RSA® NETWITNESS®
Logs
Implementation Guide

Raz-Lee
iSecurity for IBM-i 11.4

Daniel Pintal, RSA Partner Engineering
Last Modified: January 3, 2019

RSA READY

Solution Summary

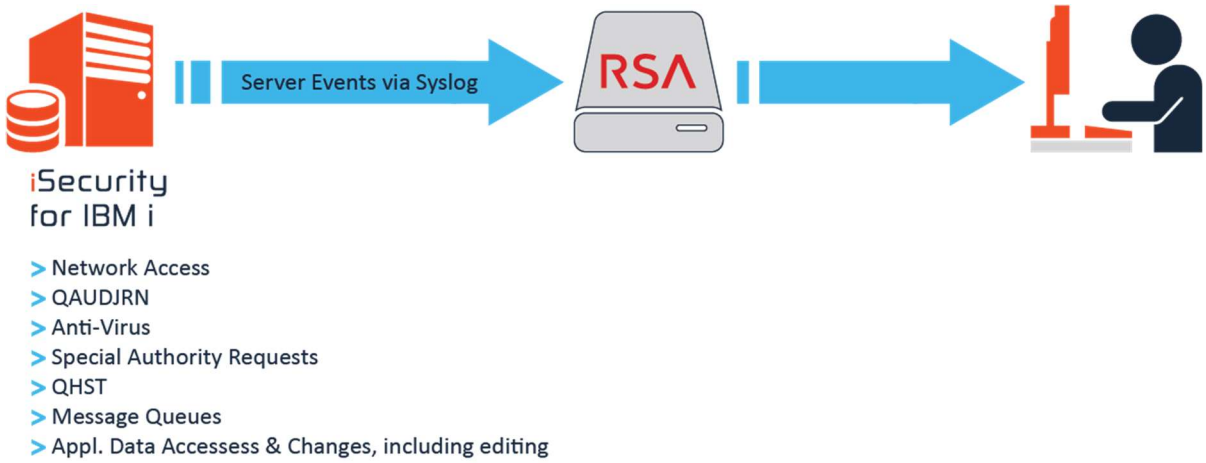
iSecurity for IBM I, by Raz-Lee, triggers in real-time information. It sends in CEF format:

- Security alerts when a potential security breach has been detected.
- Event messages when a site-defined event has occurred; messages can be of varying severity levels, from Informational through Emergency.
- User created messages
- QAUDJRN, QHST, Message Queues, Apache and other IFS logs, and more

It is all pre-defined but modify-able. All special needs can be easily be added.

Providing real-time alerts and event messages and integrating this information within the larger context of RSA Security Analytics monitoring and reporting, will provide multi-platform customers the ability to add previously unsupported IBM I Security-related events into their overall system.

RSA NetWitness Features	
Raz-Lee iSecurity for IBM-i 11.4	
Integration package name	Common Event Format
Device display name within NetWitness	razleesecurity_audit razleesecurity_firewall apache_apache
Event source class	Analysis Firewall
Collection method	Syslog



RSA NetWitness Community

The RSA NetWitness Community is an online forum for customers and partners to exchange technical information and best practices with each other. All NetWitness customers and partners are invited to register and participate in the **RSA NetWitness Community**.

Release Notes

Release Date	What's New In This Release
March 1, 2016	Initial support for Raz-Lee custom parser.
January 3, 2019	Initial support for custom Raz-Lee syslog cef parser.

! > Important: The RSA NetWitness CEF parser is dependent on the partner adhering to the CEF Rules outlined in the *ArcSight Common Event Format (CEF) Guide*. 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.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Raz-Lee iSecurity with RSA NetWitness. 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 and install the required components.

All Raz-Lee components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

! Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure Raz-Lee iSecurity is properly configured and secured before deploying to a production environment. For more information, please refer to the Raz-Lee iSecurity documentation or website (www.razlee.com).

Raz-Lee iSecurity Configuration

SIEM Syslog Configuration

Numerous iSecurity products integrate with SEM/SIEM systems by sending security alerts instantaneously to these systems. Message alerts contain detailed event information about application data changes, deletes or reads of objects and files, emergency changes in user authorities, IFS viruses detected, Ransomware, Malware and other malicious attacks on the IBM i and more.

Use iSecurity Audit to set SIEM general alert definitions and use iSecurity Action to determine if SIEM alerts will be generated in individual cases.

The iSecurity SIEM Syslog feature sends event alerts from various IBM i facilities (such as logs and message systems) to a remote RSA Security Analytics server within a range of severities such as Emergency, Alert, Critical, Error, Warning and more.

1. Type ***STRAUD*** on the IBM i command line; the iSecurity Audit main menu appears. Select option **81. System Configuration.**

```
AUAUDMN                              Audit                          iSecurity/Audit
                                                                 System:   RAZLEE3
 Settings                                   Analysis
  1. OS/400 Audit Features                  41. Queries and Reports
  2. Activation                             42. Display Log

 Real-Time Detection Rules                  Related Modules/Options
 11. Real-Time Auditing                     61. Work With Actions
 12. Firewall/Screen                        62. User Management
 13. Status & Active Job  (SysCtl)          68. Compliance
 14. Message Queue & QHST (SysCtl)          69. Other Related Modules
 15. IFS Logs

 Definitions                                General
 31. Time Groups                            81. System Configuration
 32. Copy Time Groups                       82. Maintenance Menu
 35. General Groups                         83. Central Administration
                                            89. Base Support
 Selection or command
 ===>

 F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
 F13=Information Assistant  F16=System main menu
```

2. From the iSecurity/Base System Configuration menu, select **One SIEM option, options 31-33**.

```
                    iSecurity/Base System Configuration      25/12/18 10:57:56

 Audit                                      SIEM Support
  1. General Definitions                    30. Main Control-----> Active
  3. Log QSH, PASE activity                 31. SIEM 1: S1           Y
  5. Auto start activities in ZAUDIT        32. SIEM 2: --------     N
  9. Log & Journal Retention                33. SIEM 3: --------     N
                                            34. JSON Definitions (for DAM)
 Action                                     35. SNMP Definitions
 11. General Definitions                    36. Twitter Definitions
 12. SMS/Special Definitions
 13. E-Mail Definitions                     39. Syslog test

 SIEM Event Clasification                   General
 21. QSYSOPR, QHST, MsgQ & User msgs        91. Language Support
 22. QAUDJRN Type/Sub Severity Setting      99. Copyright Notice

 Selection ===>

 Release ID . . . . . . . . . . . . . . .  13.46 18-11-07    657CD9D  E4A 5634   8
 Authorization code A (starts with 4) .                                8   RAZLEE3
 Authorization code B (starts with N) .
 F3=Exit    F22=Enter Authorization Code
```

3. In the **SIEM Definitions** screen define the syslog transmission type to use, to which **IP address**, from which **facility** (list of optional facilities below), in what range of **severity** (list below) and the **format** of the message. Preferably use ***CEF**.

```
                              SIEM 1 Definitions              25/12/18 11:04:42

SIEM 1 name . . . . . . . . . .   S1                                Port:    514
SYSLOG type . . . . . . . . . .   1            1=UDP, 2=TCP, 3=TLS
Destination address . . . . . .   10.200.1.103

"Severity" range to auto send .   0 - 7        Emergency - Debug
"Facility" to use . . . . . . .   22           Local use 6 (Local6)

Msg structure or *LEEF, *CEF  .   *CEF

*LEEF, *CEF, *CEF-SPLUNK, or mix variables and constants (ex & %):
&1=First level msg   &3=Msg Id.                &4=System              &5=Module
&6=IP                &7=Audit type &E=SubType  &8=Host name           &9=User
&H=Hour              &M=Minute                 &S=Second              &X=Time
&d=Day in month      &m=Month (mm)             &y=Year (yy)           &x=Date
&a/&A=Weekday (abbr/full)                      &b/&B=Month name (abbr/full)
Convert data to CCSID . . . . .       0        0=Default, 65535=No conversion
Maximum length  . . . . . . . .    9800        128-9800

Note: Re-activate subsystem after changes.
F3=Exit   F12=Cancel            F22=Set SYSLOG handling per audit sub-type
 Modify data, or press Enter.
```

4. From the previous screen select the appropriate option to define the severities for QAUDJRN, select **22. QAUDJRN Type/Sub Severity Setting** and modify it if needed.

```
                              QAUDJRN Severity Setting
                                                Subset by type. .
                                                       by entry .
 Type options, press Enter.                            by text. .
   blank=Do not send   0=Emergency   1=Alert   2=Critical   3=Error
   4=Warning   5=Notice   6=Info   7=Debug
 SIEM   IBM  Audit
 1 2 3  STD  Type  Type
                   *AUTFAIL   operation to which the user was not authorized.
 7 4 4   4   AF B  *PGMFAIL   A program ran a restricted machine interface
                              instruction.
 7 4 4   4   AF B  *AUTFAIL   Restricted instruction
 7 5 5   4   AF C  *PGMFAIL   A program which failed the restore-time program
                              validation checks was restored. Information about
                              the failure is in the Validation Value Violation
                              Type field of the record.
 7 5 5   4   AF C  *AUTFAIL   Validation failure
 7 4 4   4   AF D  *PGMFAIL   A program accessed an object through an
                              unsupported interface or callable program not
                              listed as a callable API.
                                                                     More...
 F3=Exit  F21=Set 1 as IBM  F22=Set 2 as IBM  F23=Set 3 as IBM
```

5. From that same screen select **21. QSYSOPR, QHST, MsgQ & User msgs for instructions**.
6. To send Message Queues, QHST to SIEM perform the following steps:
   - From iSecurity Audit main menu Select option **14. Message Queue & QHST (SysCtl).**
   - **Select 1. Control Message Queues/QHST** and **F6=Add New.**

```
                              Add Message Queue

Message queue  . . . . . . . .  QHST          Name, QHST
  Library  . . . . . . . . . .    QSYS        Name, *LIBL
Active definition  . . . . . .  Y             A=Auto start, N=No,
                                              Y=Yes, requires manual activation
Operation mode . . . . . . . .  5             1=Periodic, 5=QHST, 9=Immediate
  For 1, Number of seconds . .    300
  For 9, Break program . . . .  *STD          Name, *STD SMZ4/AUSOURCE AUMSGBRK
    Library  . . . . . . . . .                Name, *LIBL

Send to SIEM . . . . . . . . .  Y             Y=Yes, N=No
Send to user Data Queue  . . .  *NONE         Name, *NONE
           Library . . . . . .                Name, *LIBL

Check rules & perform Actions.  Y             Y=Yes, N=No
  For Check rules, Group Id  .  @9            @1, @2, ..., @9=QHST
Duplicates may appear if Action sends to SIEM/Data Queue, selected above.

QHST requires Operation mode 5, Group @9.

F3=Exit    F4=Prompt              F12=Cancel
```

7. In the same way Administrators can define Controls for any Message Queue. To specify similar rules for number of message queues, give them the same Group ID. Select **11. Message Queue rules** and follow the instructions to specify whether to perform an action that will send all or part of the messages.

8. To send IFS logs (e.g. WebSphere, Apache) to SIEM. From iSecurity Audit main menu select **15. IFS Logs**, **1. Work with Definition**, **F6=Add New, and specify the log details.**

```
                              Add IFS Log Auditing

 Subject . . . . . . . . . .  WEBSPHERE
 Description . . . . . . . .  WebSphere server
 Inform SIEM 1 2 3 . . . . .  Y                 Y=Yes
 Auto-start  . . . . . . . .  Y                 Y=Yes

 Dir . . . . . . . . . . . .  /www/webshpere/log

 File prefix . . . . . . . .  access
 Original input format . . .  *CEF              *CEF, *LEEF, *FREE
 Severity  . . . . . . . . .  7                 0-7
 Add date  . . . . . . . . .  Y                 Y=Yes
 Add system  . . . . . . . .  Y                 Y=Yes
 Add subject . . . . . . . .                    Y=Yes

 Maximum message length is 5000.
 F3=Exit   F12=Cancel
```

9. To send Firewall messages to Syslog, in command line type **STRFW** to open iSecurity Firewall, select **81. System Configuration menu**.

```
                    iSecurity (part I) Global Parameters    25/12/18 12:17:07

 Firewall  *FYI*                          SIEM Support
  1. General Definitions                  70. Main Control-----> Active
  2. Additional Settings                  71. SIEM 1: SIEM         Y
  3. User Exit Programs                   72. SIEM 2:              N
  4. Transaction Post Processing          73. SIEM 3:              N
  5. Intrusion Detection System           74. JSON                 N
  6. Password Exit Programs
  7. Enable ACTION (CL Script + more)     79. Setting Severity for Servers
  9. Log Retention

 Other Products Definitions Active        General
 11. Command                  N           81. iSecurity/Base Configuration
 21. Screen                   N           91. Language Support
 31. Password                 Y           99. Copyright Notice
 41. 2FA

 Selection ===>
 Release ID . . . . . . . . . . . . . .  17.51 18-06-14    657CD9D  E4A 5634   8
 Authorization code . . . . . . . . . .                              8   RAZLEE3
 F3=Exit    F22=Enter authority code
```

10. Select option **71-73**. Syslog Definitions.

```
                              SYSLOG Definitions                25/12/18 12:23:46

SIEM 1 name . . . . . . . . . .   SIEM                                Port:    514
SYSLOG type . . . . . . . . . .   1       1=UDP, 2=TCP, 3=TLS
Send if in FYI mode . . . . . .   Y       Y=Yes, N=No
Destination address . . . . . .   10.200.100.3

"Severity" range to auto send .   0 - 7   Emergency - DEBUG
                                          Rejects are considered 1=Alert
"Facility" to use . . . . . . .   22
Msg structure or *LEEF, *CEF  .   *CEF

*LEEF (IBM QRadar), *CEF (HP ArcSight) or mix variables and constants (ex & %):
&1=First level msg    &3=Msg Id.            &4=System              &5=Module
&6=IP                 &7=Service            &8=Host name           &9=User
&H=Hour               &M=Minute             &S=Second              &X=Time
&d=Day in month       &m=Month (mm)         &y=Year (yy)           &x=Date
&a/&A=Weekday (abbr/full)                   &b/&B=Month name (abbr/full)
Convert data to CCSID . . . . .       0   0=Default, 65535=No conversion
Maximum length  . . . . . . . .    1024   128-9800

Note: Re-activate subsystem after changes.
F3=Exit   F12=Cancel
```

11. From the previous screen, select **79**. Setting Severity for Servers and modify it if needed.
12. You may send SIEM alerts based on **selective situations** in the system.
    Messages and events might be filtered by their field values, directed to **Action**,

    Action can send alerts with text that contains fields from the events by:

    - E-mail
    - Local workstation message queue
    - Local user message queue
    - Remote user on another systems over the network
    - SMS to a cellular telephone
    - SIEM

    Among the subjects that can be handled by Action, are:
    Audit log – QAUDJRN, QHST, Message Queues, etc.
    Firewall events – ODBC, FTP, Telnet, etc.
    Changes of values on data files, including comparison to previous values (AP-Journal)
    And more.

13. In this scenario, after defining the filter, you will be presented with the following screen. Select **8=SIEM** and specify to which SIEM to direct the alert.

> **Important: More than one SIEM can be specified. Use commas or blanks to separate their numbers.**

```
                                Modify Alert Message

Type choices, press Enter.

  Action Name  . . . .      VICT150301
  Description. . . . .      Created by Action

Define alert message recipients
 1=E-mail  2=Message Queue  3=User  4=Remote User  5=LAN user  6=SMS  7=Special
 8=SIEM  9=SNMP             T=Twitter
  Message ID . . . . .      *AUTO          *AUTO, Message ID

 Type    Recipient address, *USER, *DEV, *JOB, *SYSTEM; SIEM 1/2/3
  1      VICTOR@RAZLEE.COM
  8      1
  _
  _
  _                                                                  More...

F3=Exit   F4=Prompt                          F12=Cancel
```

14. Anti-Virus, Anti-Ransomware, Screen (adjusted screen time out) allow for simple selection of reporting to 1-3 of the predefined SIEMs.

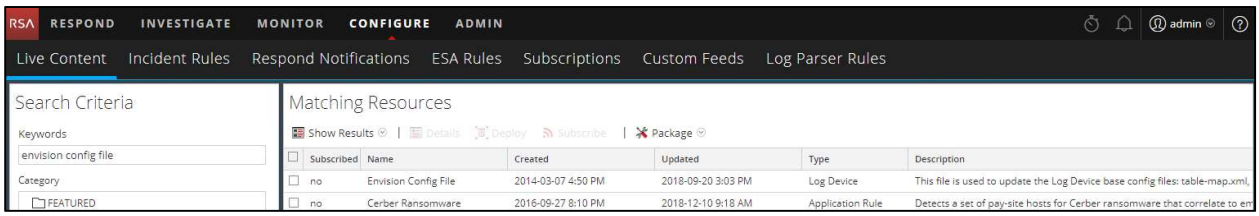
RSA NetWitness Configuration

Deploy the enVision Config File

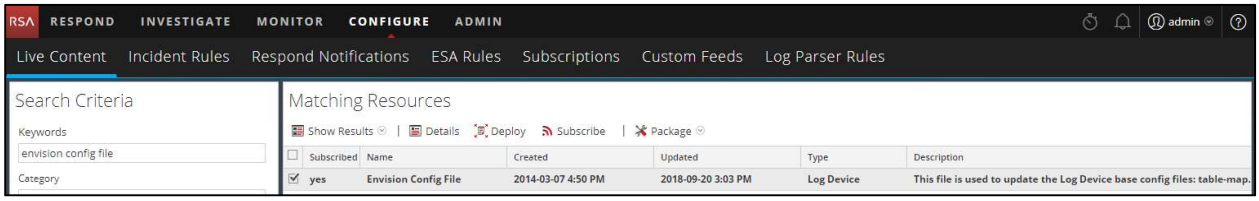
To use the RSA Common Event Format, deploy the *enVision Config File* from the **NetWitness Live** module. Log into NetWitness and perform the following actions:

! Important: Using this procedure will overwrite the existing table_map.xml.

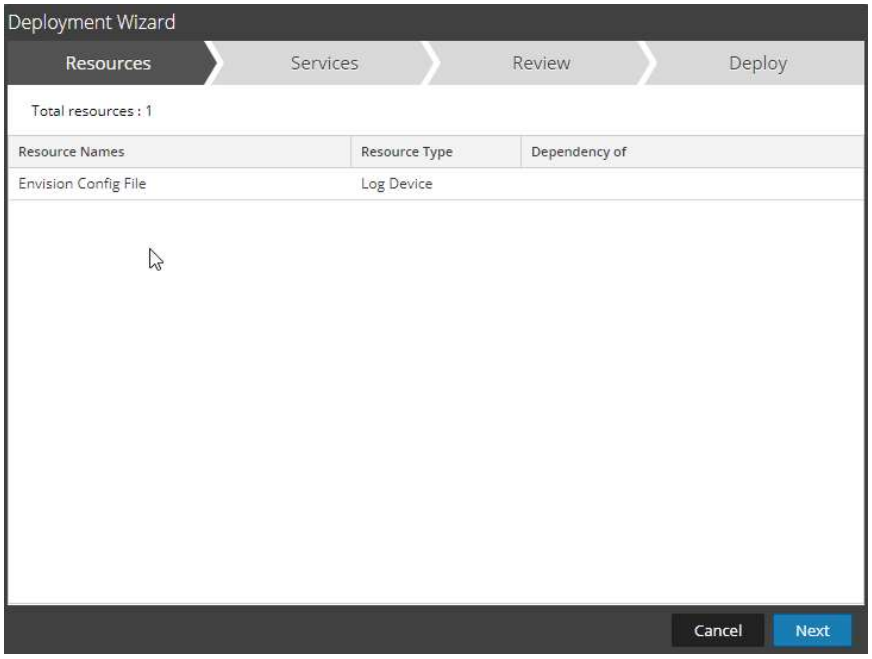
1. From the NetWitness menu, select **Configure > Live Content**.
2. In the keywords field, enter: **enVision**.
3. NetWitness will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



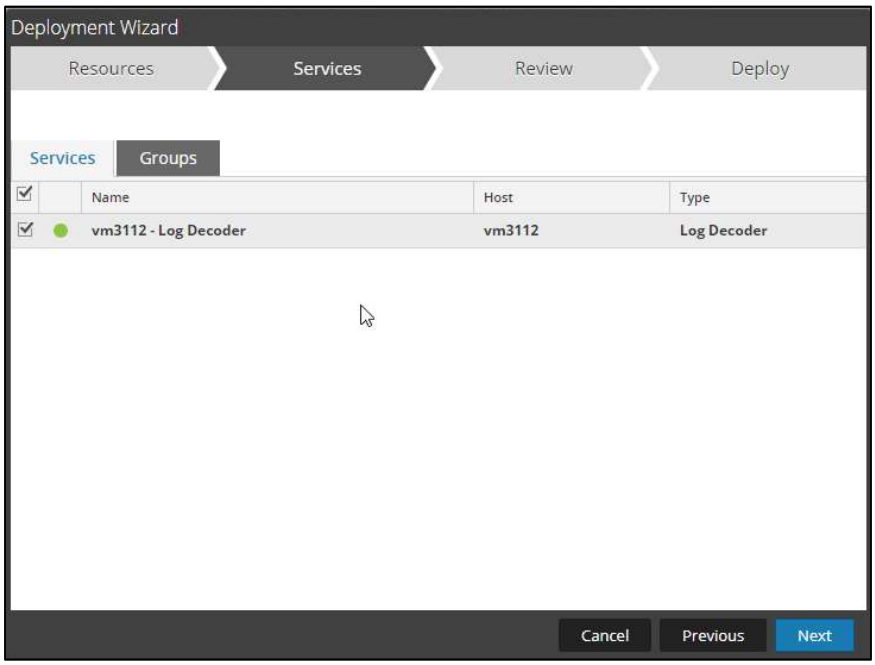
5. Click **Deploy** in the menu bar.



6. Select **Next**.

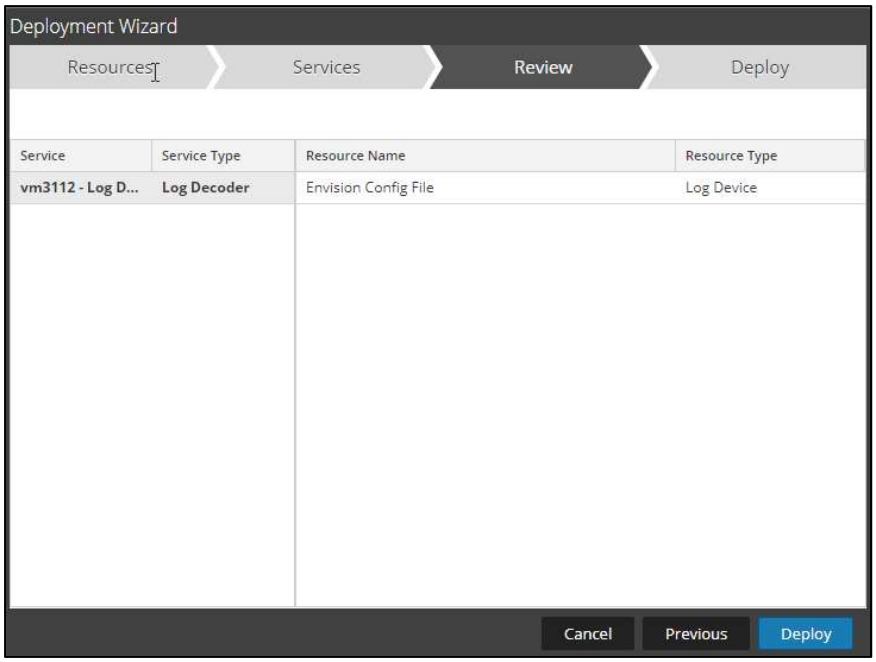


7. Select the **Log Decoder** and select **Next**.

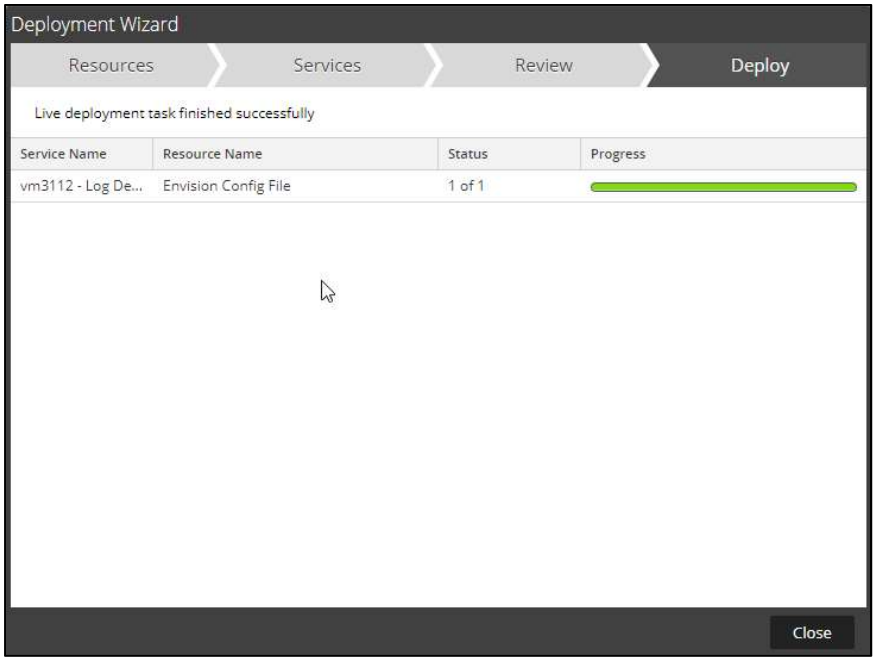


! Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



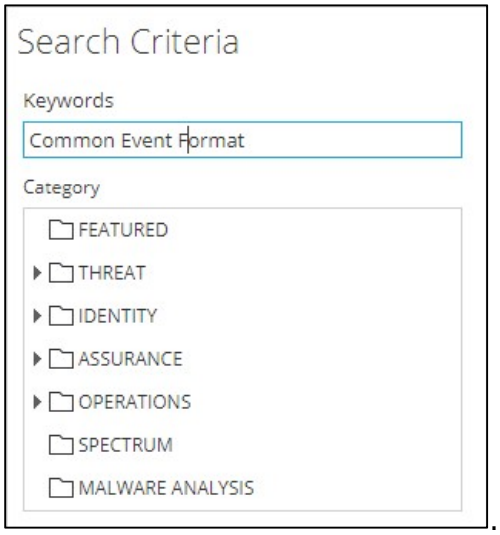
9. Select **Close**, to complete the deployment of the Envision Config file.



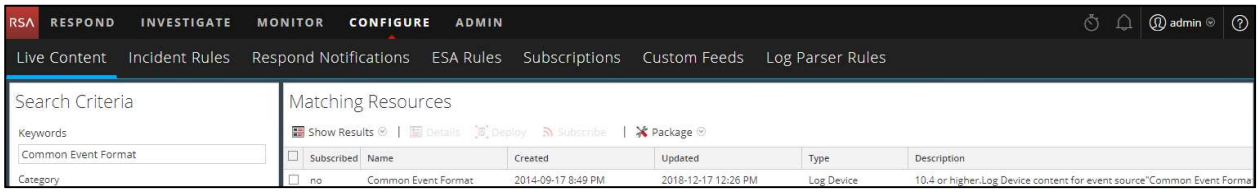
Deploy the Common Event Format

Next, you will need to deploy the *Common Event Format file* from the **NetWitness Live** module. Log into NetWitness and perform the following actions:

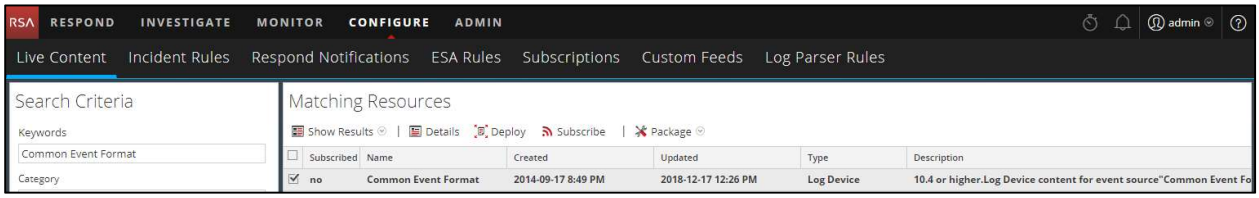
1. From the NetWitness menu, select **Live > Search**.
2. In the keywords field, enter: **Common Event Format**



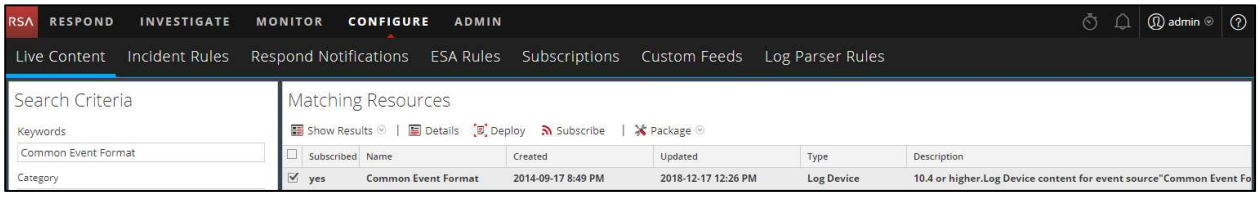
3. RSA NetWitness will display the **Common Event Format** in Matching Resources.



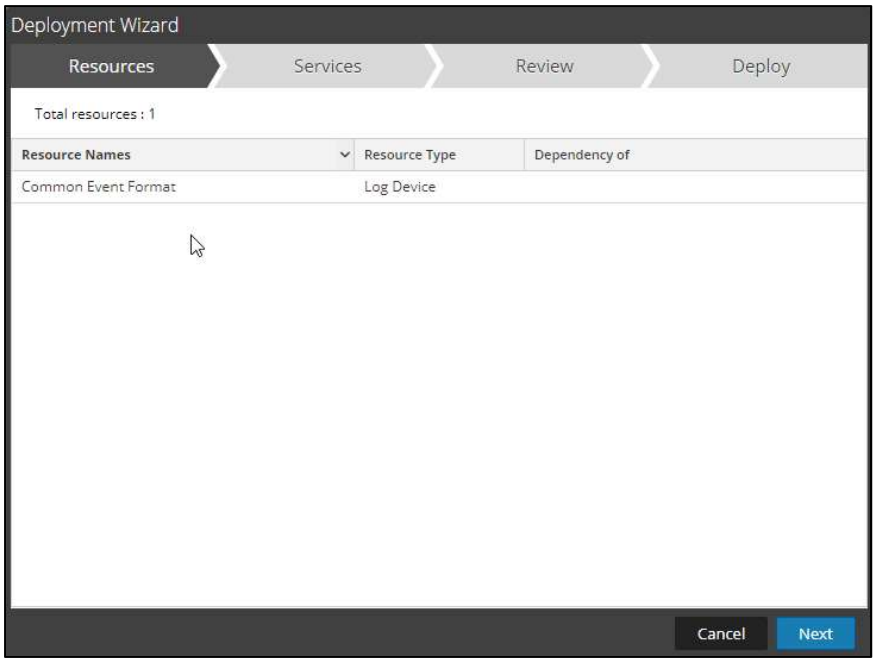
4. Select the checkbox next to **Common Event Format**.



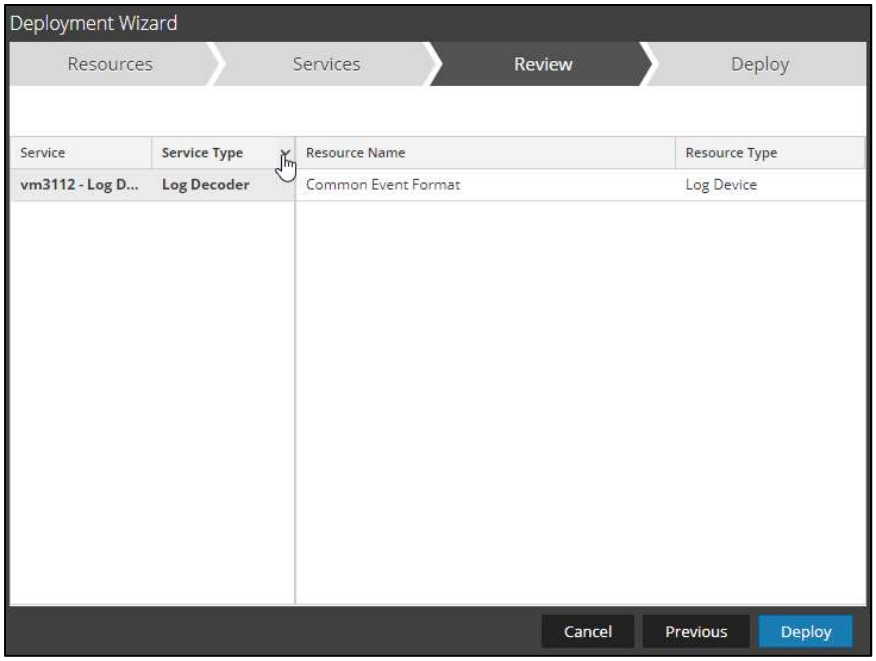
5. Click **Subscribe** and click **Deploy** in the menu bar.



6. Select **Next**.

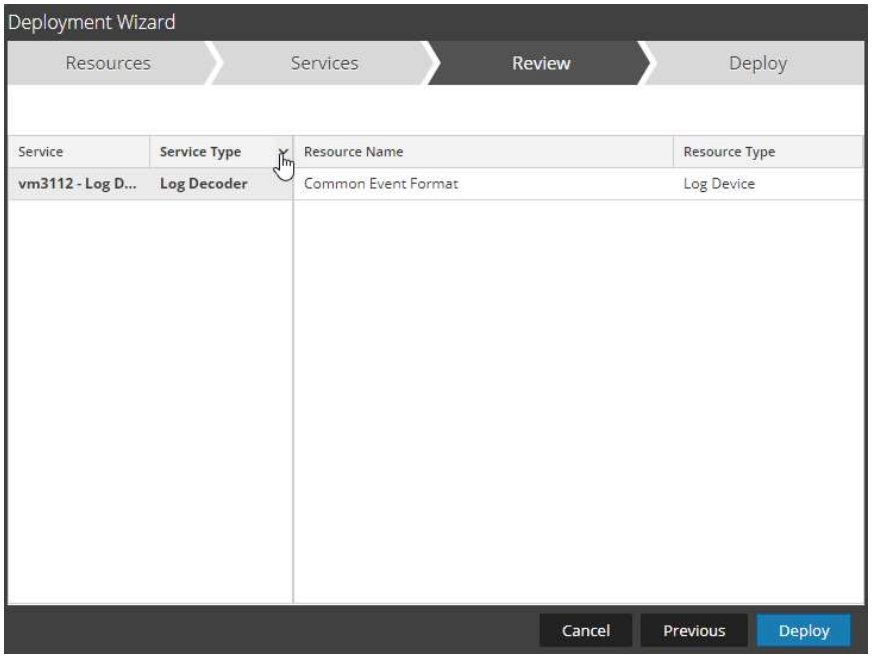


7. Select the **Log Decoder** and Select **Next**.

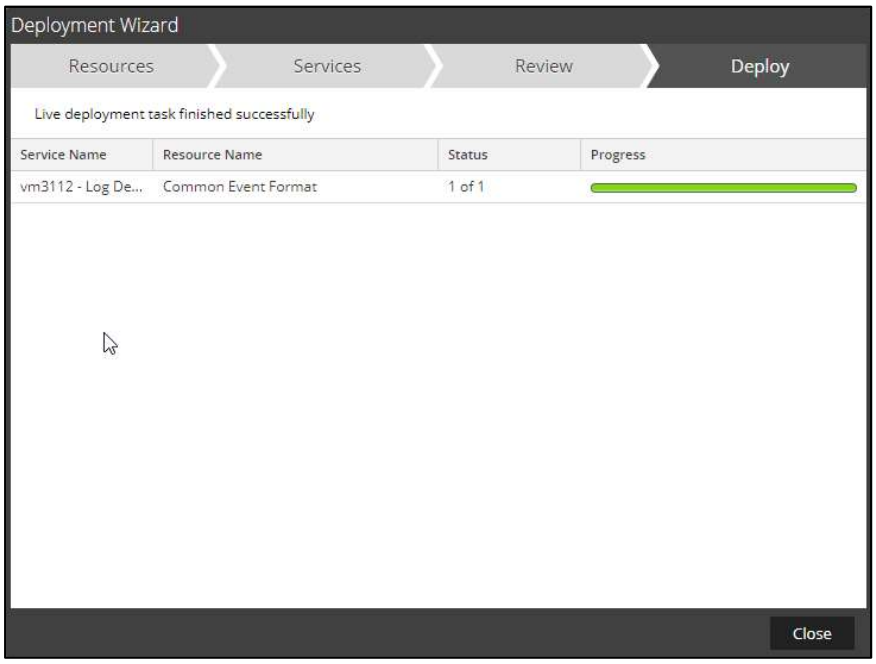


! Important: In an environment with multiple Log Decoders, deploy the Common Event Format to each Log Decoder in your network.

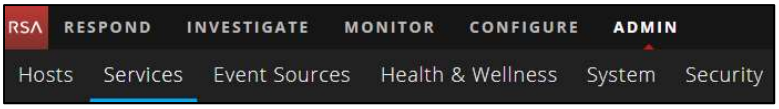
8. Select **Deploy**.



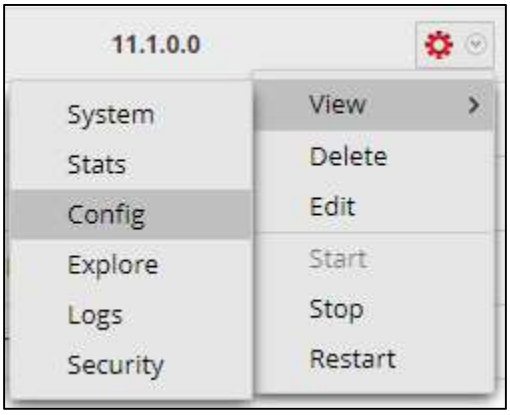
9. Select **Close**, to complete the deployment of the Common Event Format.



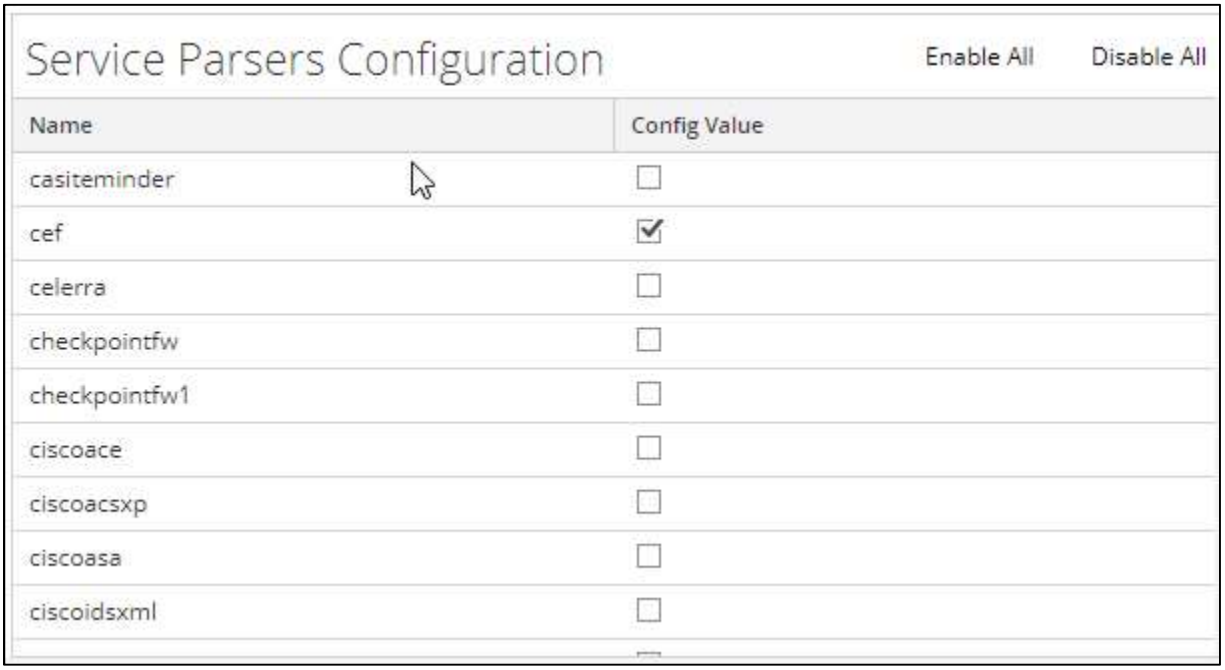
10. Ensure that the CEF Parser is enabled on the Log Decoder(s) by selecting **Admin > Services** from the NetWitness Dashboard.



11. Locate the Log_Decoder and click the gear to the right and select **View>Config**.



12. **Check** the box next to the cef Parser within the Service Parsers Configuration and select **Apply**.



13. Restart the **Log Decoder services**.

Edit the Common Event Format to collect Endgame event times

! Important: The cef.xml file is overwritten by NetWitness Live during updates, it is important to maintain backups of the file in the event of a typing error or unforeseen event.

1. Using WinSCP or other application to access the RSA NetWitness Log Decoder open a connection and locate the **/etc/netwitness/ng/envision/etc/devices/cef** folder. Backup cef.xml and edit the existing CEF.XML file.
2. Locate the end of the <MESSAGE section and copy/paste the following lines below into the file after the **/>** of the preceding <MESSAGE and contents;

Example

```
<MESSAGE
       id1="razleesecurity_audit"
       id2="razleesecurity_audit"
       functions="&lt;@msg:*PARMVAL($MSG)&gt;&lt;@event_time:*EVNTTIME($MSG,'%W-%M-%D-
%H.%T.%S',param_event_time)&gt;"
       content="&lt;param_event_time&gt;&lt;msghold&gt;" />

<MESSAGE
       id1="razleesecurity_firewall"
       id2="razleesecurity_firewall"
       functions="&lt;@msg:*PARMVAL($MSG)&gt;&lt;@event_time:*EVNTTIME($MSG,'%W-%M-%D-
%H.%T.%S',param_event_time)&gt;"
       content="&lt;param_event_time&gt;&lt;msghold&gt;" />

<MESSAGE
       id1="apache_apache"
       id2=" apache_apache"
       functions="&lt;@msg:*PARMVAL($MSG)&gt;&lt;@event_time:*EVNTTIME($MSG,'%W-%M-%D-
%H.%T.%S',param_event_time)&gt;"
       content="&lt;param_event_time&gt;&lt;msghold&gt;" />
```

Edit the Common Event Format Custom to support custom fields

! Important: The cef-custom.xml file is not overwritten by NetWitness Live during updates, however it is important to maintain backups of the file in the event of a typing error or unforeseen event.

1. Using WinSCP or other application to access the RSA NetWitness Log Decoder open a connection and locate the **/etc/netwitness/ng/envision/etc/devices/cef** folder.
2. If the **cef-custom.xml** file does not exist copy the attached **cef-custom.xml.razlee** file to the folder specified above and rename to **cef-custom.xml**.
3. If the file does exist create a backup of cef-custom.xml.
4. Edit the **cef-custom.xml** file and the attached **cef-custom.xml.razlee** file. Copy the contents of the **cef-custom.xml.razlee** file from between the **<ExtensionKeys>** and **</ExtensionKeys>**, do not include the <ExtensionKeys> tags. Paste the contents copied into the existing cef-custom.xml file between the **<ExtensionKeys>** tags.
5. The attached **cef-custom.xml.razlee** file below contains keys used specifically for the integration with Raz-Lee.

cef-custom.xml.razlee

Edit the NetWtness Table-Map-Custom.xml file

! Important: The Table-Map-Custom.xml file is not overwritten by NetWitness Live during updates, however it is important to maintain backups of the file in the event of a typing error or unforeseen event.

1. Using WinSCP or other application to access the RSA Netwitness Log Decoder open a connection and locate the **/etc/netwitness/ng/envision/etc/** folder.
2. If the **table-map-custom.xml** file does not exist copy the attached **table-map-custom.xml.razlee** file to the folder specified above and rename to **table-map-custom.xml**.
3. If a **table-map-custom.xml** file exists, backup the **table-map-custom.xml** file**.**
4. Edit the existing **table-map-custom.xml** and the attached **table-map-custom.xml.razlee** file copy and paste the contents of the **cef-custom.xml.razlee** file from between the **<mappings>…</mappings> >**, do not include the **<mappings>** tags. Paste the contents copied into the existing **table-map-custom.xml** file between the **<mappings>** tags.
5. The attached **table-map-custom.xml.razlee** file below contains keys used specifically for the integration with Raz-Lee.

table-map-custom.xml.razlee

6. Restart the **Log Decoder services** to begin log collection.

Raz-Lee razleesecurity_audit Collection partial sample from NetWitness Investigator:

device.type = 'razleesecurity_audit' Cancel

Collection Time	Event Type	Theme	Size	Details
2019-01-10T20:11:43	Log	razleesecurity_audit	1 KB	ip.src : 1.1.1.167 sessionid : 297833 device.ip : 10.165.148.47 medium : 32 device.type : razleesecurity_audit device.class : Analysis version : 1.0 event.type : MJS1300 event.desc : JS/M Actions that affect jobs Severity : 5 user.src : DB result : success jobName : 976702/QUSER/QZDASOINIT PGM : QSYS/QZDASOINIT reason : JS/M Modify profile or group profile netname : other src country.src : Australia latdec.src : -33.494 longdec.src : 143.2104 isp.src : Cloudflare org.src : Cloudflare SequenceNum : 0012250814 TypeofJob : B SubtypeJob : J Job.name : QZDASOINIT Job.user.name : QUSER job.num : 976702 Device.desc : *N Effective.user : DB Job.desc : QDFTSVR Job.desc.lib : QGPL Job.queue : *N Job.que.lib : *N Output.queue : *DEV Out.que.lib : *N Print.device : PRT01 Library.list : *N Effective.group : *N Supp.grps : *N JUID.desc : N JUID.name : DB

Raz-Lee razleesecurity_firewall Collection sample from NetWitness Investigator:

device.type = 'razleesecurity_firewall' Cancel

Collection Time	Event Type	Theme	Size	Details
2019-01-10T20:11:43	Log	razleesecurity_firewall	497 bytes	ip.src : 178.249.3.46 sessionid : 297846 device.ip : 10.165.148.47 medium : 32 device.type : razleesecurity_firewall device.class : Firewall version : 1.0 event.type : GRE6534 event.desc : 37/A *FTPCLN FTP Client-Outgoing Rqst Validation Severity : 9 user.src : RLTOOLS result : success jobName : 260790/RLTOOLS/FTP2AU PGM : *NONE/*NONE reason : 37/A FTP Client-Outgoing Rqst Validation netname : other src country.src : Germany city.src : Becherbach latdec.src : 49.6534 longdec.src : 7.6805 isp.src : PfalzConnect GmbH org.src : PfalzConnect GmbH RequestFunction : CHG_DIR ActionAllowed : 0 DecisionLevel : FWIPA AuthGrntToUser : *ALL AuthGrntForObj : 0.0.0.0 ServerId : 37 msg.id : razleesecurity_firewall device.disc : 100 device.disc.type : razleesecurity_firewall did : vm3112 rid : 418 ip.all : 10.165.148.47 user.all : RLTOOLS ip.all : 178.249.3.46

Raz-Lee apache_apache Collection partial sample from NetWitness Investigator:

device.type = 'apache_apache' Cancel

Collection Time	Event Type	Theme	Size	Details
2019-01-10T20:11:43	Log	apache_apache	704 bytes	ip.src : 1.1.1.175 sessionid : 297839 device.ip : 10.165.148.47 medium : 32 device.type : apache_apache device.class : Analysis msg.id : apache_apache event.type : 304 event.desc : GET /list.pdf Severity : Unknown app : HTTP hypertextproto : HTTP/1.1 host.src : 1.1.1.175 netname : other src country.src : Australia latdec.src : -33.494 longdec.src : 143.2104 isp.src : Cloudflare org.src : Cloudflare host.dst : S520.RAZLEE.COM ip.dstport : 80 process : apache url : /list.pdf action : GET directory : /www/webserver/htdocs/ filename : list.pdf extension : pdf Virtual Host : S520.RAZLEE.COM Responce Time : 0 bytes.src : 0 Referer : http://1.1.1.105/index1.html alias.host : S520.RAZLEE.COM ip.addr : 1.1.1.105 netname : other misc process : apache_access_log reqClientApp : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36 X-Forwarded-For : - device.disc : 100 device.disc.type : apache_apache did : vm3112 rid : 411

Certification Checklist for RSA NetWitness

Date Tested: January 10, 2019

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	11.2.1	Virtual Appliance
Raz-Lee iSecurity for IBMi	11.4	IBMi

NetWitness Test Case	Result
Device Administration	
Partner's 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	✓

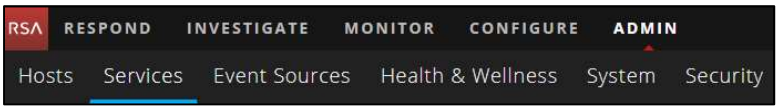
✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

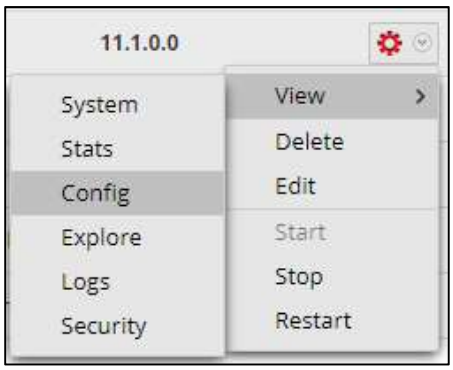
NetWitness Disable the Common Event Format Parser

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

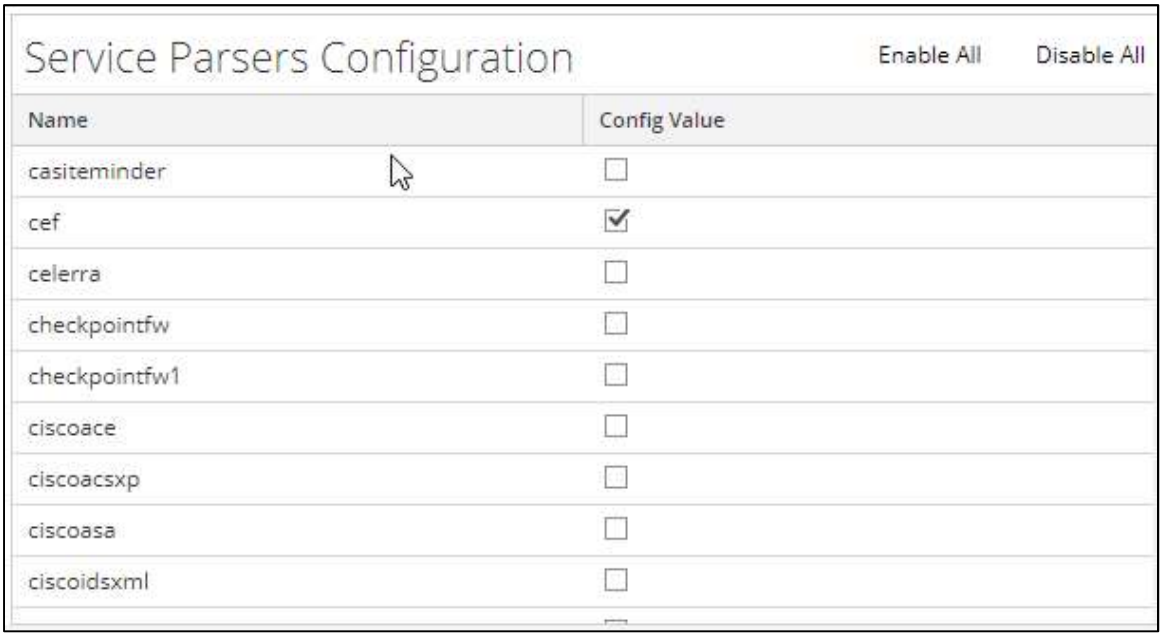
1. Select the NetWitness **Admin > Services**.



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.

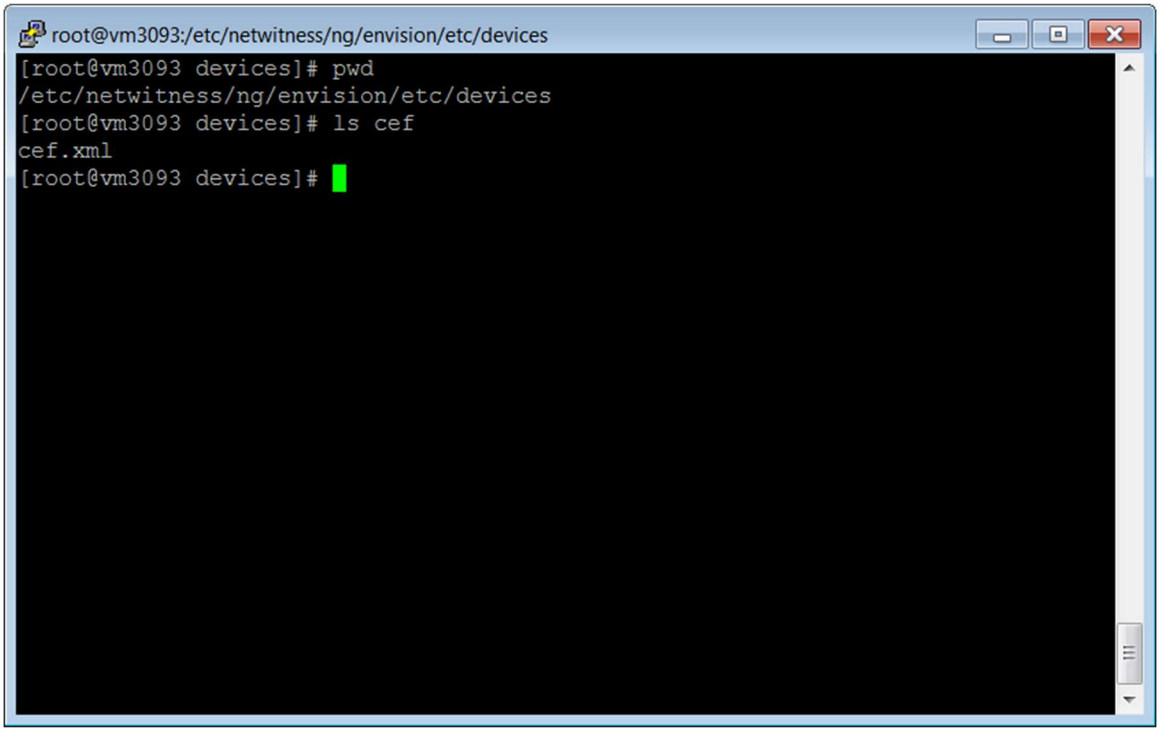


4. Click **Apply** to save settings.

NetWitness Remove Device Parser

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

1. Connect to the NetWitness 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.