CorreLog, Inc.

CorreLog SIEM Agent for IBM z/OS

RSA Security Analytics CEF Implementation Guide

Last Modified: June 22, 2015

Partner Information

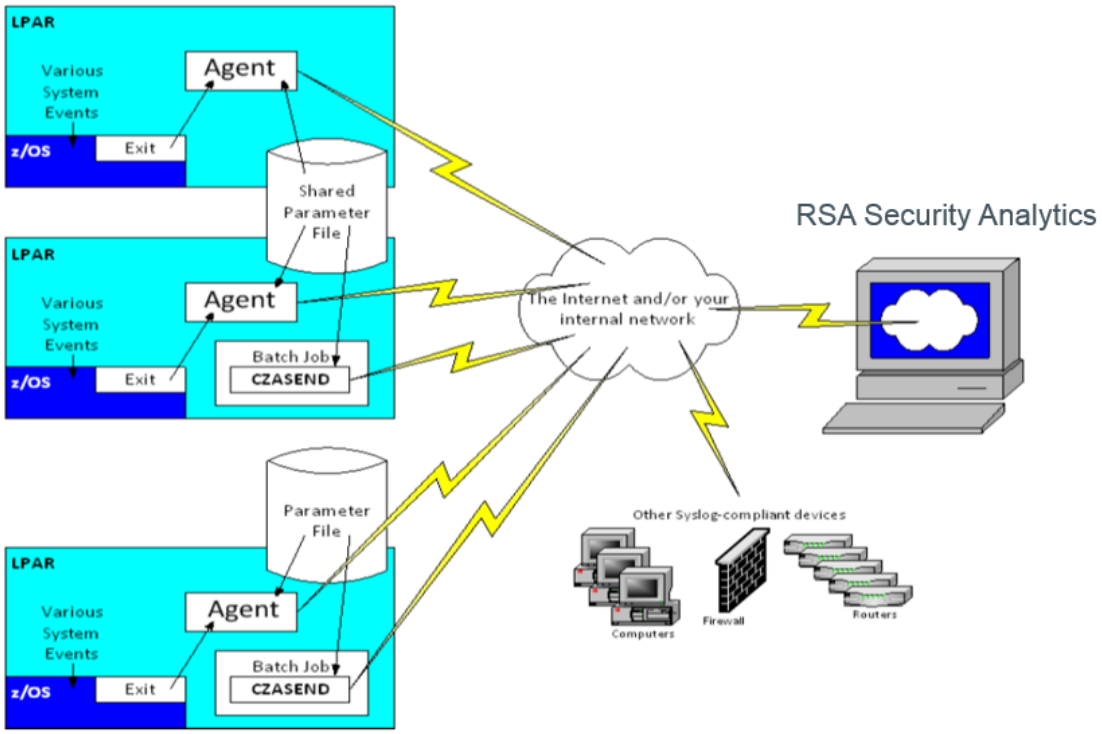
Product Information	
Partner Name	CorreLog, Inc.
Web Site	www.correlog.com
Product Name	CorreLog SIEM Agent for IBM z/OS
Version & Platform	5.5.1 z/OS
Product Description	The CorreLog SIEM Agent for IBM z/OS expands the role of your RSA Security Analytics to include real-time mainframe messages from RACF, ACF2, Top Secret, DB2 accesses, File Integrity and other important user activity data relevant to network security. Complete your SIEM strategy leveraging this powerful and unique real-time mainframe security management component.

Solution Summary

The CorreLog SIEM Agent for IBM z/OS collects and forwards events using a CEF format to RSA Security Analytics.

Enabling this feature allows RSA SA customers to monitor, track and act on any actionable event as needed.

RSA Security Analytics Features	
CorreLog SIEM Agent for IBM z/OS	
Integration package name	Common Event Format
Device display name within Security Analytics	CorreLog_Agent_for_z/OS
Event source class	NA
Collection method	syslog



Release Notes

Release Date	What's New In This Release
06/22/2015	Initial support for CorreLog SIEM Agent for IBM z/OS.

Important: The RSA SA CEF parser is dependent on the integrating partner adhering to the CEF Rules outlined in the ArcSite guidelines document for CEF Header Information. A copy of the Common Event Format guide can be found on http://protect724.hp.com/**.**

Eg. Jan 18 11:07:53 host CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|[Extension]

Important: The time displayed in the CEF log header is parsed into evt.time.str. No other time formats are parsed by default.

Security Analytics Common Event Format Integration Package

The RSA Security Analytics (SA) Community is an online forum for customers and partners to exchange technical information and best practices with each other. The forum also contains the location to download the SA Integration Package for this guide. All Security Analytics customers and partners are invited to register and participate in the **RSA Security Analytics Community**.

Once you have downloaded the Live package, the next steps are to deploy this on all log decoders.

Note: For steps to disable or remove the Security Analytics Integration Package, please refer to the Appendix of this Guide.

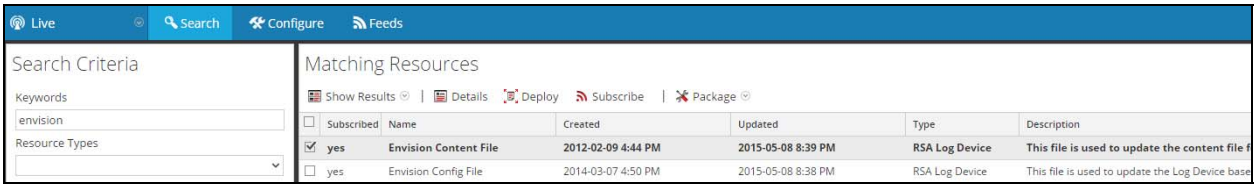
The RSA Security Analytics Common Event Format Integration package consists of the following files:

Filename	File Function
Common Event Format	SA Live package deployed to parse events from device integrations.

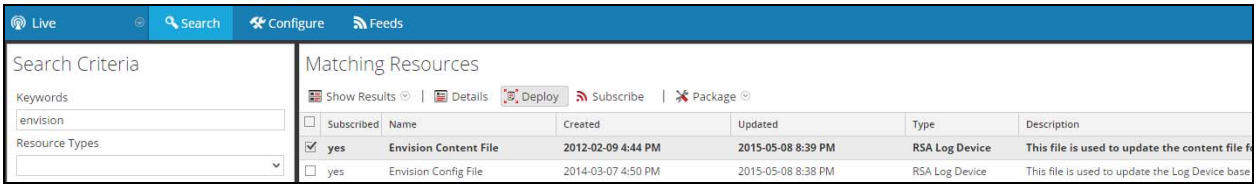
Deployment Procedure

In order to use RSA Partner created content, you must first deploy the *enVision Content File* from the **Security Analytics Live** module. Log into Security Analytics and perform the following actions:

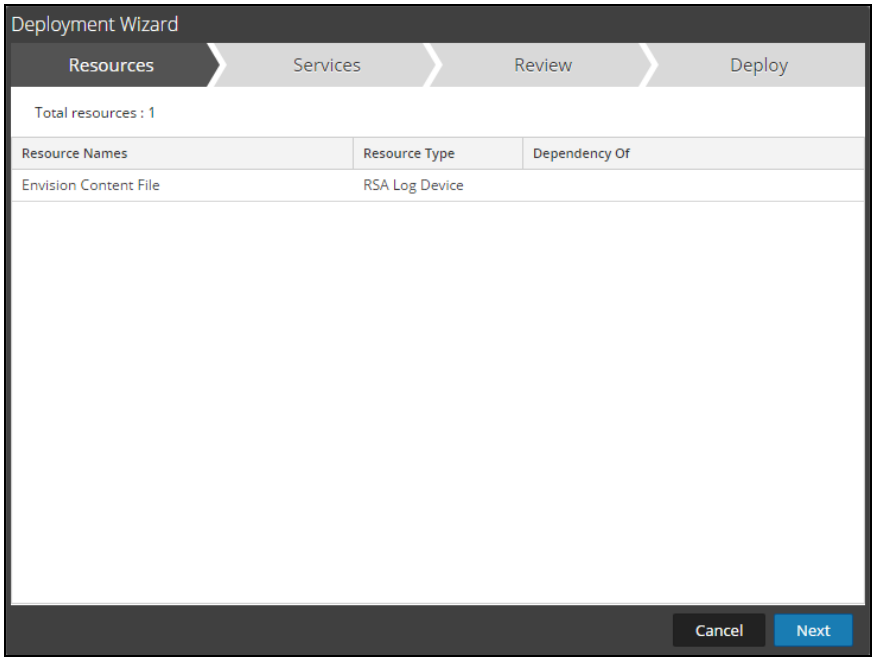
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **enVision**.
3. Security Analytics will display the **Envision Content File** in Matching Resources.
4. Select the checkbox next to **Envision Content File**.



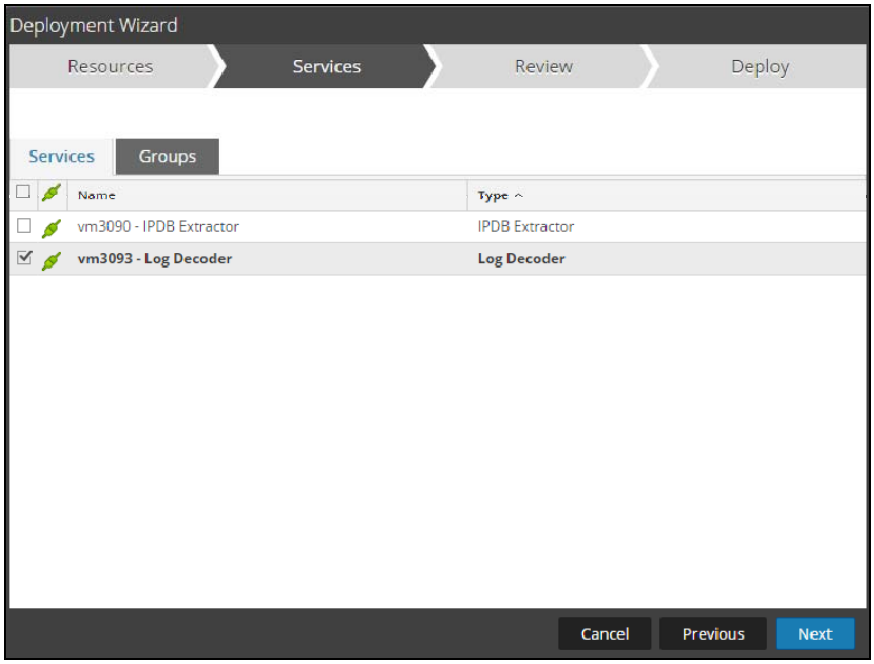
5. Click **Deploy** in the menu bar.



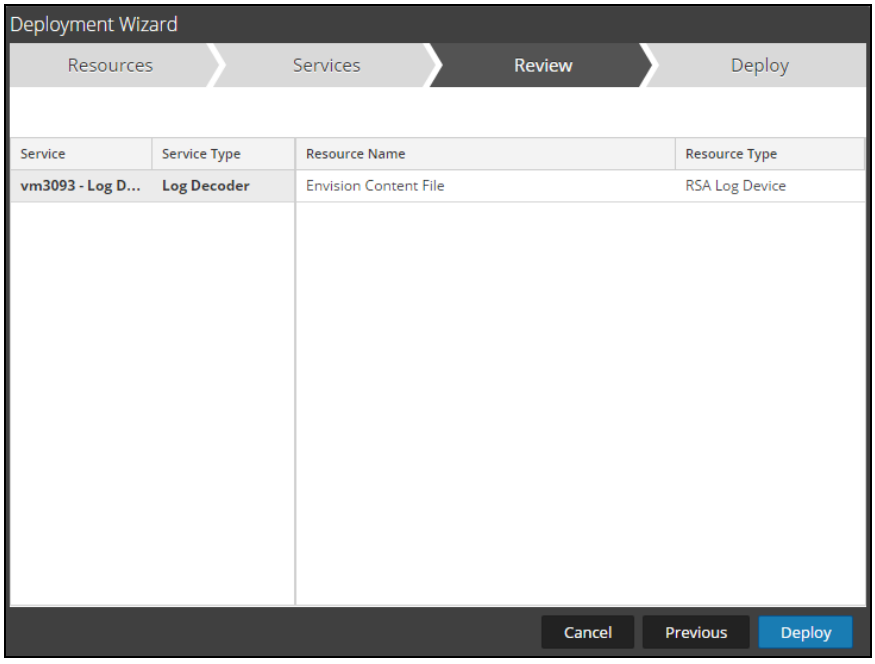
6. Select **Next**.



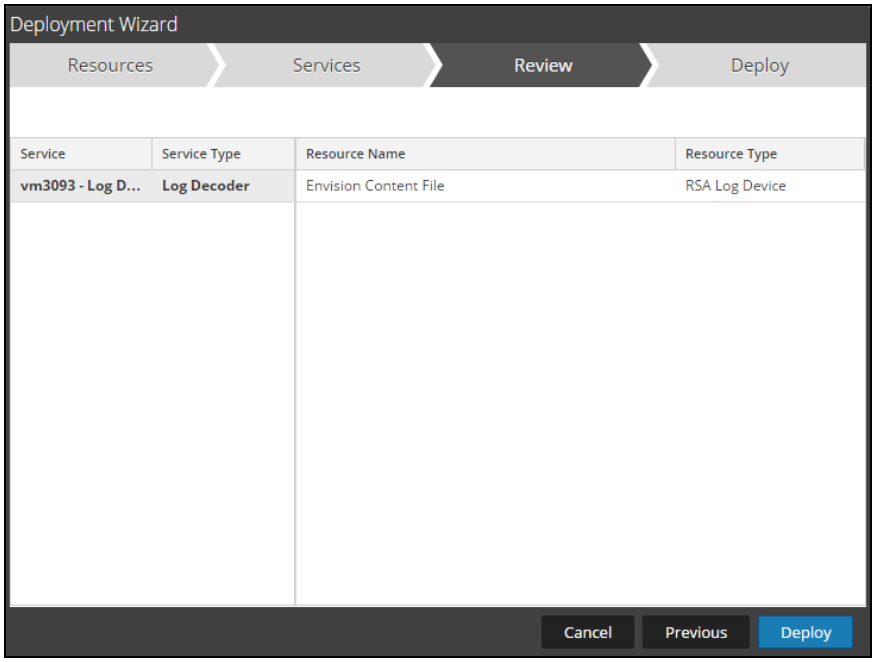
7. Select the **Log Decoder** and Select **Next**.



8. Select **Deploy**.



9. Select **Close**, to complete the deployment of the Envision Config file.

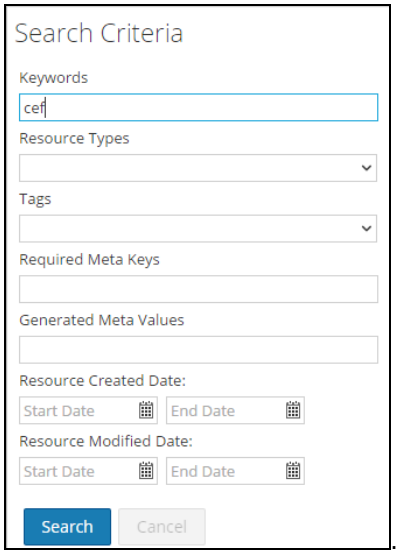


Deploy Common Event Format

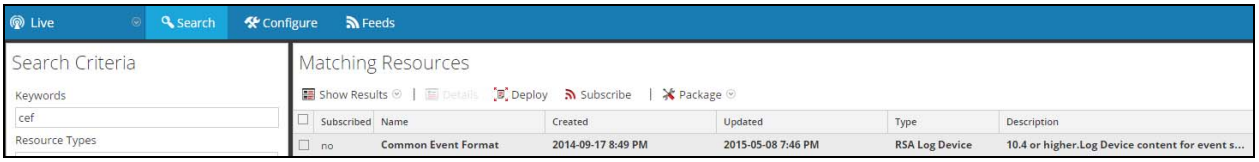
> **Note: In order to use RSA Partner created content, you must first deploy the *enVision Content File* from the Security Analytics Live module.**

Log into Security Analytics and perform the following actions:

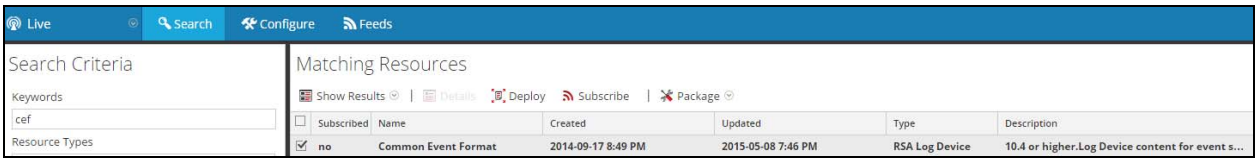
10. From the Security Analytics menu, select **Live > Search**.
11. In the keywords field, enter: **CEF**



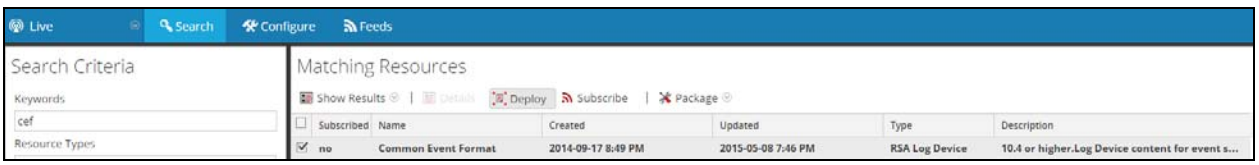
12. Security Analytics will display the **Common Event Format** in Matching Resources.



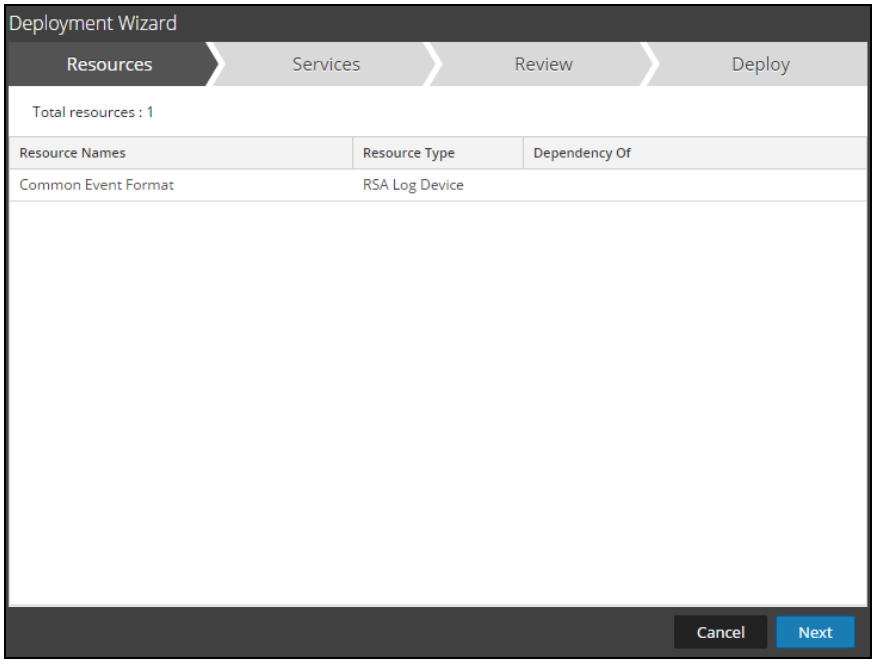
13. Select the checkbox next to **Common Event Format**.



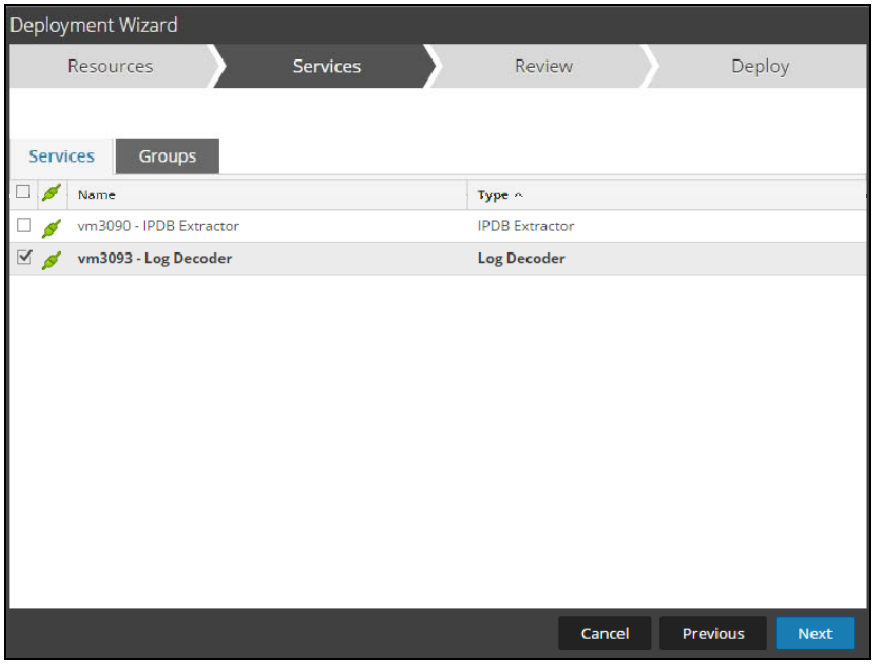
14. Click **Deploy** in the menu bar.



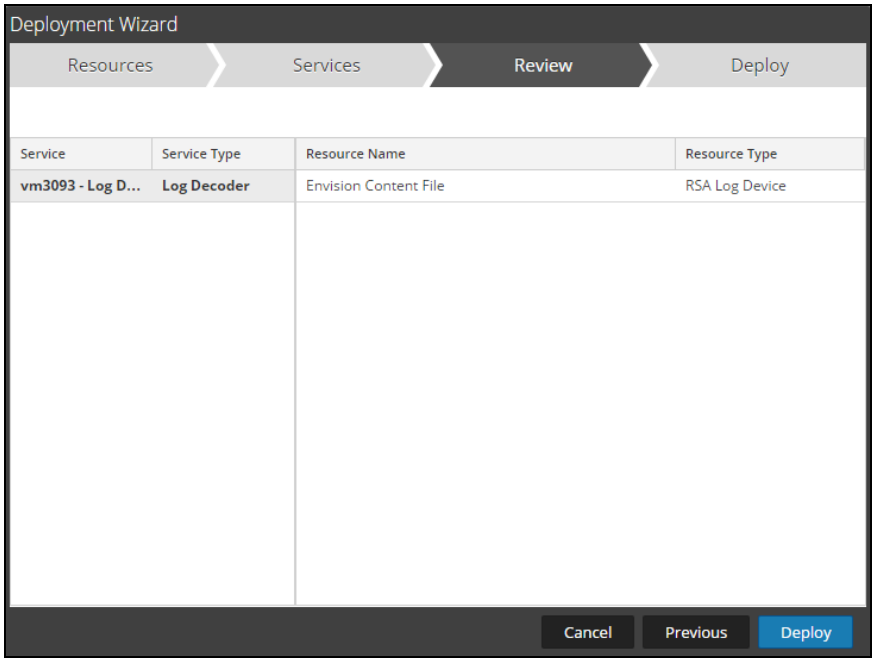
15. Select **Next**.



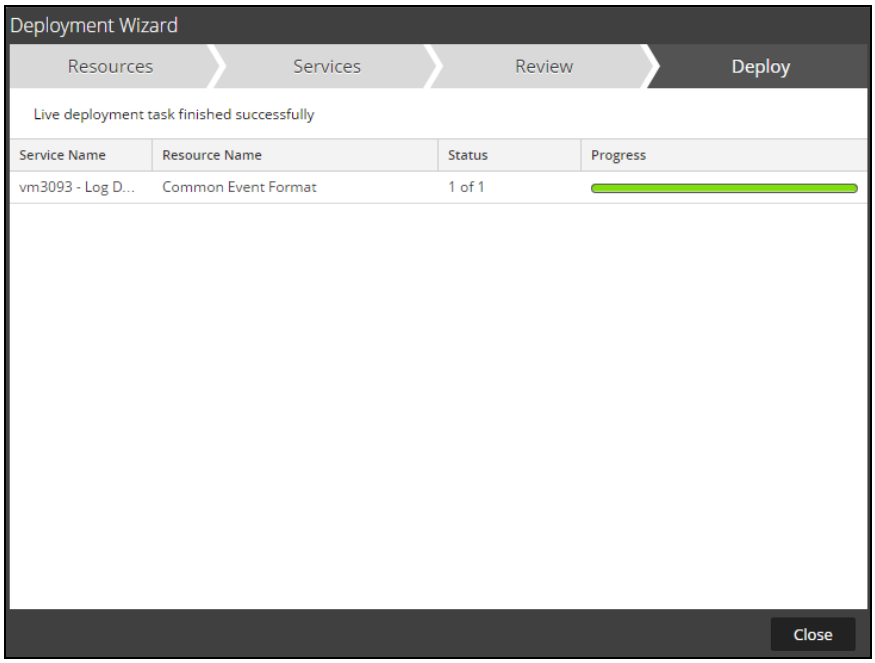
16. Select the **Log Decoder** and Select **Next**.



17. Select **Deploy**.



18. Select **Close**, to complete the deployment of the Common Event Format.



Note: In an environment with multiple Log Decoders, deploy the Common Event Format to each Log Decoder in your network.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the CorreLog SIEM Agent for IBM z/ with RSA Security Analytics. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All CorreLog SIEM Agent for IBM z/OS components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Security Analytics Common Event Format Collection

CorreLog SIEM Agent for IBM z/OS Configuration

After completing the previous section, *Deploy Common Event Format Content File*, you can now collect events from most sources supporting the Common Event Format (CEF).

To configure the CorreLog SIEM Agent for IBM z/OS software to support the RSA Security Analytics CEF format event messages, follow the installation steps detailed in the CorreLog SIEM Agent for IBM z/OS Installation and Operation guide, and further configuration options in the Configuration Reference guide.

The following excerpts have been taken from the Installation and Operations guide for reference, but it is recommended that you follow the complete instructions in the actual guide.

Tailoring the Installation for a Proprietary Syslog Extension

RSA CEF

Begin your testing by tailoring the following members of *hlq*.CZAGENT.CNTL (where *hlq* is the z/OS filename “high level qualifier” chosen during installation) as indicated in the table below. (To “comment out” a line, type an asterisk in column 3 so the line begins //*; to uncomment a line, remove the asterisk in column 3 so the line begins with // and a blank.)

Member	Comment out	Uncomment
CZAGENT	`// PARMS=CZAPARMS`	`//* PARMS=CZAPCEF`
CZAGNJOB	`// SET PRMS=CZAPARMS`	`//* SET PRMS=CZAPCEF`
CZASEND	`// SET PRMS=CZAPARMS`	`//* SET PRMS=CZAPCEF`

Parameter File

The parameter file is normally the CZAPARMS member of the *hlq*.CZAGENT.CNTL dataset (where *hlq* is the “high level qualifier” you specified during installation). For RSA CEF compatibility, use the member CZAPCEF.

Configuring the SIEM type

Ensure that the CZAPCEF parameter member contains the statement

```
OPTIONS SIEM(CEF)
```

to format the SYSLOG output messages to the Common Event Format as required by your RSA Security Analytics system.

Configuring the License statement

You must obtain a LICENSE statement from CorreLog support. Carefully paste it *without any changes* into the parameter file member between the two lines that read

```
; Insert the LICENSE statement between these two lines
; Insert the LICENSE statement between these two lines
```

Do not make any changes to the operands of the LICENSE statement. (Blanks between parameters are not significant.) For example, if your organization name is spelled incorrectly, do not change the LICENSE statement; instead contact CorreLog for a new LICENSE statement.

Configuring the Syslog Server Address

You must, at a minimum, edit the parameter file and specify the IP address of the RSA Security Analytics console. You must also specify the IP port number if it is not the standard Syslog default, port 514. The IP address and optional port are specified on the SERVER statement in the parameter file as a hostname or in standard IPv4 “dotted” format, for example

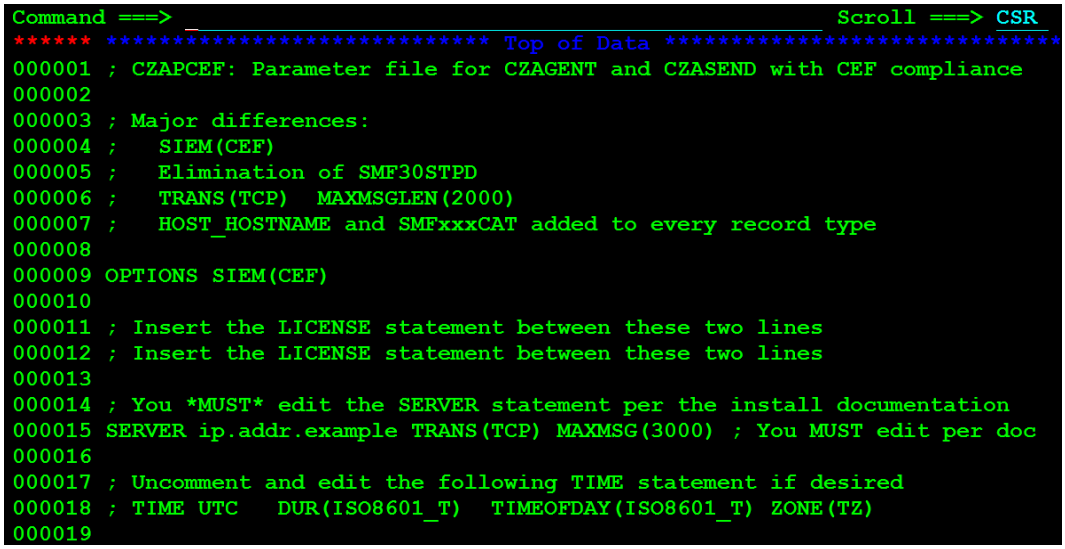
```
SERVER ip.addr.example TRANS(TCP) MAXMSG(3000)
```

or

```
SERVER serverx.ourshop.com:10514
```

(Parameter file statements are free format. You may use any reasonable number of spaces between the word SERVER and the IP address. The IP address and optional port must be punctuated as shown with no embedded blanks.)

Example CZAPCEF Parameter file in an ISPF Edit Session on z/OS



Certification Checklist for RSA Security Analytics

Date Tested: June 22, 2015

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.4	Virtual Appliance
CorreLog SIEM Agent for IBM z/OS	5.5.1	z/OS

Security Analytics Test Case	Result
Device Administration	
Partners device name appears in Device Parsers Configuration	✓
Device can be enabled from Device Parsers Configuration	✓
Device can be disabled from Device Parsers Configuration	✓
Device can be removed from Device Parsers Configuration	✓
Investigation	
Device name displays properly from Device Type	✓
Displays Meta Data properly within Investigator	✓

DRP / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function

Known Issues

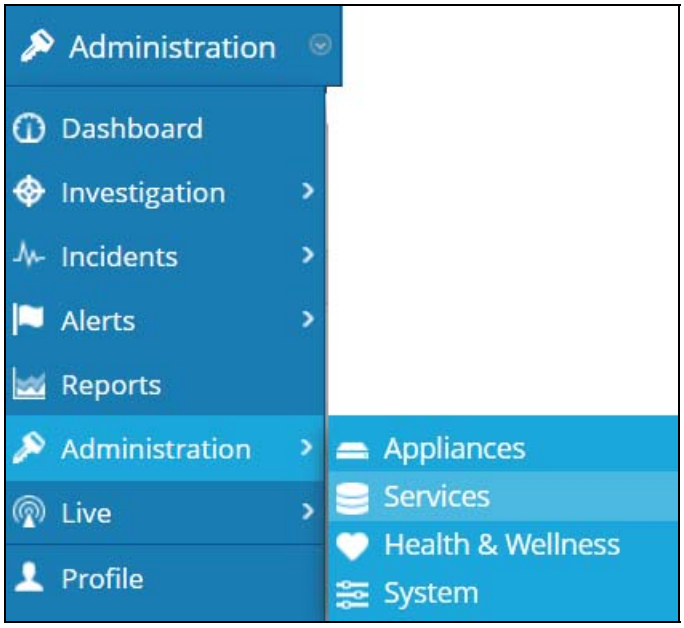
RSA Partner Engineering identified an issue with the RSA SA CEF parser when collecting and parsing cn1, cs3 and cs5 elements. The cn1, cs3 and cs5 elements cannot be viewed or parsed as a result. The issue is being investigated by RSA engineering at the time this guide was published.

Appendix

Security Analytics Disable the Common Event Format Parser

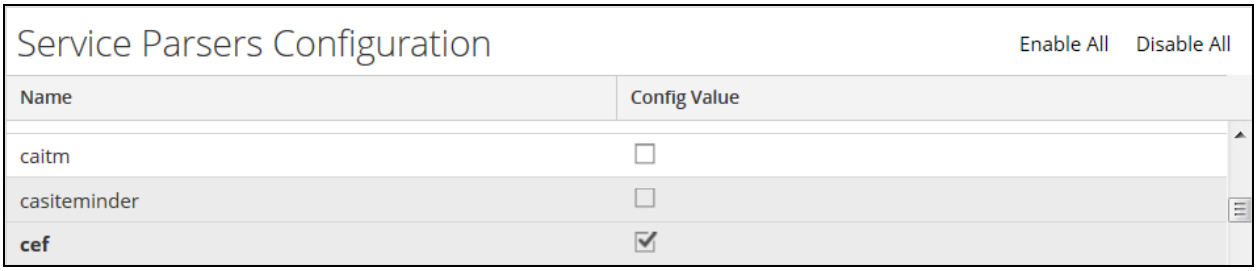
To disable the Security Analytics Common Event Format Parser and not delete it perform the following:

1. Select the Security Analytics **Administration > Services menu**.



2. Select the Log Decoder, then select **View > Config.**

3. From the **Service Parses Configuration** window, scroll down to the CEF parser and uncheck the Config Value checkbox.

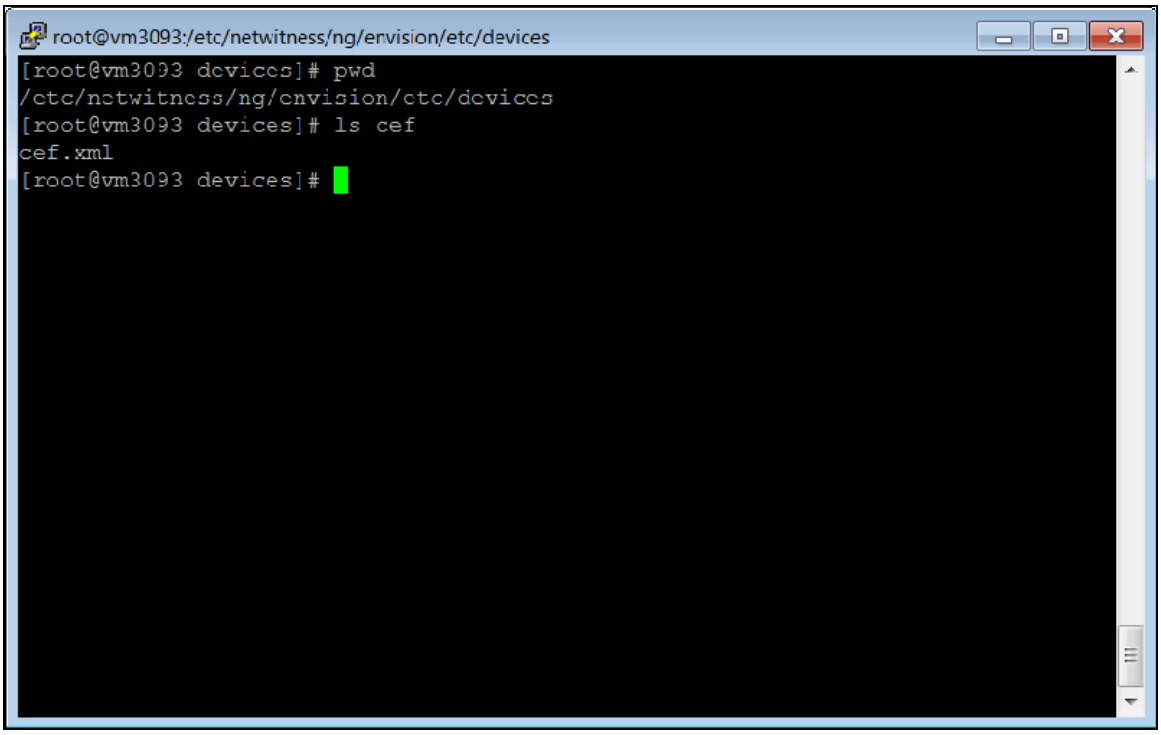


4. Click **Apply** to save settings.

Security Analytics Remove Device Parser

To remove the Security Analytics Integration Package files from the environment, perform the following:

1. Connect to the Security Analytics Log Decoder/Collector Server using SSH and open the **/etc/netwitness/ng/envision/etc/devices** folder.



2. Search for and delete the CEF folder and its contents.