RSA Ready Implementation Guide for RSA Security Analytics

Pivotal HD 2.0

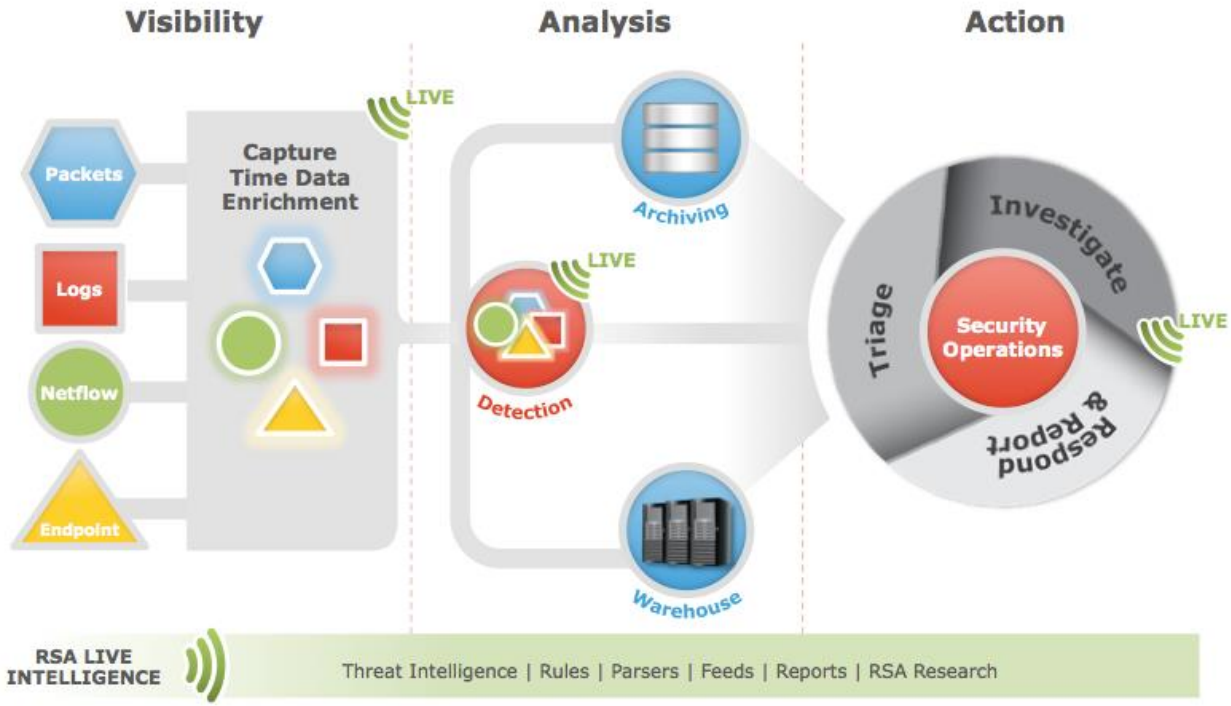
Jeffrey Carlson, RSA Partner Engineering
Last Modified: 02/26/16

RSA READY

Solution Summary

Pivotal HD 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. Pivotal HD integrates with Security Analytics via the Warehouse Connector to collect metadata and events from Decoder and Log Decoder and write them in Avro format. 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



Pivotal HD Cluster Configuration

Before You Begin

This section provides instructions for configuring Pivotal HD 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 Pivotal 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 Pivotal cluster is properly configured and secured before deploying to a production environment. For more information, please refer to the Pivotal documentation or website.

Pivotal Cluster Configuration

The RSA Analytics Warehouse is based on the version 2.0 of Pivotal HD. If you are using Pivotal HD, add the IP address and FQDN (Fully Qualified Domain Name) of the Pivotal node on which you have installed the DNS master to the /etc/hosts file in the device on which the Warehouse Connector service is installed.

If you want to enable checksum validation to validate the integrity of the AVRO files that are transferred from the Warehouse Connector to the destinations, configure SSH keys based access between the Warehouse Connector and the SAW appliance or hadoop node.

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:

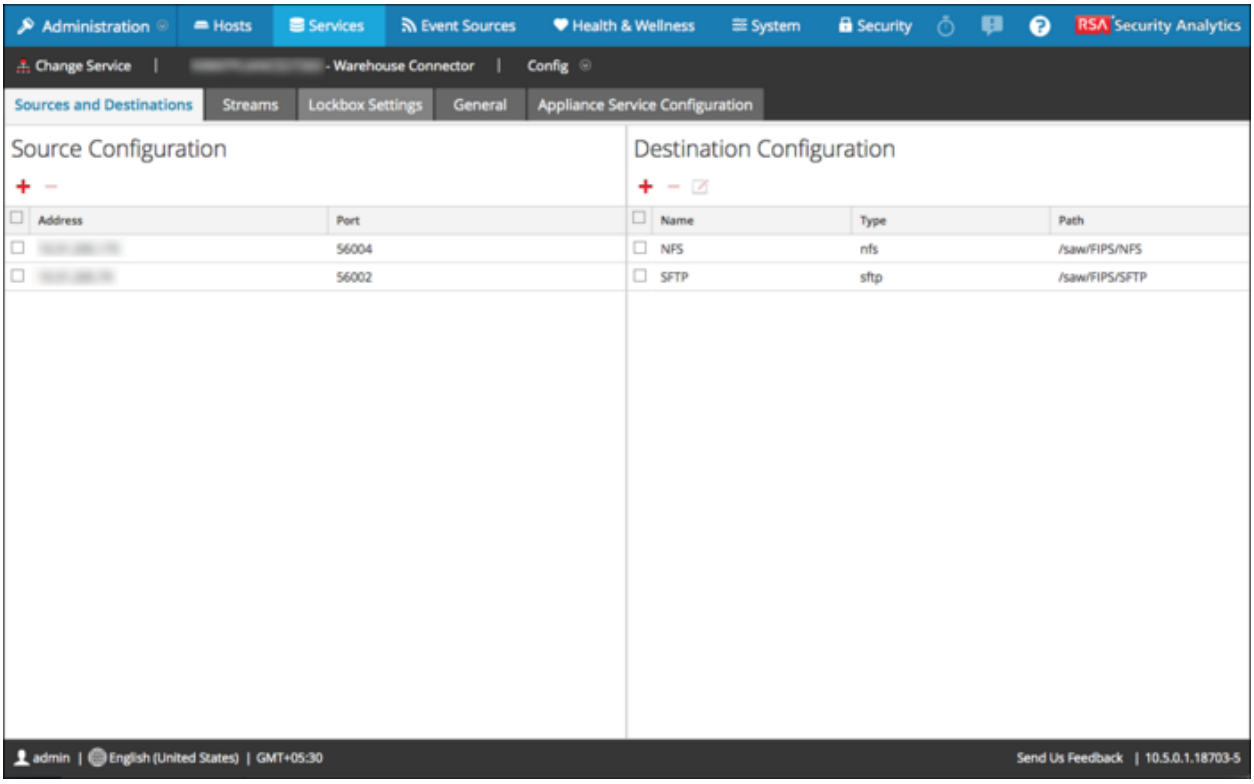
https://sadocs.emc.com/0_en-us/089_105InfCtr/120_AppSerCon/WaConCon

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.

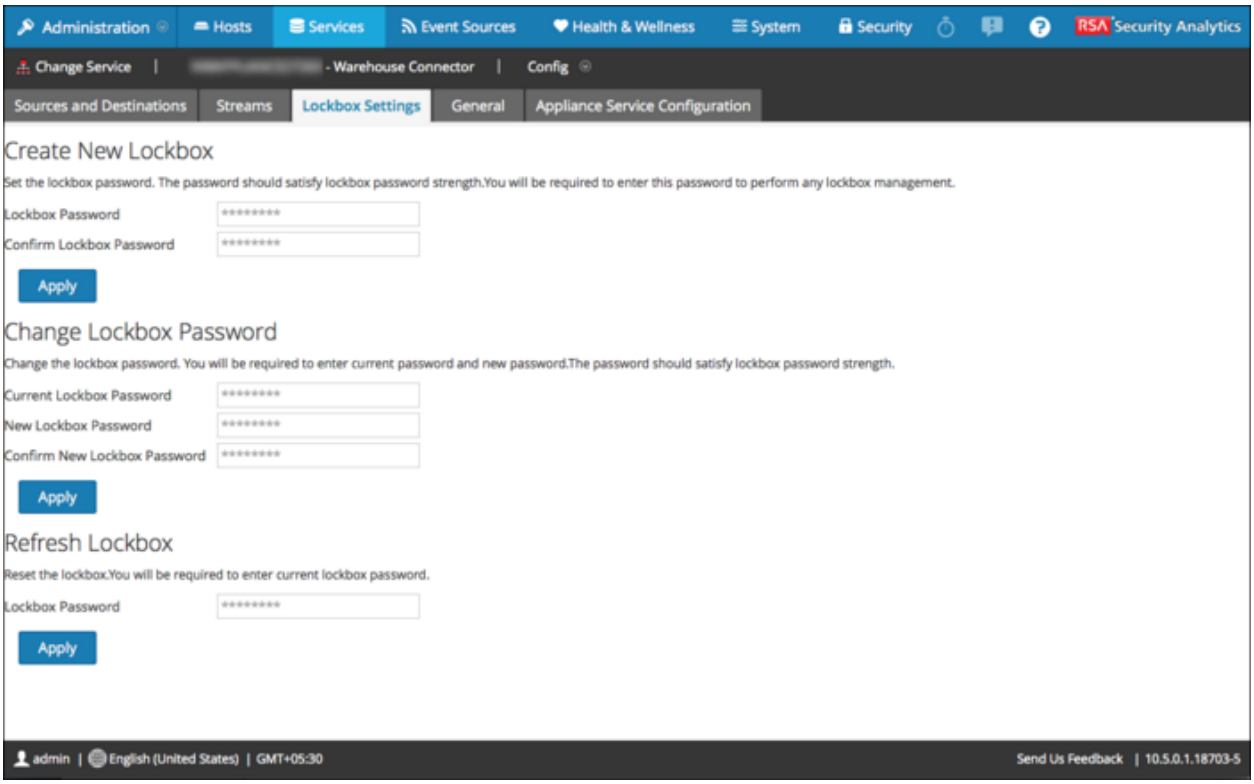
Create the Lockbox

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.



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



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

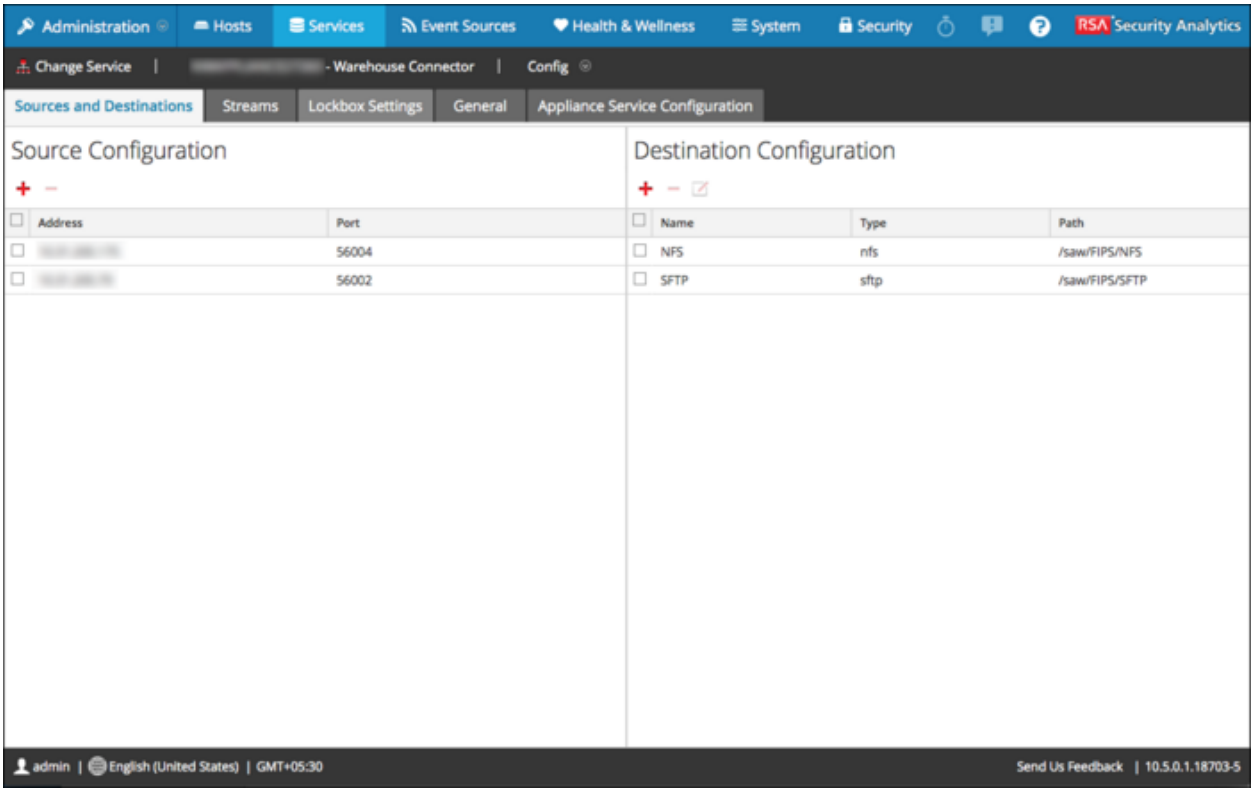
   ! Important: The lockbox password must be at least eight characters in length and they must contain at least three of the following groups: one uppercase character [A-Z], one lowercase character [a-z], one numeral [0-9], and one special character.

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

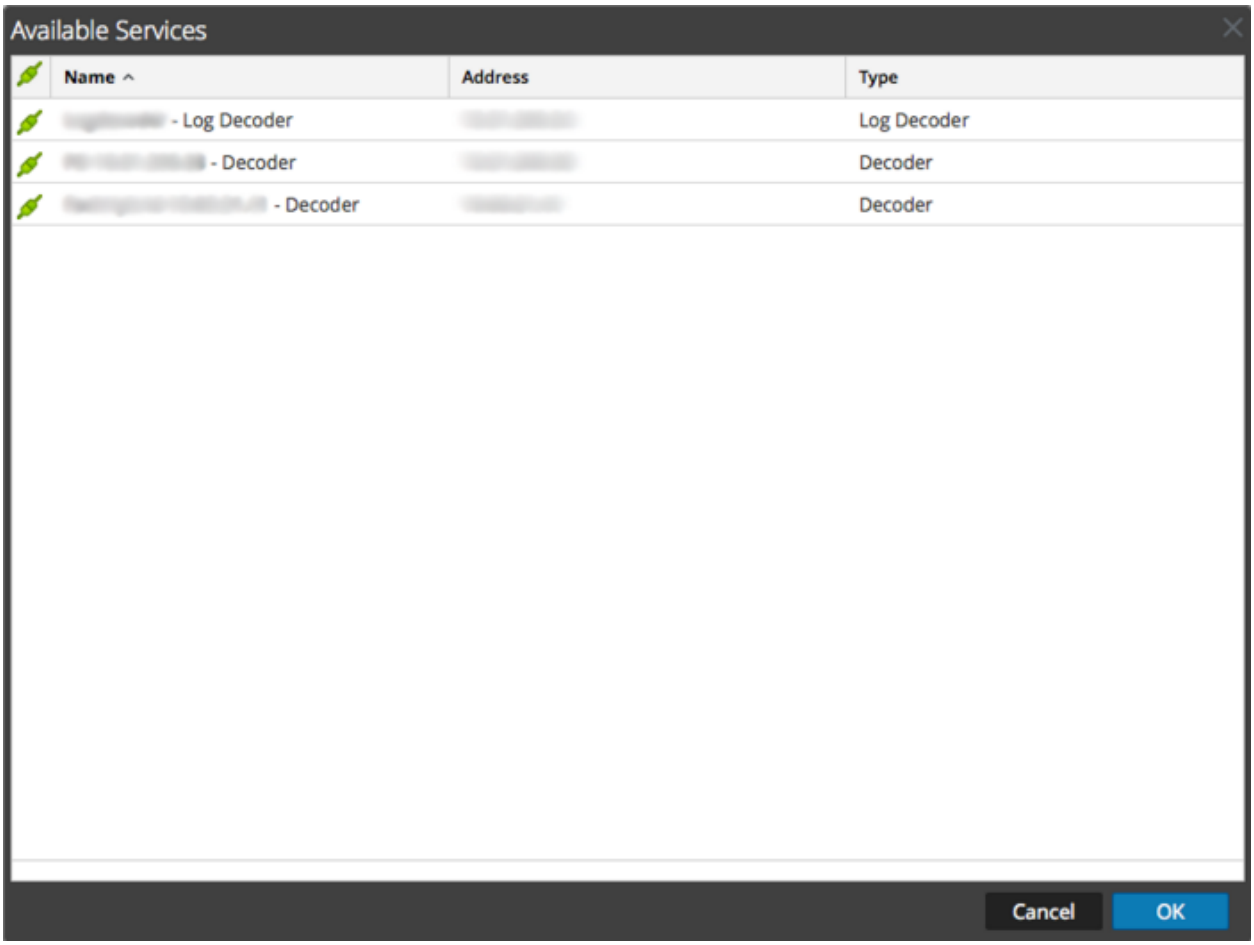
Configure the Data Source

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.



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



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.

Configure the Destination Using SFTP – Password

Before beginning to configure the Warehouse connector to support SFTP delivery of .avro files, make sure that you have:

- Installed the Warehouse Connector service or virtual appliance in your network environment.
- Added the Warehouse Connector service to Security Analytics.
- For the SFTP destination type, the destination host should be listed in the /root/.ssh/known_hosts file used by the ssh service (i.e. sshd) running on the Warehouse Connector.

  To add the destination host to the /root/.ssh/known_hosts file, from the Warehouse Connector host, initiate a secure connection to the destination host. Perform the following:

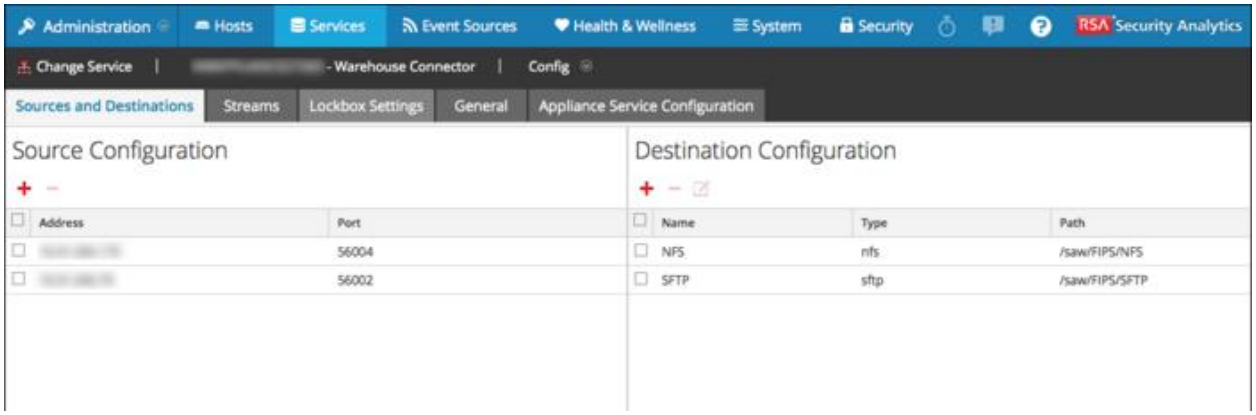
  1. Login to the Warehouse Connector.
  2. Enter ssh root@<SAWIP> or ssh username@<SAWIP>.

3. Select Yes and enter the password.
4. Add the host key in the /root/.ssh/known_hosts file.

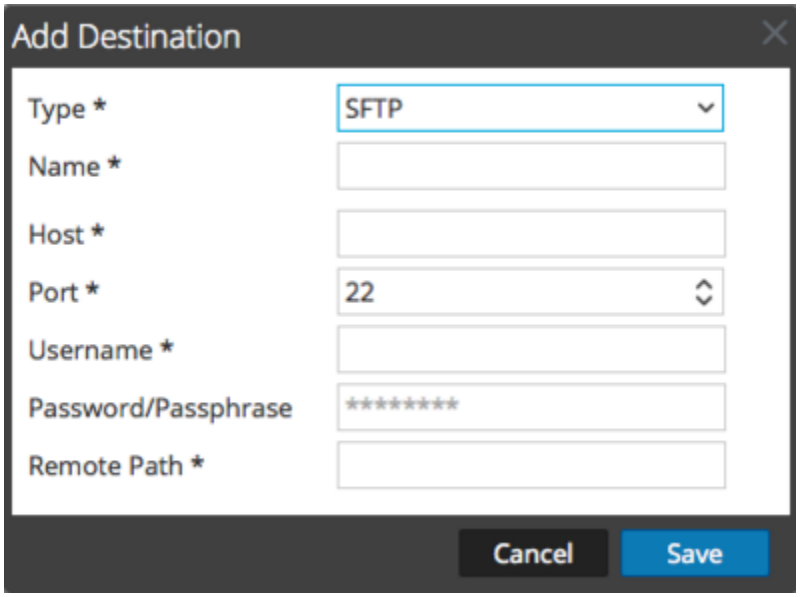
To configure the destination using a **password**:

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.



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



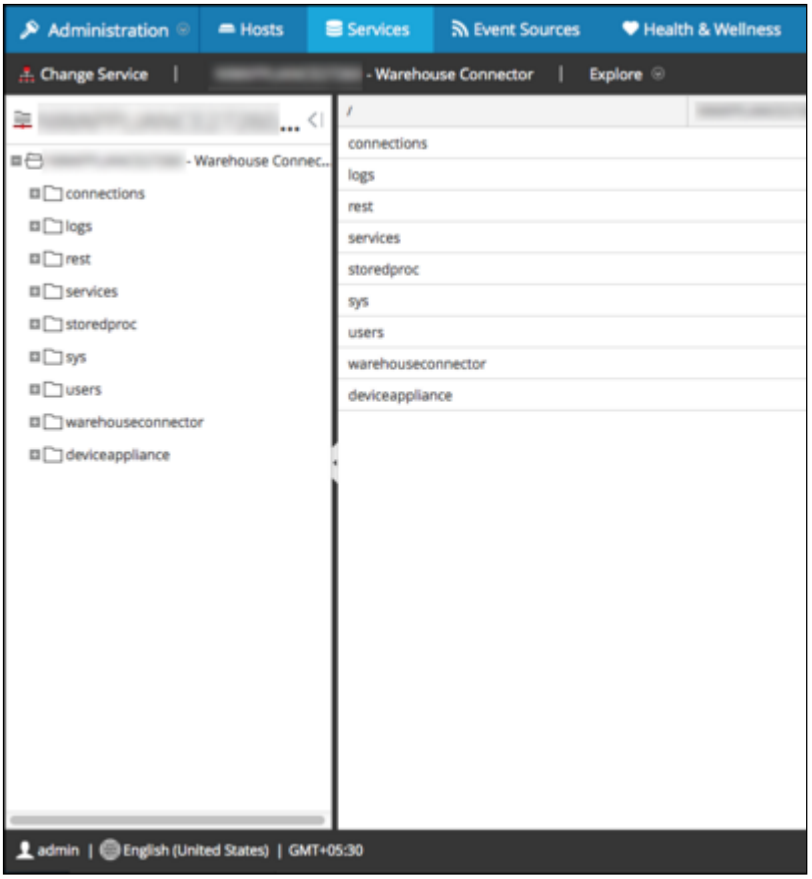
6. In the Name field, enter a unique symbolic name for the destination
7. In the **Host** field, enter the remote server IP address.
8. In the **Port** field, retain the default port, **22**.

9. In the **Username** field, enter the SSH username.

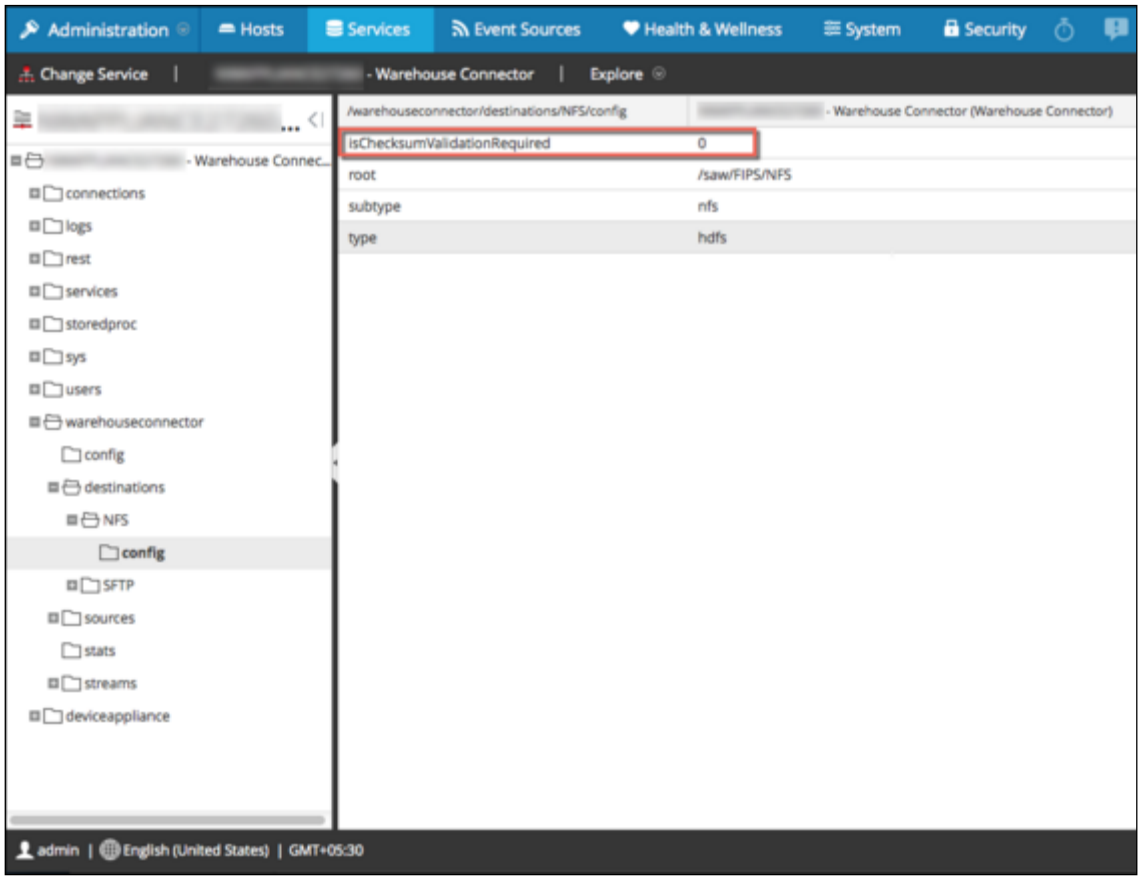
> **Important: Not all warehouses will support access via password only. Ensure that all supported methods (password or passphrase) are tested.**

10. In the Password/Passphrase field, enter the password.
11. In the Remote Path field, enter the path of the directory present on the SFTP server.
12. Click Save.
13. (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 **warehouseconnector/destinations/sftp/config**.
    d. Set the parameter `isChecksumValidationRequired` to **1**.



e. Restart the respective stream

Configure the Destination Using SFTP – Passphrase (SSH Keys)

The second SFTP test is to write data into the destination using SSH key-based access. To do this, you need to configure SSH key-based access between the Warehouse Connector and the Warehouse host or hadoop node. For more information, see the **Configure SSH Keys** section of the online documentation.

To configure the destination using a passphrase and SSH keys:

1. Generate SSH keys on the Warehouse Connector at the default location. Perform the following:
   a. Log on to the Warehouse Connector.
   b. Type the following command and press ENTER:

      ```
      $ ssh-keygen -t dsa
      ```

   c. The command prompts you to enter the file in which to save the generated key.

      ```
      Enter file in which to save the key (/root/.ssh/id_dsa):
      ```

   d. Enter the file in which you want to save the key and press ENTER.

      The command prompts you to enter and confirm the passphrase.

      ```
      Enter passphrase (empty for no passphrase):
      Enter same passphrase again:
      ```

The public key is generated and is saved in the location that you provided.

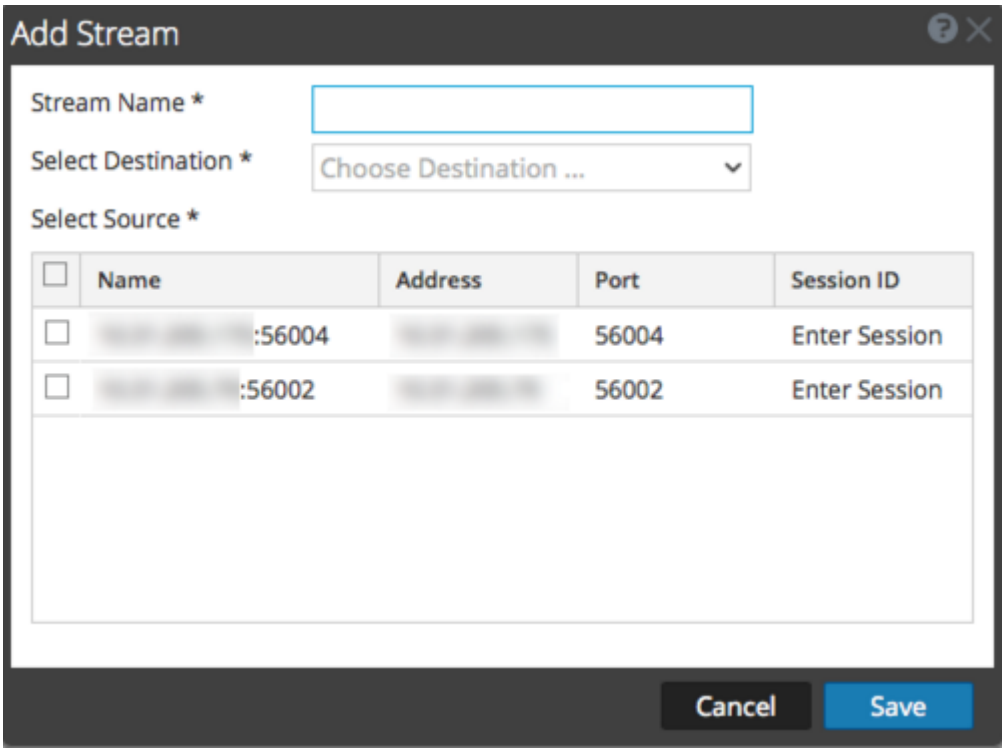
Important: If you want to enable checksum validation to validate the integrity of the AVRO files that are transferred from the Warehouse Connector to the destinations, make sure that you do not set the passphrase.

2. Append the generated public key to the remote Warehouse host or hadoop node's authorized keys list located at:`~/.ssh/authorized_keys`.

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 **+**.



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
Pivotal HD	2.0.3	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