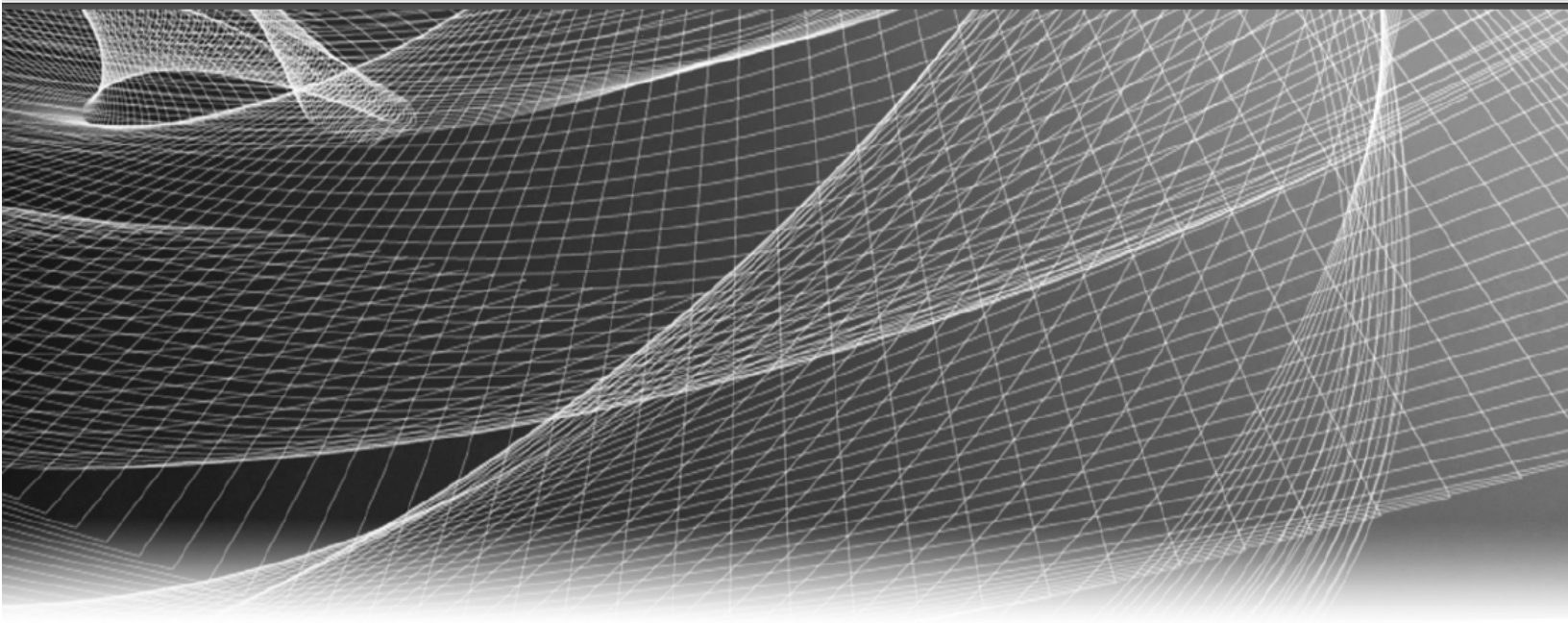


RSA Security Analytics

Investigation Feed

RSA

EMC²

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

Contents

Investigation Feed **4**

Investigation Meta 5

Deployment 5

About the Meta Keys 5

Deploy the Feed 6

Investigation Feed

This document highlights an approach to classifying collections, with a focus on business driven security. NetWitness Suite can be used to catalog application rules and parser values based on a feed that introduces two new keys. These keys will help analysts quickly determine escalation targets and bolster information security posture.

There is no secret path to success as an information security professional. Some analysts prefer to investigate malware, while others may take a network-centric approach to discover compromise. With so many different techniques utilized in data security, it is essential that NetWitness Suite provide the ability to analyze datasets with each of these inspection techniques in mind.

The Investigation feed creates meta keys and values, as detailed in the Investigation Model, on trigger of application rules and Lua parser logic within NetWitness Suite content resources on Live. This meta is used to provide a means to classify all logs and sessions in support of investigations and remediation. This is useful for front line analysts, because it minimizes the time dedicated to mining logs or sessions in support of their findings.

Default escalation targets or organizations can be directly assigned to these four investigation categories. Knowing who an escalation target may be in any given situation can be the difference between a declared incident and an internal investigation.

- *Threat*: Threat monitoring escalations may be assigned to incident response or security teams.
- *Identity*: Identity-based content tagged as such assists with rapid analysis in the NetWitness Suite Investigation module, and is useful for determining who is responsible for a certain request, or what is normal for a certain user. For example, a meta value tagged in the identity category could be directly escalated to the Information technology access management personnel responsible for provisioning access.
- *Assurance*: Similarly, the Assurance category houses all resources that a risk organization would leverage in their calculations towards potential exposure.
- *Operations*: Lastly, the Operations category contains all content that performs session analysis or protocol inspection that is most often utilized in command centers, telecommunications teams and security operations.

Investigation Meta

We have added the following two meta keys for the Investigation profile.

- The *Investigation Category* key (`inv.category`) pinpoints the purpose of a log's or session's escalation. These investigation categories help dictate one's analysis approach. There are four Investigation Categories:
  - Threat
  - Identity
  - Assurance
  - Operations
- The *Investigation Context* key (`inv.context`) expands on the aforementioned category key, but also describes the literal intent or functional objective of the resource itself. This tactic allows content engineers to organize resources based on natural language descriptors.

The model on which these keys are based is described in the Investigation Model.

Deployment

This section discusses:

- How to add the meta keys used by the feed to the Index file, and
- How to deploy the feed.

About the Meta Keys

To get value out of the Investigation feed, two new meta keys are used. The below keys should be added to your **index-concentrator-custom.xml**.

```
<key level="IndexValues" valueMax="10000" name="inv.category" format="Text" description="Investigation Category"/>
<key level="IndexValues" valueMax="10000" name="inv.context" format="Text" description="Investigation Context"/>
```

Note: These keys are now being delivered out of the box in **index-concentrator.xml** with NetWitness Suite version 10.6.2 and newer. If your installed version is prior to 10.6.2, you must add the keys to **index-concentrator-custom.xml**.

To add keys to index-concentrator-custom.xml:

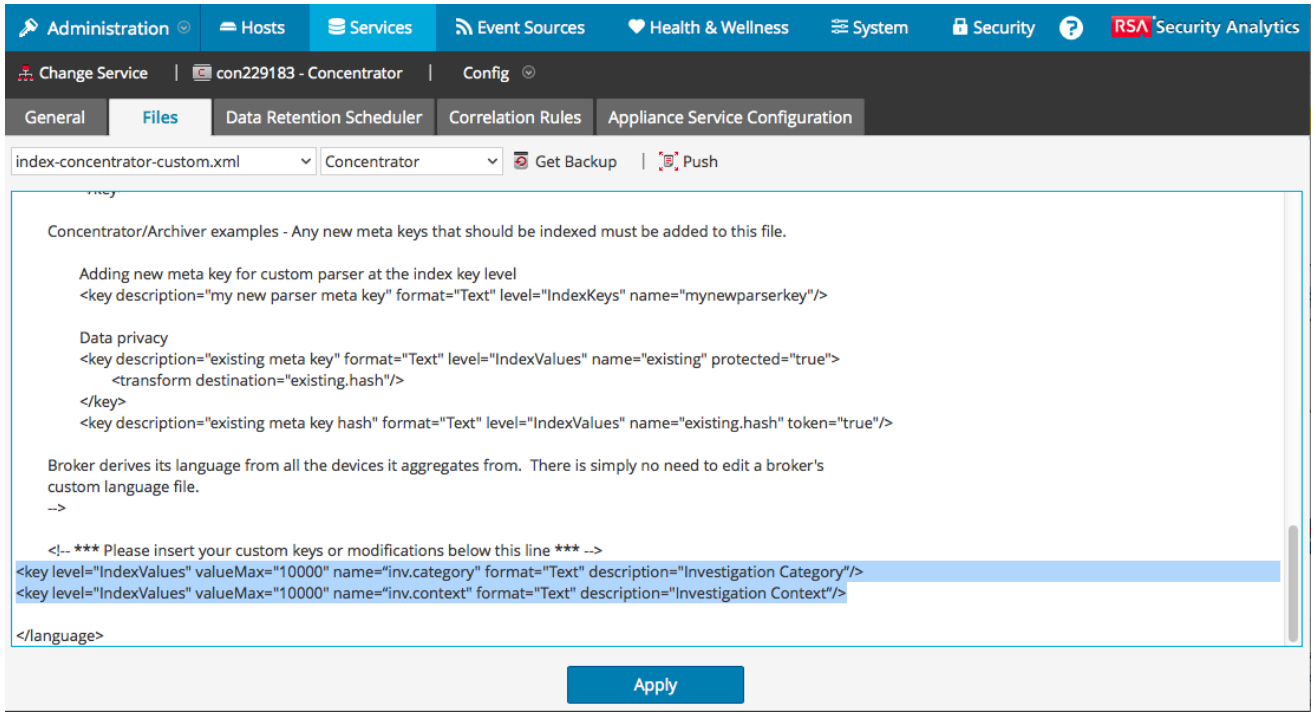
If your installed version of NetWitness Suite is 10.6.2 or newer, you can skip this procedure.

1. In the Security Analytics menu, select **Administration** > **Services**, and select a Concentrator.
2. Select **View** > **Config** from the Actions menu.
3. Select the **Files** tab, then select the **index-concentrator-custom.xml** file.
4. Add the following lines:

```
<key level="IndexValues" valueMax="10000" name="inv.category" format="Text"
description="Investigation Category"/>
<key level="IndexValues" valueMax="10000" name="inv.context" format="Text"
description="Investigation Context"/>
```

5. Click **Apply**.

This screen shows the lines being added to the file in NetWitness Suite:

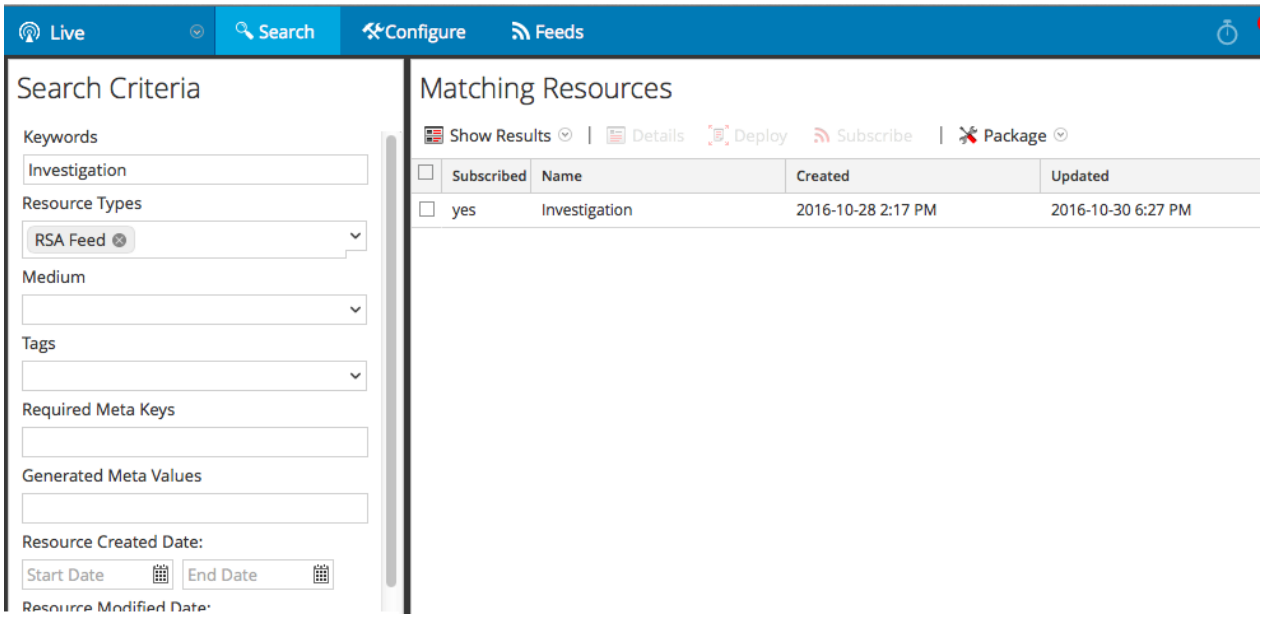


Deploy the Feed

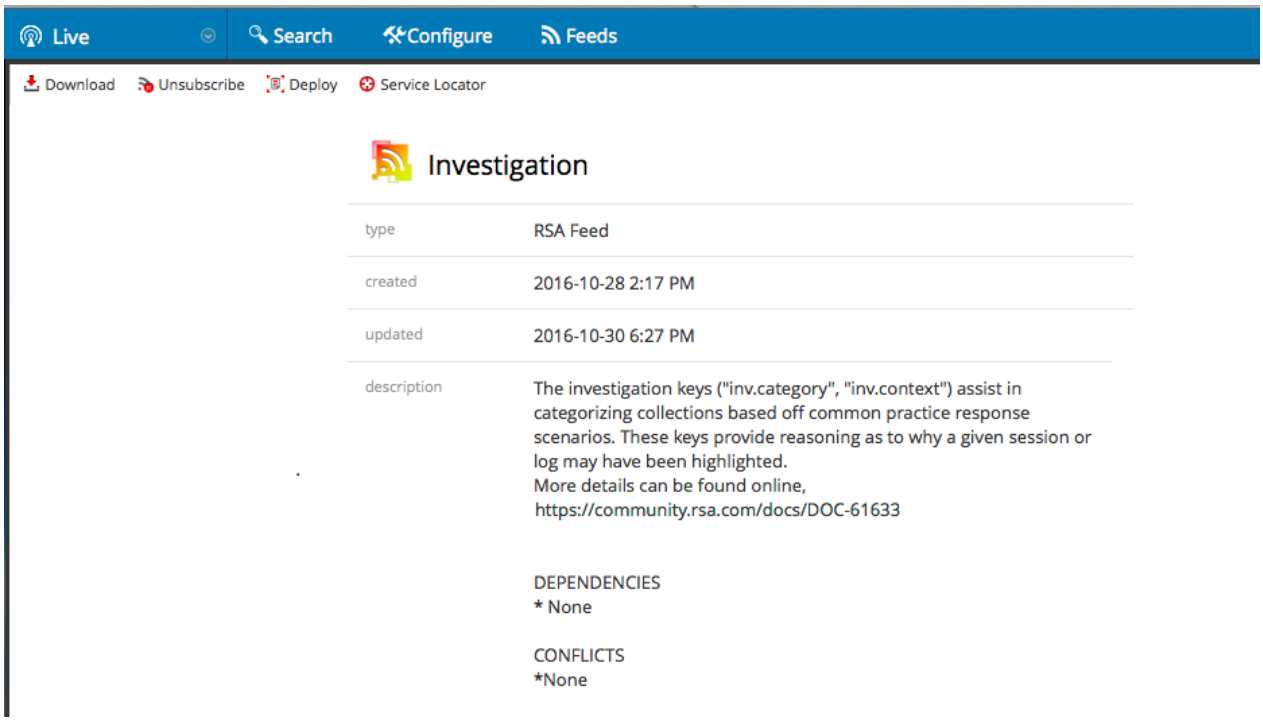
To deploy the Investigation feed:

1. From the NetWitness Suite menu, select **Live > Search**.
2. In the **Search Criteria** section, select **RSA Feed** from the **Resource Types** drop-down menu.
3. In the **Keywords** field, type **Investigation**.
4. Click **Search**.

The **Investigation** feed appears in the Matching Resources section.



And this is a sample screen of the feed's details in Live Search:



5. Select the feed and click **Deploy** from the menu bar.

   The Deployment Wizard dialog box is displayed.

6. Click through the screens of the Wizard.

a. In the **Resources** screen, confirm the correct feed is listed, and click **Next**.

b. In the **Services** screen, select the services to which you want to deploy the content. You can select any combination of services and service groups.

   - Use the **Services** tab to select individual services, list of services, and service groups that are configured in the Administration Services view.
   - Use the **Groups** tab to select groups of services.

c. Click **Next**.

d. On the **Review** page, make sure that you have selected correct resources and the services to which you want to deploy them.

e. Click **Deploy**.

   The Deploy page is displayed. The Progress bar turns green when you have successfully deployed the resources to the selected services.

f. Click **Close**.