FORUM SYSTEMS™

MANAGING & ACCELERATING XML WEB SERVICES SECURITY

FORUM SYSTEMS HANDS-ON TRAINING

LAB 18. CONFIGURE REMOTE LOGGING

Published: September 2014
Forum Systems Hands-on Training – Lab 18. Configure Remote Logging
D-ASF-SE-010029

Contents

Introduction

Lab 18. Configure Remote Logging

Skill Level

This lab is beginner skill level. Little to no prior experience with Forum Sentry or SOAPSonar is required.

Prerequisites

This lab requires the Forum Sentry Training Image, with a licensed copy Sentry and SOAPSonar.

Refer to the “FS_Training_Labs_v8-1_Introduction” document for information on the Forum Sentry Training Image and licensing SOAPSonar Enterprise Edition.

This lab utilizes the Kiwi Syslog Server that is already installed on the Forum Sentry Training Image. Ensure that the Kiwi Syslog Server console is running.

Lab Overview

All of the Sentry log messages are stored locally. It is not possible to disable the local logging, though different log levels can be configured for each log. In addition to the local logging, all of the log messages can also be sent to a remote log management platform. This is useful for log aggregation and alerting on log messages.

Sentry supports syslog to send the log messages to a remote server. With this, you can configure which logs and which log levels are used with each syslog server. Sentry supports multiple syslog formats (RFCs) and can use either UDP or TCP. When using TCP, you can enable SSL to encrypt the network traffic between Sentry and the log management platform. This is recommended if the Sentry logging information will include confidential data.

In this lab you will build a Remote Syslog Policy in Sentry and view the log messages in the Kiwi Syslog Server installed on the Training Image.

This lab will provide instructions for configuring remote logging in Forum Sentry. Topics will include:

1. Remote Syslog Policies

Remote Syslog Policy Configuration

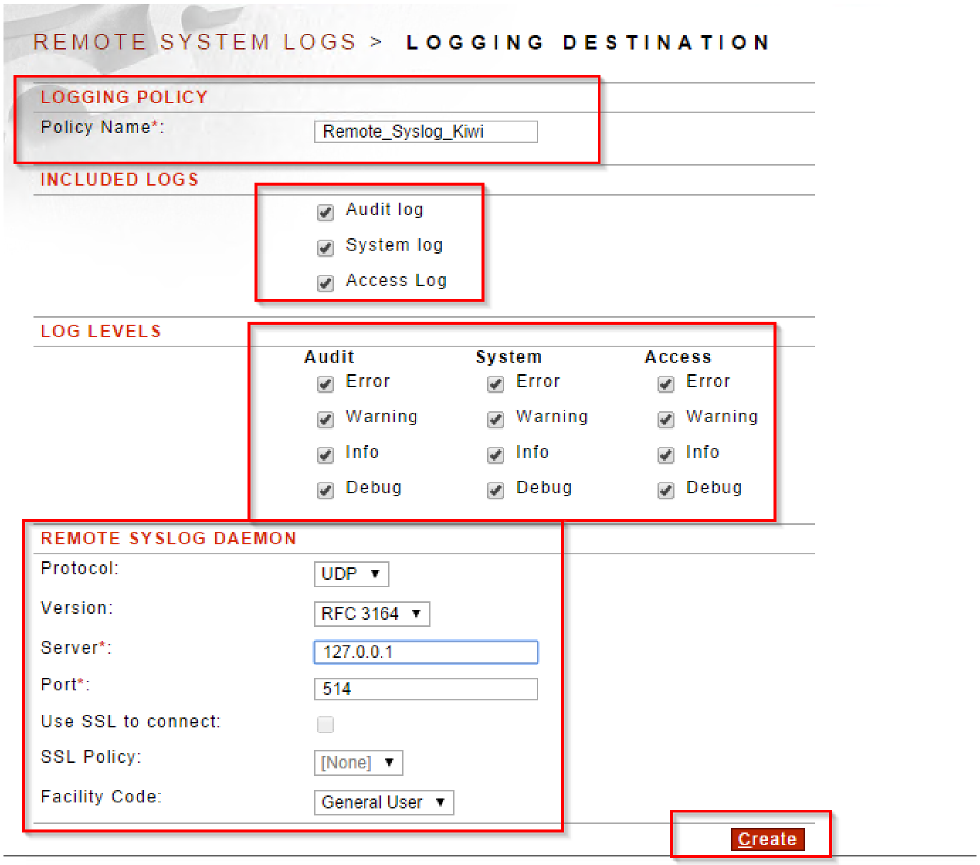
The Sentry Training Lab has Kiwi Syslog Server pre-installed. Ensure this is running before proceeding with this lab. You simply need to launch this product from the desktop shortcut.

In this step you'll build a Remote Syslog Policy to send Sentry logs to the Kiwi Syslog Server.

Building a Remote Syslog Policy

Follow the steps below to build a Remote Syslog Policy in Sentry.

1. Navigate to the Diagnostics→Logging→Remote Syslog page in Sentry.
2. Click New to create a new Remote Syslog Policy. Configure the Remote Syslog Policy with the following criteria:
   - **a.** Policy Name: Remote_Syslog_Kiwi
   - **b.** Included Logs: Audit, System, Access
   - **c.** Log Levels: CHECK ALL
   - **d.** Remote Syslog Daemon:
     - **i.** Protocol: UDP
     - **ii.** Version: RFC 3164
     - **iii.** Server: 127.0.0.1
     - **iv.** Port 514
     - **v.** Facility Code: General User
     - **vi.** Click Create



REMOTE SYSTEM LOGS > LOGGING DESTINATION

LOGGING POLICY

Policy Name*: Remote_Syslog_Kiwi

INCLUDED LOGS

☑ Audit log
☑ System log
☑ Access Log

LOG LEVELS

Audit	System	Access
☑ Error	☑ Error	☑ Error
☑ Warning	☑ Warning	☑ Warning
☑ Info	☑ Info	☑ Info
☑ Debug	☑ Debug	☑ Debug

REMOTE SYSLOG DAEMON

Protocol: UDP ▼
Version: RFC 3164 ▼
Server*: 127.0.0.1
Port*: 514
Use SSL to connect: □
SSL Policy: [None] ▼
Facility Code: General User ▼

Testing the Remote Syslog Policy

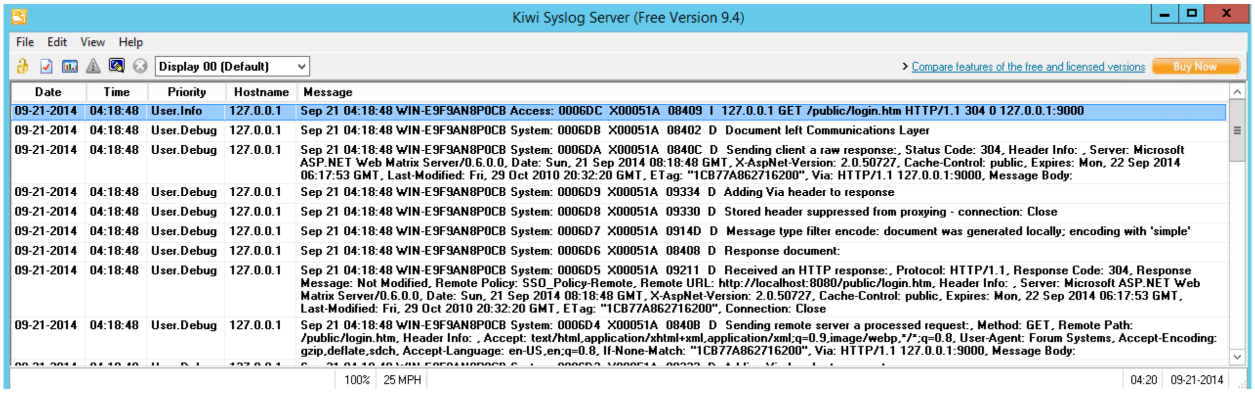
The Sentry Training Lab has Kiwi Syslog Server pre-installed. Ensure this is running before proceeding with this lab. You simply need to launch this product from the desktop shortcut.

In this step we'll validate that the Sentry log messages are received by the Kiwi Syslog Server.

Testing the Policy

Follow the steps below to test the Remote Syslog Policy in Sentry.

1. Launch the Kiwi Syslog Server if it is not already open. Note that it minimizes to the systray.
2. Generate some log messages in Sentry either by making a change to the configuration (Audit logs) or send some runtime traffic into Sentry (System and Access Logs).
3. Review the Kiwi Syslog Server and notice the logs are received.



Kiwi Syslog Server (Free Version 9.4)
File
Edit
View
Help
Display 00 (Default)
> Compare features of the free and licensed versions
Buy Now
100%
25 MPH
04:20
09-21-2014

Date	Time	Priority	Hostname	Message
09-21-2014	04:18:48	User.Info	127.0.0.1	Sep 21 04:18:48 WIN-E9F9AN8P0CB Access: 0006DC X00051A 08409 I 127.0.0.1 GET /public/login.htm HTTP/1.1 304 0 127.0.0.1:9000
09-21-2014	04:18:48	User.Debug	127.0.0.1	Sep 21 04:18:48 WIN-E9F9AN8P0CB System: 0006DB X00051A 08402 D Document left Communications Layer
09-21-2014	04:18:48	User.Debug	127.0.0.1	Sep 21 04:18:48 WIN-E9F9AN8P0CB System: 0006DA X00051A 0840C D Sending client a raw response:, Status Code: 304, Header Info: , Server: Microsoft ASP.NET Web Matrix Server/0.6.0.0, Date: Sun, 21 Sep 2014 08:18:48 GMT, X-AspNet-Version: 2.0.50727, Cache-Control: public, Expires: Mon, 22 Sep 2014 06:17:53 GMT, Last-Modified: Fri, 29 Oct 2010 20:32:20 GMT, ETag: "1CB77A862716200", Via: HTTP/1.1 127.0.0.1:9000, Message Body:
09-21-2014	04:18:48	User.Debug	127.0.0.1	Sep 21 04:18:48 WIN-E9F9AN8P0CB System: 0006D9 X00051A 09334 D Adding Via header to response
09-21-2014	04:18:48	User.Debug	127.0.0.1	Sep 21 04:18:48 WIN-E9F9AN8P0CB System: 0006D8 X00051A 09330 D Stored header suppressed from proxying - connection: Close
09-21-2014	04:18:48	User.Debug	127.0.0.1	Sep 21 04:18:48 WIN-E9F9AN8P0CB System: 0006D7 X00051A 0914D D Message type filter encode: document was generated locally; encoding with 'simple'
09-21-2014	04:18:48	User.Debug	127.0.0.1	Sep 21 04:18:48 WIN-E9F9AN8P0CB System: 0006D6 X00051A 08408 D Response document:
09-21-2014	04:18:48	User.Debug	127.0.0.1	Sep 21 04:18:48 WIN-E9F9AN8P0CB System: 0006D5 X00051A 09211 D Received an HTTP response:, Protocol: HTTP/1.1, Response Code: 304, Response Message: Not Modified, Remote Policy: SSO_Policy-Remote, Remote URL: http://localhost:8080/public/login.htm, Header Info: , Server: Microsoft ASP.NET Web Matrix Server/0.6.0.0, Date: Sun, 21 Sep 2014 08:18:48 GMT, X-AspNet-Version: 2.0.50727, Cache-Control: public, Expires: Mon, 22 Sep 2014 06:17:53 GMT, Last-Modified: Fri, 29 Oct 2010 20:32:20 GMT, ETag: "1CB77A862716200", Connection: Close
09-21-2014	04:18:48	User.Debug	127.0.0.1	Sep 21 04:18:48 WIN-E9F9AN8P0CB System: 0006D4 X00051A 0840B D Sending remote server a processed request:, Method: GET, Remote Path: /public/login.htm, Header Info: , Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8, User-Agent: Forum Systems, Accept-Encoding: gzip,deflate,sdch, Accept-Language: en-US,en;q=0.8, If-None-Match: "1CB77A862716200", Via: HTTP/1.1 127.0.0.1:9000, Message Body:

END

Additional Testing and More Reading

BACK IT UP!

It is recommended that you export your full Sentry configuration after completing this lab.

To export your full Sentry configuration, navigate to the System→Configuration→Import/Export screen and use the Export option in the center of the page to export the full Sentry configuration file as a password encrypted FSX file. This can later be imported on the same screen.

We recommend including the lab number in the name of the export files.

Additional Tests and Discussion Topics

1. Modify the log levels to see what data is logged locally compared to what is sent to the syslog server.
2. Enable SSL on the syslog policy.
3. Built alerts on the syslog policy based on Sentry logs.
4. What other alerts can we get from Sentry?
5. Aside from logs, how else can we monitor the Sentry deployment?

Additional Information

For more information, review the following Forum Sentry Admin Guide:

1. Logging Guide
2. Integrate with HP Arcsight:

   https://helpdesk.forumsys.com/entries/80493283-How-To-Integrate-Sentry-with-HP-ArcSight-Logger

3. Important log messages to alert on: https://helpdesk.forumsys.com/entries/84264333-Best-Practices-Important-Log-Messages-

About Forum Systems

Forum Systems is the global leader in API and Cloud Security technology with industry-certified, patented, and proven products deployed in the most rigorous and demanding customer environments worldwide. Forum Systems has been an industry leader for over 12 years and has built the core architecture of its technology on the foundation of FIPS 140-2 and NDPP. Forum Systems security-first mindset enables trusted, network edge deployments of its technology for protecting critical enterprise transactions.

Our product technology is purpose-built and designed for mission-critical, enterprise-class scalable solutions where business solutions require the modern day security and identity enforcement protection, while enabling a scalable architecture and low-latency, high-volume throughput.

Forum Systems supports global enterprise customers across industries in commercial, government, and military sectors. Forum Systems technology provides the leading-edge of modern-day cyber-security innovation with integrated identity and SSO features that enable out-of-the box business solutions with point-and-click technology.

Forum's patented; FIPS 140-2 and NDPP certified hardware and virtual products make modern-day business communications secure by actively protecting and accelerating data exchange and API service access across networks and business boundaries. For more information, please visit www.forumsys.com.