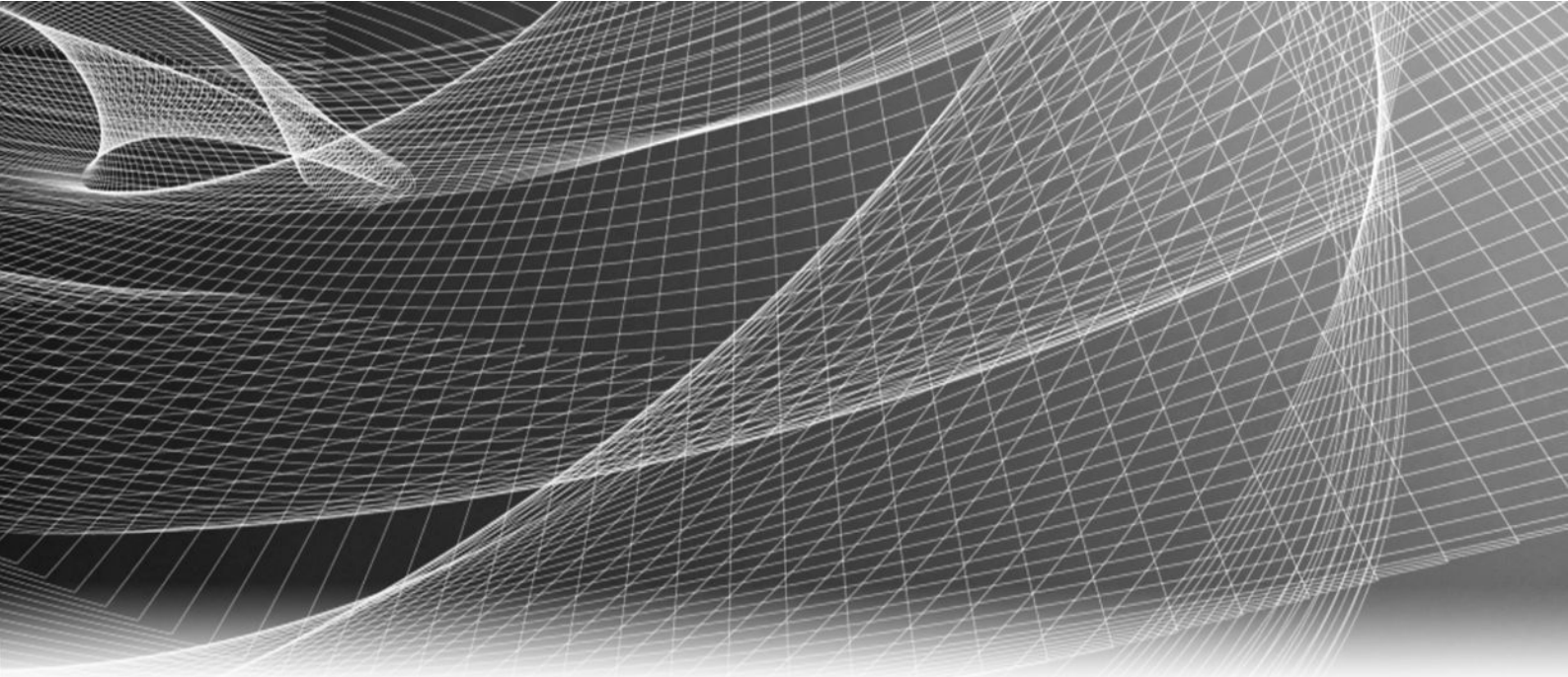




EMC[®] Storage Resource Management Suite

Version 3.0.2.0

Installation and Configuration Guide

PN 302-000-859

REV 02

Copyright © 2013-2014 EMC Corporation. All rights reserved. Published in USA.

Published April, 2014

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		5
Chapter 1	Installation Workflow	7
	Core software	8
	Supported update paths	8
	Storage Resource Management Suite SolutionPacks	8
Chapter 2	Virtual Appliance Installation	9
	Virtual Appliance installation overview	10
	Four VM vApp installation option	10
	One VM vApp installation option	10
	Installing the 4 VM vApp	11
	Verifying the deployment and starting the appliance	13
	Logging in to the User Interface	13
	Passwords	13
	Adding disk space	14
Chapter 3	Standard Installation	15
	Standard installation options	16
	Installing core software on UNIX	16
	Installing core software on Windows Server	17
Chapter 4	Configuration	19
	Starting the core software services from the command line	20
	Starting the core software services on Windows	20
	Verifying if the core software services are running	21
	Troubleshooting service start-up problems on UNIX	21
	Troubleshooting service start-up problems on Windows	22
	Logging in to the User Interface	22
	Connecting to Centralized Management	22
	Confirm configuration settings and register remote servers	23
	Installing core suite licensing	23
	Adding licenses	24
	Verifying core software licenses from Centralized Management	24
	Configuring the user process limits for the Linux installation	25
	Policy Management	25
	Creating a policy	26
	Enabling or Disabling a policy	28
	Reconfiguring the maps service	28
	Reconfiguring generic-rsc and generic-snmp	28
Chapter 5	Infrastructure Preparation for Discovery and Data Collection	31
	Host preparation for discovery data collection	32
	Host configuration required for Windows and UNIX	32
	Prerequisites for Windows 2003 Hosts	33

	Windows configuration for discovery and data collection	33
	Configuring group policy	38
	UNIX and Linux host configuration for discovery and data collection	39
	Configuring VIOS (VIO Server) for discovery	41
	Configuring ESX hosts to collect PowerPath metrics	41
	Configuring hosts to collect PowerPath metrics	42
	Installing EMC Host Interface on Windows Server	42
	Switch configuration for discovery and data collection	45
	Brocade switch configuration	45
	Cisco switch configuration	46
	Storage system preparation for discovery and data collection	49
	Preparing EMC Centera	49
	Preparing Converged Infrastructure	50
	Preparing EMC Data Domain	50
	Preparing EMC Isilon	50
	Preparing EMC VMAX	50
	Preparing EMC VNX	54
	Preparing EMC VPLEX	56
	Preparing EMC VMware vCenter	57
	Preparing Hitachi Device Manager	57
	Preparing HP 3PAR StoreServ	58
	Preparing HP EVA	58
	Preparing IBM DS	58
	Preparing IBM XIV	59
	Preparing NetApp Filer	59
	Preparing VI VirtualWisdom	59
Chapter 6	SolutionPack Installation	61
	Access credentials required for SolutionPacks	62
	Connecting to Centralized Management	65
	Installing a SolutionPack	65
	Configuration during SolutionPack installation	66
	Post-installation configuration of SolutionPacks	86
	Post-installation configuration details	89
	Configuring Solutions Enabler client access for VMAX	89
	Enabling passive host discovery through Brocade FC SolutionPack	93
	Enabling passive host discovery through Generic-SNMP	94
	Post-install configuration for SolutionPack for Physical Hosts	95
	Configuring compliance-frontend.xml	96
	Policy Management	97
Chapter 7	Suite Software Uninstallation	101
	Overview	102
	Stopping core software services on a UNIX server	102
	Uninstalling core software from a UNIX server	102
	Stopping core software services on a Windows server	102
	Uninstalling core software from a Windows server	103
	Uninstalling a SolutionPack	103

TABLES

1	Access credentials.....	62
2	SolutionPack configuration details.....	66

CHAPTER 1

Installation Workflow

This chapter includes the following topics:

- ◆ [Core software](#)..... 8
- ◆ [Storage Resource Management Suite SolutionPacks](#)..... 8

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.

Supported update paths

EMC only supports the application of specific updates in sequence.

- ◆ 3.0.0.0 › 3.0.2.0
- ◆ 3.0.1.0 › 3.0.2.0

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	10
♦ Installing the 4 VM vApp	11
♦ Verifying the deployment and starting the appliance	13
♦ Logging in to the User Interface	13
♦ Adding disk space	14

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 which are pre-configured to communicate with each other:

- ◆ 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 option provides a specific appliance as a single virtual machine which can then be manually added to your base installation to extend your environment:

- ◆ 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. This VM includes the same modules as the Minimal Installation and adds generic Collector modules (Generic-SNMP, Generic-RSC)

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.

Installing the 4 VM vApp

You can deploy the SRM Suite 4 VM appliance from an OVF template using a vSphere Client.

Before you begin

- ◆ 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
- ◆ DRS enabled

Procedure

1. Open vSphere Client and connect to the vCenter Server that manages your VMware environment.
2. Select the resource pool to which you want to deploy the VMs for SRM Suite
3. From the **File** menu, select **Deploy OVF Template**.
4. In the **Source** step, browse to the location of the `SRM_4VM_vApp.ovf` file.

Example file path: `/opt/ovf/SRM_4VM_vApp.ovf`

Example URL: `http://myHost.emc.com/ovf/snapshot/92/SRM_4VM_vApp.ovf`

5. 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.

6. In the **OVF Template Details** step, review the details of the loaded .ovf file and click **Next**.
7. In the **End User License Agreement** step, review the license agreement. Click **Accept** and then click **Next** to continue.
8. In the **Name and Location** step:
 - a. Accept the default name (SRM Suite) or type a **Name** for the appliance.
 - b. Specify an **Inventory Location** for the appliance within your VMware environment.
 - c. Click **Next**.
9. (Optionally for a 1 VM deployment only), select a deployment configuration from the drop-down menu:
 - **All-In-One**
 - **Front End Appliance**
 - **Additional Back End Appliance**
 - **Collector Appliance**
 - **Minimal Installation**
10. Select the destination storage for the virtual machine files 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 for each of the VMs and click **Next**.
13. In the **IP Address Allocation** step, choose the IP allocation policy and IP protocol to use and click **Next**.
14. In the **Properties** step, provide the values of the properties as defined in the Virtual Appliance Properties table for each of the VMs and click **Next**.
15. 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.
16. After deployment is complete, click **Close** in the **Deployment Completed Successfully** dialog box.

Verifying the deployment and starting the appliance

After deploying the appliance, verify that it is working.

Procedure

1. In the vSphere client, navigate to the **Host and Cluster** 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. Right-click each VM and select **Open Console**.
4. Right-click the vApp and select **Power On**.

Each VM in the vApp is powered on.

5. Observe the initial startup and module installations on each console.

Once the initial startup and module installations are complete, the login prompt displays.

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

Adding 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`.

CHAPTER 3

Standard Installation

This chapter includes the following topics:

- ◆ [Standard installation options](#)..... 16
- ◆ [Installing core software on UNIX](#)..... 16
- ◆ [Installing core software on Windows Server](#)..... 17

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.

CHAPTER 4

Configuration

This chapter includes the following topics:

◆ Starting the core software services from the command line	20
◆ Starting the core software services on Windows	20
◆ Verifying if the core software services are running	21
◆ Logging in to the User Interface	22
◆ Connecting to Centralized Management	22
◆ Confirm configuration settings and register remote servers	23
◆ Installing core suite licensing	23
◆ Configuring the user process limits for the Linux installation	25
◆ Policy Management	25
◆ Reconfiguring the maps service	28
◆ Reconfiguring generic-rsc and generic-snmp	28

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.

Confirm configuration settings and register remote servers

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

Before you begin

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

Procedure

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

For detailed information about the entries, click **Documentation** and view the *Centralized Management Guide*.

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.

CAUTION

Verify that all SolutionPacks you have acquired are registered in ELMS before removing the bootstrap license.

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.

ELMS licenses can only be added via a single `.LIC` file. Large customers with multiple party IDs may have hardware and entitlements at multiple locations, resulting in

multiple .LIC files. ELMS can only register one .LIC file, which contains licenses for all SolutionPacks that a customer has acquired.

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'
```

Policy Management

You can use default policies or create user-defined policies to analyze configuration changes in your data center for compliance and to detect breaches against these policies.

- ◆ [Creating a policy on page 26](#)
- ◆ [Enabling or Disabling a policy on page 28](#)
- ◆ [Editing a policy](#)
- ◆ [Copying a policy](#)
- ◆ [Deleting a policy](#)

Creating a policy

Use the existing pre-defined templates to create a new policy or the empty policy template to customize it.

Procedure

1. Click **Operations**.
2. Under **Compliance**, click **Storage Compliance** > **Manage Rules & Policies**.
3. Click **Create Policy**.
4. Select a template from the **Select Policy from template** drop-down list.
5. Click **Description** and provide the following details:

Field	Description
Policy Name	Type a name for the policy.
Policy Description	Type a brief description for the policy.-
State	Select Enabled or Disabled from the drop-down list if you want the policy to run once it is created or otherwise.

Note

If you choose the state as **Disabled**, you should manually enable the policy after creating the policy to run it.

6. Click **Scope**.
 - a. To create a new user-defined scope, click **Create Scope**.
The **Create Scope** dialog box appears.
 - b. Provide the following details:

Field	Description
Name	Type a name for the scope.
Criteria	Type a criteria for the scope in the following format: <Property Name> <Operator> <Value>, such as; devtype = 'Array' & devicetype = 'FabricSwch' & parttype = 'port', and so on.

Note

Some examples of well-defined properties that can be used in criteria are:

- For Switch: devtype = 'Objecttype', device = 'SwitchName'.
- For Fabric: parttype = 'Fabric/VSAN', part = 'FabricName'.
- For Array: serialnb = 'Array S/N', ip = 'IP Address', revision = 'Microcode'.
- For Host: domain = 'Domain Name', devdesc = 'Operating System Version', pmodel = 'HBA Model'.

Note

The **Criteria** allows the following operators: & (AND), I (OR), and= (Equal To). You can also use wild card entry, such as, % for starts with, ends with, and contains expressions.

- c. Click **Show Members** to validate the criteria.

The **Show Members** dialog box listing members with matching criteria appears. A warning message is displayed for invalid criteria.

- d. Click **Save**.

The new user-defined scope is listed in the Scope table.

Note

Click **Show Members** to view the list of members associated with the scope.

7. Click **Rules**.
 - a. Click **Create Rule**.
 - b. Select a rule name from the drop-down list.
 - c. Double-click a rule to enable or disable it in the corresponding **State** column of the rule.
 - d. Double-click a rule to set the **Severity** to **Critical**, **Major**, **Minor**, or **Normal** using the drop-down list.
 - e. To provide criteria values for the rule, click **Criteria For Selected Rule** and select one of the following criteria and type a value in the corresponding text box:
 - Select the corresponding check box to enable the criteria or otherwise.
 - Select **LE** in the drop-down list to represent the Less than or Equal to value for the criteria.
 - Select **EQ** in the drop-down list to represent the Equal to value for the criteria.
 - Select **IN** in the drop-down list to represent the value(s) that the criteria contains.
-

Note

You can type multiple values that are comma separated. The values can contain different patterns and need not be restricted only to strings.

Note

Rules validate objects when its *vstatus* value is active. The other objects are ignored.

- f. Click **Recommendation** to view the recommendation for the rule.
8. Click **Schedule**.
 - a. Select a **Schedule** option and specify appropriate values from the drop-down lists to run the policy at a scheduled time.
9. Click **Save**.

Enabling or Disabling a policy

If you want the suite to run the policy after it is created, you must enable the policy. After enabling the policy, you can stop it any time by disabling it.

Procedure

1. Click **Operations**.
2. Under **Compliance**, click **Storage Compliance** › **Manage Rules & Policies**.
3. Right-click on a policy and select either:
 - **Enable** - To enable the policy to run.
 - **Disable** - To disable the policy.

Reconfiguring the maps service

If a host is setup via binary installation, or if the maps-service is installed manually in a binary installation, edit properties that affect the map service.

Procedure

1. Edit the `maps-service.properties`.
2. Update the properties `topoSvc.baseFeedUrl` and `topoSvc.endpointUrl` to use the pattern specified.

```
# Base URL for topology feeds

topoSvc.baseFeedUrl=https://<backend_hostname>:48443/Backends/
Topology-Service/Default/topology/
# URL for SPARQL endpoint

topoSvc.endpointUrl=https://<backend_hostname>:48443/Backends/
Topology-Service/Default/topology/repository/sparql
```

`<backend_hostname>`

represents the host where Topology Service is installed, typically the primary backend.

Reconfiguring generic-rsc and generic-snmp

If the collector host is installed via the binary installer, or if an additional collector host is added to a vApp, use this procedure.

Note

Use this procedure whether or not the collector host is being used for host and SAN discoveries.

Procedure

1. Click **Administration**.
2. Select **Centralized Management** › **SolutionPacks**.
3. Select Independent **SolutionPackBlocks**. A table appears listing **generic-rsc** and **generic-snmp**.
4. Click the pencil icon.

5. If the Topology Service has the default value `localhost`, update to correct values, and click **Reconfigure**.

CHAPTER 5

Infrastructure Preparation for Discovery and Data Collection

This chapter includes the following topics:

- ◆ [Host preparation for discovery data collection](#) 32
- ◆ [Switch configuration for discovery and data collection](#) 45
- ◆ [Storage system preparation for discovery and data collection](#) 49

Host preparation for discovery data collection

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

- ◆ [Host configuration required for Windows and UNIX on page 32](#)
- ◆ [Windows configuration for discovery and data collection on page 33](#)
- ◆ [UNIX and Linux host configuration for discovery and data collection on page 39](#)
- ◆ [Configuring ESX hosts to collect PowerPath metrics on page 42](#)
- ◆ [Installing host agent software on Windows hosts on page 42](#)

Host configuration required for Windows and UNIX

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

- ◆ [Considerations for hostname and IP address on page 32](#)
- ◆ [Considerations for SNIA libraries and HBA drivers on page 32](#)

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.

Prerequisites for Windows 2003 Hosts

Specific third-party software is required to permit discovery.

- ◆ Powershell (2.0 or above) needs to be installed on the host. Powershell can be downloaded from <http://support.microsoft.com/kb/968929/en-us>
- ◆ Fcinfo is required to fetch HBA & Host device information. `fcinfo.exe` can be downloaded from <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=17530>. Use the latest version of `fcinfo` and the default install location recommended by Windows.
- ◆ INQ 7.6.1.0 needs to be made available on the host. Platform specific INQ can be downloaded from: <ftp://ftp.emc.com/pub/symm3000/inquiry/v7.6.1.0/> The downloaded platform specific binary should be renamed to `inq` and placed in any one of the below specified locations:
 - `C:\inq.exe`
 - `C:\temp\inq.exe`
 - `C:\windows\Temp\nl_dwd\inq.exe`

Windows configuration for discovery and data collection

For a successful discovery of Windows hosts, configure a listener.

One of the following listeners needs to be configured:

- ◆ WinRM HTTP listener with the following configuration:
 - `Basic / Negotiate` authentication mode should be `true`.
 - `AllowUnencrypted` should be set to `true`
 - Firewall exception to be added for port 5985.
- ◆ WinRM HTTPS listener with following configuration:
 - `Basic / Negotiate` authentication mode should be `true`.
 - A certificate needs to be generated and placed in personal store.
 - Firewall exception to be added for port 5986.

These changes can be accomplished via two methods:

- ◆ Host Configuration utility - To be run on each host.
- ◆ Group policy configuration - To be run on domain server.

Protocol	Procedure
HTTP	• Creating a WSMAN listener for HTTP on page 34
HTTPS	• Generating a certificate on page 35 • Creating a WSMAN listener for HTTPS on page 37

Creating a WSMAN listener for HTTP

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

This procedure requires `hostconfig-srm.ps1` script, which is packaged along with SolutionPack for Physical Hosts. It is available @ <APG Home Directory/Collecting/Remote Shell Collector/Generic-RSC/scripts/windows>

Procedure

1. Run the Host-configuration powershell script on the target host to set the pre-requisite:

```
C:\Users\administrator.PLUGIN\Desktop> .\hostconfig-srm.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 host. Please create a listener using the command"
winrm create winrm/config/listener?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> .\hostconfig-srm.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> .\hostconfig-srm.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. To get help, run the script with the -help option: **C:\Users\administrator.PLUGIN\Desktop> .\hostconfig-srm.ps1 -help**

Generating a certificate

WinRM HTTPS requires a local computer server authentication certificate that is not expired, revoked, or self-signed to be installed.

Perform the following to create certificates:

Procedure

1. [Generate a .pfx certificate on page 35](#)
2. [Exporting the .pfx certificate on page 36](#)
3. [Importing the .pfx certificate on page 36](#)
4. [Generate a .cer file on page 37](#)
5. [Import the .cer file on page 36](#)

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 **C:\>makecert.exe -ss MY -sr LocalMachine -n "CN=<certificatename>" -sky exchange -pe -a sha1 -eku 1.3.6.1.5.5.7.3.1**

This creates a certificate under the personal store. Use the following steps to verify the certificate created using `makecert`.

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.
9. On the left pane, double click **Certificates (Local Computer)** > **Personal** > **Certificates**.
10. On the right pane double click the certificate listed.
11. Navigate to **Details** tab. Select **Subject** to get the CN Name and **Thumbprint** to get the Thumbprint of the certificate.

Note the **CN Name** and **Thumbprint** value, which will be used later while creating a WSMAN listener for HTTPS.

Exporting the .pfx certificate

To use the same certificate on multiple hosts, the generated certificate has to be imported on other hosts.

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 on other hosts 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** as DER or Base-64, 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>`

The command prompts for keystore's password. The default password is **changeit**.

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
```

Creating a WSMAN listener for HTTPS

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.

Before you begin

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

Procedure

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

```
\administrator.PLUGIN\Desktop> hostconfig-srm.ps1 -set-authType
Basic -ssl -thumbprint "aaa0ffd0ceac6165e33f480bc98a56573cade9e9" -
CN <hostname>
```

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
linbgb109.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 39](#)
- ◆ [Generating a public and private key pair for SSH key based authentication on page 40](#)

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.

By default, most of the command files have the following location: `/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin`

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.

Some packages are not installed by default.

- `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 VIOS (VIO Server) for discovery

Create a sudo user and provide the sudo user credentials while discovering the VIO Server

When the VIOS Server is installed the padmin user is automatically created and this user provides restricted shell access. The Storage Resource Management Suite 3.0 host data collection mechanism does not work in the restricted shell environment, hence the need to create and configure the sudo user.

- ◆ [Configuring sudo for host discovery on page 39](#)

The VIO Server and VIO Clients needs to be discovered using Generic-RSC independent block.

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.
- ◆ Register ESX and enable performance for reporting. Refer to the Powerpath /Ve or Rtools documentation about how to register an ESX server and enable performance.
- ◆ Configure the host where RTOOLS resides in generic-RSC based on the operating system type (ESX-LINUX or ESX-Windows).

To collect PowerPath metrics, do the following:

Procedure

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

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

PowerPath reports can also be accessed from **Explore View > Host > Storage Connectivity**.

PowerPath reports are available for the SolutionPack for IBM LPAR.

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 Storage Resource Management Suite *version* Host Interface Setup File (`emc-host-interface-version-platform.exe`) 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 Storage Resource Management Suite *version* Host Interface Setup File (`emc_host_interface-version-platform.exe`) 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 45](#)
- ◆ [Cisco switch configuration on page 46](#)

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 45](#)
- ◆ [Configuring Brocade switches for alert consolidation on page 46](#)

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 46](#)
- ◆ [Configure switches for SNMPv1 and SNMPv2 on page 47](#)
- ◆ [Configure switches for SNMPv3 on page 47](#)
- ◆ [Configure Cisco switches for alert consolidation on page 48](#)

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 data collection before installing the SolutionPack for EMC VMAX and perform the necessary pre-configuration.

SRM Suite requires EMC Solutions Enabler to collect array topology details for VMAX arrays; optionally SRM Suite requires UniSphere for VMAX and/or the EMC SMI-S Provider to collect array performance details. If both EMC Solutions Enabler and EMC SMI-S Provider are present, they must be on the same host. There are two supported scenarios for topology collection. The Solutions Enabler proxy scenario is recommended because the Collector and the Solutions Enabler are not competing for host resources.

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.

To support collection using the SYMAPI Server, two additional gatekeepers will be required per array on the remote Solutions Enabler host. For example, if there are already six gatekeepers per array then you will need to add two more for a total of eight gatekeepers per array.

Local Solutions Enabler scenario

The Local Solutions Enabler scenario supports topology collection for VMAX arrays using a VMAX Solution Pack Collector which has been installed on the same host as the Solution Enabler software.

- ◆ Implementing the Local Solutions Enabler scenario includes the advantages of reduced network calls and a more secure configuration. However, the Collector software will require additional Solutions Enabler host CPU and memory resources.
- ◆ The Solutions Enabler (proxy) scenario is the preferred configuration since the Collector and Solutions Enabler are not competing for host resources.
- ◆ The Local Solutions Enabler scenario requires that each VMAX array have at least 6 Gatekeeper Devices be created on the host.

Note

If the Solutions Enabler was installed to a Virtual Machine then Raw Device Mappings must be used when creating the Gatekeeper Devices

- ◆ If the Local Solutions Enabler is desired and if VMAX LUN Performance details are required, then it is recommended that you install the EMC SMI-S Provider kit on your host since it includes the required Solutions Enabler components. This is in contrast to installing a standalone Solutions Enabler kit and then installing the SMI-S Provider over it which could potentially cause incompatibility issues if the Solutions Enabler versions are different. Refer to EMC SMI-S Provider documentation for installation details.

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 communication with the server host over TCP/IP (port 2707, which is the default). 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 `stord daemon 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 <code>set</code> 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.

Option	Description
Linux	Use the env command to show the environment variables. To establish persistent variables use export to create the two variables as shown above.

- 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

- From the SYMAPI server host, type `sympd list` to display a list of devices that are visible to the host. Note the results.
- 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.
- To isolate the issue:
 - Verify that the same command works on the host with the FC connection to the Symmetrix array.
 - Verify that the environment variables for Solutions Enabler are set using the `symcli -def` command.
 - Verify that the `netcfg` file has been edited using the `symcfg -services list` command.
 - Verify the arrays you intend to monitor using the `symcfg list` command.
 - Verify that two additional 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, srdfa 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 55](#).

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 EMC VMware vCenter

Configure the **Statistic-Level** setting.

Procedure

1. Select **Administration > vCenter Server Settings > Statistics** to view the **Statistic-Level** settings.

Option	Description
Statistic-Level 3	Collects all Watch4net metrics including virtual-interface IO and virtual disk latency.
Statistic-Level 2	Provides all possible reports, except virtual-interface IO and Virtual Disk Latency.
Statistics collection interval	Use the value of 5 minutes, which is the default. If 5 Minutes is not selectable as a collection interval, configure it using the Edit button. This setting is mandatory.

2. Configure a full read-only account using the vSphere client **Permissions** tab for vCenter objects that will be discovered.

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 IP, username, password, SSH Port no (default is 22), and NetApp Filer Mode (7-Mode or C-Mode).
2. Identify the Cluster management IP for C-Mode Filer discovery.
3. 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>. 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:

♦ Access credentials required for SolutionPacks	62
♦ Connecting to Centralized Management	65
♦ Installing a SolutionPack	65
♦ Configuration during SolutionPack installation	66
♦ Post-installation configuration of SolutionPacks	86
♦ Post-installation configuration details	89

Access credentials required for SolutionPacks

W4N uses different accounts when running SolutionPacks. Configure the necessary accounts.

Table 1 Access credentials

SolutionPack	Access credentials
SolutionPack for ProSphere-SCA	Watch4net will use the ProSphere user account that has system administrator access.
SolutionPack for VMware vCenter	Watch4net requires a vCenter user account to communicate to the vSphere vCenter server that has Read-Only privilege and 5-minute static logging set to 3. This user account is different from what is required for ProSphere, which has a minimum privilege level of Browse DataStore and all StorageViews. This same user account requested for ProSphere can be used for Watch4net.
SolutionPack for Brocade FC Switch	Watch4net requires SNMP to communicate to each of the Brocade Switches. To discover the Zoning details from Brocade switches, the username, password, portnumber, and SSL enabled/status for the SMI-S provider are required.
SolutionPack for Cisco MDS/Nexus	Watch4net requires SNMP to communicate to each of the Cisco MDS Switches.
SolutionPack for EMC VNX	Watch4net requires NavisecCLI to access the VNX arrays. The user account needs to have administrator privileges to collect performance statistics Watch4net will use the apg user account: Linux default path - /opt/Navisphere/bin To validate your access to the VNX array, run this block command: <code>naviseccli -h (host) -user <user> -password <password> -scope 0 getagent</code> If the customer has already set up the NavisecCLI security file and has defined the user/password that you will be using, then you can enter anything for a user/password during the installation because you will be deleting the entries in all of the text collector xml files. You will need to edit all of the parser files in the various Text-Collector/conf directories as shown in step 3. 1. Create the following folder on the APG Server collecting the VNX Block: <code>...\APG\Collecting\Text-Collector\context</code> 2. Then use the naviseccli command to store the security file into that directory: <code>naviseccli -AddUserSecurity -User (deleted) - Password (deleted) -Scope 1 - secfilepath D:\Program Files\APG\Collecting\Text-Collector\context</code>

Table 1 Access credentials (continued)

SolutionPack	Access credentials
	3. Then each call to the naviseccli (from the parser-*.xml APG configuration files) should be used as the following: <pre>naviseccli -secfilepath D:\Program Files\APG\Collecting\Text-Collector\context -h <IP> ...</pre>
SolutionPack for EMC Isilon	Watch4net will use SSH and a user account.
SolutionPack for EMC VPLEX	Watch4net will use SSH and a user account.
SolutionPack for NetApp Filer	Watch4net requires SNMP v2c and NetApp CLI for latency to communicate to each of the NetApp Filers v1.2. The NetApp Filer v1.2 SolutionPack will use CLI exclusively. - SSH connection to the Netapp devices with the following roles: login-ssh, cli-stats*, cli-snap*, cli-aggr*, cli-vol*, cli-disk*, cli-environment, cli-nfs*, cli-cifs*, cli-df, cli-sysconfig, cli-ifconfig, cli-version - Make sure we are polling the real filer (not a vFiler) Note Make sure your hostnames are consistent.
SolutionPack for IBM DS	Watch4net requires SMIS and SSH, to be configured. - For IBM DS 3K/4K/5K requires IBM SMIS Provider - For IBM DS 6K/8K
SolutionPack for IBM SVC/V7000	Watch4net requires SMIS to be configured on each of IBM Management servers. The level of privilege required is administrator. - SVC/V7000 cluster IP address/hostname for SSH & CIMOM communication. - Username and password (User requires administrator level). Performance data retrieval will not work/be supported for “monitoring” security level - SSH public key (to retrieve performance data files over SSH)
SolutionPack for HP EVA	Watch4net requires SMIS and SSH, to be configured on each of the HP EVA ManagementHosts. The level of privilege required is administrator. - IP address/hostname for SSH & CIMOM communication. - Username and password for the HP EVA Element Manager
SolutionPack for Hitachi Device Manager	Watch4net requires SMIS and SSH, to be the HiCommand Device Manager for Hitachi Arraydata. The level of privilege required is administrator. - IP address/hostname for SSH & CIMOM communication - Username and Password

Table 1 Access credentials (continued)

SolutionPack	Access credentials
SolutionPack for EMC Centera	This SolutionPack requires EMC Centera CLI to be installed and configured on the Collectorhost. EMC Centera CLI is available on EMC Support Center (emc.support.com). Note Centera Collector-Manager is supported on Windows 2008.
SolutionPack for HP 3PAR StoreServ	- Port 2 A valid account with "browse" privileges to connect and access statistic data on the HP3PAR StoreServ2 (SSH) must be opened between the Watch4net collector and the HP 3PAR StoreServ Array - A valid account with "browse" privileges to connect and access statistic data on the HP3PAR StoreServ
SolutionPack for EMC Data Domain	Data Domain must be configured to allow the Watch4net collector host to communicate to it via SNMP. Utilize the following command on the Data Domain system to view the SNMP configuration: <pre># snmp show config</pre> Utilize the following command to add the Watch4net host: <pre># snmp add ro-community <public> hosts <watch4net.collector.com></pre> where <public> is the read-only community string
SolutionPack for Microsoft Hyper-V	- Hyper-V Collector Manager must have the right to query WMI objects from Hyper-Vhosts - PowerShell must allow the execution of unassigned PowerShell scripts
SolutionPack for Oracle Database	Refer to the EMC ASD Storage Resource Management W4N Prerequisite Checklist document for Watch4net for details on how to prepare the Oracle database. The latest JDBC driver jar file needs to be in the folder <pre>.../APG/Databases/JDBC-Drivers/Default/lib</pre> Currently the driver is needed is ojdbc5.jar
SolutionPack for EMC VMAX	VMAX Performance collection via EMC SMI Provider for VMAX: - Username - no default SMI Provider Username is provided during the deployment of SolutionPack for EMC VMAX but the EMC SMI Provider out-of-the-box username is admin - Password - no default SMI Provider Password is provided during the deployment of SolutionPack for EMC VMAX but the EMC SMI Provider out-of-the-box password is #1Password VMAX Performance collection via UniSphere for VMAX: - Username - the default is smc - Password - the default is smc

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 2 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 2 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 2 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 Primary 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 2 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/P 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 Atmos	In the Data Collection window: • In Atmos Node IP, type the Atmos system management node IP address. • In the Atmos System Administrator section, type the login credentials for the SysAdmin User. • In the Atmos Tennant section, type the login credentials for TenantAdmin User. • In Atmos CRT IP, type the Atmos Capacity Reporting Tool IP Address. • In Period to Collect Data, type the polling frequency.
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.

Table 2 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	• 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 49. • Select Use advanced settings to configure polling settings. • Click the plus (+) sign to add additional Centera devices. In the Reports window: • 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 Alert Consolidation, select the Primary Backend host. • 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 Hostname or IP address type the Primary Backend host. The default port is 2040. • 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

Table 2 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	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 Reports window: - In Administration Web-Service Instance, select the Frontend host.
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. - 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: <code>primary_backend:48443</code>. 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. - Click the plus (+) sign to add more hosts.
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.

Table 2 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
SolutionPack for EMC 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: • In Administration Web-Service Instance, select the Frontend host.
SolutionPack for EMC ViPR	In the Select the components to install window: • In Data Collection, select the Collector host. • In Events, select the Primary 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. • In Event server hostname or IP address, select the Backend host on which the events server is running. The default port is 22000. • Enter the friendly name, provide the IP address, username, and password of the ViPR instance.
SolutionPack for EMC VMAX	In the Select the components to install window:

Table 2 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	• 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: <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. • 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 50

Table 2 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	- In SYMAPI Connection name, type the connection name. This is the name of a netconfig file, not a host. To view the name that is configured, use the symcfg list -services 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 symcfg list command to view a list of arrays. - In Array Full Serial Number, type the Symmetrix SID from which data will be collected by Solutions Enabler or SMI-S. 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 Primary Backend 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 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.

Table 2 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	• 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: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 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. • 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:

Table 2 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	• 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. 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.

Table 2 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	• 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. • 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.

Table 2 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 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 HP StorageWorks P9000	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 StorageWorks P9000, type the HP StorageWorks 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 HP StorageWorks hosts. In the Reports window: • In Administration Web-Service Instance, select the Frontend host.
SolutionPack for IBM LPAR	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 2 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. In the ibm-lpar configuration window: - In HMC Hostname/IP, provide the hostname of the Hardware management console. - In Username, enter the username of the HMC. - In Password, enter the password of the HMC. In Advanced Setting, the polling interval of HMC is 3600 seconds by default. You can redefine the polling interval. Note The SolutionPack for SolutionPack for IBM LPAR depends on the reports and scripts of Physical Hosts SolutionPack.
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. - 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:

Table 2 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	• 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. 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.

Table 2 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 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 Hostname, provide the NetApp hostname. • In IP address, provide the IP address of NetApp Filer (7-Mode) or Cluster Management IP (C-Mode), depending on the mode selected. • In Port number, provide SSH port (default is 22). • In Username, provide the username of NetApp. • In Password, provide the password of NetApp. 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. • Optionally select the Enable property import for server enrichment checkbox. • In the Backend configuration section, type the host information and credentials for the Primary Backend Host.

Table 2 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	- 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 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

Table 2 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	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. • 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 webservices 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.

Table 2 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	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 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 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 Topology Service hostname or IP address, type 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 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 Primary Backend Host.

Table 2 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	- 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.
SolutionPack for XtremIO	In the Select the components to install window: - In Data Collection, select Data collection for XtreamIO. Recommended to be installed the host where collector is running. - In Reports, select EMC XtremIO Reports. Recommended to be installed on frontend host where tomcat is running. In the Data Collection window: Failover-Filter must be enabled, which is the default. HostName or the IP address to send data to must point to the host where the collector is installed (localhost in a one-VM deployment and collector host in a four-VM deployment). Network port to send data to must be set to the port to which the collected data will sent. Specify your Arbiter port or legacy Backend data port. If you have chosen a port other than 2020 for Arbiter, then the same port has to be configured in this field. The default port of 2020 is recommended. Enable alerting on data collected must be checked, which is the default. Alerting Backend hostname or IP address must point to the host where the collector is installed (localhost in a one-VM deployment and collector host in a four-VM deployment). Select the Primary Backend host. The default port is 2020 Alerting Backend data port must be set to the port on which alerts will be collected by the Primary Backend Host. 2010 is the default value. - In the section XtremIO configuration, enter the IP and credentials of the XtremIO array's Management IP address or hostname. - If the polling interval must be decreased, use Select Advanced Settings and enter a value between 900 (15 minutes) and 3600 (1 hour). - In Management IP address or hostname, type the management host.

Table 2 SolutionPack configuration details (continued)

SolutionPack	Configuration Details
	In Please select the credentials, select Add new credentials. Type credentials for the management 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 for EMC Atmos	You do not need to perform any additional configuration.
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	You do not need to perform any additional configuration.
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 <code>http://Frontend-Host:58080/device-discovery</code> .
SolutionPack for EMC ViPR	You do not need to perform any additional configuration.
SolutionPack for EMC VMAX	Refer to Configuring Solutions Enabler client access for VMAX on page 89 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	Configuration Details
SolutionPack for EMC VNX	To enable events reporting, edit your Web-Application configuration file (<code>APG.xml</code>), by uncommenting the <code>emc-vnx</code> section (uncomment the <code>ResourceLink</code> tag). You will then need to restart the Tomcat service in order to make the change effective. The Tomcat Catalina <code>APG.xml</code> file is located in: <code>/APG/Web-Servers/Tomcat/Default/conf/Catalina/localhost</code> 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 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 HP P9500	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 LPAR	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:

SolutionPack	Configuration Details
	- You may see a severe error: Failed to load properties for name [/cache.ccf]. 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 EMC 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: - Go to <code>/OPT/APG/bin</code> - Run the command <code>./manage-modules.sh service restart tomcat instance-name</code> To restart the backend service: - Navigate to Administration > Centralized Management > Physical View and select the host on which the backend is installed. - Select backend. The backend service details view appears. - Click Restart. If you reset the web service password, then you have to reconfigure the Storage Compliance SolutionPack as follows: - Navigate to Administration > Centralized Management > SolutionPacks > Storage Compliance. - Click  to reconfigure the <code>Compliance Backend SolutionPackBlock</code> instance. - Type the new password in the web service details section. - Click Reconfigure. - 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</code> directory - Edit <code>LunMappingDetection.pl</code> script.

SolutionPack	Configuration Details
	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</code> directory. - Edit <code>LunMappingDetection.ps1</code> script. - Set <code>powerPathPerformanceCollection=enabled</code>. Note By default, the <code>powerPathPerformanceCollection</code> flag is set to disabled. - To enable events reporting, - Edit your Web-Application configuration file (<code>APG.xml</code>), by uncommenting the <code>vmware-vcenter</code> section (uncomment the <code>ResourceLink</code> tag). - Restart the Tomcat service in order to make the change effective.
SolutionPack for XtremIO	You do not need to perform any additional configuration.

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 86](#).

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 50](#)

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.
Enabled	Symmetrix Authorization is configured. In this case, you must configure the <code>apg</code> 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 90](#)
 - b. [Adding client hosts to existing SYMAUTH configuration on page 91](#)
 - c. [Enabling client authorization on page 91](#)
 - d. [Validating Symmetrix access controls on page 92](#)

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 90](#).

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 91](#).
 - 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 90](#). For example:

```
assign user H:system_name\apg to role Admin;
```
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 91](#).

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 Admin;
```
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.

Limitation: some alerts not displayed

Storage Resource Management Suite fails to receive and display some alerts

If a trap is lost in the network communication, Solutions Enabler is not aware of the host and is not able to resend the lost information.

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 or modify the existing zone naming patterns:

Procedure

1. Add or modify the regex patterns in the following VFH xml files:

SolutionPack for Brocade FC:	/opt/APG/Collecting/Variable-Handling-Filter/brocade-fc-switch-sp-instance-name/conf/vhf-mds-zone-dns.xml
SolutionPack for CISCO MDS/Nexus:	/opt/APG/Collecting/Variable-Handling-Filter/Generic-SNMP-block-instance-name/conf/vhf-mds-zone-dns.xml

2. After modifying these xml files, restart either of the following:

- collection-manager service of SolutionPack for Brocade FC
- collection-manager service of Generic SNMP instance in case of SolutionPack for CISCO MDS/Nexus

How to add or modify zone naming patterns

Edit regex patterns in VFX XML files.

The regex patterns in the xml file is based on Java's regular expression format.

The following section of XML code needs to be added or modified for supporting new zone name patterns:

```
<regex-property name="zname" keep="true">
  <!-- <regex>(.)</regex>-->
  <!-- supporting hostname format (z_%h) -->
  <regex>^(z_) ([A-Z0-9a-z]+)$</regex>      <!-- zone member name
pattern -->
  <part name="hostname" value="{1}" /> <!-- hostname position in
the pattern -->
  <part name="createdBy" value="System" />
  <part name="devtype" value="PassiveHost" />
</regex-property>
```

The following examples explain how to read and interpret these patterns in simple terms:

Regex is <code>^(z_)([A-Z0-9a-z]+)\$</code> and hostname position is 2	Matches all the zone names that start with 'z_' and extracts the hostname from that matches the rest of the string that follows 'z_'
--	--

	Example: For zone name z_lingz099, the hostname extracted is lingz099.
Regex is <code>^([z_][A-Z0-9a-z]+)_([A-Za-z0-9]+)</code> and hostname position is 1	Matches all the zone names that doesn't start with 'z_' and extracts the hostname from zone name that is before the first underscore. Example: For lgloe111_1106, the hostname extracted is lgloe111.

For more information on writing Java's regular expression refer to <http://docs.oracle.com/javase/tutorial/essential/regex/>

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 95](#)
2. [Configure remote shell collector on page 95](#)

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"/>

```

## Policy Management

You can use default policies or create user-defined policies to analyze configuration changes in your data center for compliance and to detect breaches against these policies.

- ◆ [Creating a policy on page 26](#)
- ◆ [Enabling or Disabling a policy on page 28](#)
- ◆ [Editing a policy](#)
- ◆ [Copying a policy](#)
- ◆ [Deleting a policy](#)

### Creating a policy

Use the existing pre-defined templates to create a new policy or the empty policy template to customize it.

#### Procedure

1. Click **Operations**.
2. Under **Compliance**, click **Storage Compliance > Manage Rules & Policies**.
3. Click **Create Policy**.
4. Select a template from the **Select Policy from template** drop-down list.
5. Click **Description** and provide the following details:

| Field       | Description                 |
|-------------|-----------------------------|
| Policy Name | Type a name for the policy. |

| Field              | Description                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Policy Description | Type a brief description for the policy.-                                                                                       |
| State              | Select <b>Enabled</b> or <b>Disabled</b> from the drop-down list if you want the policy to run once it is created or otherwise. |

---

**Note**

If you choose the state as **Disabled**, you should manually enable the policy after creating the policy to run it.

---

6. Click **Scope**.
  - a. To create a new user-defined scope, click **Create Scope**.  
The **Create Scope** dialog box appears.
  - b. Provide the following details:

| Field    | Description                                                                                                                                                                       |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name     | Type a name for the scope.                                                                                                                                                        |
| Criteria | Type a criteria for the scope in the following format: <Property Name> <Operator> <Value>, such as; devtype = 'Array' & devicetype = 'FabricSwch' & parttype = 'port', and so on. |

---

**Note**

Some examples of well-defined properties that can be used in criteria are:

- For Switch: devtype = 'Objecttype', device = 'SwitchName'.
  - For Fabric: parttype = 'Fabric/VSAN', part = 'FabricName'.
  - For Array: serialnb = 'Array S/N', ip = 'IP Address', revision = 'Microcode'.
  - For Host: domain = 'Domain Name', devdesc = 'Operating System Version', pmodel = 'HBA Model'.
- 

---

**Note**

The **Criteria** allows the following operators: & (AND), I (OR), and= (Equal To) . You can also use wild card entry, such as, % for starts with, ends with, and contains expressions.

---

- c. Click **Show Members** to validate the criteria.  
The **Show Members** dialog box listing members with matching criteria appears. A warning message is displayed for invalid criteria.
- d. Click **Save**.  
The new user-defined scope is listed in the Scope table.

---

**Note**

Click **Show Members** to view the list of members associated with the scope.

---

7. Click **Rules**.
    - a. Click **Create Rule**.
    - b. Select a rule name from the drop-down list.
    - c. Double-click a rule to enable or disable it in the corresponding **State** column of the rule.
    - d. Double-click a rule to set the **Severity** to **Critical**, **Major**, **Minor**, or **Normal** using the drop-down list.
    - e. To provide criteria values for the rule, click **Criteria For Selected Rule** and select one of the following criteria and type a value in the corresponding text box:
      - Select the corresponding check box to enable the criteria or otherwise.
      - Select **LE** in the drop-down list to represent the Less than or Equal to value for the criteria.
      - Select **EQ** in the drop-down list to represent the Equal to value for the criteria.
      - Select **IN** in the drop-down list to represent the value(s) that the criteria contains.
- 

**Note**

You can type multiple values that are comma separated. The values can contain different patterns and need not be restricted only to strings.

---

**Note**

Rules validate objects when its *vstatus* value is active. The other objects are ignored.

---

- f. Click **Recommendation** to view the recommendation for the rule.
8. Click **Schedule**.
  - a. Select a **Schedule** option and specify appropriate values from the drop-down lists to run the policy at a scheduled time.
9. Click **Save**.

## Enabling or Disabling a policy

If you want the suite to run the policy after it is created, you must enable the policy. After enabling the policy, you can stop it any time by disabling it.

**Procedure**

1. Click **Operations**.
2. Under **Compliance**, click **Storage Compliance** > **Manage Rules & Policies**.
3. Right-click on a policy and select either:
  - **Enable** - To enable the policy to run.
  - **Disable** - To disable the policy.



# CHAPTER 7

## Suite Software Uninstallation

This chapter includes the following topics:

|                                                            |     |
|------------------------------------------------------------|-----|
| ◆ Overview.....                                            | 102 |
| ◆ Stopping core software services on a UNIX server.....    | 102 |
| ◆ Uninstalling core software from a UNIX server.....       | 102 |
| ◆ Stopping core software services on a Windows server..... | 102 |
| ◆ Uninstalling core software from a Windows server.....    | 103 |
| ◆ Uninstalling a SolutionPack.....                         | 103 |

## 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**.

