

RSA NetWitness Logs

Event Source Log Configuration Guide



RSA Adaptive Auth OnPrem

Last Modified: Friday, April 14, 2017

Event Source Product Information:

Vendor: [RSA](#)

Event Source: Adaptive Auth OnPrem

Versions: 6.0.2.1

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: rsaaaop

Collection Method: Syslog

Event Source Class.Subclass: Security.Access Control

Configure RSA Adaptive Auth OnPrem

To configure Syslog collection for the RSA Adaptive Auth OnPrem event source, you must:

- I. Configure Syslog Output on RSA Adaptive Auth OnPrem
- II. Configure RSA NetWitness Suite for Syslog Collection

Configure Syslog Output on RSA Adaptive Auth OnPrem

To configure RSA Adaptive Authentication, you configure the **log4j.properties** files to send syslog messages.

To configure RSA Adaptive Authentication OnPrem:

1. Configure the platform or server log as follows.

- a. The file is in the following location:

```
WEB-APPS-DIRECTORY/AdaptiveAuthentication/WEB-INF/classes/log4j.properties
```

- b. Append **auditSyslog** to the **AuditLogger** property as follows:

```
log4j.logger.com.passmarksecurity.utils.AuditLogger=INFO,auditor, auditSYSLOG
```

- c. Append **alarmSyslog** to the **AlarmLogger** property as follows:

```
log4j.logger.com.passmarksecurity.utils.AlarmLogger=INFO,alarm, alarmSYSLOG
```

- d. Add the following lines to the file.

```
# Begin audit syslog appender ---
log4j.appender.auditSYSLOG=org.apache.log4j.net.SyslogAppender
log4j.appender.auditSYSLOG.SyslogHost=SA-IP-address
log4j.appender.auditSYSLOG.Facility=USER
log4j.appender.auditSYSLOG.FacilityPrinting=false
log4j.appender.auditSYSLOG.layout=org.apache.log4j.PatternLayout
log4j.appender.auditSYSLOG.layout.ConversionPattern=%AAOP-Audit %d{yyyy-MM-dd HH:mm:ss,SSS Z} | [%X{clntsessid}] | [%X{sesstag}] | [%X{usertag}] | %X{orgtag} | %X{deviceidtag} | %X{iptag} | %X{hashediptag} | %X{eventtypetag} | %X{eventidtag} | %X{txidtag} | %X{txtypetag} | [%m]%n
# End audit SYSLOG appender ---
# Begin alarm syslog appender ---
```

```
log4j.appender.alarmSYSLOG=org.apache.log4j.net.SyslogAppender
log4j.appender.alarmSYSLOG.SyslogHost=SA-IP-address
log4j.appender.alarmSYSLOG.Facility=USER
log4j.appender.alarmSYSLOG.FacilityPrinting=false
log4j.appender.alarmSYSLOG.layout=org.apache.log4j.PatternLayout
log4j.appender.alarmSYSLOG.layout.ConversionPattern=%AAOP-
Alarm %d{yyyy-MM-dd HH:mm:ss,SSS Z} %p - [%X{clntsessid}] |
[%X{sesstag}] | [%X{usertag}] | [%m]%n
# End alarm SYSLOG appender ---
```

Where **SA-IP-address** is the IP address of the RSA NetWitness Suite Log Decoder or Remote Log Collector.

- e. Restart the Apache Tomcat Windows service for these changes to take effect.
2. Configure the admin log as follows.
 - a. The file is in the following location:

```
WEB-APPS-DIRECTORY/AdaptiveAuthenticationAdmin/WEB-INF/classes/log4j.properties
```

- b. Append **auditSyslog** to the **AuditLogger** property as follows:

```
log4j.logger.com.passmarksecurity.utils.AuditLogger=INFO,
auditor, auditSYSLOG
```

- c. Append **alarmSyslog** to the **AlarmLogger** property as follows:

```
log4j.logger.com.passmarksecurity.utils.AlarmLogger=INFO,
alarm, alarmSYSLOG
```

- d. Add the following lines to the file.

```
# Begin audit syslog appender ---
log4j.appender.auditSYSLOG=org.apache.log4j.net.SyslogAppender
log4j.appender.auditSYSLOG.SyslogHost=SA-IP-address
log4j.appender.auditSYSLOG.Facility=USER
log4j.appender.auditSYSLOG.FacilityPrinting=false
log4j.appender.auditSYSLOG.layout=org.apache.log4j.PatternLayout
log4j.appender.auditSYSLOG.layout.ConversionPattern=%AAOP-
Admin-Audit %d{yyyy-MM-dd HH:mm:ss,SSS Z} | [%X{clntsessid}] |
[%X{sesstag}] | [%X{usertag}] | %X{orgtag} | %X{deviceidtag} |
%X{iptag} | %X{eventtypetag} | %X{eventidtag} | %X{txidtag} |
%X{txtypetag} | [%m]]%n
# End audit SYSLOG appender ---
```

```
# Begin alarm syslog appender ---
log4j.appender.alarmSYSLOG=org.apache.log4j.net.SyslogAppender
log4j.appender.alarmSYSLOG.SyslogHost=SA-IP-address
log4j.appender.alarmSYSLOG.Facility=USER
log4j.appender.alarmSYSLOG.FacilityPrinting=false
log4j.appender.alarmSYSLOG.layout=org.apache.log4j.PatternLayout
log4j.appender.alarmSYSLOG.layout.ConversionPattern=%AAOP-Admin-Alarm %d{yyyy-MM-dd HH:mm:ss,SSS Z} %p - <m>%n
# End alarm SYSLOG appender ---
```

Where **SA-IP-address** is the IP address of the RSA NetWitness Suite Log Decoder or Remote Log Collector.

- e. Restart the Apache Tomcat Windows service for these changes to take effect.

3. Configure the access management log as follows.

- a. The file is in the following location:

```
WEB-APPS-DIRECTORY/accessmanagement/WEB-INF/classes/log4j.properties
```

- b. Append **auditSyslog** to the **AuditLogger** property as follows:

```
log4j.logger.com.passmarksecurity.utils.AuditLogger=INFO,auditor, auditSYSLOG
```

- c. Add the following lines to the file.

```
# Begin audit syslog appender ---
log4j.appender.auditSYSLOG=org.apache.log4j.net.SyslogAppender
log4j.appender.auditSYSLOG.SyslogHost=SA-IP-address
log4j.appender.auditSYSLOG.Facility=USER
log4j.appender.auditSYSLOG.FacilityPrinting=false
log4j.appender.auditSYSLOG.layout=org.apache.log4j.PatternLayout
log4j.appender.auditSYSLOG.layout.ConversionPattern=%AAOP-AM-Audit %d{yyyy-MM-dd HH:mm:ss,SSS Z} | [%X{clntsessid}] | [%X{sesstag}] | [%X{usertag}] | [%X{orgtag}] | [%X{deviceidtag}] | [%X{iptag}] | [%X{eventtypetag}] | [%X{eventidtag}] | [%X{txidtag}] | [%X{txtypetag}] | [%m]]%n
# End audit SYSLOG appender ---
```

Where **SA-IP-address** is the IP address of the RSA NetWitness Suite Log Decoder or Remote Log Collector.

- d. Restart the Apache Tomcat Windows service for these changes to take effect.

4. Configure the case management log as follows.

- a. The file is in the following location:

```
WEB-APPS-DIRECTORY/casemanagement/WEB-INF/classes/log4j.properties
```

- b. Append **auditSyslog** to the **AuditLogger** property as follows:

```
log4j.logger.com.passmarksecurity.utils.AuditLogger=INFO,auditor, auditSYSLOG
```

- c. Add the following lines to the file.

```
# Begin audit syslog appender ---
log4j.appender.auditSYSLOG=org.apache.log4j.net.SyslogAppender
log4j.appender.auditSYSLOG.SyslogHost=SA-IP-address
log4j.appender.auditSYSLOG.Facility=USER
log4j.appender.auditSYSLOG.FacilityPrinting=false
log4j.appender.auditSYSLOG.layout=org.apache.log4j.PatternLayout
log4j.appender.auditSYSLOG.layout.ConversionPattern=%AAOP-CM-Audit %d{dd MMM yyyy HH:mm:ss} | [%m] %n
# End audit SYSLOG appender ---# Begin alarm syslog appender --
```

Where **SA-IP-address** is the IP address of the RSA NetWitness Suite Log Decoder or Remote Log Collector.

- d. Restart the Apache Tomcat Windows service for these changes to take effect.



Configure RSA NetWitness Suite for Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > System**.
3. Depending on the icon you see, do one of the following:

- If you see  **Start Capture**, click the icon to start capturing Syslog.
- If you see  **Stop Capture**, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View > Config > Event Sources**.
3. Select **Syslog/Config** from the drop-down menu.
The Event Categories panel displays the Syslog event sources that are configured, if any.
4. In the Event Categories panel toolbar, click **+**.
The Available Event Source Types dialog is displayed.
5. Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.
The Add Source dialog is displayed.
7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.
Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Copyright © 2017 EMC Corporation. All Rights Reserved.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.