Article

Service Assurance Suite

Release number 9.4

How To Set Up SAM, EMC M&R, and Smarts SolutionPack

January, 2015

- Overview 2
- Workflow for setting up SAM 3
- Workflow for setting up EMC M&R 6
- SSL setup for SAM and EMC M&R 12

EMC²

Overview

Service Assurance Suite combines some of the best features of Service Assurance Manager and EMC M&R to provide a common interface for viewing Notifications and reports on historical events. You must install and configure EMC Service Assurance Manager (SAM), EMC M&R, and the SolutionPack for EMC Smarts before you can view notifications or reports from the EMC M&R Report Library.

When EMC M&R platform and the SolutionPack for EMC Smarts are deployed with Service Assurance Manager, these features may be accessed from the EMC M&R interface:

- Notifications
- Reports showing geographical representation of Smarts network devices, physical inventory of device groups, and a physical inventory of the IP network
- IP Configuration Manager settings such as polling and thresholds
- Discovery and topology settings for underlying domain managers

In addition, the EMC Smarts Failover System now supports failover of the services used to communicate between Service Assurance Manager and EMC M&R platform. The *EMC Smarts Failover System User Guide* provides more information.

The order in which you install SAM and EMC M&R does not matter. But the licensing and configuration of both products must be completed and the services for both products must be installed and running before you install the SolutionPack for EMC Smarts.

Additional information is described in these documents:

- *EMC M&R Installation and Configuration Guide*
- *SolutionPack for EMC Smarts Summary Sheet*
- *How to Maintain IP Manager Settings*
- *Troubleshooting the Deployment of SAM, EMC M&R, and the SolutionPack for EMC Smarts*

Resource allocation for SAM and EMC M&R

Ensure you dedicate resources (4CPU, 16GB) to SAM and also to the EMC M&R servers.

Typically, EMC M&R deployment is divided among different virtual machines (Backend, Frontend, Collector, and so forth). Ensure that sufficient memory and CPU are available in the virtual machine. Otherwise the system will fail.

Port configuration between SAM and the SolutionPack for EMC Smarts

When you install the SolutionPack for EMC Smarts, you must configure the ports between EMC M&R and the server hosting the Smarts EDAA (EMC Data Access API) to ensure communication across the firewalls.

The default port for the Smarts EDAA is 8080 (8443 in SSL mode). However, this port can be configured manually. If EMC M&R (with SolutionPack for EMC Smarts) and SAM are installed on different hosts, you must open the access to the EDAA port. Additionally, the Smarts Collector used by the SolutionPack connects to the Smarts Domain Manager servers via the ports they are started on. You must open a range of ports, including the Broker, in order for data to pass between the Smarts domains and EMC M&R.

Workflow for setting up SAM

Configure the Presentation Service Assurance Manager (SAM-PRES) server to communicate with the SolutionPack for EMC Smarts installed on the EMC M&R platform.

During SAM installation you have a choice between two SAM services:

- EMC Smarts Service Assurance Manager Server (Notification Cache Publishing)
  - Start the Presentation SAM server with the EMC Smarts Service Assurance Manager Server (Notification Cache Publishing) service if you plan to integrate EMC M&R with this installation. When the SAM server is started with this service, SAM communicates with both EMC M&R and Smarts analysis domains.
- EMC Smarts Service Assurance Manager Server
  - Start Aggregation-level SAM servers with the EMC Smarts Service Assurance Manager Server service in environments with hierarchical SAM configurations.

One Presentation SAM server may be configured to work with one SolutionPack for EMC Smarts. By default, the SolutionPack for EMC Smarts connects to the Smarts Broker. When installing or updating the SAM software, you must enable Notification Cache Publishing so that notifications will flow into EMC M&R. Notification Cache Publishing enables SAM to publish its notifications to the Notification Cache. The Notification Cache is a separate collection of components, including RabbitMQ, ElasticSearch, and two webapps running under Tomcat (Ingestion and the Alert EDAA). Services for all of these components must be installed and running before notifications display in the EMC M&R User Interface.

Note

Both Smarts Web Console and the SAM Tomcat Server use the same default port (8080). If installing both on the same machine, change the port for one of them.

---

1. Ensure the Presentation SAM server has been upgraded to the latest version of the Service Assurance Suite. Select these options:
   - Under **Core Services**, select **EMC Smarts Broker** if you plan to run the Broker from the Presentation SAM server. If you run the Broker from another server, make note of the Fully Qualified Domain Name (FQDN) of the server.
   - Under **Service Assurance Manager Services**, select **EMC Smarts Service Assurance Manager Server (notification cache publishing)**
   - Under **EMC Data Access API**, select all of the entries:
     - **EMC Smarts Data Web Applications (Tomcat)**
     - **EMC Smarts Data Web Applications (Tomcat)**
     - **EMC Smarts Notification Exchange (Rabbit MQ)**
     - **EMC Smarts Notification Cache (ElasticSearch)**
   - Enter the port for the Broker service.
2. Configure your SAM license using smarts.lic or the license server.
3. Add the parameter, `SM_CAS_SERVER`, to the `runcmd_env.sh` file in the Presentation SAM server. `SM_CAS_SERVER` is the URL that identifies the EMC M&R Tomcat server host, and it has to specify the protocol and port used to log into EMC M&R. Example: `SM_CAS_SERVER=http://smartslin03.svtdomain.us.dg.com:58080`. You must use the `SM_CAS_SERVER` entry to connect to the EMC M&R server.

Note

The entries in the Reports configuration screen of the SolutionPack for EMC Smarts must match the values in `SM_CAS_SERVER`. In the example above:

- Set `EMC M&R tomcat hostname or IP address` to `www.smartslin03.svtdomain.us.dg.com`
- Ensure `EMC M&R tomcat port number` matches the port specified in `SM_CAS_SERVER` (58080 in the example)
- If using a secure protocol (https) in the `SM_CAS_SERVER` URL, ensure the `HTTPS enabled` is checked
- Ensure the Frontend server in the Physical Overview uses the same naming convention (You must use the FQDN across all field entries.)
- Use the FQDN, not the IP address, for hostnames; otherwise CAS (Central Authentication Service) will not work properly.

4. Set the `SM_TOMCAT_SERVER` parameter in the `runcmd_env.sh` file of the Presentation SAM server to specify the Fully Qualified Domain Name (FQDN) of the SAM Tomcat server. Example: `SM_TOMCAT_SERVER=http://<hostname.com>:8080`. This `SM_TOMCAT_SERVER` entry must match the name and port values in the **Smarts EDAA host name or IP address** and **Smarts EDAA port number** fields of the Reports configuration block in the SolutionPack for EMC Smarts.
5. Start the services. (Start the Broker service before starting the Tomcat service in your Presentation SAM installation.)
6. Issue the `sm_service show` command to ensure these services associated with the Presentation SAM installation are running:

Service name	Description of feature
`ic-broker`	Broker connected to Presentation SAM server
`ic-sam-server-pres`	SAM server with Notification Cache
`smarts-tomcat`	Smarts EDAA (controlled by Tomcat server)
`smarts-rabbitmq`	Rabbit MQ
`smarts-elasticsearch`	Elastic Search

7. When connecting to domain managers running pre-9.4 versions of Service Assurance Suite software, add two parameters that control security settings to the `runcmd_env.sh` file in the Presentation SAM server:
   - `SM_TLS_PROTOCOLS=+TLSv1.1`
   - `SM_ALLOW_LEGACY_CRYPTO=TRUE`

Note

When upgrading from older versions of SAM to version 9.3 or higher, you must manually register and start the SAM Notification Cache service (INCHARGE-SA-PRES). Command syntax for registering the SAM Notification Cache service on page 5

Command syntax for registering the SAM Notification Cache service

After an upgrade of older SAM software to version 9.3 or higher, you must register the SAM Notification Cache service and start it manually if you intend to use the SolutionPack for EMC Smarts to view notifications from the EMC M&R User Interface.

Register the SAM Notification Cache service

```
sm_service install --force  --unmanaged  --startmode=runonce '--
name=ic-sam-server-pres' '--description=EMC Smarts Service Assurance
Manager Server (notification cache publishing)' '/opt/InCharge/SAM/
smarts/bin/sm_server' '-n' 'INCHARGE-SA-PRES' '--config=ics' '--
port=0' '--edaa=sam-presentation/2.0' '--bootstrap=bootstrap-
amqp.conf' '--ignore-restore-errors' '--output'

sm_service show --cmdline ic-sam-server-pres
```

Start the SAM Notification Cache service

From the `SAM/smarts/bin` folder, issue the command, `sm_service start ic-sam-server-pres`

Check on status of running services

```
sm_service show
RUNNING ic-broker
RUNNING ic-sam-server-pres
NOT RUNNING ic-mbim-server
RUNNING smarts-tomcat
RUNNING smarts-rabbitmq
RUNNING smarts-elasticsearch
NOT RUNNING ic-sam-server
```

Smarts ElasticSearch service syntax for manual startup

```
smarts-elasticsearch
/opt/InCharge/SAM/smarts/bin/sm_service install --force
--unmanaged --startmode=runonce
--name=smarts-elasticsearch
--description=”EMC Smarts Notification Cache (ElasticSearch)”
/opt/InCharge/SAM/smarts/bin/sm_elasticsearch
--ignoreme
```

EMC Smarts Notification Exchange (Rabbit MQ) service syntax for manual startup

```
/opt/InCharge/SAM/smarts/bin/sm_service install --force
--unmanaged --startmode=runonce
--name=smarts-rabbitmq
--description=”EMC Smarts Notification Exchange (Rabbit MQ)”
/opt/InCharge/SAM/smarts/bin/sm_rabbitmq
--ignoreme
```

EMC Smarts Data Web Applications (Tomcat) service syntax for manual startup

```
/opt/InCharge/SAM/smarts/bin/sm_service install --force --unmanaged --
startmode=runonce
--name=smarts-tomcat'
--description=”EMC Smarts Data Web Applications (Tomcat)”
/opt/InCharge/SAM/smarts/bin/sm_tomcat
--ignoreme
```

Server tool limitations in the EMC M&R User Interface

Only server tools available from the Presentation SAM server may be invoked from the EMC M&R User Interface.

In a hierarchical SAM deployment, server tools that need to be executed at the Aggregate Sam (SAM-AGG) layer will fail if they rely on communication with an underlying Smarts domain manager. When the server tool executes a script, it will still work at the Aggregate SAM level (for example, the LSP Ping server tool in MPLS or the Remedy Adapter).

If your server tool is not working as expected, you may need to edit the ASL scripts to invoke the SAM-AGG layer to work around this problem.

Workflow for setting up EMC M&R

1. Install or upgrade to the latest version of EMC M&R. The *EMC M&R Installation and Configuration Guide* provides more information.
2. Start the services. For example, `/opt/APG/bin/manage-modules.sh service start all`
3. New installations of EMC M&R provide a 30-day trial license for all SolutionPacks. Ensure you obtain and install permanent licenses for SolutionPacks you plan to use longer than 30 days.
4. Install the SolutionPack for EMC Smarts.
   The article, *SolutionPack for EMC Smarts Summary Sheet*, provides more information.
   - On the Reports page of the SolutionPack installation wizard, you must enter the Fully Qualified Domain Name (FQDN) of the EMC M&R Tomcat server. This address must match the entry in the `SM_CAS_SERVER` parameter setting in the `runcmd_env.sh` file in the Presentation SAM server.

     Note

     Use the FQDN, not an IP address, when configuring the SolutionPack for EMC Smarts.

   - Enter the FQDN for the server hosting the Smarts EDAA.
   - Accept the default values for the other fields unless your deployment has a non-default SAM setup. For example,
     - SAM Presentation server is not named `INCHARGE-SA-PRES`
     - SAM server is using SSL
     - The admin-profile in SAM has changed
   - On the Reports page of the SolutionPack installation wizard, enter the Smarts Configuration Manager domain name if you plan to manage settings for your IP domains from the EMC M&R interface.

   After installation of the SolutionPack for EMC Smarts, configure IP settings in the Configuration Manager and push them to the remote IP domain managers. Access the IP settings from **Administration** › **Modules** › **Smarts**. Additional information is provided in this article:

   - *How to Maintain IP Manager Settings*

5. Create user accounts for operators in EMC M&R. The Administrator must also create new Roles for these users and map them to existing profiles in Service Assurance Manager (SAM).
6. Hide the ViPR SRM-related report nodes in the navigation tree if you do not plan to install ViPR SRM. (The Smarts-related nodes are under **Network** in the tree.)
7. Run manual Topology import from **Administration** › **Centralized Management** › **Scheduled Tasks** › **Topology**. Click **sm-collector/import-smarts-topology** and click **Run**.
   By default the task runs every day at midnight.

User management for SolutionPack for EMC Smarts

In order to manage notifications from the SolutionPack for EMC Smarts, the Administrator must set up users and roles in EMC M&R that correspond to the profiles set up in Service Assurance Manager (SAM).

In the SAM Global Manager Administration Console, the Administrator configures profiles that define which Notifications, Actions, and Tools are available to each group of users (for example, OPER profile and so forth).

The Administrator providing access to SolutionPack for EMC Smarts views has to create users and roles in EMC M&R that reflect the characteristics of the SAM profiles that are in use.

If Administrators need to restrict Notifications, Actions, or Tools available to a user in EMC M&R, they need to define the restrictions first in the corresponding SAM profile.

Note

The Administrator should not duplicate EMC M&R users in SAM unless a user needs access to both the SolutionPack for EMC Smarts views and classic SAM Consoles. Users working only in EMC M&R need only the user login and role definition created in EMC M&R.

Set role restrictions for non-administrator users of SolutionPack for Smarts

If you want additional user roles, such as oper (operator), or profiles configured in your Presentation SAM server, you must set role restrictions after installing the SolutionPack for Smarts.

The default role is assigned to administrator. Add additional roles as needed.

Procedure

1. From **Administration** › **Roles**, click **New Role**.
2. Click **Modules & Restrictions Access** and expand the **Smarts** module.
3. Add an existing smarts profile (such as `oper-profile` or `default-profile`) and click **Save**.
4. From **Administration** › **Users**, create a new user and assign them the role.

SAM user profile mapping and EMC M&R role-based access

After you set up the user profiles and assign them to roles in EMC M&R, the administrator must associate those profiles and roles with users who need to access both Service Assurance Manager (SAM) Consoles and the EMC M&R User Interface.

Administrator profile behavior

The EMC M&R administrator role is mapped to the EMC Smarts Admin profile when the SolutionPack for EMC Smarts is installed.

Note

If you try to assign a SAM profile to the EMC M&R Admin user, that SAM profile will be overwritten with the EMC M&R profile.

User profile behavior

The administrator can assign a SAM profile to an EMC M&R non-administrator user from **Administration** › **Modules & Restrictions Access** › **Smarts**.

- Ensure you assign an existing SAM Profile to the user, (for example, oper-profile, default-profile, and so forth)
- Do not assign more than one Role with a SAM Profile to a user.

Hide unused entries in the navigation tree

You can hide default entries in the navigation tree if you have not installed the products that populate them with data.

Before you begin

The default EMC M&R platform displays nodes such as **Operations**, **Explore**, **Dashboards**, and **Planning** in the navigation tree. Other product suites that also use EMC M&R as their platform display entries under these nodes by default. However, no data populates these entries unless you are using those products. The SolutionPack for EMC Smarts populates data in the **Network** block under **Operations**, **Explore**, and **Dashboards**.

Procedure

1. To hide entries in the navigation tree, click **Edit Mode** from the EMC M&R User Interface.
2. Find the storage-related blocks in the list and select, **Always Hide**.

   Do not hide the **Network** block under the **Operations**, **Explore**, or **Dashboards** nodes. The **Network** block contains all of the SolutionPack for EMC Smarts views and reports. The **Planning** node is not used by the SolutionPack for EMC Smarts.

Viewing notifications from the EMC M&R User Interface

Launch Object Details from the Notifications view.

Before you begin

You can view notifications coming from the Presentation SAM server in the EMC M&R User Interface.

Procedure

1. To view Notifications where an element name is collected, launch the Object Details report with map, details, containment, and so forth.
2. To view Notifications with an element name that is not collected by the SolutionPack for EMC Smarts, launch only the Details view.

   The SolutionPack for EMC Smarts does not collect every class and instance that exists in the Smarts domains. It selects "top level" classes like Routers, Switch and some of their underlying components.

Troubleshooting an empty notification list

After creating a new Notification List in Service Assurance Manager, the notifications are not visible in the EMC M&R User Interface.

When you create a new Notification List in Service Assurance Manager, you must issue this command to have notifications populate the correct reports in EMC M&R. This command ensures notifications are re-cached so they display in the correct Notification List.

Issue this command from the Presentation Service Assurance Manager ‹*install_directory*› \SAM\smarts\bin folder: `dmctl> invoke ICS_NLManager::ICS-NLManager renotifyAllEvents`

Creating client tools

Client tools are programs the operator invokes by right-clicking on a notification.

The default client tool, **Launch EMC M&R**, launches the EMC M&R home page. You can create others by editing the `SmartsTools.json` file.

Note

You cannot call other scripts using client tools.

Procedure

1. To create client tools, log in to **Centralized Management** and expand **Logical Overview** › **Miscellaneous** › **Custom**.
2. Click **Webapps-Resources::Default** and expand the list of Configuration files.
3. Select the checkbox for `/conf/SmartsTools.json` and click the pencil icon to edit the file.

   Use this file to add or modify options that appear in the Notifications **Client Tools** right-click menu. You can edit the tool to launch any URI and pass in any notification property as a parameter by surrounding it with brackets.

   You must encode `&` characters as `%26`.

   Column headers which are available in Notifications can be passed as arguments to the URI. The various notification properties that can be used are Acknowledged, Active, Category, Certainty, ClassName, ClassDisplayName, ClearOnAcknowledge, ElementClassName, ElementName, EventText, EventName, EventState,EventType, EventDisplayName, FirstNotifiedAt, Impact, InstanceName, IsProblem, IsRoot, InMaintenance, LastClearedAt, LastNotifiedAt, LastChangedAt, Name, NotificationID, OccurrenceCount, Owner, Severity, SourceDomainName, SourceEventType, TroubleTicketID, UserDefined 1 to 20.

   Example client tool:

```
{
         "name": "Example 1",
         "url": " http://www.emc.com/?class={ClassName}
%26source={SourceDomainName}"
        },
```

   In this example, `"name":"Example 1"` is the name which appears on the sub-menu for the right click action on the notification. This causes the text, "Example 1" to display. When you right-click on a Notification, you will see **Client Tools** › **Example 1**.

In this example, `"url": " http: //www.emc.com/?class={ClassName}%26source={SourceDomainName}"` provides the URL to which a notification attribute can be appended as a parameter. In this example, ClassName and SourceDomainName are used. When invoked, this tool would launch, `http://www.emc.com/?class=Host&source=INCHARGE-AM-PM`.

Additional files that may be used when creating client tools include `conf/common.properties` and `mib-browser/mib-browser.xml`.

Enrich device location data in Smarts geographical maps

The Smarts geographical map (geomap) shows the location of Smarts-enabled devices in the network. Before viewing Smarts geomaps, perform data enrichment of the device locations to provide more details in the map.

Before you begin

Ensure device discovery has finished and devices display in the user interface before enriching the location data. Look in the **Explore** › **Network** tree to view the discovered devices. The **Location** attribute of the device object in Smarts IP Manager populates the **Device Location** dropdown after discovery.

The *APG-Centralized-Management-Guide*, found in the `/APG/Doc` folder in your EMC M&R installation, provides additional information.

Procedure

1. Register the Collector Manager module with the hostname of the EMC M&R installation.
   a. From **Centralized Management** › **Data Enrichment**, click **Register** for New Module.
   b. Click **‹hostname›** in the first column.
   c. Click **Collecting** in the second column.
   d. Click **Collector Manager :: emc-smarts :: DataEnrichment** in the third column.

      Do not select any other modules from the list. They are not required for geomaps.
2. Select **Collector Manager :: emc-smarts :: DataEnrichment** and click **geo-map-enrichment**.

   The DataEnrichment property is used to enrich the values in **Device Location** to match meaningful values in the **smlocale** column.

   a. Find the columns for **Device Location** and **smlocale**.

      By default the first row displays `@MATCHALL` for **Device Location** and `@NULL` for **smlocale**.
   b. Replace the default values with meaningful names, for example, **`*white`**, in **Device Location** can map to **`White Plains, New York`** for the **smlocale** value.

      Enter a valid **smlocale** name which will be identifiable on the geomap.

      The **Device Location** dropdown menu displays accurate data only after device discovery has finished. For example, typing **`'w'`** displays all locations having names with **`'w'`**. Typing **`*`** displays all locations.
   c. Save the changes.
   d. Click **Update** in the **Save Data Enrichment** window.

   All values in the dropdown windows must be enriched to get all locations in the geomap.

To add a new row for enrichment, right-click the icon appearing in front of the row. This gives options to **Insert Before**, **Insert After**, or **Delete** a row.

3. Restart the Database and Backend.
   a. Go to **Centralized Management** › **Scheduled Tasks**.
   b. Click **Select All**.
   c. Uncheck the **Update Online** option.
   d. Click **Run now** to restart the Database and Backend.
4. Restart the EMC M&R services.

   This restarts the Collector Manager.

   After some time, the Smarts Geography geomap will be uploaded to **Dashboard** › **Network** › **EMC Smarts Geography**. Click the icons on the map to view devices present at that location.

Alternate method of data enrichment using file import

Use the Import/Export function in the UI to import CSV or XLS files with Device Location and smlocale mapping as an alternative method of enriching Smarts geomap data.

The XLS or CSV files must have two columns of values in the same order as the columns mentioned in data enrichment. Here is an example:

Table 1 Sample data enrichment import file column layout

Device Location column data	smlocale column data
white*	White Plains, NY
10;PUGET SOUND;United States;REDMOND, WA;11	Redmond, Washington
Westchester Ave	White Plains, NY
LOCATION	Bangalore, India
EMC E-Labs Building 119	Bangalore, India
Hopkinton	Hopkinton, MA
DevLab, row 2-rack 2, 44 S Broadway, 7th floor	Bangalore, India
10.3.2	Delhi, India
Chicago, IL	Chicago, IL

Although the value, *‹city›*, is enough for **smlocale** to render points in the map, enter *‹city, state›* or *‹city,country›* to avoid duplicates or conflicts. Ensure the location name is valid because it will display in the maps report.

Map reports

A map report is basically a standard table report where each child node displays as a point in a geographical map. You can edit the location and the name of the location as well as the size, color, and shape of marker displayed on the map.

In **Report Type** on the **Report Configuration** tab, you select the map report from the miscellaneous section.

You can edit the following attributes on a map report:

- **Location** locates an element on the map.
- **Name** provides a name to a location, such as device name, region, and sitename.
- **Size** sets the size of the marker. The size of the marker is based on a given metric value, such as the number of devices at the site.
- **Color** sets the color of the marker. The color relies on the threshold definition where green represents no thresholds, yellow represents a major threshold, and red represents a critical threshold.
- **Marker** sets the shape of the marker, such as circle, square, triangle, inverted triangle, pentagon, and sector.

Switch between OpenStreetMap and Google Maps

OpenStreetMap is used as the default platform mapping software. Use this procedure to configure EMC M&R to use other mapping software, such as Google Maps.

Procedure

1. To switch from OpenStreetMaps (osm) to Google Maps (google), navigate to `APG/Web-Applications/APGFrontend/APG/conf/common.properties`.
   a. Add these lines to `common.properties`:

   ```
   #==========================================================
   Setting for Google Maps (client-side)
   #==========================================================
   apg.maps.geocode=false
   apg.maps.provider=google
   apg.maps.geocoder=google
   ```

   b. Restart all managed module services including tomcat.
2. To switch back to OpenStreetMaps from Google Maps
   a. Comment the lines of code you added to `common.properties` file to disable them.
   b. Restart all managed module services including tomcat.

SSL setup for SAM and EMC M&R

Adjust the port and protocol settings when enabling SSL encryption in SAM and EMC M&R.

The procedures for SSL setup assume use of the Java Keytool. You may, optionally, use a different encryption tool.

This keytool generates keystore files in the location where the commands are issued. For these SSL procedures, the following assumptions are made:

1. When configuring EMC M&R (Watch4net) with CLI commands, issue the commands from the `bin` folder of the installation path. For example, `/opt/APG/bin` or from `c:\Program Files\APG\bin`.
2. When configuring Service Assurance Manager (SAM) with CLI commands, issue the commands from the base directory path. For example, `/opt/InCharge/SAM/smarts` or from `c:\Program Files\InCharge\SAM\smarts`.
3. Both EMC M&R and SAM installations include versions of Java. Check to ensure the correct versions of Java are in use in both the EMC M&R server and in the SAM server. Java is usually installed into the `...usr/bin` path. (The versions may differ between EMC M&R and SAM.)

Workflow

1. Edit the Reports configuration settings in the SolutionPack for EMC Smarts to adjust port and protocol settings.
2. Generate the SSL certificate for the EMC M&R (Watch4net) server where the Tomcat server is running. The Java documentation provides details.
3. Generate the SSL certificate for the Service Assurance Manager (SAM) server where the Tomcat server is running. The Java documentation provides details.
4. Ensure the configuration settings have been adjusted for SSL. For example, check the **SM_CAS_SERVER** and **SM_TOMCAT_SERVER** settings in the `runcmd_env.sh` file in SAM and edit the settings to add the secure port numbers and change the protocol from `http` to `https`. (When you change runcmd_env.sh, you must stop and restart the SAM service. For example, `sm_service stop|start ic-sam-server-pres`)
5. Enable the `https` protocol in the `server.xml` files in both the SAM and EMC M&R deployments. Add the `Http11Protocol` and `Http11NioProtocol` sections if missing from the `server.xml` file.
6. Export the EMC M&R certificate and import to the SAM server.
7. Export the SAM certificate and import to the EMC M&R server.
8. Stop and start the SAM Tomcat server.
9. Restart the EMC M&R Tomcat server.

Linux SSL Setup

Enable SSL port and protocol settings in SolutionPack for EMC Smarts

When enabling SSL, you must edit the Reports configuration of the SolutionPack for EMC Smarts and ensure use of secure port and protocol settings.

Before you begin

This procedure assumes the SolutionPack for EMC Smarts is already installed and running. If not, the *SolutionPack for EMC Smarts Summary Sheet* article provides installation instructions.

Edit the Reports configuration page to enable SSL for the SolutionPack for EMC Smarts. Access this page from **Centralized Management.** Expand **SolutionPacks** › **Infrastructure** and click **EMC Smarts**.

Procedure

1. Click the **Pencil** icon by the Reports SolutionPackBlock.

   The Reports reconfiguration page appears.
2. Expand Tomcat Configuration and choose **Add a new Tomcat configuration** in the dropdown box.
3. Click the checkbox for **HTTPS Enabled for EMC M&R and Smarts**.
4. Enter the Fully Qualified Domain Name or IP address of the EMC M&R Tomcat server.

   This name must match the host name portion of the entry in **SM_CAS_SERVER** in the Presentation SAM `runcmd_env.sh` file. Ensure consistent use of either IP address or FQDN in all of the field entries. Do not mix the entry formats.
5. Enter the secure port for the EMC M&R Tomcat server. (Default SSL port is 58443).

6. Expand the Smarts and Alerts EDAA Configuration and choose **Add a new Smarts and Alerts EDAA Configuration** in the dropdown box.

   Check the entry in the **Smarts EDAA hostname or IP address** field. This entry must match the host name portion of the entry in **SM_TOMCAT_SERVER** in the Presentation SAM `runcmd_env.sh` file.

7. Enter the secure port for the Smarts EDAA server. (Default SSL port is 8443).
8. Adjust other entries if needed and then click **Reconfigure**.

After you finish

Continue with the SSL certificate generation, import, and export steps. The changes will not take effect until the Tomcat servers are restarted in both SAM and EMC M&R.

Linux: Generate the keystore file for EMC M&R

Create the keystore file for the EMC M&R host. This file stores the tomcat server's private key and self-signed certificate.

Before you begin

Stop the EMC M&R Tomcat service. For example, `opt/APG/bin/manage-modules.sh service stop tomcat`

Procedure

1. Generate the keystore: `/opt/APG/Java/Sun-JRE/7.0u51/bin/keytool -genkey -alias tomcat -keyalg RSA -keystore /opt/APG/.keystore`
   a. Enter `changeit` for the keystore password.
   b. When asked for your first and last name, enter the fully qualified name of the machine, for example, itops-dev-204.lss.emc.com.
   c. Answer the other questions and type, `yes`, when asked for confirmation.

Results

This creates a keystore file inside `/opt/APG` folder with name `.keystore`. This is a hidden file in Linux.

Linux: Editing the EMC M&R server.xml file

Edit the server.xml file to tell Tomcat server which secure port to use.

Update the `https` connector configuration in `server.xml` in this path, `/opt/APG/Web-Servers/Tomcat/Default/conf`.

Procedure

1. Uncomment the `https` connector configuration in server.xml.
2. Add the path to the keystore file. For example,

```
 <Connector port="58443" protocol="HTTP/1.1" SSLEnabled="true"
              maxThreads="150" scheme="https" secure="true"
              compression="2048" compressableMimeType="text/"
              clientAuth="false" sslProtocol="TLS"
URIEncoding="UTF-8"
        keystoreFile="/opt/APG/.keystore" keystorePass="changeit"
              SSLDisableCompression="true" />
```

Configuring SAM environment variables to support SSL

Edit the environment variables in the SAM runcmd_env.sh file to support SSL.

Before you begin

Both SM_CAS_SERVER and SM_TOMCAT_SERVER must be configured to support SSL. The SM_CAS_SERVER environment variable is set to the URL for EMC M&R. The SM_TOMCAT_SERVER environment variable is set to the URL for the SAM Tomcat server.

Procedure

1. Enter the secure port and protocol used to log into EMC M&R in the SM_CAS_SERVER variable. For example, `SM_CAS_SERVER=https://<cas-serverhost>:58443`
2. Enter the secure port and protocol used to log into SAM Tomcat server in the SM_TOMCAT_SERVER variable. For example, `SM_TOMCAT_SERVER=https://<smarts-tomcat-server-host>:8443`

After you finish

Stop and restart the SAM service to make the changes take effect. For example:

```
sm_service stop ic-sam-server-pres
```

```
sm_service start ic-sam-server-pres
```

Linux: Generating the SAM Tomcat server keystore file and certificate

Create the Tomcat server keystore file and certificate.

Before you begin

Generate the keystore file in the home directory where you issue the command.

Procedure

1. Issue the command to generate the keystore file. For example, `usr/bin/keytool -genkey -alias tomcat -keyalg RSA`

   To specify a different location or filename, add the `-keystore` parameter followed by the complete pathname to the keystore file. For example, `$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA -keystore /opt/InCharge/SAM/smarts/.keystore`

   a. Enter `changeit` for the keystore password.

   b. When asked for your first and last name, enter the fully qualified name of the machine, for example, itops-dev-204.lss.emc.com.

   c. Answer the other questions and type, `yes`, when asked for confirmation.

Results

This creates a keystore file inside `/opt/InCharge/SAM/smarts` folder with name `.keystore`.

Linux: Editing the SAM server.xml file

Edit the server.xml file to tell the SAM Tomcat server which secure port and protocol to use.

Update the `https` connector configuration in `server.xml` in this path, `/opt/InCharge/SAM/smarts/tomcat/conf`.

Procedure

1. Uncomment the `https` connector configuration in server.xml.
2. Add the path to the keystore file and the password. For example,

```
 <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
             maxThreads="150" scheme="https" secure="true"
              keystoreFile="/opt/InCharge/SAM/smarts/.keystore"
keystorePass="changeit"
              clientAuth="false" sslProtocol="TLS" />
```

3. Configure the Connector protocols in server.xml as follows. (Copy in this code if it is missing.)

```
 <Connector protocol="org.apache.coyote.http11.Http11Protocol"
          port="8443"
          maxThreads="150" scheme="https" secure="true"
          keystoreFile="/opt/InCharge/SAM/smarts/.keystore"
keystorePass="changeit"
          clientAuth="false" sslProtocol="TLS" />
```

```
<Connector protocol="org.apache.coyote.http11.Http11NioProtocol"
          port="8443"
          maxThreads="150" scheme="https" secure="true"
          keystoreFile="/opt/InCharge/SAM/smarts/.keystore"
keystorePass="changeit"
          clientAuth="false" sslProtocol="TLS" />
```

Linux: Creating the trust relationship between SAM and EMC M&R

You must export and import certificates to get the SAM Tomcat server and EMC M&R Tomcat server to trust each other.

Before you begin

First, export a certificate on the SAM server. Then import it into the EMC M&R Tomcat server. Then export a certificate from the EMC M&R server and import it into the SAM Tomcat server.

Procedure

1. Export a certificate from the SAM Tomcat server. For example,

```
$JAVA_HOME/bin/keytool -export -keystore /opt/InCharge/SAM/
smarts/.keystore -alias tomcat -rfc > SAMtomcat.cert
```

   a. Copy SAMtomcat.cert to the host where EMC M&R Tomcat server is installed.
   b. On the EMC M&R host, import the SAMtomcat.cert. For example,

```
$JAVA_HOME/bin/keytool -import -file SAMtomcat.cert -alias
SAMtomcat -keystore /opt/APG/.keystore
```

   c. Back up the original EMC M&R `cacerts` file.

```
cp /opt/APG/Java/Sun-JRE/7.0u51/lib/security/cacerts /opt/APG/
Java/Sun-JRE/7.0u51/lib/security/cacerts-SAVE    # Backup old
cacerts file
```

   d. Copy `.keystore` and rename it to `cacerts`.

```
cp /opt/APG/.keystore /opt/APG/Java/Sun-JRE/7.0u51/lib/security/
cacerts
```

2. Restart Tomcat server on the EMC M&R host.

```
/opt/APG/bin/manage-modules.sh service restart tomcat
```

3. Export a certificate from the EMC M&R host. For example,

```
•    $JAVA_HOME/bin/keytool -export -keystore /opt/APG/.keystore -
alias tomcat -rfc > W4Ntomcat.cert
```

4. Copy W4ntomcat.cert to the SAM server host.
5. On the SAM server host, run this command to import a certificate copied from the EMC M&R server host.

```
$JAVA_HOME/bin/keytool -import -file W4Ntomcat.cert -alias
W4Ntomcat -keystore /opt/InCharge/SAM/smarts/.keystore
```

6. Copy the keystore file.

```
cp /opt/InCharge/SAM/smarts/jre/lib/security/cacerts /opt/
InCharge/SAM/smarts/jre/lib/security/cacerts-SAVE    # Backup old
cacerts file
```

```
cp /opt/InCharge/SAM/smarts/.keystore /opt/InCharge/SAM/
smarts/jre/lib/security/cacerts
```

7. Confirm the certificates copied properly (review entries).

   For SAM

```
/usr/bin/keytool -list -keystore /opt/InCharge/SAM/smarts/.keystore
```

   For EMC M&R

```
/usr/bin/keytool -list -keystore /opt/APG/.keystore
```

8. Stop and start the Tomcat service on the SAM server:
   a. `/opt/InCharge/SAM/smarts/bin/sm_service stop smarts-tomcat`
   b. `/opt/InCharge/SAM/smarts/bin/sm_service start smarts-tomcat`
9. Restart the EMC M&R services.

```
/opt/APG/bin/manage-modules.sh service restart all
```

Windows SSL Setup

Enable SSL port and protocol settings in SolutionPack for EMC Smarts

When enabling SSL, you must edit the Reports configuration of the SolutionPack for EMC Smarts and ensure use of secure port and protocol settings.

Before you begin

This procedure assumes the SolutionPack for EMC Smarts is already installed and running. If not, the *SolutionPack for EMC Smarts Summary Sheet* article provides installation instructions.

Edit the Reports configuration page to enable SSL for the SolutionPack for EMC Smarts. Access this page from **Centralized Management.** Expand **SolutionPacks** › **Infrastructure** and click **EMC Smarts**.

Procedure

1. Click the **Pencil** icon by the Reports SolutionPackBlock.

   The Reports reconfiguration page appears.
2. Expand Tomcat Configuration and choose **Add a new Tomcat configuration** in the dropdown box.
3. Click the checkbox for **HTTPS Enabled for EMC M&R and Smarts**.
4. Enter the Fully Qualified Domain Name or IP address of the EMC M&R Tomcat server.

   This name must match the host name portion of the entry in **SM_CAS_SERVER** in the Presentation SAM `runcmd_env.sh` file. Ensure consistent use of either IP address or FQDN in all of the field entries. Do not mix the entry formats.
5. Enter the secure port for the EMC M&R Tomcat server. (Default SSL port is 58443).
6. Expand the Smarts and Alerts EDAA Configuration and choose **Add a new Smarts and Alerts EDAA Configuration** in the dropdown box.

   Check the entry in the **Smarts EDAA hostname or IP address** field. This entry must match the host name portion of the entry in **SM_TOMCAT_SERVER** in the Presentation SAM `runcmd_env.sh` file.
7. Enter the secure port for the Smarts EDAA server. (Default SSL port is 8443).
8. Adjust other entries if needed and then click **Reconfigure**.

After you finish

Continue with the SSL certificate generation, import, and export steps. The changes will not take effect until the Tomcat servers are restarted in both SAM and EMC M&R.

Windows: Generate the keystore file for EMC M&R

Create the keystore file for the EMC M&R host. This file stores the tomcat server's private key and self-signed certificate.

Before you begin

Stop the EMC M&R Tomcat service. For example, `c:\Program Files\APG\bin \manage-modules.cmd service stop tomcat`

Procedure

1. Generate the keystore: `C:\Program Files\Java\ jdk1.7.0_07\keytool.exe -genkey -alias tomcat -keyalg RSA -keystore C:\Program Files\APG\.keystore`

   a. Enter `changeit` for the keystore password.

   b. When asked for your first and last name, enter the fully qualified name of the machine, for example, itops-dev-204.lss.emc.com.

   c. Answer the other questions and type, `yes`, when asked for confirmation.

Results

This creates a keystore file inside `C:\Program Files\APG` folder with name `.keystore`.

Windows: Editing the EMC M&R server.xml file

Edit the server.xml file to tell Tomcat server which secure port to use.

Update the `https` connector configuration in `server.xml` in this path, `c:\Program Files\APG\Web-Servers\tomcat\Default\conf`.

Procedure

1. Uncomment the `https` connector configuration in server.xml.
2. Add the path to the keystore file. For example,

```
 <Connector port="58443" protocol="HTTP/1.1" SSLEnabled="true"
               maxThreads="150" scheme="https" secure="true"
               compression="2048" compressableMimeType="text/"
               clientAuth="false" sslProtocol="TLS"
URIEncoding="UTF-8"
        keystoreFile="C:\Program Files\APG\.keystore"
keystorePass="changeit"
               SSLDisableCompression="true" />
```

Configuring SAM environment variables to support SSL

Edit the environment variables in the SAM runcmd_env.sh file to support SSL.

Before you begin

Both SM_CAS_SERVER and SM_TOMCAT_SERVER must be configured to support SSL. The SM_CAS_SERVER environment variable is set to the URL for EMC M&R. The SM_TOMCAT_SERVER environment variable is set to the URL for the SAM Tomcat server.

Procedure

1. Enter the secure port and protocol used to log into EMC M&R in the SM_CAS_SERVER variable. For example, `SM_CAS_SERVER=https://<cas-serverhost>:58443`
2. Enter the secure port and protocol used to log into SAM Tomcat server in the SM_TOMCAT_SERVER variable. For example, `SM_TOMCAT_SERVER=https://<smarts-tomcat-server-host>:8443`

After you finish

Stop and restart the SAM service to make the changes take effect. For example:

```
sm_service stop ic-sam-server-pres
```

```
sm_service start ic-sam-server-pres
```

Windows: Generating the SAM Tomcat server keystore file and certificate

Create the Tomcat server keystore file and certificate.

Before you begin

Generate the keystore file in the home directory where you issue the command.

Procedure

1. Issue the command to generate the keystore file. For example, `$JAVA_HOME\bin\keytool -genkey -alias tomcat -keyalg RSA`

   To specify a different location or filename, add the `-keystore` parameter followed by the complete pathname to the keystore file. For example, `C:\Program Files`

```
\Java\jdk1.7.0_07\bin\keytool.exe" -genkey -alias tomcat -
keyalg RSA -keystore C:\InCharge\SAM\smarts\.keystore
```

a. Enter `changeit` for the keystore password.

b. When asked for your first and last name, enter the fully qualified name of the machine, for example, itops-dev-204.lss.emc.com.

c. Answer the other questions and type, `yes`, when asked for confirmation.

Results

This creates a keystore file inside `C:\InCharge\SAM\smarts\keystore` folder with name `.keystore`.

Windows: Editing the SAM server.xml file

Edit the server.xml file to tell the SAM Tomcat server which secure port and protocol to use.

Update the `https` connector configuration in `server.xml` in this path, `c:\InCharge\SAM\smarts\tomcat\conf`.

Procedure

1. Uncomment the `https` connector configuration in server.xml.
2. Add the path to the keystore file and the password. For example,

```
 <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
             maxThreads="150" scheme="https" secure="true"
              keystoreFile="C:\InCharge\SAM\smarts\keystore"
keystorePass="changeit"
              clientAuth="false" sslProtocol="TLS" />
```

3. Configure the Connector protocols in server.xml as follows. (Copy in this code if it is missing.)

```
 <Connector protocol="org.apache.coyote.http11.Http11Protocol"
          port="8443"
          maxThreads="150" scheme="https" secure="true"
          keystoreFile="C:\InCharge\SAM\smarts\keystore"
keystorePass="changeit"
          clientAuth="false" sslProtocol="TLS" />
```

```
<Connector protocol="org.apache.coyote.http11.Http11NioProtocol"
          port="8443"
          maxThreads="150" scheme="https" secure="true"
          keystoreFile=”C:\InCharge\SAM\smarts\keystore"
keystorePass="changeit"
          clientAuth="false" sslProtocol="TLS" />
```

Windows: Creating the trust relationship between SAM and EMC M&R

You must export and import certificates to get the SAM Tomcat server and EMC M&R Tomcat server to trust each other.

Before you begin

First, export a certificate on the SAM server. Then import it into the EMC M&R Tomcat server. Then export a certificate from the EMC M&R server and import it into the SAM Tomcat server.

Procedure

1. Export a certificate from the SAM Tomcat server. For example,

```
"c:\Program Files\Java\jdk1.7.0_07\bin\keytool.exe" -export -
keystore C:\InCharge\SAM\smarts\keystore -alias tomcat -rfc >  C:
\InCharge\SAM\smarts\SAMtomcat.cert
```

   a. Copy SAMtomcat.cert to the host where EMC M&R Tomcat server is installed.

   b. Import the SAMtomcat.cert into the EMC M&R host. (Copy the files manually using Windows Explorere and CTRL+C and CTRL+V commands.) For example,

```
c:\Program Files\APG>"C:\Program Files\Java\jdk1.7.0_07\bin
\keytool.exe" -import -file "c:\Program Files\APG\
SAMtomcat.cert" -alias SAMtomcat -keystore "C:\Program Files\APG
\.keystore
```

   c. Back up the original `cacerts` file before this next step.

```
c:\Program Files\APG>"C:\Program Files\Java\jdk1.7.0_07\bin
\keytool.exe" -import -file "c:\Program Files\APG\
SAMtomcat.cert" -alias SAMtomcat -keystore "C:\Program Files\APG
\.keystore
```

```
Rename file C:\Program Files\APG\Java\Sun-JRE\7.0u51\lib
\security\cacerts to C:\Program Files\APG\Java\Sun-JRE
\7.0u51\lib\security\cacerts-SAVE    # Backup old cacerts file
```

   d. Copy `.keystore` located at `c:\Program Files\APG\.keystore` to this location, `C:\Program Files\APG\Java\Sun-JRE\7.0u51\lib \security`, and rename it to `cacerts`

2. Restart Tomcat server on the EMC M&R host.

```
/opt/APG/bin/manage-modules.sh service restart tomcat
```

3. Export a certificate from the EMC M&R host. For example,

```
o    c:\Program Files\APG>"C:\Program Files\Java\jdk1.7.0_07\bin
\keytool.exe" -export  -keystore "C:\Program Files\APG\.keystore" -
alias tomcat -rfc > "C:\Program Files\APG\W4Ntomcat.cert"
```

   a. Copy `W4ntomcat.cert` to the SAM server host.

   b. On the SAM server host, run these commands to import a certificate copied from the EMC M&R server host. (Copy the files manually using Windows Explorere and CTRL+C and CTRL+V commands.)

```
"C:\Program Files\Java\jdk1.7.0_07\bin\keytool.exe" -import -
file C:\InCharge\SAM\smarts\ W4Ntomcat.cert -alias W4Ntomcat -
keystore C:\InCharge\SAM\smarts\keystore
```

   c. Back up the original `cacerts` file before this next step. Rename the `cacerts` file located at `C:\InCharge\SAM\smarts\jre\lib\security\cacerts` to `C:\InCharge\SAM\smarts\jre\lib\security\cacerts-SAVE # Backup old cacerts file`

   d. Copy the keystore file from `C:\InCharge\SAM\smarts\keystore` and rename it to `cacerts` at this location `C:\InCharge\SAM\smarts\jre\lib \security\cacerts`

4. Stop and start the Tomcat service on the SAM server:

a. `c:\Program Files\InCharge\SAM\smarts\bin\sm_service stop smarts-tomcat`

b. `c:\Program Files\InCharge\SAM\smarts\bin\sm_service start smarts-tomcat`

5. Restart the EMC M&R services.

```
c:\Program Files\APG\bin\manage-modules.sh service restart all
```

Copyright © 2014-2015 EMC Corporation. All rights reserved. Published in USA.

Published January, 2015

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

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

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

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