RSA Archer GRC

RSA Archer Security Operations Management

Splunk Implementation Guide

5.4 SP1 P1, 5.5, 5.5 SP1, 5.5 SP2, and 5.5 SP3

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers:
http://www.emc.com/support/rsa/index.htm.

Trademarks

RSA, the RSA Logo, RSA Archer, RSA Archer Logo, and EMC are either registered trademarks or trademarks of EMC Corporation ("EMC") in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to **www.rsa.com/legal/trademarks_list.pdf**.

License agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-party licenses

This product may include software developed by parties other than RSA.

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

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.

November 2015

Contents

Revision History

Revision	Date	Description
1	11/12/2015	Updated the About This Guide topic.

Preface

About This Guide

This guide is for RSA® Archer® GRC administrators who need to install the RSA Archer Security Operations Management solution. For more information, see the RSA Archer GRC Platform Help.

This guide assumes that the reader is knowledgeable about the GRC industry and RSA Archer GRC.

RSA Archer GRC Documentation

You can access the RSA Archer GRC documentation from the RSA Archer Exchange and RSA Archer Community.

Documentation	Location
Platform	On the RSA Archer Community at: **https://community.emc.com/community/connect/grc_ecosystem/rsa_archer**
Solutions, Applications, and Content	On Content tab on the RSA Archer Exchange at: **https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange**

RSA continues to assess and improve the documentation. Check the RSA Archer Community and RSA Archer Exchange for the latest documentation.

Support and Service

Customer Support Information	**www.emc.com/support/rsa/index.htm**
Customer Support E-mail	**archersupport@rsa.com**

Other Resources

RSA Archer Community enables collaboration among GRC clients, partners, and product experts. Members actively share ideas, vote for product enhancements, and discuss trends that help guide the RSA Archer GRC product roadmap.
https://community.emc.com/community/connect/grc_ecosystem/rsa_archer

RSA Archer Exchange is an online marketplace dedicated to supporting GRC initiatives that delivers on-demand applications with service, content, and integration providers to drive the success of RSA Archer GRC clients.
https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange

RSA Solution Gallery provides information about third-party hardware and software products that have been certified to work with RSA products. The gallery includes Secured by RSA Implementation Guides with instructions and other information about interoperation of RSA products with these third-party products.
https://gallery.emc.com/community/marketplace/

RSA SecurCare Online (SCOL) provides unlimited access to a wealth of resources on the Web, 24 hours a day. The secure system provides members access to a support knowledgebase, to download current platform patches and bug fixes, to sign up for notifications, to manage your support cases and more.
https://knowledge.rsasecurity.com/

Chapter 1: Integration Overview

RSA Archer Security Operations Management Integration

The RSA Archer Security Operations Management integration facilitates the transport of alerts from Splunk Enterprise to the RSA Archer Security Operations Management solution, where you can assess, prioritize, and analyze them within the larger business context of your organization.

RSA Archer Security Operations Management

The RSA Archer Security Operations Management solution enables you to aggregate all actionable security alerts, allowing you to become more effective, proactive, and targeted in your incident response and SOC management.

RSA Archer Security Operations Management helps you do the following:

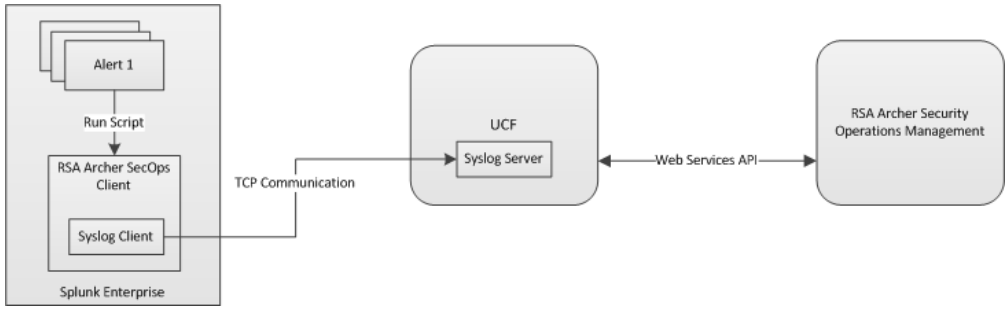
- Prioritize and respond faster to security incidents by leveraging business context and actionable threat intelligence.
- Engage key business and IT stakeholders in the incident management process.
- Simplify incident investigation and breach response procedures through industry best practice methodologies and response procedures.
- Optimize SOC investments through SOC Key Performance Indicators (KPI) monitoring and staff time management tracking.

Splunk Enterprise

Splunk Enterprise monitors the multiple data streams that are generated across your entire enterprise and generates an alert when abnormal activity is noticed.

RSA Archer Security Operations Management Integration Architecture

The following figure provides a high level overview of the integration between RSA Archer Security Operations Management and Splunk Enterprise.



RSA Archer Security Operations Management Integration Files

The RSA Archer Security Operations Management - Splunk Enterprise integration uses the following files, which are included in the Splunk_Integration_1.0.zip file.

- rsa-secops-service-1.0.0.jar
- setup.sh (This file is necessary only for Linux systems)

Note: You also need the alert template files provided in the *Install_Dir*\RSA\SA IM Integration Service\config\mapping\templates folder on your UCF machine.

Requirements

Before installing the RSA Archer Security Operations Management integration, your system must meet the requirements for the following components:

- **RSA Archer Security Operations Management Requirements**
- **Splunk Enterprise Requirements**

RSA Archer Security Operations Management Requirements

Your RSA Archer Security Operations Management system must meet the following requirements:

Requirement	Description
RSA Archer Security Operations Management 1.3	This guide assumes that you have installed RSA Archer Security Operations Management 1.3. *For installation instructions, see the RSA Archer Security Operations Management 1.3 Installation Guide*.
Unified Collector Framework	This guide assumes that you have installed the Unified Collector Framework. For installation instructions, see the *RSA Archer Security Operations Management 1.3 Installation Guide*.

Note: If your RSA Archer GRC system is SSL-enabled, ensure that you have enabled SSL communication between RSA Archer Security Operations Management and the UCF. For instructions, see the *RSA Archer Security Operations Management 1.3 Installation Guide*.

Splunk Enterprise Requirements

Your Splunk Enterprise system must meet the following requirements.

Requirement	Windows 2008	Linux RHEL 6.5
Splunk 6.0.1 or later	X	X
JRE 7 32-bit or 64-bit	X	X
Dos2unix	--	X
Jsvc (Jakarta) **Note:** Dependencies include jakarta-commonsdaemon and jakarta-commons-daemon-jsvc.	--	X

Note: RSA strongly recommends that your system use the Common Information Model (CIM). For instructions on installing and configuring the CIM for Splunk Enterprise, see the *Splunk Common Information Model Add-On Manual*.

Using the RSA Archer Security Operations Management Integration with Other Alert Sources

You can use the RSA Archer Security Operations Management integration alongside other SIEM tools—such as RSA Security Analytics (SA)—to send alerts to RSA Archer Security Operations Management. If you choose to do so, you must configure the same syslog port for each integration.

Chapter 2: Setting Up the RSA Archer SecOps Service

RSA Archer SecOps Service

The RSA Archer SecOps Service facilitates communication between Splunk Enterprise and the Syslog Server on the UCF through the Transmission Control Protocol (TCP).

Set Up the RSA Archer SecOps Service

Procedure

1. Download the Integration Files
2. Install the SecOps Service

Download RSA Archer Security Operations Management Files

Procedure

Download the RSA Archer Security Operations Management file, Splunk_Integration_1.0.zip, from the Applications Exchange page on the RSA Archer Exchange at https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange.

Installing the RSA Archer SecOps Service

The RSA Archer SecOps Service can be installed on either a Windows or Linux operating system.

- Install on Windows
- Install on Linux

Install the RSA Archer SecOps Service on Windows

Procedure

1. From the Splunk_Integration_1.0.zip file, extract the rsa-secops-service-1.0.0.jar file to any location on your local drive, referred to as *extracted-jar-location* in this guide.
2. From the *extracted-jar-location*, do one of the following to install the service:
   - If you are running JRE 7 32-bit, right-click the installService_32.bat file and select Run as Administrator.
   - If you are running JRE 7 64-bit, right-click the installService_64.bat file and select Run as Administrator.

Install the RSA Archer SecOps Service on Linux

Procedure

1. Log on to the Splunk console.

   Important: You must log in with the same credentials used when installing Splunk, and as the user and group assigned to: /opt/splunk/var/run/splunk/dispatch/*.

2. Extract the contents of the Splunk_Integration_1.0.zip file to a location on your local drive.
3. From the extracted folder, copy setup.sh and rsa-secops-service-1.0.0.jar to any location on your local drive.
4. Run dos2unix on setup.sh. Type:

   ```
   dos2unix setup.sh
   ```

5. Assign privileges, if required. Type:

   ```
   chmod 777 setup.sh
   ```

6. Run setup.sh script. Type:

   ```
   ./setup.sh
   ```

Chapter 3: Configuring the RSA Archer Security Operations Management Integration

Configure Splunk Enterprise

Procedure

1. Configure the Syslog Properties
2. Set Up Alert Scripts
3. Start the RSA Archer SecOps Service
4. Set Up Alerts

Configure the Syslog Properties

You must define specific settings in the rsa-secops-client.properties file to enable communication between the RSA Archer SecOps service and the UCF.

Procedure

1. From the *extracted-jar-location*/conf folder, open the rsa-secops-client.properties file.

2. Enter values for the following properties:

Property	Description
Syslog.server.ip	Enter the IP address/hostname of the UCF machine.
Syslog.server.port	Specify the port number on which you want the UCF to listen for Syslog alert messages. **Important:** If you have configured multiple integrations, ensure that the port number is the same for each.
Syslog.server.facility	Enter the facility number. You need to enter the same value for Facility when you configure the Unified Collector Framework. Note this value, if necessary. Valid values are between 16 - 23. The default value is 23.
Syslog.maxMessageLength	Enter the maximum message length of the syslog message. The default value is 10000.

3. Save and close the properties file.

Important: Whenever you make changes to the rsa-secops-client.properties file you must restart the service. For instructions, see **Restart the RSA Archer SecOps Service**.

Set Up Alert Scripts

The integration provides alert scripts that run when an alert triggers and send the alert to the UCF. You must move these files to a specific directory on your Splunk system.

Procedure

1. From the *extracted-jar-location*/conf folder, do the following:
   - On Windows, do the following:
     a. Verify that the Splunk installation path is C:/Program Files/Splunk/bin/python.exe. If Splunk is installed in another location, you must update the secops-client_windows.py script to point to your *Splunk_Install_Dir*/bin/python.exe path.
     b. Copy the secops-client_windows.py file to *Splunk_Install_Dir*\bin\scripts.
   - On Linux, do the following:

a. Verify that the Splunk installation path is /opt/splunk. If it is not, you must update the secops-client_linux.py script to point to the *Splunk_Install_Dir*/bin/python path.

b. Copy the secops-client_linux.py file to *Splunk_Install_Dir*/bin/scripts.

c. Assign the required privileges in the respective python files using the chmod command to enable the system to execute the script.

2. Restart Splunk.

a. Log on to Splunk Enterprise.

b. Click Settings > Server Controls (Server) > Restart Splunk.

Start the RSA Archer SecOps Service

Procedure

Do one of the following:

- On Windows:

a. From the *extracted-jar-location*:

- If you are running JRE 7 32-bit, double-click rsaSecOps_32w.exe
- If you are running JRE 7 64-bit, double-click rsaSecOps_64w.exe

b. Click START.

- On Linux:

a. Change your current directory to /opt/rsa/secops/.

b. Type:

```
./service.sh start
```

Note: You must start the RSA Archer SecOps service each time you reboot your Linux machine.

Set Up Alerts

In Splunk Enterprise, alerts are generated based on the results of predefined automated searches. You define searches for each scenario about which you would like to generate an alert. In order to create an alert in Splunk, you must define a search condition, add an alert template, and configure the alert.

Procedure

1. Create an alert.

a. Log on to your instance of Splunk.

b. Define your search condition by typing in the Search menu.

c. Click the Save As button and select Alert.

2. Configure the alert:
   a. Add the alert template to the search condition. The template files for Splunk are located on the UCF server in the *Install_Dir*\RSA\SA IM Integration Service\config\mapping\templates folder.
      - Splunk (without CIM): Use SecOps_Splunk_templates.txt.
      - Splunk (with CIM): Use Secops_splunk_CIM_Templates.txt.
   b. On page 1 of the Save As Alert dialog box, define the properties as required by your company, and click Next.
   c. On page 2 of the Alert dialog box, select the Run a script checkbox and enter one of the following:
      - On Windows, enter: secops-client_windows.py
      - On Linux, enter: secops-client_linux.py
   d. Save the alert. The corresponding script will run at the given time schedule or real time that you selected.

Restart the RSA Archer SecOps Service

Note: You only need to complete this procedure if you make changes to the rsa-secops-client.properties file after the initial setup.

Procedure

- On Windows:
  a. From the *extracted-jar-location*, double-click the rsaSecOps_32w.exe or rsaSecops_64w.exe file, depending on the JRE version your system is running.
  b. Click STOP.
  c. Click START.
- On Linux:
  a. On the Splunk console, navigate to /opt/rsa/secops/.
  b. Type one of the following:
     - `./service.sh restart`
     - `./service.sh stop`

       `./service.sh start`

Chapter 4: Customizing the RSA Archer Security Operations Management Integration

Customizing the RSA Archer SecOps UCF Plug-in

The RSA Archer SecOps UCF plug-in comes with default alert message templates and a mapping file that define how data from Splunk Enterprise is mapped to RSA Archer GRC fields and the criteria by which alerts are aggregated into incidents. If these default options do not meet your needs, you can create your own custom alert template and modify the mapping file to define your own mapping and aggregation criteria.

Alert Template Example

The following example alert template aggregates alerts based on the value of Source IP meta data.

Note: If you copy and paste any of the examples in this section into Splunk Enterprise, you may introduce carriage returns that break the template. Use the provided template files instead.

```
| eval _raw="CEF:0|Splunk|Splunk|6.0.1|20|This incident is
based on the aggregation criteria sourcetype where Source Type
is " + sourcetype + "|3|RCFApplicationName=secops
aggregationcriteria=splunk-sourcetype-" + sourcetype + "
sourcetype=" + sourcetype + " msg=Grouped by sourcetype - "+
sourcetype + " eventsource=" + source + " host=" + host + "
rt=" + strftime(_time-32400, "%m/%d/%Y %l:%M:%S %p")
```

Alert Template Components

The alert template is comprised of the following four sections:

- Prefix
- Name

- **Severity**
- **Extension**

Prefix

These fields identify the mandatory CEF prefix, the device vendor, product, and version of the message sender, and the signature ID of the event type. These fields are required in your template and should not be modified.

```
CEF:0|Splunk|Splunk|6.0.1|20|
```

Name

This field describes the event. This field is required, but you may enter whatever you want to name the template.

Important: Whatever you enter for this field displays in the Incident Summary field in the RSA Archer Security Incidents application.

```
"This incident is based on the aggregation criteria Source
where Source is " + source
```

Severity

This field identifies the severity of the message. This field is required in your template. The default value is 3, but you may select a different value. Only numbers from 0-10 are allowed where 10 indicates the highest severity or the most important event.

```
3
```

Extension

This section is made up of key-value pairs that follow the format *key= field name* where *key* is a predefined CEF key value and *field name* is the Splunk field name that you want to include in the alert. For example, in the key-value pair " dst=" + dest, dst is the predefined CEF key value and dest is the field name based on the CIM model standards.

The CEF standard provides a number of predefined keys such as dst, but also allows you to define keys for custom fields, cs*n*, where *n* is a number. For any custom fields, you must also define a label for the key, cs*n*Label.

Important: Key-value pairs must be separated with a single space.

In the following example, cs1 is the custom field name and cs1Label is the custom key name.

```
" cs1=" + service + " cs1Label=service"
```

You can include any number of key-value pairs in your alert template, but you must include the following pairs.

- aggregationcriteria
- UCFApplicationName
- msg

Note: These key-value pairs can be any custom string number.

The syntax for aggregating alerts into an incident is as follows:

```
" aggregationcriteria=splunk-fieldname-" + fieldname
```

Here, the key is a custom string and the field name that you define is the value by which the UCF aggregates alerts into incidents. For example:

```
" aggregationcriteria=splunk-src-"+src
```

You can also aggregate alerts into incidents based on multiple aggregation criteria by defining multiple values for the key, using the following syntax:

```
" aggregationcriteria=splunk-" + fieldname1 + " - " +
fieldname2
```

In the following example, alerts are aggregated based on both source and destination IP:

```
" aggregationcriteria=splunk-" + src + " - " + dest
```

Note: Ensure that the meta names that you select for your aggregation criteria contains actual values in Splunk.

Create Custom Alert Templates

To define your own mapping and aggregation criteria, you must create a custom alert template, ensure that you have all the necessary fields to map to in your RSA Archer GRC system, modify the mapping file that the UCF uses to map the data, and add the alert template to Splunk.

Procedure

1. Write a custom alert template.
2. Modify the mapping file. For each Splunk meta data that you define with a key-value pair in an alert template, you must decide to which RSA Archer GRC field you want to map the meta data.
   a. Open secops_import_archer.xml, located in the *Install_Dir*\RSA\SA IM Integration Service\config\mapping directory.
   b. Modify or add field mapping as needed, based on the example below.
      The following mapping file entry defines the mapping of a single Splunk meta data type to a single RSA Archer GRC field.

```
<field name="DestinationAddress">
        <UUID>4D5E3CF5-B5B8-4DA9-B374-BFE23A7A553D</UUID>
        <fieldType>IP_ADDRESS</fieldType>
        <keyName>dst</keyName>
</field>
```

You can either modify the existing entries or add new entries as needed.

The keyName value is the key name that you defined in the alert template. For example, if you defined " dst=" + dest in your alert template, you would enter dst for the keyName in the mapping file.

The field name value is the RSA Archer GRC field to which you want to map Splunk meta data.

Note: If your UUID value and field type are different from the default, or if you are adding an entirely new field, you also need to enter values for those two fields in the mapping file. For information about customizing the mapping files, see the *RSA Archer Security Operations 1.3 Installation Guide*.

c. Save and close the mapping file.

3. Restart the UCF service.
4. Add the template to Splunk. For instructions, see step 2 of **Set Up Alerts**.

Chapter 5: Using the RSA Archer Security Operations Management Integration

View Alerts in RSA Archer Security Operations Management

Procedure

Do one of the following:

- To view a list of all the open alerts from Splunk Enterprise, go to the Navigation Menu and select Incident Response > Security Alerts > Display All.
- To view the alerts associated with a specific incident, go to the Incident Handler dashboard, and from the Incident Queue iView, open an incident to review. Click the Alerts tab to display all the alerts associated with that particular incident.

Additional Use Cases for the RSA Archer Security Operations Management Integration

The RSA Archer Security Operations Management integration can be used with the existing RSA Archer Security Operations Management solution use cases. For more information about specific personas, managing security operations compliance, breach and incident response workflows, and remediating issues, see the *RSA Archer Security Operations Management 1.3 Practitioner Guide*.

Appendix A: Troubleshooting

This appendix contains resolutions to common problems you may encounter while configuring your integration.

Troubleshooting

Issue	Remediation
Triggered events for a particular alert are not visible in the Splunk Alert Manager.	Review your alert settings in the Save As alert dialog and ensure that the "List In Triggered Alerts" option is selected. This ensures that the event exists in search mode for that alert.
Events are triggered on the Splunk Alert Manager, but no information is communicated to the SecOps service.	Verify the following: • The python script file is in the correct directory ($SPLUNK_HOME/bin/scripts). • You restarted Splunk Enterprise after putting the python files in the same directory. • The secops-client_linux.py and the secops-client_ windows.py files are pointing to the correct python location for Splunk Enterprise.
Events are triggered from Splunk, but no alert is created in RSA Archer Security Operations Management.	Verify the following: • Your RSA SecOps service is running. If the service is not running, start the service. • On your Splunk machine, review the RSA SecOps service logs under *extracted-jar-location*/logs to determine whether alerts were sent to the UCF. If no alert was sent to the UCF, ensure that the service has the same ownership as the user and group assigned to $SPLUNK_HOME/var/run/splunk/dispatch/* • Confirm that your RSA Unified Collector Framework service is running. If the service is not running, start the service.

Issue	Remediation
Alerts from Splunk are being sent to the RSA Unified Collector Framework, but no alert is created in RSA Archer Security Operations Management.	Check the collector.log log for any errors (*Install_Dir*\SA IM Integration Service\logs). **Note:** For additional UCF troubleshooting information, see the *RSA Archer Security Operations Management 1.3 Installation Guide*.

Appendix B: Mapped Fields

This appendix lists the fields that are mapped out-of-the-box from Splunk Enterprise to the RSA Archer Security Operations Management solution.

Splunk field name	RSA Archer GRC field name	RSA Archer GRC application
sourcetype	SourceType	Security Alerts
host	Host	Security Alerts
rt	Alert timestamp	Security Alerts
act	Alert action	Security Alerts
eventsource	Alert source	Security Alerts
eventtype	Alert type	Security Alerts
externalId	Session ID	Security Alerts
src	Source IP address	Security Alerts
sourcedomain	Source Domain	Security Alerts
smac	Source Ethernet Address	Security Alerts
dst	Destination IP Address	Security Alerts
destinationdomain	Destination Domain	Security Alerts
dmac	Destination Ethernet Address	Security Alerts
deviceip	Device IP	Security Alerts
	Incident Summary	Security Incidents
	Incident Details	Security Incidents
	hash_code	Security Incidents

The following fields are mapped from the alert template.

Alert template element	RSA Archer GRC field	RSA Archer GRC application
Severity	Severity level	Security Alerts
msg	Incident Summary	Security Incidents
summary	Incident Details	Security Incidents
aggregationcriteria	hash_code	Security Incidents

The following fields are mapped from the alert script in Splunk Enterprise.

Alert script element	RSA Archer GRC field	RSA Archer GRC application
Alert name	Alert Name	Security Alerts
n/a	Splunk Link	Security Alerts
Alert name	Title	Security Incidents