# RSA Ready Implementation Guide for RSA Security Analytics

# MapR Converged Data Platform 3.1

Jeffrey Carlson, RSA Partner Engineering

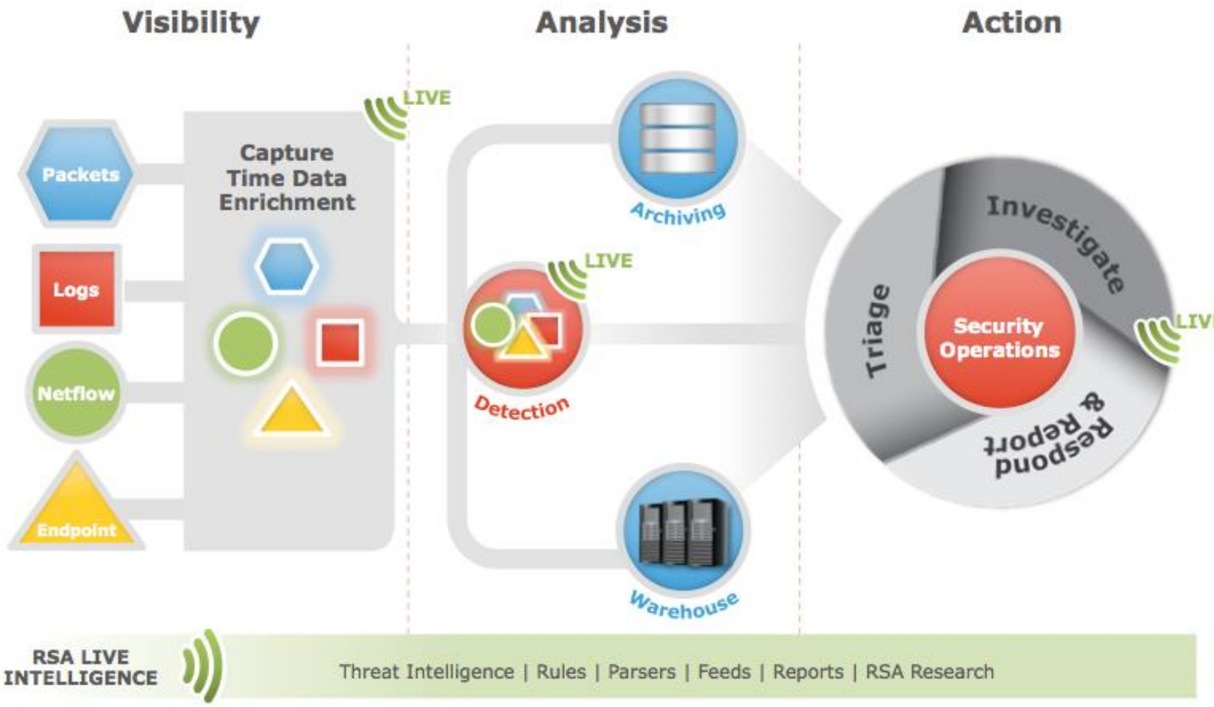
Last Modified: 02/25/2016

RSA READY

## Solution Summary

RSA Analytics Warehouse provides the capacity to process large amounts of current and longer term data through a Hadoop-based distributed computing system that collects, manages, and enables advanced analytics and reporting on Security Analytics data. RSA Analytics Warehouse requires a service called Warehouse Connector to collect metadata and events from Decoder and Log Decoder and write them in Avro format into a Hadoop-based distributed computing system. For more information on the Warehouse Connector, see the Warehouse Connector Overview section of the Security Analytics documentation.

The Warehouse can be made up of three or more nodes depending on the organization's analytic, archiving, and resiliency requirements.



# MapR Cluster Configuration

## *Before You Begin*

This section provides instructions for configuring the MapR Warehouse with RSA Security Analytics. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All MapR components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

**! Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure the MapR cluster is properly configured and secured before deploying to a production environment. For more information, please refer to the MapR documentation or website.**

## *MapR Cluster Configuration*

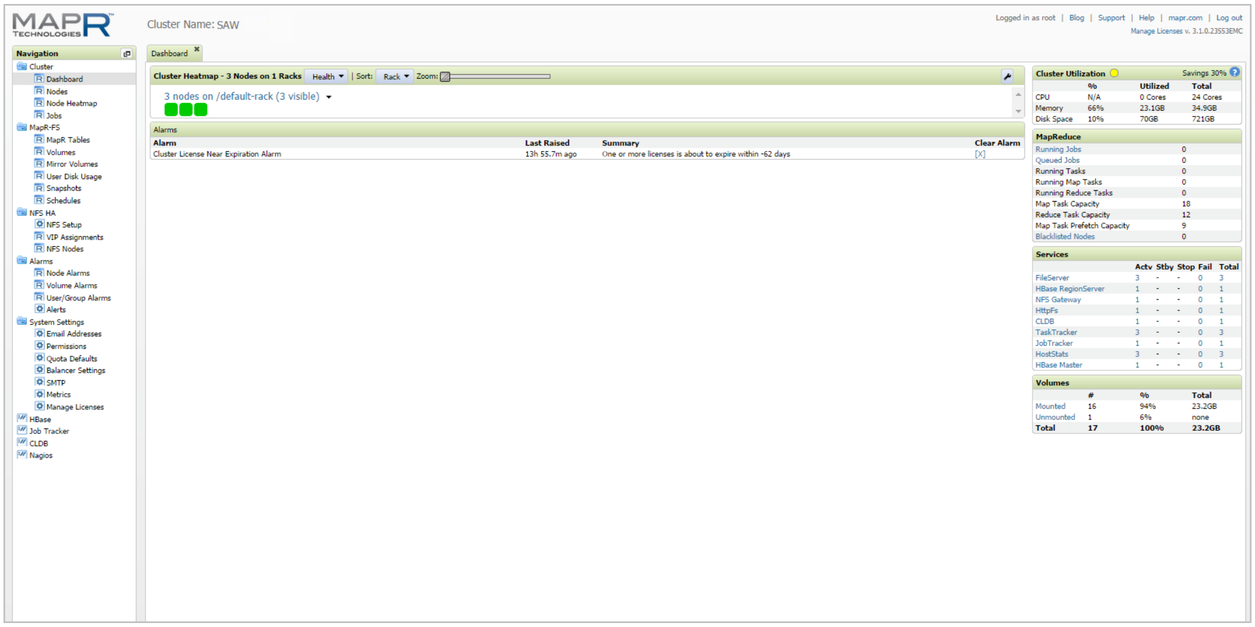
The RSA Analytics Warehouse is based on the version 3.1 distribution of MapR. For a comprehensive set of instructions for configuring the Warehouse, consult the RSA Analytics Warehouse (MapR) Configuration Guide found at:

**https://sadocs.emc.com/0_en-us/090_10.4_User_Guide/120_ApplServConf/WHMapRConfGd**

Once the cluster is installed, you may need to create a virtual IP address for the Warehouse cluster. To do so, perform the following steps:

## Create a Virtual IP Address

1. Log on to the MapR Control System.



Alarms

| Alarm | Last Raised | Summary | Clear Alarm |
|---|---|---|---|
| Cluster License Near Expiration Alarm | 13h 55.7m ago | One or more licenses is about to expire within -62 days | [X] |

Cluster Utilization — Savings 30%

| | % | Utilized | Total |
|---|---|---|---|
| CPU | N/A | 0 Cores | 24 Cores |
| Memory | 66% | 23.1GB | 34.9GB |
| Disk Space | 10% | 70GB | 721GB |

| MapReduce | |
|---|---|
| Running Jobs | 0 |
| Queued Jobs | 0 |
| Running Tasks | 0 |
| Running Map Tasks | 0 |
| Running Reduce Tasks | 0 |
| Map Task Capacity | 18 |
| Reduce Task Capacity | 12 |
| Map Task Prefetch Capacity | 9 |
| Blacklisted Nodes | 0 |

Services

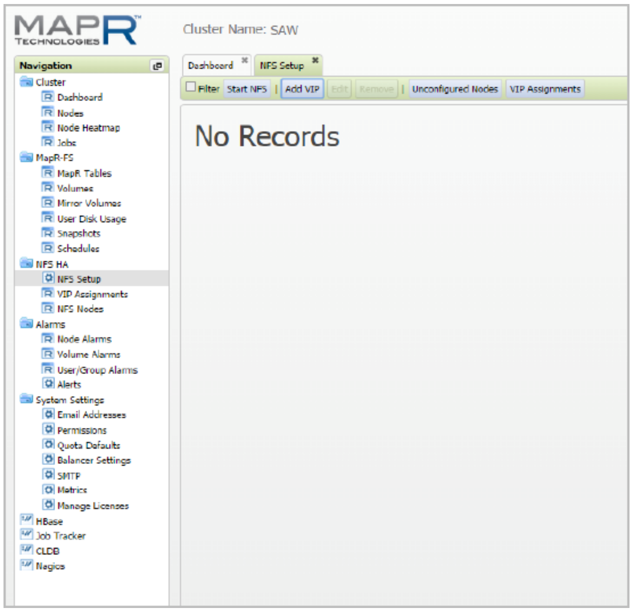
| | Actv | Stby | Stop | Fail | Total |
|---|---|---|---|---|---|
| FileServer | 3 | - | - | 0 | 3 |
| HBase RegionServer | 1 | - | - | 0 | 1 |
| NFS Gateway | 1 | - | - | 0 | 1 |
| HttpFs | 1 | - | - | 0 | 1 |
| CLDB | 1 | - | - | 0 | 1 |
| TaskTracker | 3 | - | - | 0 | 3 |
| JobTracker | 1 | - | - | 0 | 1 |
| HostStats | 3 | - | - | 0 | 3 |
| HBase Master | 1 | - | - | 0 | 1 |

Volumes

| | # | % | Total |
|---|---|---|---|
| Mounted | 16 | 94% | 23.2GB |
| Unmounted | 1 | 6% | none |
| **Total** | **17** | **100%** | **23.2GB** |

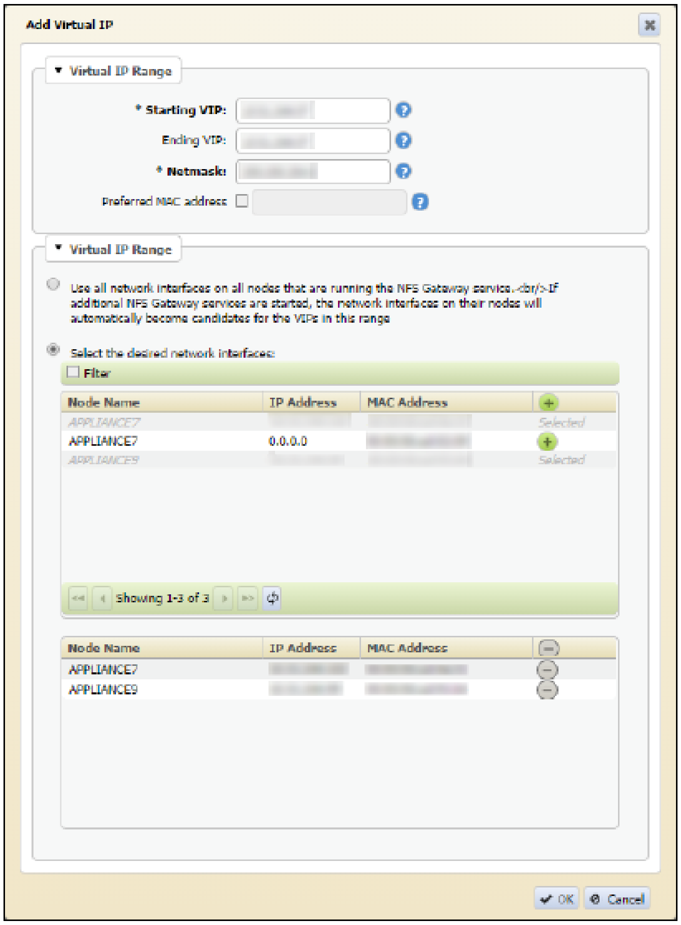
2. In the Navigation pane, select **NFS HA > NFS Setup**. The NFS Setup tab is displayed. The NFS Setup tab enables you to edit, remove or add VIPs in the Warehouse cluster.

3. On the NFS Setup tab, click the **Add VIP** button.



No Records

The Add Virtual IP dialog is displayed.



Add Virtual IP

▾ Virtual IP Range

* Starting VIP: [redacted]

Ending VIP: [redacted]

* Netmask: [redacted]

Preferred MAC address □

▾ Virtual IP Range

○ Use all network interfaces on all nodes that are running the NFS Gateway service.<br/>If additional NFS Gateway services are started, the network interfaces on their nodes will automatically become candidates for the VIPs in this range

● Select the desired network interfaces:

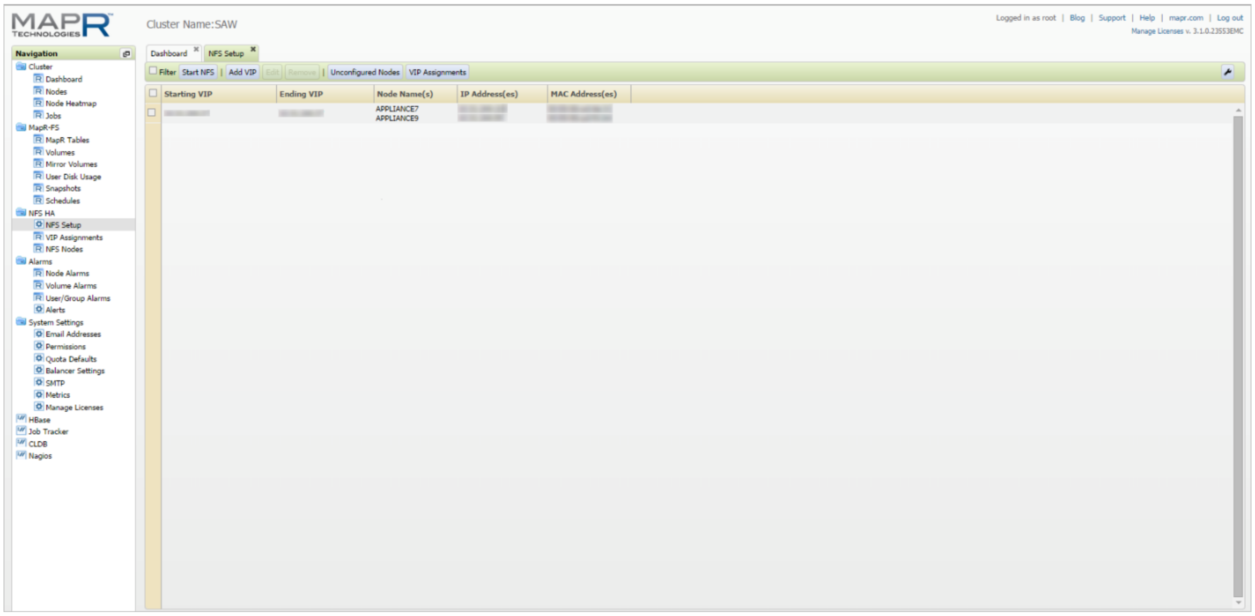
□ Filter

| Node Name | IP Address | MAC Address | + |
|---|---|---|---|
| APPLIANCE7 | [redacted] | [redacted] | Selected |
| APPLIANCE7 | 0.0.0.0 | [redacted] | + |
| APPLIANCE9 | [redacted] | [redacted] | Selected |

Showing 1-3 of 3

| Node Name | IP Address | MAC Address | ⊖ |
|---|---|---|---|
| APPLIANCE7 | [redacted] | [redacted] | ⊖ |
| APPLIANCE9 | [redacted] | [redacted] | ⊖ |

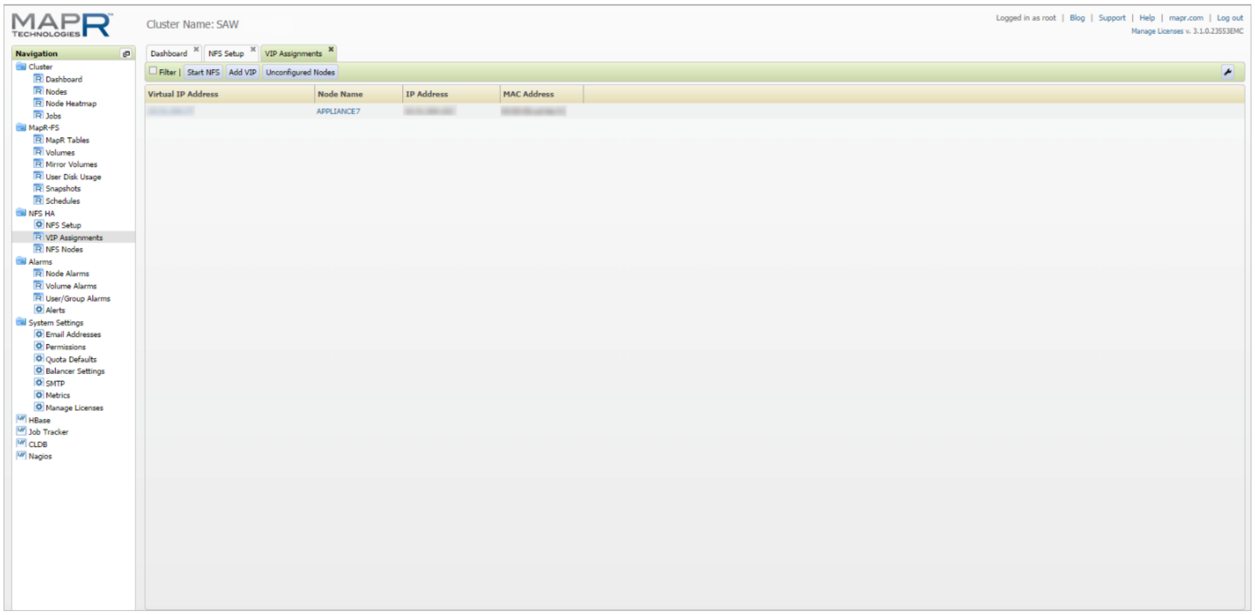
4. In the **Add Virtual IP** dialog, do the following:
   a. In the **Starting VIP** field, type the starting IP Address for VIP.
   b. In the **Ending VIP** field, type the ending IP Address for VIP. If this field is left blank, only one IP address is used for VIP allocation.
   c. In the **Netmask** field, type the Netmask for the deployment.
   d. Select **Select Desired Network Interfaces** to choose the available Network Interfaces that need to be used for VIP assignment. Select all of the external Interfaces from the list of available nodes by clicking the plus button next to the interface entry. Selected Interfaces will appear in the bottom list.
   e. Click **OK** to add the VIP.
   f. The newly added VIP appears in the list on the NFS Setup tab.



| ☐ | Starting VIP | Ending VIP | Node Name(s) | IP Address(es) | MAC Address(es) |
|---|---|---|---|---|---|
| ☐ | [redacted] | [redacted] | APPLIANCE7<br>APPLIANCE9 | [redacted] | [redacted] |

VIP allocation can also be removed or edited from the NFS HA > NFS Setup tab by selecting a VIP and clicking the Edit or Remove button.

5. In the Navigation pane, select NFS HA > VIP Assignment to view the node that is assigned to the newly added VIP.



| Virtual IP Address | Node Name | IP Address | MAC Address |
|---|---|---|---|
| [redacted] | APPLIANCE7 | [redacted] | [redacted] |

# RSA Security Analytics Configuration

Please consult the latest Warehouse Connector Configuration Guide on sadocs.emc.com.  As of SA 10.5 it can be found here:

https://sadocs.emc.com/0_en-us/089_105InfCtr/120_AppSerCon/WaConCon

It is assumed before performing the following steps that the Warehouse Connector Appliance has been installed and is communicating properly with the rest of your Security Analytics Infrastructure.

Step 1: Create the Lockbox

Step 2: Configure the Data Source

Step 3: Mount the Warehouse on the Warehouse Connector (NFS)

Step 4: Configure the Destination Using NFS

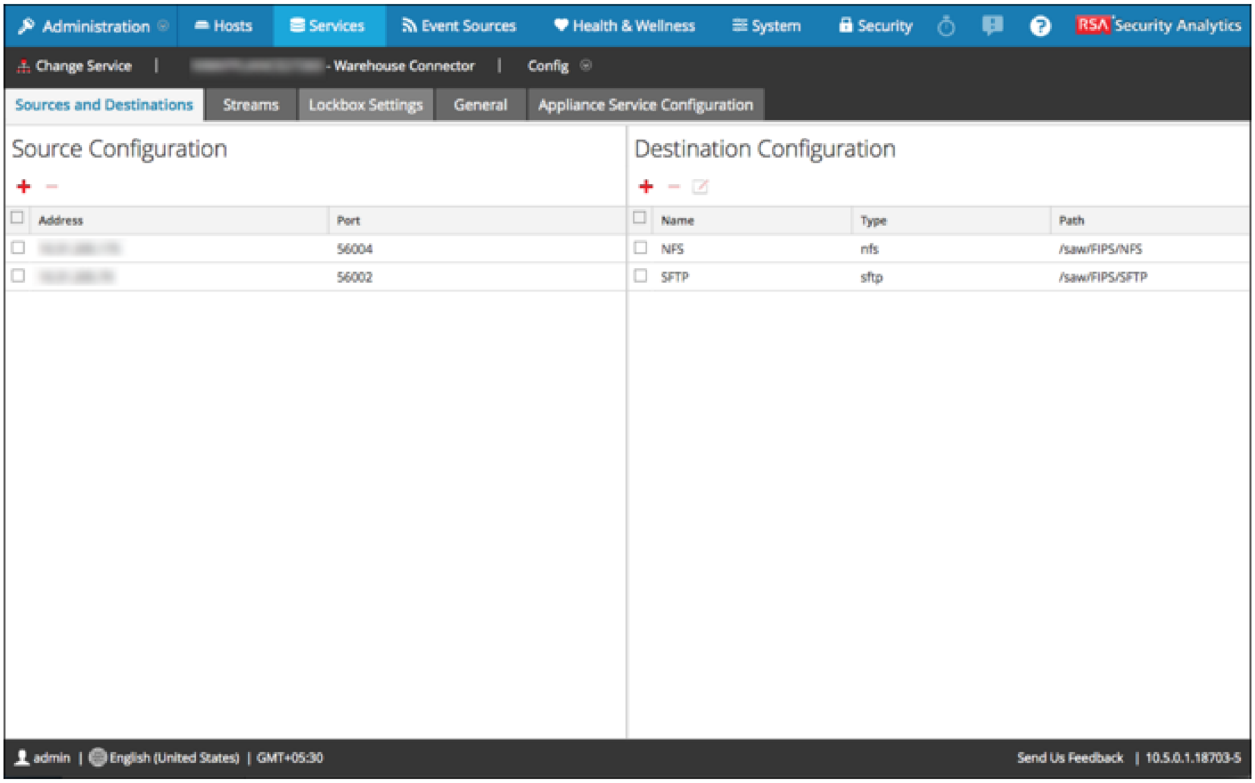
Step 5: Configure Streams

## *Create the Lockbox*

To set the Lockbox password, perform the following steps:

1. Log on to Security Analytics.
2. In the Security Analytics menu, select **Administration > Services**.
3. In the Services view, select the added Warehouse Connector service, and ⚙ > View > Config.

   The Services Config view of Warehouse Connector is displayed.



Source Configuration

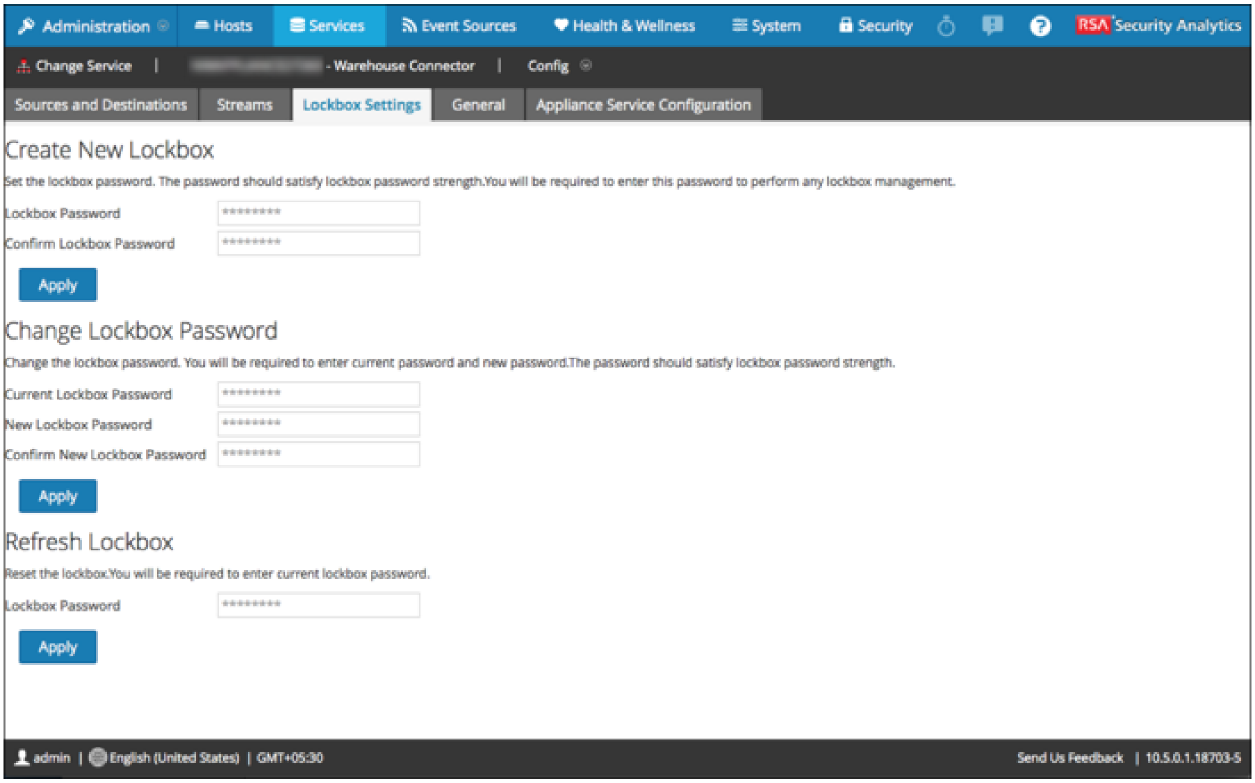
| □ | Address | Port |
|---|---|---|
| □ | [redacted] | 56004 |
| □ | [redacted] | 56002 |

Destination Configuration

| □ | Name | Type | Path |
|---|---|---|---|
| □ | NFS | nfs | /saw/FIPS/NFS |
| □ | SFTP | sftp | /saw/FIPS/SFTP |

admin | English (United States) | GMT+05:30
Send Us Feedback | 10.5.0.1.18703-5

4. Click the **Lockbox Settings** tab.



Create New Lockbox

Set the lockbox password. The password should satisfy lockbox password strength.You will be required to enter this password to perform any lockbox management.

Lockbox Password ********

Confirm Lockbox Password ********

Change Lockbox Password

Change the lockbox password. You will be required to enter current password and new password.The password should satisfy lockbox password strength.

Current Lockbox Password ********

New Lockbox Password ********

Confirm New Lockbox Password ********

Refresh Lockbox

Reset the lockbox.You will be required to enter current lockbox password.

Lockbox Password ********

5. In the **Create New Lockbox** section, perform the following:
   a. In the Lockbox Password field, enter the new lockbox password.

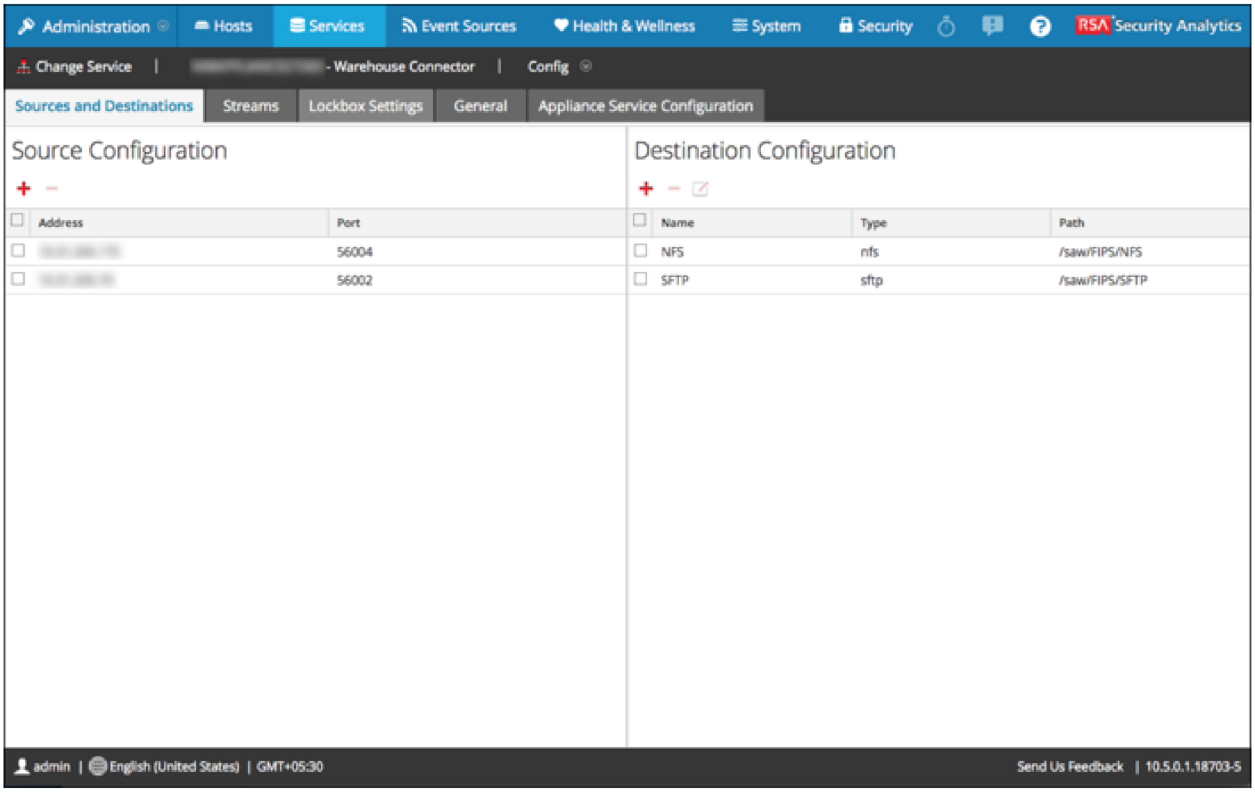
   **! > Important: The lockbox password must be at least eight characters in length and they must contain at least three of the following groups: one uppercase character [A-Z], one lowercase character [a-z], one numeral [0-9], and one special character.**

   b. In the **Confirm Lockbox Password** field, enter the added lockbox password to confirm.
   c. Click **Apply**.

## *Configure the Data Source*

To configure the data source perform the following steps:

1. Log on to Security Analytics.
2. In the **Security Analytics** menu, select **Administration > Services**.
3. In the Services view, select the added Warehouse Connector service, and ⚙ ⌄ **> View > Config**. The Services Config view of Warehouse Connector is displayed.



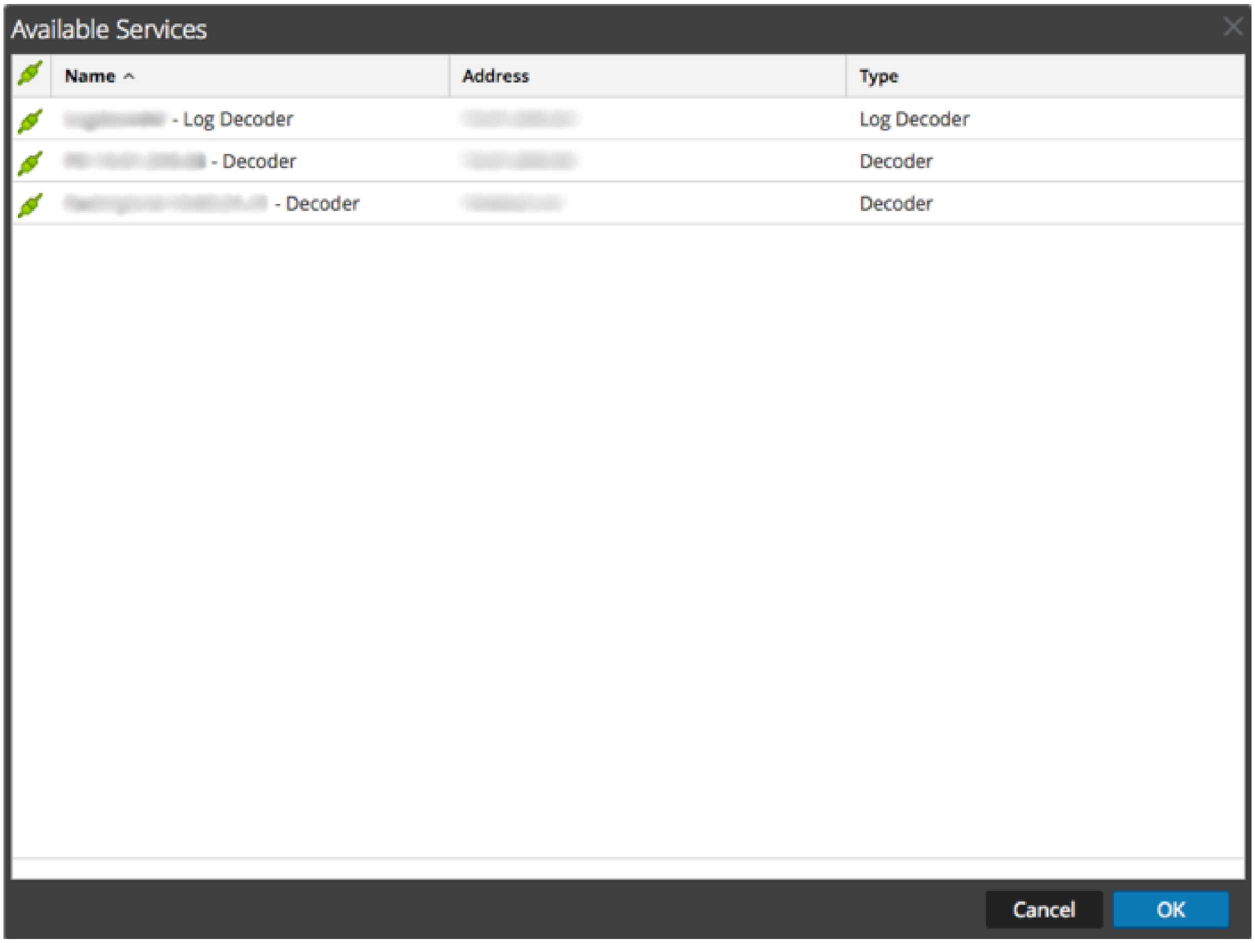
Source Configuration

| □ | Address | Port |
|---|---|---|
| □ | [redacted] | 56004 |
| □ | [redacted] | 56002 |

Destination Configuration

| □ | Name | Type | Path |
|---|---|---|---|
| □ | NFS | nfs | /saw/FIPS/NFS |
| □ | SFTP | sftp | /saw/FIPS/SFTP |

4. On the **Sources and Destinations** tab, in the **Source Configuration** section, click **+**.



Available Services

| | Name ^ | Address | Type |
|---|---|---|---|
| | [redacted] - Log Decoder | [redacted] | Log Decoder |
| | [redacted] - Decoder | [redacted] | Decoder |
| | [redacted] - Decoder | [redacted] | Decoder |

5. In the **Available Services** dialog, select the Log Decoder or Decoder services that you want to add as source to the Warehouse Connector service and click **OK**.

   The selected Log Decoder and Decoder services should now be listed in the **Source Configuration** section.

### Mount the Warehouse on the Warehouse Connector

Perform the following steps to mount the MapR cluster on the appliance where you have installed the Warehouse Connector service.

1. To create a new directory named /saw, enter the following command:

   ```
   mkdir /saw
   ```

2. Enter the following command:

   ```
   ll /
   ```

   The new directory is displayed.

3. To mount the Warehouse, enter the following command:

```
mount -t nfs -o nolock,tcp,hard,intr <IP_Address_for_cluster>:/mapr/<cluster-
name> /saw
```

Where <IP_Address_for_cluster> is the IP address of the primary appliance in the cluster and <cluster-name> is the name provided in the template file.

**! Important: If a virtual IP address is configured for the Warehouse, you have to use it as the IP address in <IP_Address_for_SAW>.**

4. To verify if the Warehouse is mounted successfully, enter the following command:

   ```
   mount
   ```

   The IP address of the primary Warehouse appliance and other details you have provided in step 3 appear in the last line of the output message.

5. To list the content in the newly created directory, /saw, enter the following command:

   ```
   ll /saw
   ```

   The following directories are displayed:

   ```
   hbase
   index-scratch
   jars
   logs
   user
   var
   ```

6. To add NFS to the Auto-mount options. Do the following:

   a. To check if the IP address of the primary Warehouse appliance and other details you have provided while mounting Warehouse appears in /etc/fstab, enter the following command:

      ```
      cat /etc/fstab
      ```

      If the detail does not appear in the /etc/fstab file, perform the following steps.

   b. Enter the following command:

      ```
      tail -n 1 /etc/mtab
      ```

      The IP address of the primary Warehouse appliance and other details you provided while mounting Warehouse appear in the last line of the output message.

   c. Enter the following command:

      ```
      tail -n 1 /etc/mtab >> /etc/fstab
      ```

   d. Edit the /etc/fstab file to add the word 'auto' at the end of the file. Enter the following command:

      ```
      vi /etc/fstab
      ```

      For example,

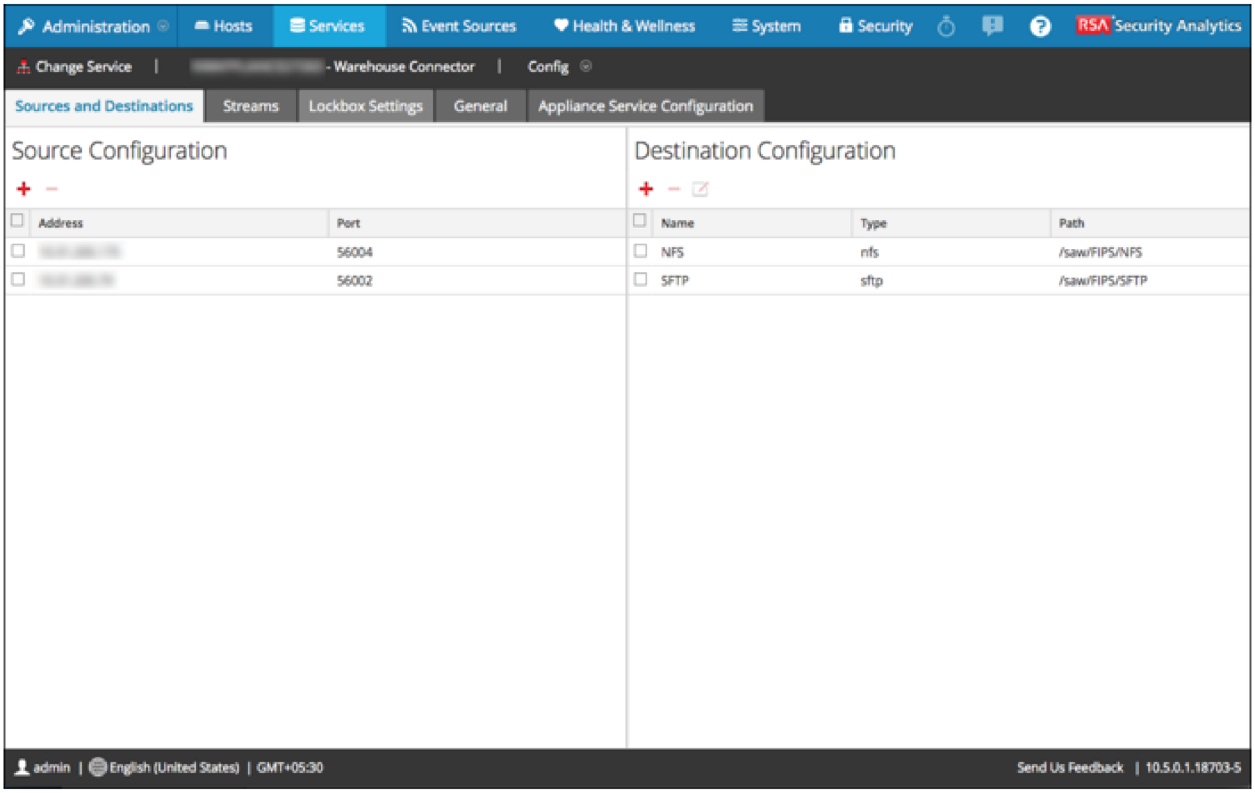
```
10.11.111.11:/mapr/saw /saw nfs rw,nolock,tcp,auto,addr=10.11.111.11 0 0
```

## Configure the Destination Using NFS

The MapR cluster supports connections via NFS, perform the following steps in to configure the NFS destination:

1. Log on to Security Analytics.
2. In the **Security Analytics** menu, select **Administration > Services**.
3. In the Services view, select the Warehouse Connector service, and ⚙ ⌄ **> View > Config**.

   The Services Config View of Warehouse Connector is displayed.



[redacted] - Warehouse Connector | Config

Source Configuration

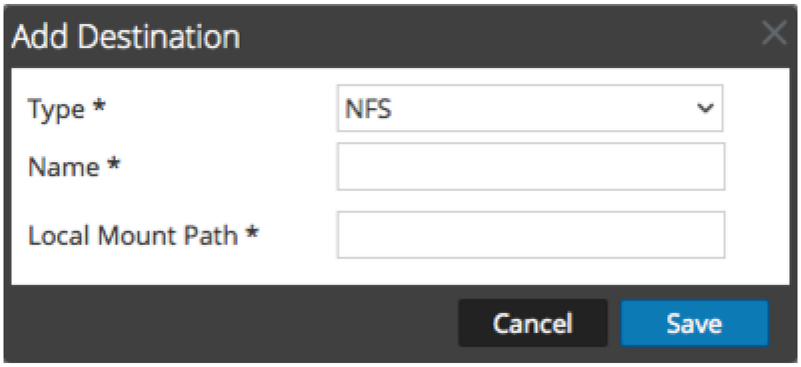
| □ | Address | Port |
|---|---|---|
| □ | [redacted] | 56004 |
| □ | [redacted] | 56002 |

Destination Configuration

| □ | Name | Type | Path |
|---|---|---|---|
| □ | NFS | nfs | /saw/FIPS/NFS |
| □ | SFTP | sftp | /saw/FIPS/SFTP |

admin | English (United States) | GMT+05:30 Send Us Feedback | 10.5.0.1.18703-5

4. On the **Sources and Destinations** tab, in the **Destination Configuration** section, click +
5. In the **Add Destination** dialog, select **NFS** from the **Type** drop-down list.



Add Destination

Type * NFS

Name *

Local Mount Path *

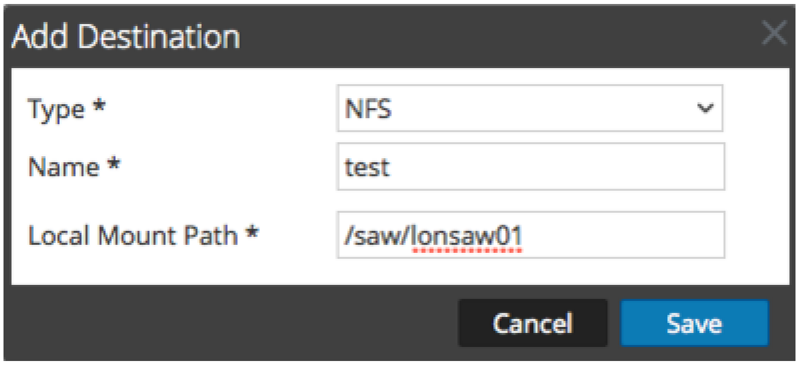
6. In the **Name** field, enter a unique symbolic name for the destination.

   **! Important: The Name field does not support space or special characters except underscore (_).**

7. In the **Local Mount Path** field, enter the locally mounted directory for HDFS where you want the Warehouse Connector to write the data.

   For example:

   If /saw is the local mount point for HDFS that you have configured while mounting the mapr NFS cluster on the host where you have installed the Warehouse Connector service to write to RSA Analytics Warehouse (MapR), create a directory named Ionsaw01 under /saw and the corresponding Local Mount Path for the destination would be /saw/Ionsaw01.

   Add Destination

   Type * NFS

   Name * test

   Local Mount Path * /saw/lonsaw01

   The /saw mount point implies to / as the root path for HDFS. The Warehouse Connector writes the data to /Ionsaw01 in HDFS.

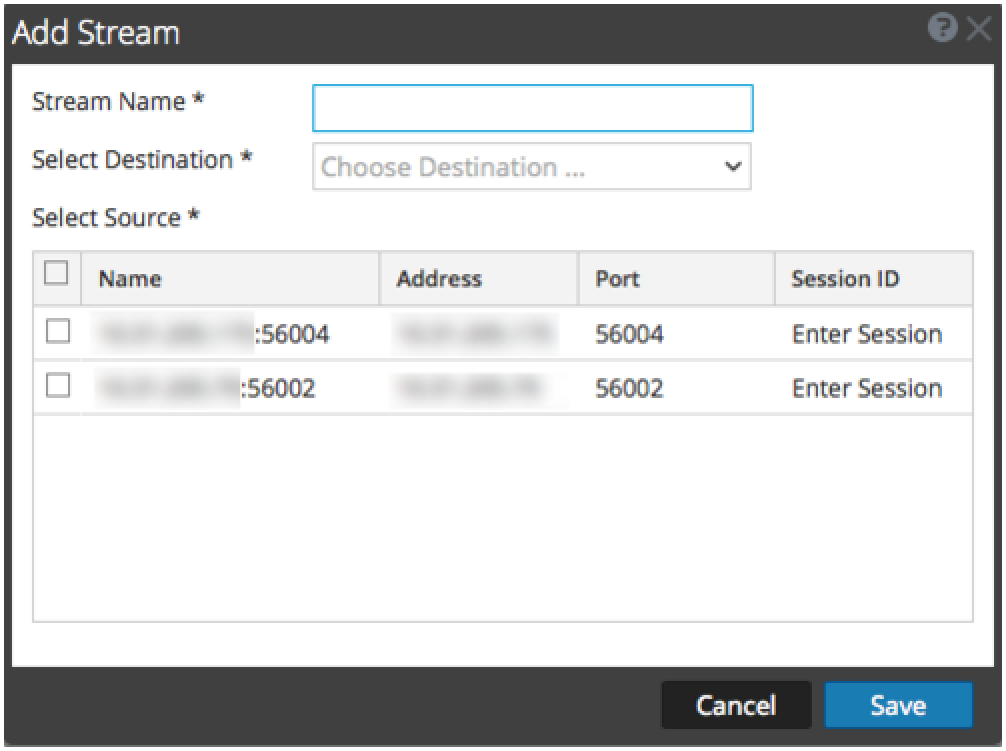
8. Click **Save**.
9. (Optional) If you want to enable checksum validation, perform the following:
   a. In the Security Analytics menu, select Administration > Services.
   b. In the Services view, select the added Warehouse Connector service, and ⚙ ⌄ **> View > Explore**.

      The Explore view of Warehouse Connector is displayed.
   c. In the options panel, navigate to **warhouseconnector/destinations/nfs/config**.
   d. Set the parameter `isChecksumValidationRequired` to 1.
   e. Restart the respective stream.

## *Create, Finalize, and Start the Stream*

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the Services view, select the added Warehouse Connector service and ⚙ ⌄ **> View > Config**.

   The Services Config view of Warehouse Connector is displayed.
3. Click the **Streams** tab.
4. On the Streams tab, click **+**.



Add Stream

Stream Name *

Select Destination * Choose Destination ...

Select Source *

| □ | Name | Address | Port | Session ID |
|---|---|---|---|---|
| □ | [redacted]:56004 | [redacted] | 56004 | Enter Session |
| □ | [redacted]:56002 | [redacted] | 56002 | Enter Session |

5. In the Add Stream dialog, perform the following:

   a. In the **Stream Name** field, enter a name for the stream.

   b. The Stream Name field does not support space or special characters except underscore (_).

   c. In the Select Destination drop-down menu, select a destination from the list of destinations added to the Warehouse Connector.

   d. In the Select Source field, select sources from the list of sources displayed.

   e. In the Session ID column, enter "0" as the SessionID

   **! Important: First sessionid and last sessionid value can be found in Select source device->View->Explore->database->stats.**

   f. If you provide any session id, the Warehouse Connector will start the aggregation from that session, whereas if this is left blank, the aggregation will start from the current session.

   g. Click **Save**.

6. On the **Streams** tab, select the stream that you have created.
7. Click **Finalize**.
8. On the **Streams** tab, select the stream that you have created.
9. Click **Start**.

# Certification Checklist for RSA Security Analytics

Date Tested: January 26th, 2016

| Certification Environment | | |
|---|---|---|
| **Product Name** | **Version Information** | **Operating System** |
| RSA Security Analytics | 10.5 | Virtual Appliance |
| MapR Cluster | 3.1 | Virtual Appliance |
| | | |

| Security Analytics Test Case | Result |
|---|---|
| **Reporting** | |
| Generate Meta | ✓ |
| Add Data Source in Reporting Engine | ✓ |
| Run Test Report | ✓ |
| **Data Transfer** | |
| Generate Data | ✓ |
| Write Data | ✓ |
| Retrieve Data | ✓ |

✓ = Pass ✗ = Fail N/A = Non-Available Function