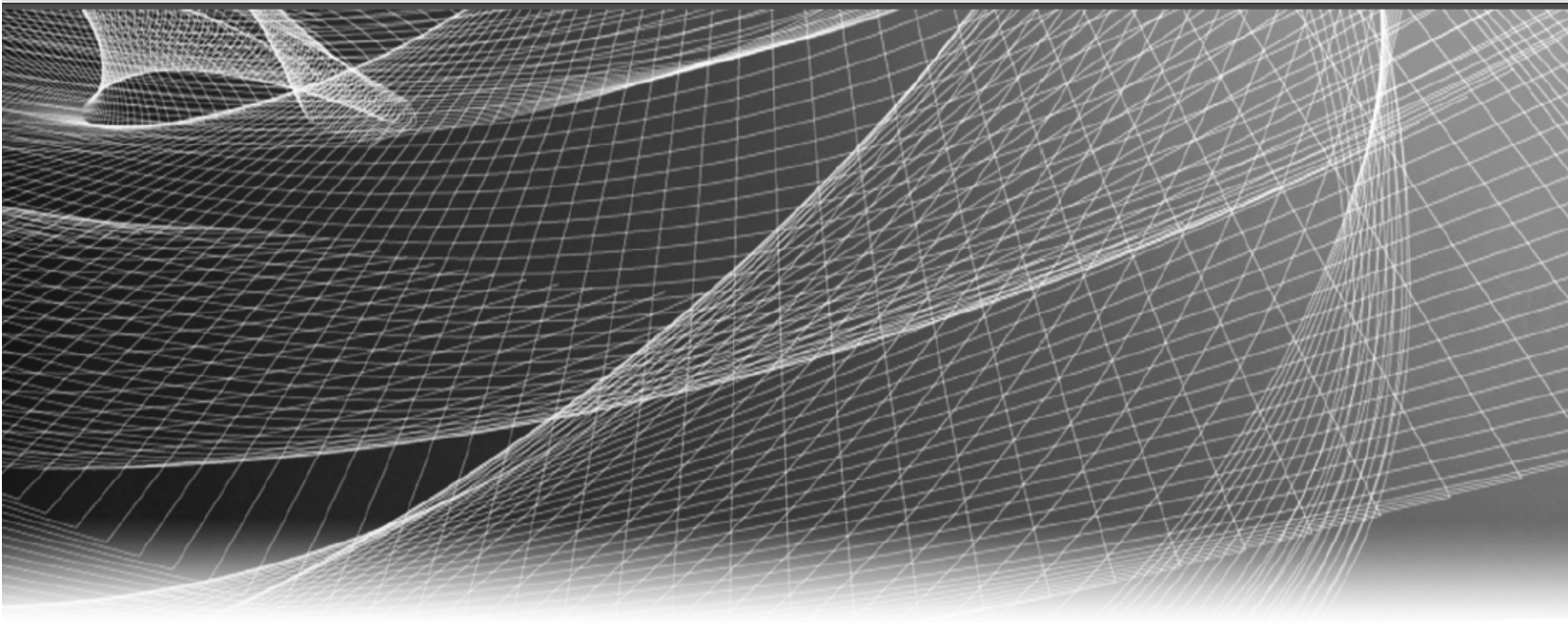


RSA Security Analytics

Event Stream Analysis Configuration 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.

January 2019

Contents

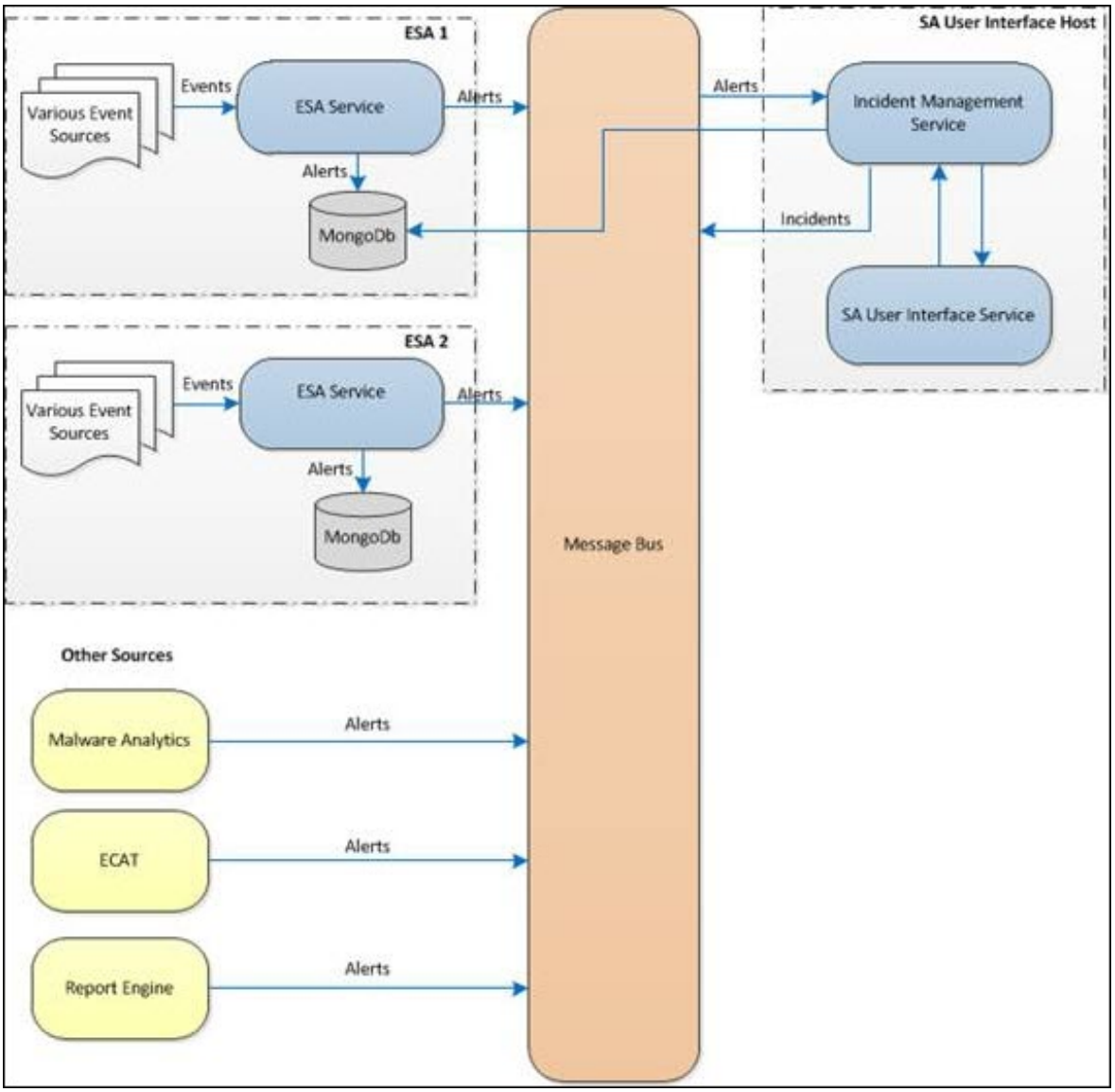
Event Stream Analysis Overview

This topic provides an overview of the Event Stream Analysis module.

The Security Analytics Event Stream Analysis (ESA) service provides advanced stream analytics such as correlation and complex event processing at high throughputs and low latency. It is capable of processing large volumes of disparate event data from Concentrators.

ESA's advanced Event Processing Language allows you to express filtering, aggregation, joins, pattern recognition and correlation across multiple disparate event streams. Event Stream Analysis helps to perform powerful incident detection and alerting.

The following diagram shows the workflow:



Configure Event Stream Analysis (ESA)

This topic provides high-level tasks to configure the Security Analytics Event Stream Analysis.

Prerequisites

Make sure that you:

- Install the Event Stream Analysis service in your network environment.
- Install and configure one or more Concentrators in your network environment.

Procedure

Note: You can configure ESA using an SSL port (50030) only. There is no option to configure a Non-SSL port.

To configure Event Stream Analysis:

Tasks	Reference
1. You can discover, update or add the host on which the ESA service is installed. (Optional) If ESA is not set up, you need to add Event Stream Analysis as a core service and add the Event Stream Analysis service to the host.	Refer to "Step 1 : Add or Update a Host" in the "Host and Services Getting Started Guide". Refer to Step 1. Add Event Stream Analysis Service.
2. Apply license to the Event Stream Analysis service.	Refer to "View Current Entitlements" in the "Licensing Guide."
3. Add the Concentrator as data source to the Event Stream Analysis service.	Refer to Step 2. Add a Data Source to an ESA Service
4. Configure notifications for Event Stream Analysis service.	Refer to "Notification Methods" in the "Alerting Using ESA Guide."
5. Download Event Stream Analysis content using Live.	Refer to "Live Search View" in the "Live Resource Managment Guide".

Tasks	Reference
6. (Optional) Advanced configuration for Event Stream Analysis service.	Refer to Step 3. Configure Advanced Settings for an ESA Service.
7. (Optional) Enable Context Hub.	Refer to "Step 1. Add the Context Hub Service" in the "Context Hub Configuration Guide".
8. (Optional) Configure ESA to connect to the Context Hub on another ESA.	Refer to Step 4. Configure an ESA to Connect to the Context Hub on Another ESA.

Result

The Event Stream Analysis service is configured and you can now add ESA Rules for event processing and alerting. For information on adding ESA Rules, see "Add Rules to the Rule Library" in the "Alerting Using ESA Guide."

Step 1. Add Event Stream Analysis Service

This topic provides information on how to add the Event Stream Analysis (ESA) service on a host.

Prerequisites

Ensure that you have installed an ESA service and added the host in Security Analytics. For more information, see "Step 1: Add or Update a Host" in the "Host and Services Getting Started Guide."

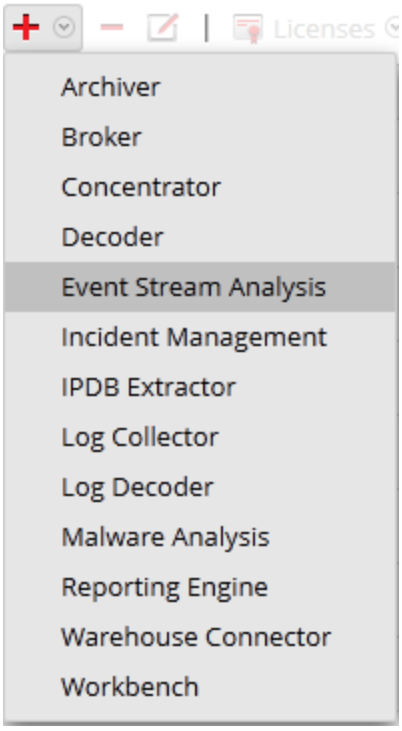
Procedure

To add the Event Stream Analysis service:

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

   The services view is displayed.

2. In the Services panel, select + **> Event Stream Analysis**.



The **Add Service** dialog is displayed.

3. Provide the following details.

Field	Description
Host	Select the host on which you want to install the ESA service.
Name	Type a name for the service.
Port	Default port is 50030. **Note:** ESA can be configured using the SSL port 50030 only. You cannot configure a Non-SSL port.
Entitle Service	Select if you want to apply the entitlements currently configured to this service.

4. Click **Test Connection** to determine if Security Analytics connects to the service.

Note: While adding the service, Security Analytics sends ICMP packets to the service to verify if the hostname/ip address entered is valid for successful test connection.

5. When the result is successful, click **Save**.

The added service is now displayed in the Services panel.

Note: If the test is unsuccessful, edit the service information and retry.

Step 2. Add a Data Source to an ESA Service

This topic describes how to add a new or existing data source to the Event Stream Analysis service.

An ESA service ingests data from a Concentrator to detect incidents and alert the user. For ESA to analyze data, you need to configure the sources from which the ESA will read data. Use the procedures in this topic to add data sources for your ESA.

Prerequisites

You must have one or more Concentrators configured in Security Analytics.

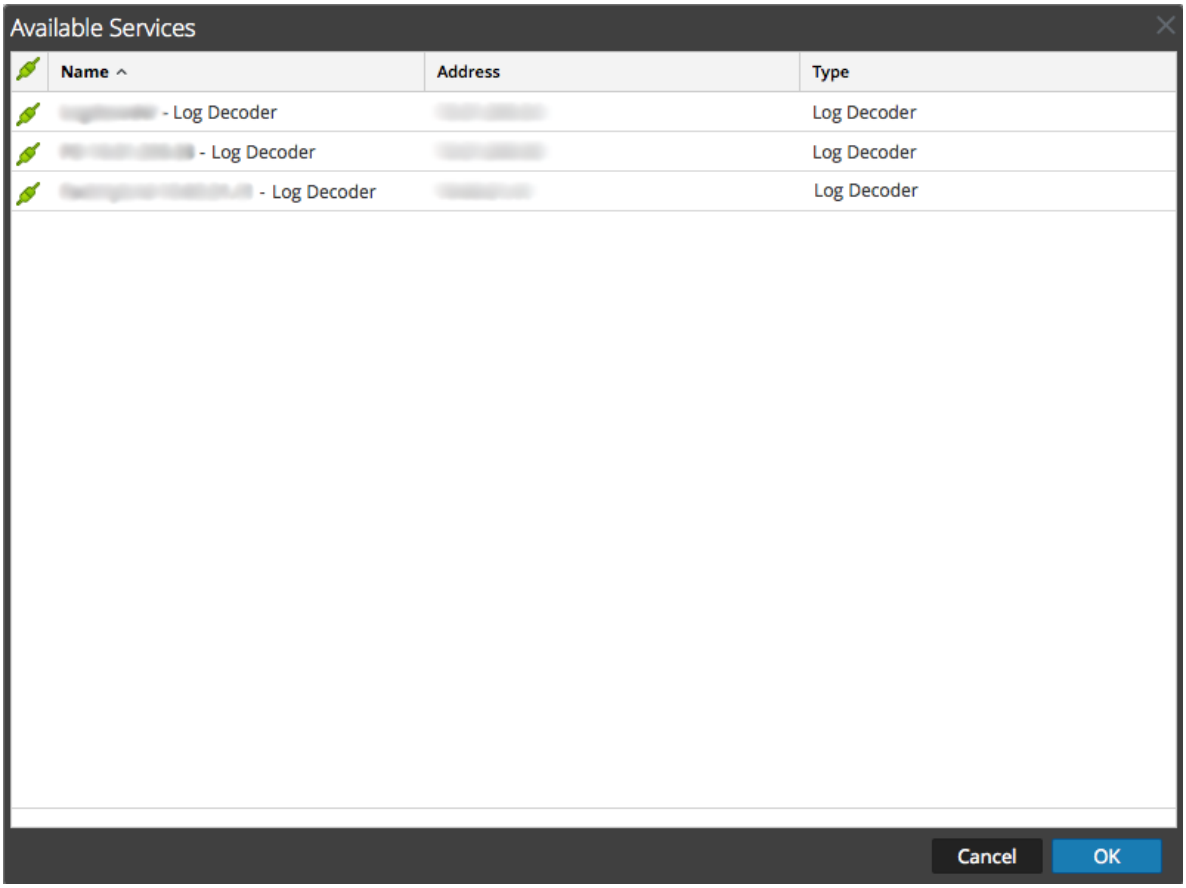
You must perform the following steps to add a data source:

- Add an Available Data Source
- Specify username and password for the Data Source

Procedures

Add Existing Services as Data Source

1. In the **Security Analytics** menu, select **Administration > Services**.
   The Services view is displayed.
2. In Services view, select an ESA service.
3. In the **Actions** column, select **View > Config**.
4. In the **Data Sources** tab, click + .
   The available services are displayed as shown in the following figure.



5. Select one or more services and click **OK**.
   The service is added to the list of services in the **DataSources** tab.
6. (Optional) Click **Enable** to enable the data source.
7. Click **Apply** to save the configuration.

Specify Username and Password for the Data Source

Note: You can add a Log Decoder as a data source for ESA but RSA recommends you add a Concentrator to take advantage of undivided aggregation as the Decoder may have other processes aggregating from it.

To specify the username and password for the data source:

1. In the **Security Analytics** menu, select **Administration > Services**.
   The Services view is displayed.
2. In the **Services** view, select a Concentrator service.
3. Click .

4. Specify the username and password.
5. Click **Save**.

Step 3. Configure Advanced Settings for an ESA Service

This topic provides instructions to configure advanced settings for an Event Stream Analysis service.

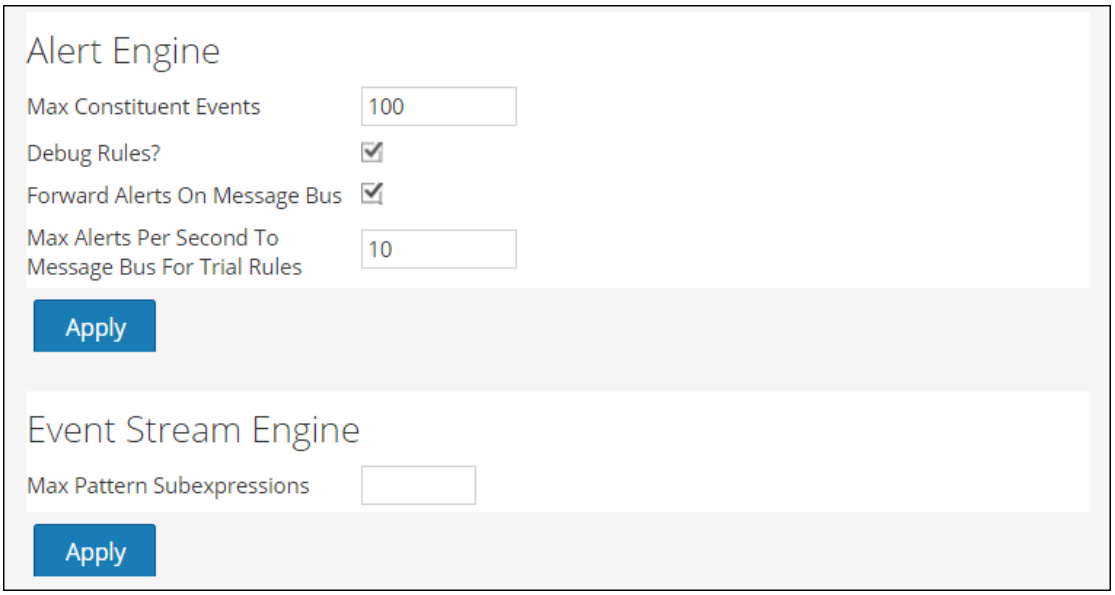
In the Advanced view, you can configure advanced settings to improve performance, to preserve events for rules with multiple events, to buffer events in memory, and the number of events to be stored on the ESA.

Procedures

Configure Advanced Settings

To access the Advanced view and configure advanced settings for an ESA service:

1. In the **Security Analytics** menu, select **Administration > Services**.
   The Services view is displayed.
2. In Services view, select an ESA service.
3. In the **Actions** column, select **View > Config**.
4. Select the **Advanced** tab.
   The Advanced view is displayed.

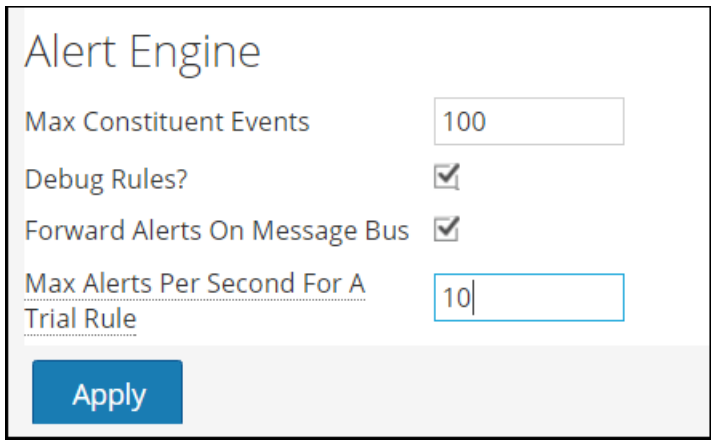


Configure Alert Engine Settings

In the Alert Engine section, you specify values to preserve events for rules that choose multiple events.

Note: After you upgrade to 10.5, the Debug Rules option if enabled previously will be disabled. You will need to enable this option after upgrade.

The following figure shows the Alert Engine section.



To configure Alert Engine settings:

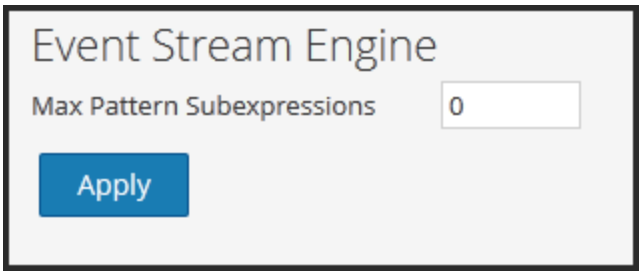
1. In the Alert Engine section, specify a value for **Max Constituent Events**. The default value is 100.
2. Select **Debug Rules?** to enable debugging rules.
3. If you want alerts to be sent to Message Bus and Incident Management, select the **Forward Alerts On Message Bus** option.
4. To specify the maximum number of alerts to be forwarded to the Message Bus for the trial rule, select **Max Alerts Per Second for a Trial Rule**. The The default value is **10**.
5. Click **Apply** to save the changes and put them into effect immediately.

Note: For more information on the parameters in the Alert Engine section, see Alert Engine Settings in ESA Advanced View.

Configure Event Stream Engine Settings

In the Event Stream Engine section, you specify details to improve performance.

The following figure shows the Event Stream Engine section.



To configure Event Stream Engine settings:

1. In the Event Stream Engine section, specify **Max Pattern Subexpressions**.
2. Click **Apply** to save the changes and put them into effect immediately.

Note: For more information on the parameters in the Event Stream Engine section, see Event Stream Engine Settings in ESA Advanced View.

Step 4. Configure an ESA to Connect to the Context Hub on Another ESA

This topic tells administrators how to configure an ESA to connect to the Context Hub on another ESA. Only one Context Hub can be installed per Security Analytics installation. If you have more than one ESA and you run the Context Hub, you need to enable the ESA without the Context Hub to communicate with the Context Hub on another ESA.

Prerequisites

You must be running multiple ESAs and a Context Hub.

Procedure

Configure ESA to connect to the Context Hub on another ESA.

1. Note the IP address of the ESA that is running the context hub service.
2. From Administration > Services, select the ESA service that is not running the Context Hub and then  > **View** > **Explore**.
3. In the left hand panel, navigate to **Service** > **ContextHub**, then select **contextHubTransport**.
4. Edit the **Host** field to point to the Domain name or IP address of the ESA that is running the Context Hub service.

Result

The ESA connects to the Context Hub on another ESA service.

Additional Procedures

This topic is a collection of individual procedures, which an Administrator may perform at any time and they are not required to complete the initial setup of ESA. These procedures are presented in alphabetical order.

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

Change Default Storage Passwords

This topic tells administrators how to change default storage passwords for database accounts that store alerts in ESA, Incident Management and Data Science.

Security Analytics 10.5 uses MongoDB as the database to store alerts in the following modules:

- ESA
- Incident Management
- Data Science

The database in each module has an account to control access and each Security Analytics service account has a default password.

To strengthen security, RSA recommends that you change default passwords. Some organizations do not allow default passwords. In those cases, the procedures in this topic would be required.

This topic explains how to change the default storage password for the database account in each module.

Previous ESA Storage Password

ESA was introduced in Security Analytics 10.3 when the database was in PostgreSQL. If you used ESA in version 10.3 and created a custom password for the PostgreSQL database, it has no impact on MongoDB. When you install or or upgrade to Security Analytics 10.5, MongoDB is installed with a default password.

Incident Management and Data Science were introduced in Security Analytics 10.4 so they have only used MongoDB.

Dependencies

MongoDB has a master admin account that has privileges over the database accounts for the ESA, IM and Data Science services.

Note: You must change the admin account password first. You can change passwords for the services in any sequence.

ESA is a requirement for Incident Management and Data Science. The configuration for each module points to the host that runs the ESA service. Databases for ESA, Incident Management and Data Science are located on the host that runs the ESA service.

Database Privileges

The following figure shows the privileges assigned to each account during the installation or upgrade process.

Account	Privileges	Database
admin	readWriteAnyDatabase userAdminAnyDatabase dbAdminAnyDatabase	All
Event Stream Analysis	readWrite dbAdmin clusterAdmin	ESA
Incident Management	readWrite dbAdmin clusterAdmin	IM

Account	Privileges	Database
Data Science	readWrite dbAdmin clusterAdmin	Data Science

For details on changing each password, see:

- Change MongoDB Password for admin Account
- Change ESA Storage Password
- Change Incident Management Storage Password
- Change Data Science Storage Password

Change MongoDB Password for admin Account

This topic tells administrators how to change the default storage password for the MongoDB admin account.

In Security Analytics, this procedure is optional. However, it is always a best practice for administrators to change any default password for added security. Some organizations do not allow default passwords.

Note: You must change the MondoDB admin account password first. You must enter it before you can change the passwords for ESA, Incident Management and Data Science.

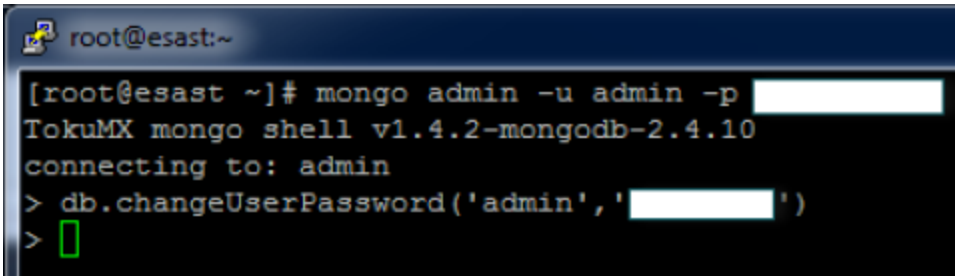
Prerequisites

You must have Administrator role privileges.

Procedure

1. Log on to the ESA host that runs the ESA service:
    a. SSH to the ESA host.
    b. Log on as root.

2. Log on to MongoDB as admin. The default password is netwitness.
   `mongo admin -u admin -p <current_password>`



3. To change the admin account password, type
   `db.changeUserPassword('admin','<new_password>')`

   Now you can change the password for the ESA, Incident Management and Data Science services.

Change ESA Storage Password

This topic tells administrators how to change the default storage password for the ESA database.

In Security Analytics, this procedure is optional. However, it is always a best practice for administrators to change any default password for added security. Some organizations do not allow default passwords and make this procedure mandatory.

Prerequisites

You must have Administrator role privileges.

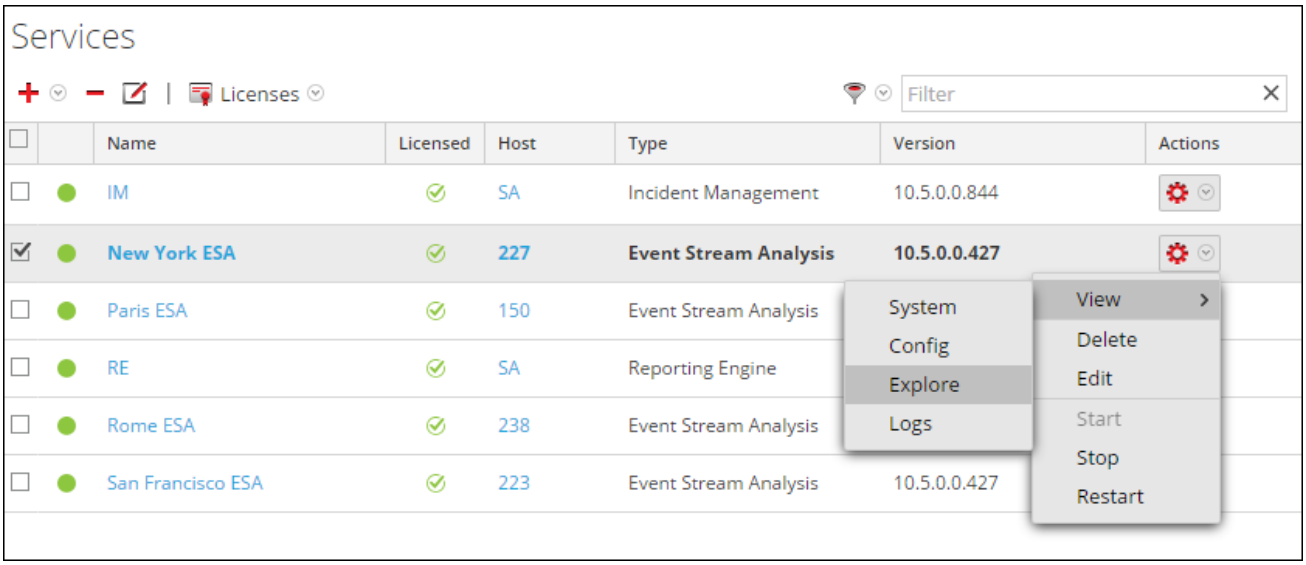
Procedures

Change Password for ESA Database Account

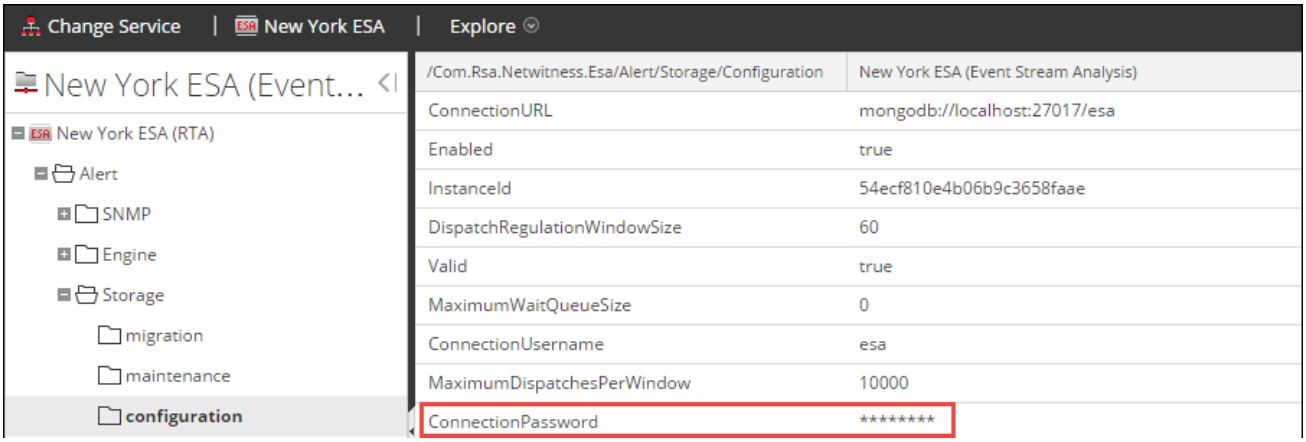
1. Log on to the host that runs the ESA service:
   a. SSH to the ESA host.
   b. Log on as **root**.
2. Log on to the MongoDB as the admin user:
   `mongo esa -u admin -p <current_admin_password> --authenticationDatabase admin`
3. Type the following command to change the ESA account password. The default pasword is esa.
   `db.changeUserPassword('esa','<new_password>')`

Change Password for ESA Service

1. Log on to Security Analytics as admin.
2. In the **Security Analytics** menu, select **Administration > Services**.



3. Select the ESA service, then  **> View > Explore**.
4. In the Explore view on the left, select **Alert > Storage > configuration**.



5. In the right panel, type the database account password in the **ConnectionPassword** field.

> **Note:** The password for the database and for the Security Analytics service configuration must be the same.

6. To validate that the database and Security Analytics passwords match, in the Security Analytics menu select **Alerts > Summary**.
   If content appears in the Summary tab, the passwords match and were changed

successfully.

If you do not see content in the Summary tab, revise the service password to match the MongoDB password.

Change Incident Management Storage Password

This topic tells administrators how to change the default storage password for the Incident Management database.

In Security Analytics, this procedure is optional. However, it is always a best practice to change any default password for added security. In organizations that do not allow default passwords, this procedure is mandatory.

Prerequisites

You must have Administrator role privileges.

The default password for the MongoDB admin account must be changed.

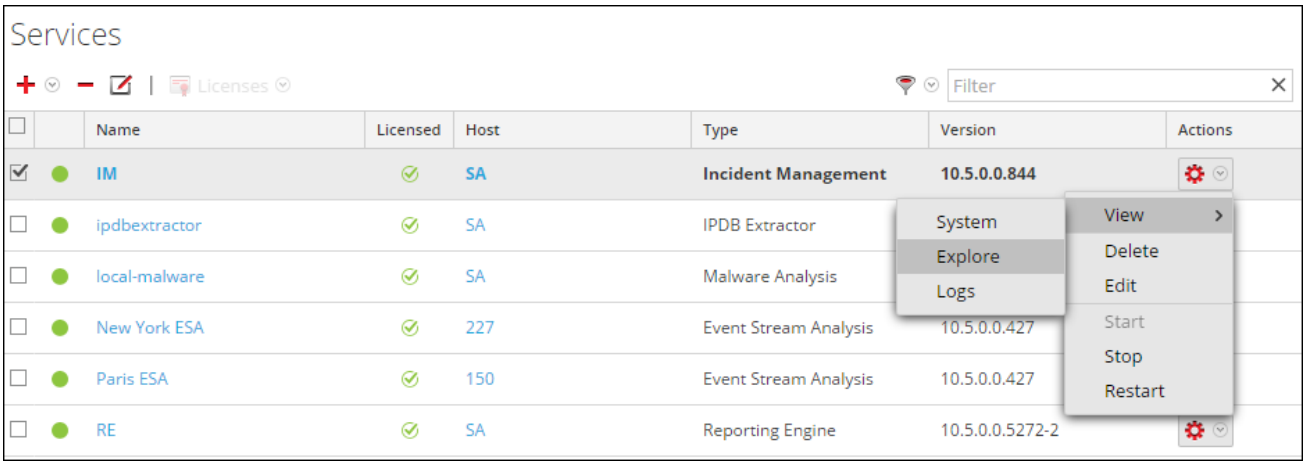
Procedures

Change Password for Incident Management Database Account

1. Log on to the host that runs the ESA service:
   a. SSH to the ESA host.
   b. Log on as root.
2. Log on to the MongoDB as admin:
   ```
   mongo im -u admin -p {current_admin_password} --
   authenticationDatabase admin
   ```
3. Type the following command to change the Incident Management account password. The default password is **im**.
   ```
   db.changeUserPassword('im','{new_password}')
   ```

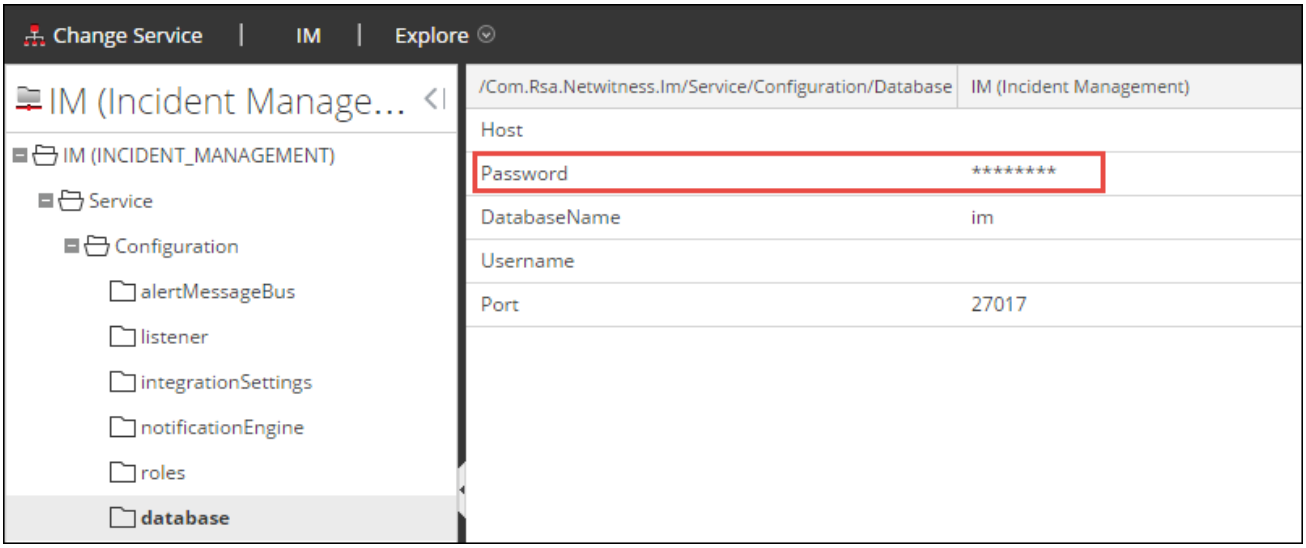
Change Password for Incident Management Service

1. Log on to Security Analytics as admin.
2. In the **Security Analytics** menu, select **Administration** > **Services**.



3. Select the Incident Management service, then > **View** > **Explore**.

4. In the Explore view on the left, select **Configuration** > **database**.



5. In the right panel, type the database account password in the **Password** field.

Note: The password for the database and for the Security Analytics service configuration must be the same.

6. Restart the Incident Management service to accept the password change and force the session to start using the new password.

   a. Select **Administration** > **Services**.

   b. Select the Incident Management service, and click > **Restart**.

7. To validate the new passwords match, select **Incidents** > **Alerts**.
   If you see content in the Alerts tab, you changed the passwords successfully.

If you do not see content in the Alerts tab, revise the service password to match the MongoDB password.

Change Data Science Storage Password

This topic tells administrators how to change the default storage password for the Data Science database.

In Security Analytics, this procedure is optional. However, it is always a best practice to change any default password for added security. In organizations that do not allow default passwords, this procedure is mandatory.

Prerequisites

You must have Administrator role privileges.

The default password for the MongoDB admin account must be changed.

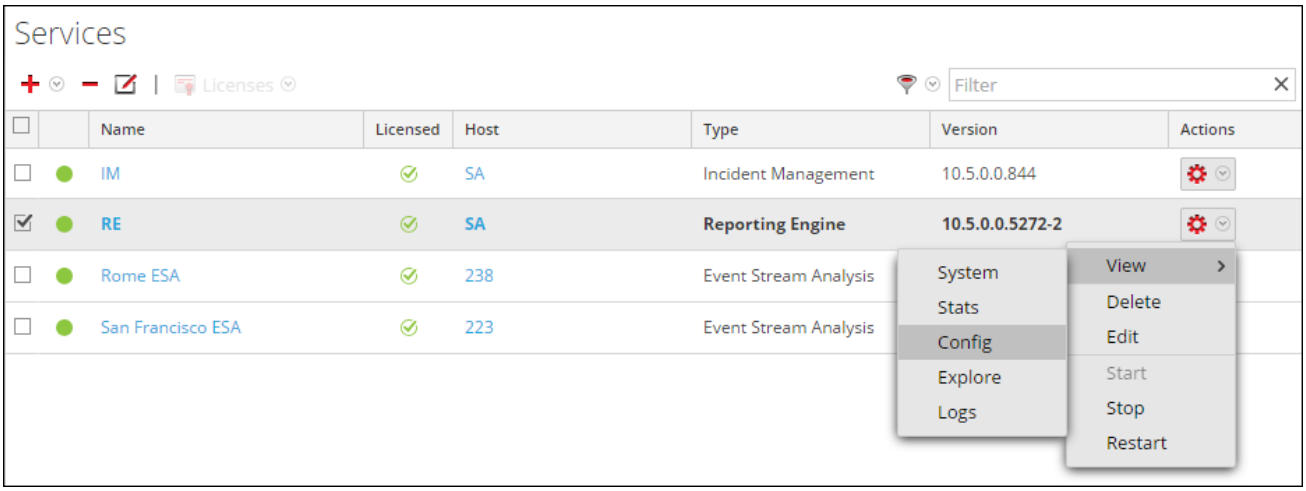
Procedures

Change Data Science Password for Database Account

1. Log on to the host that runs the ESA service.
   a. SSH to the ESA host.
   b. Log on as root.
2. Log on to MongoDB as admin.
   ```
   mongo ds -u admin -p {current_admin_password} --
   authenticationDatabase admin
   ```
3. To change the Data Science account password, type
   ```
   db.changeUserPassword('ds','{new_password}')
   ```

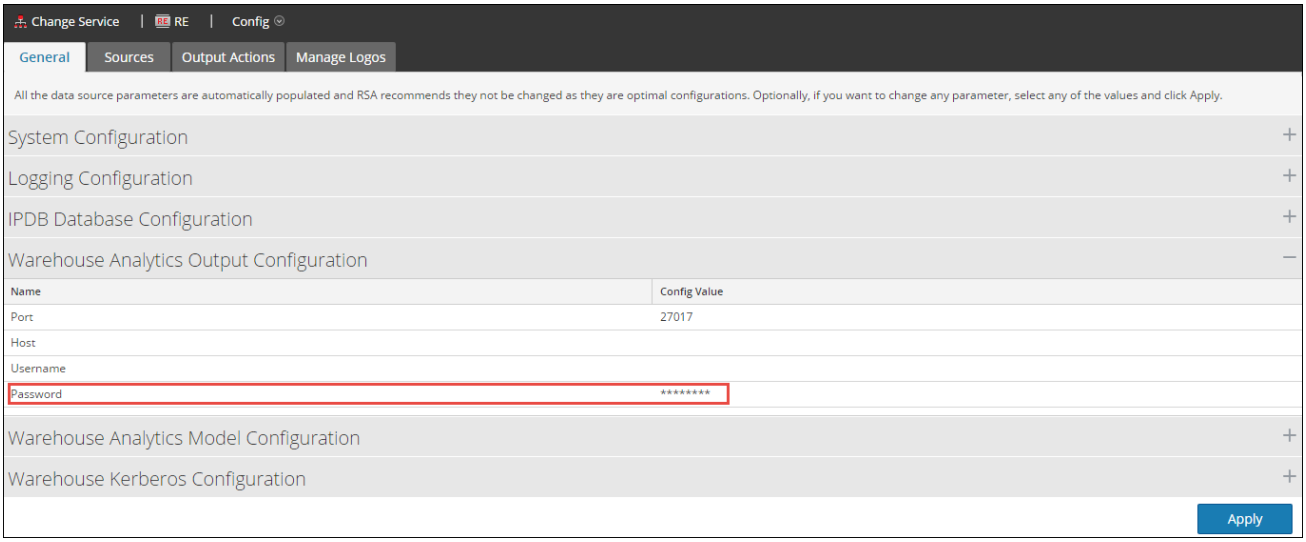
Change Data Science Password for Security Analytics

1. Log on to Security Analytics as admin.
2. In the **Security Analytics** menu, select **Administration > Services**.



3. Select the Reporting Engine service, then  **> View > Config**.

   The Config view is displayed with the General tab open.



4. Select **Warehouse Analytics Output Configuration**.
5. Type the database account password in the **Password** field.

> **Note:** The password for the database and for the Security Analytics service configuration must be the same.

6. To validate the new passwords match, execute a Report in Reporting Engine that uses Warehouse Analytics.

Change Memory Threshold for Trial Rules

This topic tells administrators how to set a memory usage threshold for trial rules. When the threshold is exceeded, all deployed trial rules are disabled.

This procedure is optional. Administrators can increase or decrease the memory threshold for trial rules. Threshold refers to the ESA memory usage, which includes ESA base memory, trial rules and non-trial rules. When the threshold is exceeded, all deployed trial rules on an ESA service are disabled.

You use trial rules to see if a rule runs efficiently and does not use excessive memory, which can impact performance or force the service to shut down.

By default, the memory threshold is 85, which is the percentage of Java Virtual Memory (JVM).

- The memory threshold is per ESA, not per rule.
- When the memory threshold is exceeded, all trial rules running on the ESA are automatically disabled.
- The ESA configuration has two parameters for trial rules:
  - MemoryThresholdforTrialRules
  - MemoryCheckPeriod, which has a default value of 300 seconds

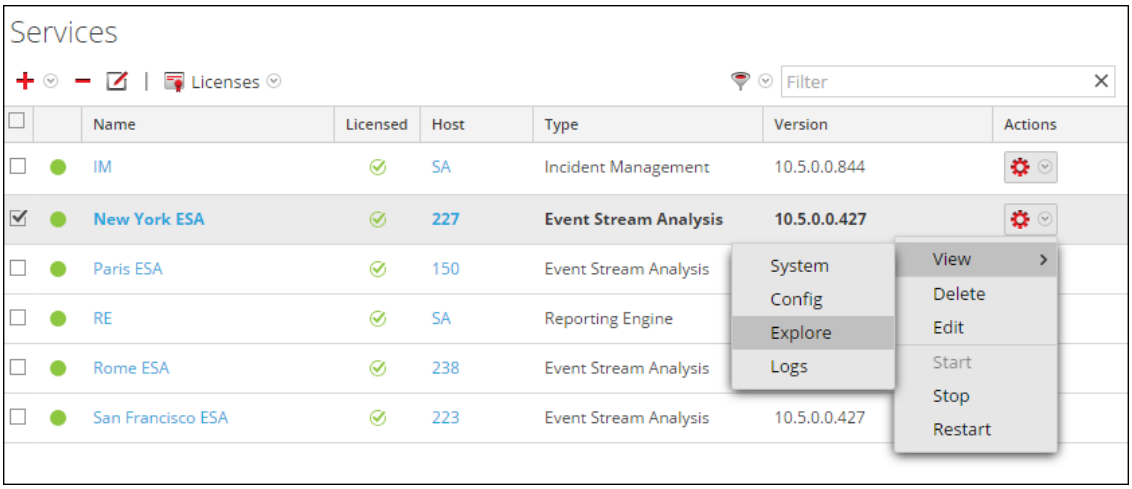
For more information, see "Work with Trial Rules" in the "Alerting Using ESA Guide".

Prerequisites

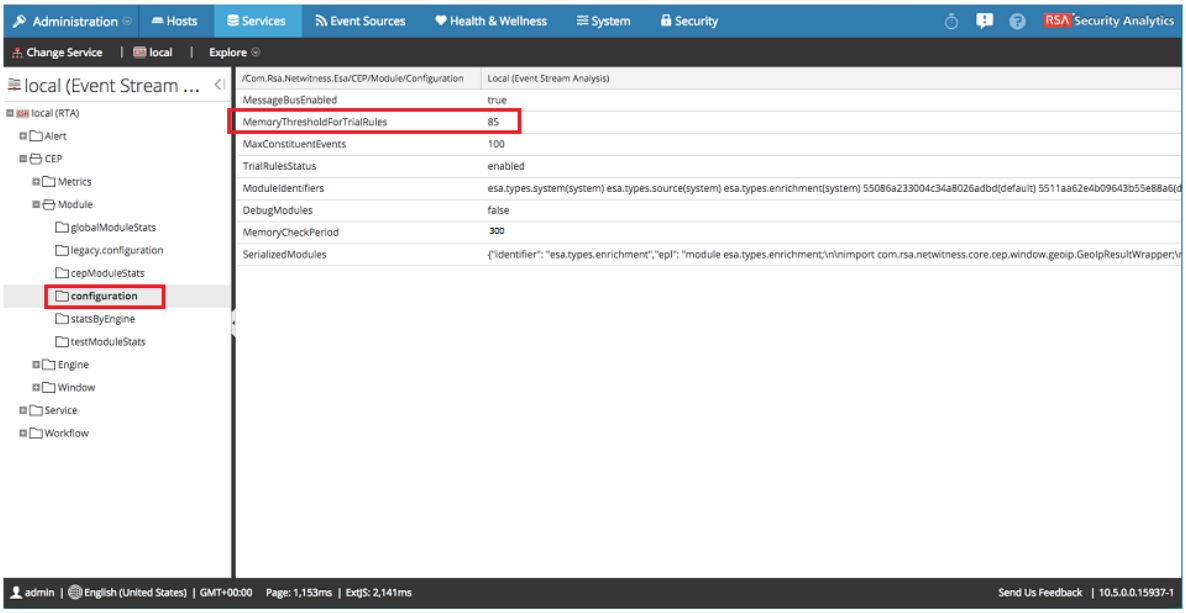
A role with administrative privileges must be assigned to you.

Procedure

1. Log on to Security Analytics as admin.
2. In the **Security Analytics** menu, select **Administration** > **Services**.



3. Select the ESA service, then  > **View** > **Explore**.
4. On the left, select **CEP > Module** > **configuration**.



5. In the right panel, in **MemoryThresholdForTrialRules** type a percentage of JVM that trial rules on the ESA can not exceed.

   The new memory threshold takes effect immediately.

Configure ESA Storage

This topic explains how to configure the ESA database to maintain a healthy level of alerts.

This procedure is optional. Administrators can specify a retention period for alerts. Deleting old alerts is a best practice to maintain the alerts database. Otherwise, the database could continue to grow and eventually have a negative impact on performance.

By default, the feature to automatically delete alerts is not enabled because each company has its own policies. This topic teaches you how to perform the following tasks:

- Enable automatic deletion of alerts
- Specify criteria to delete alerts
  - By database size
  - By alert age
  - By both database size and alert age

Configuration Parameters

The configuration parameters are as follows:

Parameter	Description
Maintenance	
Enabled	Turns on alert retention feature.
NextMaintenanceScheduledAt	(Read only) When the next maintenance is scheduled to run.
HaveAlertForDays	(Read-only) Current number days that alerts have been stored in the database. For example, if this number is checked on June 4th, and there were alerts generated every day from June 1st, then value would be 4.
DatabaseDiskUsage	(Read-only) Current database size.

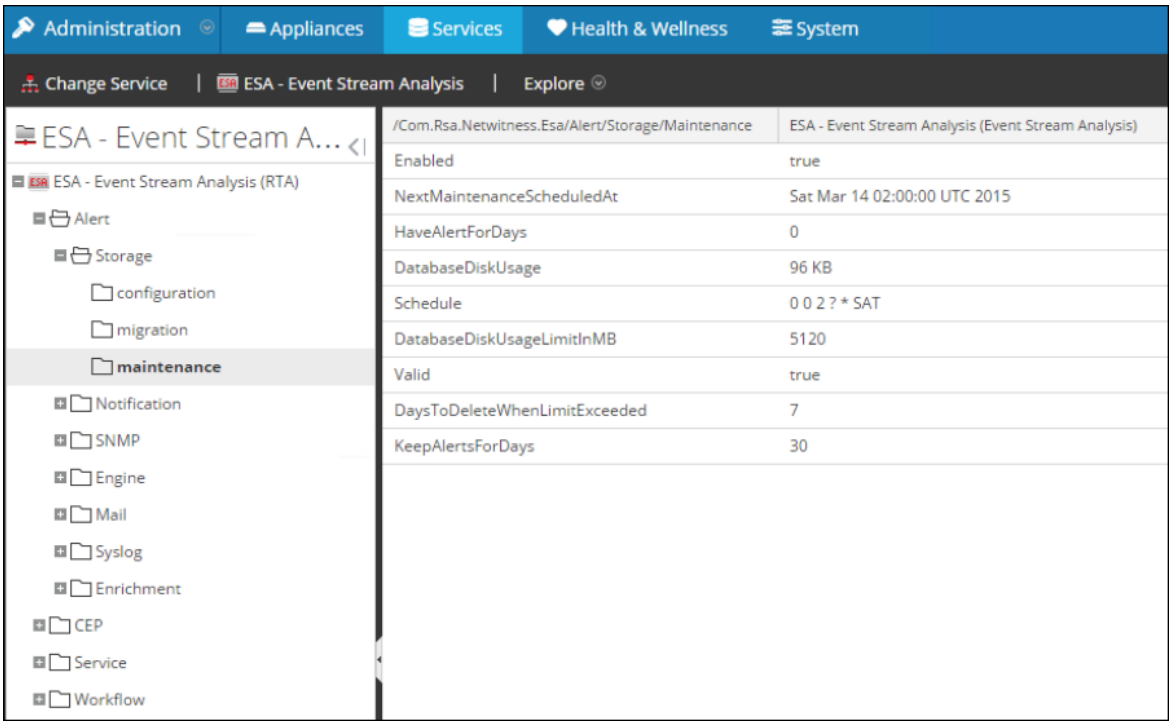
Parameter	Description
Schedule	Schedule for running the alert maintenance. The scheduling uses the UNIX Cron tab and must be specified in the correct Cron tab format. The default value is displayed in the procedure below. For more information on Cron scheduling, see http://www.cronmaker.com.
DatabaseDiskUsageLimtInMB	Database size threshold; when exceeded, alerts will be deleted.
Valid	Read-only parameter indicating whether the current configuration is valid.
DaysToDeleteWhenLimitExceeded	Number of days to remove when DatabaseDiskUsageLmitInMB is exceeded.
KeepAlertsForDays	Number of days to keep the alerts in the database before they are removed.
Configuration	
MaximumDispatchesPerWindow	Number of dispatches allowed inside a 'regulation window'. The value of 0 means unbound dispatches.
DispatchRegulationWindowSize	Specifies the length of the regulation window (in seconds). After the first alert is dispatched, the system starts counting the alerts sent and the counts are reset after the specified number of seconds. Within the window, if the number of alerts sent exceeds the value specified for MaximumDispatchesPerWindow, the system slows down which delays the dispatches. The default value is 60 seconds.
MaximumWaitQueueSize	Alerts are queued before they are dispatched. This attribute specifies the queue size. The default is 0 (unbounded queue). The queue size may increase if the maximum value is set to low, and when the queue is full the alerts will be dropped. **Note:** The ingest is not reduced, rather the alerts are dropped on the outbound side.

Prerequisites

You must have Administrator permissions.

Procedure

1. Log on to Security Analytics as admin.
2. In the Security Analytics menu, select **Administration > Services**.
3. Select the ESA service, then **View > Explore**.
4. On the left, select **Alert > Storage > maintenance**.



5. In the **Enabled** field, select true to turn on the alert retention feature.
6. Configure how you want to remove old alerts:
   - By database size – Enter the maximum database size in the **DatabaseDiskUsageLimitInMB** field. Specify how many days of the oldest alerts to delete in the **DaysToDeleteWhenLimitExceeded** field. For example, If you set the **DatabaseDiskUsageLimitInMB** value as 5120 MB and **DaysToDeleteWhenLimitExceeded** value as 7. When disk usage reaches 5120 MB and there are 10 days of alerts in the database, 7 days of alerts are deleted starting with the oldest alert.

- By alert age – Enter how many days of alerts must be retained in the **KeepAlertsForDays** field. For example, if you set the **KeepAlertsForDays** value as 10, 10 days of alerts are retained in the database and alerts older than 10 days are deleted.
- By database size and alert age – If you configure both these parameters, the parameter that deletes the higher number of days with alerts is used. For example, If the database has 15 days of alerts and if you specify the following settings:
  - **DatabaseDiskUsageLimitInMB**: 5120 MB
  - **DaysToDeleteWhenLimitExceeded**: 7
  - **KeepAlertsForDays**: 10

  KeepAlertsForDays deletes only 5 days of old alerts and **DatabaseDiskUsageLimitInMB** deletes 7 days of old alerts. As a result, **DatabaseDiskUsageLimitInMB** is used for deleting old alerts.

7. **Schedule**
   Use the schedule parameter to tell the ESA how frequently to run the alert maintenance job (i.e. how frequently to check the database and apply the deletion rules). Use the syntax for a Cron schedule job. For more information on Cron scheduling, see http://www.cronmaker.com.
8. **Refresh** the browser.
   - Date and time of next maintenance run is displayed in the **NextMaintenanceScheduledAt** field.
   - In the **Valid** field, true is displayed to indicate the configuration is valid. If false is displayed, correct the disk size or alert age settings.
9. (Optional) The maintenance status can also be monitored in the /opt/rsa/esa/logs/esa.log file on the ESA host, which will display messages similar to the example below.

Example

The maintenance status can also be monitored in the /opt/rsa/esa/logs/esa.log file on the ESA service, which will display messages similar to the example below.

```
2015-03-12 09:46:48,197 [Carlos@65dd6c04-56] INFO
com.rsa.netwitness.carlos.config.ConfigurationMXBean -
 MongoStorageMaintenance changed by admin
 2015-03-12 09:46:51,121 [scheduler_Worker-1] INFO
  com.rsa.netwitness.core.alert.dispatch.SQLStorageMaintenance -
Starting the scheduled database maintenance
 job with policy {keepAlertForDays=30, maxDiskUsageInMb=5120}
 2015-03-12 09:46:51,122 [Carlos@3801f0b3-58] INFO
  com.rsa.netwitness.core.alert.dispatch.SQLStorageMaintenance -
```

```
Scheduled a database maintenance job with
 policy {keepAlertForDays=30, maxDiskUsageInMb=5120} to run at 2/28/15
2:00 AM
 2015-03-12 09:46:51,129 [Carlos@3801f0b3-58] INFO
com.rsa.netwitness.carlos.config.ConfigurationMXBean -
 MongoStorageMaintenance changed by admin
 2015-03-12 09:46:51,133 [scheduler_Worker-1] INFO
  com.rsa.netwitness.core.alert.dispatch.SQLStorageMaintenance -
Finished the database maintenance job,
 deleted 0 partitions, next run scheduled at 3/14/15 2:00 AM
```

Configure ESA to Use a Memory Pool

This topic tells administrators how to configure the ESA to use a memory pool.

A memory pool is a customized implementation of virtual memory for events held by rules in ESA. This helps in scaling the capability of rules by an order of magnitude. When you want to create rules that cover a large time span or which are very complex, you may want to use a memory pool to handle memory more efficiently. When you use a memory pool, instead of holding all of the events in memory, they can be written to disk. This is helpful because when a rule exists that is complex or extends over a long time frame, a large number of events must be held in memory.

You can configure memory pool to run in non-batch mode or batch mode:

- **Non-batch mode**. In non-batch mode, events are written to disk as they enter the memory pool. To configure non-batch mode, set the **MapPoolBatchWriteSize** attribute to 1. Non-batch mode provides a more stable solution because each event is landed and fetched separately without creating memory spikes.

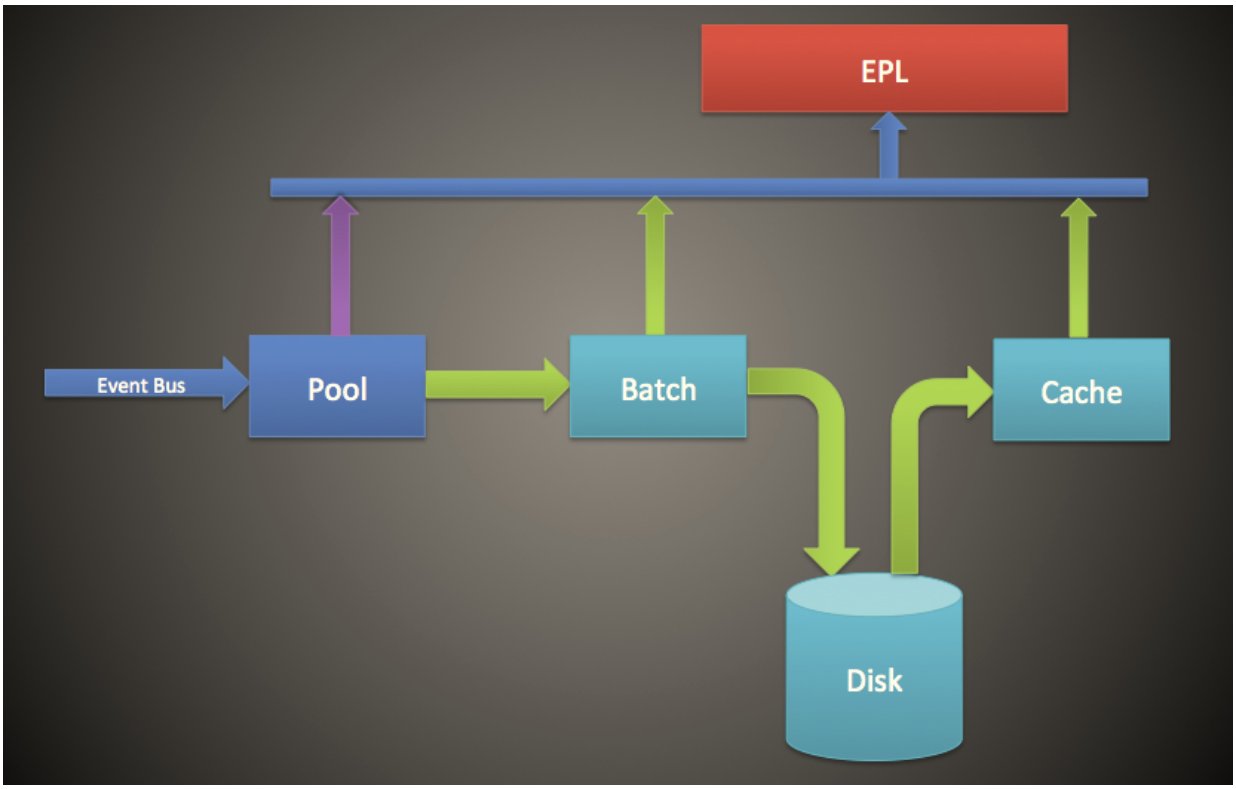
- **Batch mode**. In batch mode, events are grouped into batches and then written to disk. To configure batch mode, set the batch size attribute **MapPoolBatchWriteSize** to a value greater than 1. Batch mode gives better performance since the disk activity for landing events to disk are optimized.

Note: Any changes to these settings will require you to restart the ESA. When ESA restarts, if any events are currently being held by the memory pool, they will be discarded upon restart.

Caution: While this feature can be very helpful in managing memory, it can impact the event processing rate of the ESA. Performance can be affected from 10 to 30 percent, depending on your rules and configuration settings.

Workflow

The following diagram shows the data flow using the memory pool for batch mode:



1. Events are added to the memory pool and references to the events are stored in the memory pool.
2. The events are then batched to be sent to disk (in non-batch mode, this step is skipped).
3. Once the batch has met the threshold, the events are written to disk (in non-batch mode no threshold is required).
4. When the EPL requires an event that was written to disk, the event is sent to the cache and used in the EPL rule.

Procedure

Complete the following steps to configure an ESA memory pool.

1. From **Administration** > **Services**, select your ESA service and then > **View** > **Explore**.
2. Select **CEP** > **EsperPool** > **Configuration**.
3. Enter values for the following fields:

Attribute	Description	Configuration

MapPoolPersistenceURI	Location to store the memory pool file.	The default value is **/opt/rsa/esa/pool/esperPool**. RSA recommends you do not modify the default value. If you modify this setting to use a different partition, ensure the partition contains at least 10 times more space than the memory allocated for ESA. **Caution:** If the memory pool is in use while this path is changed,a n ESA restart is required. When this occurs, ESA does not discard the stored events so you must manually purge them.
MapPoolEnable	Enable or disable the memory pool.	The default value is **false**. Set the value to **true** to enable the memory pool. Requires a restart when you enable or disable memory pool.
MapPoolFlushIntervalSecs	Time interval to flush events to disk. For example, any event held in Esper longer than 15 minutes gets flushed to disk.	The default value is **15 minutes**. A smaller value ensures that the ESA is more stable when there are EPLs holding a large number of events in memory. A larger value (greater than 30 minutes), ensures that only relevant events required over a longer period of time are flushed to disk. **Note:** Due to Java memory management design, sometimes events not held by EPL may be sent to disk. To help prevent this from occurring, you can set a higher value for MapPoolFlushIntervalSecs.

MapPoolBatchWriteSize	Specify the batch size (and whether to use batch mode). The events are batched into groups and then flushed to disk. To use non-batch mode, set this value to 1. To use batch mode, set this value to greater than 1.	The default batch size is **100,000** events. At the end of flush interval, if the batch capacity is not reached, the batch expires in 30 seconds and all contents of the batch are written to disk as memory pool files. A smaller value for the batch size (for example, 10,000 events) ensures that when events are fetched from disk, they do not pose a risk of bloating the memory, which creates more stability. However, a larger batch size (100,000 events) minimizes the input/output activity when writing events to disk, which can create better performance.
MapPoolMinSize	Minimum size of the memory pool. This value is used for initialization, so it does not typically require editing.	The default value is **10,000** events. A higher value may increase performance. A lower value ensures that the system is more stable.
MapPool Persist Type	This is a view-only parameter that displays the type of optimization used.	The default value is **RMSerialize**.

Note: The effectiveness of this feature depends on your environment. If you write rules that require frequent access of events over a period of time, this feature may degrade performance with no or minimal improvement in scalability.

Note: Memory pool files get deleted when all the events held in the pool file are no longer referenced by an EPL.

Result

For a simple EPL rule, ESA typically improves memory approximately 8 to 9 times.

Configure ESA to Use Capture Time Ordering

This topic tells administrators how to configure the ESA to use capture time ordering when using two or more Concentrators as a source.

By default, ESA uses the ESA time stamp (time at which events are received by the ESA) to correlate events. However, ESA also supports session-ordering based on capture time (the time at which the packet or log event reached the Decoders). This feature is useful if you are correlating events from two or more Concentrators. When you have two or more Concentrators as sources, time ordering ensures that their sessions are correlated together by capture time. This ensures that sessions captured at the same time are correlated together and alerts are consistent with user's expectation even with transmission delays. If any of the sources go offline or are slow to send sessions, the ESA will pause to ensure that sessions with same capture timestamps are correlated together.

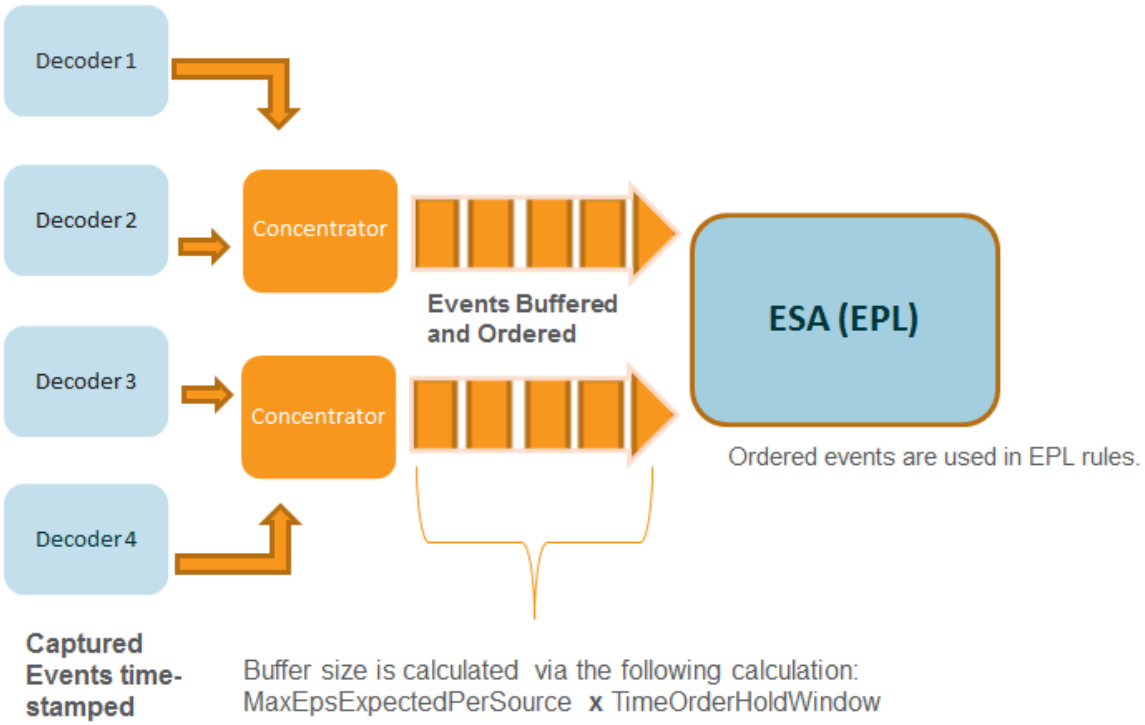
For example, you have two sources with events that occur at 10:00 a.m. Using Capture Time Ordering, these events are held in the buffer until the ESA detects that all events occurring at 10:00 a.m. have been added to the buffer. Once all the events have arrived, events are then processed using EPL rules. This ensures that a rule has all events with the same time-stamp from different sources in order to obtain correct results. If, for example, one Concentrator lags behind another, the ESA pauses until it has all the events time-stamped at 10:00 a.m. from both sources before it runs the EPL rules against the events.

Caution: Although this feature increases accuracy, it impacts performance. The default configuration of the ESA ensures that data is constantly streaming, but because Capture Time Ordering uses a buffer, it takes longer to process events. This is especially true if the ESA must pause for any length of time to wait for the buffer to fill. There are several parameters you can configure (see below) to handle this situation; however, there may still be performance impact.

By default, this feature is disabled.

Capture Time Order Workflow

The following diagram shows the workflow when Capture Time Ordering is enabled.



1. Events are time-stamped as they are captured by the Decoder.
2. After Concentrator processing, events are buffered and ordered. The buffer size is calculated via two parameters MaxEPSExpectedPerSource (the maximum volume of traffic (EPS) you expect **per source** for the ESA to receive) times TimeOrderHoldWindow(the amount of time to allow for events to arrive from all sources).
3. The ordered events are then correctly correlated in EPL rules.

Prerequisites

Two or more Concentrators must be configured as a data source in ESA.

When the **StreamEnabled** parameter is set to true, it is important that all the machines running Core Services should be in NTP Sync.

Procedures

The following procedures tell you how to enable and configure Capture Time Ordering.

Enable Buffering and Capture Time Ordering

Note: After an upgrade or in a high EPS environment, you need to re-add datasources to start seeing the benefits. Or, you must wait until the sessions catch up before you enable Capture Time Ordering.

1. In the Security Analytics menu, select **Administration** > **Services**. Select your ESA service and then  > **View** > **Explore**.
2. Go to **Workflow** > **Source** > **nextgenAggregationSource**.
3. Set the **StreamEnabled** attribute to **true**. StreamEnabled allows ESA to buffer events received from Concentrators.
4. Set the **TimeOrdered** attribute to **true**. This enables the buffered events to be ordered by the time stamp from the Concentrator.

Configure Capture Time Ordering

When you work with Capture Time Ordering, you need to configure several other parameters to ensure performance. The following table shows parameters and their function. Configuring these parameters requires knowledge of your traffic volume and rate.

Note: If you do not know your traffic volume or latency, consult with your Professional Services representative before configuring this feature.

MaxEPSExpectedPerSource	Specify the maximum volume of traffic (EPS, or events per second) you expect for the ESA service to receive from your busiest source (for example, if one source receives 20K EPS, and another receives 25K EPS, set the value at 25K EPS). If you set this rate too low, there is a short-term impact on performance. However, ESA automatically increases the value for `MaxEPSExpectedPerSource` as needed to make progress in Time Ordered mode. The default value is 20K.

TimeOrderHoldWindow	Specify in seconds (whole integers) the amount of time to allow for events to arrive from all sources. Configure this value based on the latency between the sources. The default value is 2 seconds. Decreasing this value can increase the chance of dropped events. Increasing this value can decrease performance because more memory is consumed.
IdleSourceAdvanceAfterSeconds	Specify the interval (in seconds) after which the ESA takes an idle source (no events are coming from the source, but the source is not offline) out of the equation to allow progress on a capture time ordered stream. The default value is 0, meaning that the ESA waits indefinitely for events to arrive.
OfflineSourceAdvanceAfterSeconds	Specify the interval (in seconds) after which the ESA takes an offline source out of the equation to allow progress on a capture time ordered stream. The default value is 0, which means the ESA waits indefinitely. This parameter does not affect the re-connection retries; those which are performed in all cases.

Troubleshooting Tips

Using this feature, it is possible to encounter a situation where events become backlogged. To fix this issue, you can perform one of the following options.

Disable Capture Time Ordering

1. In the Security Analytics menu, select **Administration** > **Services**. Select your ESA service and then  > View > Explore.
2. Go to **Workflow** > **Source** > **nextgenAggregationSource**.
3. Set the StreamEnabled attribute to false.
4. Set the TimeOrdered attribute to false.

If you disable Capture Time Ordering, you will lose the backlogged data, and events will no longer be ordered by capture time.

Disable Position Tracking

Position tracking allows ESA to track where it stopped processing events if the ESA stops or is shut down. Position tracking is enabled by default with Capture Time Ordering. If you disable position tracking, this allows ESA to skip the backlogged events. For example, if the ESA goes down at 7:00 a.m., and you restart it at 11:00 a.m. with position tracking disabled, the ESA will start processing events that occurred at 10:55 a.m. With position tracking enabled, the ESA will start processing events at the point at which it stopped.

1. In the Security Analytics menu, select **Administration** > **Services**. Select your ESA service and then  > **View** > **Explore**.
2. Go to **Workflow** > **Source** > **nextgenAggregationSource**.
3. Set the **PositionTrackingEnabled** attribute to false.

If you disable Position Tracking, you will lose the backlogged data, but going forward, events will be ordered by capture time.

Start, Stop, or Restart ESA Service

This topic provides instructions to start, stop, or restart Event Stream Analysis service.

Start ESA Service

Before you start:

- Make sure that MongoDB is running.
- If the MongoDB service is not running, use the following command to start the MongoDB service:
  ```
  service tokumx start
  ```

To start ESA service:

1. Use ssh to connect to the ESA service and log in as the root user.
2. Type the following command and press ENTER:
   ```
   service  rsa-esa start
   ```

Stop ESA Service

To stop ESA service:

1. Use ssh to connect to the ESA service and log in as the root user.
2. Type the following command and press ENTER:
   ```
   service rsa-esa stop
   ```

Restart ESA Service

To restart ESA service:

1. Use ssh to connect to the ESA service and log in as the root user.
2. Type the following command and press ENTER:
   `service rsa-esa restart`

Audit Logs and Verify ESA Component Versions and Status

This topic provides details about audit logging and instructions to verify the versions of the Event Stream Analysis components installed.

Audit Log Rules

Audit logging allows you to view details about rules that are created and edited in Security Analytics.

For details on how to access your audit logs, see Local Audit Log Locations in the System Configuration Guide.

The following sample shows a create, update, and delete log for a given rule.

- **Create log example:** 2016-03-10 14:19:37,951 deviceVersion: "10.6.1.0-SNAPSHOT" deviceService: "EVENT_STREAM_ANALYSIS" category: SYSTEM operation: **"CREATE RULE"** parameters: "Epl Module Identifier: 56e1f2adbee8290008241296, Esper Instance: default, Rule Enabled: true, Trial Rule: false " key: "Epl Rule: @RSAAlert select * from Event;" identity: "admin" userRole: "ROLE_ESA_ADMINISTRATOR"
- **Update log example:** 2016-03-10 14:19:37,951 deviceVersion: "10.6.1.0-SNAPSHOT" deviceService: "EVENT_STREAM_ANALYSIS" category: SYSTEM operation: **"UPDATE RULE"** parameters: "Epl Module Identifier: 56e1f2adbee8290008241296, Esper Instance: default, Rule Enabled: true , Trial Rule: false " key: "Epl Rule: @RSAAlert select * from Event;" identity: "admin" userRole: "ROLE_ESA_ADMINISTRATOR
- **Delete log example:** 2016-03-10 14:19:37,951 deviceVersion: "10.6.1.0-SNAPSHOT" deviceService: "EVENT_STREAM_ ANALYSIS"category: SYSTEM operation: **"DELETE RULE"** parameters: "Epl Module Identifier: 56e1f2adbee8290008241296, Esper

```
Instance: default, Rule Enabled: true , Trial Rule: false "
key: "Epl Rule: @RSAAlert select * from Event;" identity:
"admin" userRole: "ROLE_ESA_ADMINISTRATOR "
```

Each log contains the following parameters:

- Time stamp: Time the rule was modified. Example: 2016-03-10 14:19:37,951
- DeviceVersion: Version of your ESA device. Example: "10.6.1.0-SNAPSHOT"
- DeviceService: Example: EVENT_STREAM_ANALYSIS
- Category: Example: SYSTEM
- Operation:Example:DELETE/CREATE/UPDATE RULE
- Parameters:Placeholder for the following keys:
- Epl Module Identifier: unique identifier for the rule. Example: 56e1f2adbee8290008241296
- Esper Instance: Esper instance on which rule is deployed. Example: default
- Rule Enabled: Displays if the rule is enabled or not. Example: Rule Enabled: true
- Trial Rule: Displays if the rule is configured as a trial rule or not. Example: Trial Rule: false
- Epl Rule: Displays the rule syntax. Example:

  ```
  @RSAAlert select * from Event;" identity: "admin" userRole:
  "ROLE_ESA_ADMINISTRATOR+ROLE_ESA_ADMINISTRATOR+ROLE_ESA_ADMIN"
  ```

- Identity: Example: “admin"
- userRole: Example: "ROLE_ESA_ADMINISTRATOR"

Note: When a rule is disabled, two logs are generated for the same rule. First a ‘Delete Rule’ [Rule enabled attribute = true] audit log is created, followed by a ‘Create Rule’ [Rule enabled attribute =false] audit log.

Verify ESA Server Version

To verify the ESA Server version:

1. Use ssh to connect to the ESA service and log in as the root user.
2. Type the following command and press ENTER:

   ```
   rpm -qa | grep rsa-esa-server
   ```

   The ESA server version is displayed.

Verify MongoDB Version

To verify the MongoDB version:

1. Use ssh to connect to the ESA service and log in as the root user.
2. Type the following command and press ENTER:
   ```
   mongo --version
   ```
   The MongoDB version is displayed.

Verify MongoDB Status

To verify the MongoDB status:

1. Use ssh to connect to the ESA service and log in as the root user.
2. Type the following command and press ENTER:
   ```
   service tokumx status
   ```
3. Run the following command if MongoDB is not running.
   ```
   service tokumx start
   ```

Troubleshooting

Error Trying to Deploy ESA Rule with Custom Meta	1. Created a custom meta key to enrich rule results and used that key in an ESA rule. 2. Deployed rule, but received error.
Cause	ESA schema is not updated with the custom meta.
Recommended Action	Restart ESA service.
Test Connection fails while updating Schema in ESA	1. Created a custom meta key using custom feed. 2. Test connection fails while updating schema in ESA.
Cause	Lost connection to the Concentrator or ESA services.
Recommended Action	Complete one of the following actions: • Restart the ESA service • Delete the Concentrator data source from the ESA service and add it back to the ESA service.
When an All In One host is deployed, ESA cannot connect to the Concentrator	On the **ESA > Config page > Data Sources** tab, when you try to add a Concentrator service running on an All In One installation, the following error condition occurs: `com.rsa.net-witness.carlos.transport.TransportException`
Cause	When an AIO host (either Packet or Log) is deployed, SA automatically assigns the loopback address 127.0.0.1 to the AIO host.
Recommended Action	1. On the **Administration > Host** page, manually create a new host using the AIO host's fixed IP address (for example, 10.10.10.10). 2. The Concentrator service on the host should be automatically added to the **Administration > Services** page. If not, manually create the Concentrator service. 3. On the **Administration > Service > ESA > Config > Data Sources** tab, click the plus sign (+) to add the Concentrator service that is mapped to the fixed IP address.

References

This topic is a collection of references, which describe the user interface for ESA in Security Analytics. These topics are presented in alphabetical order.

Use this section when you are looking for descriptions of the entitlements user interface and definitions of the features of the user interface.

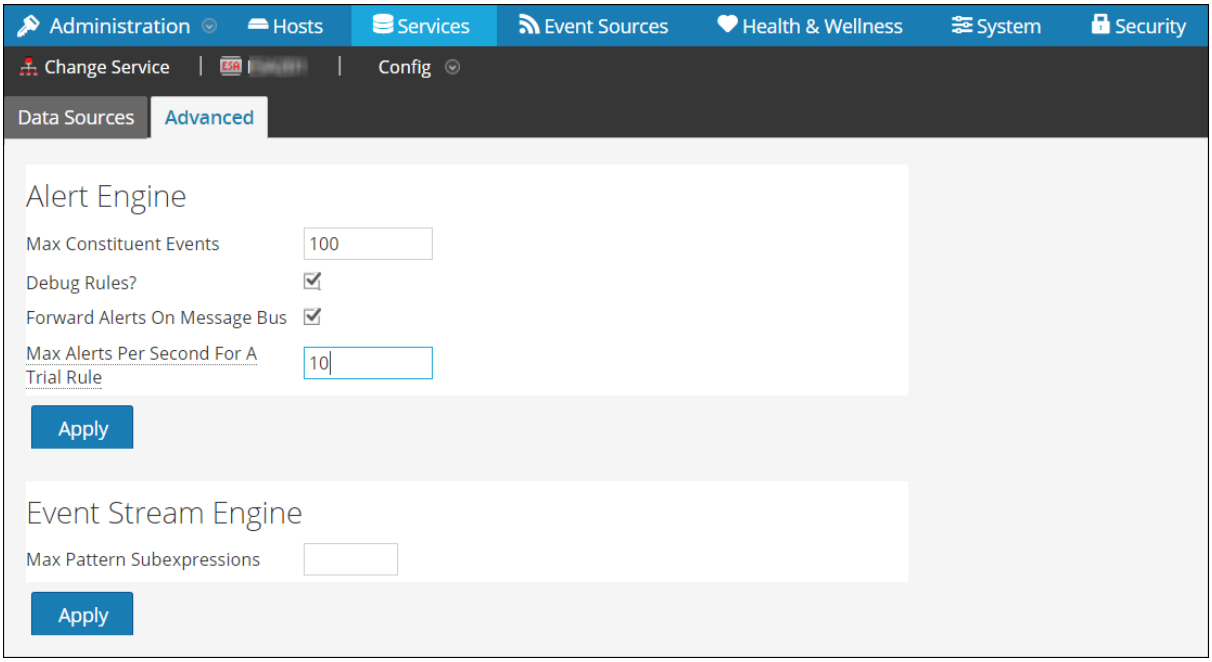
See the following sections for details:

- Services Config View Advanced Tab
- Services Config View Data Sources Tab

Services Config View Advanced Tab

This topic describes the components of the Services Config view Advanced tab for ESA.

If you want to configure advanced settings for an ESA service, you can do that from the **Services Config view > Advanced** tab of the ESA.



Features

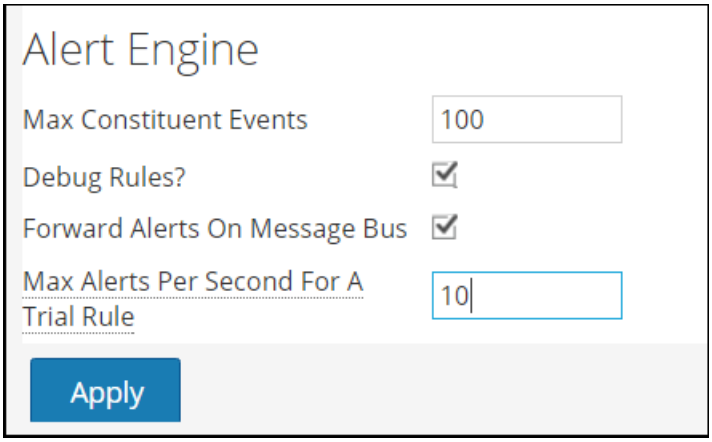
The following are the sections in the Advanced view:

- Alert Engine
- Event Stream Engine

Alert Engine Settings

In the Alert Engine section, you specify values to preserve events for rules that choose multiple events.

The following figure shows the Alert Engine section.



The following table lists the parameters in the Alert Engine section and their descriptions.

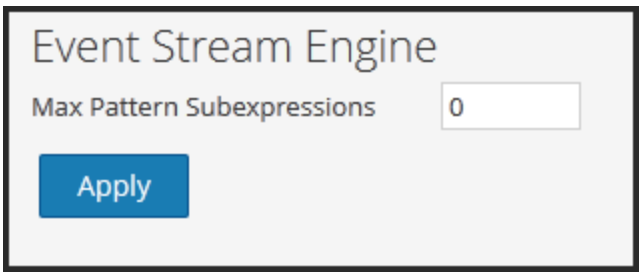
Parameter	Description
Max Constituent Events	For rules that choose multiple events, this configuration value decides how many of the associated events are preserved. For example, if a rule fires an alert with 200 associated events and this parameter is set to 100, only the first 100 are preserved by ESA, the rest are dropped. The default value is **100**.
Debug Rules?	Selecting enables debugging rules.
Forward Alerts On Message Bus	To forward ESA alerts for Incident Management, you must select this option. The ESA alerts generated will be sent to the Message Bus and subsequently to Incident Management. This option is selected by default. You may want to ensure that the Incident Management service is running.

Parameter	Description
Max Alerts Per Second for a Trial Rule	You can specify the maximum number of alerts to be forwarded to the Message Bus for the trial rule. For example, if the value is set to **50**, only 50 alerts will be forwarded to the Message Bus for the trial rule. If the value is set to **0**, then the alerts generated by the trial rule will not be forwarded to the Message Bus. The default value is **10**.

Event Stream Engine Settings

In the Event Stream Engine section, you specify details to improve performance.

The following figure shows the Event Stream Engine section.



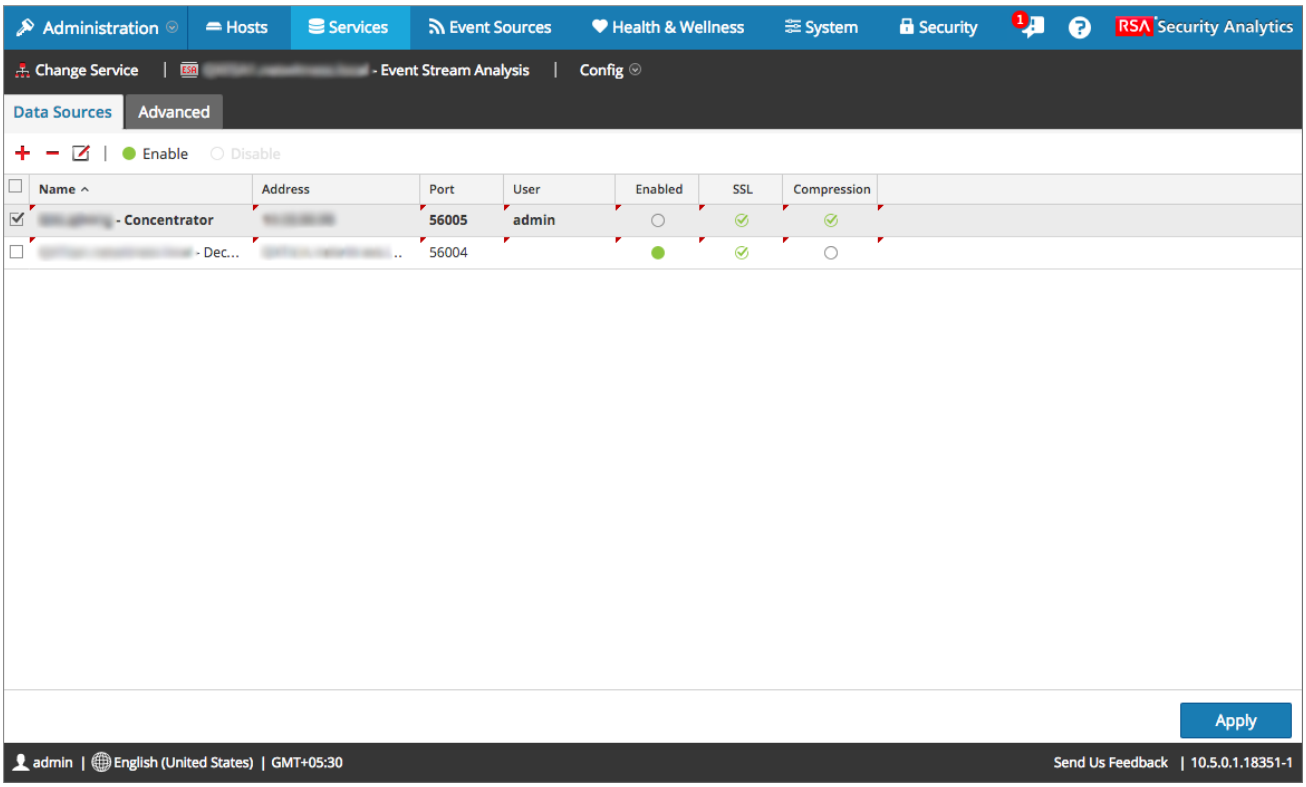
The following table lists the parameter in the Event Stream Engine section and its description.

Parameter	Description
Max Pattern Subexpressions	Certain rules require ESPER to maintain subexpressions in memory before deciding to fire them or not. These subexpressions consume memory and if left unchecked may cause the service to go down with memory exhaustion. This parameter is a safety measure that keeps such memory hogging rules under check. If a rule exceeds the specified number of subexpressions, its processing is delayed. The default value is **0** which means this setting is disabled. You must set a value if there are service stability issues.

Services Config View Data Sources Tab

This topic describes the components of the Services Config view Data Sources tab for ESA.

The **Services Config view > Data Sources** tab of the ESA is used to configure data sources for ESA.



Features

The following are the sections in the Data Source tab:

- Toolbar
- Data Source grid

Toolbar

The following table describes the options in the toolbar.

Parameter	Description
+	Adds a new data source to ESA.
−	Deletes a data source from ESA.
	Edits a data source. You must have the username and password credentials for the service in order to make changes.
Enable	Enables the selected data source.

Parameter	Description
Disable	Disables the selected data source.

Data Source Grid

In the Data Source grid, all data sources which have been added to the ESA service are displayed. The following table describes the parameters in the Data Source grid.

Parameter	Description
Name	The name of the data source service.
Address	The address of the data source service.
Port	The port used by the data source.
User	The user connected with the data source.
Enabled	Indicates if the data source is enabled.
SSL	Indicates if SSL communication is enabled.
Compression	Indicates if compression is enabled.