CyberArk

Privileged Threat Analytics

RSA Ready Implementation Guide for RSA Security Analytics

Last Modified: January 11, 2016

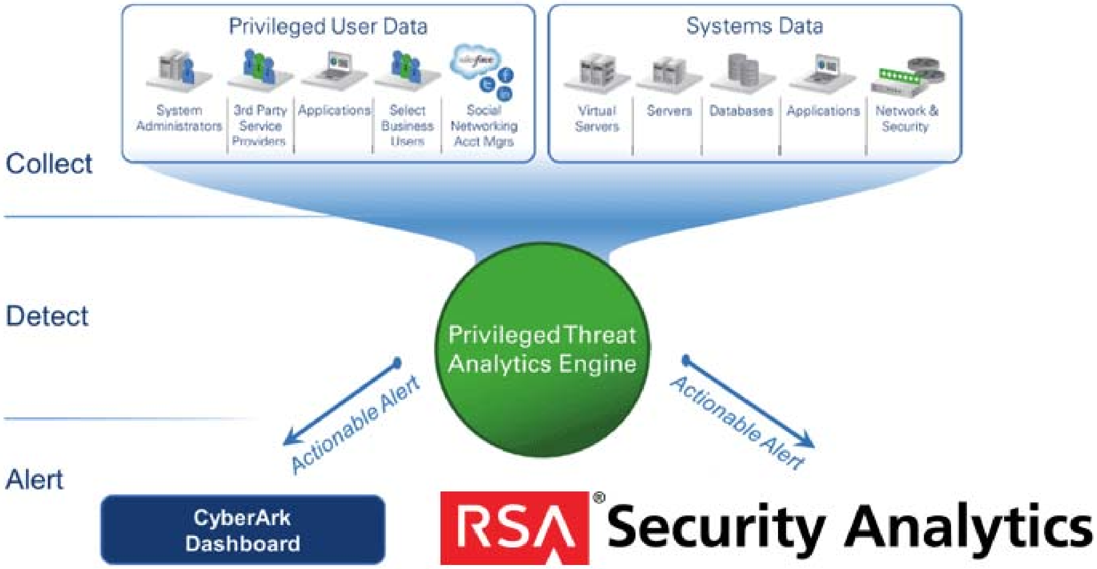
Partner Information

Product Information	
Partner Name	CyberArk
Web Site	www.cyberark.com
Product Name	Privileged Threat Analytics
Version & Platform	2.6.3.1 (CentOS Release 6.4)
Product Description	CyberArk Privileged Threat Analytics™ is an expert system for privileged account security intelligence, providing targeted, immediately actionable threat analytics by identifying previously undetectable malicious privileged user and account activity.

Solution Summary

This solution can be used as a method to configure RSA Security Analytics to forward all logon events from Windows or UNIX systems. In addition, it will provide CyberArk customers with the steps necessary to forward CyberArk PTA events to RSA SA.

RSA Security Analytics Features	
Privileged Threat Analytics	
Integration package name	Common Event Format
Device display name within Security Analytics	cyberark_pta
Collection method	Syslog



RSA Security Analytics (SA) Community

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

Release Notes

Release Date	What's New In This Release
12-11-2015	Initial support for CyberArk PTA

! › 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.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the CyberArk Privileged Threat Analytics 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.

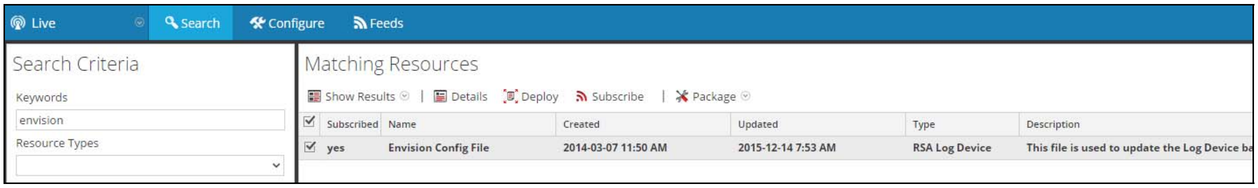
All CyberArk Privileged Threat Analytics components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Deploy enVision Config File

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

Note: Using this procedure will overwrite the existing table_map.xml.

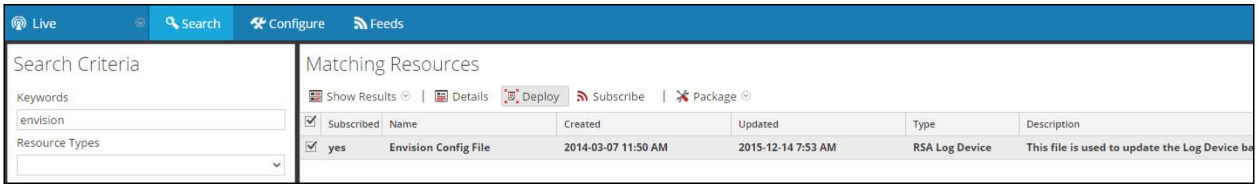
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **enVision**.
3. Security Analytics will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



Keywords: envision

☑	Subscribed	Name	Created	Updated	Type	Description
☑	yes	Envision Config File	2014-03-07 11:50 AM	2015-12-14 7:53 AM	RSA Log Device	This file is used to update the Log Device ba

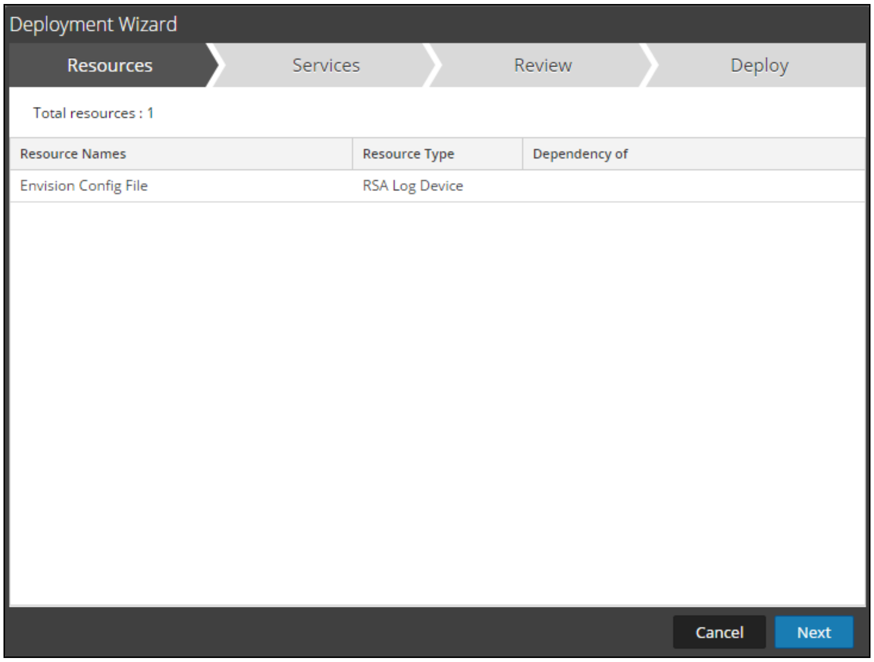
5. Click **Deploy** in the menu bar.



Keywords: envision

☑	Subscribed	Name	Created	Updated	Type	Description
☑	yes	Envision Config File	2014-03-07 11:50 AM	2015-12-14 7:53 AM	RSA Log Device	This file is used to update the Log Device ba

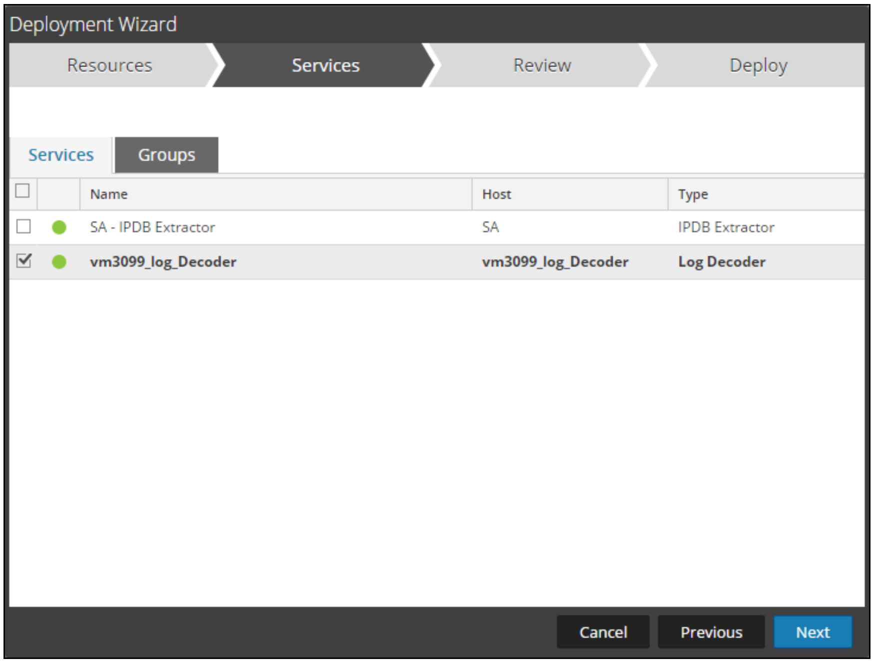
6. Select **Next**.



Total resources : 1

Resource Names	Resource Type	Dependency of
Envision Config File	RSA Log Device	

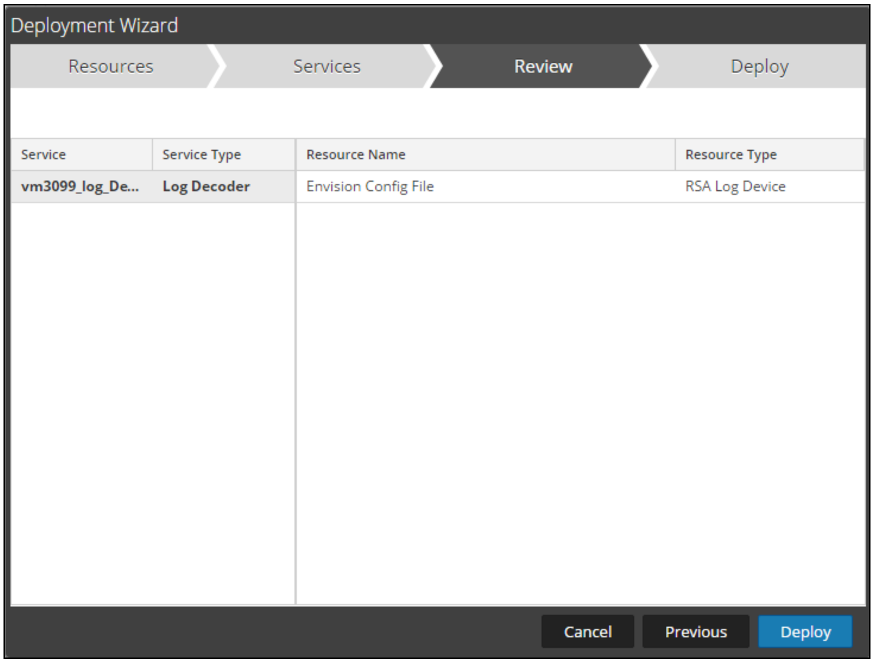
7. Select the **Log Decoder** and select **Next**.



□		Name	Host	Type
□	●	SA - IPDB Extractor	SA	IPDB Extractor
☑	●	**vm3099_log_Decoder**	**vm3099_log_Decoder**	**Log Decoder**

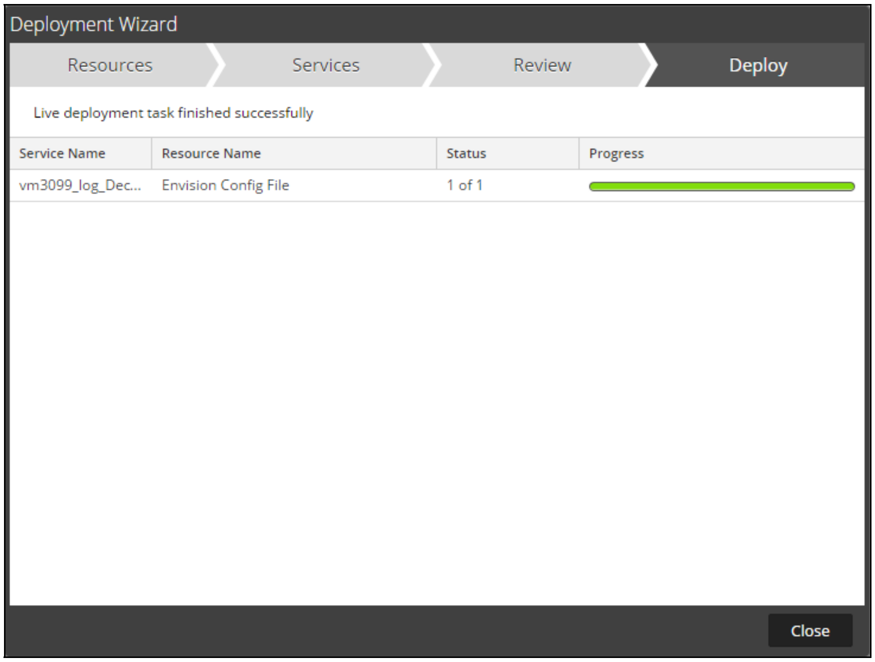
Note: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



Service	Service Type	Resource Name	Resource Type
vm3099_log_De...	Log Decoder	Envision Config File	RSA Log Device

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



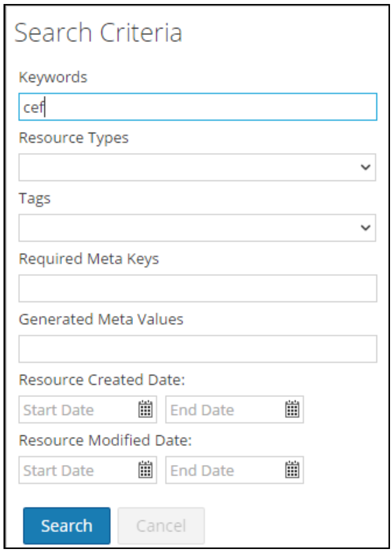
Live deployment task finished successfully

Service Name	Resource Name	Status	Progress
vm3099_log_Dec...	Envision Config File	1 of 1	

Deploy Common Event Format

In order to use RSA Partner created content, you must first deploy the *Common Event Format 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: **CEF**



Search Criteria

Keywords: cef

Resource Types:

Tags:

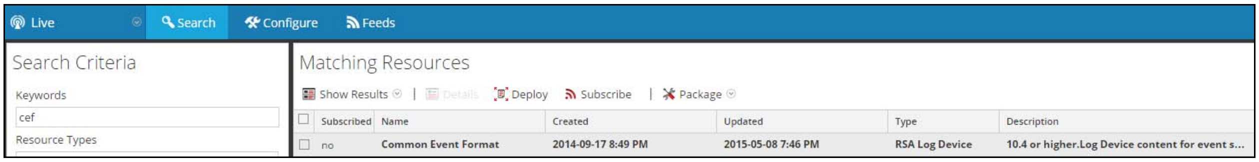
Required Meta Keys:

Generated Meta Values:

Resource Created Date: Start Date / End Date

Resource Modified Date: Start Date / End Date

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

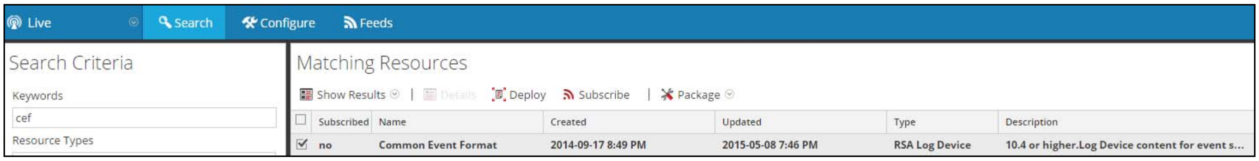


Search Criteria — Keywords: cef; Resource Types

Matching Resources

☐	Subscribed	Name	Created	Updated	Type	Description
☐	no	Common Event Format	2014-09-17 8:49 PM	2015-05-08 7:46 PM	RSA Log Device	10.4 or higher.Log Device content for event s...

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

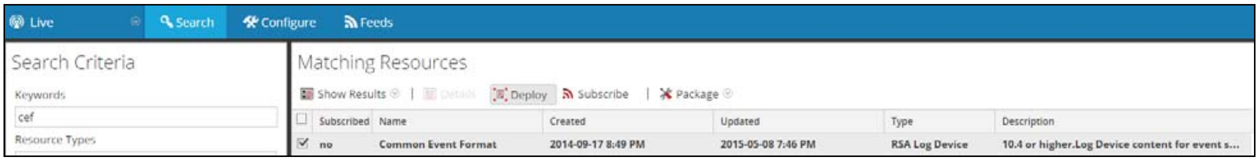


Search Criteria — Keywords: cef; Resource Types

Matching Resources

☐	Subscribed	Name	Created	Updated	Type	Description
☑	no	Common Event Format	2014-09-17 8:49 PM	2015-05-08 7:46 PM	RSA Log Device	10.4 or higher.Log Device content for event s...

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

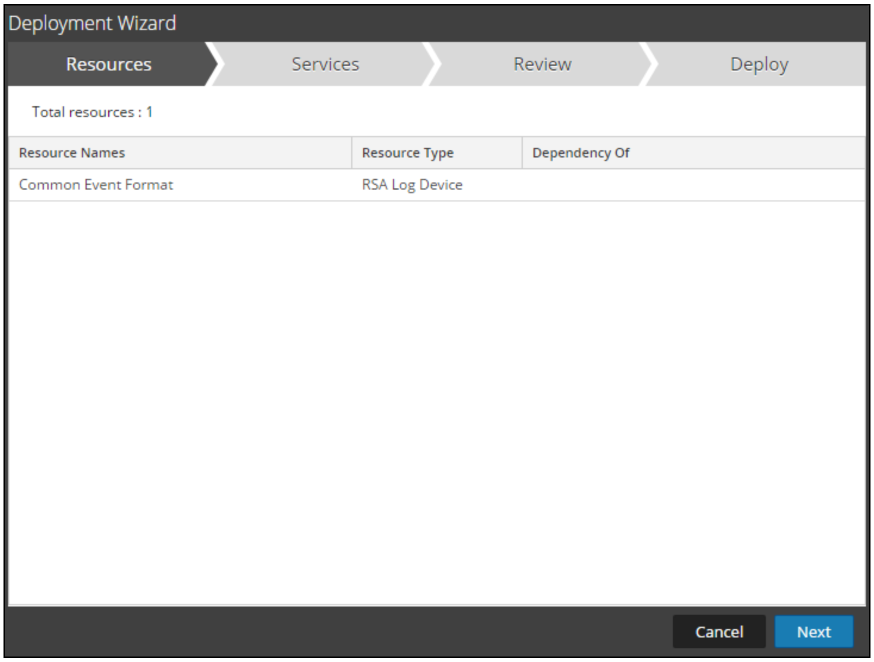


Search Criteria — Keywords: cef; Resource Types

Matching Resources

☐	Subscribed	Name	Created	Updated	Type	Description
☑	no	Common Event Format	2014-09-17 8:49 PM	2015-05-08 7:46 PM	RSA Log Device	10.4 or higher.Log Device content for event s...

6. Select **Next**.

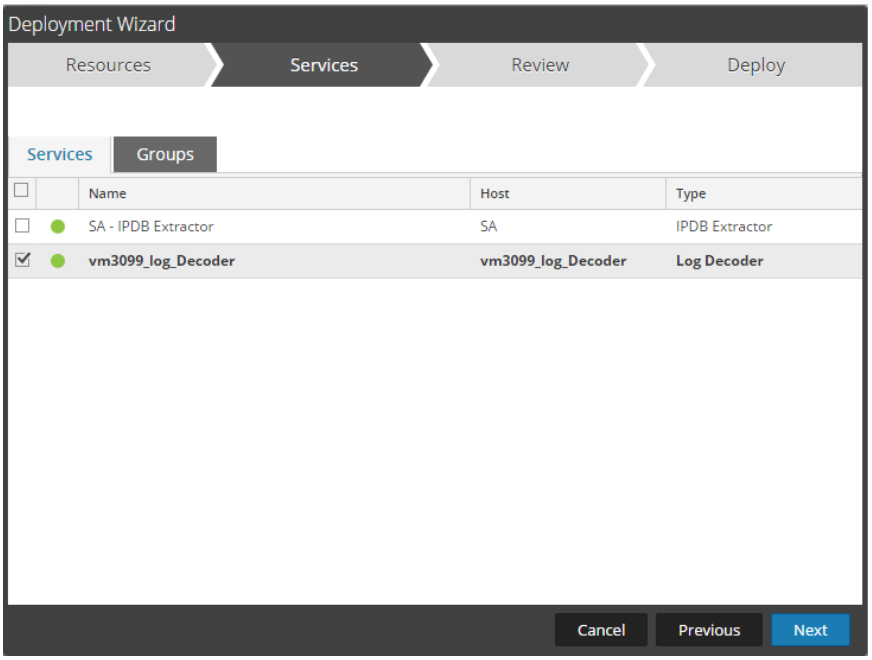


Deployment Wizard

Total resources : 1

Resource Names	Resource Type	Dependency Of
Common Event Format	RSA Log Device	

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

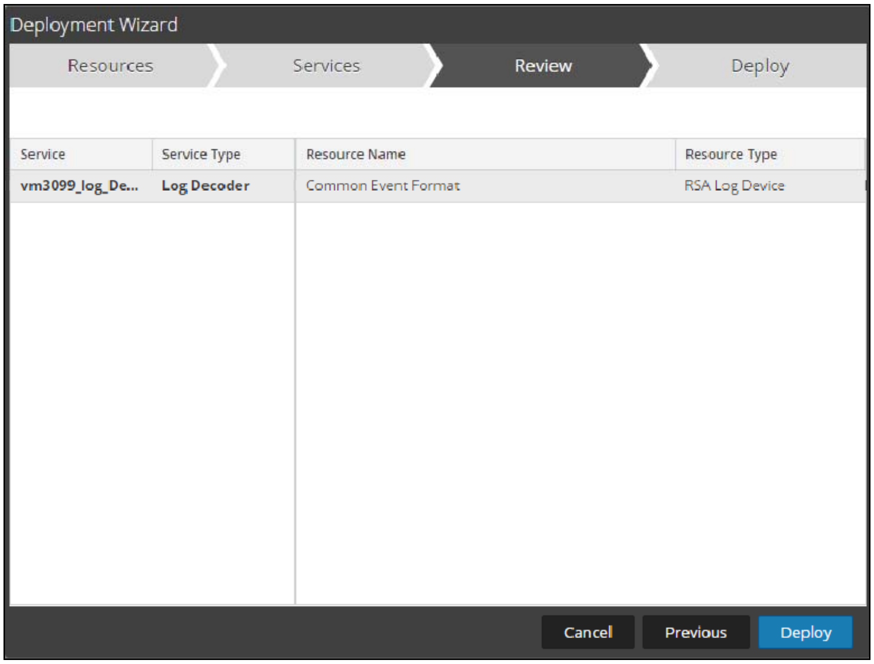


Deployment Wizard

□		Name	Host	Type
□	●	SA - IPDB Extractor	SA	IPDB Extractor
☑	●	vm3099_log_Decoder	vm3099_log_Decoder	Log Decoder

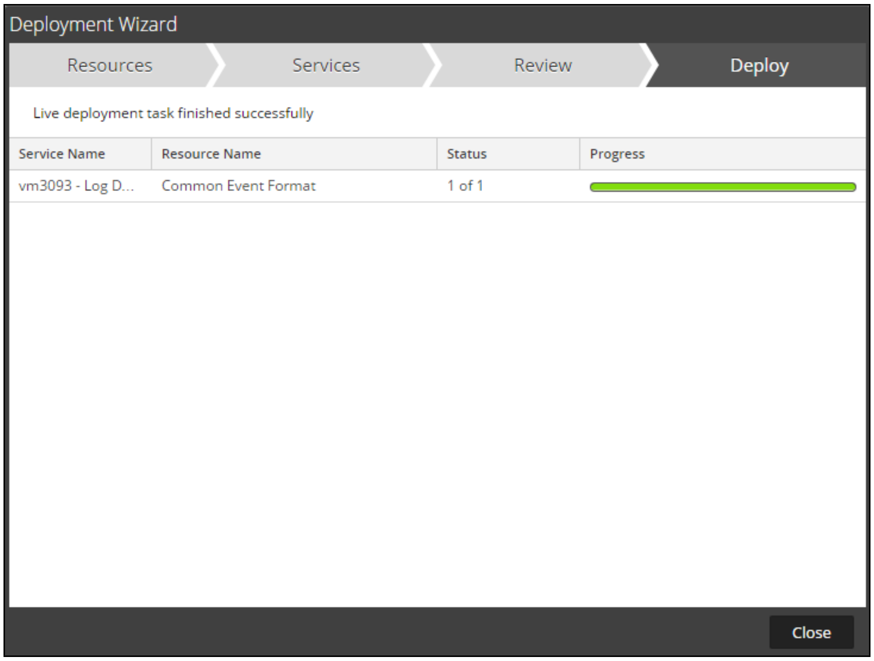
Note: In an environment with multiple Log Decoders, deploy the Common Event Format to each Log Decoder in your network.

8. Select **Deploy**.



Service	Service Type	Resource Name	Resource Type
vm3099_log_De...	Log Decoder	Common Event Format	RSA Log Device

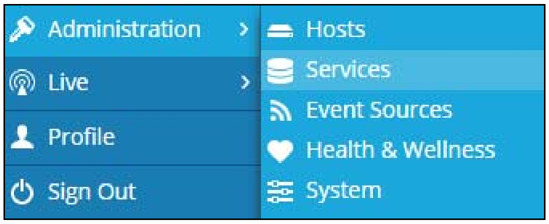
9. Select **Close**, to complete the deployment of the Common Event Format.



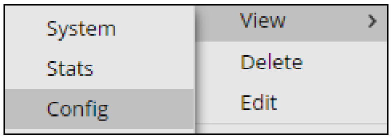
Live deployment task finished successfully

Service Name	Resource Name	Status	Progress
vm3093 - Log D...	Common Event Format	1 of 1	🟩

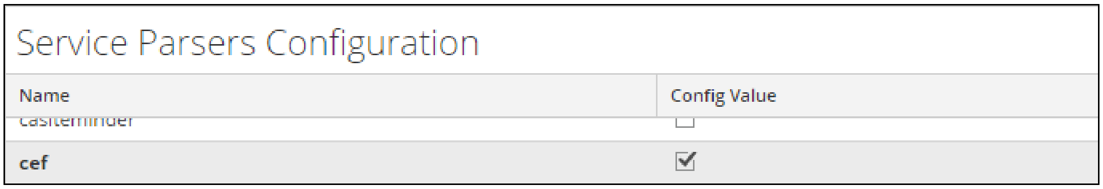
10. Insure that the CEF Parser is enabled on the Log Decoder(s) by selecting **Administration, Services** from the SA Dashboard.



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**.



Service Parsers Configuration

Name	Config Value
casteminder	☐
cef	☑

13. Restart the **Log Decoder services**.
14. Using WinSCP or other application to access the RSA SA Concentrator open a connection and locate the **/etc/netwitness/ng** folder. Create a new file named **index-concentrator-custom.xml** and copy/paste the following lines below into the new file.

```
<?xml version="1.0" encoding="utf-8"?>
<language level="IndexNone" defaultAction="Auto">
        <key description="severity" format="Text" level="IndexValues" name="severity"
valueMax="100000"/>
        <key description="url" format="Text" level="IndexValues" name="url" valueMax="100000"/>
        <key description="hardware_id" format="Text" level="IndexValues" name="hardware.id"
        valueMax="100000"/>
</language>
```

15. Save index-concentrator-custom.xml and restart the **Concentrator services**.

Note: If the contents of the index-concentrator-custom.xml already exists add only the section between the <language…>, </language> tags.

Security Analytics Common Event Format Collection

CyberArk Privileged Threat Analytics Configuration

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

Once CyberArk Privileged Threat Analytics is configured following the PTA Implementation Guide, the inbound data received from RSA Security Analytics will be parsed (using inbound plugins delivered with the product), and once consumed, and analyzed by PTA the findings (if any) output can be forwarded to RSA Security Analytics for further analysis, correlation, or monitoring. Please follow the next steps to configure the PTA outbound messages to be sent to Security Analytics:

1. On the PTA machine, open the **systemparm.properties** configuration file using a text editor such as vi:

   ```
   vi /opt/tomcat/diamond-resources/local/systemparm.properties
   ```

2. Uncomment the **syslog_outbound** property and edit the following parameters in the sample configuration:

   - **Host** – The Host/IP address of the your RSA Security Analytics log decoder.
   - **Port** – The port number through which the syslog records will be sent to the log decoder.
   - **Protocol** – The protocol used to transfer the syslog records to the log decoder.
   - **Format** – The format used to transfer the syslog records. Set it to rsacefv2.

3. Save the configuration file and close it.
4. Restart the **PTA**.

Security Analytics Logon Event Forwarding to PTA

Configure RSA Security Analytics Forwarding Rule

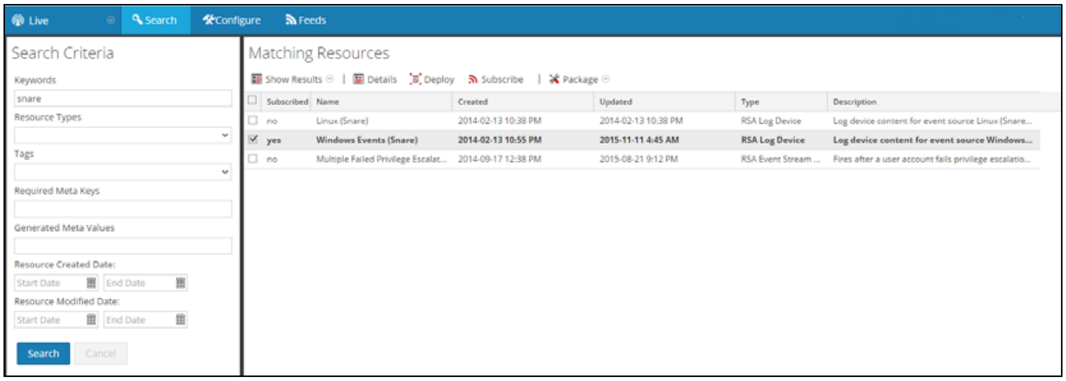
To enable forwarding logon events from Windows or UNIX systems a forwarding rule within RSA Security Analytics must be created.

1. Login to RSA Security Analytics with an administrator account.
2. Using steps above on how to Deploy the enVision Config and Common Event Format File's deploy the **Windows Events (Snare)** and **rhlinux** parsers.

Note: In this example SA is configured to forward Windows Events (Snare) and rhlinux logon events. A forwarding rule is not limited to only these device types or for this integration.The RSA SA Forwarding rule can be tailored to support any single or combination of device xml's.

Reference RSA SA Configure Syslog Forwarding to Destination **for more information.**

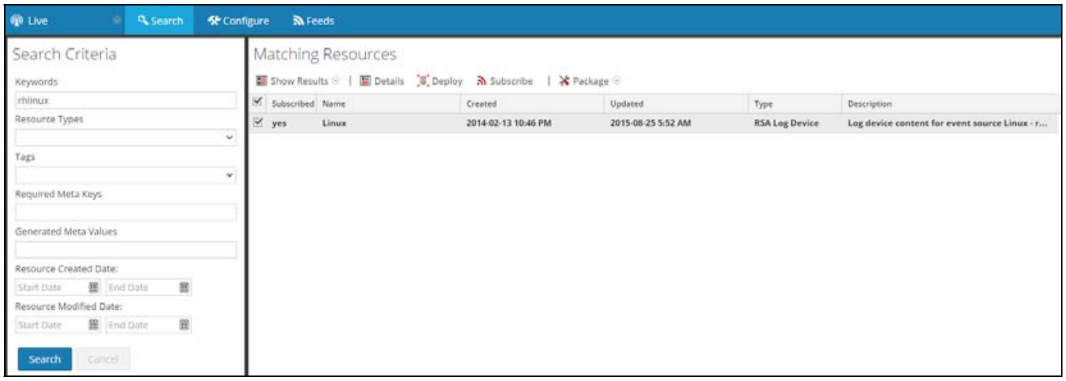
3. Search RSA Live for the **Windows Events (Snare)** parser and **Deploy to Log Decoders**.



Keywords: snare

☐	Subscribed	Name	Created	Updated	Type	Description
☐	no	Linux (Snare)	2014-02-13 10:38 PM	2014-02-13 10:38 PM	RSA Log Device	Log device content for event source Linux (Snare...
☑	**yes**	**Windows Events (Snare)**	**2014-02-13 10:55 PM**	**2015-11-11 4:45 AM**	**RSA Log Device**	**Log device content for event source Windows...**
☐	no	Multiple Failed Privilege Escalat...	2014-09-17 12:38 PM	2015-08-21 9:12 PM	RSA Event Stream ...	Fires after a user account fails privilege escalatio...

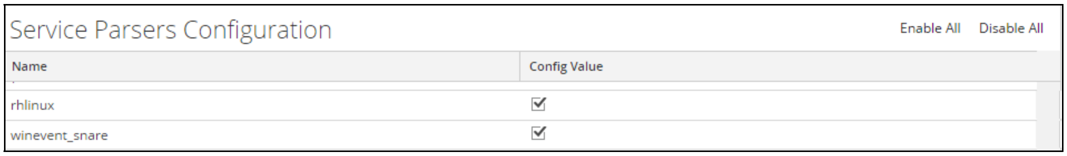
4. Search RSA Live for the **rhlinux** parser and **Deploy to Log Decoders**.



Keywords: rhlinux

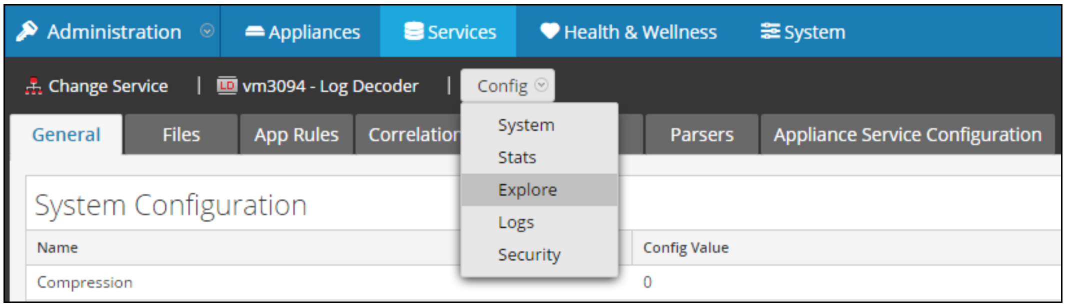
☑	Subscribed	Name	Created	Updated	Type	Description
☑	**yes**	**Linux**	**2014-02-13 10:46 PM**	**2015-08-25 5:52 AM**	**RSA Log Device**	**Log device content for event source Linux - r...**

5. View the configuration of the Log Decoder to insure that the rhlinux and Windows Events (Snare) parser's have been installed and are enabled.



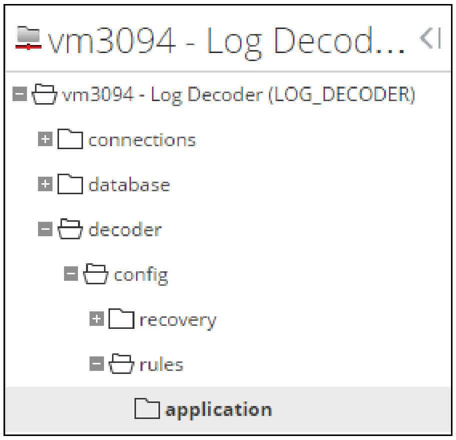
Name	Config Value
rhlinux	☑
winevent_snare	☑

6. Select **Explore** from the Config tab**.**

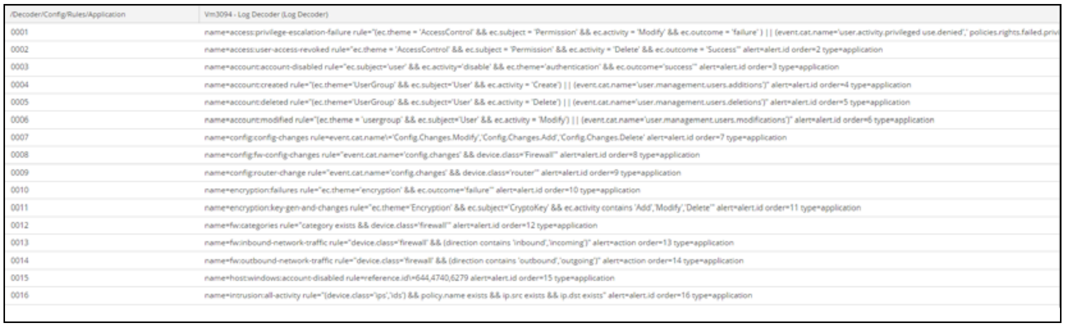


Name	Config Value
Compression	0

7. Browse the tree and locate **decoder>config>rules>application**.

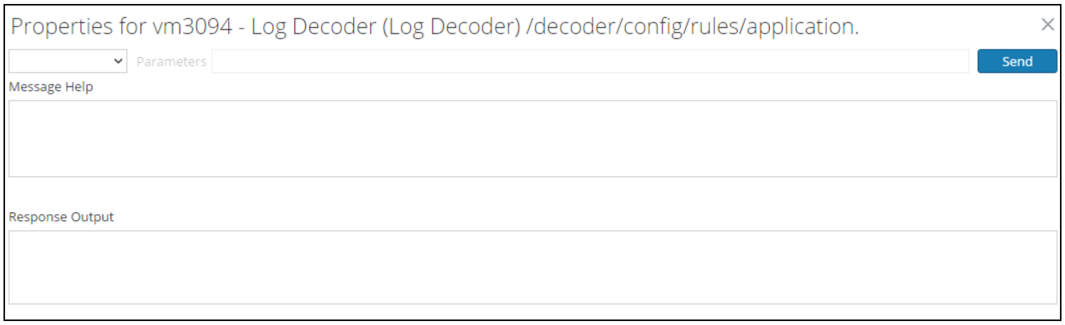


8. The Decoder Application Rules are displayed within the right window frame.

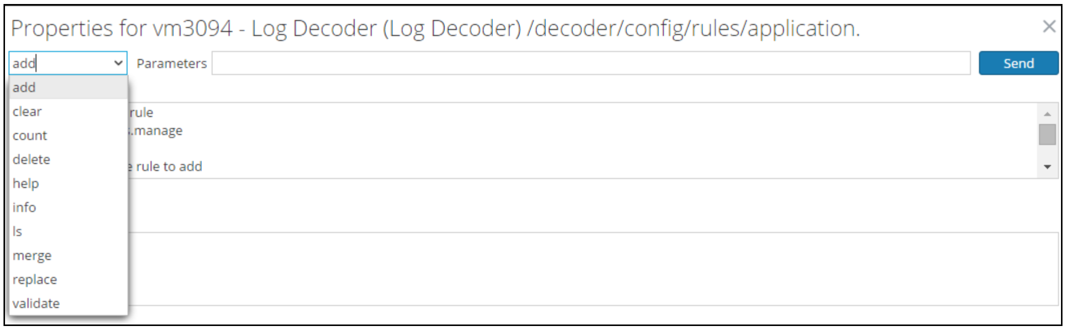


/Decoder/Config/Rules/Application	Vm3094 - Log Decoder (Log Decoder)
0001	name=access:privilege-escalation-failure rule="(ec.theme = 'AccessControl' && ec.subject = 'Permission' && ec.activity = 'Modify' && ec.outcome = 'failure') || (event.cat.name='user.activity.privileged use.denied',' policies.rights.failed.privi
0002	name=access:user-access-revoked rule="ec.theme = 'AccessControl' && ec.subject = 'Permission' && ec.activity = 'Delete' && ec.outcome = 'Success'" alert=alert.id order=2 type=application
0003	name=account:account-disabled rule="ec.subject='user' && ec.activity='disable' && ec.theme='authentication' && ec.outcome='success'" alert=alert.id order=3 type=application
0004	name=account:created rule="(ec.theme='UserGroup' && ec.subject='User' && ec.activity = 'Create') || (event.cat.name='user.management.users.additions')" alert=alert.id order=4 type=application
0005	name=account:deleted rule="(ec.theme='UserGroup' && ec.subject='User' && ec.activity = 'Delete') || (event.cat.name='user.management.users.deletions')" alert=alert.id order=5 type=application
0006	name=account:modified rule="(ec.theme = 'usergroup' && ec.subject='User' && ec.activity = 'Modify') || (event.cat.name='user.management.users.modifications')" alert=alert.id order=6 type=application
0007	name=config:config-changes rule=event.cat.name!='Config.Changes.Modify','Config.Changes.Add','Config.Changes.Delete' alert=alert.id order=7 type=application
0008	name=config:fw-config-changes rule="event.cat.name='config.changes' && device.class='Firewall'" alert=alert.id order=8 type=application
0009	name=config:router-change rule="event.cat.name='config.changes' && device.class='router'" alert=alert.id order=9 type=application
0010	name=encryption:failures rule="ec.theme='encryption' && ec.outcome='failure'" alert=alert.id order=10 type=application
0011	name=encryption:key-gen-and-changes rule="ec.theme='Encryption' && ec.subject='CryptoKey' && ec.activity contains 'Add','Modify','Delete'" alert=alert.id order=11 type=application
0012	name=fw:categories rule="category exists && device.class='firewall'" alert=alert.id order=12 type=application
0013	name=fw:inbound-network-traffic rule="device.class='firewall' && (direction contains 'inbound','incoming')" alert=action order=13 type=application
0014	name=fw:outbound-network-traffic rule="device.class='firewall' && (direction contains 'outbound','outgoing')" alert=action order=14 type=application
0015	name=host:windows:account-disabled rule=reference.id!=644,4740,6279 alert=alert.id order=15 type=application
0016	name=intrusion:all-activity rule="(device.class='ips','ids') && policy.name exists && ip.src exists && ip.dst exists" alert=alert.id order=16 type=application

9. Right click the word application listed in the left hand window frame to display the Properties for **** - Log Decoder window frame.


Properties for vm3094 - Log Decoder (Log Decoder) /decoder/config/rules/application.

10. From the drop-down menu select **add**.



11. Paste into the Parameters field the following;

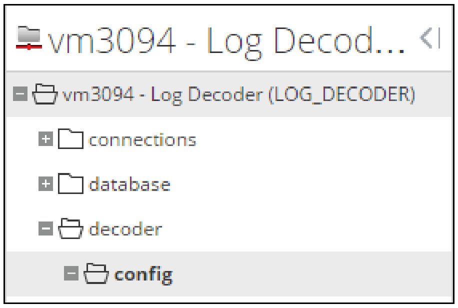
Rule Example:
name=Forward:CyberArk:Logons rule="(device.type='rhlinux' && (event.desc contains 'ession opened')) || (device.type='winevent_snare' && event.cat.name='User.Activity.Successful Logins') " type=application forward alert

Note: Reference RSA SA Configure Application Rules for more information on how the rule was created.

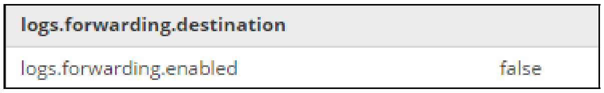
The name defined "Forward:CyberArk:Logons" will be referenced in the next section.

Enable Forwarding to CyberArk PTA

1. Click the word **config** to display the Log Decoder properties.

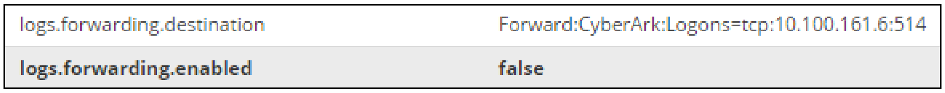


2. Click **logs.forwarding.destination** and set the value to true to enable event forwarding.


logs.forwarding.destination
logs.forwarding.enabled false

Note: Reference RSA SA Configure Syslog Forwarding to Destination for more information.

3. Scroll down to logs.forwarding.enabled and click the field to set the forward address destination. Set the value to true to enable forwarding.



logs.forwarding.destination	Forward:CyberArk:Logons=tcp:10.100.161.6:514
logs.forwarding.enabled	**false**

4. All properties are immediately set and as a result no restart of the Log Decoder is required.

Certification Checklist for RSA Security Analytics

Date Tested: January 11, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.4	Virtual Appliance
Privileged Threat Analytics	2.6.3.1	CentOS 6.4Virtual Appliance

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

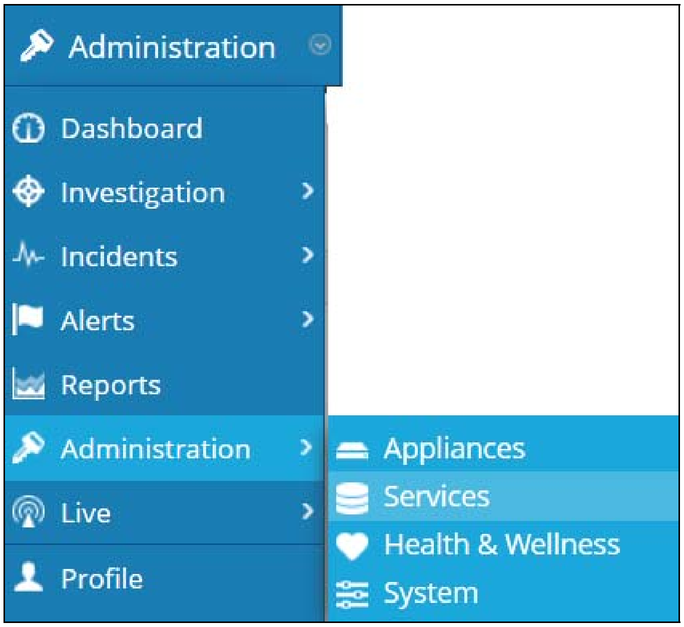
✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

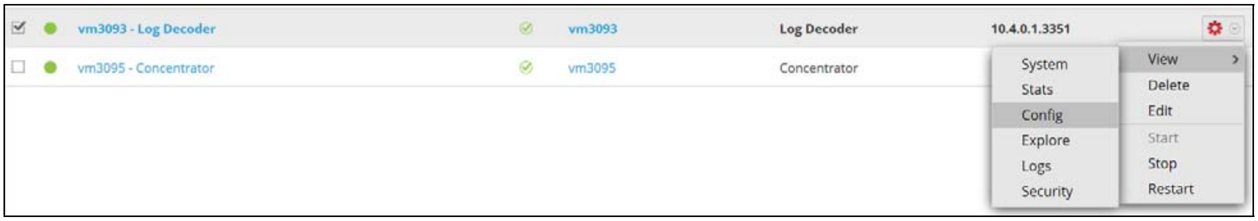
Security Analytics Disable the Common Event Format Parser

To disable the Security Analytics Common Event Format Parser without deleting it perform the following:

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

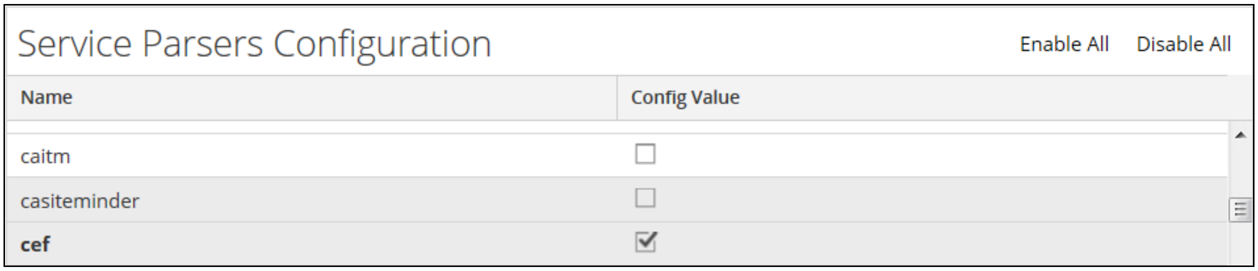


2. Select the Log Decoder, then select **View > Config.**



☑	●	vm3093 - Log Decoder	✓	vm3093	Log Decoder	10.4.0.1.3351
☐	●	vm3095 - Concentrator	✓	vm3095	Concentrator	

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



Service Parsers Configuration

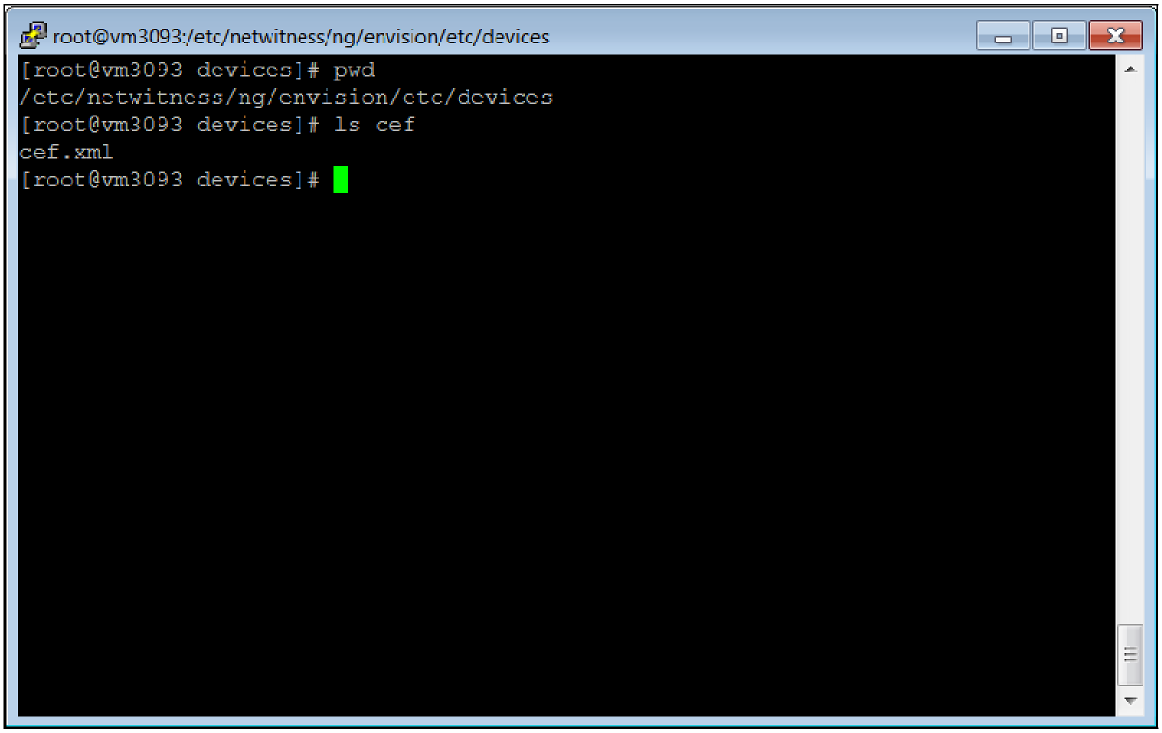
Name	Config Value
caitm	☐
casiteminder	☐
cef	☑

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.



```
[root@vm3093 devices]# pwd
/etc/netwitness/ng/envision/etc/devices
[root@vm3093 devices]# ls cef
cef.xml
[root@vm3093 devices]# 
```

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