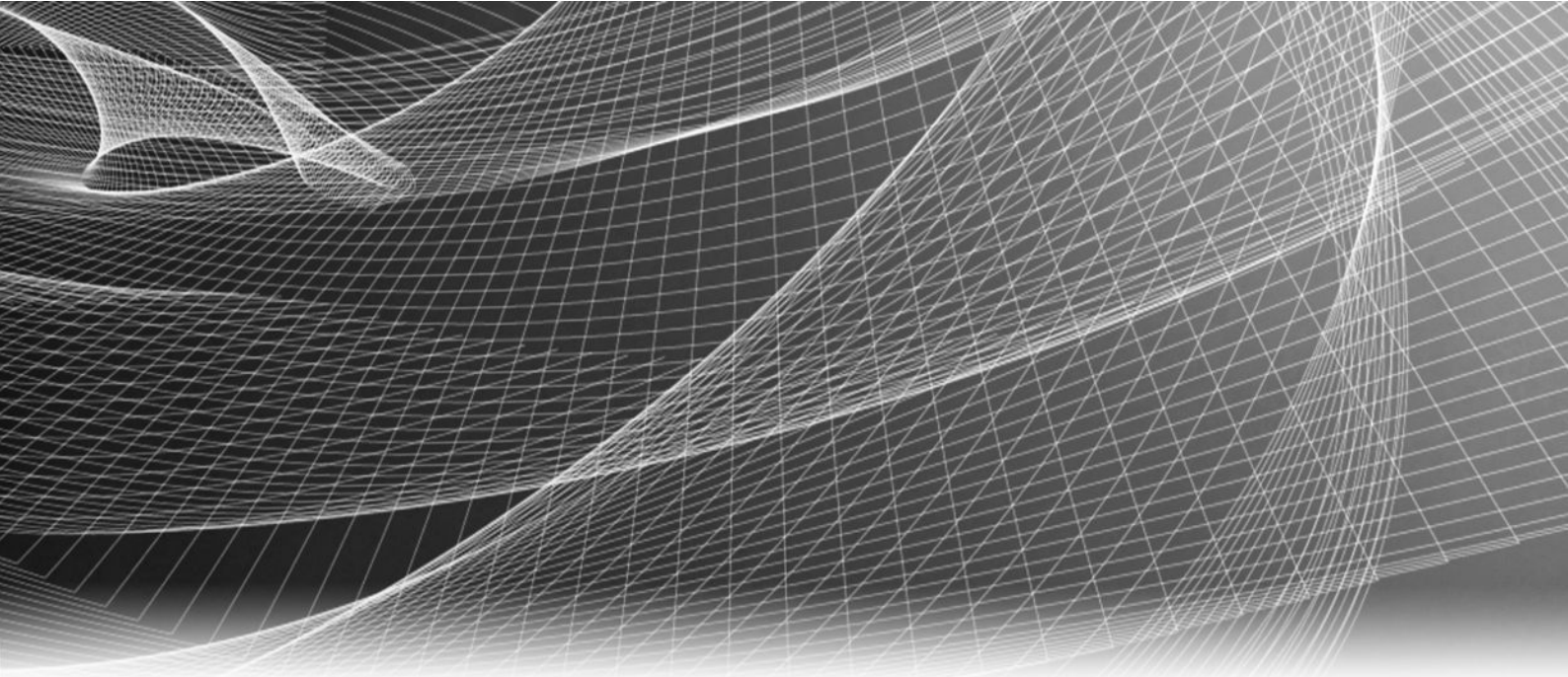




EMC[®] SolutionPack for Acme Packet SBC

Version 1.0

Installation and Configuration Guide

302-000-666

01

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

Published February, 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

Chapter 1	SolutionPack for Acme Packet SBC workflow	5
	SolutionPack workflow.....	6
	Support.....	6
	License management.....	6
Chapter 2	Installing the SolutionPack	7
	Installation.....	8
	Logging in to Centralized Management.....	8
	Installing the SolutionPack.....	8
	Adding devices for monitoring.....	9
	Log files.....	9
	Configuring the user process limits for the Linux installation.....	10
	Installing a SolutionPack Center Upgrade.....	10
	Uninstalling a SolutionPack.....	11
Chapter 3	Reports	13
	Viewing SolutionPack reports.....	14
	SolutionPack for Acme Packet SBC Reports.....	14
Appendix A	Metrics	17
	Report metrics	18
Appendix B	Troubleshooting	21
	SSL certificates.....	22
	SSL certificate error examples.....	22
	Troubleshooting an SSL certificate error: Accepting the exception....	23
	Installing a self-signed SSL certificate from an Internet Explorer browser.....	23
	Importing an SSL certificate into your truststore.....	23
	Exporting an SSL certificate from an Internet Explorer browser.....	24
	Contacting EMC Support.....	25

CHAPTER 1

SolutionPack for Acme Packet SBC workflow

This chapter includes the following topics:

◆	SolutionPack workflow	6
◆	Support	6
◆	License management	6

SolutionPack workflow

With this SolutionPack you can monitor and report on your Acme Packet devices to view performance and utilization information as well as inventory for all devices and other session metrics.

Use these guidelines in the following sections to prepare your environment for installation of the SolutionPack for Acme Packet SBC.

- ◆ Use support information to verify that prerequisite software is installed in your environment.
- ◆ Check that your Watch4net network configuration has the minimum requirements to run reports.
- ◆ Manage licenses for the SolutionPack

Support

This table lists the prerequisite support for this SolutionPack.

Device	Version
EMC Watch4net	6.3
Acme Packet Net-Net	9200 X
Acme Packet Net-Net	4500 X
Acme Packet Net-Net	4000 Series SBC X
Acme Packet Net-Net	3820 X
Acme Packet Net-Net	3800 X

License management

You can evaluate features in the SolutionPack Center using 30-day temporary licenses included with Watch4net software. If you install or plan to use the SolutionPack for longer than 30 days, contact EMC Online Support for permanent license files.

If you have an existing permanent license or a temporary license that requires updating, use the license upload feature in Watch4net Centralized Management. Both permanent and temporary licenses are distributed in .zip files.

The Watch4net license name is either Watch4net for Acme Packet SBC or ReportPack for Acme Packet SBC. If either license is present, the system will use it.

CHAPTER 2

Installing the SolutionPack

This chapter includes the following topics:

◆ Installation	8
◆ Logging in to Centralized Management	8
◆ Installing the SolutionPack	8
◆ Adding devices for monitoring	9
◆ Log files	9
◆ Configuring the user process limits for the Linux installation	10
◆ Installing a SolutionPack Center Upgrade	10
◆ Uninstalling a SolutionPack	11

Installation

Review this information before beginning the installation.

- ◆ Make sure you review and perform the prerequisites outlined in the first chapter.
- ◆ Perform the installation with administrative privileges on the Watch4net User Interface.

Logging in to Centralized Management

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

Procedure

1. Point your browser to the URL.

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

2. Log in.

- a. Type the login credentials.

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

- b. Click **Sign In**.

After you finish

Note

You are automatically logged off after four hours.

Installing the SolutionPack

After you log in as an administrator, you can install this 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). The recommended module update order varies. Refer to the EMC *Watch4net Installation and Configuration Guide* for information on module update order for multiple hosts or single host deployments.

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 Acme VoIP SolutionPack on 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 **Collector**, and **Reports** 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, verify the SolutionPack version number along with SolutionPackBlock information. Select **Centralized Management** › **SolutionPacks** › **Acme VoIP**.

Adding devices for monitoring

After installation, you must manually add devices for monitoring.

Before you begin

Procedure

1. Create the collector. In the Watch4net console, navigate to **Device discovery** › **Collectors** › **Add New Collector**.
2. Add a device for collection. Navigate to **Device discovery** › **Devices** › **Add New Device**.
 - a. In Main Parameters, enter the name of the device and IP address.
 - b. Configure SNMP Credentials by adding a collector that was previously created.
 - c. Select appropriate Acme Capabilities.

Repeat this procedure until all desired devices are added.
3. Distribute device(s). Navigate to **Device discovery** › **Dashboard**, and then click on **Distribute all approved devices with Capabilities on all enabled collectors**.

Log files

Information on the log files for this SolutionPack follows.

This SolutionPack does not have Acme Packet SBC-specific log files. Logging for the SolutionPack is part of the Generic SNMP collector: <APG_install>/Collecting/Collector-Manager/Generic-SNMP/logs.

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.
- ◆ 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
```

After restarting, check the status of services, enter: `./manage-modules.sh service status all`

5. Type the following command to verify the changes:

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

Installing a SolutionPack Center Upgrade

Periodically, updates of the SolutionPacks are available in a .zip file called SolutionPackCenter Update on EMC Online Support. This .zip file contains a README file that describes the changes made to each SolutionPack and individual `<solution>.pkg` files for installing each update.

Before you begin

- ◆ Install the required license file to enable your SolutionPack.
- ◆ Ensure any Domain Managers that supply data to the SolutionPack are installed and configured.
- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user `apg` is the account that the core software application uses instead of root.
- ◆ Update the core modules in all servers before you update or install a SolutionPack after upgrading your base installation.

Core modules are modules that are not installed by a SolutionPackBlock. Examples of core modules include `webapps`, `module-manager`, `license-manager`, `java`, `mysql`, `backend`, `tools`, and so forth. Update these core modules: **Databases, Backends,**

Frontends, Miscellaneous (except Blocks). Since the recommended module update order varies, refer to the Module Update Order section for the multiple hosts or single host deployments. Also, the *EMC Watch4net Centralized Management Guide* provides more information.

Examples of modules that are installed with SolutionPackBlocks include collector-manager, event-processing-manager, and collector or event components.

Procedure

1. Locate the Watch4net downloads area on EMC Online Support.
 - a. Go to <https://support.emc.com>.
 - b. Click **Support by Product**.
 - c. Type **watch4net** in the **Find a Product** field, and then click the arrow next to it.
 - d. Click **Downloads**.

The **Downloads for Watch4net** page appears.

2. Download the latest SolutionPackCenter Update to a local directory.
For example: SolutionPackCenter Update <month> <year>
3. Browse to **Administration** > **Centralized-Management** > **Packages Management** and click **Upload**.
4. Browse to the SolutionPackCenter Update .zip file and click **OK**.

After you finish

Update the SolutionPackBlocks after installing the SolutionPack update. Browse to **Administration** > **Centralized Management** > **SolutionPacks** > **SolutionPack Center** and install the SolutionPack.

You can confirm the SolutionPack version number by browsing **SolutionPacks** in the left panel.

Uninstalling a SolutionPack

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

Procedure

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

CHAPTER 3

Reports

This chapter includes the following topics:

- ◆ [Viewing SolutionPack reports](#)..... 14
- ◆ [SolutionPack for Acme Packet SBC Reports](#)..... 14

Viewing SolutionPack reports

You can view your reports from the Watch4net console.

Before you begin

After installing the SolutionPack, access the Watch4net User Interface.

Procedure

1. Point your web browser to `http://[serverIP:port]/APG`.
An example default URL is `http://localhost:58080/APG`.
2. On the login screen, enter your Watch4net username and password, and click **Sign In**.
3. View SolutionPack reports by expanding **Report Library** > *Your SolutionPack Name*.

SolutionPack for Acme Packet SBC Reports

A list of "out-of-the box" reports available with this SolutionPack appears in the table that follows.

You can drill-down on some top-level reports to view sub-level reports with specific metrics related to objects in the top-level report.

Top-level reports	Description
CPU Usage %	Lists the CPU Utilization (%) for each polled device.
Memory Usage %	Lists the Physical Memory Utilization (%) for each polled device.
Global active Sessions NB	Displays the total instant number of Global Concurrent Sessions as of report generation time.
Inventory	Displays the inventory for all devices that are Acme Packet Net-Net capable including: • Routers: number of routers • Interfaces: number of couple routers / interfaces • KPIs: number of Key Performance Indicators (KPI) polled by APG for each object
Router Summary	This report lists all Acme devices with their global performance information. Click a device to get a full summary of the performance of that device
Realms Performance	Includes: • Realm Sessions Active: The active sessions report includes the sum of the number of active inbound realm sessions and the number of active outbound realm sessions. • Realm Sessions Rejected: The Realm Sessions Rejected Ratio is calculated as a percentage of the sum of realm rejected (outbound and inbound) indicator that identify the total number of sessions rejected (outbound and inbound) due to insufficient bandwidth divided by the sum of total realm number of sessions.

Top-level reports	Description
	• Realm Sessions ASR%: This report displays the Answered to Seizures Ratio (ASR). This ratio is calculated as a percentage of total number of answered realm sessions by total number of seized realm sessions
Sessions Performance	Includes: • Sessions Active: This report displays the total active sessions by device. The total active sessions by device is the sum of active sessions for all sessions. The active sessions is the sum of the number of active inbound sessions and the number of active outbound sessions. • Sessions Rejected: This report displays the total active sessions by device which equals the sum of active sessions for all sessions. Active sessions equals the sum of the number of active inbound sessions and the number of active outbound sessions. • Sessions ASR %: The report displays the Answered to Seizures Ratio (ASR) The ratio is calculated as a percentage of total number of answered sessions by total number of seizures sessions • Registration Statistics

APPENDIX A

Metrics

- ◆ [Report metrics](#) 18

Report metrics

The SolutionPack software uses report metrics to gather information from your ACME Packet SBC devices for monitoring and report creation.

This table lists metrics for the SolutionPack.

Metric type	Table	Metric name	W4n Collection Mode
ACME Session	InboundActionNSEPSession		SNMP
	apCombinedSessionAgentStatsTable	InboundActive	SNMP
		OutboundActive	
		TotalInbound	
		InboundRejected	
		TotalOutbound	
		OutboundRejected	
		Seizures	
		Answered	
	apSigRealmStatsTable	InboundActive	SNMP
		OutboundActive	
		TotalInbound	
		InboundRejected	
		TotalOutbound	
		OutboundRejected	
		Seizures	
		Answered	
		Rfactor	
ACME-RESOURCES	apSysTable	ArpUtilization	SNMP
		ContactCount	
		CurrentLoad	
		GatewayCount	
		H323Count	
		MessagesRejected	
		NatUtilization	
		CurrentUtilization	CPU
		CurrentUtilization	Memory
		Health	

Metric type	Table	Metric name	W4n Collection Mode
		SessionCount	
		CallCount	
	apEnvMonFanStatusTable		SNMP
	apEnvMonPhyCardStatusTable		SNMP
	apEnvMonPowerSupplyStatusTable		SNMP
	apEnvMonTemperatureStatusTable		SNMP

APPENDIX B

Troubleshooting

- ◆ [SSL certificates](#) 22
- ◆ [Contacting EMC Support](#).....25

SSL certificates

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

[SSL certificate error examples on page 22](#) provides a list of sample errors.

Temporary resolution

Accept the certificate exception temporarily: [Troubleshooting an SSL certificate error: Accepting the exception on page 23](#).

Permanent resolution

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

You can:	Perform:
Install the self-signed SSL certificate that is provided with the EMC product using an Internet Explorer browser.	Installing a self-signed SSL certificate from an Internet Explorer browser on page 23
Install the self-signed SSL certificate that is provided with the EMC product using a Chrome or Firefox browser.	1. Export the self-signed SSL certificate to save it to the export location: Exporting an SSL certificate from an Internet Explorer browser on page 24 2. Importing an SSL certificate into your truststore on page 23
Import an exported SSL certificate that you or another administrator prepared.	Importing an SSL certificate into your truststore on page 23

If you need to prepare an SSL certificate to share with other users, use: [Exporting an SSL certificate from an Internet Explorer browser on page 24](#).

SSL certificate error examples

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

Chrome error examples

This site's security certificate is not trusted!

Or, a blank pane.

Firefox error example

This Connection is Untrusted

Internet Explorer error examples

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

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

Troubleshooting an SSL certificate error: Accepting the exception

An SSL certificate error appears in your browser.

To resolve this issue,

Procedure

- ◆ Accept the exception.

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

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

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

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

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

Procedure

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

After you finish

Refresh the browser window.

Importing an SSL certificate into your truststore

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

Procedure

- ◆ Import the certificate using one of the following procedures:
 - [Importing an SSL certificate in Chrome on page 23](#)
 - [Importing an SSL certificate in Firefox on page 24](#)
 - [Importing an SSL certificate in Internet Explorer on page 24](#)

Importing an SSL certificate in Chrome

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

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

Procedure

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

Importing an SSL certificate in Firefox

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

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

Procedure

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

Importing an SSL certificate in Internet Explorer

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

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

Procedure

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

Exporting an SSL certificate from an Internet Explorer browser

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

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

Procedure

1. Access the host for which you want to export the SSL certificate from the browser.
For example: `https://<myHostname>.emc.com`
2. Select **Continue to this website (not recommended)** in the **There is a problem with this website's security certificate** window.
3. Click the red **Certificate Error** indicator next to the address bar.
4. In the **Untrusted Certificate** window, select **View certificates**.
5. In the **Certificate** dialog box, select the **Details** tab and ensure that the Show field is set to All. Click **Copy to File**.
6. In the **Certificate Export Wizard**,
 - a. Click **Next** in the **Welcome** screen.
 - b. Click **Next** to accept the default DER encoded binary X.509 setting in the **Export File Format** screen.
 - c. Browse to the location where you want to save the certificate.
 - d. Specify the certificate file name and click **Save**.
 - e. In the **File name** field, ensure that the location and the certificate file name are correct. Click **Next**.
 - f. Click **Finish**.
 - g. Click **OK** when The export was successful appears.
7. In the **Certificate** dialog box, click **OK** in the **Details** tab.
8. Share the resulting exported SSL certificate with other users to use.

Contacting EMC Support

EMC support, product, and licensing information can be obtained through EMC online support.

Procedure

- ◆ For documentation, videos, release notes, software updates, or information about EMC products, go to EMC Online Support at <https://support.emc.com>.
- ◆ For technical support, go to EMC Online Support and click **Service Center**.
You must have a valid support agreement to open a service request.
- ◆ Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

