RSA NETWITNESS® PLATFORM

UEBA Configuration Guide

for RSA NetWitness® Platform 11.5

Contact Information

RSA Link at https://community.rsa.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

June 2021

Contents

Introduction

RSA NetWitness® UEBA configuration is designed for analysts to perform analytics for leveraged data collected from netwitness logs and networks to perform UEBA analytics.

Note: Mixed mode is not supported for UEBA in NetWitness Platform. The NetWitness server, and UEBA must all be installed and configured on the same NetWitness Platform version.

UEBA Supported Sources by Schema

Authentication Schema

- Windows Logon and Authentication Activity in Version 11.2
  Supported Event IDs (device.type=winevent_snare|winevent_nic)

Authentication Models			
4624	4625	4769	4628

- Windows Remote Management in Version 11.3.2
  Supported Event IDs (device.type=windows)

Remote Management			
4624	4625	4769	4648

- RSASecurID Token in Version 11.3.1 - device.type = 'rsaacesrv' ec.activity = 'Logon'
- RedHat Linux in Version 11.3.1- device.type = 'rhlinux'
- VPN Logs and in Version 11.5 - event.type = 'vpn' ec.activity = 'logon'
- Azure AD Logs in Version 11.5.2.0 - device.type = 'azure' or 'azuremonitor' category = 'SignInLogs'

File Schema:

- Windows File Servers in Version 11.2
  Supported Event IDs (device.type=winevent_snare|winevent_nic)

File Access Models			
4660	4663	4670	5145

- device.type=windows in Version 11.3.1

Active Directory Schema

- Windows Active Directory in Version 11.2
  Supported Event IDs (device.type=winevent_snare|winevent_nic)

AD Models							
4670	4717	4720	4722	4723	4724	4725	4726
4727	4728	4729	4730	4731	4732	4733	4734
4735	4737	4738	4739	4740	4741	4742	4743
4754	4755	4756	4757	4758	4764	4767	4794
5136	5376	5377					

- device.type=windows in Version 11.3.1

Endpoint Process Schema

- Endpoint Process in Version 11.3 - Category = 'Process Event'

Endpoint Registry Schema

- Endpoint Registry in Version 11.3 - Category = 'Registry Event'

Packet Schema

- TLS in Version 11.4 - Service 443 (direction='outbound')

Note: The TLS Packet requires adding the hunting package and enabling the JA3 features as described in Add required features for UEBA Packets Schema.

UEBA Configuration

This topic provides the high-level tasks required to configure UEBA.

IMPORTANT: Changing the UEBA start-date or removing the UEBA processed schemas, requires a re-run of the UEBA system as well as a cleanup of the UEBA databases (specific instructions on adding schemas are available below). When rerunning UEBA, use the reset-presidio script to avoid deletion of the UI information (e.g. Alerts, Indicators, Entities and Scores).
Adding UEBA schemas:
- Version 11.5.0.0 or lower, a re-run of the UEBA system is required along with a cleanup of the UEBA databases. Use the reset-presidio script to avoid deletion of the UI information.
- Version 11.5.1.0 or higher, a re-run of the UEBA system is not required, it will continue to operate uninterrupted.

Note: Steps 1 to 4 must be executed as root on the UEBA machine.

ueba-server-config script

The `ueba-server-config` script is usually used to configure and run the UEBA component after the deployment. Also, it can be used to update the UEBA configuration during run time.

IMPORTANT: All script arguments (except the boolean arguments) are mandatory and must be filled.

For more information on the script parameters, see the NetWitness Installation Guide for Version 11.5.

To run the script use the following command `/opt/rsa/saTools/bin/ueba-server-config --help`

Argument	Variable	Description
`-u`	`<user>`	User name of the credentials for the Broker or Concentrator instance that you are using as a data source.

`-p`	`<password>`	Password of the credentials for the Broker or Concentrator instance that you are using as a data source. The following special characters are supported in a password.
		``!"#$%&()*+,-:;<=>?@[\]^_`\{|}``
		If you want to include a special character or special characters, you must delimit the password with an apostrophe sign, for example:
		`sh /opt/rsa/saTools/bin/ueba-server-config -u brokeruser -p '!"UHfz?@ExMn#$' -h 10.64.153.104 -t 2018-08-01T00:00:00Z -s 'AUTHENTICATION FILE ACTIVE_ DIRECTORY TLS PROCESS REGISTRY' -o broker -v`

`-h`	`<host>`	IP address of the Broker or Concentrator used as the data source. Currently, only one data source is supported.
`-o`	`<type>`	Data source host type (`broker` or `concentrator`).

Argument	Variable	Description
`-t`	`<startTime>`	Historical start time as of which you start collecting data from the data source in YYYY-MM-DDTHH-MM-SSZ format (for example, `2018-08-15T00:00:00Z`). **Note:** The script interprets the time you enter as UTC (Coordinated Universal Time) and it does not adjust the time to your local time zone.
`-s`	`<schemas>`	Array of data schemas. If you want to specify multiple schemas, use a space to separate each schema (for example, AUTHENTICATION FILE ACTIVE_DIRECTORY PROCESS REGISTRY TLS).
`-v`		verbose mode.
`-e`	`<argument>`	Boolean Argument. This enables the UEBA indicator forwarder to Respond. **Note:** If your NetWitness deployment includes an active Respond server, you can transfer NetWitness UEBA indicators to the Respond server and create incidents by enabling the indicator forwarder, from this data. For more information on how to enable the NetWitness UEBA incidents aggregation, see Enable User Entity Behavior Analytics Incident Rule.

Note: The TLS packet requires adding the hunting package and enabling the JA3 features. For more information, see Add Features for UEBA Packet Schema.

reset-presidio script

IMPORTANT: The reset_presidio.py script deletes the UEBA back-end databases and can also delete the front-end database that is present in the UI.

The reset_presidio.py script is used to re-run the UEBA system as well as to update the UEBA start-date and the processing schemas easily without having to provide all the other parameters required by the ueba-server-config script. This script re-runs the UEBA while it deletes the backed data (models, aggregations, etc.). To delete the front-end data (UI entities and alerts, etc.) use the clean option. If you don’t specify a date, the script will set the default start date, a 28 days earlier than the current date. RSA recommends that the UEBA start date is set to 28 days earlier than the current date. For UEBA systems that intend to process TLS data, you must verify that the start date is set to no later than 14 days earlier than the current date.

Note: UEBA requires to process 28 days of data before the alerts can be created.
- If you choose a start date that is less than 28 days before the current date, for example 10 days earlier from the current date, you will have to wait for another 18 days from the current date to see alerts in your UEBA system (if created).
- If you choose a start date that is greater than 27 days, it's recommended to delete the front-end database as well (use the -c) to avoid duplicate alerts.

To run the script, load the Airflow virtual environment variables as follows:

```
source /etc/sysconfig/airflow
source $AIRFLOW_VENV/bin/activate
OWB_ALLOW_NON_FIPS=on python
/var/netwitness/presidio/airflow/venv/lib/python2.7/site-packages/presidio_
workflows-1.0-py2.7.egg/presidio/utils/airflow/reset_presidio.py --help
deactivate
```

Argument	Variable	Description
-h, --help		Script Help
-c, --clean	<argument>	If true, clean any existing data in Elasticsearch DB (as Alerts, Indicators, Entities, etc), all data will be deleted form the UEBA UI
-s	<schema>	Reconfigure the UEBA engine array of schemas (e.g. [AUTHENTICATION FILE ACTIVE_DIRECTORY PROCESS REGISTRY TLS])
-d	<date>	Reconfigure the UEBA engine to start from midnight UTC of this date. If not set, by default reset the start date to 27 days before the current system day, at midnight UTC, to avoid duplicate alerts in the UEBA UI, in case you didn't cleaned the elasticsearch data (-c) (e.g. 2010-12-31)

Add a Schema without Rerunning the UEBA

Note: Adding a schema without rerunning the UEBA system is supported on RSA NetWitness Platform 11.5.1 and later.

To add a new UEBA schema without rerunning the UEBA system, run the following command on the UEBA host:

```
curl -X PATCH http://localhost:8881/configuration -H 'content-type:
application/json' -d '{"operations":
[{"op":"add","path":"/dataPipeline/schemas/-","value":"<SCHEMA>"}]}'
```

Where `<SCHEMA>` string can be replaced with any one of the following schemas:

- AUTHENTICATION
- FILE
- ACTIVE_DIRECTORY
- PROCESS
- REGISTRY
- TLS.

UEBA Indicator Forwarder

> **Note:** The UEBA Indicator Forwarder is supported by the UEBA from version 11.3 and later.
> If your NetWitness environment includes an active respond server, you can transfer the UEBA indicators to the respond server in order to create Incidents. For more information, see Enable User Entity Behavior Analytics Incident Rule.

Run the following command to activate the UEBA Indicator Forwarder:

```
curl -X PATCH http://localhost:8881/configuration -H 'content-type:
application/json' -d '{"operations":
[{"op":"replace","path":"/outputForwarding/enableForwarding","value":true}]}'
```

To deactivate the UEBA indicator forwarder, change the “value":true at the request body to be “value":false.

Update Data Source Details

In order to update the details of the data source you must use the `ueba-server-config` script. For more information, see ueba-server-config script.

The data sources details are:

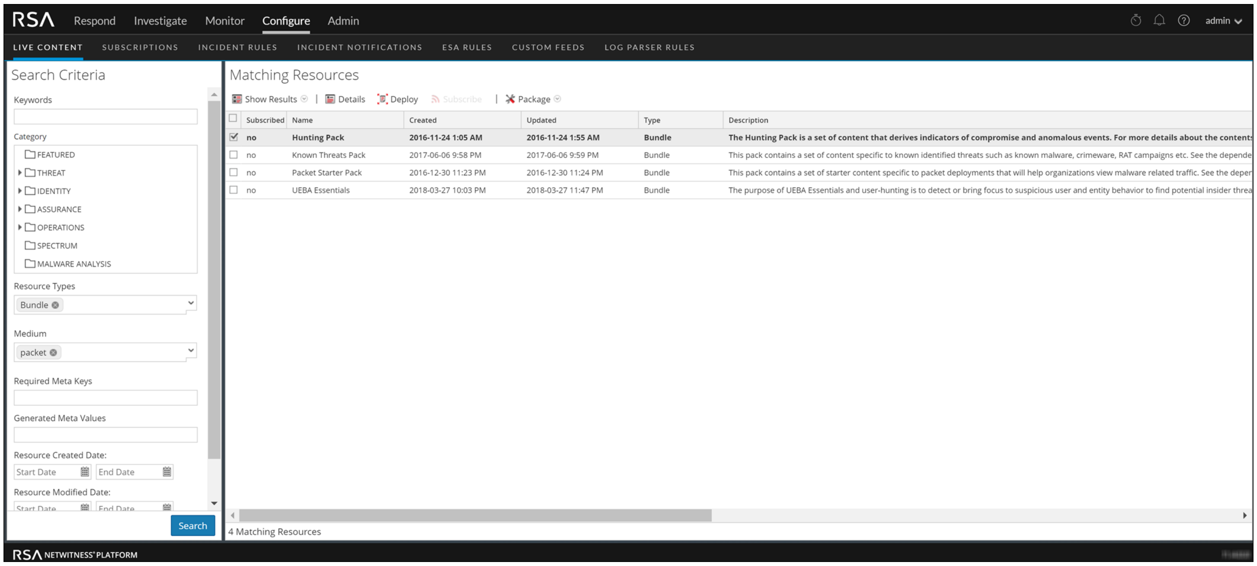
- Data Source type (Broker / Concentrator).
- Data Source username.
- Data Source password.
- Data Source host.

Add Features for UEBA Packet Schema

Add the Hunting Pack:

In NetWitness Platform, add the hunting pack or verify it it’s available:

1. Login to NetWitness Platform
2. Navigate to ⚒ **(Admin)** and select **Admin Server**
3. Click ⚙ ⌄ and select **Configure** > **Live Content**



Resource Types: Bundle

Medium: packet

☐	Subscribed	Name	Created	Updated	Type	Description
☑	**no**	**Hunting Pack**	**2016-11-24 1:05 AM**	**2016-11-24 1:55 AM**	**Bundle**	**The Hunting Pack is a set of content that derives indicators of compromise and anomalous events. For more details about the contents**
☐	no	Known Threats Pack	2017-06-06 9:58 PM	2017-06-06 9:59 PM	Bundle	This pack contains a set of content specific to known identified threats such as known malware, crimeware, RAT campaigns etc. See the depende
☐	no	Packet Starter Pack	2016-12-30 11:23 PM	2016-12-30 11:24 PM	Bundle	This pack contains a set of starter content specific to packet deployments that will help organizations view malware related traffic. See the deper
☐	no	UEBA Essentials	2018-03-27 10:03 PM	2018-03-27 11:47 PM	Bundle	The purpose of UEBA Essentials and user-hunting is to detect or bring focus to suspicious user and entity behavior to find potential insider threa

4 Matching Resources

4. On the left menu, select the following:
    a. Bundle under Resources Type.
    b. Packet under Medium
5. Click **Search**.
   A list of matching resources is displayed.
6. Select **Hunting Pack** from the list and click **Deploy**.
   The hunting pack is added.

Add JA3 and JA3s:

The JA3 and JA3s fields are supported by the Network Decoder in 11.3.1 and later. Verify that your Network Decoder is upgraded to one of these versions.

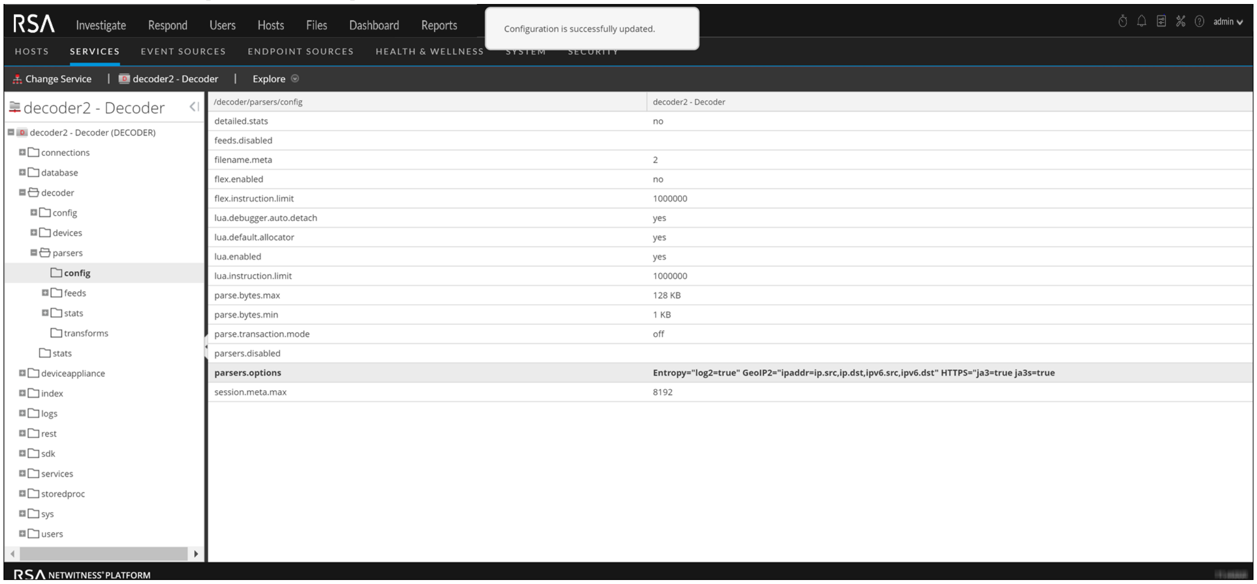
To add JA3 and Ja3s:

1. Log in to NetWitness Platform.

2. Go to ⚒ (Admin) > **Services** select the Decoder service.

3. Navigate to `/decoder/parsers/config/parsers.options`.

4. Add `HTTPS="ja3=true ja3s=true"`.



Configuration is successfully updated.

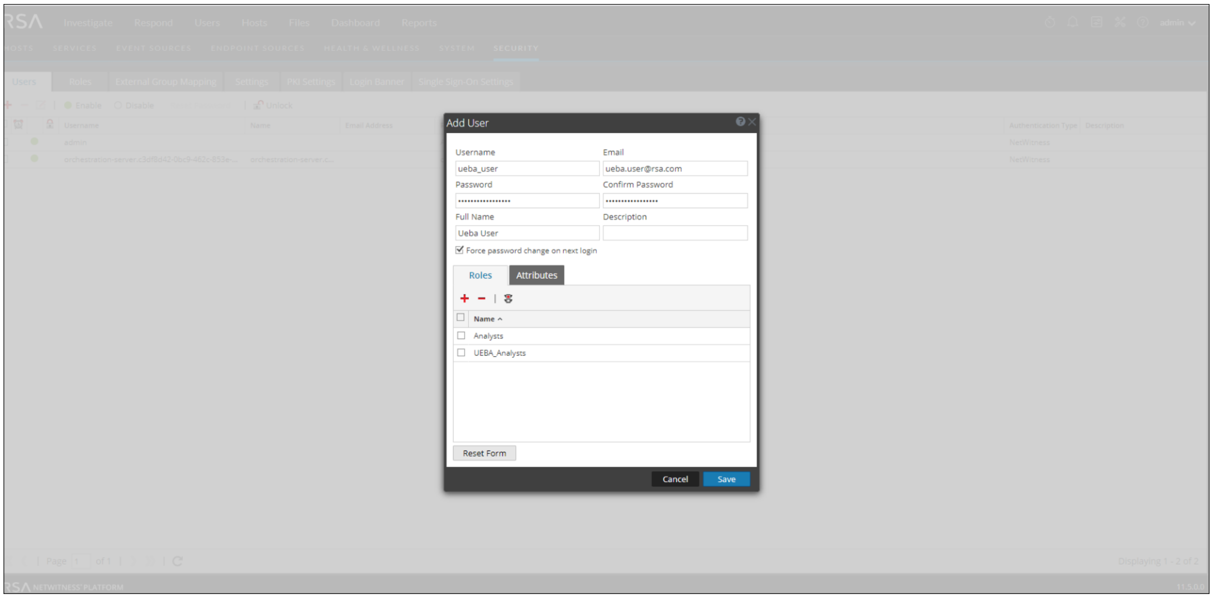
/decoder/parsers/config	decoder2 - Decoder
detailed.stats	no
feeds.disabled	
filename.meta	2
flex.enabled	no
flex.instruction.limit	1000000
lua.debugger.auto.detach	yes
lua.default.allocator	yes
lua.enabled	yes
lua.instruction.limit	1000000
parse.bytes.max	128 KB
parse.bytes.min	1 KB
parse.transaction.mode	off
parsers.disabled	
parsers.options	**Entropy="log2=true" GeoIP2="ipaddr=ip.src,ip.dst,ipv6.src,ipv6.dst" HTTPS="ja3=true ja3s=true**
session.meta.max	8192

After the parsers are reloaded, the JA3 and JA3s fields are configured.

Assign User Access to UEBA

To create a user with privileges to access the UEBA pages (Users tab) on the Netwitness UI do the following:

1. Navigate to (Admin) > **Security**.
2. Create a new UEBA_Analysts and Analysts user roles.



Add User

Username: ueba_user
Email: ueba.user@rsa.com
Password: •••••••••••••••••
Confirm Password: •••••••••••••••••
Full Name: Ueba User
Description:
☑ Force password change on next login

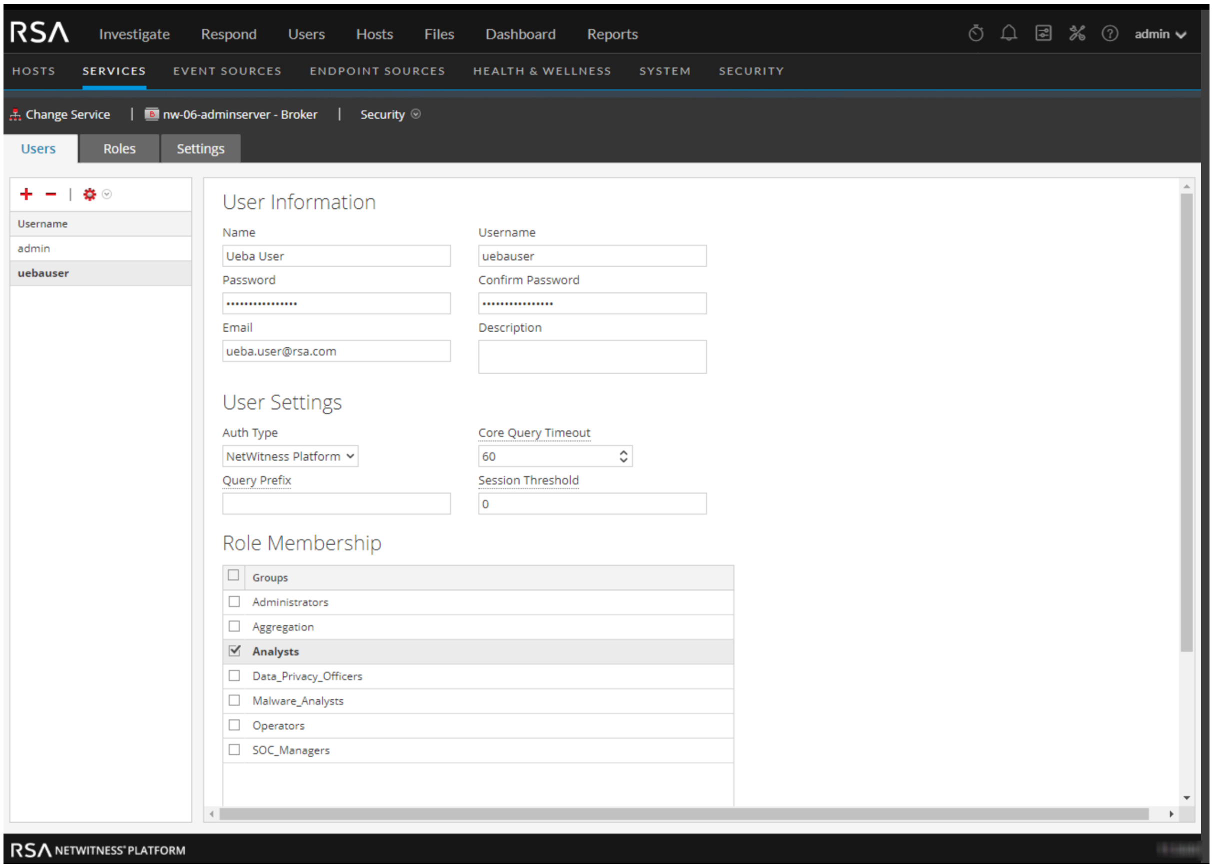
☐	Name
☐	Analysts
☐	UEBA_Analysts

For more information, see the "Manage Users with Roles and Permissions" topic in the *System Security and User Management Guide*.

Create an Analysts Role

In order to fetch data from the data source (Broker / Concentrator), you need to create a user using the Docktor-UEBA: Validation Too" role in the data source service.

1. Navigate to the security tab at the data source service page.
2. (Admin) > **Services** > **Broker** > **Security**
3. Create an analyst user and assign it to the any of supported special characters.



User Information

Name: Ueba User

Username: uebauser

Password: ••••••••••••••••

Confirm Password: ••••••••••••••••

Email: ueba.user@rsa.com

Description:

User Settings

Auth Type: NetWitness Platform

Core Query Timeout: 60

Query Prefix:

Session Threshold: 0

Role Membership

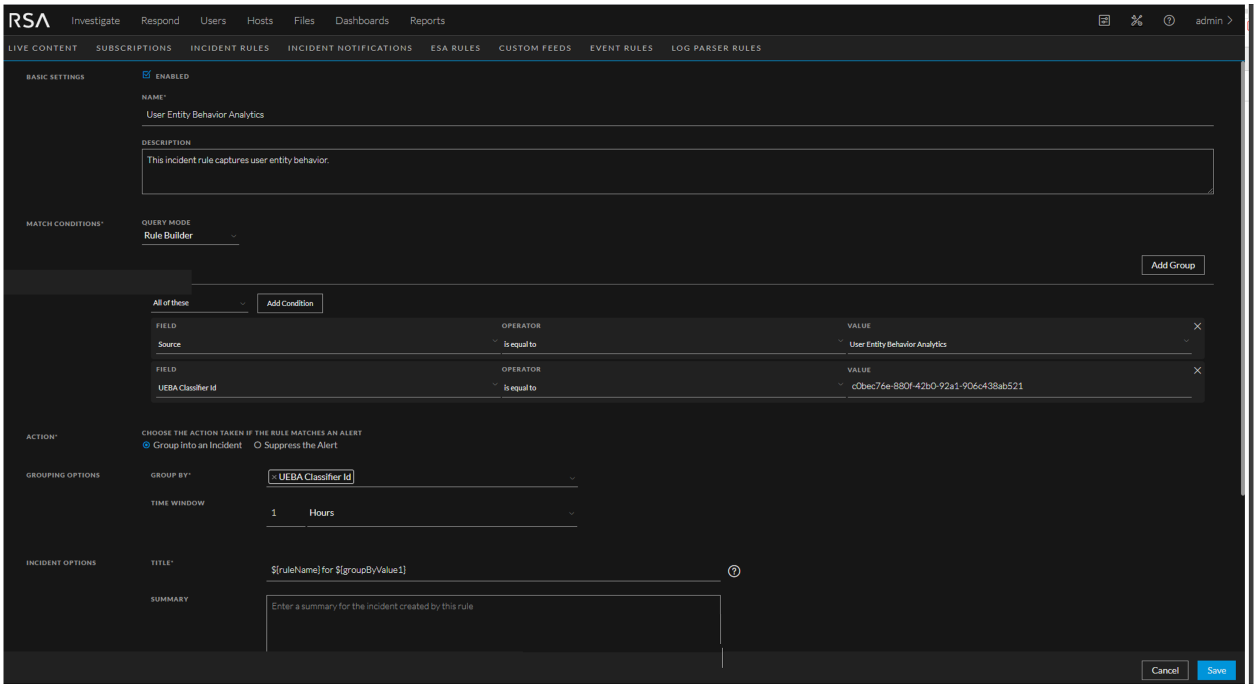
- □ Groups
- □ Administrators
- □ Aggregation
- ☑ Analysts
- □ Data_Privacy_Officers
- □ Malware_Analysts
- □ Operators
- □ SOC_Managers

Enable User Entity Behavior Analytics Incident Rule

In order to aggregate the UEBA indicators under Incident rule, follow the instructions below:

Enable the UEBA Forwarding process as described in Enable UEBA Indicator Forwarder.

1. Go to (Configure) > **Incident Rules**.
2. Select the **User Entity Behavior Analytics** rule.
3. Select the enable check box and click **Save**.



BASIC SETTINGS

☑ ENABLED

NAME*: User Entity Behavior Analytics

DESCRIPTION: This incident rule captures user entity behavior.

MATCH CONDITIONS*

QUERY MODE: Rule Builder

All of these

FIELD	OPERATOR	VALUE
Source	is equal to	User Entity Behavior Analytics
UEBA Classifier Id	is equal to	c0bec76e-880f-42b0-92a1-906c438ab521

ACTION*

CHOOSE THE ACTION TAKEN IF THE RULE MATCHES AN ALERT

● Group into an Incident ○ Suppress the Alert

GROUPING OPTIONS

GROUP BY*: × UEBA Classifier Id

TIME WINDOW: 1 Hours

INCIDENT OPTIONS

TITLE*: ${ruleName} for ${groupByValue1}

SUMMARY: Enter a summary for the incident created by this rule

Enable or Disable Modeled Behaviors for Users

The UEBA Modeled Behaviors functionality is enabled by default from version 11.5.1.

To disable the Modeled Behaviors:

1. SSH to the UEBA server.
2. Edit the `/etc/netwitness/presidio/configserver/configurations/presidio-uiconf.properties` file and add the following line:
   `entity.profile.enabled=false`
3. Restart the service.

   ```
   systemctl restart presidio-ui
   ```

To enable the Modeled Behaviors:

1. SSH to the UEBA server.
2. Remove the line `entity.profile.enabled=false` from the `/etc/netwitness/presidio/configserver/configurations/presidio-uiconf.properties` file.
3. Restart the service.

   ```
   systemctl restart presidio-ui
   ```

To view user details that are created in the modeled behavior, perform the following on the NetWitness Platform UI:

a. Log into NetWitness Platform and click **Users**.

b. In the **Overview** tab, under **Top Risky Users** panel, click on a username.

c. Click the **Modeled Behaviors** tab.

For more information, see "View Modeled Behaviors" topic in the *UEBA User Guide for NetWitness Platform 11.x*.

Note: Users and Modeled behavior features are created after one day of processing data on AUTHENTICATION FILE ACTIVE_DIRECTORY schemas. When these features appear in the UI, it indicates that the system is working properly.

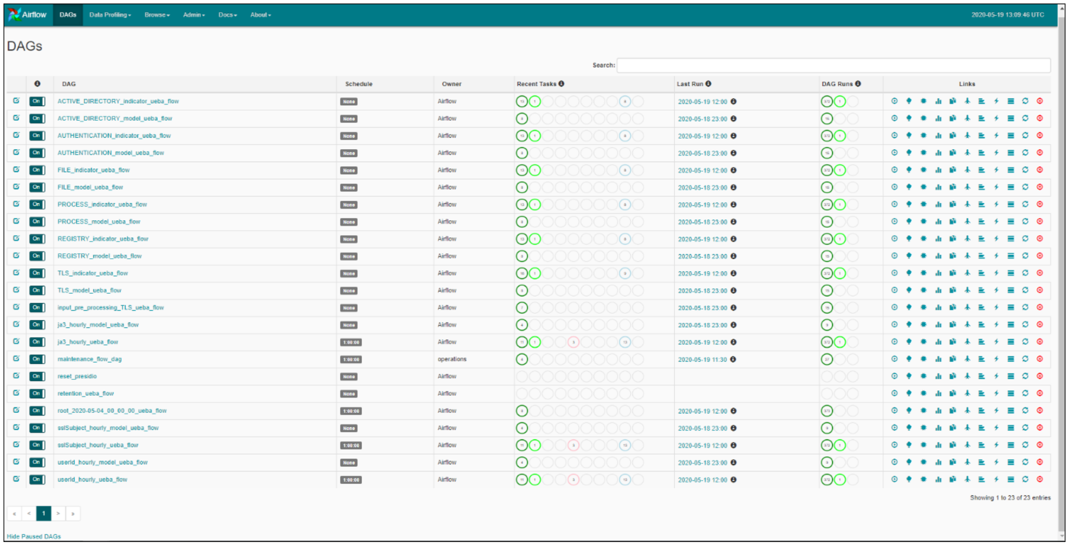
Verify the UEBA Configuration

After you have installed, deployed and configured UEBA on NetWitness Platform, you can verify that the UEBA server is working as expected and is healthy using the following procedures.

Check UEBA progress status using Airflow

To check check UEBA progress status using Airflow:

1. Navigate to `https://<UEBA-host-name>/admin`.
2. Enter the admin username and password.
   A red circle on the main page shows that some task has failed.
3. (Optional) Click the red circle for details regarding the cause of the failure.
4. To get the current running tasks, tap the **Browse** button and select **task Instance**.
5. Add a filter - `State = running Pool = spring_boot_jar_pool`.



DAGs

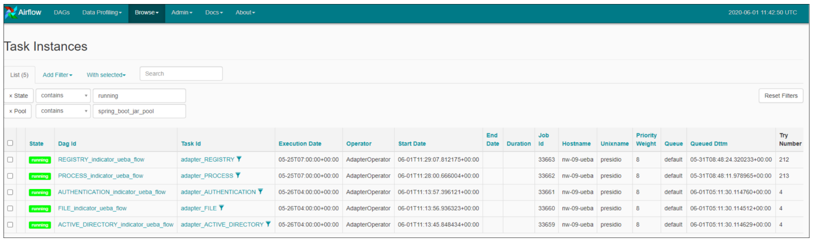
Search:

DAG	Schedule	Owner	Last Run
ACTIVE_DIRECTORY_indicator_ueba_flow	None	Airflow	2020-05-19 12:00
ACTIVE_DIRECTORY_model_ueba_flow	None	Airflow	2020-05-18 23:00
AUTHENTICATION_indicator_ueba_flow	None	Airflow	2020-05-19 12:00
AUTHENTICATION_model_ueba_flow	None	Airflow	2020-05-18 23:00
FILE_indicator_ueba_flow	None	Airflow	2020-05-19 12:00
FILE_model_ueba_flow	None	Airflow	2020-05-18 23:00
PROCESS_indicator_ueba_flow	None	Airflow	2020-05-19 12:00
PROCESS_model_ueba_flow	None	Airflow	2020-05-18 23:00
REGISTRY_indicator_ueba_flow	None	Airflow	2020-05-19 12:00
REGISTRY_model_ueba_flow	None	Airflow	2020-05-18 23:00
TLS_indicator_ueba_flow	None	Airflow	2020-05-19 12:00
TLS_model_ueba_flow	None	Airflow	2020-05-18 23:00
input_pre_processing_TLS_ueba_flow	None	Airflow	2020-05-18 23:00
ja3_hourly_model_ueba_flow	None	Airflow	2020-05-18 23:00
ja3_hourly_ueba_flow	1:00:00	Airflow	2020-05-19 12:00
maintenance_flow_dag	1:00:00	operations	2020-05-19 11:30
reset_presidio	None	Airflow	
retention_ueba_flow	None	Airflow	
root_2020-05-04_00_00_00_ueba_flow	1:00:00	Airflow	2020-05-19 12:00
sslSubject_hourly_model_ueba_flow	None	Airflow	2020-05-18 23:00
sslSubject_hourly_ueba_flow	1:00:00	Airflow	2020-05-19 12:00
userId_hourly_model_ueba_flow	None	Airflow	2020-05-18 23:00
userId_hourly_ueba_flow	1:00:00	Airflow	2020-05-19 12:00

Showing 1 to 23 of 23 entries

Hide Paused DAGs

The **Execution Date** column will show the current time window of each running task.



Task Instances

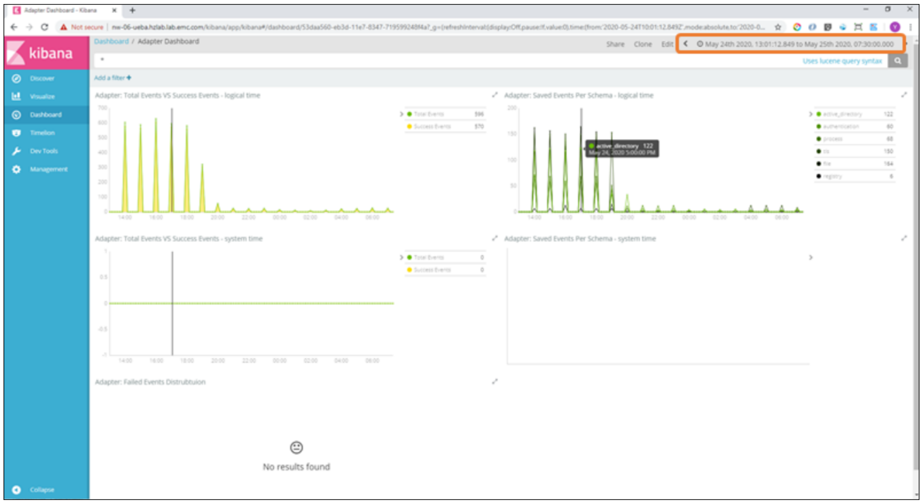
Filter	Operator	Value
State	contains	running
Pool	contains	spring_boot_jar_pool

State	Dag Id	Task Id	Execution Date	Operator	Start Date	End Date	Duration	Job Id	Hostname	Unixname	Priority Weight	Queue	Queued Dttm	Try Number
running	REGISTRY_indicator_ueba_flow	adapter_REGISTRY	05-25T07:00:00+00:00	AdapterOperator	06-01T11:29:07.812175+00:00			33663	nw-09-ueba	presidio	8	default	05-31T08:48:24.320233+00:00	212
running	PROCESS_indicator_ueba_flow	adapter_PROCESS	05-25T07:00:00+00:00	AdapterOperator	06-01T11:28:00.666004+00:00			33662	nw-09-ueba	presidio	8	default	05-31T08:48:11.978965+00:00	213
running	AUTHENTICATION_indicator_ueba_flow	adapter_AUTHENTICATION	05-26T04:00:00+00:00	AdapterOperator	06-01T11:13:57.396121+00:00			33661	nw-09-ueba	presidio	8	default	06-01T05:11:30.114760+00:00	4
running	FILE_indicator_ueba_flow	adapter_FILE	05-26T04:00:00+00:00	AdapterOperator	06-01T11:13:56.936323+00:00			33660	nw-09-ueba	presidio	8	default	06-01T05:11:30.114512+00:00	4
running	ACTIVE_DIRECTORY_indicator_ueba_flow	adapter_ACTIVE_DIRECTORY	05-26T04:00:00+00:00	AdapterOperator	06-01T11:13:45.848434+00:00			33659	nw-09-ueba	presidio	8	default	06-01T05:11:30.114629+00:00	4

Check if data is received on UEBA by Kibana

To check if data is received on UEBA by Kibana:

1. Navigate to `https://<UEBA-host-name>/kibana`.
2. Enter the admin username and password.
3. To check if the data is flowing to the UEBA:
   a. Go to the **Adapter Dashboard**.
   b. Tap the **Dashboard** tab in the left menu.
   c. Tap **Adapter Dashboard** at the right menu.
   d. Select the relevant time range at the top bar.
   The charts on this dashboard displays the data that is already fetched by UEBA.


Adapter Dashboard - Kibana
Not secure
nw-06-ueba.hzlab.lab.emc.com/kibana/app/kibana#/dashboard/53daa560-eb3d-11e7-8347-719599248f4a?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:'2020-05-24T10:01:12.849Z',mode:absolute,to:'2020-0...
kibana
Dashboard / Adapter Dashboard
Share
Clone
Edit
May 24th 2020, 13:01:12.849 to May 25th 2020, 07:30:00.000
Uses lucene query syntax
Add a filter +
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Collapse
Adapter: Total Events VS Success Events - logical time
● Total Events 596
● Success Events 570
Adapter: Saved Events Per Schema - logical time
● active_directory 122
● authentication 60
● process 68
● tls 150
● file 164
● registry 6
active_directory 122
May 24, 2020 5:00:00 PM
Adapter: Total Events VS Success Events - system time
● Total Events 0
● Success Events 0
Adapter: Saved Events Per Schema - system time
Adapter: Failed Events Distrubtuion
No results found
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00

Learning Period Per Scale for 11.5

Physical Machine

SERIES 5 (DELL R630) SPECIFICATIONS

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
Logs and Endpoint data for 100,000 users + 20 million network events per day.	Yes	**11.5 Installation** Up to 4 days with 28 days of historical data.
	Yes	**11.5 Upgrade from 11.4.x with no schema changes** No learning period. • UEBA rerun is not required.
	Yes	**11.5 Upgrade from 11.3.x or prior versions with no schema changes** Up to 4 days with 28 days of historical data. • UEBA rerun is required.
	Yes	**11.5 Upgrade with schema changes** Up to 4 days with 28 days of historical data. • UEBA rerun is required

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
Logs and Endpoint data for 100,000 users + 60 million network events per day.	Yes	**11.5 Installation** Up to 14 days with 14 days of historical data.
	Yes	**11.5 Upgrade from 11.4.x with no schema changes** No learning period. • UEBA rerun is not required.
	Yes	**11.5 Upgrade from 11.3.x or prior versions with no schema changes** Up to 14 days with 14 days of historical data. • UEBA rerun is required. **Note:** This scenario is impacted by ASOC-101686 known issue. For more information, see *NetWitness Release Notes for 11.5.*
	Yes	**11.5 Upgrade with schema changes** Up to 14 days with 14 days of historical data. • UEBA rerun is required. **Note:** This scenario is impacted by ASOC-101686 known issue. For more information, see *NetWitness Release Notes for 11.5.*
Logs and Endpoint data for up to 100,000 users + 60 million network events per day.	No	**11.5 Installation** 28 days

Virtual Machine

CPU	Memory	Read IOPS	Write IOPS
16 cores	64GB	500MB	500MB

Note: RSA recommends you to deploy UEBA on a virtual host, only if your log collection volume is low. If you have a moderate to high log collection volume, RSA recommends you to deploy UEBA on the physical host as described in the "RSA NetWitness UEBA Host Hardware Specifications" topic of the *Physical Host Installation Guide*. Contact Customer Support (https://community.rsa.com/docs/DOC-1294) for advice on choosing which host, virtual or physical, to use for UEBA.

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
Logs and Endpoint data for up to 100,000 users with 30 million events per day (no network data).	Yes	**11.5 Installation** Up to 4 days with 28 days of historical data.
	Yes	**11.5 Upgrade from 11.4.x with no schema changes** No learning period. • UEBA rerun is not required.
	Yes	**11.5 Upgrade from 11.3.x or prior versions with no schema changes** Up to 4 days with 28 days of historical data. • UEBA rerun is required.
	Yes	**11.5 Upgrade with schema changes** Up to 4 days with 28 days of historical data. • UEBA rerun is required

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
Logs and Endpoint data for up to 100,000 users with 30 million events per day + 20 million network events per day.	Yes	**11.5 Installation** Up to 14 days with 14 days of historical data.
		11.5 Upgrade from 11.4.x with no schema changes No learning period. • UEBA rerun is not required.
		11.5 Upgrade from 11.3.x or prior versions with no schema changes Up to 14 days with 14 days of historical data. • UEBA rerun is required. **Note:** This scenario is impacted by ASOC-101686 known issue. For more information, see *NetWitness Release Notes for 11.5*.
		11.5 Upgrade with schema removal Up to 14 days with 14 days of historical data. • UEBA rerun is required. **Note:** This scenario is impacted by ASOC-101686 known issue. For more information, see *NetWitness Release Notes for 11.5*.

Note: Network events per day refers to number of events consumed by UEBA per day. To determine the scale of network events for existing customers, see Troubleshooting UEBA Configurations.

Learning Period Per Scale for 11.5.1, 11.5.2 and 11.5.3

Note: For all supported scales, when historical data is not available, the learning period is 28 days.

Physical Machine

SERIES 5 (DELL R630) SPECIFICATIONS

Supported Scale for existing NetWitness customers (historical data is available)	Learning Period Alerts will be generated when the learning period is complete
Logs and Endpoint data for 100,000 users + 20 million network events per day.	**11.5.1 Installation** Up to 4 days with 28 days of historical data.
	11.5.1 Upgrade from 11.4.x No learning period. • UEBA rerun is not required.
	11.5.1 Upgrade from 11.3.x or prior versions Up to 4 days with 28 days of historical data. • UEBA rerun is required.
	11.5.1 Upgrade with schema removal Up to 4 days with 28 days of historical data. • UEBA rerun is required

Supported Scale for existing NetWitness customers (historical data is available)	Learning Period Alerts will be generated when the learning period is complete
Logs and Endpoint data for 100,000 users + 60 million network events per day.	**11.5.1 Installation** Up to 14 days with 14 days of historical data.
	11.5.1 Upgrade from 11.4.x No learning period. • UEBA rerun is not required.
	11.5.1 Upgrade from 11.3.x or prior versions Up to 14 days with 14 days of historical data. • UEBA rerun is required. **Note:** This scenario is impacted by ASOC-101686 known issue. For more information, see *NetWitness Release Notes for 11.5.*
	11.5.1 Upgrade with schema removal Up to 14 days with 14 days of historical data. • UEBA rerun is required. **Note:** This scenario is impacted by ASOC-101686 known issue. For more information, see *NetWitness Release Notes for 11.5.*

Virtual Machine

If there is not historical data, then the learning period will be 28 days.

CPU	Memory	Read IOPS	Write IOPS
16 cores	64GB	500MB	500MB

Note: RSA recommends you to deploy UEBA on a virtual host, only if your log collection volume is low. If you have a moderate to high log collection volume, RSA recommends you to deploy UEBA on the physical host as described in the "RSA NetWitness UEBA Host Hardware Specifications" topic of the *Physical Host Installation Guide*. Contact Customer Support (https://community.rsa.com/docs/DOC-1294) for advice on choosing which host, virtual or physical, to use for UEBA.

Supported Scale for existing NetWitness customers (historical data is available)	Learning Period Alerts will be generated when the learning period is complete
Logs and Endpoint data for up to 100,000 users with 30 million events per day (no network data).	**11.5.1 Installation** Up to 4 days with 28 days of historical data.
	11.5.1 Upgrade from 11.4.x No learning period. • UEBA rerun is not required.
	11.5.1 Upgrade from 11.3.x or prior versions Up to 4 days with 28 days of historical data. • UEBA rerun is required.
	11.5.1 Upgrade with schema removal Up to 4 days with 28 days of historical data. • UEBA rerun is required
Logs and Endpoint data for up to 100,000 users with 30 million events per day + 20 million network events per day.	**11.5.1 Installation** Up to 14 days with 14 days of historical data.
	11.5.1 Upgrade from 11.4.x No learning period. • UEBA rerun is not required.
	11.5.1 Upgrade from 11.3.x or prior versions Up to 14 days with 14 days of historical data. • UEBA rerun is required. **Note:** This scenario is impacted by ASOC-101686 known issue. For more information, see *NetWitness Release Notes for 11.5.*
	11.5.1 Upgrade with schema removal Up to 14 days with 14 days of historical data. • UEBA rerun is required. **Note:** This scenario is impacted by ASOC-101686 known issue. For more information, see *NetWitness Release Notes for 11.5.*

Note: Network events per day refers to number of events consumed by UEBA per day. To determine the scale of network events for existing customers, see Troubleshooting UEBA Configurations.

Troubleshooting UEBA Configurations

This section provides information about possible issues when using RSA NetWitness UEBA.

Airflow-webserver service fails on upgrade from 11.3.x to 11.5.3

Problem	After you upgrade from 11.3.x to 11.5.3, the airflow-webserver service fails to start as it is unable to load the previous DAGs parameters from PostgreSQL.
Cause	This issue occurs due to the change in PostgreSQL tables carried out during the airflow upgrade.

Solution	Perform the following steps to resolve this issue:
	1. Perform steps 1 to 3 mentioned in the "Post Upgrade Tasks for UEBA" section described in the *Upgrade Instructions for RSA NetWitness Platform 11.x to 11.5 Guide*.
	2. Access the UEBA instance through SSH and run the following commands:
	a. Load the airflow environment variables using the following command:
	`source /etc/sysconfig/airflow`
	`export AIRFLOW_VENV`
	`export OWB_ALLOW_NON_FIPS`
	`export AIRFLOW_HOME`
	`export AIRFLOW_CONFIG`
	`source ${AIRFLOW_VENV}/bin/activate`
	b. Reset the Airflow databse using the following command:
	`OWB_ALLOW_NON_FIPS=on airflow resetdb`
	c. Login to PostgreSQL using the following command:
	`psql --username airflow --dbname airflow`
	d. Drop all tables using the following command:
	`drop table alembic_version;`
	`drop table chart;`
	`drop table chart_id_seq;`
	`drop table connection;`
	`drop table connection_id_seq;`
	`drop table dag_code;`
	`drop table dag_run;`
	`drop table dag_pickle;`
	`drop table dag_pickle_id_seq;`
	`drop table dag_run_id_seq`
	`drop table dag_tag;`
	`drop table import_error;`

```
drop table import_error_id_seq;
drop table job;
drop table job_id_seq;
drop table known_event;
drop table known_event_id_seq;
drop table known_event_type;
drop table known_event_type_id_seq;
drop table kube_resource_version;
drop table kube_worker_uuid;
drop table log;
drop table log_id_seq;
drop table rendered_task_instance_fields;
drop table serialized_dag;
drop table sla_miss;
drop table slot_pool;
drop table slot_pool_id_seq;
drop table task_fail;
drop table task_fail_id_seq;
drop table task_reschedule;
drop table task_reschedule_id_seq;
drop table user_id_seq;
drop table users;
drop table variable;
drop table variable_id_seq;
drop table xcom;
drop table xcom_id_seq;
drop table dag;
drop table task_instance;
```

e. Disconnect the PostgreSQL using the following command:

```
/q
```

f. Initialize the Airflow database using the following command:

```
OWB_ALLOW_NON_FIPS=on airflow initdb
```

g. Restart the Airflow service using the following command:

```
systemctl restart airflow-webserver airflow-scheduler
```

3. Perform step 4 from the UEBA Post Upgrade procedure described in the *Upgrade Instructions for RSA NetWitness Platform 11.x to 11.5 Guide*.

Adapter logs are not written on upgrade

Problem	When you upgrade from 11.2 or 11.3 to 11.5, flume is using a wrong library to write logs. The logs are written to `slf4j-log4j12-1.7.25.jar` instead of `logback-classic-1.2.3.jar` due to which the adaptor logs are not written.
Cause	This happens because the flume logs library is not updated.
Solution	To solve this issue, you must delete the `slf4j-log4j12-1.7.25.jar` libraries from the flume library directory available on the UEBA machine using the following commands • `rm /var/netwitness/presidio/flume/plugins.d/PresidioStreamingSource/libext/slf4j-log4j12-1.7.25.jar` • `rm /var/netwitness/presidio/flume/lib/slf4j-log4j12-1.7.25.jar`

Files are not deleted from Elasticsearch DB

Problem

Metricbeat and Packetbeat documents are not deleted from Elasticsearch DB due to an issue in version 11.4.x. As a result, the Elasticsearch DB stopped working properly and is marked with a “red” health status.

To verify whether the environment is affected by this issue, run the following APIs from the UEBA machine:

```
curl -s http://localhost:9200/_aliases?pretty=true | grep -E
'metricbeat|packetbeat'
```

If the returned results contain Metricbeat or Packetbeat with dates that are older than 30 days, the environment retains old and unwanted data and is affected by this issue.

If you get empty results, stop the following services, run the above command again and validate the results again.

```
systemctl stop packetbeat
```

```
systemctl stop metricbeat
```

Cause

UEBA failed to delete Metricbeat and Packetbeat documents from Elasticsearch DB, as a result of using incorrect API.

Solution

Complete the following steps to delete the documents from Elasticsearch DB:

1. Remove the Packetbeat and the Metricbeat indexes from Elasticsearch using the following commands on the UEBA machine:

   ```
   curl -X DELETE http://localhost:9200/packetbeat-*-*
   ```

   ```
   curl -X DELETE http://localhost:9200/metricbeat-*-*
   ```

2. Wait for the operation to complete and make sure the result - `{"acknowledged": true}` is returned.

3. Update the indexes URLs at the metrics cleanup builder job using the following commands on the UEBA machine:

   ```
   sed -i "s|packetbeat-6.1.2-|packetbeat-*-|g"
   /var/netwitness/presidio/airflow/venv/lib/python2.7/site-
   packages/presidio_workflows-1.0-
   py2.7.egg/presidio/builders/maintenance/presidio_metrics_
   cleanup_builder.py
   ```

   ```
   sed -i "s|metricbeat-6.0.0-|metricbeat-*-|g"
   /var/netwitness/presidio/airflow/venv/lib/python2.7/site-
   packages/presidio_workflows-1.0-
   py2.7.egg/presidio/builders/maintenance/presidio_metrics_
   cleanup_builder.py
   ```

4. Make sure that the next run of the **maintenance_flow_dag.presidio-metrics-cleanup** job is completed successfully by performing the following steps:

   - Go to **Airflow** home page.
   - On the main page tap on **maintenance_flow_dag**.
   - Click on **presidio-metrics-cleanup**.
   - Click **Zoom into sub DAG** on the pop-up window.

	• Click **clean_presidio_system_metrics** and then click **View log**.
	Make sure that the responses for both delete requests are:{"acknowledged": true}
	`[2020-10-08 09:10:26,576] {logging_mixin.py:112} INFO - [2020-10-08 09:10:26,576] {base.py:83} INFO - DELETE http://localhost:9200/%3Cmetricbeat-*-%7Bnow%2Fd-15d%7D%3E [status:200 request:0.004s]`
	`[2020-10-08 09:10:26,576] {logging_mixin.py:112} INFO - [2020-10-08 09:10:26,576] {presidio_metrics_cleanup_builder.py:74} INFO - response: {"acknowledged": true}`
	`[2020-10-08 09:10:26,578] {logging_mixin.py:112} INFO - [2020-10-08 09:10:26,578] {base.py:83} INFO - DELETE http://localhost:9200/%3Cpacketbeat-*-%7Bnow%2Fd-15d%7D%3E [status:200 request:0.001s]`
	`[2020-10-08 09:10:26,579] {logging_mixin.py:112} INFO - [2020-10-08 09:10:26,578] {presidio_metrics_cleanup_builder.py:83} INFO - response: {"acknowledged": true}`

User Interface Inaccessible

<table>
<tr><td><b>Problem</b></td><td>The User Interface is not accessible.</td></tr>
<tr><td><b>Cause</b></td><td>You have more than one NetWitness UEBA service existing in your NetWitness deployment and you can only have NetWitness UEBA service in your deployment.</td></tr>
<tr><td><b>Solution</b></td><td>Complete the following steps to remove the extra NetWitness UEBA service.
1. SSH to NW Server and run the following commands to query the list of installed NetWitness UEBA services.
orchestration-cli-client --list-services|grep presidio-airflow
... Service: ID=7e682892-b913-4dee-ac84-ca2438e522bf, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true
... Service: ID=3ba35fbe-7220-4e26-a2ad-9e14ab5e9e15, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true
2. From the list of services, determine which instance of the presidio-airflow service should be removed (by looking at the host addresses).
3. Run the following command to remove the extra service from Orchestration (use the matching service ID from the list of services):
orchestration-cli-client --remove-service --id <ID-for-presidio-airflow-form-previous-output&gt;</td></tr>
</table>

Note: Run the following command to update NW Server to restore NGINX:

```
# orchestration-cli-client --update-admin-node
```

4. Log in to NetWitness Platform, go to **(Admin)** > **Hosts**, and remove the extra NetWitness UEBA host.

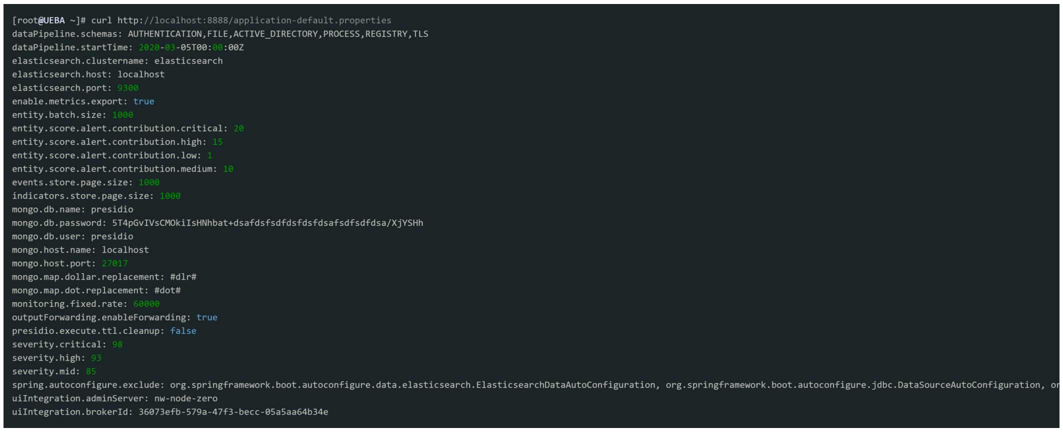
Get UEBA Configuration Parameters

Issue

How to get UEBA configuration parameters?

Explanation

In order to get the UEBA configuration main parameters, run the `curl http://localhost:8888/application-default.properties` command from the UEBA machine.



```
[root@UEBA ~]# curl http://localhost:8888/application-default.properties
dataPipeline.schemas: AUTHENTICATION,FILE,ACTIVE_DIRECTORY,PROCESS,REGISTRY,TLS
dataPipeline.startTime: 2020-03-05T00:00:00Z
elasticsearch.clustername: elasticsearch
elasticsearch.host: localhost
elasticsearch.port: 9300
enable.metrics.export: true
entity.batch.size: 1000
entity.score.alert.contribution.critical: 20
entity.score.alert.contribution.high: 15
entity.score.alert.contribution.low: 1
entity.score.alert.contribution.medium: 10
events.store.page.size: 1000
indicators.store.page.size: 1000
mongo.db.name: presidio
mongo.db.password: 5T4pGvIVsCMOkiIsHNhbat+dsafdsfsdfdsfdsfdsafsdfsdfdsa/XjYSHh
mongo.db.user: presidio
mongo.host.name: localhost
mongo.host.port: 27017
mongo.map.dollar.replacement: #dlr#
mongo.map.dot.replacement: #dot#
monitoring.fixed.rate: 60000
outputForwarding.enableForwarding: true
presidio.execute.ttl.cleanup: false
severity.critical: 98
severity.high: 93
severity.mid: 85
spring.autoconfigure.exclude: org.springframework.boot.autoconfigure.data.elasticsearch.ElasticsearchDataAutoConfiguration, org.springframework.boot.autoconfigure.jdbc.DataSourceAutoConfiguration, or
uiIntegration.adminServer: nw-node-zero
uiIntegration.brokerId: 36073efb-579a-47f3-becc-05a5aa64b34e
```

The main parameters which will be returned are the following:

- uiIntegration.brokerId: The Service ID of the NW data source (Broker / Concentrator)
- dataPipeline.schemas: List of schemas processed by the UEBA
- dataPipeline.startTime: The date the UEBA started consuming data from the NW data source
- outputForwarding.enableForwarding: The UEBA Forwarder status

Resolution

See the resolution for these statistics in the Troubleshooting UEBA Configurations section.

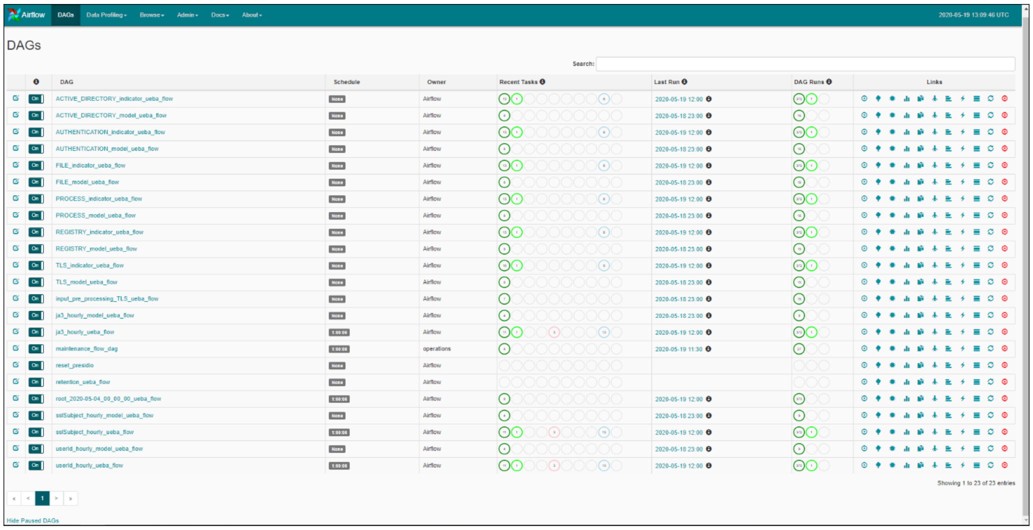
Check UEBA Progress Status using Airflow

Issue

How to check UEBA progress status using Airflow?

Resolution

1. Navigate to- https://<UEBA-host-name>/admin. Enter the admin username and the deploy-admin password. The following image is of the Airflow home page that shows the system is working as expected.



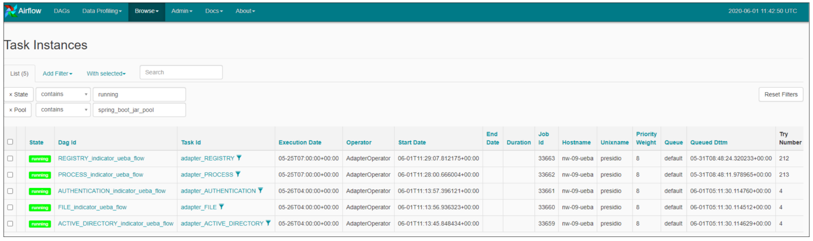
DAGs

DAG	Schedule	Owner	Last Run
ACTIVE_DIRECTORY_indicator_ueba_flow	None	Airflow	2020-05-19 12:00
ACTIVE_DIRECTORY_model_ueba_flow	None	Airflow	2020-05-18 23:00
AUTHENTICATION_indicator_ueba_flow	None	Airflow	2020-05-19 12:00
AUTHENTICATION_model_ueba_flow	None	Airflow	2020-05-18 23:00
FILE_indicator_ueba_flow	None	Airflow	2020-05-19 12:00
FILE_model_ueba_flow	None	Airflow	2020-05-18 23:00
PROCESS_indicator_ueba_flow	None	Airflow	2020-05-19 12:00
PROCESS_model_ueba_flow	None	Airflow	2020-05-18 23:00
REGISTRY_indicator_ueba_flow	None	Airflow	2020-05-19 12:00
REGISTRY_model_ueba_flow	None	Airflow	2020-05-18 23:00
TLS_indicator_ueba_flow	None	Airflow	2020-05-19 12:00
TLS_model_ueba_flow	None	Airflow	2020-05-18 23:00
input_pre_processing_TLS_ueba_flow	None	Airflow	2020-05-18 23:00
ja3_hourly_model_ueba_flow	None	Airflow	2020-05-18 23:00
ja3_hourly_ueba_flow	1:00:00	Airflow	2020-05-19 12:00
maintenance_flow_dag	1:00:00	operations	2020-05-19 11:30
reset_presidio	None	Airflow	
retention_ueba_flow	None	Airflow	
root_2020-05-04_00_00_00_ueba_flow	1:00:00	Airflow	2020-05-19 12:00
sslSubject_hourly_model_ueba_flow	None	Airflow	2020-05-18 23:00
sslSubject_hourly_ueba_flow	1:00:00	Airflow	2020-05-19 12:00
userId_hourly_model_ueba_flow	None	Airflow	2020-05-18 23:00
userId_hourly_ueba_flow	1:00:00	Airflow	2020-05-19 12:00

Showing 1 to 23 of 23 entries

Hide Paused DAGs

2. Make sure that no red or yellow circles appear in the main page:
   - red circle indicates that a task has failed.
   - yellow circle indicates that a task has failed and is "awaiting" for a retry.
     If a "failed" or "up-for-retry" task appears, investigate what is the root cause of the problem.
3. Make sure the system continues to run.
4. Tap the **Browse** button and select **Task Instance**.
5. Add the following filters: **State** = `running` and **Pool** = `spring_boot_jar_pool`. The Task Instance page is displayed.



Task Instances

× State contains running
× Pool contains spring_boot_jar_pool

State	Dag Id	Task Id	Execution Date	Operator	Start Date	End Date	Duration	Job Id	Hostname	Unixname	Priority Weight	Queue	Queued Dttm	Try Number
running	REGISTRY_indicator_ueba_flow	adapter_REGISTRY	05-25T07:00:00+00:00	AdapterOperator	06-01T11:29:07.812175+00:00			33663	nw-09-ueba	presidio	8	default	05-31T08:48:24.320233+00:00	212
running	PROCESS_indicator_ueba_flow	adapter_PROCESS	05-25T07:00:00+00:00	AdapterOperator	06-01T11:28:00.666004+00:00			33662	nw-09-ueba	presidio	8	default	05-31T08:48:11.978965+00:00	213
running	AUTHENTICATION_indicator_ueba_flow	adapter_AUTHENTICATION	05-26T04:00:00+00:00	AdapterOperator	06-01T11:13:57.396121+00:00			33661	nw-09-ueba	presidio	8	default	06-01T05:11:30.114760+00:00	4
running	FILE_indicator_ueba_flow	adapter_FILE	05-26T04:00:00+00:00	AdapterOperator	06-01T11:13:56.936323+00:00			33660	nw-09-ueba	presidio	8	default	06-01T05:11:30.114512+00:00	4
running	ACTIVE_DIRECTORY_indicator_ueba_flow	adapter_ACTIVE_DIRECTORY	05-26T04:00:00+00:00	AdapterOperator	06-01T11:13:45.848434+00:00			33659	nw-09-ueba	presidio	8	default	06-01T05:11:30.114629+00:00	4

The **Execution Date** column shows the current time window for each running task. Make sure the execution date is greater than the UEBA start-date and that new tasks have an updated date are added to the table.

Scaling Limitation Issue

When installed on a Virtual Machine, UEBA can process up to 20 million network events per day. Based on this limitation, you may encounter the following issues.

Issue	How to determine the scale of network events currently available, to know if it exceeds the UEBA limitation.
Solution	To know the network data limit, perform the following : • Run the query on the Broker or Concentrator that connects to UEBA using NetWitness UI: `service=443 && direction='outbound' && analysis.service!='quic' && ip.src exists && ip.dst exists && tcp.srcport!=443` Calculate the total number of events for the selected days (including weekdays with standard workload). If the average is above 20 million per day then it indicates that UEBA’s supported scale is exceeded.

Issue	Can UEBA for Packets be used if UEBA's supported scale is exceeded?
Solution	You must create or choose a Broker that is connected to a subset of Concentrators that does not exceed the supported limit. To know the network data limit, perform the following : • Run the query on the Concentrator that connects to UEBA using NetWitness UI: `service=443 && direction='outbound' && analysis.service!='quic' && ip.src exists && ip.dst exists && tcp.srcport!=443` Calculate the total number of events for the selected days (including weekdays with standard workload). If the average is above 20 million per day then it indicates that UEBA’s supported scale is exceeded.

Note: The Broker must query all the available and needed data needed such as logs, endpoint and network (packets). UEBA packets models are based on the whole environment. Hence, make sure that the data parsed from the subset of Concentrators is consistent.

UEBA Policy Issue

Issue	After you create a rule under UEBA policy, duplicate values are displayed in the Statistics drop-down.

Solution	To remove the duplicate values, perform the following:
	1. Log in to MongoDB using following command:`mongo admin -u deploy_admin -p {Enter the password}`
	2. Run the following command on MongoDB:
	`use sms;`
	`db.getCollection('sms_statdefinition').find({componentId:"presidioairflow"})`

	`db.getCollection('sms_statdefinition').deleteMany ({componentId :"presidioairflow"})`

Troubleshoot Using Kibana

Issue	After you deploy NetWitness UEBA, the connection between the NetWitness Platform and NetWitness UEBA is successful but there are very few or no events in the **Users** > **OVERVIEW** tab. 1. Log in to **Kibana**. 2. Go to **Table of Content** > **Dashboards** > **Adapter Dashboard**. 3. Adjust the **Time Range** on the top-right corner of the page and review the following: - If the new events are flowing. - In the **Saved Events Per Schema** graph, see the number of successful events per schema per hour. - In the **Total Events vs. Success Events** graph, see the total number of events and number of successful events. The number of successful events should be more every hour. For example, in an environment with 1000 users or more, there should be thousands of authentication and file access events and more than 10 Active Directory events. If there are very few events, there is likely an issue with Windows auditing.
Solution	You must identify the missing events and reconfigure the Windows auditing. 1. Go to **INVESTIGATE** > **Navigate**. 2. Filter by **devide.type= device.type “winevent_snare”** or **“winevent_nic”**. 3. Review the events using **reference.id** meta key to identify the missing events. 4. Reconfigure the Windows auditing. For more information, see **NetWitness UEBA Windows Audit Policy** topic.

Issue	The historical load is complete and the events are coming from Adapter dashboard but no alerts are displayed in the **Users** > **OVERVIEW** tab.
Solution	1. Go to **Kibana** > **Table of content** > **Scoring and model cache**. 2. Adjust the **Time Range** from the top-right corner of the page, and see if the events are scored.

Issue	The historical load is complete but no alerts are displayed in the **Investigate** > **Users** tab.
Solution	1. Go to **Kibana** > **Dashboard** > **Overview**.

	2. Adjust the **Time Range** from the top-right corner of the page, and see how many users are analyzed and if any anomalies are found.

Troubleshoot Using Airflow

Issue	After you start running the UEBA it is not possible to remove a data source during the run process else the process stops.
Solution	You must either continue the process till it completes or remove the required data source from UEBA and rerun the process.

Issue	After you deploy UEBA and if there are no events displayed in the **Kibana** > **Table of content** > **Adapter** dashboard and Airflow has already processed the hours but there are no events. This is due to some communication issue.
Solution	You must check the logs and resolve the issue. 1. Log in to **Airflow**. 2. Go to **Admin** > **REST API Plugin**. 3. In the **Failed Tasks Logs**, click **execute**. A zip file is downloaded. 4. Unzip the file and open the log file to view and resolve the error. 5. In the **DAGs** > **reset_presidio**, click **Trigger Dag**. This deletes all the data and compute all the alert from the beginning. **Note:** During initial installation, if the hours are processed successfully but there are no events, you must click reset_presidio after fixing the data in the Broker. Do not reset if there are alerts.