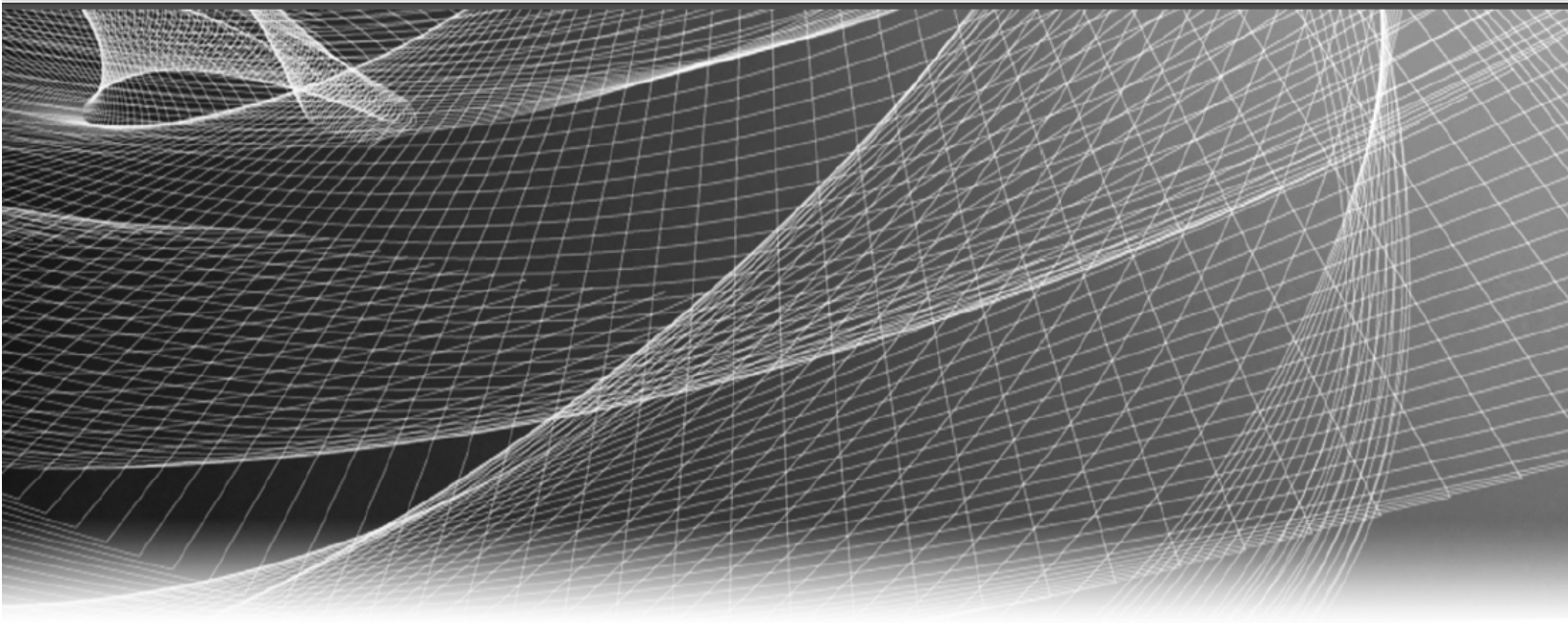


RSA Security Analytics

Warehouse Analytics Guide

for Version 10.6.5

RSA EMC²

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

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

Warehouse Analytics Overview

This topic describes how Data Analysts can analyze and identify the indicator of compromise (IOC), leveraging the RSA Analytics Warehouse data. You can analyze session and log data in your Warehouse using data science techniques. As Cyber Threat Intel analysts, you can view reports of early indicators of compromise. The following Warehouse Analytics models are supported for packet data:

- Suspicious Domains
- Suspicious DNS Activity
- Host Profile

Extract, Transform, and Load (ETL) Jobs

The ETL job runs a backend process on the Warehouse and pre-processes the data, which the models can use. The ETL job runs automatically every day at the prescribed time on the packet data. In this version, the module handles the packets data. The output of the ETL job is used as the input to the Suspicious Domains, Suspicious DNS Activity and Host Profile models. You must import the latest jobs for all the models from Live.

When the ETL job runs for the first time, the job processes data from the past 14 days (in UTC time zone) and subsequently processes data from the previous day (in UTC time zone). If you want to run the ETL jobs for any other date range, you can use the 'Test job' option.

Note: You cannot use ETL jobs to generate any viewable reports. If the ETL job fails for the first time, you can use the 'Test Job' to re-process the data for that time range.

Suspicious Domains

The Suspicious Domains model identifies malicious or suspicious domains based on its communication behavior. It uses a data-driven, automatic approach that is reactive and designed to identify the risky activity that is likely to be missed by other, signature-based solutions. This model generates profiles that describe the behaviors of the domains and applies a probabilistic-based risk assessment method on these profiles to reveal the most suspicious domains. Using these scores, you can find the domains that are most likely to be used for malicious activity within your network.

You can view a report with the following information:

- List of high risk destination domains and a ranking for all observed domains based on level of anomaly

- A comprehensive report explaining why each domain is high risk
- Risk scoring for each domain
- Unified risk score of the domain relative to all domains and based on multi-dimensional analysis of features about the connection.

Based on this information you can further investigate, block and recommend changes to the security policies to prevent future occurrences of such connections. You can also generate your own local domain blacklists and use it in incident investigation or to define a new security policy that prevents your assets from connecting to similar malicious domains in the future.

Suspicious DNS Activity

The Suspicious DNS Activity model can identify malicious domains based on a particular DNS communication pattern, common to botnets. This module uses an automatic method to identify the domains exhibiting a hosting pattern, in which the IP address of the malicious domains is constantly changing. This pattern is found in botnets, load-balanced hosts and content distribution networks (CDNs), and this model can differentiate between them and only detect the malicious domains. Once the domain is identified, you can isolate the host making the requests and block the access to the network.

You can view a report with the following information:

- List of domains showing suspicious fast-flux DNS with an associated risk score.
- Graph of the associated CDN communication with a score indicating whether the domain is showing the fast-flux pattern or not.

Host Profile

The Host Profile model collects and summarizes all HTTP, HTTPS, and DNS activity for each internal host in the network data. The module allows a fast investigation into the different types of usage patterns by the host and enables the analyst with answers to the questions that might arise during an investigation that require multiple queries or manual comparisons.

You can view a report with color coded heat maps to identify the risk of beacon traffic by the host. You can also view graphs that provide details on the traffic.

After the report is generated, you can perform the following tasks:

- Use a blacklist to alert and whitelist to ignore IPs or Domains that are benign.
- Create actionable security incidents from incoming alerts.

- Integrate incidents with a third-party help desk system to track the remediation process.
- Integrate with RSA Archer eGRC for incident management and remediation.

- Use the Investigation module to identify the root causes.

Required Procedures

This topic describes all the required procedures for working with Warehouse Analytics. They are presented in the order that you should complete the procedures.

Topics

Step 1. Configure Warehouse Analytics

The topic describes a high-level workflow on how to configure RSA Analytics Warehouse so you can perform advanced analytics on the data. To perform advanced analytics on your Warehouse, enable the Warehouse in the Reporting Engine.

Prerequisites

Make sure that:

- RSA Analytics Warehouse is installed and running.
- Warehouse Connector is configured. For more information, see the *Warehouse Connector Configuration Guide*.

Tasks

The following table provides the list of tasks required to configure the Warehouse Analytics.

Step	Process	Task/Instructions
1	Add Warehouse as a Data Source in the Reporting Engine and select the Enable Jobs checkbox.	See the **Add Warehouse Data Sources to Reporting Engine** topic in the *Host and Services Configuration Guide*.
2	Set up user access for Warehouse Analytics.	See Step 2. Manage Access to Warehouse Analytics Module.
3	Configure Warehouse Analytics models.	See Step 3. Configure Warehouse Analytics Models.
4	Set up the Warehouse Analytics configurations on the Reporting Engine.	See the **Warehouse Analytics Output Configuration** and **Warehouse Analytics Model Configuration** sections in Reporting Engine General Tab topic in the *Host and Services Configuration Guide*. **Note:** You must define the 'Warehouse Analytics Output Configuration' to use Warehouse Analytics. The 'Warehouse Analytics Model Configuration' is optional.

Next steps

After you configure RSA Analytics Warehouse, perform the following tasks:

- Analyze the Warehouse Analytics reports. For instructions, see Step 4. Analyze a Warehouse Analytics Report.
- Investigate the Warehouse Analytics reports. For instructions, see Step 5. Investigate a Warehouse Analytics Report.

Step 2. Manage Access to Warehouse Analytics Module

This topic describes how you can set up access and permissions to manage the Warehouse Analytics job. The access control for the Warehouse Analytics module is provided at the job level. Only a user who has the right set of permissions can perform the tasks in the Warehouse Analytics module. The access control is managed by the administrator from the **Administration > Security > Roles** tab.

As an administrator you must ensure that the roles created for specific tasks have access to all the permissions higher in the hierarchy of roles.

Jobs are tied to a specific set of user roles so when a user logs into Security Analytics, the only jobs the user can access are that to which the user belongs. Users that belong to a user role with the ‘Read & Write’ access permission have full access rights on the job. Further, the access can be strengthened so that jobs are accessed only by those who have the ‘Read Only’ access.

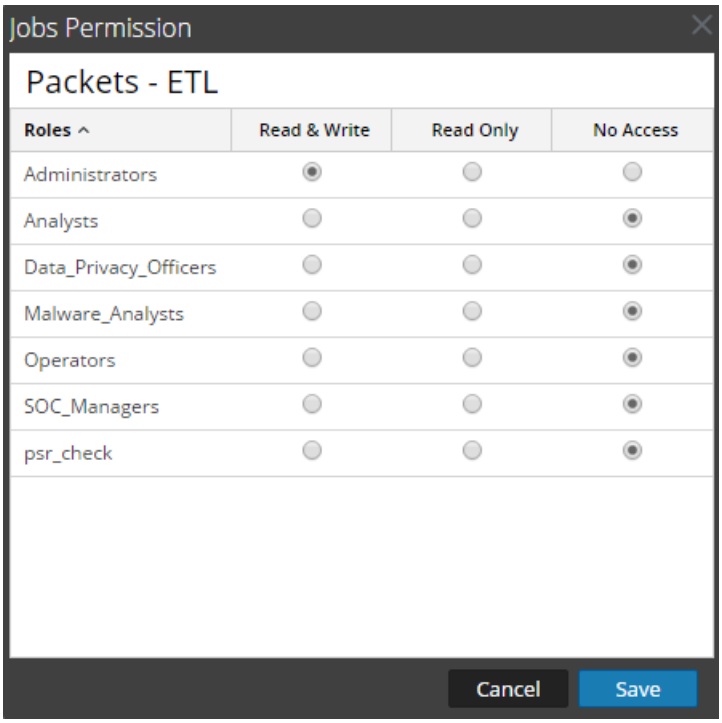
At the job level, you can set the following access permissions for the user roles in Security Analytics:

- Read & Write
- Read Only
- No Access

Access Control for a Warehouse Analytics Module

When you want to change the job permissions, you must select a job and set their access permissions using the Jobs Permission panel.

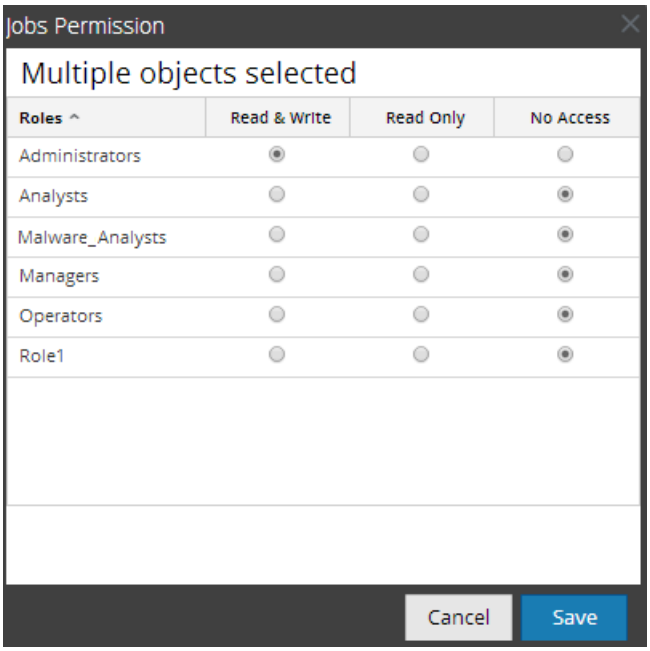
Except for Administrators, the default permission set for all the other user roles is 'No Access' before applying job permissions.



If you want to change the access permission for a specific user role, you must set these at the job level.

Access Control for a Job When Multiple Jobs are Selected

When you want to change permissions of multiple jobs, you can select multiple jobs at a time and set their access permissions on the Jobs Permission panel. The access permission that you select is applied to all the selected jobs.



Tabular Listing

The following table lists the various columns in the Jobs Permission panel:

Column	Description
Roles	The role of the user who has logged into Security Analytics.
Read & Write	The user can access, view, edit, delete jobs on the Warehouse Analytics view. The user can also change the permission on the job.
Read Only	The user can only access and view the job on the Warehouse Analytics view
No Access	The user cannot access or view the job for which this permission is set.

Topics

- Add a Role and Assign Permissions for Warehouse Analytics
- Set Access Control for a Warehouse Analytics Job

Add a Role and Assign Permissions for Warehouse Analytics

This topic describes how to add a role and assign permissions to the role.

Pre-configured Roles

Although Security Analytics has five pre-configured roles, you can add custom roles. For example, in addition to the pre-configured Analysts role you can add custom roles for AnalystsEurope and AnalystsAsia.

Role	Permission
Administrators	Full system access
Operators	Access to configurations but not to data
Analysts	Access to data but not to configurations
SOC_Managers	Same access as Analysts plus additional permission to handle incidents
Malware_Analysts	Access to malware events only

Depending on the user role, you can set the following access permissions to access the Warehouse Analytics module:

- Define Jobs
- Delete Jobs
- Manage Jobs
- View Jobs

Note: You must enable all of these permissions for a user role to be able to define, delete, manage, and view jobs.

For more information on the list of permissions, see **Role Permissions** topic in the *System Security and User Management Guide*.

Add Roles

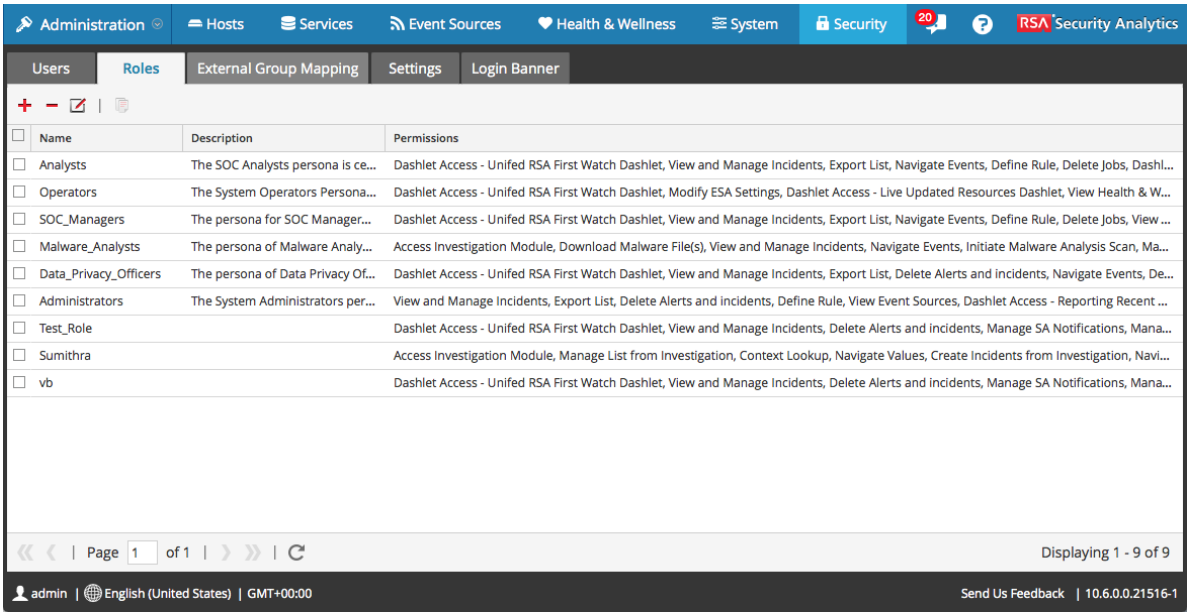
To add roles and assign permissions on the Roles tab:

1. In the **Security Analytics** menu, select **Administration** > **Security**.

   The Administration Security view is displayed.

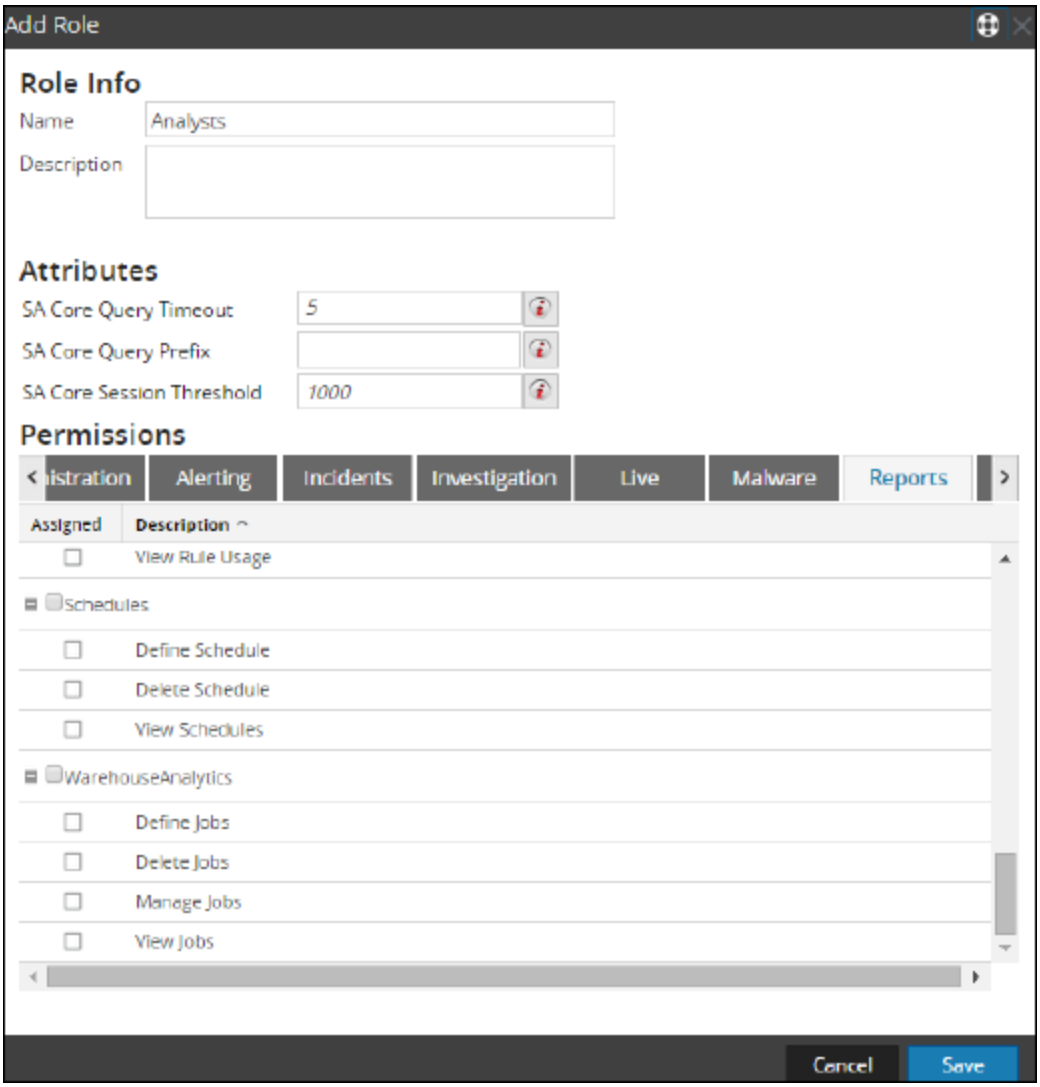
2. Click the **Roles** tab.

   The **Roles** tab is displayed.



3. In the **Roles** tab, click + in the toolbar.

   The **Add Role** dialog is displayed.



4. In the **Role Info** section, enter the following information for the role:
   - **Name**
   - (Optional) **Description**
5. In the **Permissions** section, select the Reports module that the role will access and select each permission the role will have.
6. Repeat step 5 to select all the permissions required for the role.
7. Click **Save**.

Next steps

You can now assign the new role to users.

Set Access Control for a Warehouse Analytics Job

This topic provides instructions on how to set access control for a Warehouse Analytics job.

Prerequisites

Make sure that:

- You understand the components of the Warehouse Analytics view. For more information, see Warehouse Analytics View.
- You understand the access permissions the user will have depending on the user role. For more information, see Step 2. Manage Access to Warehouse Analytics Module.
- You have a Read & Write access permission to set up the access for a Warehouse Analytics job.

Set Access Permissions

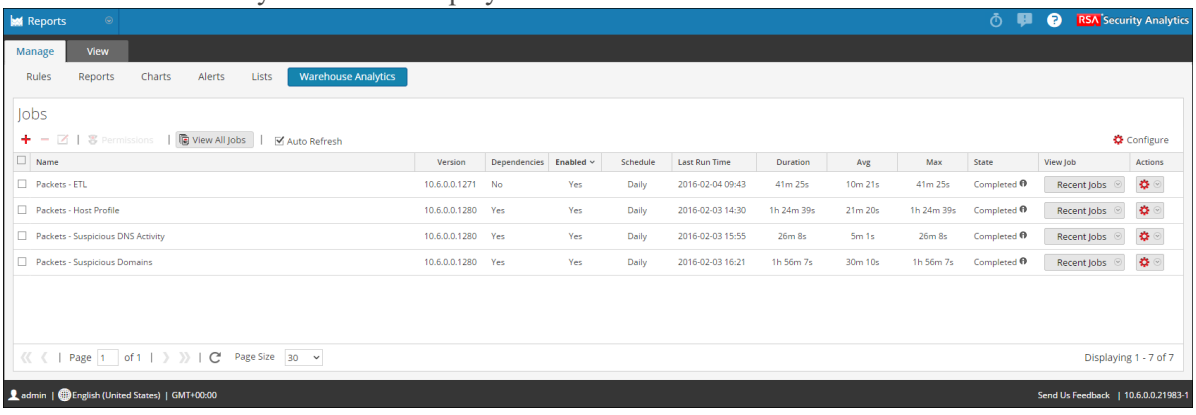
To set access permissions for a Warehouse Analytics job:

1. In the Security Analytics menu, click **Reports.**.

   The Manage tab is displayed.

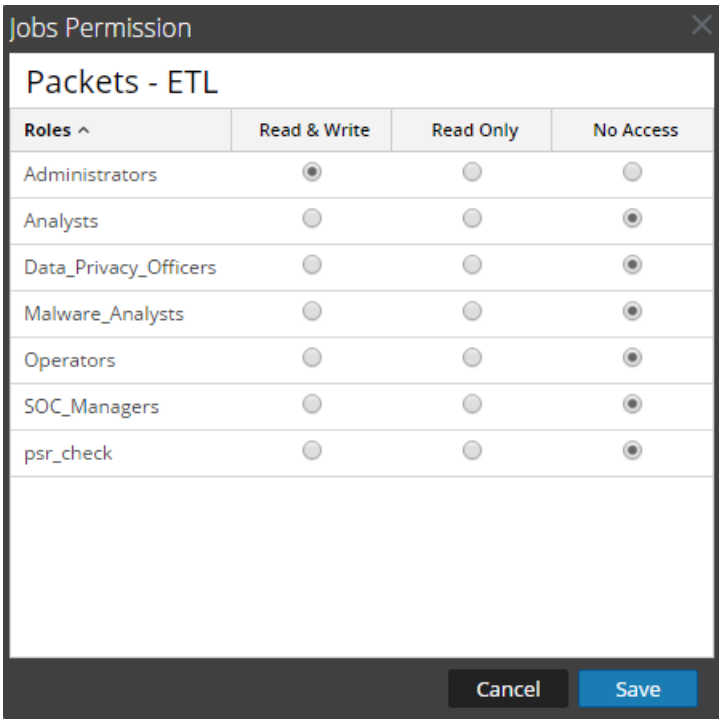
2. Click **Warehouse Analytics**.

   The Warehouse Analytics view is displayed.



3. Select a job and click Permissions.

   The Jobs Permission dialog is displayed.



4. Based on the user role, select the appropriate radio buttons.
5. Click **Save**.

   A confirmation message that the permission is successfully set for the selected job is displayed.

Step 3. Configure Warehouse Analytics Models

This topic provides instructions on how to import and define Warehouse Analytics models and schedule them for execution. You can schedule a job for the Warehouse Analytics model from the Warehouse Analytics view.

Prerequisites

Make sure that:

- You have understood the components of the Warehouse Analytics view. For more information, see Warehouse Analytics View.
- You have understood the components of the Job Definition view. For more information, see Job Definition View.

Procedure

To configure Warehouse Analytics Models:

Step	Process	Task / Instructions
1	Download the Warehouse Analytics models from the Live.	See Deploy Warehouse Analytics Models
2	Define the Warehouse Analytics Job	See Deploy Warehouse Analytics Models

Topics

- Deploy Warehouse Analytics Models
- Define a Warehouse Analytics Job
- Use a Whitelist in a Warehouse Analytics Job

Deploy Warehouse Analytics Models

This topic describes a high level workflow to download a Warehouse Analytics Model from the RSA Live Server.

Prerequisite

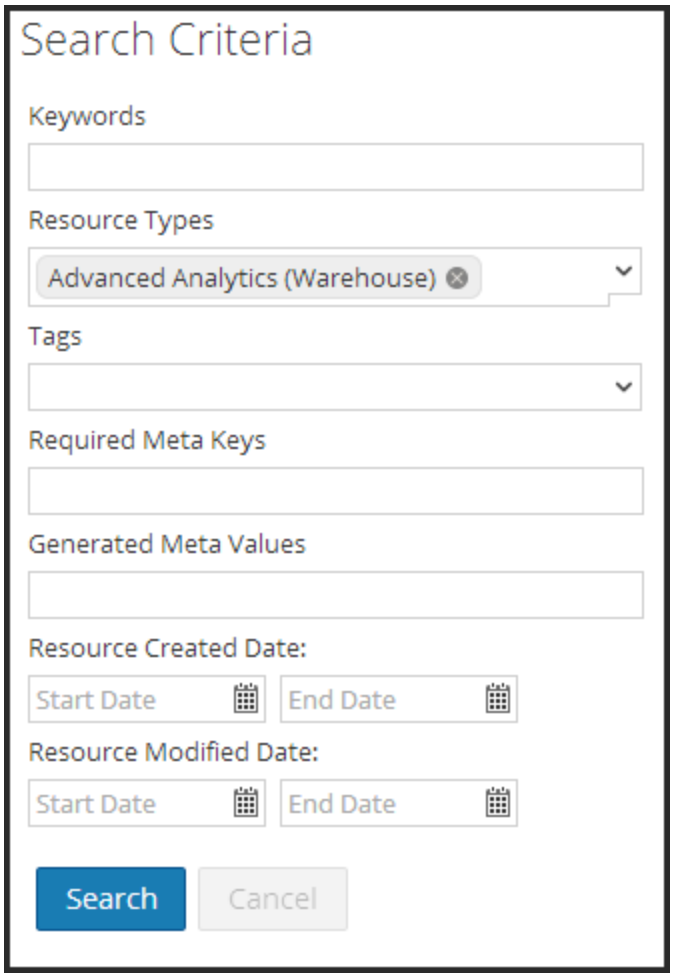
Make sure that you have done the following:

- You have created a Live Account. For more information, see **Step 1. Create Live Account** in the *Live Services Management Guide*.
- You have configured the connection and synchronization between the CMS server and Security Analytics. For more information, see **Step 2. Set Up Live on Security Analytics** in the *Live Services Management Guide*.

Deploy a Warehouse Analytics Model

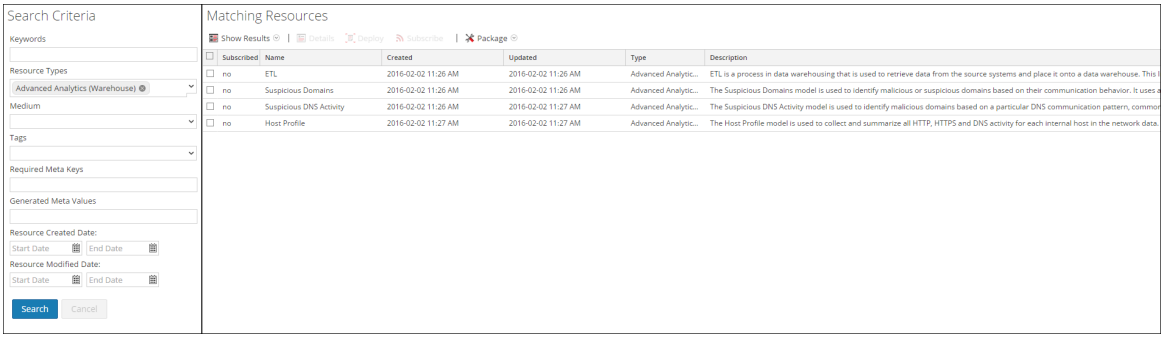
To deploy a Warehouse Analytics model:

1. Search for and find a Warehouse Analytics model.
   a. In the Security Analytics menu, select **Live > Search**.
   b. In the **Search Criteria** panel, specify the search criteria. In the **Resource Types**, select **Advanced Analytics (Warehouse)**.



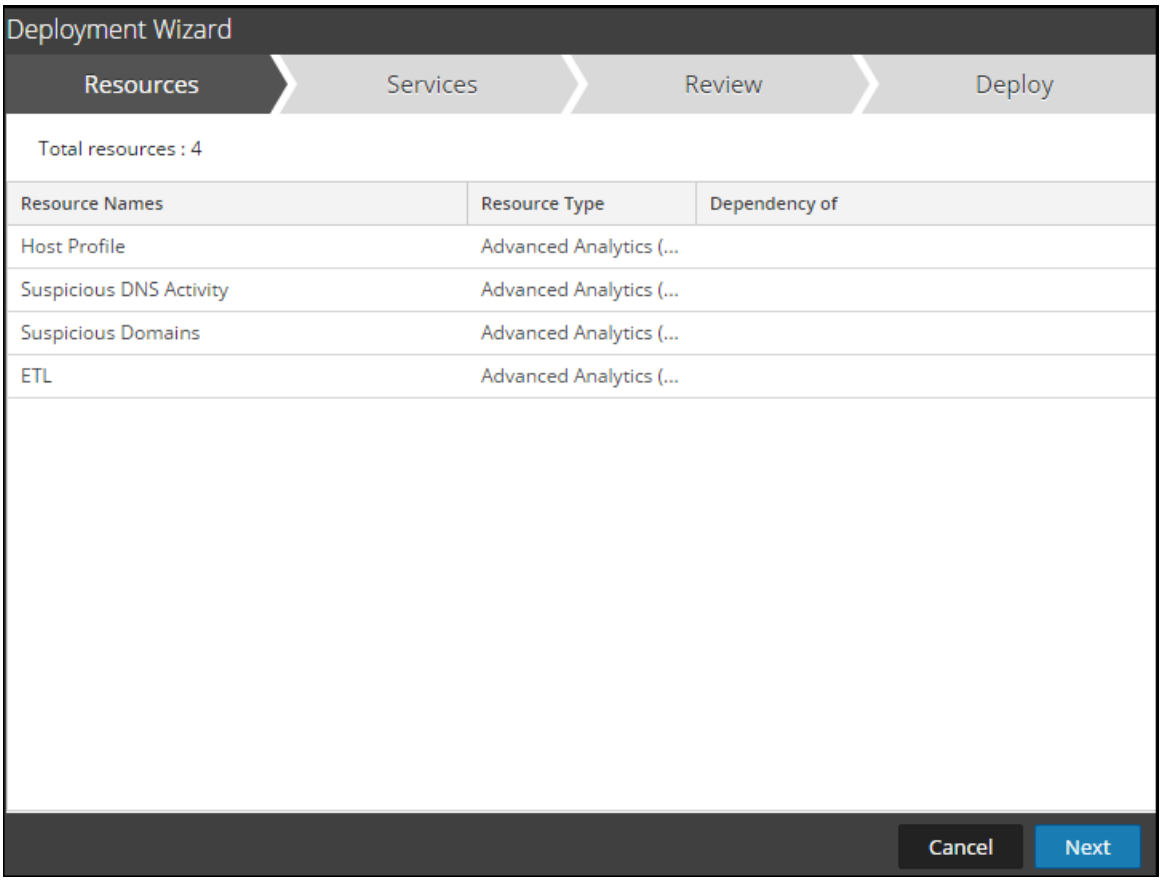
c. Click **Search**.

The Warehouse Analytics models are listed as shown in the Matching Resources panel.



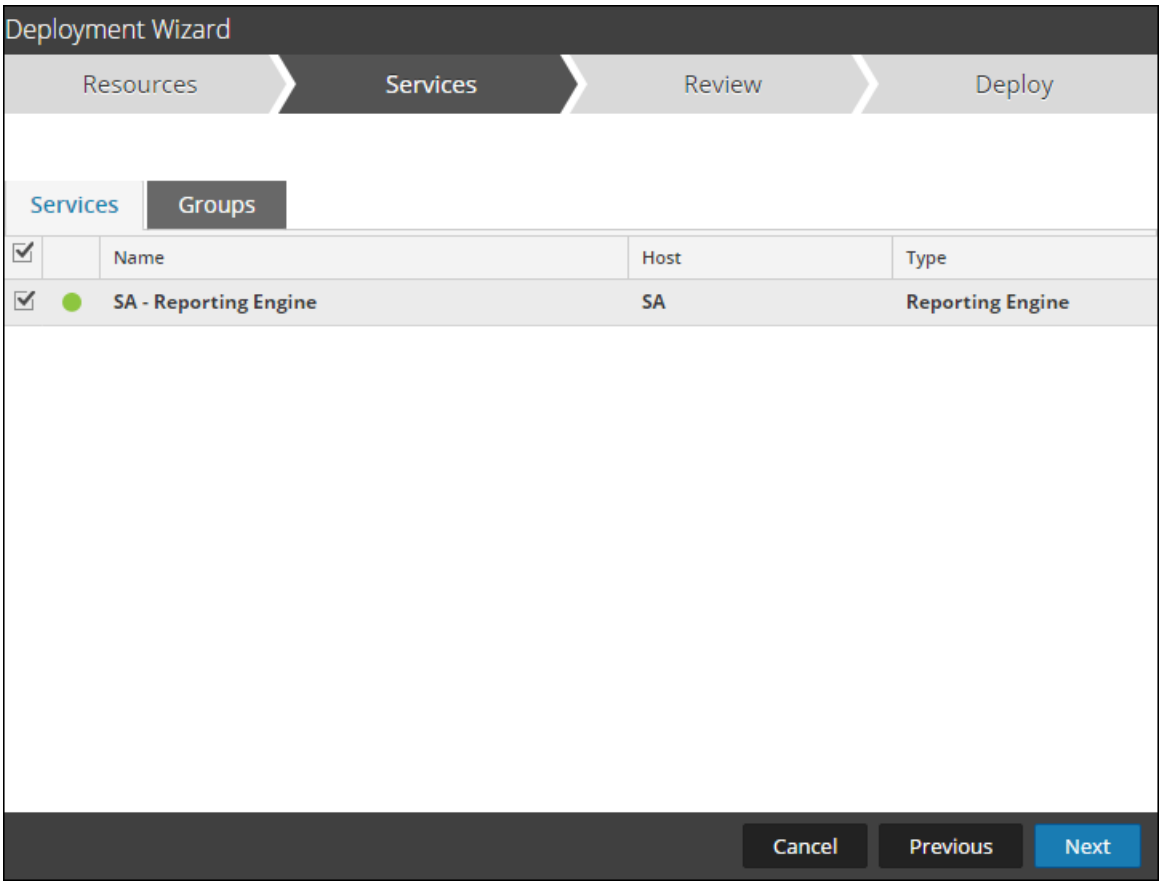
2. Select the desired resource and click Deploy.

The **Deployment Wizard** page is displayed.



3. Click **Next**.

   The **Services** page is displayed.

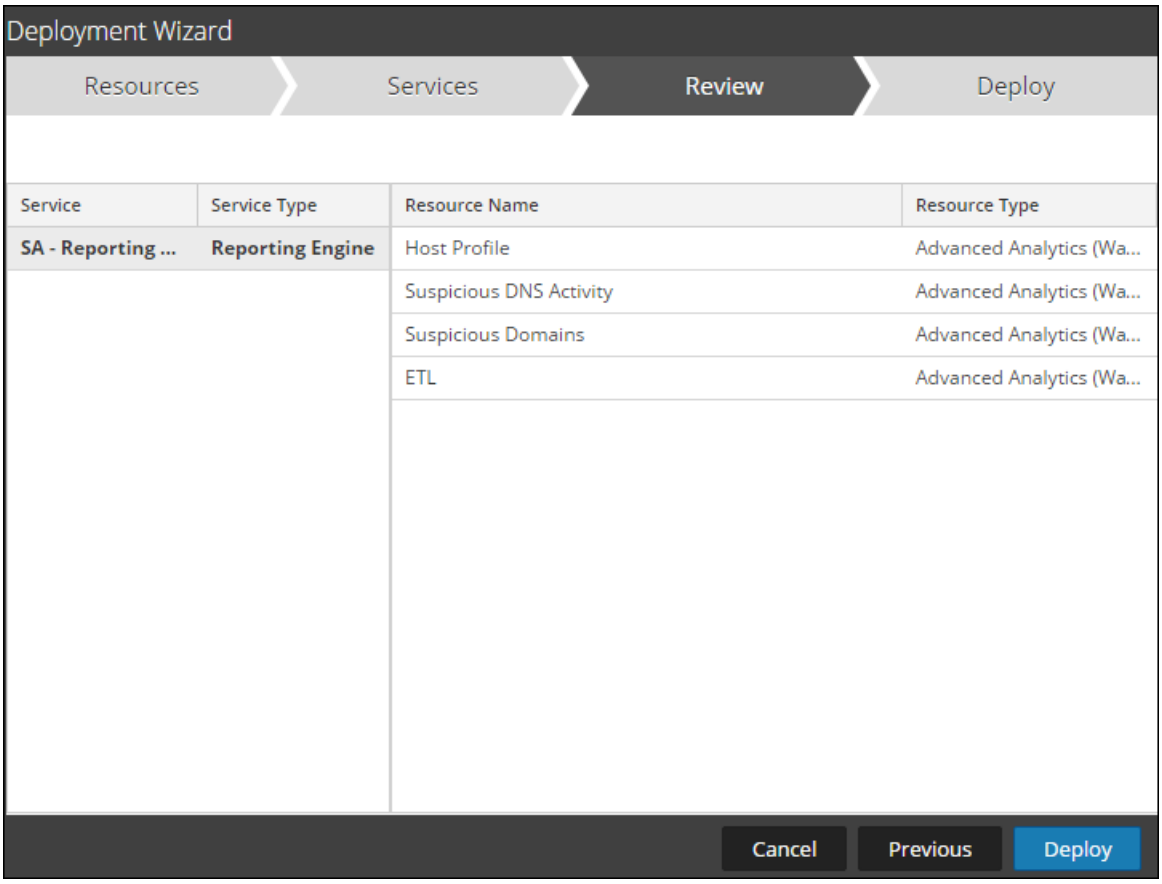


The **Services** page contains two tabs, **Services** and **Groups.** These tabs provide a list of services and service groups that are configured in the **Administration > Services** view. The columns are a subset of the ones available in the Services View. You can select a combination of services and service groups as explained below:

- 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.

4. Click **Next**.

   The **Review** tab is displayed.



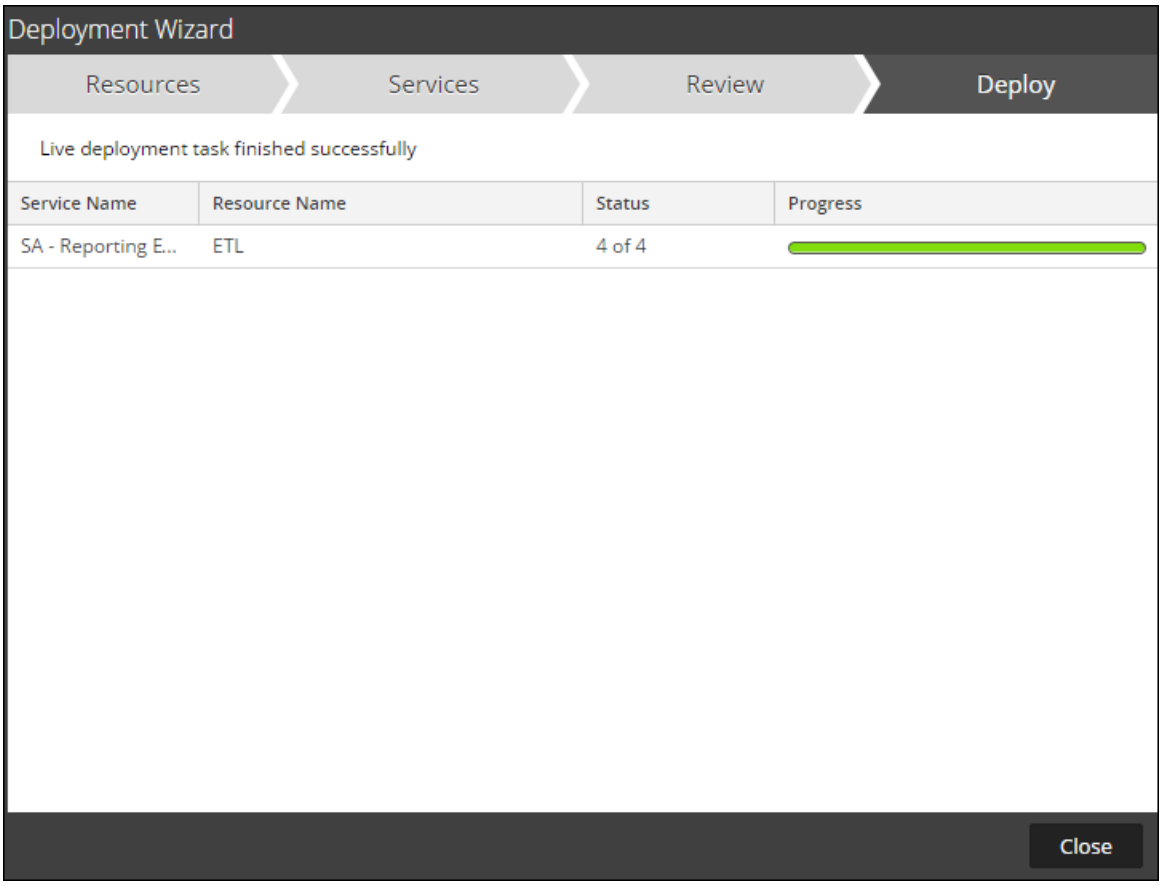
Note: Make sure that you have selected the correct resources and the services to which you want to deploy them.

5. Click **Deploy** to initiate the Live deployment.

   The **Deploy** tab is displayed with the progress bar that indicates the Live deployment status.

   If you try to deploy resources and services that are not compatible, Security Analytics displays Errors to review the errors and you can click Retry to review the errors and re-attempt the deployment.

   After the deployment completes, the following message is displayed and the bar turns green: "**Live deployment task finished successfully**".



6. Click **Close**.

Define a Warehouse Analytics Job

This topic provides instructions to define and schedule a job. To define a Warehouse Analytics job, you must first import the Warehouse Analytics model from the RSA Live and then schedule the job.

Prerequisites

Make sure that you understand the following:

- Deploying Warehouse Analytics Models from Live. For more information, see Deploy a Warehouse Analytics Model.

  Note: It is recommended that you always deploy Warehouse Analytics models from Live.

- The components of the Warehouse Analytics view. For more information, see Warehouse Analytics View.
- The components of the Job Definition view. For more information, see Job Definition View.

Add and Schedule a Job

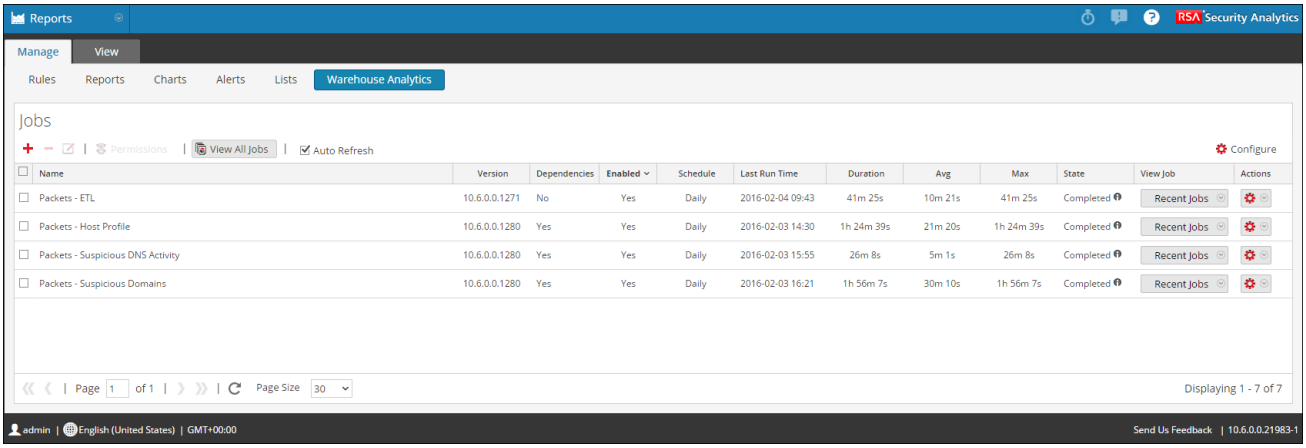
To add and schedule a job:

1. In the Security Analytics menu, click **Reports**.

   The Manage tab is displayed.

2. Click **Warehouse Analytics**.

   The Warehouse Analytics view is displayed.



3. In the Warehouse Analytics toolbar, click

 .

The Job definition tab is displayed.

4. To execute the jobs as per the schedule, select **Enable** checkbox.
5. In the **Name** field, enter a name for the job configuration.
6. From the **Model** field, click **Browse** to select a jar file to be imported.

   Security Analytics provides a file system view.
7. Locate the jar file and click **Open**.

   The file is added to the job definition view.
8. From the **Warehouse** field, select the data source created in the Reporting Engine configuration page. (For example, Pivotal or MapR).
9. Do one of the following:
   - For specific number of days, select the date range to run the query based on **Past**
   - For a specific time frame, specify the **From** and **To** date from the calendar

   Note: When you upgrade from 10.6, the jobs for Suspicious Domains, Suspicious DNS Activity and Host Profile models are deprecated and disabled. They appear under the **Manage > Warehouse Analytics** tab as "DEPRECATED" jobs and can be used as a reference to create new jobs.
10. In the **Advanced Options** field, do the following:
    - In the **Model Params** field, enter the DS model or job parameters from the List Selection window. For more information on using a whitelist, see Use a Whitelist in a Warehouse Analytics Job
    - In the **HDFS Params** field, enter the HDFS configuration parameters.
    - In the **MapReduce Params** field, enter the Hadoop or MapR configuration parameters.
    - In the **SandBox JVM Params** field, enter the JVM or "-D" system parameters for JVM executing DS model.

    Note: On uploading the job, several important parameters are automatically populated. If the parameters are not specified, the job runs with the default values.
11. Click **Save**.

    The Warehouse Analytics executes the job as scheduled and provides the configured outputs.

Next steps

You can view the scheduled job on the Warehouse Analytics view.

Use a Whitelist in a Warehouse Analytics Job

This topic provides instructions on how you can use whitelists in a Warehouse Analytics job. You can use a whitelist in a Warehouse Analytics job so that domains that are not suspicious can be ignored while processing. You can use whitelists only in the Suspicious Domains and Suspicious DNS Activity report.

Prerequisites

Make sure that:

- You have created the whitelist. For example, a list of domains that are confirmed to not be suspicious or a whitelist of domains on which no DNS activities occur. For more information on creating a list, see Add a list topic in the *Reporting Guide*.
- You have downloaded the Warehouse Analytics Jobs from the Live Server. For more information, see Deploy Warehouse Analytics Models.
- You understand the components of the Warehouse Analytics view. For more information, see Warehouse Analytics View.
- You understand the components of the Job Definition view. For more information, see Job Definition View.

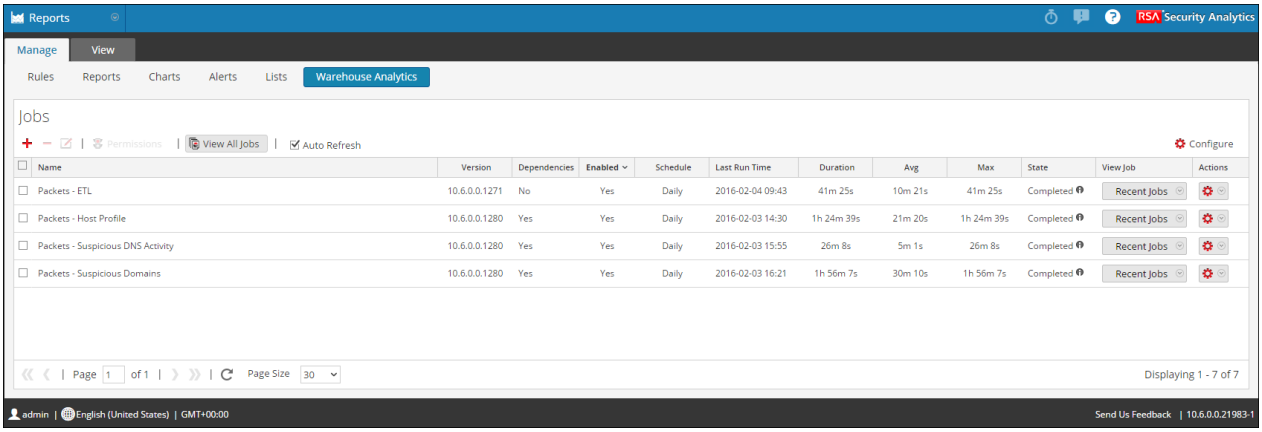
Procedure

Perform the following steps to add and schedule a job for execution:

1. In the Security Analytics menu, click **Reports.**
   The Manage tab is displayed.

2. Click **Warehouse Analytics**.

   The Warehouse Analytics view is displayed.



3. In the Warehouse Analytics toolbar, click +.

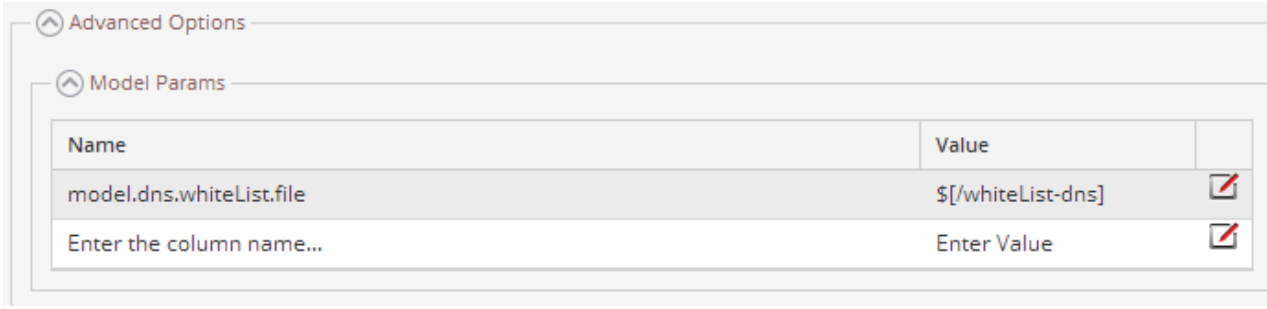
   The Job definition tab is displayed.

4. Define the job and the schedule. For more information, see Step 3. Configure Warehouse Analytics Models.

5. In the **Advanced Options:**

   1. In the **Model Params** field, enter the parameters to include the whitelist.

   - For Suspicious Domains model, enter the parameter name as **model.suspiciousDomains**.whiteList.file and select the list using . For more information, see Analyze a Suspicious Domains Report.
   - For Suspicious DNS Activity model, enter the parameter name as **model.dns.whiteList.file** and select the list using . For more information, see Analyze a Suspicious DNS Activity Report.



6. Click **Save**.

   The Warehouse Analytics executes the job scheduled and provides the configured outputs.

Step 4. Analyze a Warehouse Analytics Report

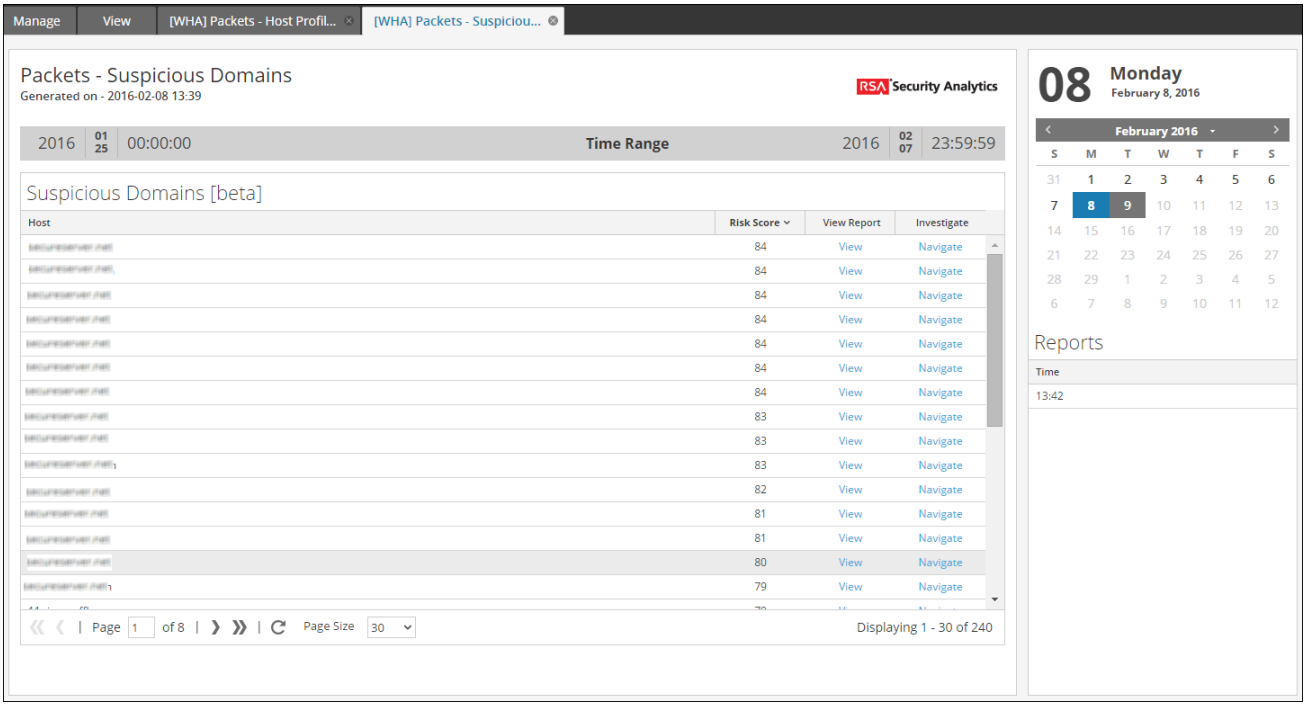
This topic covers all the instances for analyzing a Warehouse Analytics report. The Warehouse Analytics modules provide analysts with reports of early indicators of compromise. The following Warehouse Analytics reports can be analyzed in Security Analytics:

- Suspicious Domains report. For more information, see Analyze a Suspicious Domains Report.
- Suspicious DNS Activity report. For more information, see Analyze a Suspicious DNS Activity Report.
- Host Profile report. For more information, see Analyze a Host Profile Report.

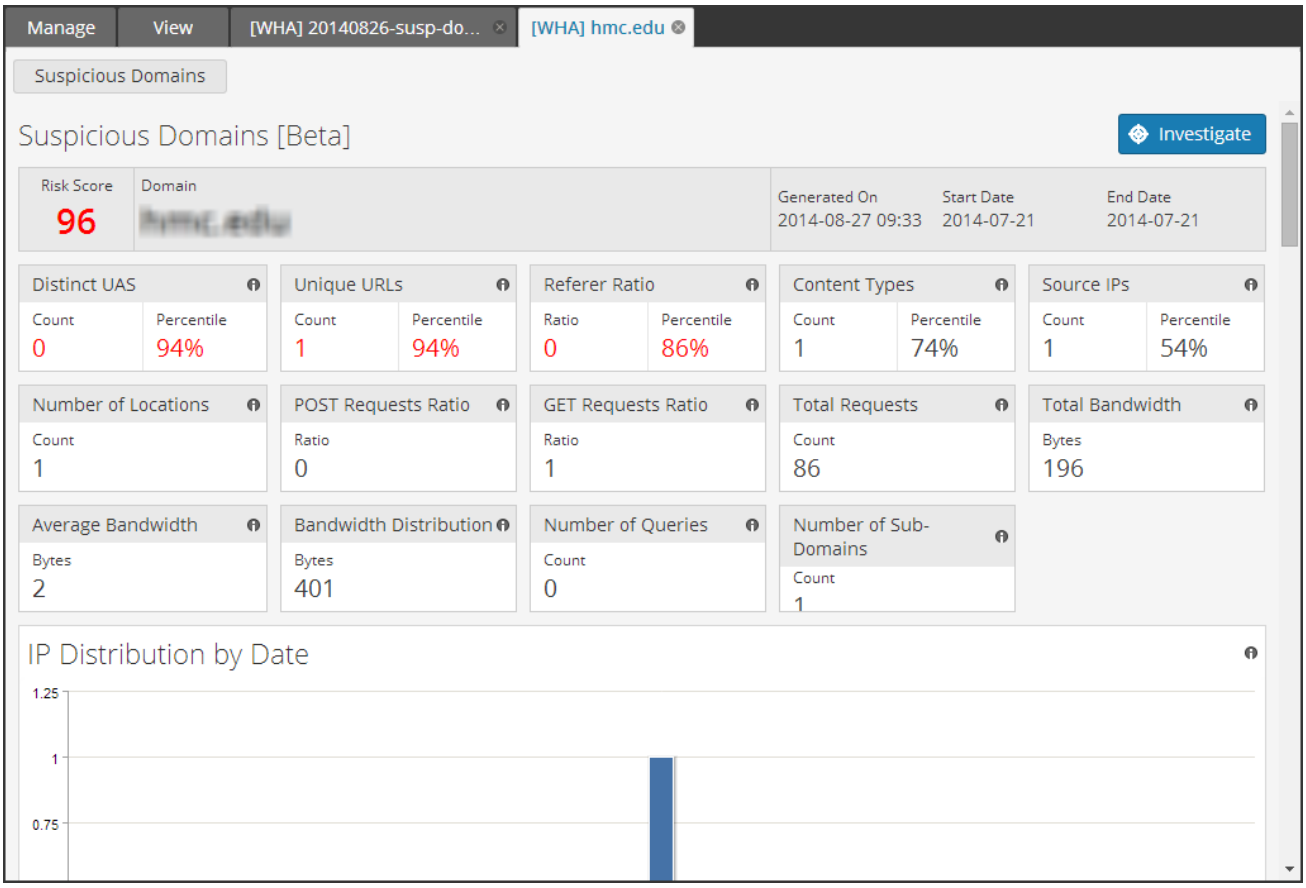
Topics

Analyze a Suspicious Domains Report

This topic describes the Suspicious Domain report. The following figure shows the Suspicious Domains report that lists all the potential suspicious domains and the risk score for each.



The following figure shows the different panels in this view.



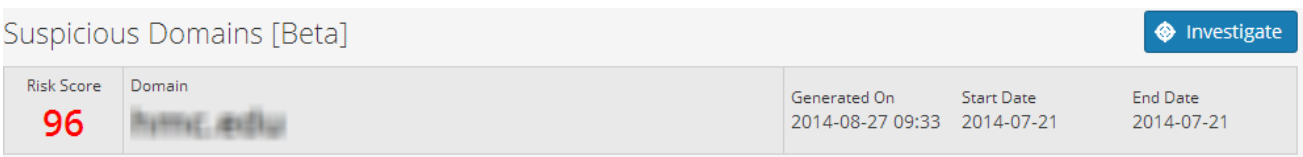
The Suspicious Domains report has the following panels:

1. Domain Heading
2. Domain Fields
3. Domain Histograms
4. Domain Lists

Domain Heading Panel

The Domain Heading panel allows you to view the risk score, domain name (example, hmc.edu), time the report is generated, along with the start and end date when the report is executed.

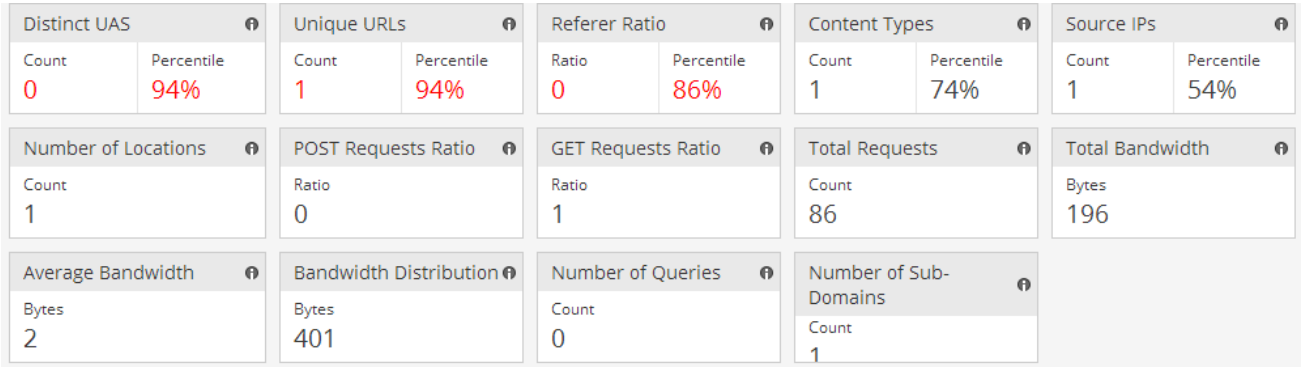
Note: If the risk score is greater than or equal to 50, the color coding is red else the color coding is green.



Domain Fields Panel

The Domain Fields panel displays the following fields from the Mongo DB database.

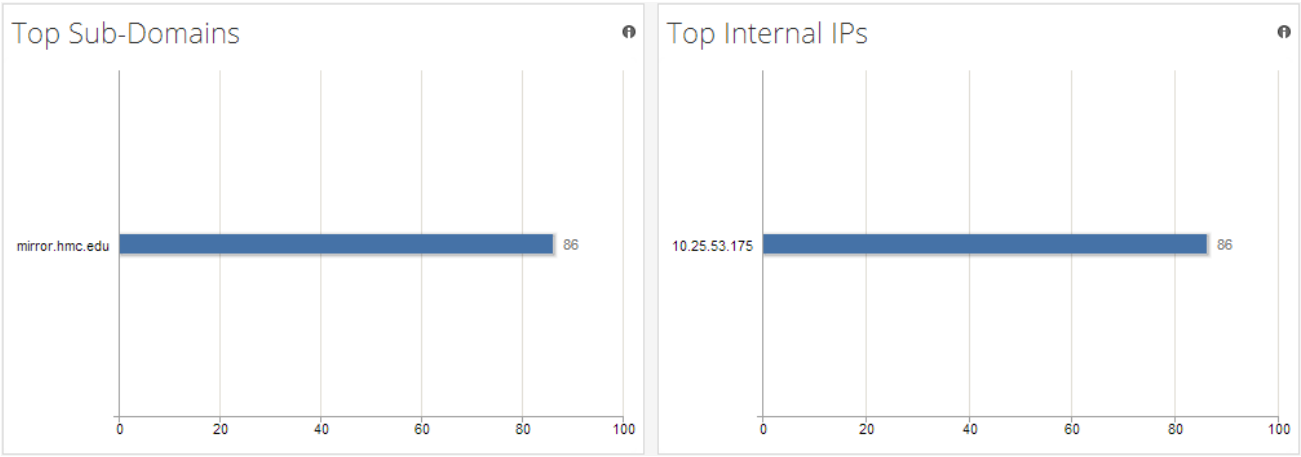
Note: The values for the fields are based on the selected suspicious domain. All the fields are populated with values at run time.



Domain Histograms Panel

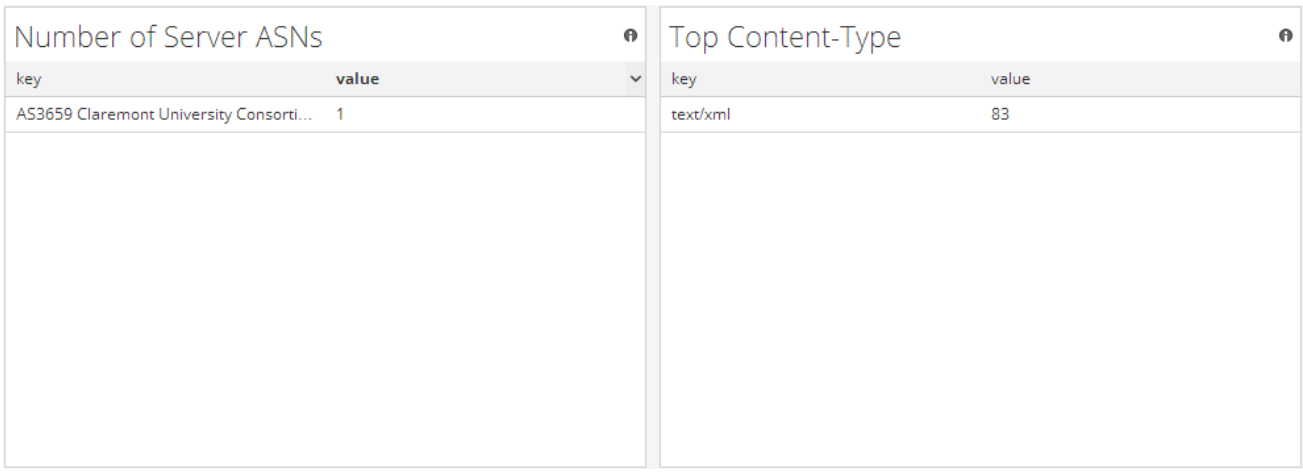
The Domain Histograms panel displays the Vertical Histogram which depicts the suspicious sub domains or internal IP addresses in dark blue color.

Vertical Histogram



Domain List Panel

The Domain List panel lists the number of server Autonomous System Number (ASN) and top content types.



View the Suspicious Domains Report

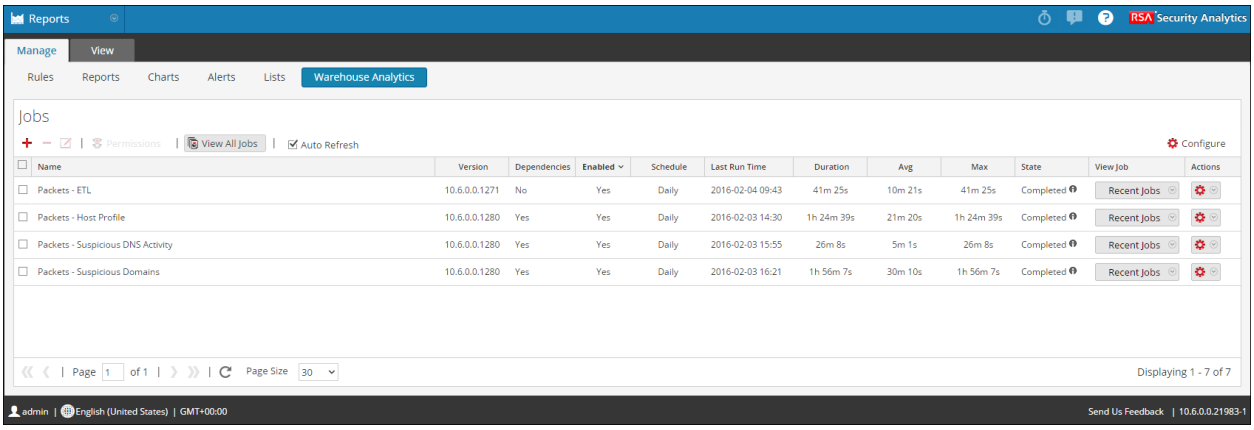
Perform the following steps to view the suspicious domains report:

1. In the Security Analytics menu, click **Reports**.

   The Manage tab is displayed.

2. Click **Warehouse Analytics**.

   The Warehouse Analytics view is displayed.



3. In the Warehouse Analytics toolbar, click **View All Jobs**.

   A list of jobs along with their schedule name and time are displayed on the View tab.

   Note: If no list is displayed, select a date from the calendar to view a list of jobs.

4. Double-click on an execution based on the Suspicious Domain.

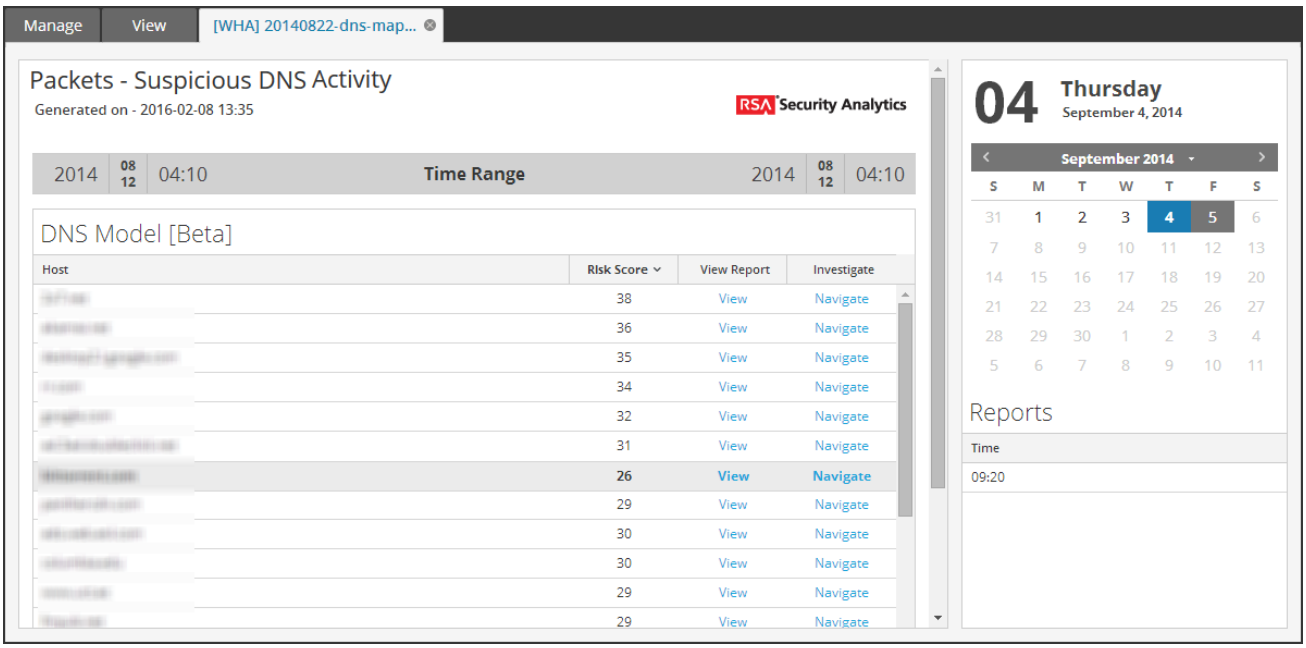
   The Suspicious Domains report is displayed.

Next steps

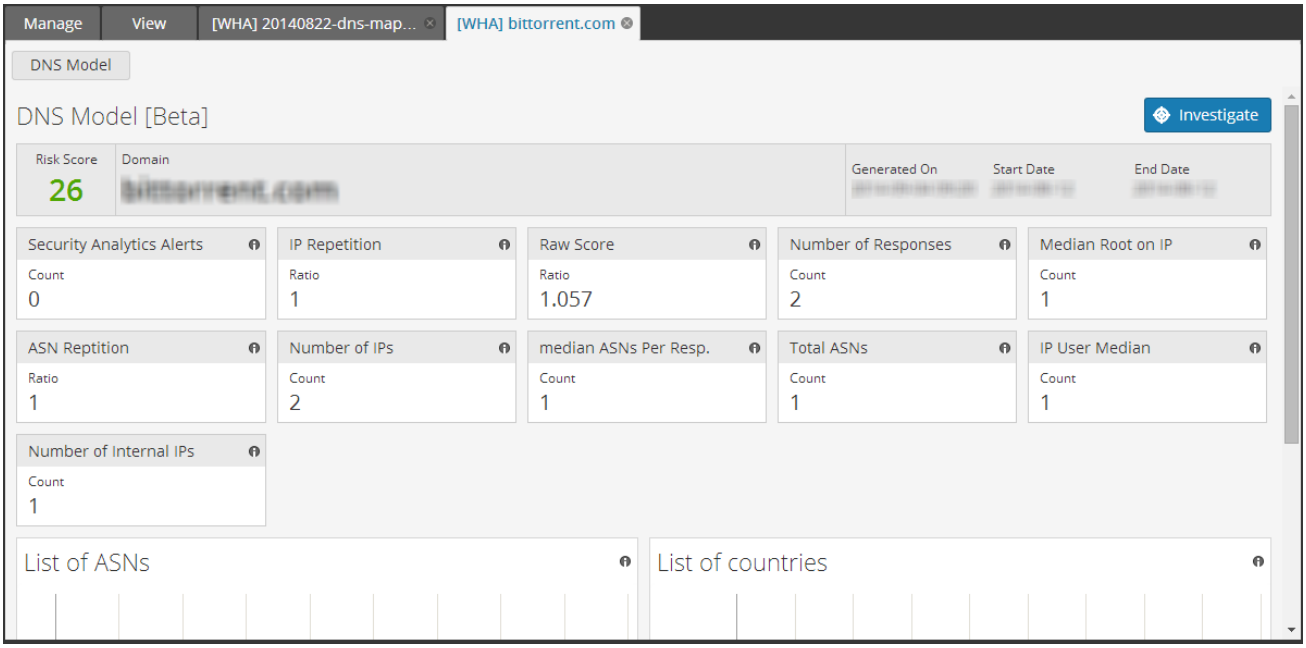
Perform the following task: Click the **Navigate** button to investigate a suspicious domain.

Analyze a Suspicious DNS Activity Report

This topic describes the Suspicious DNS Activity report. The following figure shows the Suspicious DNS Activity report listing all the suspicious domains and the risk score for each.



The following figure shows the different panels in this view.



Context

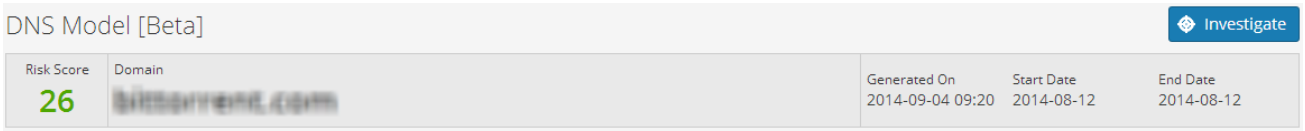
The Suspicious DNS Activity report has the following panels:

- Domain Heading
- Domain Fields
- Domain Histograms

Domain Heading Panel

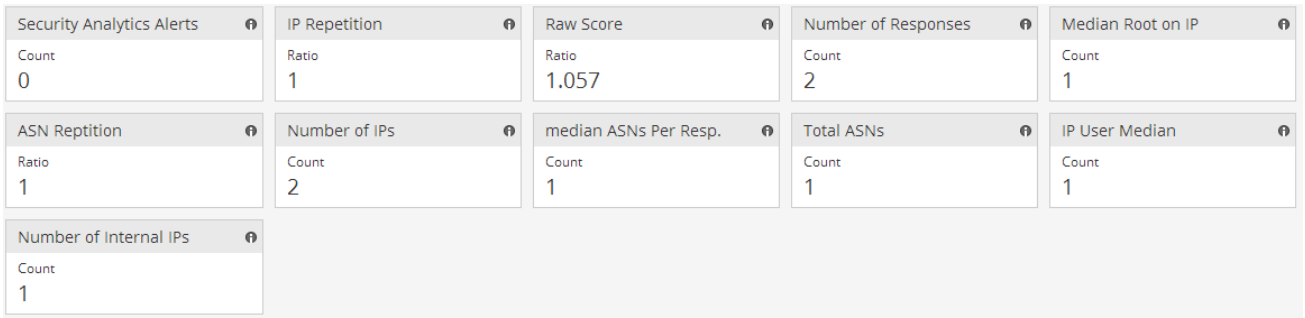
The Domain Heading panel allows you to view the risk score, domain name (example, bitminter.com), the time the report is generated, along with the start and end date when the report is executed.

Note: If the risk score is greater than or equal to 50, the color coding is red, else is green.



Domain Fields Panel

The Domain Fields panel displays the following fields from the Mongo DB database.



Note: All the fields populated in the Domain Fields panel, have values displayed based on run time.

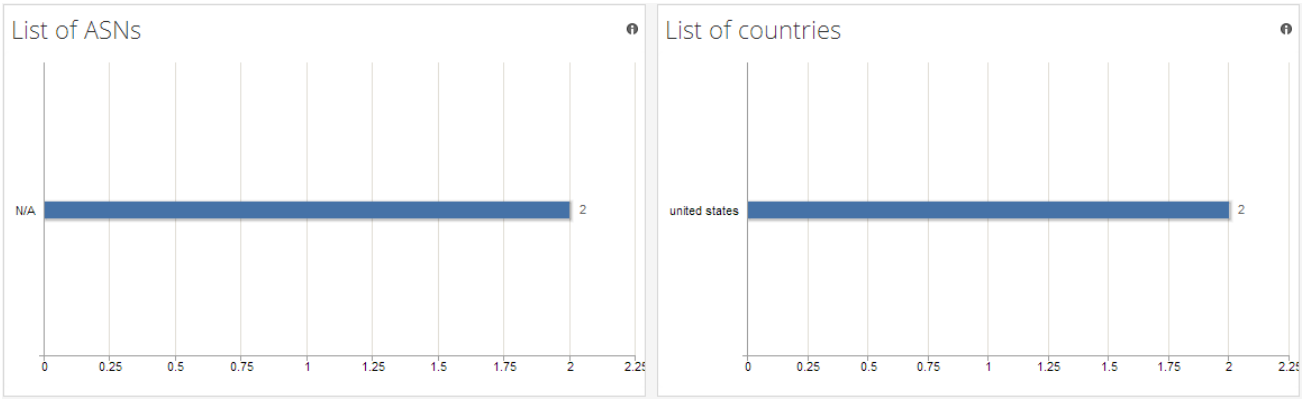
Field	Description
Security Analytics Alerts	The number of Security Analytics alerts per response.
IP Repetition	The number of distinct pairs for the IP and date divided by the overall number of IPs in the domain.

Field	Description
Raw Score	The raw score.
Number of Responses	The number of DNS responses (with the requests ignored).
Median Root on IP	The median of the number of distinct roots per returned IP.
ASN Repetition	The percentage of ASNs that is seen daily from the total IPs seen on the domain.
Number of IPs	The overall number of IPs.
Median ASNs per Resp.	The Median of number of ASNs per response.
Total ASNs	The overall number of ASNs.
IP User Median	The Median of internal IPs over domain IPs.
Number of Internal IPs	The number of source IP addresses from which the domain was addressed.

Domain Histograms Panel

The Domain Histograms panel displays the Vertical Histogram which depicts the suspicious ASNs or countries in dark blue color.

Vertical Histogram



View a Suspicious DNS Activity Report

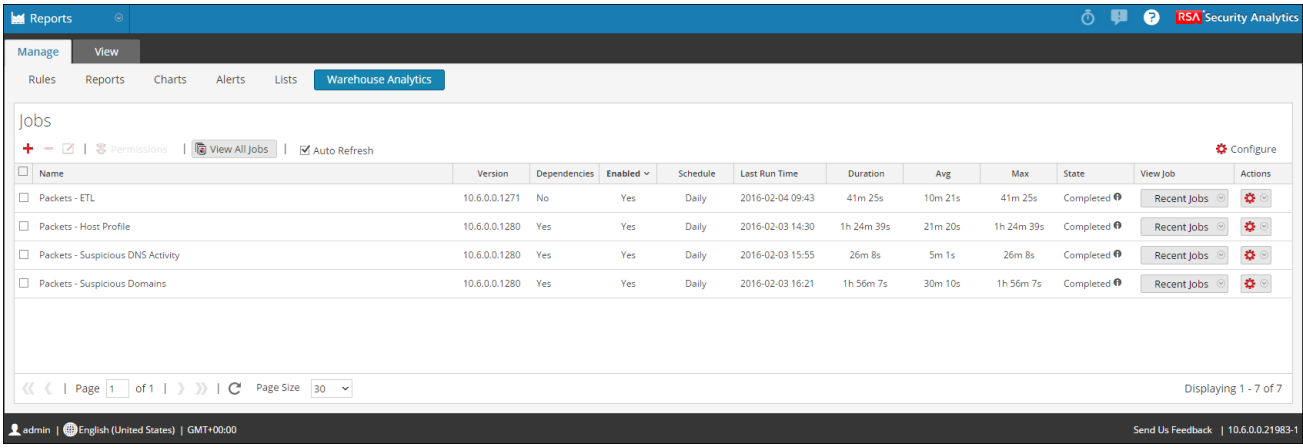
To view a Suspicious DNS Activity report:

1. In the Security Analytics menu, click **Reports**.

   The Manage tab is displayed.

2. Click **Warehouse Analytics**.

   The Warehouse Analytics view is displayed.



3. In the Warehouse Analytics toolbar, click **View All Jobs**.

   A list of jobs along with their schedule name and time is displayed on the View tab.

   Note: If no list is displayed, select a date from the calendar to view a list of jobs.

4. Double-click on an execution based on the Suspicious DNS Activity.

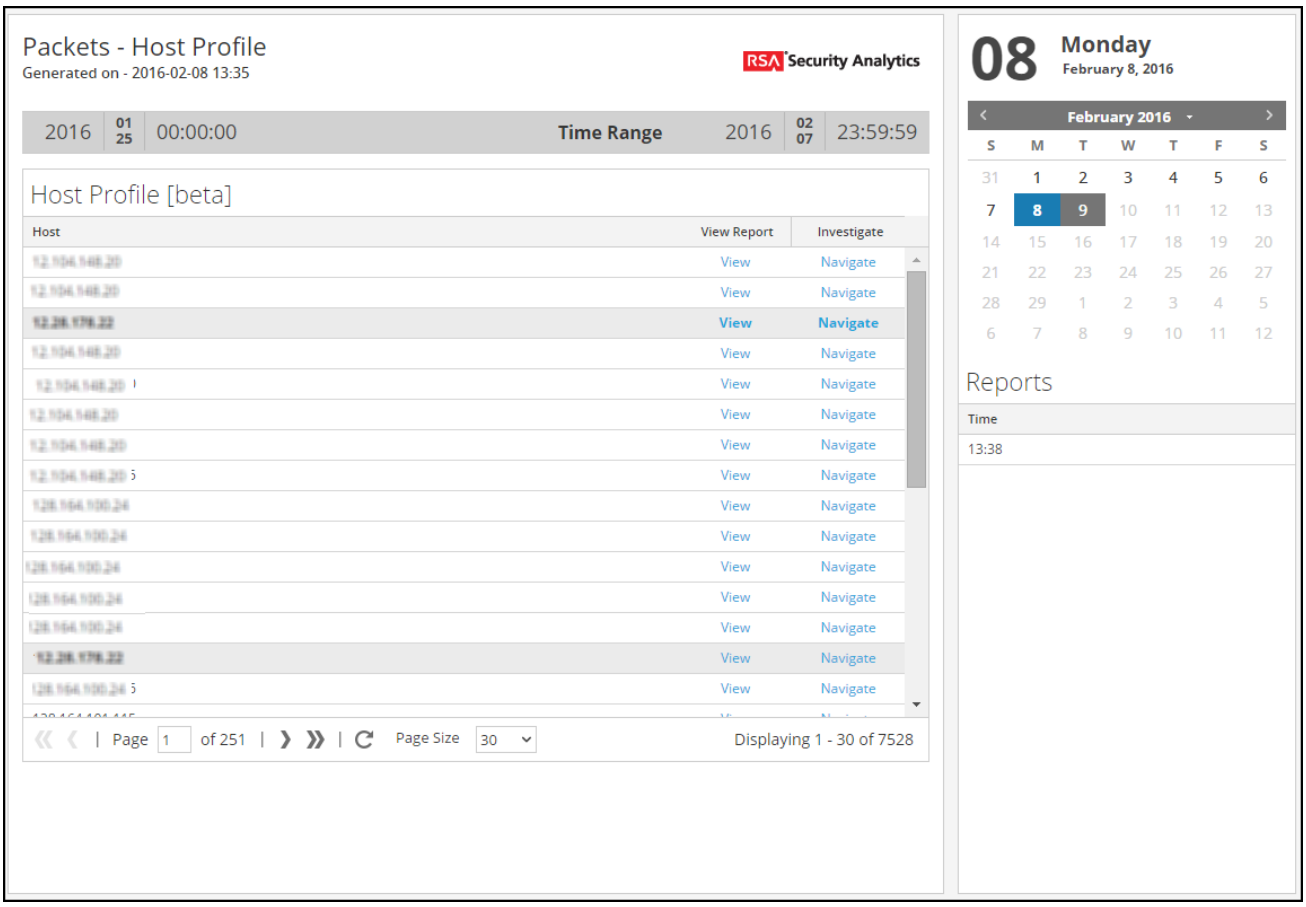
   The Suspicious DNS Activity report for the domain is displayed.

Next steps

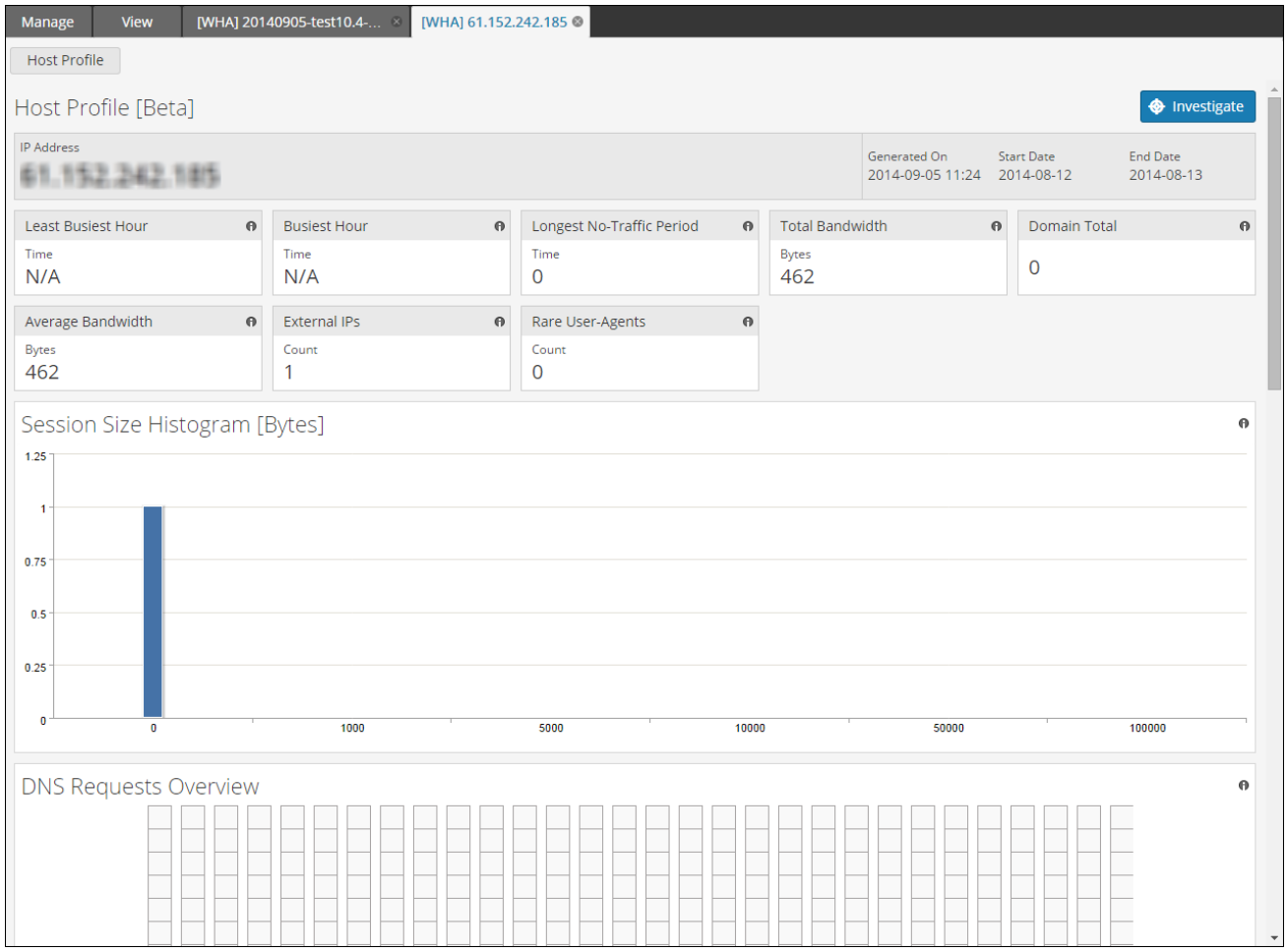
Perform the following task: Click the **Investigate** button to review the Suspicious DNS Activity.

Analyze a Host Profile Report

This topic describes the Host Profile report. The following figure shows the Host Profile report, listing all the suspicious hosts.



The following figure shows the different panels of this view.

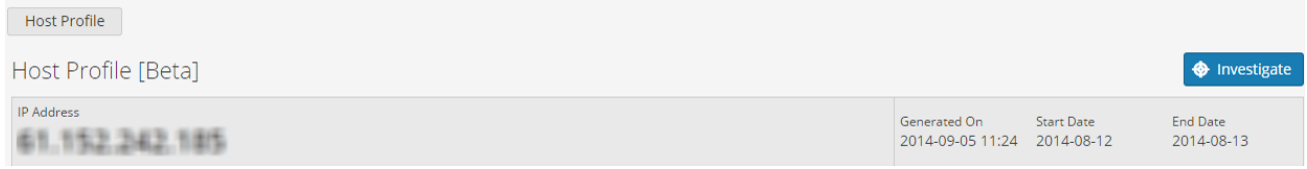


The Host Profile Report has the following panels:

- Activity Heading
- Activity Fields
- Activity Histograms
- Activity Heat Maps
- Activity List

Activity Heading Panel

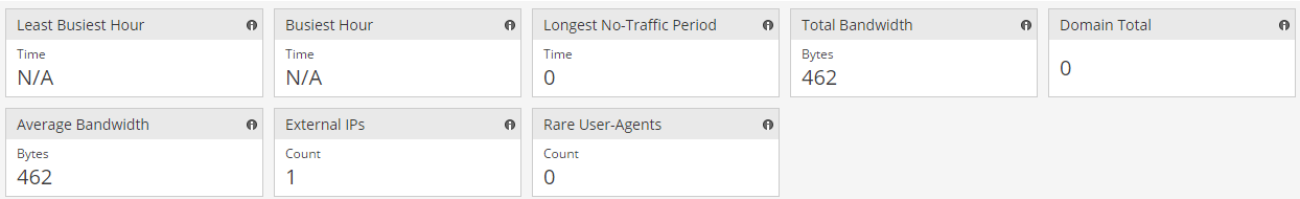
On the Activity Heading panel allows you can view the activity name, IP address, the time the report was generated, along with the start and end date.



Note: The Host Profile report does not display a score in the Activity heading panel.

Activity Fields Panel

The Activity Fields panel displays the following fields from the Mongo DB database.



Field	Description
Least Busiest Hour	The hour with the lower number of requests.
Busiest Hour	The hour with the highest number of requests.
Longest No-traffic Period (hours)	The longest break without any traffic for this IP.
Total Bandwidth	The total bandwidth consumed for sending and receiving.
Domain Total	The total number of domains accessed by this IP.
Average Bandwidth	The average bandwidth to send or receive per session.
External IPs	The number of external IPs accessed.
Rare User-Agents	The number of rare User-Agent strings seen from this IP.

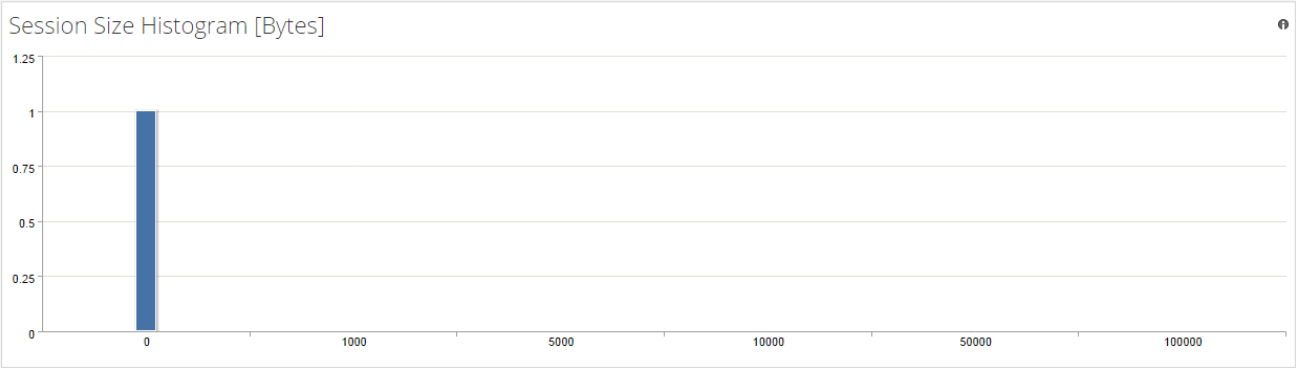
Activity Histograms Panel

The Activity Histograms panel displays the Session Size Histogram. This is a vertical histogram which depicts the host activity in blue color.

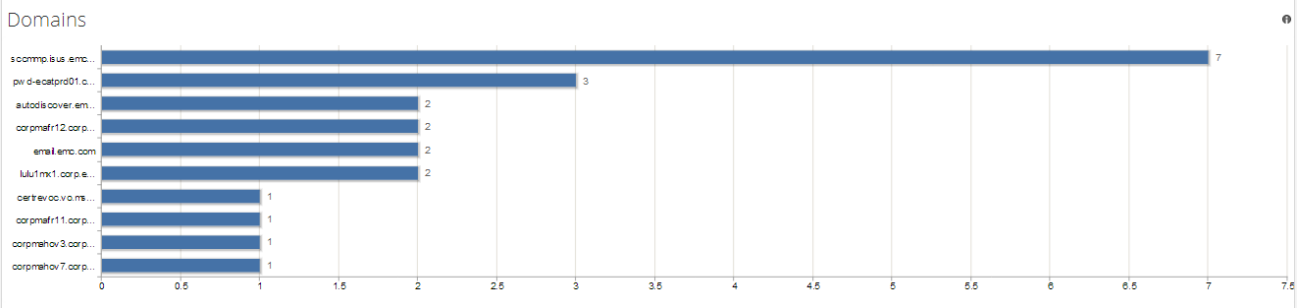
There are two types of histograms:

- Vertical Histogram: The data is depicted in the form of a vertical histogram in case of an Hours or Session Size Histogram.
- Horizontal Histogram: The data is depicted in the form of an horizontal histogram in case of Domains Histogram.

Vertical Histogram



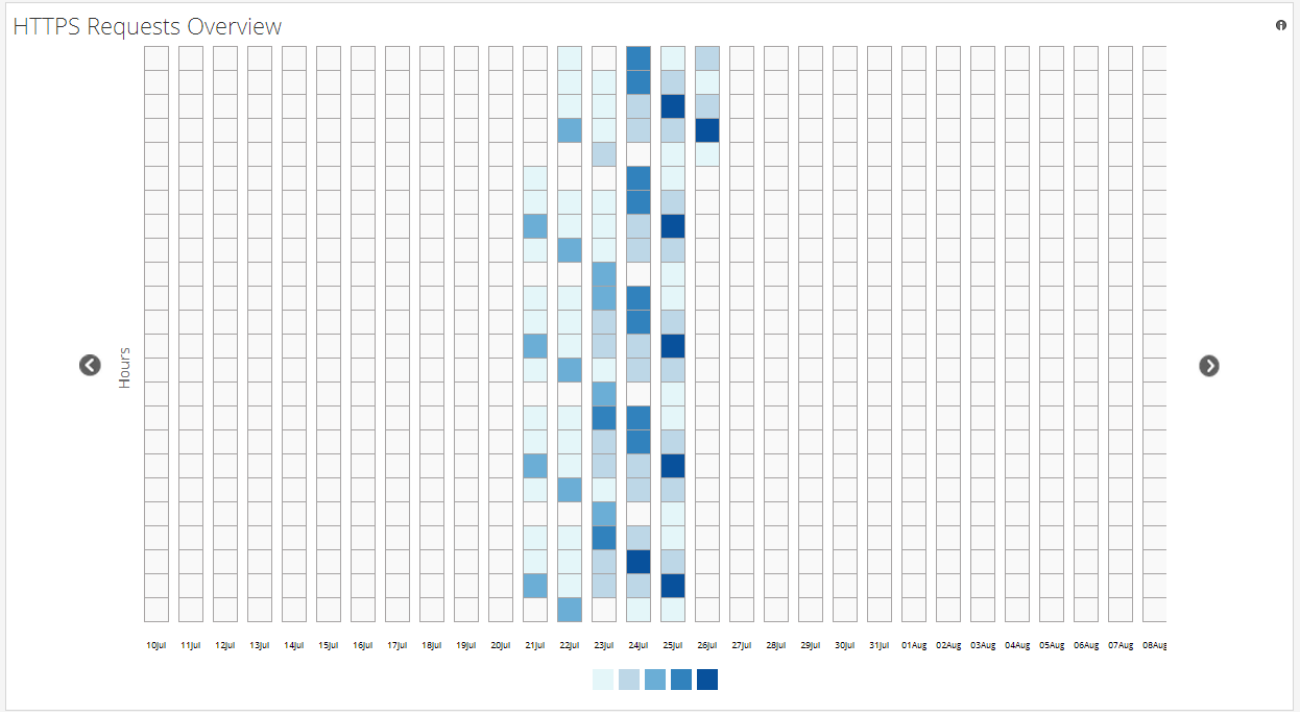
Horizontal Histogram



Activity Heat Maps Panel

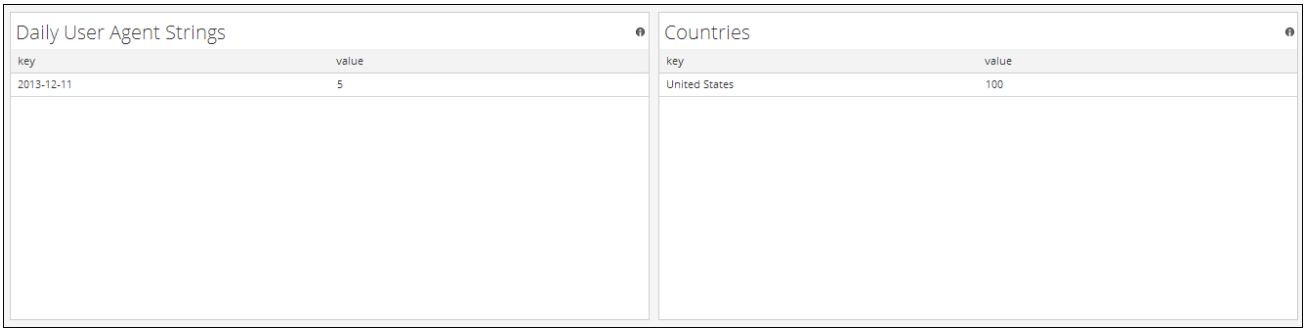
The Activity Heat Maps panel displays the HTTPS Requests Overview heat map. The heat map is plotted based on days (X-axis) and hours (Y-axis). The count of the activities is computed based on the average of several activities. The color codes displayed for the activities vary as it is dynamic. The heat map is displayed from the start date of the report which is displayed above the Heading panel. For example, on a particular day on the 23rd hour if the activity is high then the dark blue color code is displayed on the heat map.

Note: The high rate of activities during a particular period is not indicative of suspicious activity on the host. The color codes only depict the rate of activities during any period.



Activity List Panel

The Activity List panel is displayed based on the percentage of traffic on the field it accessed. For example, Daily User Agent Settings and Countries.



View a Host Profile Report

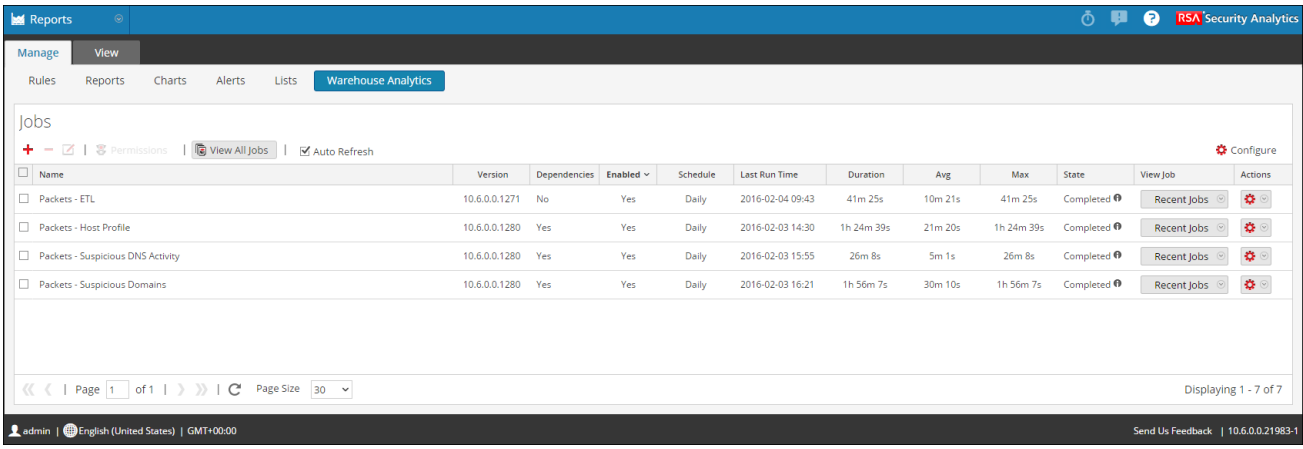
To view a host profile report:

1. In the Security Analytics menu, click **Reports**.

   The Manage tab is displayed.

2. Click **Warehouse Analytics**.

   The Warehouse Analytics view is displayed.



3. In the Warehouse Analytics toolbar, click **View All Jobs**.

   A list of jobs along with their schedule name and time are displayed on the View tab.

   Note: If no list is displayed, select a date from the calendar to view a list of jobs.

   Double-click on an execution based on the Host Profile model.

   The Host Profile report is displayed.

Next steps

You can investigate a host profile report.

Step 5. Investigate a Warehouse Analytics Report

This topic provides instructions on how to investigate from a Warehouse Analytics report. You can investigate from a Warehouse Analytics report by directly navigating to the Investigation module from the report. You can do the following to investigate from the report or details in the report:

- Use the Navigate option on the View Job view to investigate the job.
- Use the Investigate option to investigate the domain or activity.

Prerequisites

Make sure that:

- You understand the components of the Warehouse Analytics view. For more information, see Warehouse Analytics View.
- You understand the components of the View All Jobs. For more information, see View All Jobs Panel.

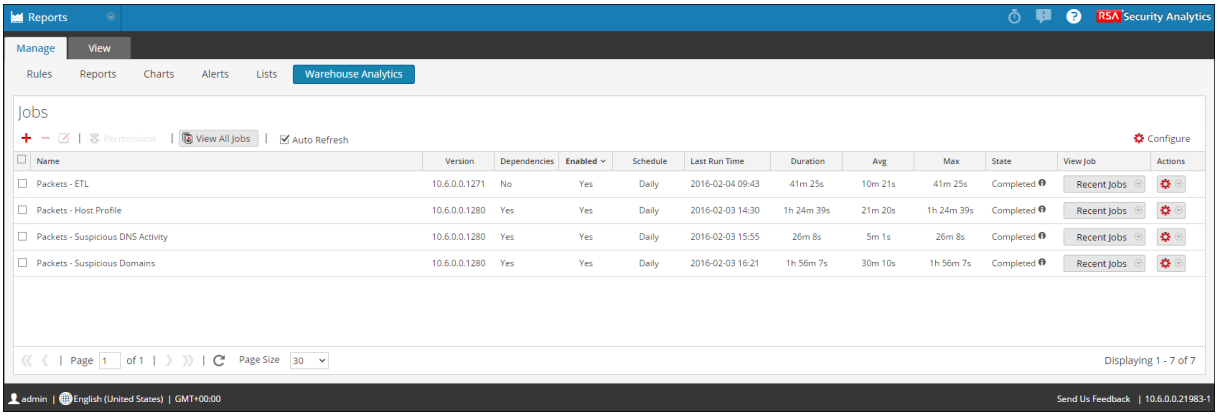
Investigate a Warehouse Analytics Report

To investigate from a Warehouse Analytics report:

1. In the Security Analytics menu, click **Reports**.

   The Manage tab is displayed.

2. Click **Warehouse Analytics**.
   The Warehouse Analytics view is displayed.

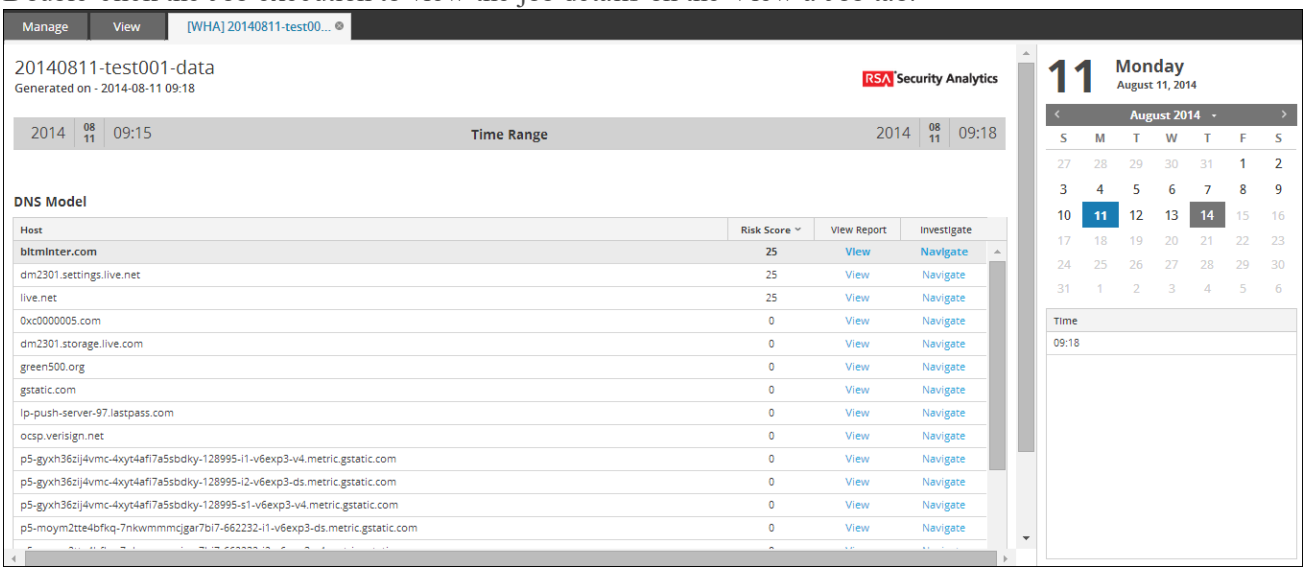


3. In the Warehouse Analytics toolbar, click **View All Jobs**.

   The View All Jobs tab is displayed.

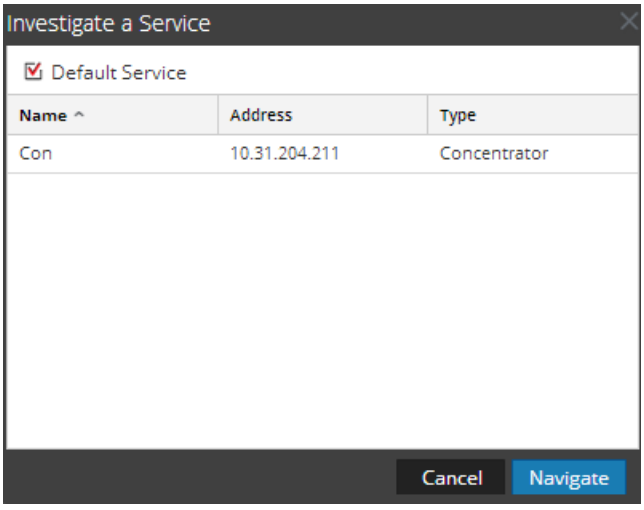
Note: If no jobs are displayed in the View All Jobs, select a date for which you want to display the jobs.

4. Double-click the Job execution to view the job details on the View a Job tab.



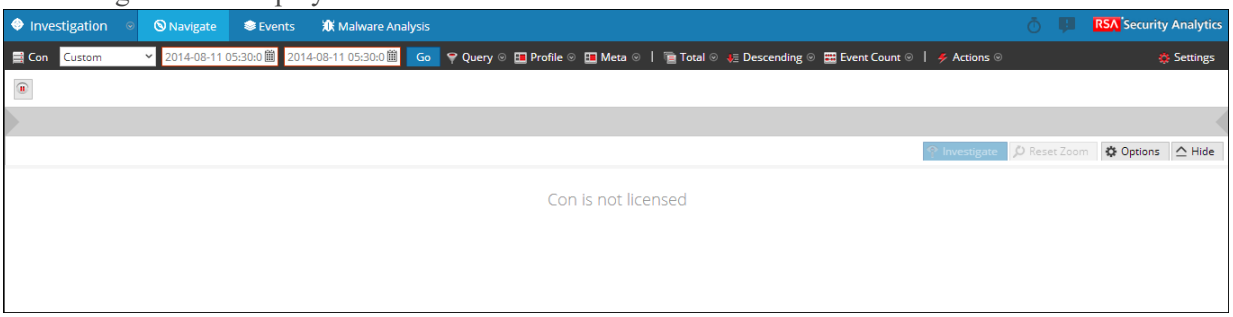
5. From the Investigate column, click **Navigate**.

   The Investigate a Service dialog box is displayed.



6. Select the concentrator service.
7. Click **Navigate**.

The Navigate UI is displayed.



8. Select a data point on the navigate UI.
9. Click **Investigate** to view it in the Investigation module.

Next steps

You can change the chart type and visualization.

Additional Procedures

This topic is a set of additional procedures for Warehouse Analytics. These procedures are for certain cases that are not part of the required procedures to use Warehouse Analytics, and they are presented in alphabetical order.

Topics

Delete a Warehouse Analytics Job

This section provides instructions on how to delete Warehouse Analytics jobs.

Prerequisites

Make sure you have understood the components of the Job Definition view. For more information, see Job Definition View.

Delete a Warehouse Analytics Job

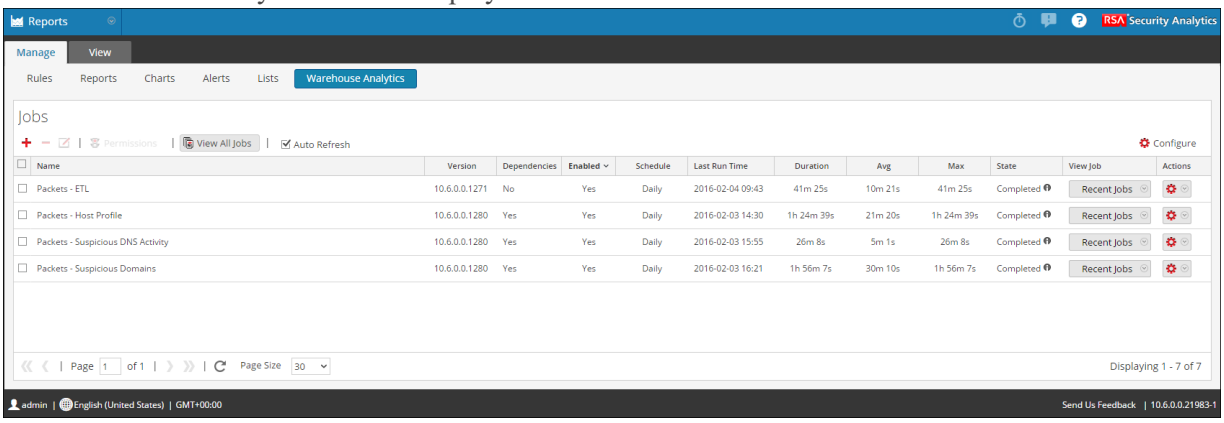
Note: ETL jobs cannot be edited or deleted.

To delete Warehouse Analytics jobs:

1. In the Security Analytics menu, click **Reports**.

   The Manage tab is displayed.

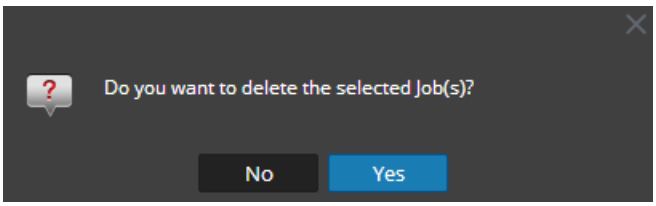
2. Click **Warehouse Analytics**.
   The Warehouse Analytics view is displayed.



3. In the Warehouse Analytics list panel, do one of the following:

   - Select the jobs and click .
   - Hover the mouse on a job and click > **Delete**.

A confirmation dialog is displayed.



4. Click **Yes** to delete the job.

   A confirmation message that the job is deleted successfully is displayed.

Edit a Warehouse Analytics Job

This topic provides instructions on how to edit a Warehouse Analytics job.

Prerequisites

Make sure that:

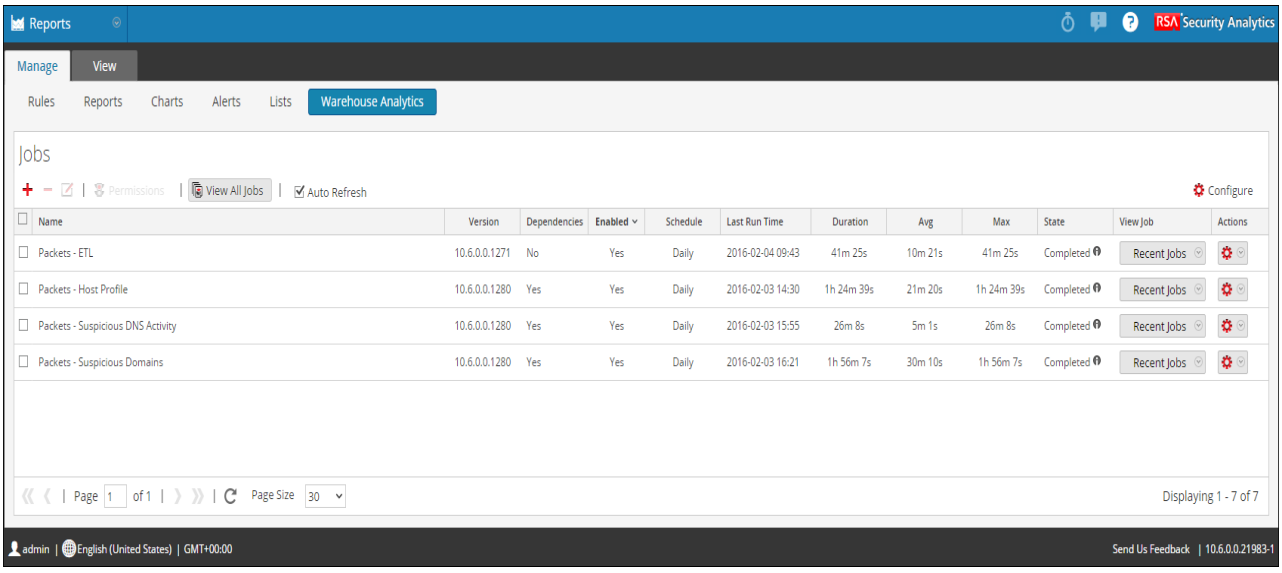
- You understand the components of the Warehouse Analytics view. For more information, see Warehouse Analytics View.
- You understand the components of the Job Definition view. For more information, see Job Definition View

Procedure

Perform the following steps to edit a Warehouse Analytics job:

Note: ETL job names are Read-only and cannot be edited.

1. Click **Warehouse Analytics**.
   The Warehouse Analytics view is displayed.



2. In the Warehouse Analytics list panel, select a job and click  .
   The **Job Builder** screen is displayed.
3. (Optional) Modify the job **Name**.

4. (Optional) From the **Warehouse** drop down, select the data source created on the Reporting Engine configuration page. (For example, Pivotal or MapR).
5. From the **On** drop down, select the type of run schedule (Past or Range), for that time range.

Note: While scheduling a job, if you select **Past** option or **Range (specific)** option close to the current time, you must ensure that the aggregate data in the data source is returned. If there is an aggregation delay in the data source, the end time you choose must account for the delay, otherwise jobs lose non-aggregated data for that time range.

(Optional) In the **Advanced Options** field, do the following:

a. In the **Model Params** field, enter a column name and select the column value from the List Selection window.

b. In the **HDFS Params** field, enter a column name and value.

c. In the **MapReduce Params** field, enter a column name and value.

d. In the **SandBox JVM Params** field, enter a column name and value.

Note: To run a Data Science (DS) job on Horton Works, you will be required to add the parameter "fs.DefaultFS" to the job. To add this parameter, add a JVM Parameter '-Dfs.defaultFS' in the Job Configuration, where the value for this parameter depends on the cluster configuration. For example, if you run the DS Jobs on an HDP Sandbox, the parameter value is defined as 'hdfs://sandbox.hortonworks.com'. This value is usually set by the Cluster Administrator.

e. Click **Save**.

A confirmation message that the job is saved successfully is displayed.

Enable or Disable a Scheduled Job

This topic provides instructions on how to enable or disable a scheduled Warehouse Analytics job.

Prerequisites

Make sure that you understand the components of the Warehouse Analytics view. For more information, see Warehouse Analytics View.

Enable or Disable a Scheduled Job

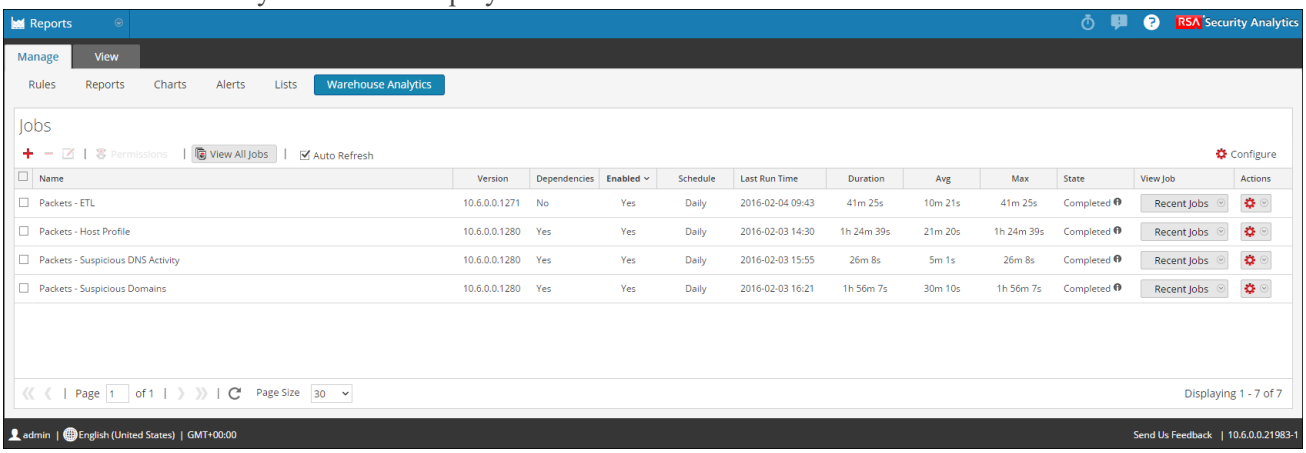
To enable or disable a scheduled job from the Warehouse Analytics List panel:

1. In the Security Analytics menu, click **Reports**.

   The Manage tab is displayed.

2. Click **Warehouse Analytics**.

   The Warehouse Analytics view is displayed.



3. In the Warehouse Analytics list panel, select a job and do either of the following:

   - Click  > **Enable**.

     The state of the job is changed to 'Running', if the report is scheduled to run immediately.

   - Click  > **Disable**.

     The state of the report is changed to 'Inactive'.

Refresh a Jobs List

This topic provides instructions on how to refresh a Warehouse Analytics jobs list.

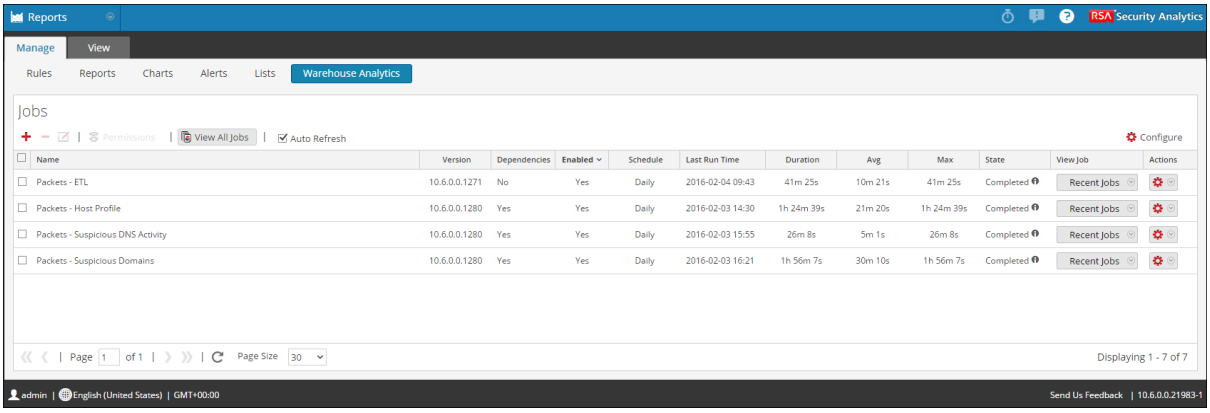
Prerequisites

Make sure you understand the components of the Warehouse Analytics view. For more information, see Warehouse Analytics View.

Procedure

Perform the following steps to refresh a jobs list:

1. In the Security Analytics menu, click **Reports.**
   The Manage tab is displayed.
2. Click **Warehouse Analytics**.
   The Warehouse Analytics view is displayed.



3. In the Warehouse Analytics List panel, drag and drop the jobs.
   The jobs are moved to the new location.
4. Do the following to refresh a jobs list:
   - In the Warehouse Analytics toolbar, select **Auto Refresh**.
     The jobs list is automatically refreshed.
   - In the Warehouse Analytics List panel, click .
     The jobs list is refreshed immediately.

Test a Warehouse Analytics Job

This topic provides instructions on how to test a Warehouse Analytics job.

Prerequisites

Make sure that:

- You understand the components of the Warehouse Analytics view. For more information, see Warehouse Analytics View.
- You understand the components of the Job Definition view. For more information, see Job Definition View.

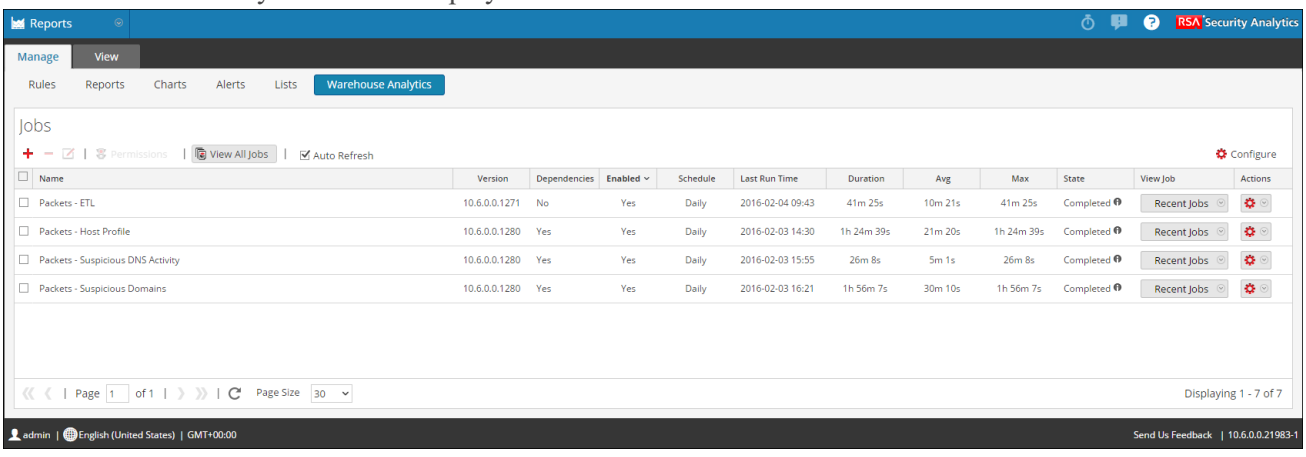
Test a Job

To test a job from the Warehouse Analytics list panel:

1. In the Security Analytics menu, click **Reports**.

   The Manage tab is displayed.

2. Click **Warehouse Analytics**.
   The Warehouse Analytics view is displayed.



3. In the Warehouse Analytics List Panel, select a job and click > **Test**.

   The Test Job Configuration page is displayed.

   Note: The **Name**field displays the name of the job being tested and is 'Read-only'.

4. (Optional) From the **Warehouse** drop down, select the data source created in the Reporting Engine configuration page. (For example, Pivotal or MapR).

5. From the **On** drop down, select the type of run schedule:
   - **Past -** Select the number of days.
   - **Range (specific) -** Select the date and time in the **From** and **To.**
   - **Past -** Select the number of days.
   - **Range (specific) -** Select the date and time in the **From** and **To.**
6. (Optional) In the **Advanced Options** field, do the following:
   a. In the **Model Params** field, enter a column name and select the column value from the List Selection window.
   b. In the **HDFS Params** field, enter a column name and value.
   c. In the **MapReduce Params** field, enter a column name and value.
   d. In the **SandBox JVM Params** field, enter a column name and value.
7. Click **Save**.

   A confirmation message that the job is successfully saved is displayed.

View All Jobs

This topic provides instructions on how to view a list of all Warehouse Analytics jobs.

Prerequisites

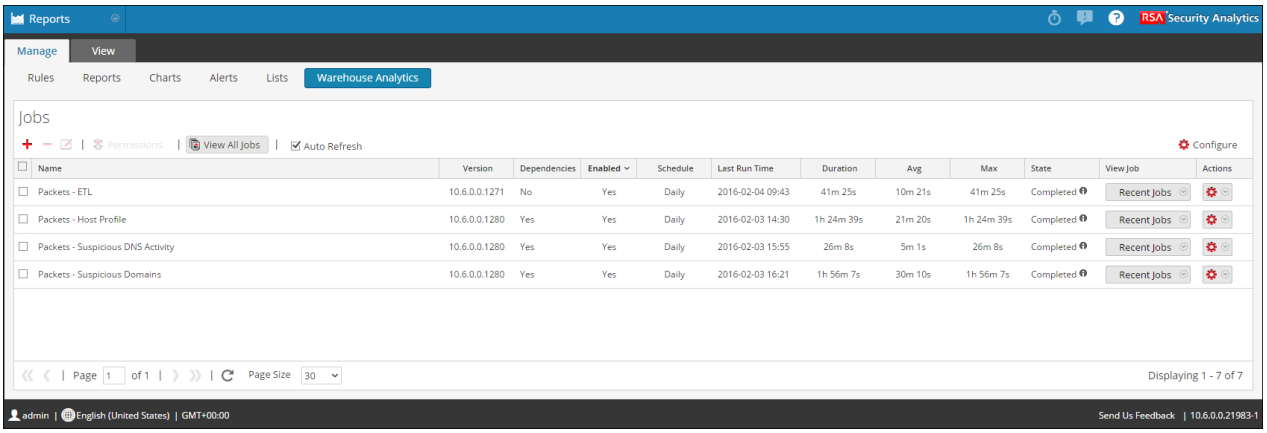
Make sure that:

- You understand the components of the Warehouse Analytics view. For more information, see Warehouse Analytics View.
- You understand the components of the View All Jobs. For more information, see View All Jobs Panel.

Procedure

Perform the following steps to view a list of all jobs:

1. In the Security Analytics menu, click **Reports.**
   The Manage tab is displayed.
2. Click **Warehouse Analytics**.
   The Warehouse Analytics view is displayed.



3. In the Warehouse Analytics toolbar, click **View All Jobs**.
   A list of jobs along with their schedule names and time is displayed on the View tab.

Note: If no list is shown, select a date from the calendar to view a list of jobs.

4. Double-click on an execution to view the job details in full screen.

Next Steps

Perform the following tasks:

1. You can view jobs in full screen.
2. You can select a date from the calendar to view a list of successfully run jobs for the chosen date.

View a Scheduled Job

This topic provides instructions on how to view a scheduled job consisting of a list of suspicious domains. By viewing a scheduled job you can understand the risk score, view a job report and investigate a scheduled job. If the scheduled job is in **Stop** or **Disable** state, you can start or enable the job.

Prerequisites

Make sure that:

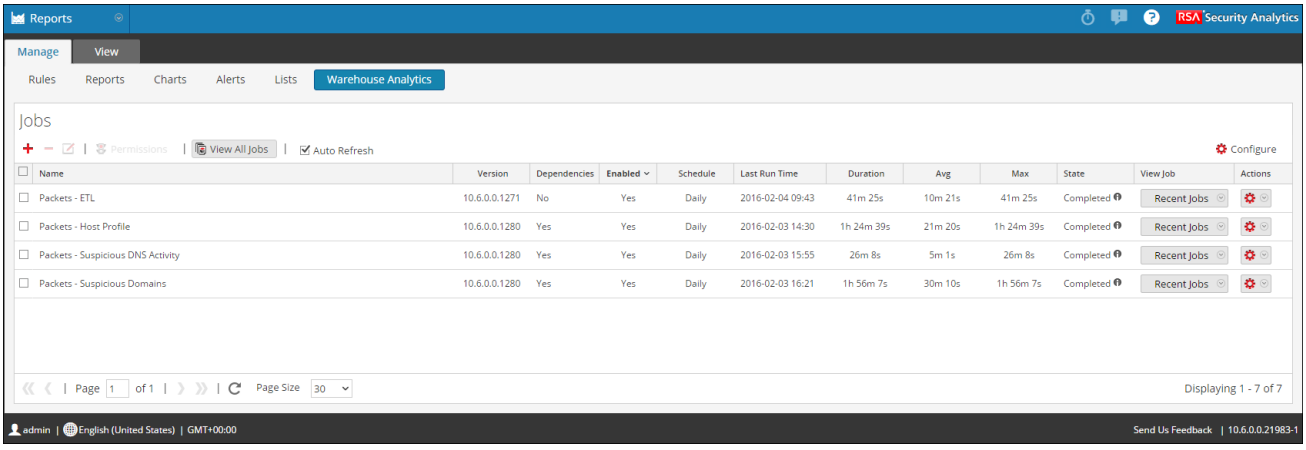
- You understand the components of the Warehouse Analytics view. For more information, see Warehouse Analytics View.
- You understand the components of the View Scheduled Job. For more information, see View a Scheduled Job Panel.

Procedure

Perform the following steps to view a scheduled job:

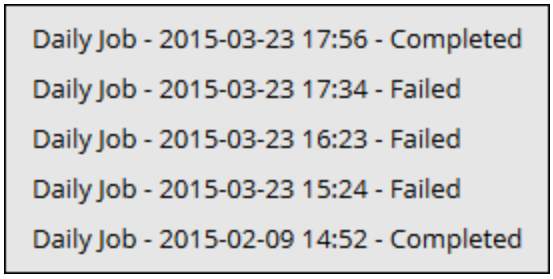
Note: ETL jobs do not have recent jobs list and hence no reports can be viewed.

1. Click **Warehouse Analytics**.
   The Warehouse Analytics view is displayed.



2. Select the job and in the **View Job** column, select **Recent Jobs**.

The list of recent jobs is displayed.



Next Steps

Perform the following tasks:

1. You can view the Warehouse Analytics report details on full screen.
2. You can investigate from a Warehouse Analytics report.
3. You can select a date from the calendar to view a list of successfully run jobs for the chosen date.

References

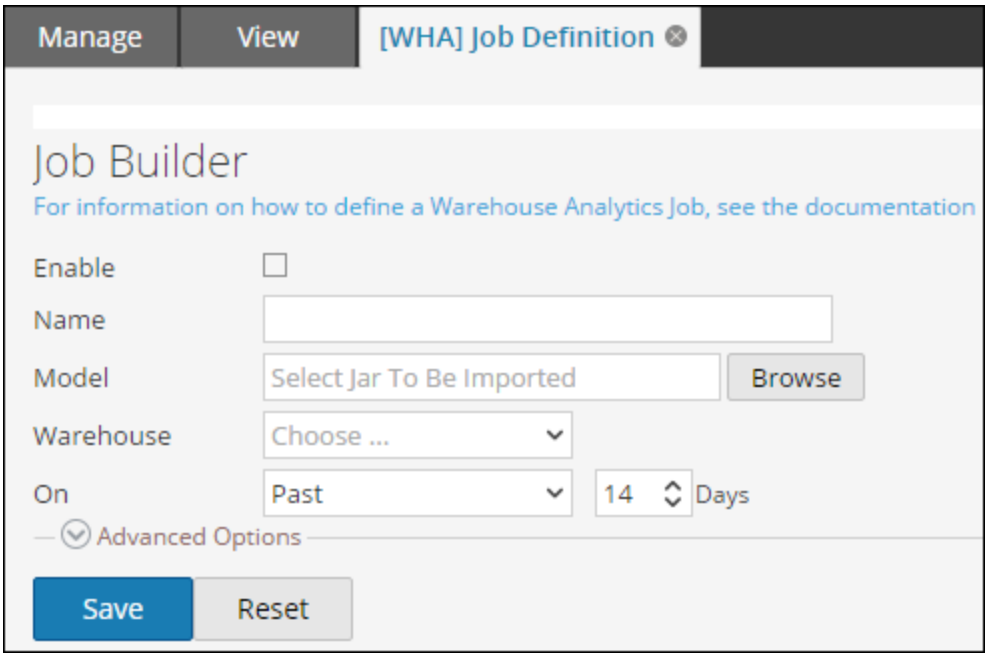
This topic is a collection of references that describe the Warehouse Analytics features.

Topics

Job Definition View

This topic describes the features and tasks of the Job Definition view. The Job Definition view allows you to create and manage new jobs.

The following figure shows the Job Definition view.

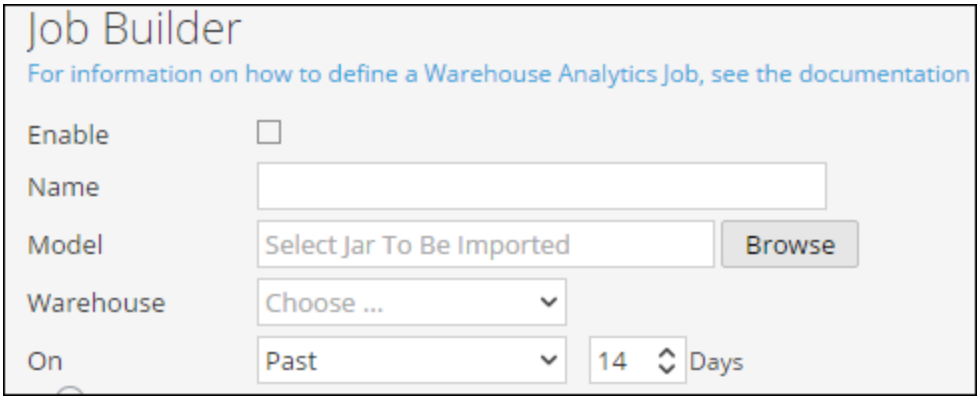


The Job Definition view consists of the following sections:

1. Job Definition
2. Advanced Options

Job Definition Panel

The Job Definition panel allows you to define and schedule Warehouse Analytics jobs.



The following table describes the fields on the Job Definition panel.

Field	Description
Enable	Enables the report schedules and runs the report.
Name	The unique name for the report.
Model	The name of the Data Science model or jar file to be imported. This option is visible only when you define a Job. **Note:** Depending on the model you select, the values are pre-populated in the Advanced Options panel.
Warehouse	The name of the Warehouse data source. (For example, MapR or Pivotal).
On	Past - Allows you to specify the number of days on which the query is run. Range Specific - Allows you to select a date range **From** and **To** for which the query is run.

Advanced Options Panel

The Advanced Options panel allows you to define or customize several parameters such as: Model, HDFS, MapR, Sandbox JVM of the Warehouse Analytics job.

The following table lists the fields in the Advanced Options panel.

Field	Description
Model Parameters	Warehouse Analytics model or job parameter. **Note:** Depending on the model selected, you get a list of white listed domains in the Model Parameters section. The domains are listed but with the score of **-1**. For instance, a domain by name *example.com*, does not appear in the list of suspicious domains.
Name	The name of the model parameter.
Value	The value of the model parameter.
	Displays the List Selection window. For more information, see Generate a List Panel topic in the *Reporting Guide*.
HDFS Parameters	HDFS config parameters.
Name	The name of the Hadoop Distributed File System (HDFS) parameter.
Value	The value of the HDFS parameter.
MapR Parameters	Hadoop or MapR configuration parameters.
Name	The name of the MapR parameter.
Value	The value of the MapR parameter.
Sandbox JVM Parameters	JVM parameters or system parameters for JVM executing the Warehouse Analytics model.
Name	The name of the Sandbox JVM parameter.
Value	The value of the Sandbox JVM parameter.
Save	Schedules the job.
Reset	Resets the scheduled job.

Live Resource View

The Live Resource View shows a detailed view of a selected resource, and has options to:

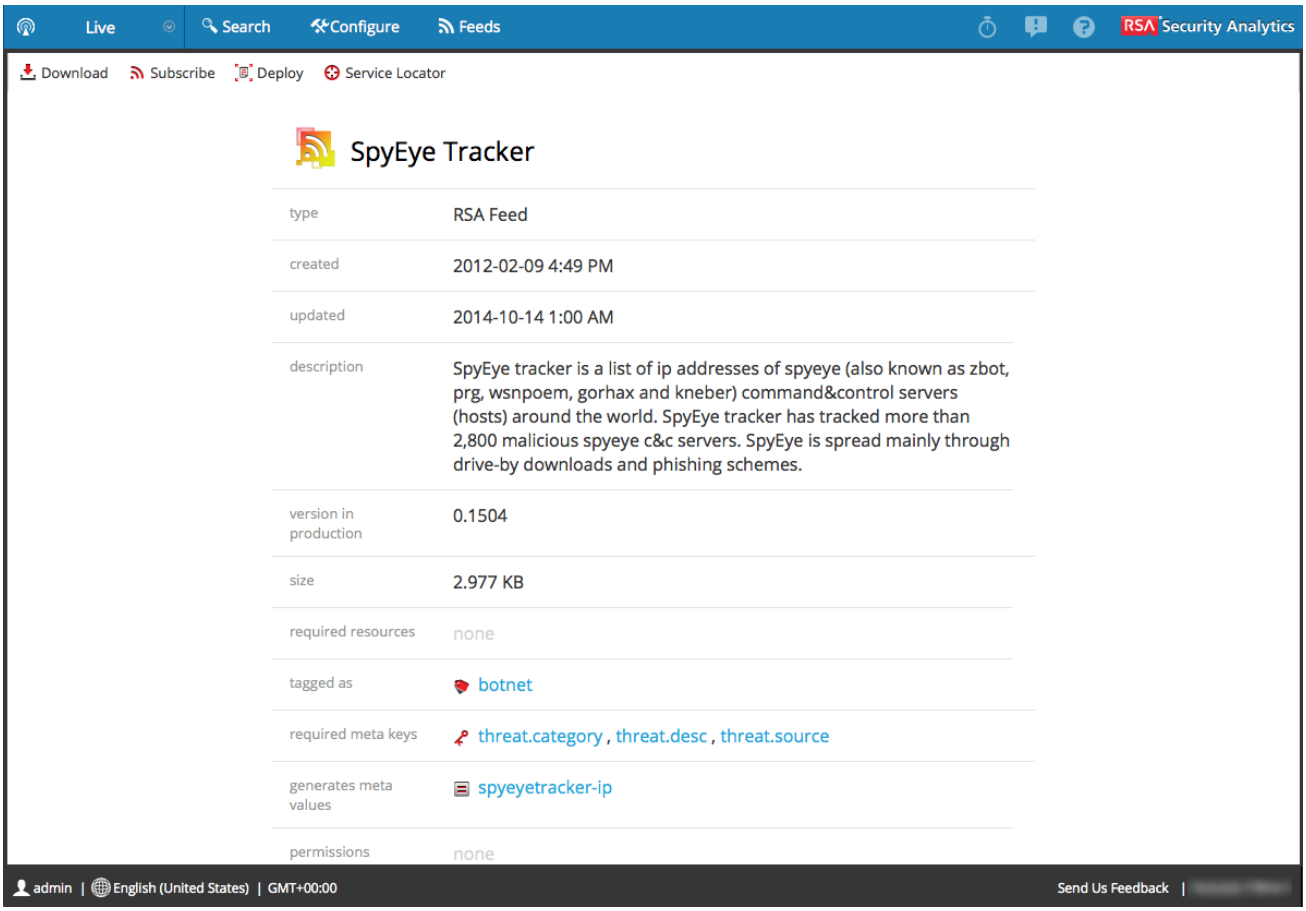
- Download the resource.
- Subscribe or unsubscribe the resource.
- Deploy the resource to services.
- Locate services on which the resource is deployed and remove the resource from services.

The required permission to access this view is View Live Resource Details.

To access this view, do one of the following:

1. In the **Security Analytics** menu, select **Live > Search > Resource Types.**
2. In the Live Search view, **Detailed Results**, click the resource type icon or the resource name.
3. In the Live Search view, **Grid Results**, double-click a resource or select a resource and click **Details**.

This is an example of the Resource view.



The Live Resource View has a detailed view of a single resource and a toolbar.

Resource Details

This is an example of the resource details displayed in the Resource View.

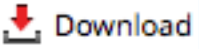
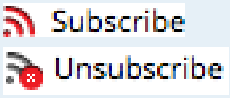
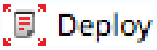
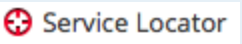
The following table describes the elements in the Resource Details section.

Feature	Description
Resource Type Icon	A graphic representation of the resource type, for example  .
Name	The name of the resource, for example, **fingerprint_office_lua**.

Feature	Description
Type	The type of resource, for example, **RSA Lua Parser**.
Created	The date the resource was created, for example, **2013-09-15 02:16 PM**.
Updated	The date the resource was last updated, for example, **2013-09-15 02:16 PM**
Description	The description of the resource, for example, **Identifies Microsoft Office 95, 2007 Word, Excel, and PowerPoint documents**.
Version in production	The version of the resource, for example, **0.1**.
Size	The size of the resource, for example, **9.079 KB**.
Required Resources	A list of resources on which this resource depends, for example, **NetWitness Lua Library**. Clicking a resource replaces the currently displayed details with the details of the one you clicked.
Tagged as	The tags that apply to the resource. In the example, the tag is **featured, informational**. Clicking a tag opens the Live Search View with the search narrowed to match resources with that tag.
Required Meta Keys	The meta keys that apply to the resource. In the example, there are no meta keys required. Clicking a meta key opens the Live Search View with the search narrowed to match resources with that meta key.
Generates Meta Values	The meta values that the resource generates. In the example, there are no meta values generated. Clicking a meta value opens the Live Search View with the search narrowed to match resources with that meta value.
Permissions	The permissions required for the resource.

Resource View Toolbar

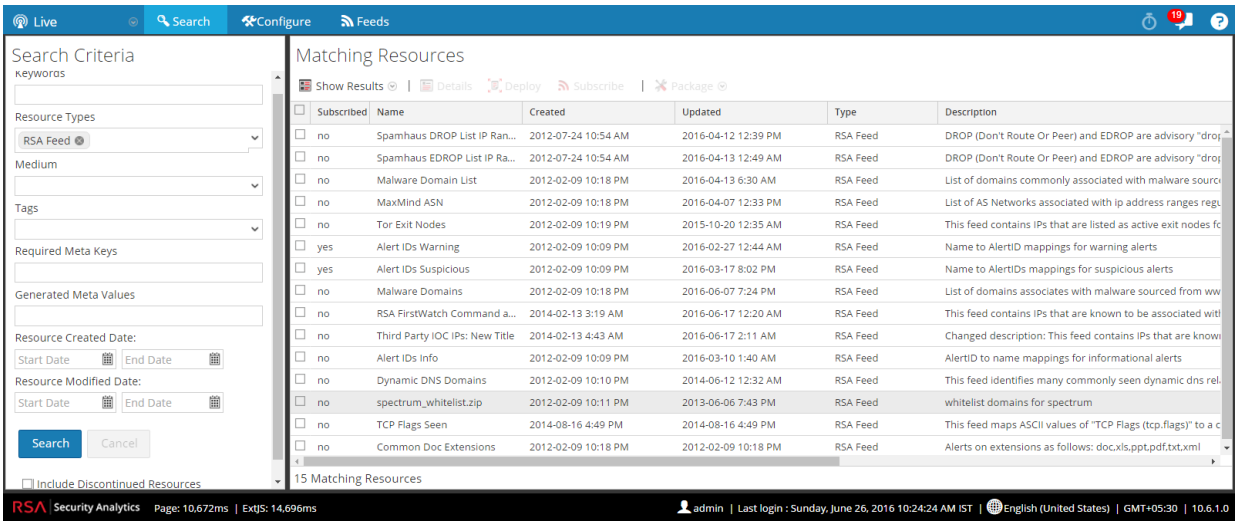
This table describes the Live Resource view toolbar options.

Feature	Icon	Description
Download		This option downloads the resource currently displayed in the Resource View.
Subscribe or Unsubscribe		This option subscribes to or unsubscribes from the resource currently displayed in the Resource View. • Clicking **Subscribe** opens a dialog notifying that you are agreeing to receive notification when the selected resources are updated. You can cancel or click **OK**. • Clicking **Unsubscribe** asks for confirmation that you want to stop receiving notification when the selected resources are updated. You can then choose to cancel or you can click **Unsubscribe** or **Unsubscribe and Remove**, which also removes the resource from services on which it is deployed.
Deploy		This option provides a way to deploy the resource currently displayed in the Resource View. Clicking **Deploy** opens the Manual Resource Deployment dialog.
Service Locator		This option displays a list of services on which the currently displayed resource is deployed. You can remove the resource from all services or selected services.

Live Search View

The Live Search view provides the ability to browse the configured Live CMS for resources. Once matching resources are found, you can view details, subscribe to resources, and deploy resources to services and service groups.

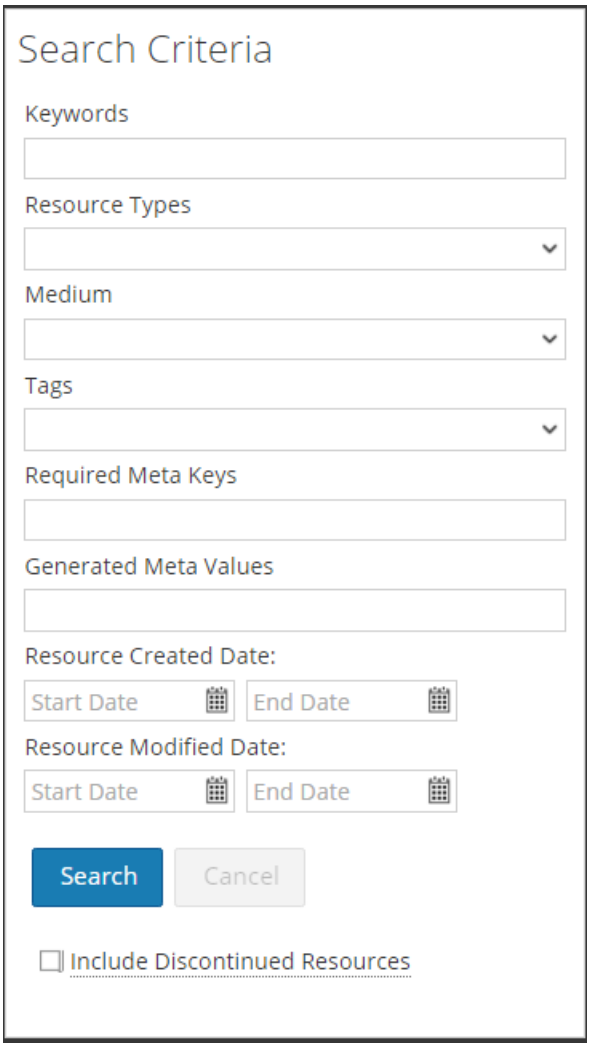
This is an example of the Search view.



The Live Search view has a panel for specifying search criteria and a panel that displays matching resources. The Search Criteria panel is collapsible to provide more width for viewing the Matching Resources panel.

Search Criteria Panel

This is an example of the Search Criteria panel.



The following table provides descriptions of the Search Criteria panel features.

Feature	Description
Keyword(s)	Enter a keyword or keywords to browse for resources that have the keyword in the resource name or the resource description. You can use wildcards when you enter a keyword.
Resource Types	Select resources types from the drop-down list to filter resources by type of resource, for example **RSA Correlation Rule** or **RSA Lua Parser**.

Feature	Description
Medium	Select one or more mediums from the drop-down list to search for content based on the meta data source. Available values for medium are as follows: • **log**: applied to content that uses meta derived from log data • **packet**: applied to content that uses meta derived from network packets • **log and packet**: applied to content that correlates meta derived across log and packet data Additionally, some resources receive data from either log or packet data: in this case, both mediums are listed (but without the **and**).
Tags	Select meta tags from the drop-down list to browse based on how the meta is tagged. For example, to browse resources for a Log Decoder, select the **netwitness for logs** tag. Alternatively, you can click a tag in the Matching Resources panel to insert that tag in this field. **Note:** When you search in Live, note that tags you enter are ORed. That is, if you search for **accounting** and **assurance**, all content that is tagged as either accounting *or* assurance is returned. For more details on the model used for tagging content, see the Investigation Model on RSA Link: https://community.rsa.com/docs/DOC-62313.
Required Meta Key(s)	Enter a specific meta key; for example, **threat.source**. Alternatively, you can click a meta key in the Matching Resources panel to insert that tag in this field.
Generated Meta Value (s)	Enter a generated meta value; for example, **netwitness**. Alternatively, you can click a generated meta key in the Matching Resources panel to insert that tag in this field.
Research Created Date	Specify a date range during which resources were created. For example, to browse resources that were created between January 1 and January 4, you select January 1 as the start date and January 4 as the end date. You must enter dates in mm/dd/yyyy format or you click and pick dates from a calendar.

Feature	Description
Research Modified Date	Specify a date range during which resources were modified. For example, to browse resources that were modified between January 1 and January 4, you select January 1 as the start date and January 4 as the end date. You must enter dates in mm/dd/yyyy format or you click and pick dates from a calendar.
Search	Click **Search** to send the search request to the Live server. More specific search criteria return matching resources more quickly.
Cancel	Click **Cancel** to cancel the search in progress.
Include Discontinued Resources	Check **Include Discontinued Resources** to include the discontinued resources in the search result.

Matching Resources Panel

The Matching Resources panel presents search results based on the selections made in the Search Criteria panel. Results are initially displayed in a grid, but you can switch between two Show Results options: Detailed or Grid.

Detailed Results

In the detailed results, you can click a tag, meta key, or resource meta value to auto fill the Search Criteria panel and pivot the search results.

The following table describes the elements in the detailed results.

Feature	Description
Resource Type Icon	A graphic representation of the resource type. For example 
Name	The name of the resource, for example, **Group Management**. **Note:** (Discontinued) is displayed next to the resource name if a resource is discontinued.
Type	The type of the resource, for example, **Rule**.

Feature	Description
Updated	The date the resource was last updated, for example, **2015-09-15 4:27 PM**.
Version	The version of the resource, for example, **0.1**.
Size	The size of the resource, for example, **153 B**.
Subscribed	Subscription status: • **yes**: This Security Analytics instance is subscribed to this content resource. • **no**: This Security Analytics instance has not subscribed to this content resource.
Description	The description of the resource, for example, **Compliance Rule-Group Management**.
Tags	The tags that apply to the resource. Clicking a tag narrows the search to resources with that tag. For example, featured, apt.
Meta Keys	The meta keys that apply to the resource. Clicking a meta key narrows the search to resources with that meta key. For example, threat.category, threat.desc, threat.source.
Resource Meta Values	The meta values generated by the resource. Clicking a meta value narrows the search to resources that generated the meta value. For example, netwitness.

Grid Results

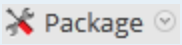
In the grid view, you can select one or more resources and use additional options in the toolbar to view the details of a single resource, subscribe to resources, and deploy resources.

The following table describes the elements in the grid results.

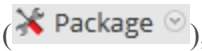
Feature	Description
	Grid

Feature	Description
Subscribed	Subscription status: • **yes**: This Security Analytics instance is subscribed to this content resource. • **no**: This Security Analytics instance has not subscribed to this content resource.
Name	The name of the resource, for example, **Group Management**. **Note:** The resource name is displayed in red color if it is discontinued.
Created	The date the resource was created, for example, **2015-08-12 3:11 PM**.
Updated	The date the resource was last updated, for example, **2015-09-15 4:27 PM**.
Type	The type of the resource, for example, **Rule**.
Discontinued	The status of the discontinued resources: **yes** - The resource that matches the search criteria is discontinued. **no** - The resource is not discontinued. **--** - The Live Server is not checked for the discontinued resources.
Description	The description of the resource, for example, **Compliance Rule-Group Management**.
	Toolbar
Show Results	This menu offers two ways to view search results: **Detailed** and **Grid**.
Details	This option applies to a single selected resource. Clicking **Details** opens the selected resource in the Live Resource view.
Deploy	This option applies to one or more selected resources.
Subscribe	This option applies to one or more selected resources. Clicking **Subscribe** opens a dialog that asks for confirmation that you want to receive notification when the selected resources are updated.

Feature	Description

	This menu offers two packaging functions for the selected resources:
	• **Create**: creates a **resourceBundle.zip** file that contains the selected resources and opens a dialog in which you can either:
	  • open the file, or
	  • save the file for subsequent deployment.
	• **Deploy**: opens the Deployment Wizard, in which you can choose a **resourceBundle.zip** file and deploy it.

See Also

- For more details on Deployment (), see Deploy Resources Manually topic in *Live Services Guide*.
- For more details on Deploying a Package (), see the Resource Package Deployment Wizard topic in *Live Services Guide*.

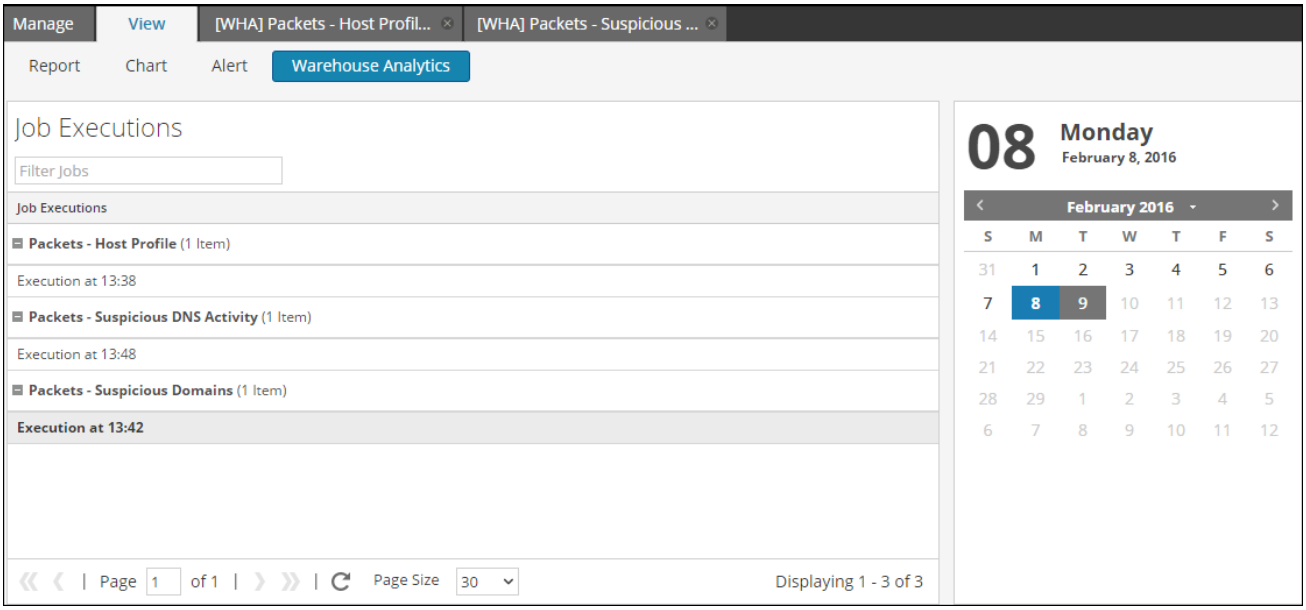
View All Jobs Panel

The View All Jobs panel displays all jobs and their information.

The View All Jobs page has the following panels:

1. Jobs Output
2. Jobs Calendar
3. Jobs Time

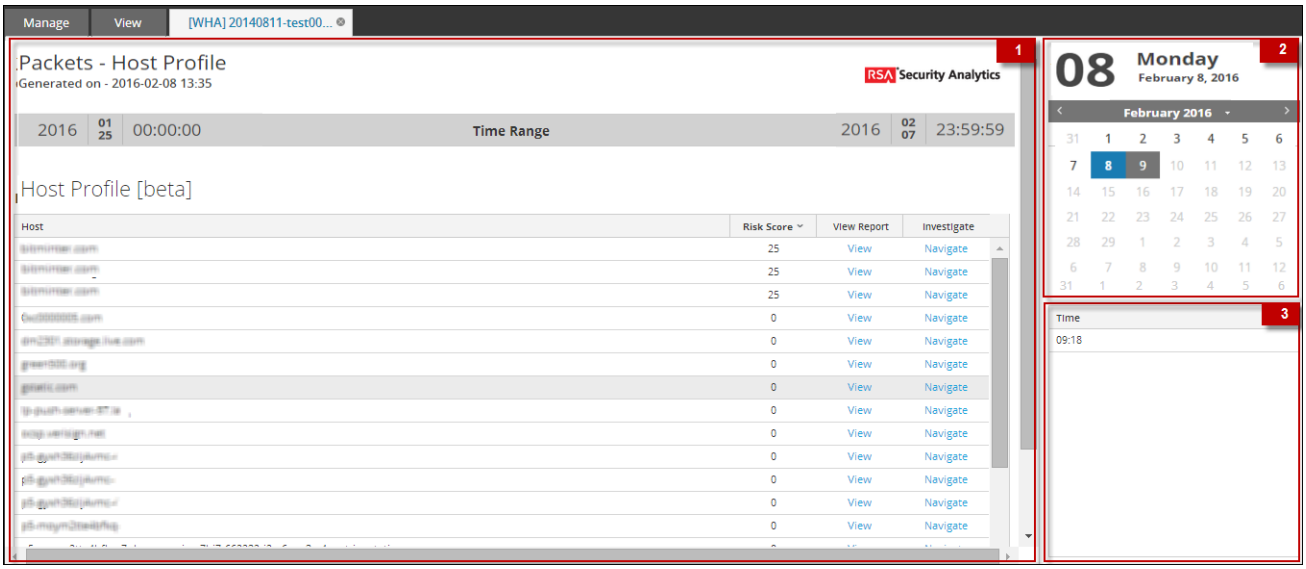
The following figure shows the different panels in this view.



The following table lists the operations in the Job Executions toolbar.

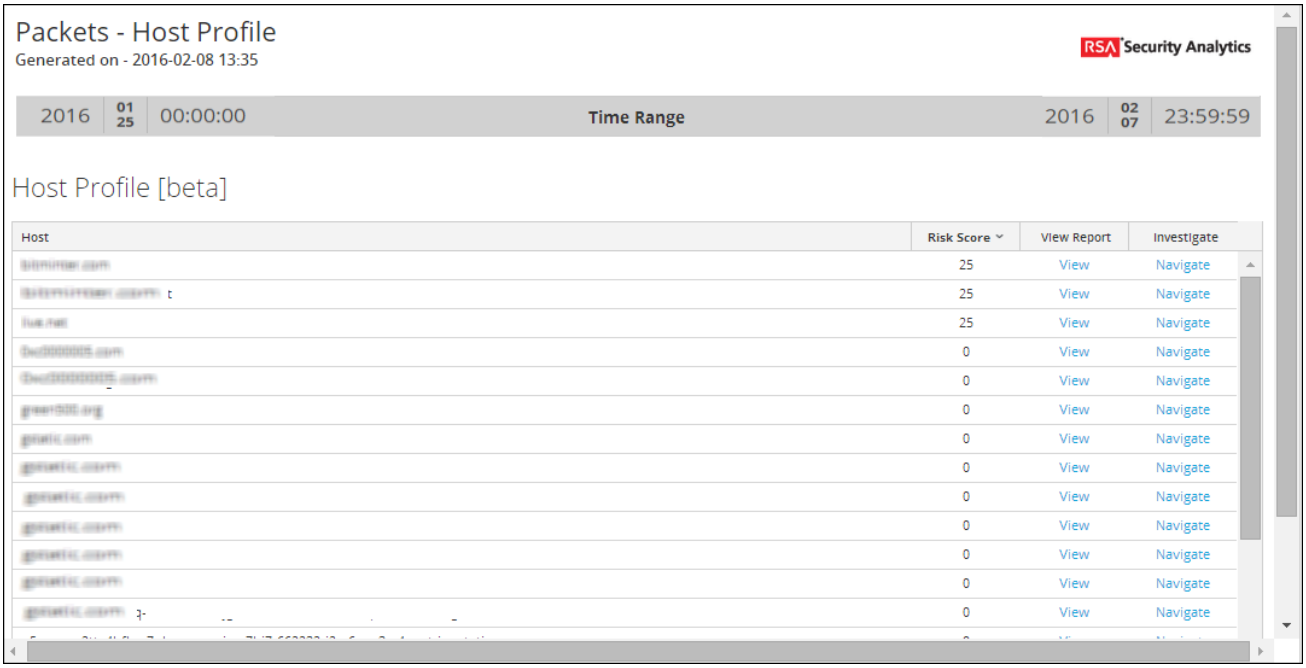
Operation	Description
Filter Jobs	Searches schedules based on the scheduled job name for a selected calendar day.

Click on any of the jobs listed to view the job.



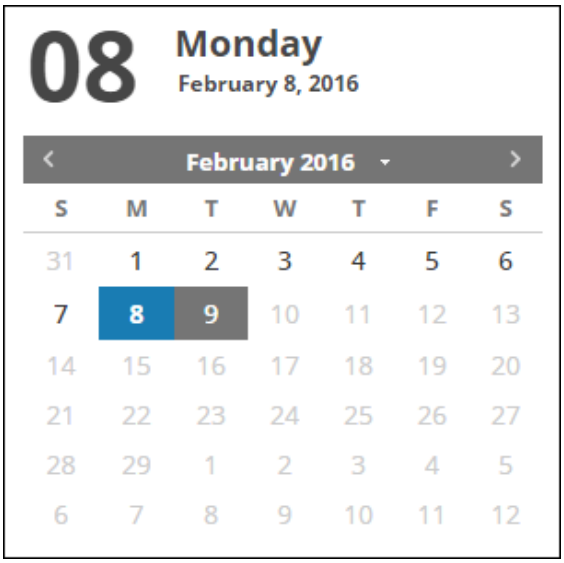
Jobs Output Panel

The Job Output panel displays the job with the job schedule name, job generated time and the actual job with the list of suspicious domains along with their risk score.



Jobs Calendar Panel

The Job Calendar panel is used to select a date from the Calendar. Based on the date you select the list of successfully run jobs for the date is displayed.



Jobs Time Panel

The Reports Time panel displays the time when the job was actually run.

View a Scheduled Job Panel

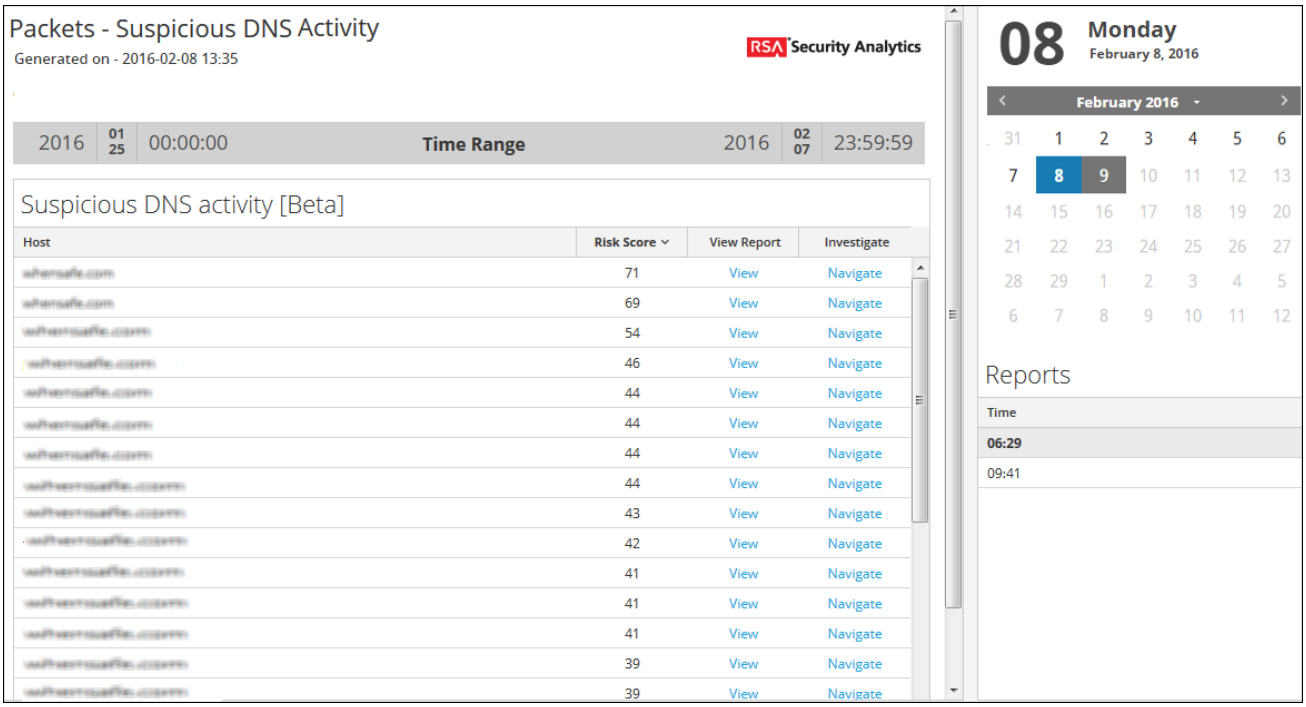
This topic describes the features on the View a Scheduled Job panel. The View a Scheduled Job panel displays all scheduled jobs and options for each job, and allows you to view reports.

The View a Scheduled Job panel has the following panels:

- Jobs Output
- Jobs Calendar
- Jobs Time

For more information on each of these panels, see View All Jobs Panel.

The following figure shows the View a Scheduled Job panel.

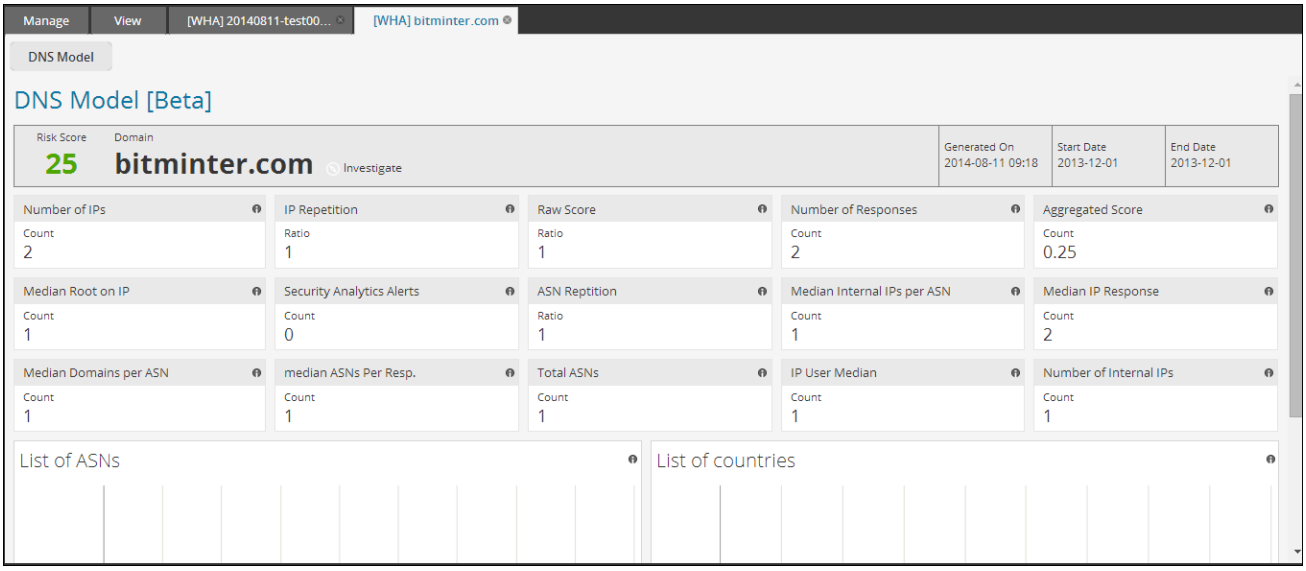


The following table lists the various columns in the View a Scheduled Job panel.

Column	Description
Host	The list of suspicious domains.
Risk Score	Indicates the score based on which the domain is considered as suspicious. For instance, the risk score 100 indicates that the domain is highly suspicious.

Column	Description
View Report	Click to view a report on the Step 4. Analyze a Warehouse Analytics Report page.
Investigate	Click to investigate from a Warehouse Analytics report.

Click on any of the suspicious domains listed and click **View** to view the desired report.

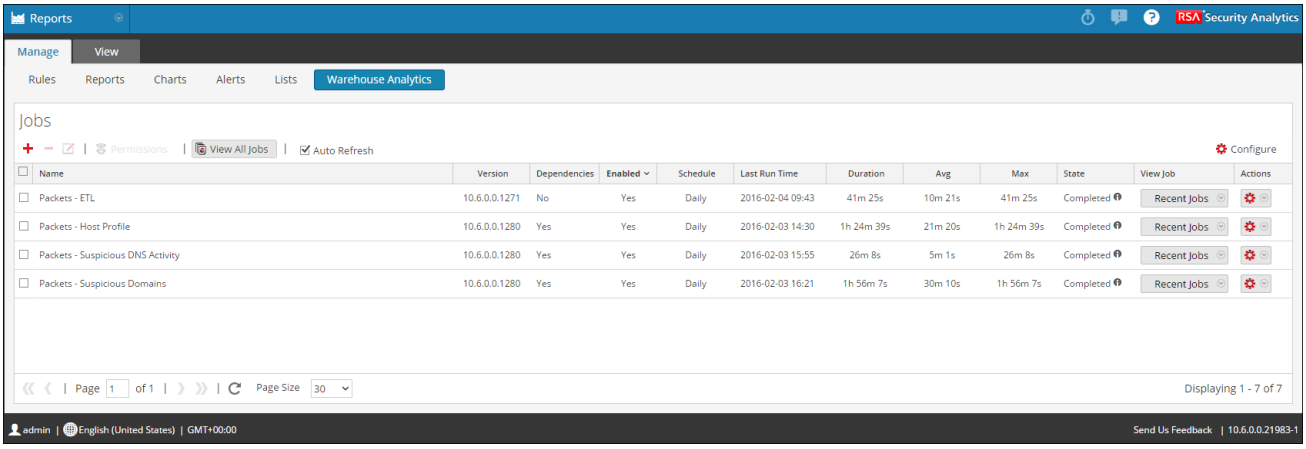


Warehouse Analytics View

This topic describes the features on the Warehouse Analytics view. The Warehouse Analytics view allows you to manage, view, and set permissions for jobs.

The Warehouse Analytics view consists of the following:

- Warehouse Analytics toolbar
- Warehouse Analytics list



Warehouse Analytics Toolbar

The Warehouse Analytics toolbar allows you to add, edit, delete, and view all jobs. Using this panel, you can also set permissions for a job.

The following table lists the operations in the Warehouse Analytics toolbar.

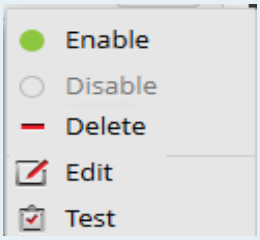
Operation	Description
+	Create a new job schedule or scheduled job.
−	Deletes the selected job schedule.
	Edits the selected job schedule. **Note:** Double-click on a desired job schedule to edit it.
Permissions	Set access permission for a job schedule.

Operation	Description
View All Jobs	View all job schedules.
Auto Refresh	Automatically refresh the scheduled jobs list.
Configure	Allows you to configure Warehouse Analytics jobs.

Warehouse Analytics List

The Warehouse Analytics list provides all the jobs in a tabular format. The following table lists the various columns in the Warehouse Analytics list and their description.

Column	Description
Name	The name of the job. **Note:** When you upgrade to 10.6, the jobs for Suspicious Domains, Suspicious DNS Activity, and Host Profile models appear as DEPRECATED. You must create new jobs for each of these models and can use the "DEPRECATED" jobs as reference.
Version	The version of the job.
Dependencies	If the job has a dependency, then it is listed as **Yes** in this column. When you mouse the dependency, you can view the name of the dependency.
Enabled	Whether the job is enabled or not.
Schedule	The type of schedule for run configuration. This is a Daily execution.
Last Run Time	The last time the job was run.
Duration	The time duration taken to run the job.
Avg	The average time taken to run the job.
Max	The maximum time taken to run the job.

Column	Description
State	Indicates the state of the scheduled job. • **Scheduled**: If a job is scheduled to run on a daily, weekly, monthly, or later time, the state of the report is displayed as scheduled, for the first run. • **Queued**: If a job is waiting to be executed, the state of the job is displayed as queued. • **Running**: If the job schedule is in progress, the state of the job is displayed as running. • **Failed**: If the schedule executions failed in a job with a selected model, the state of the job is displayed as failed. • **Completed**: If a job schedule is successfully executed, the state of the job is displayed as completed.
View Job	The list of recent jobs.
Actions 	• Enable a scheduled job, see Enable or Disable a Scheduled Job. • Disable a scheduled job, see Enable or Disable a Scheduled Job • Delete a job, see Delete a Warehouse Analytics Job • Edit a job, see Edit a Warehouse Analytics Job • Test a job, see Test a Warehouse Analytics Job.