RSA NETWITNESS® SUITE

NetWitness Respond Configuration Guide

for Version 11.0

Contact Information

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

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, 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 EMC.

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

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

October 2017

Contents

About this Document

This guide provides an overview of NetWitness Respond, detailed instructions on how to configure NetWitness Respond in your network, additional procedures that are used at other times, and reference materials that describe the user interface for configuring NetWitness Respond in your network.

Topics

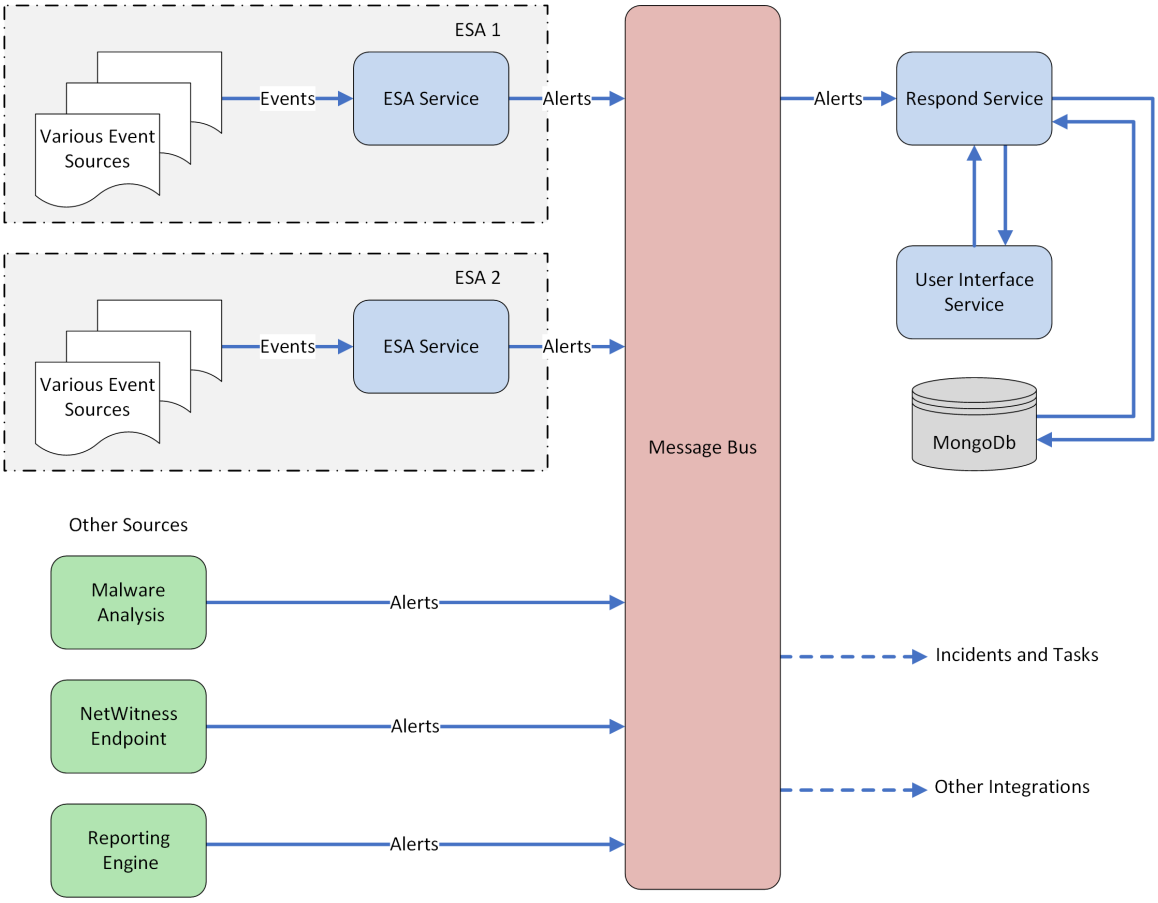
NetWitness Respond Configuration Overview

RSA NetWitness® Suite NetWitness Respond consumes Alert data from various sources via the Message Bus and displays these alerts on the NetWitness Suite user interface. The Respond Server service allows you to group the alerts logically and start a NetWitness Respond workflow to investigate and remediate the security issues raised.

The Respond Server service consumes alerts from the message bus and normalizes the data to a common format (while retaining the original data) to enable simpler rule processing. It periodically runs rules to aggregate multiple alerts into an incident and set some attributes of the Incident (for example, severity, category, and so on). The incidents are persisted into MongoDb by the Respond Server service. Incidents are also posted onto the message bus for consumption by other systems (for example, Archer integration).

Note: NetWitness Respond requires an ESA primary server that contains the MongoDb. Alerts, Incidents, and Task records are persisted into this MongoDb by the Respond Server.

The following diagram illustrates the high level flow of alerts.



You have to configure various sources from which the alerts are collected and aggregated by the Respond Server service.

Configuring NetWitness Respond

This topic provides the high-level tasks required to configure the Respond Server service. The administrator needs to complete the steps in the sequence provided.

Topics

Step 1. Configure Alert Sources to Display Alerts in Respond View

This procedure is required so that alerts from the alert sources are displayed in NetWitness Respond. You have an option to enable or disable the alerts being populated in the Respond view. By default this option is disabled in the Reporting Engine, Malware Analytics, and NetWitness Endpoint and enabled only in Event Stream Analysis. So when you install the Respond Server service you need to enable this option in the Reporting Engine, Malware Analytics, and NetWitness Endpoint to populate the corresponding alerts in the Respond view.

Prerequisites

Ensure that:

- The Respond Server service is installed and running on NetWitness Suite.
- A database is configured for the Respond Server service.
- NetWitness Endpoint is installed and running.

Configure Reporting Engine to Display Alerts Triggered by Reporting Engine in Respond View

The Reporting Engine alerts are by default disabled from being displayed in Respond view. To display and view the Reporting Engine alerts, you have to enable the NetWitness Respond alerts in the Services Config view > General tab for the Reporting Engine.

1. Go to **ADMIN > Services,** select a Reporting Engine service, and select  **> View > Config**.
   The Services Config view is displayed with the Reporting Engine General tab open.
2. Select **System Configuration**.
3. Select the checkbox for **Forward Alerts to Respond**.
   The Reporting Engine now forwards the alerts to NetWitness Respond.

For details on parameters in the General tab, see the "Reporting Engine General Tab" topic in the *Reporting Engine Configuration Guide*.

Configure Malware Analytics to View Alerts Triggered by Malware Analytics in Respond view

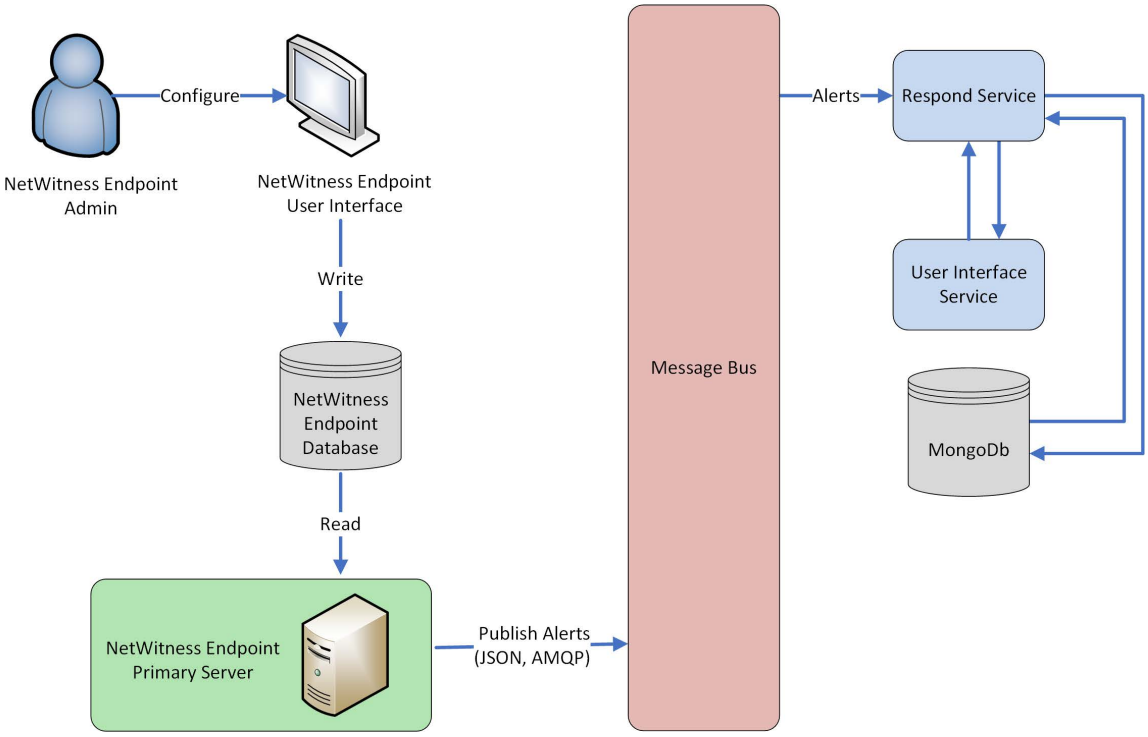
Viewing NetWitness Respond alerts is a function of auditing in Malware Analysis. The procedure of enabling NetWitness Respond alerts is described in the "(Optional) Configure Auditing on Malware Analysis Host" topic in the *Malware Analysis Configuration Guide*.

Configure NetWitness Endpoint to View Alerts Triggered by NetWitness Endpoint in Respond View

This procedure is required to integrate NetWitness Endpoint with NetWitness Suite so that the NetWitness Endpoint alerts are picked up by the NetWitness Respond component of NetWitness Suite and displayed in the **RESPOND > Alerts** view.

Note: RSA supports NetWitness Endpoint versions 4.3.0.4, 4.3.0.5, or later for NetWitness Respond integration. For more detailed information, see the "RSA NetWitness Suite Integration" topic in the *NetWitness Endpoint User Guide*.

The diagram below represents the flow of NetWitness Endpoint alerts to the NetWitness Suite Respond Server service and its display in the **RESPOND > Alerts** view.

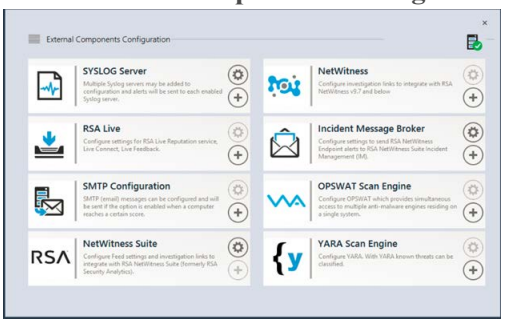


Configure NetWitness Endpoint to Display NetWitness Endpoint Alerts

To configure NetWitness Endpoint to display NetWitness Endpoint alerts in the NetWitness Suite user interface:

1. In the NetWitness Endpoint user interface, click **Configure > Monitoring and External Components**.

The **External Components Configuration** dialog is displayed.



2. From the components listed, select **Incident Message Broker** and click + to add a new IM broker.
3. Enter the following fields:
   a. **Instance Name**: Enter a unique name to identify the IM broker.
   b. **Server Hostname/IP address**: Enter the Host DNS or IP address of the IM broker (NetWitness Server).
   c. **Port number**: The default port is 5671.
4. Click **Save**.
5. Navigate to the **ConsoleServer.exe.Config** file in **C:\Program Files\RSA\ECAT\Server**.
6. Modify the virtual host configurations in the file as follows:
   `<add key="IMVirtualHost" value="/rsa/system" />`

   Note: In NetWitness Suite 11.0, the virtual host is "/rsa/system". For version 10.6.x and below, the virtual host is "/rsa/sa".
7. Restart the API Server and Console Server.
8. To set up SSL for Respond Alerts, perform the following steps on the NetWitness Endpoint primary console server to set the SSL communications:
   a. Export the NetWitness Endpoint CA certificate to .CER format (Base-64 encoded X.509) from the personal certificate store of the local computer (without selecting the private key).
   b. Generate a client certificate for NetWitness Endpoint using the NetWitness Endpoint CA certificate. (You MUST set the CN name to ecat.)

      ```
      makecert -pe -n "CN=ecat" -len 2048 -ss my -sr LocalMachine -a
      sha1 -sky exchange -eku 1.3.6.1.5.5.7.3.2 -in "NWECA" -is MY -ir
      LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -
      cy end -sy 12 client.cer
      ```

> **Note:** In the above code sample, if you upgraded to Endpoint version 4.3 from a previous version and did not generate new certificates, you should substitute "EcatCA" for "NWECA".

c. Make a note of the thumbprint of the client certificate generated in step b. Enter the thumbprint value of the client certificate in the IMBrokerClientCertificateThumbprint section of the ConsoleServer.Exe.Config file as shown.

```
<add key="IMBrokerClientCertificateThumbprint"
value="896df0efacf0c976d955d5300ba0073383c83abc"/>
```

9. On the NetWitness Server, copy the NetWitness Endpoint CA certificate file in .CER format into the import folder:
`/etc/pki/nw/trust/import`

10. Issue the following command to initiate the necessary Chef run:
`orchestration-cli-client --update-admin-node`
This appends all of those certificates into the truststore.

11. Restart the RabbitMQ server:
`systemctl restart rabbitmq-server`
The NetWitness Endpoint account should automatically be available on RabbitMQ.

12. Import the **/etc/pki/nw/ca/nwca-cert.pem** and **/etc/pki/nw/ca/ssca-cert.pem** files from the NetWitness Server and add them to the Trusted Root Certification stores in the Endpoint Server.

Step 2. Assign Respond View Permissions

Add users with the required permissions to investigate incidents and alerts in NetWitness Respond. Users with access to the Respond view need both Incidents and Respond-server permissions.

The following pre-configured roles have permissions in the Respond view:

- **Analysts**: The Security Operations Center (SOC) Analysts have access to Alerting, NetWitness Respond, Investigation, and Reporting, but not system configurations.
- **Malware Analysts**: Malware Analysts have access to investigations and malware events.
- **Operators**: Operators have access to configurations, but not Investigation, ESA, Alerting, Reporting and NetWitness Respond.
- **SOC_Managers**: The SOC Managers have the same access as Analysts plus additional permissions to handle incidents and configure NetWitness Respond.
- **Data_Privacy_Officers**: Data Privacy Officers (DPOs) are like Administrators with additional focus on configuration options that manage obfuscation and viewing of sensitive data within the system. See *Data Privacy Management* for additional information.
- **Respond_Administrator**: The Respond Administrator has full access to NetWitness Respond.
- **Administrators**: the Administrator has full system access to NetWitness Suite and has all permissions by default.

The NetWitness Respond default permissions are shown in the following tables. You need to assign user permissions from both the **Incidents** and **Respond-server** tabs, which are the Permissions tab names in the ADMIN > Security view Add or Edit Roles dialogs.You may want to add additional user permissions for Alerting, Context Hub, Investigate, Investigate-server, and Reports.

Respond-server

Permissions	Analysts	SOC Mgrs	DPOs	Respond Admin	Operators	MAs
respond-server.alert.delete			Yes*	Yes*		
respond-server.alert.manage	Yes	Yes	Yes*	Yes*		Yes
respond-server.alert.read	Yes	Yes	Yes*	Yes*		Yes
respond-server.alertrule.manage		Yes	Yes*	Yes*		
respond-server.alertrule.read		Yes	Yes*	Yes*		
respond-server.configuration.manage			Yes*	Yes*		
respond-server.health.read			Yes*	Yes*		
respond-server.incident.delete			Yes*	Yes*		
respond-server.incident.manage	Yes	Yes	Yes*	Yes*		Yes
respond-server.incident.read	Yes	Yes	Yes*	Yes*		Yes
respond-server.journal.manage	Yes	Yes	Yes*	Yes*		Yes
respond-server.journal.read	Yes	Yes	Yes*	Yes*		Yes
respond-server.logs.manage			Yes*	Yes*		
respond-server.metrics.read			Yes*	Yes*		
respond-server.process.manage			Yes*	Yes*		
respond-server.remediation.manage	Yes	Yes	Yes*	Yes*		Yes

Permissions	Analysts	SOC Mgrs	DPOs	Respond Admin	Operators	MAs
respond-server.remediation.read	Yes	Yes	Yes*	Yes*		Yes
respond-server.security.manage			Yes*	Yes*		
respond-server.security.read			Yes*	Yes*		

* Data Privacy Officers and Respond Administrators have the **respond-server.*** permission, which gives them all of the Respond-server permissions.

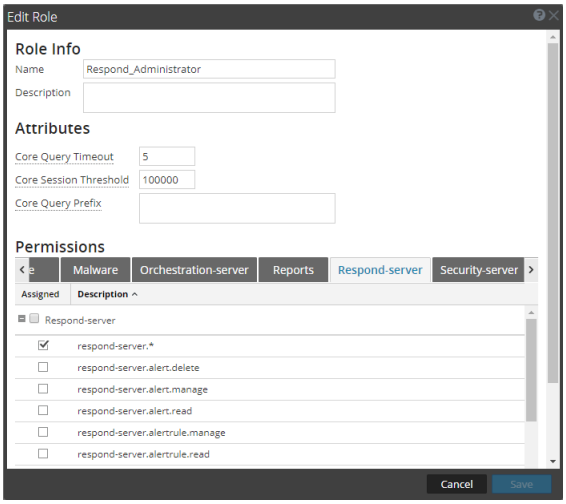
Incidents

Permissions	Analysts	SOC Mgrs	DPOs	Respond Admin	Operators	MAs
Access Incident Module	Yes	Yes	Yes	Yes		Yes
Configure Incident Management Integration		Yes	Yes	Yes		
Delete Alerts and Incidents			Yes	Yes		
Manage Alert Handling Rules		Yes	Yes	Yes		
View and Manage Incidents	Yes	Yes	Yes	Yes		Yes

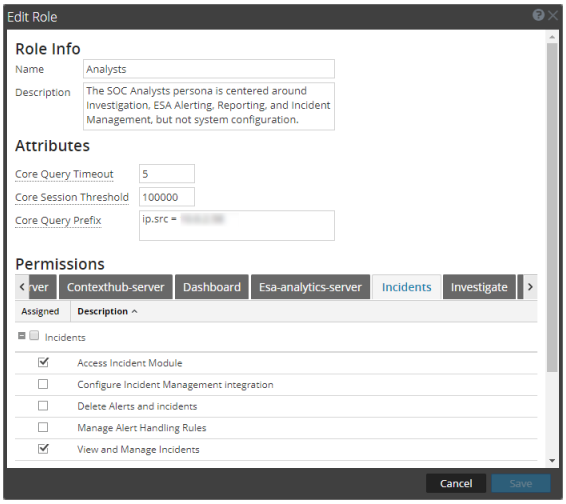
The Respond Administrator has all of the Respond-server and Incidents permissions.

Caution: It is very important that you assign equivalent user permissions from BOTH the Respond-Server tab AND the Incidents tab.

The following figure shows Respond-Server permissions for the default Respond Administrator role. The Respond Administrator role contains all of the NetWitness Respond permissions.



The following figure shows the Incidents permissions for the default Analysts role:



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

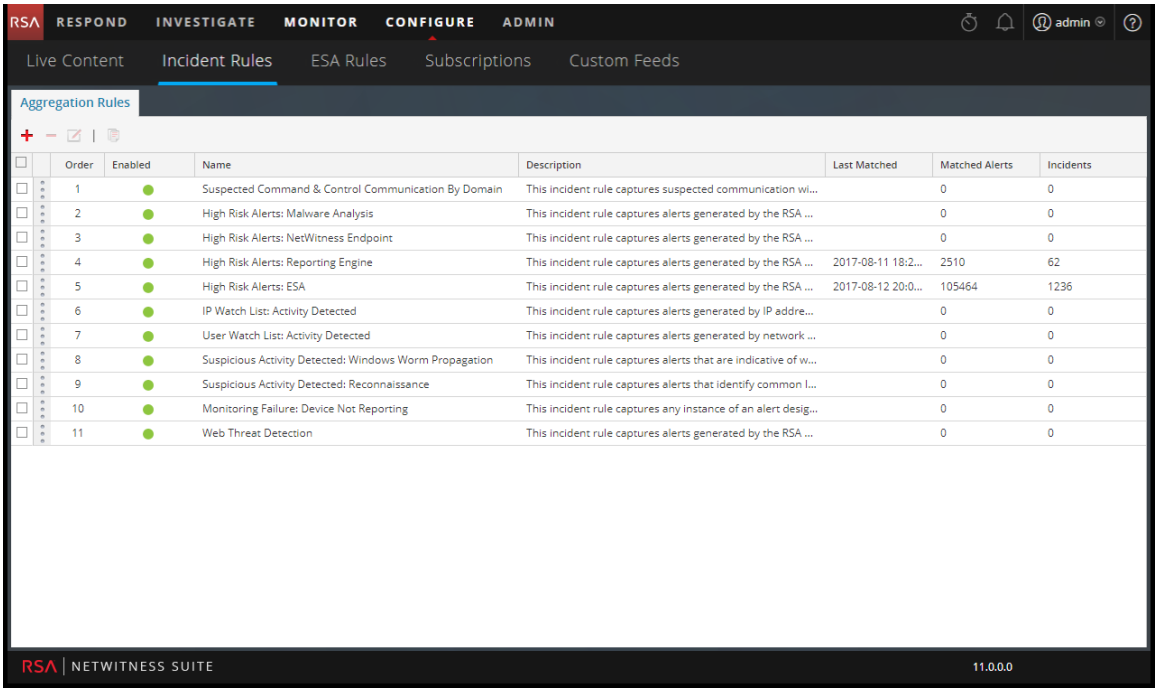
Step 3. Create an Aggregation Rule for Alerts

You can create aggregation rules with various criteria to automate the incident creation process. Alerts that meet the rule criteria are grouped together to form an incident. This is useful when you know a particular set of alerts can be grouped into an incident and you can set an aggregation rule that takes care of grouping the alerts instead of spending time in manually creating an incident and adding the alerts to that incident individually. To create incidents automatically you need to create an aggregation rule.

To create an aggregation rule:

1. Go to **CONFIGURE > Incident Rules**.

   The **Aggregation Rules** tab is displayed.



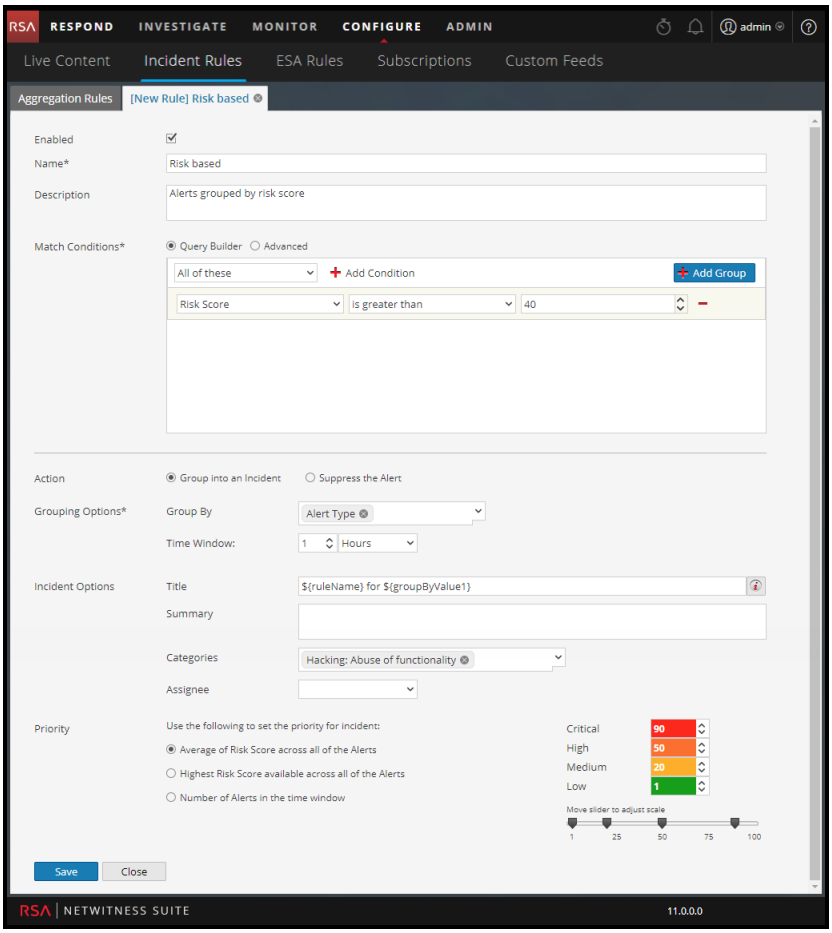
   A list of 11 predefined rules is displayed. You can do one of the following:

   - add a new rule
   - edit an existing rule
   - clone a rule

2. To add a new rule, select +.

   The **New Rule** tab is displayed.

   The example below shows grouping alerts into an incident based on the risk score.



3. Click **Save**.

   The rule is displayed in the **Aggregations Rules** tab. The rule will be enabled and it starts creating incidents depending on the incoming alerts that are matched as per the criteria selected.

See Also:

- For details about various parameters that can be set as criteria for an aggregation rule, see New Rule Tab.
- For details on the parameter and field descriptions in the Aggregation Rules tab, see Aggregation Rules Tab.

Additional Procedures for Respond Configuration

Use this section when you are looking for instructions to perform a specific task after the initial setup of NetWitness Respond.

Set a Retention Period for Alerts and Incidents

Sometimes data privacy officers want to retain data for a certain period of time and then delete it. A shorter retention period frees up disk space sooner. In some cases, the retention period must be short. For example, laws in Europe state that sensitive data cannot be retained for more than 30 days. After 30 days, the data must be obfuscated or deleted.

Setting a retention period for data is an optional procedure. The time that NetWitness Respond receives alerts and creates an incident determine when retention begins. Retention periods range from 30 to 365 days. If you set a retention period, one day after the period ends data is permanently deleted.

Retention is based on the time that NetWitness Respond receives the alerts and the incident creation time.

Caution: Data deleted after the retention period cannot be recovered.

When the retention period expires, the following data is **permanently deleted**:

- Alerts
- Incidents
- Tasks
- Journal entries

Logs track retention and manual deletion so you can see what has been deleted. You can view Respond Server logs in the following locations:

- **Respond Server Service log**: /var/log/netwitness/respond-server/respond-server.log
- **Respond Server Audit log**: /var/log/netwitness/respond-server/respond-server.audit.log

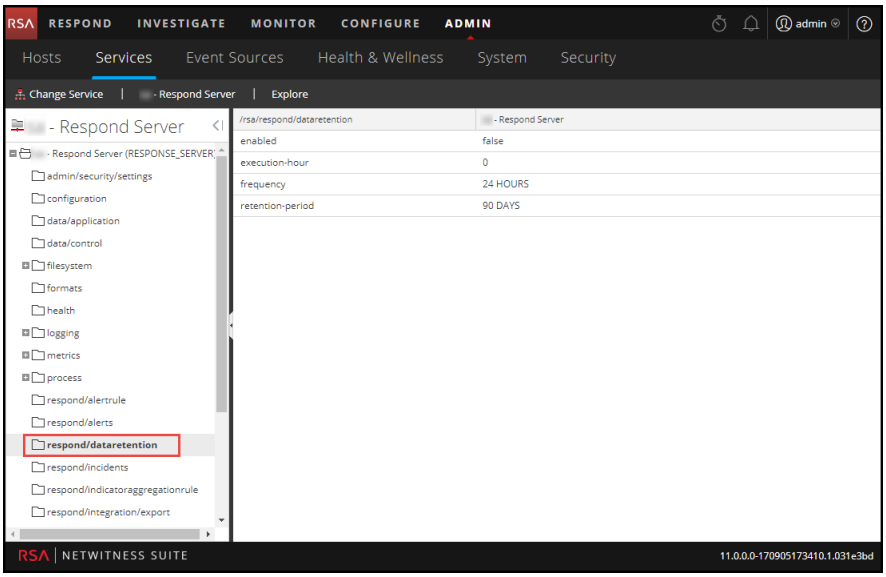
The data retention period that you set here does not apply to Archer or other third-party SOC tools. Alerts and incidents from other systems must be deleted separately.

Prerequisites

The Administrator role must be assigned to you.

Procedure

1. Go to **ADMIN > Services** , select the Respond Server service, and select > **View** > **Explore**.
2. In the Explore view node list, select **respond/dataretention**.



3. In the **enabled** field, select **true** to delete incidents and alerts older than the retention period. The scheduler runs every 24 hours at 23:00.
   You will see a notice that the configuration was successfully updated.
4. In the **retention-period** field, type the number of days to retain incidents and alerts. For example, type 30 DAYS, 60 DAYS, 90 DAYS, 120 DAYS, 365 DAYS, or any number of days.
   You will see a notice that the configuration was successfully updated.

Result

Within 24 hours after the retention period ends, the scheduler permanently deletes all alerts and incidents older than the specified period from NetWitness Respond. Journal entries and tasks associated with the deleted incidents are also deleted.

Obfuscate Private Data

The Data Privacy Officer (DPO) role can identify meta keys that contain sensitive data and should display obfuscated data. This topic explains how the administrator maps those meta keys to display a hashed value instead of the actual value.

The following caveats apply to hashed meta values:

- NetWitness Suite supports two storage methods for hashed meta values, HEX (default) and string.
- When a meta key is configured to display a hashed value, all security roles see only the hashed value in the Incidents module.
- You use hashed values the same way you use actual values. For example, when you use a hashed value in rule criteria the results are the same as if you used the actual value.

This topic explains how to obfuscate private data in NetWitness Respond. Refer to the **Data Privacy Management Overview** topic in the *Data Privacy Management* guide for additional information about data privacy.

Mapping File to Obfuscate Meta Keys

In the NetWitness Respond, the mapping file for data obfuscation is data_privacy_map.js. In it you type an obfuscated meta key name and map it to the actual meta key name.

The following example shows the mappings to obfuscate data for two meta keys, ip.src and user.dst:

```
'ip.src.hash' : 'ip.src',
 'user.dst.hash' : 'user.dst'
```

You determine the naming convention for obfuscated meta key names. For example, ip.src.hash could be ip.src.private or ip.src.bin. You must choose one naming convention and use it consistently on all hosts.

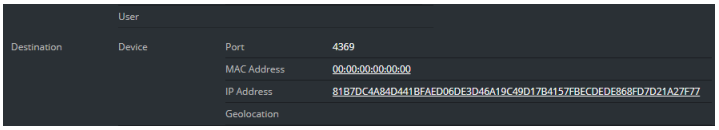
Prerequisites

- DPO role must specify which meta keys require data obfuscation.
- Administrator role must map meta keys for data obfuscation.

Procedure

1. Open the data privacy mapping file:
   /var/lib/netwitness/respond-server/scripts/data_privacy_map.js

2. In the `obfuscated_attribute_map` variable , type the name of a meta key to hold obfuscated data. Then map it to the meta key that does not contain obfuscated data according to this format:
   `'ip.src.hash' : 'ip.src'`
3. Repeat step 2 for every meta key that should display a hashed value.
4. Use the same naming convention as in step 2 and use it consistently on all hosts.
5. Save the file.
   All mapped meta keys will display hashed values instead of actual values.
   In the following figure, a hashed value displays for the destination IP address in the Event Details:



   New alerts will display obfuscated data.

Note: Existing alerts still display sensitive data. This procedure is not retroactive.

Manage Incidents in NetWitness SecOps Manager

If you want to manage incidents in RSA NetWitness® SecOps Manager instead of NetWitness Respond, you have to configure system integration settings in the Respond Server service Explore view. After you configure the system integration settings, all incidents are managed in NetWitness SecOps Manager. Incidents created before the integration will not be managed in NetWitness SecOps Manager.

Caution: If you are managing incidents in NetWitness SecOps Manager instead of NetWitness Respond, do not use the following in the Respond view: Incidents List view, Incident Details view, and Tasks List view. Do not create incidents from the Respond Alerts List view or from Investigate.

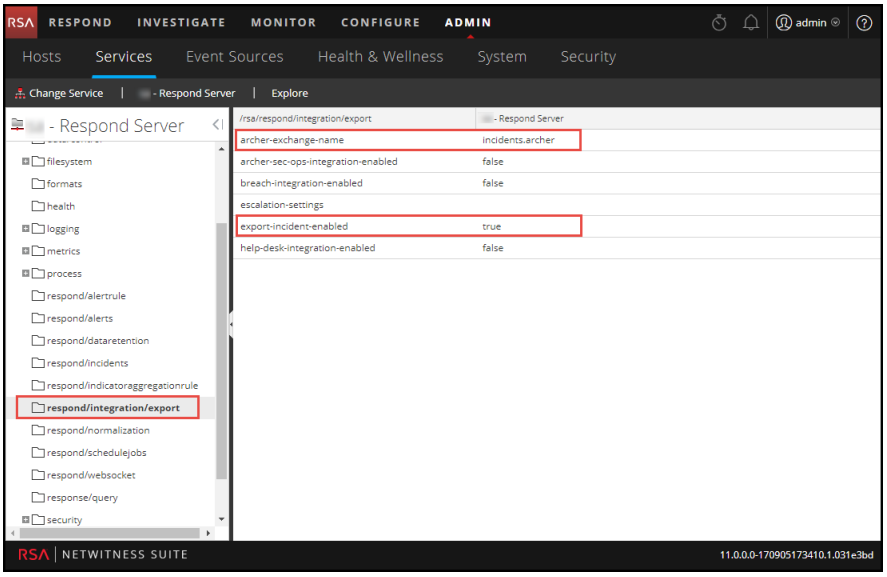
Prerequisites

- NetWitness SecOps Manager 1.3.1.2 (NetWitness Suite11.0 will only work with NetWitness SecOps Manager 1.3.1.2.)

Procedure

Follow this procedure to configure Respond Server service settings to manage incidents in NetWitness SecOps Manager.

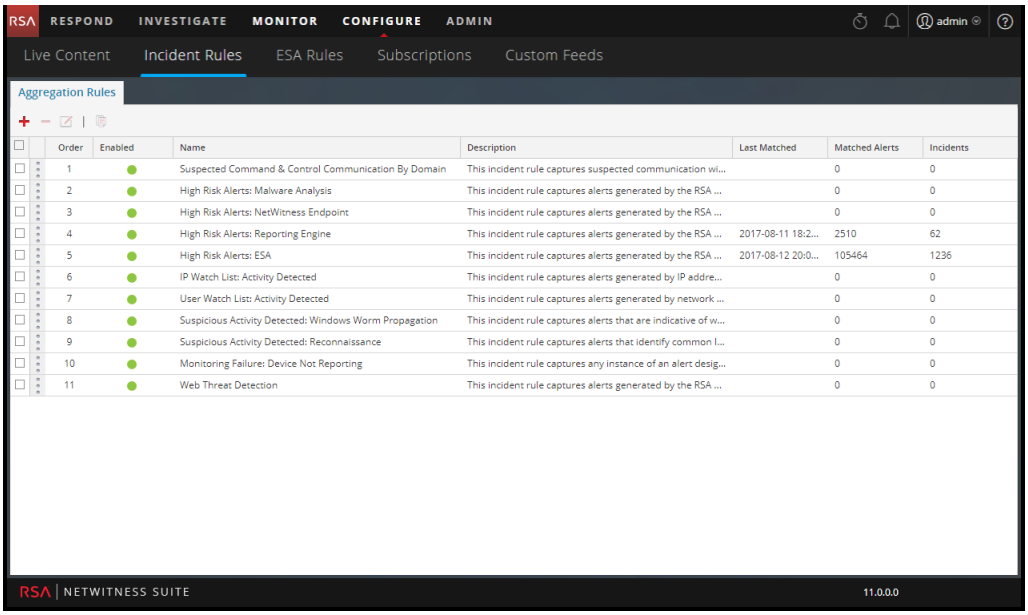
1. Go to **ADMIN > Services**, select the Respond Server service, and select > **Config** > **Explore**.
2. In the Explore view node list, select **respond/integration/export**.



3. In the **archer-exchange-name** field, type the NetWitness SecOps Manager exchange name.
   You will see a notice that the configuration was successfully updated.
4. In the **archer-sec-ops-integration-enabled** field, select **true**.
   You will see a notice that the configuration was successfully updated.
   Incidents will be managed exclusively in NetWitness SecOps Manager.

Set Counter for Matched Alerts and Incidents

This procedure is optional. Administrators can use it to change when the count for matched alerts is reset to 0. The Aggregation Rules tab displays these counts in columns on the right.



These columns provide the following information for a rule:

- **Last Matched** column shows the time when the rule last matched alerts.
- **Matched Alerts** column displays the number of matched alerts for the rule.
- **Incidents column** displays the number of incidents created by the rule.

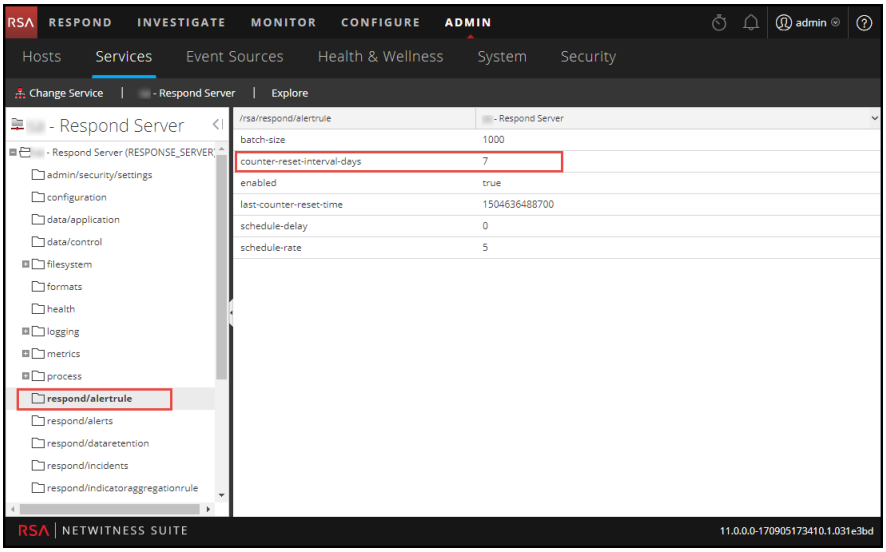
By default, these values reset to zero every 7 days. Depending on how long you want the counts to continue, you can change the default number of days.

Note: When the counter resets to zero, only the numbers in the three columns change to zero. No alerts or incidents get deleted.

To set a counter for matched alerts and incidents:

1. Go to **ADMIN > Services**, select the Respond Server service and select  **> View > Explore**.

2. In the Explore view node list, select **respond/alertrule**.



3. In the right panel, type the number of days in the **counter-reset-interval-days** field.
4. Restart the Respond Server service for the new setting to take effect. To do this, go to **ADMIN > Services**, select the Respond Server service, and select > **Restart**.

Configure a Database for the Respond Server Service

This procedure is required only if you need to change the database configuration for Respond Server after the deployment of the NetWitness or ESA Primary hosts and their corresponding services. You have to select the ESA Primary server to act as the database host for NetWitness Respond application data, such as alerts, incidents, and tasks. You also have to select the NetWitness Server to act as the database host for NetWitness Respond control data, such as aggregation rules and categories.

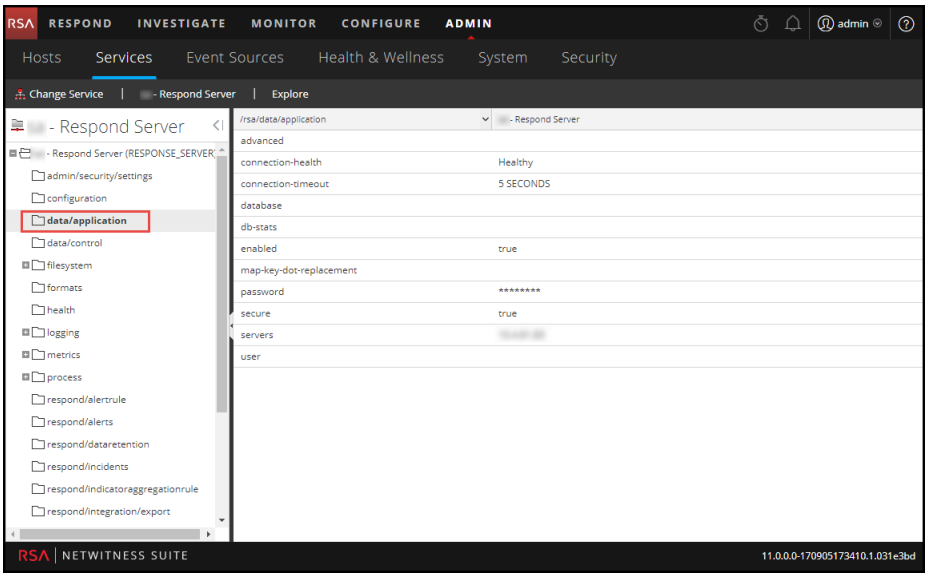
Prerequisites

Ensure that:

- You have installed a host on which you want to run the Respond Server service. Refer to "Step 1: Deploy a Host" in the *Hosts and Services Getting Started Guide* for the procedure to add a host.
- The Respond Server service is installed and running on NetWitness Suite.
- An ESA host is installed and configured.

Procedure

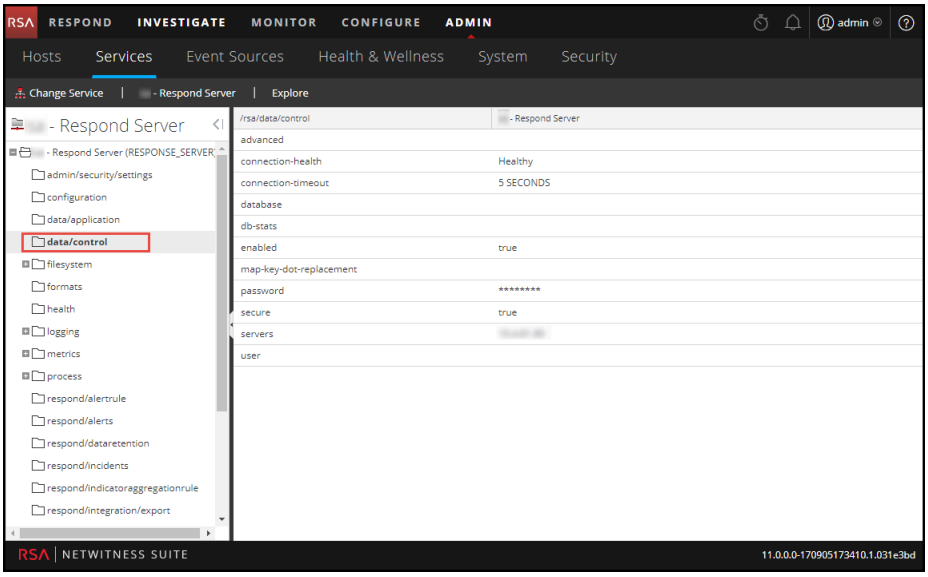
1. Go to **ADMIN > Services**.
   The Services view is displayed.
2. In the Services panel, select the **Respond Server** service and select  **> View > Explore**.
3. In the Explore view node list, select **data/application**.



4. Provide the following information:

   - **database**: The database name. The default value is respond-server.
   - **password**: The password used for the deployment of the ESA primary server (password for deploy_admin user).
   - **servers**: The hostname or IP address of the **ESA primary server** to act as the database host for NetWitness Respond application data, such as alerts, incidents, and tasks.
   - **user**: Enter **deploy_admin**.

5. In the Explore view node list, select **data/control**.



6. Provide the following information:

- **database**: The database name. The default value is respond-server.
- **password**: The password used for the deployment of the NetWitness Server (password for deploy_admin user).
- **servers**: The hostname or IP address of the **NetWitness Server** to act as the database host for NetWitness Respond control data, such as aggregation rules and categories.
- **user**: Enter **deploy_admin**.

7. Restart the Respond Server service. To do this, go to **ADMIN > Services**, select the Respond Server service, and select  **> Restart**.

Note: Restarting the Respond Server service is important for the database configuration to be complete.

NetWitness Respond Configuration Reference

This section contains reference information for configuring NetWitness Respond.

Configure View

The Configure view enables you to configure NetWitness Respond functionality.

You can configure aggregation rules to automate the Respond workflow for automatically creating incidents.

Aggregation Rules Tab

The Aggregation Rules tab enables you to create and manage aggregation rules for automating the incident creation process. NetWitness Suite provides 11 preconfigured rules. You can add to and adjust these rules for your own environment.

What do you want to do?

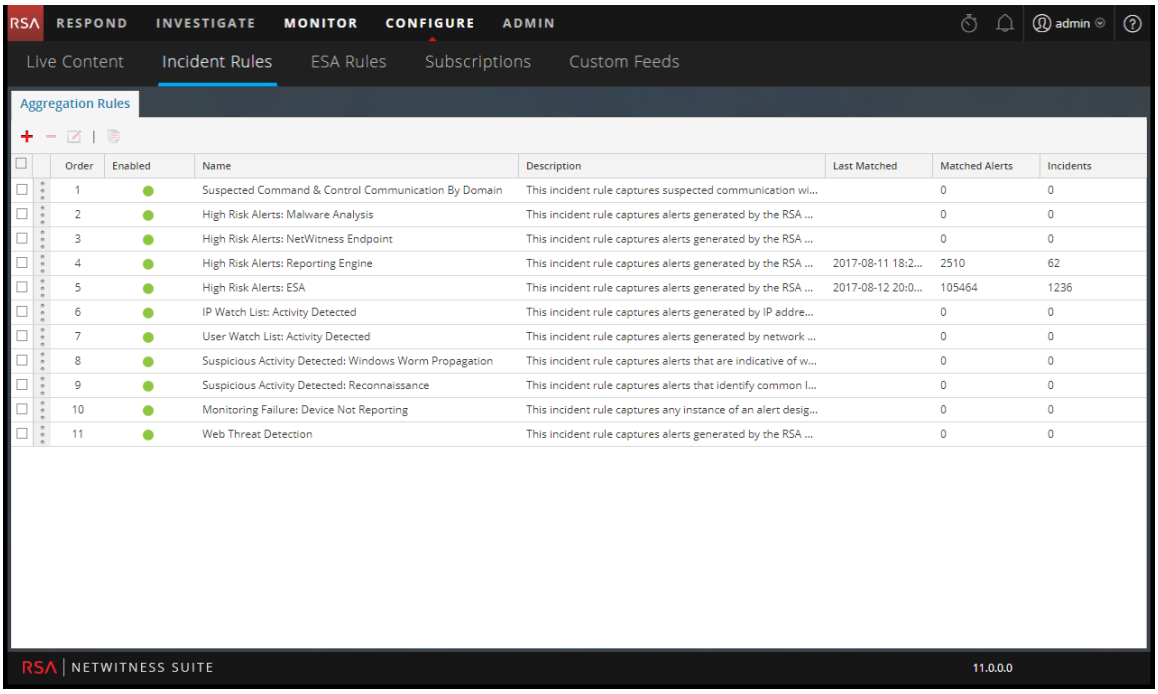
Role	I want to ...	Show me how
Analyst, Content Expert, SOC Manager	Create an aggregation rule.	Step 3. Create an Aggregation Rule for Alerts
Incident Responders, Analysts, Content Experts, SOC Manager	View the results of my aggregation rule (View Detected Threats).	See "Responding to Incidents" in the *NetWitness Respond User Guide*.

Related Topics

- New Rule Tab

Aggregation Rules

To access the Aggregation Rules tab, go to **CONFIGURE > Incident Rules > Aggregation Rules** tab.



The Aggregation Rules tab consists of a list and toolbar.

Aggregation Rules List

The following table describes the columns in the Aggregation Rules list.

Column	Description
Order	Shows the order in which the rule is placed. The rule order determines which rule takes effect if the criteria for multiple rules match the same alert.
Name	Displays the name of the rule.
Enabled	Shows whether the rule is enabled or not. The ● specifies the rule is enabled.
Description	Displays the description of the rule.
Last Matched	Displays the time when an alert was successfully matched with the rule. This value is reset once a week.
Matched Alerts	Displays the number of matched alerts. This value is reset once a week. To change the setting, see Set Counter for Matched Alerts and Incidents.

Column	Description
Incidents	Displays the number of incidents created by the rule. This value is reset once a week. To change the setting, see the Set Counter for Matched Alerts and Incidents.

Aggregation Rules Toolbar

The following table shows the operations that can be performed in the Aggregation Rules tab.

Option	Description
	Allows you to add a new rule.
	Allows you to edit a rule.
	Allows you to delete a rule.
	Allows you to duplicate a rule.

New Rule Tab

The New Rules tab enables you to create custom aggregation rules for automating the incident creation process. This topic describes the information required when creating a new rule.

What do you want to do?

Role	I want to ...	Show me how
Analyst, Content Expert, SOC Manager	Create an aggregation rule.	Step 3. Create an Aggregation Rule for Alerts
Incident Responders, Analysts, Content Experts, SOC Manager	View the results of my aggregation rule (View Detected Threats).	See "Responding to Incidents" in the *NetWitness Respond User Guide*.

Related Topics

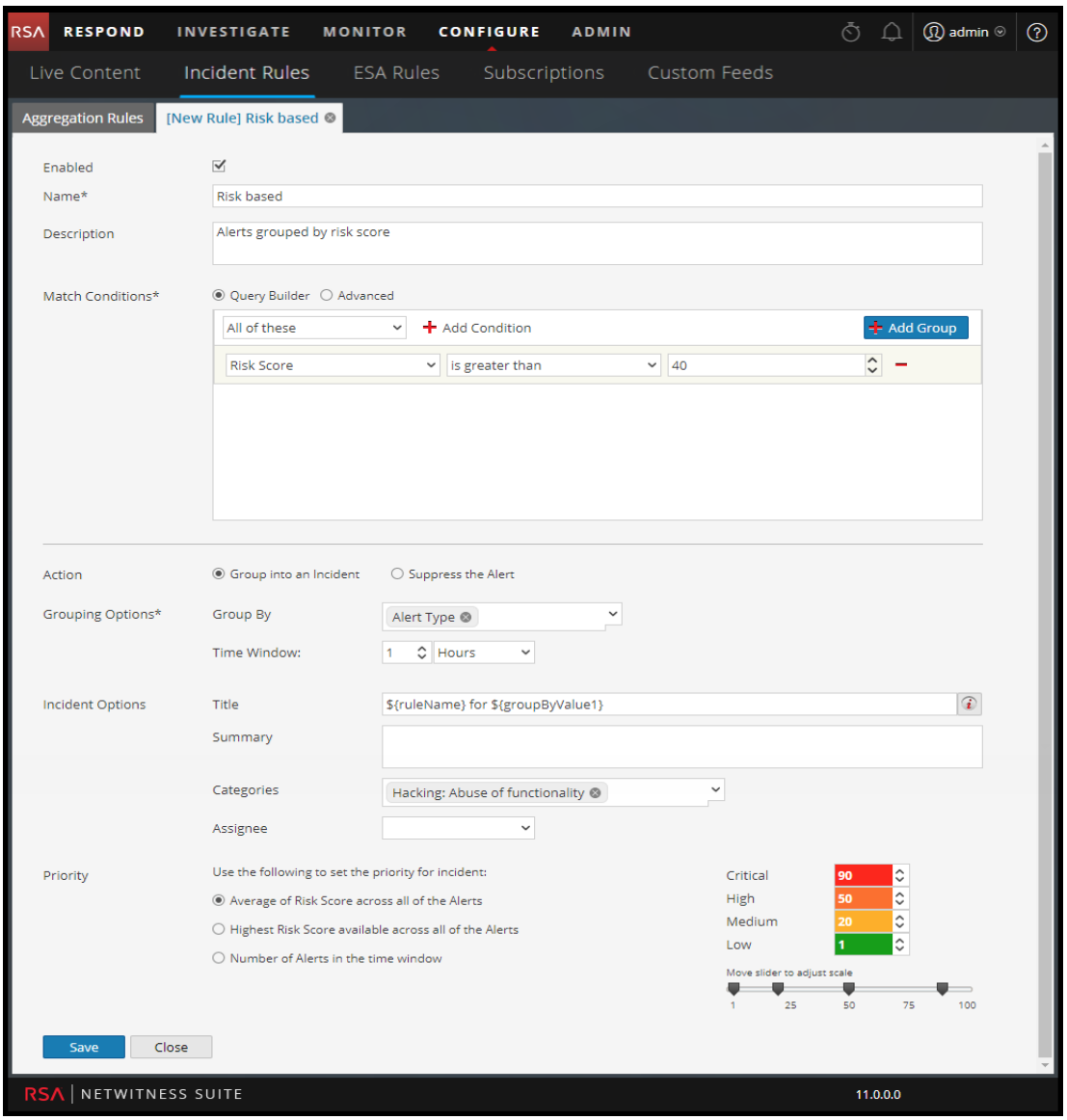
- Aggregation Rules Tab

New Rule

To access the New Rule tab view:

1. Go to **CONFIGURE > Incident Rules > Aggregation Rules** tab.
2. Click +.

The **New Rule** tab is displayed.



The following table describes the options available when creating customized aggregation rules.

Field	Description
Enabled	Select to enable the rule.
Name*	Name of the rule. This is a required field.
Description	A description for the rule to give an idea about what alerts get aggregated.

Field	Description
Match Conditions*	**Query Builder** - Select if you want to build a query with various conditions that can be grouped. You can also have nested groups of conditions. Match Conditions - You can set the value to **All of these**, **Any of these**, or **None of these**. Depending on what you select the the criteria types specified in the Conditions and Group of conditions are matched to group the alerts. **For example**, if you set the match condition to All of these, alerts that match the criteria mentioned in the Conditions and Group Conditions are grouped into one incident. • Add a Condition to be matched by clicking + **Add Condition**. • Add a Group of Conditions by clicking + **Add Group** and adding conditions by clicking + **Add Condition**. You can include multiple Conditions and Groups of Conditions that can be matched as per criteria set and group the incoming alerts into incidents.
	Advanced - Select if you want to add an advanced query builder. You can add a specific condition that needs to be matched as per the matching option selected. **For example:** you can type the criteria builder format **{"$and": [{"alert.severity" : {"$gt":4}}]}** to group alerts that have severity greater than 4. For advanced syntax, refer to http://docs.mongodb.org/manual/reference/operator/query/ or http://docs.mongodb.org/manual/reference/method/db.collection.find/
Action	**Group into an Incident** - If enabled, the alerts that match the criteria set are grouped into an alert. **Suppress the Alert** - If enabled, the alerts that match the criteria are suppressed.
Grouping Options*	**Group By:** The criteria to group the alerts as per the specified category. You can use a maximum of two attributes to group the alerts. You can group the alerts with one or two attributes. You can no longer group alerts with attributes that do not have values (empty attributes). Grouping on an attribute means that all matching Alerts containing the same value for that attribute are grouped together in the same incident. **Time Window:** The time range specified to group alerts. For example if the time window is set to 1 hour, all alerts that match the criteria set in Group By field and that arrive within an hour of each other are grouped into an incident.

Field	Description
Incident Options	**Title -** (Optional) Title of the incident. You can provide placeholders based on the attributes you grouped. Placeholders are optional. If you do not use placeholders, all Incidents created by the rule will have the same title. For example, if you grouped them according to the source, you can name the resulting Incident as Alerts for **${groupByValue1}**, and the incident for all alerts from NetWitness Endpoint would be named **Alerts for NetWitness Endpoint**.
	Summary - (Optional) Summary of the incident.
	Category - (Optional) Category of the incident created. An incident can be classified using more than one category.
	Assignee - (Optional) Name of the assignee to whom the incident is assigned to.
Priority	**Average of Risk Score across all of the Alerts** - Takes the average of the risk scores across all the alerts to set the priority of the incident created. **Highest Risk Score available across all of the Alerts** - Takes the highest score available across all the alerts to set the priority of the incident created. **Number of Alerts in the time window** - Takes the count of the number of alerts in the time window selected to set the priority of the incident created. **Critical, High, Medium, and Low** - Specify the incident priority threshold of the matched incidents. The defaults are: • Critical: 90 • High: 50 • Medium: 20 • Low: 1 For example, with the Critical priority set to 90, incidents with a risk score of 90 or higher will be assigned a Critical priority for this rule. You can change these defaults by manually changing the priorities or by moving the slider under **Move slider to adjust scale**.