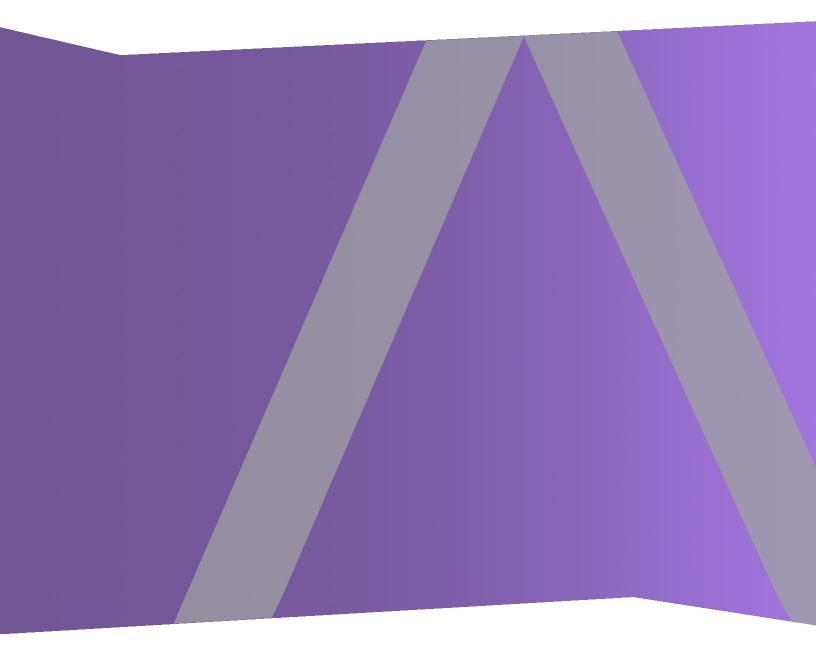


# Warehouse Connector Configuration Guide

for Version 11.1



Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

#### **Contact Information**

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

#### Trademarks

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

#### **License Agreement**

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

#### **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

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

March 2018

## Contents

How Warehouse Connector Works	5
Install Warehouse Connector Service on a Log Decoder or Dec	oder or
Hybrid	8
Configure a Warehouse Connector Service	9
Configure the Data Source for Warehouse Connector	10
Update the Port Number and SSL Settings of the Data Source	11
Configure the Destination	
Configure the Destination Using NFS	15
Configure the Destination Using SFTP	
Configure the Destination Using WebHDFS	
Configure a Stream	
Create a Stream	
Finalize the Stream	
Start the Stream	
Monitor a Warehouse Connector	33
Add Warehouse as a Data Source to Reporting Engine	
Analyze a Warehouse Report	
View the Warehouse Connector Service	
Troubleshoot the Warehouse Connector	
Manage a Stream and Lockbox	40
Warehouse Connector Configuration References	
General Tab Settings	
Appliance Service Configuration Tab Settings	
Sources and Destinations Configuration	
Add Stream Dialog	

Streams Configuration	.64
Lockbox Settings	. 72

## **How Warehouse Connector Works**

Warehouse Connector collects meta and events from Decoder and Log Decoder and writes them in AVRO format into a Hadoop-based distributed computing system. You can set up Warehouse Connector as a service on existing Log Decoders or Decoders.

The Warehouse Connector contains the following components:

- Data Source
- Destination
- Data Stream

## Data Source

A data source is the service from which the Warehouse Connector collects data to store in the destination. The supported data sources are Log Decoder and Decoder services.

## Destination

Destination is the Hadoop-based distributed computing system that collects, manages, and enables reporting on security data. The following are the supported destinations:

- RSA NetWitness Warehouse (MapR) deployments
- HortonWorks Data Platform
- Any Hadoop-based distributed computing system that supports WebHDFS or NFS mounting of HDFS file systems.
- Example: Commercial MapR M5 Enterprise Edition for Apache Hadoop

## Data Streams

A data stream is a logical connection between the data source and destination. You can have multiple streams for different subsets of data collected. You can setup streams to segregate data from multiple Decoder and Log Decoder services. You can create a stream with multiple data sources and a single destination or with a single data source and destination.

The Warehouse Connector does the following:

- Aggregates session and raw log data from Decoders and Log Decoders.
- Transfers the aggregated data into supported destinations like Hadoop based deployments.
- Serializes the aggregated data that includes both schema and data into AVRO format.

In addition the Warehouse Connector also supports the following:

## Meta Filters

Meta filters enables you to filter the meta keys that should be written into the Warehouse. For more information, see <u>Specify Meta Filters for a Stream</u>.

## Support for Multi-Valued Meta Keys

RSA NetWitness Warehouse supports multi-valued meta keys. The multi-valued meta keys is the meta field with the array type. You can use the meta keys library to determine the meta fields of type array and write HIVE queries with the correct syntax for arrays. By default, the following meta keys are treated as multi-valued and are defined in the file, **multivalue-bootstrap.xml** located at /etc/netwitness/ng in the Warehouse Connector:

- alias.host
- action
- username
- alias.ip
- alias.ipv6
- email
- device.group
- event.class

## **Checksum Validation**

Warehouse Connector enables you to validate the file integrity of the AVRO files that are transferred from the Warehouse Connector to the data destinations. You need to enable checksum validation while you configure the Warehouse Connector.

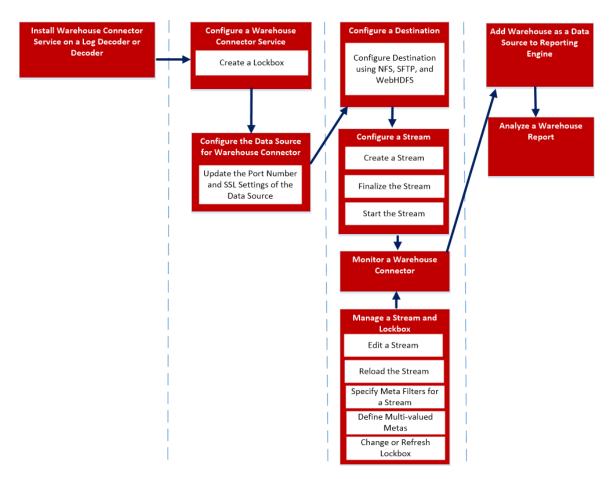
## Lockbox Support

Lockbox provides an encrypted file that Warehouse Connector uses to store and protect sensitive data. You need to create the lockbox by providing a lockbox password while configuring the Warehouse Connector for the first time.

You can orchestrate Warehouse Connector on a Log Decoder or a Decoder appliance.

The following is an overview of the entire process of installing and configuring the Warehouse Connector service on Log Decoder or Decoder, configuring the Warehouse Connector service on NetWitness, configuring data sources, destinations, streams for Warehouse Connector, and configuring alert notifications on NetWitness.

#### Warehouse Connector Configuration Guide



To install and configure the Warehouse Connector service, perform the following:

- 1. Install Warehouse Connector service on a Log Decoder or Decoder
- 2. Configure a Warehouse Connector service
- 3. Configure the Data Source for Warehouse Connector
- 4. Configure a Destination
- 5. Configure a Streams
- 6. Monitor a Warehouse Connector
- 7. Add Warehouse as a Data Source to Reporting Engine
- 8. Analyze a Warehouse Report
- 9. Manage a Stream and Lockbox

# Install Warehouse Connector Service on a Log Decoder or Decoder or Hybrid

To install (fresh install) the Warehouse Connector service on a Log Decoder or Decoder or Hybrid:

- 1. Log on to the Log Decoder or Decoder host.
- Enter the following command on NetWitness Server: warehouse-installer --help The command line interface (CLI) usage descriptions are displayed.
- 4. Install Warehouse Connector service by executing either of the following commands:

```
warehouse-installer --host-addr 10.0.0.0
warehouse-installer --host-id 5928b9d8-83be-4143-9602-fa936de5c41e
warehouse-installer --host-name NW11AdminServer
Where,
10.0.0.0 - IP address of the Host
5928b9d8-83be-4143-9602-fa936de5c41e - Host ID
NW11AdminServer - Host name
```

The Warehouse Connector service is successfully installed on the Log Decoder or Decoder or Hybrid.

## **Configure a Warehouse Connector Service**

You can configure the Warehouse Connector service using the following procedure.

To set the Lockbox password:

- 1. Log on to NetWitness.
- 2. Go to **ADMIN** > Services.
- In the Services view, select the added Warehouse Connector service, and select
   View > Config.
- 4. In the Services Config view of Warehouse Connector, click the Lockbox Settings tab.

RSA RESPOND	ESTIGATE MONITOR CONFIGURE ADMIN	Š 💭 🕅 admin 🏾 🥎
Hosts Services		
A Change Service   Wa	rehouse Connector   Config 🐵	
Sources and Destinations	Streams Lockbox Settings General Appliance Service Configuration	
Create New Lockbox		
Set the lockbox password. The pass	vord should satisfy lockbox password strength.You will be required to enter this password to perform any lockbox management.	
Lockbox Password	****	
Confirm Lockbox Password	******	
Apply		
Change Lockbox Pas	sword	
Change the lockbox password. You	vill 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	*******	
Apply		
Refresh Lockbox		
Reset the lockbox.You will be requir	ed to enter current lockbox password.	
Lockbox Password	*******	
Apply		
RSA NETWITNESS SU		1110001798380386010000

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

**Note:** The lockbox password must be at least eight characters in length and it 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.

The Lockbox password is set.

# Configure the Data Source for Warehouse Connector

To configure the data source:

- 1. Log on to NetWitness.
- 2. Go to **ADMIN** > Services.
- 3. In the Services view, select the added Warehouse Connector service, and select > View > Config.
   The Services Config view of Warehouse Connector is displayed.
- 4. On the Sources and Destinations tab, in the Source Configuration section, click +.

Ava	ilable Services		×
ø	Name ^	Address	Туре
ø	Decoder		Decoder
ø	Log Decoder		Log Decoder
			Cancel OK

 In the Available Services dialog, select the Log Decoder or Decoder services that you want to add as a source to the Warehouse Connector service and click OK. The selected Log Decoder and Decoder services are listed in the Source Configuration section.

#### Update the Port Number and SSL Settings of the Data Source

If there is change in the port number or SSL settings of the data sources used in the Warehouse Connector, you can directly update these details in Warehouse Connector, using the Explore view of the Warehouse Connector.

Make sure that:

- You have the updated port number or SSL settings of the data source.
- You stop the streams related to the data source that you want to update the port number or SSL settings.

To update the port number or SSL settings:

- 1. Log on to NetWitness.
- 2. Go to **ADMIN** > **Services**.
- In the Services view, select the added Warehouse Connector service and select
   View > Explore.

The Service Explore view of Warehouse Connector is displayed.

RSA RESPOND INVESTIGATE	MONITOR CONFIGURE AD	MIN	
Hosts <b>Services</b> Event			
A Change Service   Warehouse Conr	nector   Explore ⊚		
≡Warehouse Connect <	undefined	Warehouse Connector (Warehouse Connector)	
Connector (WAREHOUSE C	connections		
	logs		
	rest		
□ rest	services		
□ services	storedproc		
storedproc	sys users		
□ □ sys	warehouseconnector		
	deviceappliance		
□ □ warehouseconnector			
Config .			
□ stats			
C deviceappliance			
1			
1			
< >			
RSA NETWITNESS SUITE			11000017 <b>1010010100</b> 11000010

4. Navigate to **warehouseconnector/sources**, right-click the source, and click **Properties**. The Properties section of the source is displayed.

Hosts Services     Ventrouse Connection     Warehouse Connection     Warehouse Connection     Onnections     Image: Connection (WAREHOUSE Connection (WAR	RSA RESPOND INVESTIGATE	MONITOR CONFIGURE ADM	11N	Ŏ	
Warehouse Connector (Warehouse Connector (Warehouse Connector)         connections         connections           Warehouse Connector (Warehouse Connector)         logs         connections           Logs         services         rest           Logs         services         services           Loss readpoint         services         services	Hosts Services Event				
Warehouse Connector (WAREHOUSE.con         omnectors           B Connector (WAREHOUSE.con         bgs           B Connectors         services           B Loss         services           B Loss         services           B Loss         services           B Loss         derse services	A Change Service   Warehouse Conn	nector   Explore ⊚			
Warehouse Connector (WAREHOUSE, Warehouse Connections     Important Sector (WAREHOUSE, Sector Sector S	≡Warehouse Connect <	1	Warehouse Connector (Warehouse Connector)		
B         B           B         B           B         C					
Import     services       Import     sordeproc       Import     ss       Import     services					
Bit Nota         Bit Nota           Bit Nota         Aircle A	III C logs				
Imported     Spanne					
□     users	services				
□     ys     warhouseconnector       □     deviceapplance	II C storedproc				
Image: market billing: market bill: market billing: market billing: market bi	II 🗋 sys				
	II 🗋 users				
	II 🗋 warehouseconnector				
	C1 config				
Properties	C destinations				
		L			
	Properties				
	C stats				
	II C deviceappliance				

- 5. In the drop-down menu, select update. In the Parameters field, perform the following:
  - To update the port number of the source, enter port=<new\_source\_portnumber> and click Send.

Parameters port=443

• To update the SSL settings of the source, enter ssl=<new\_ssl\_settings> and click Send.

Parameters ssl=on

**Note:** You can also update the port number and ssl settings simultaneous by adding space between the parameters.

- 6. Restart the Warehouse Connector service.
- 7. Start the streams.

## **Configure the Destination**

You can configure the destination using NFS, SFTP, and WebHDFS. Change the destination to which the Warehouse Connector service needs to write the collected data using NFS:

- RSA NetWitness Warehouse (MapR) deployments
- Commercial MapR M5 Enterprise Edition for Apache Hadoop deployments

You can configure the Warehouse Connector to write to a remote destination using Secure File Transfer Protocol (SFTP). The remote destination can be a remote server that is NFS mounted to the MapR cluster or it can be a remote staging server.

By default, in the remote destination the Warehouse Connector writes data in the following directory structure:

• /<staging\_</pre>

```
folder>/rsasoc/v1/sessions/data/<year>/<month>/<day>/<hour>/
```

• /<staging\_</pre>

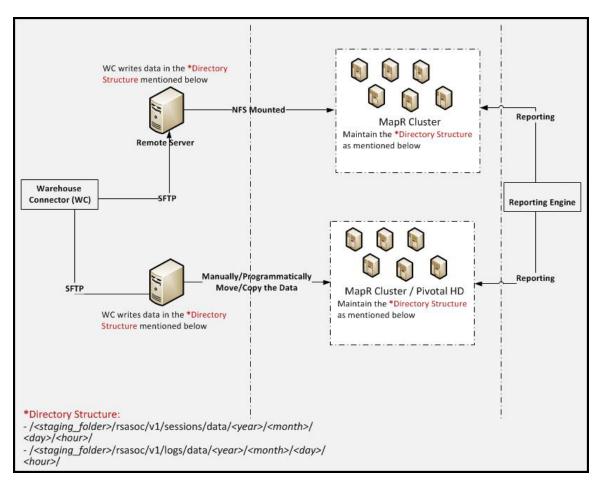
```
folder>/rsasoc/v1/logs/data/<year>/<month>/<day>/<hour>/
```

Where <staging\_folder> is the folder on the remote server where the Warehouse Connector writes the data.

If you are using a remote staging server as the remote destination, you need to manually copy or move the directory structure to any of the following deployments:

- RSA NetWitness Warehouse (MapR)
- Commercial MapR M5 Enterprise Edition for Apache Hadoop
- HortonWorks HD

To generate reports from the data written by Warehouse Connector, make sure that in your Hadoop deployment you maintain a similar directory structure that is created by Warehouse Connector in the remote destinations.



The following illustration describes how you can use SFTP to write data from Warehouse Connector to a remote destination.

You can configure the Warehouse Connector service to write the collected data to a Hadoopbased distributed computing system that supports WebHDFS.

### **Configure the Destination Using NFS**

Make sure that you have:

- Installed the Warehouse Connector service or virtual appliance in your network environment.
- Added the Warehouse Connector service to NetWitness. For more information, see "Add a Service to a Host" in the *Hosts and Services Getting Started Guide*.
- Set up NFS on Warehouse Connector. For more information on how to set up NFS on Warehouse Connector, see "Configure Warehouse Connector to Write to Warehouse" in the *Warehouse (MapR) Configuration Guide*.

To configure the destination using NFS:

- 1. Log on to NetWitness.
- 2. Go to **ADMIN** > Services.
- 3. In the Services view, select the Warehouse Connector service, and select > View
   > Config.

KRESPOND INVESTIGATE MONITOR CONFIGURE ADMIN Ô Ω @ damin ⊕ ⑦					
A Change Service   Warehouse Connector   Config	≜ Change service   Warehouse Connector   Config ⊙				
Sources and Destinations Streams Lockbox Settings	Sources and Destinations Streams Lockbox Settings General Appliance Service Configuration				
Source Configuration		Destination Configuration			
+ -		+ - 🗵			
Address	Port	Name	Туре	Path	
10.31.125.245	56004	NFS	nfs	/root/test/kaushal	
10.31.125.248	56002	SFTP SFTP	sftp	/root/test	

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 NFS from the Type drop-down list.
- 6. In the Name field, enter a unique symbolic name for the destination.

**Note:** The **Name** field does not support spaces 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 NetWitness Warehouse (MapR), create a directory named **Ionsaw01** under /saw and the corresponding Local Mount Path for the destination

would be /saw/Ionsaw01.

For more information, see "Mount the Warehouse on the Warehouse Connector" topic in the *Warehouse (MapR) Configuration Guide*.

Add Destination				×
Type *	NFS		~	
Name *				
Local Mount Path *				
		Cancel	Save	

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. Go to **ADMIN > Services**.
  - b. In the Services view, select the added Warehouse Connector service, and select > View > Explore.
     The Explore view of Warehouse Connector is displayed.

RSA RESPOND INVESTIGATE	MONITOR CONFIGURE AD	MIN	Ö ⊥ (D) admin ⊗ (D)
Hosts Services Event			
A Change Service   Warehouse Con	nector   Explore 😔		
≡ Warehouse Connect <	undefined	Warehouse Connector (Warehouse Connector)	
Warehouse Connector (WAREHOUSE_C	connections		
Connections	logs		
	rest		
II Crest	services storedproc		
C services	sys		
II 🗀 storedproc	users		
II 🗀 sys	warehouseconnector		
III 🗀 users	deviceappliance		
warehouseconnector			
C config	•		
stats	1		
C deviceappliance			
	1		
	1		
<	1		
RSA   NETWITNESS SUITE	•		1 10000 1 7 <b>8 6 8 6 6 1 1 1000 1 1 1000</b>

- c. In the options panel, navigate to **warehouseconnector/destinations/nfs/config**. This is the name of the destination and is dynamic.
- d. Set the parameter is ChecksumValidationRequired to 1.

Change Service   Warehouse Coni	nector   Explore ⊙		
∎Warehouse Connect <	/warehouseconnector/destinations/NFS/config	Warehouse Connector (Warehouse Connector)	
Harehouse Connector (WAREHOUSE_CO	isChecksumValidationRequired	1	
	root	/root/test/kaushal	
	subtype	nfs	
III rest	type	hdfs	
services			
Storedproc			
III sys			
■ sys			
Users			
warenouseconnector			
Config			
III C NFS			
in config			
II Contig			
stats			
deviceappliance			
III] deviceappliance			

e. Restart the respective stream.

### **Configure the Destination Using SFTP**

Make sure that you have:

- Installed the Warehouse Connector service or virtual appliance in your network environment.
- Added the Warehouse Connector service to NetWitness. For more information, see the "Add a Service to a Host" in the *Hosts and Services Getting Started Guide*.
- For the SFTP destination type, the destination host should be listed in the /root/.ssh/known\_ hosts file used by the ssh service (for example, sshd) running on the Warehouse Connector.

## Add Destination from Warehouse Connector Host

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:

- 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

**Note:** After you upgrade Warehouse Connector to 11.0, you must make sure that the destination host is listed in the /root/.ssh/known\_hosts file used by the ssh service (i.e. sshd) running on the Warehouse Connector. If you do not perform this action, the streams configured with SFTP in Warehouse Connector will not start.

• If you want to use SFTP to write data into the destination using SSH key-based access, you need to configure SSH key-based access between the Warehouse Connector and the Warehouse host or Hadoop node. For more information, see **Configure SSH Keys** below.

**Note:** 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 generate the keys without setting the passphrase and do a key exchange between warehouse connector and the warehouse nodes.

#### Configure Warehouse Connector to use SFTP destination

To configure the destination:

- 1. Log on to NetWitness
- 2. Go to **ADMIN** > **Services**.
- 3. In the Services view, select the added Warehouse Connector service, and select 🌣 📀

> View > Config.

The Services Config view of Warehouse Connector is displayed.

SA RESPOND INVESTIGATE MONITOR CONFIGURE ADMIN ③ ①					
Hosts Services Event Sources Health & Wellness System Security					
È Charge Service   Warehouse Connector   Config ©					
Sources and Destinations Streams Lockbox Settings	General Appliance Service Configuration				
Source Configuration		Destination Configuration			
+ -		+ - 🗷			
Address	Port	Name	Туре	Path	
10.31.125.245	56004	NFS	nfs	/root/test/kaushal	
0.31.125.248	56002	SFTP SFTP	sftp	/root/test	
RSA   netwitness suite					

- 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.

Add Destination			×
Type *	SFTP		~
Name *			
Host *			
Port *	22		\$
Username *			
Password/Passphrase	*******		
Remote Path *			
		Cancel	Save

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

**Note:** The **Name** field does not support spaces or special characters except underscore ( ).

- 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.

**Note:** In the case of HortonWorks HD, ensure that the username is gpadmin and for password based access the password for gpadmin should be used. For passphrase-based access, the passphrase used to generate the keys for gpadmin user should be used.

- 10. In the Password/Passphrase field, enter one of the following:
  - SSH password If you are using SFTP to write data into the destination using passwordbased access.
  - SSH passphrase If you are using SFTP to write data into the destination using SSH keybased access.
- 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. Go to **ADMIN > Services**.
  - b. In the Services view, select the added Warehouse Connector service, and select 🌞 📀

#### > View > Explore.

The Explore view of Warehouse Connector is displayed.

RSA RESPOND INVESTIGATE	MONITOR CONFIGURE AD	MIN	Ö
Hosts Services Event			
A Change Service   Warehouse Conr	nector   Explore 👳		
≡Warehouse Connect <	undefined	Warehouse Connector (Warehouse Connector)	
Warehouse Connector (WAREHOUSE_C	connections		
□ □ connections	logs		
II 🗋 logs	rest		
II i rest	services		
□ services	storedproc sys		
Storedproc	users		
■ 🗋 sys	warehouseconnector		
II 🗅 users	deviceappliance		
II 🗋 warehouseconnector			
C1 config			
□] stats			
deviceappliance			
< >			
RSA NETWITNESS SUITE			1110001173868033868111221108

- c. In the options panel, navigate to warehouseconnector/destinations/sftp/config.
- d. Set the parameter is Checksum Validation Required to 1.

	ONITOR CONFIGURE ADMIN		5 🔍   ⑦ ① admin ⊗
HOSTS SERVICES		🖀 SYSTEM 🔞 SECURITY	
A Change Service   Warehouse Con	nector   Explore ⊚		
≡Warehouse Connect <	-	Warehouse Connector (Warehouse Connector)	
H Warehouse Connector (WAREHOUSE CO	known.hosts.file		
Connections	password	*****	
	root	/root/test	
I Crest	isChecksumValidationRequired	1	
rest     services	host	10.31.204.44:22	
	type	hdfs	
II Storedproc	username	root	
□ <u></u> 5y5	subtype	sftp	
□ □ users			
warehouseconnector	l		
C config			
destinations			
■ C] NFS			
SFTP			
Config			
II 🗋 sources			
C1 stats			
C deviceappliance			
< >			

e. Restart the respective stream.

## **Configure SSH Keys**

To configure SSH key-based access between the Warehouse Connector and the Warehouse host or Hadoop node:

- 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:

\$ OWB FORCE FIPS MODE OFF=1 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.

**Note:** 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**. Then, the below steps e, f, g, and h are not applicable.

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

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

e. Change the directory by entering the following command:

cd /root/.ssh/

f. Move the generated key to the below location:

mv id\_dsa id\_dsa.old

g. Type the following command and press ENTER:

```
$ OWB_FORCE_FIPS_MODE_OFF=1 openssl pkcs8 -topk8 -v2 des3 -in id_
dsa.old -out id dsa
```

The command prompts you to enter and confirm the passphrase.

- h. Enter the encryption passphrase.
- i. Run the following command to change the file permission:

chmod 600 id\_dsa

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

**Note:** Make sure that you copy the public keys to the Hadoop node and while copying the public key ensure that you provide the login details of the user using which the WebHDFS destination would be added.

You can now securely communicate between Warehouse Connector and Warehouse nodes or Hadoop nodes.

## Configure the Destination Using WebHDFS

Make sure that you have:

- Installed the Warehouse Connector service or virtual appliance in your network environment.
- Added the Warehouse Connector service to NetWitness. For more information, see the "Add a Service to a Host" in the *Hosts and Services Getting Started Guide*.
- Added the hostname (or FQDN) and IP address of the warehouse nodes and Warehouse Connector to the DNS server. If the DNS server is not configured, add the hostname (or FQDN) and IP address of the warehouse nodes and Warehouse Connector to the file in the host on which the Warehouse Connector service is installed.
- If you want Kerberos authentication between the warehouse connector and the warehouse cluster, make sure that you perform the following:
  - Kerberos Key Distribution Center (KDC) Server is configured in your network environment and the Kerberos Keytab file is copied to the host on which you have installed Warehouse Connector.
  - Kerberos authentication is enabled in the warehouse cluster.
- 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 generate the keys without setting the passphrase and do a key exchange between the Warehouse Connector and the warehouse nodes. You need to configure SSH key-based access between the Warehouse Connector and the Warehouse host or hadoop node. For more information, see 'Configure SSH Keys' in Configure the Destination Using SFTP.

## Configure Warehouse Connector to Write to SFTP destination

To configure the destination:

- 1. Log on to NetWitness.
- 2. Go to **ADMIN** > Services.
- 3. In the Services view, select the added Warehouse Connector service and select  $\diamond$



#### > View > Config.

The Services Config view of Warehouse Connector is displayed.

RSA RESPOND INVESTIGATE MONITOR	CONFIGURE ADMIN					
Hosts Services Event Sources Health & Wellness System Security						
🚠 Change Service   Warehouse Connector   Config						
Sources and Destinations Streams Lockbox Settings	General Appliance Service Configuration					
Source Configuration		Destination Configuration				
+ -		+ - 🗷				
Address	Port	□ Name	Туре	Path		
10.31.125.245	56004	NFS	nfs	/root/test/kaushal		
10.31.125.248	56002	SFTP SFTP	sftp	/root/test		
<b>RS∧</b> NETWITNESS SUITE				1 - 1000 - 10000 - 10000 - 10000000		

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

5. In the Add Destination dialog, select WebHDFS from the drop-down list.

Add Destination			×
Type *	WebHDFS	~	
Name *			
Hadoop IP *			
Hadoop Port *		¢	
Username *			
Hadoop Path *			
Kerberos Authentication			
	Cancel	Save	

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

**Note:** The **Name** field does not support spaces or special characters except underscore (\_).

- 7. In the Hadoop IP field, enter the namenode IP address of the warehouse cluster.
- 8. In the **Hadoop Port** field, enter the base port that is used by the namenode web user interface.
- 9. In the **Username** field, enter the owner of the directory in the warehouse to which Warehouse Connector should write the data.
- 10. In the **Hadoop Path** field, enter the path of the directory in the warehouse to which Warehouse Connector should write the data.
- 11. Select the **Kerberos Authentication** checkbox, if you want the warehouse connector to securely communicate with the warehouse using Kerberos authentication.

Add Destination				×
Type *	WebHDFS	5	~	
Name *				
Hadoop IP *				
Hadoop Port *			\$	
Username *				
Hadoop Path *				
Kerberos Authentication	$\checkmark$			
Kerberos Principal *				
Kerberos Keytab File Path *				
		Cancel	Save	

Perform the following:

- a. In the **Kerberos Principal** field, enter the KDC Principal used for Kerberos authentication.
- b. In the **Kerberos Keytab File Path** field, enter the path of the Kerberos Keytab file in the Warehouse Connector.
- 12. Click Save.
- 13. (Optional) If you want to enable checksum validation, perform the following:
  - a. Go to **ADMIN > Services**.
  - b. In the Services view, select the added Warehouse Connector service and select
    > View > Explore.

The Explore view of Warehouse Connector is displayed.

RSA RESPOND INVESTIGATE	E MONITOR CONFIGURE AD	MIN	Š 💭 🕅 admin 🏾 🕃
Hosts Services Event			
A Change Service   Warehouse Con	nector   Explore ©		
■Warehouse Connect <	undefined	Warehouse Connector (Warehouse Connector)	
Warehouse Connector (WAREHOUSE_C	connections		
	logs		
	rest		
I Crest	services		
	storedproc		
Storedproc	sys		
□ <u>□</u> 5y5	users warehouseconnector		
□ users	deviceappliance		
Warehouseconnector	Geviceappirance		
config			
stats			
C deviceappliance			
	1		
	1		
	1		
< >	1		
RSA   NETWITNESS SUITE			11100001788438938461714413

- c. In the options panel, navigate to warehouseconnector/destinations/webhdfs/config.
- d. Set the parameter  $\verb"isChecksumValidationRequired"$  to 1.

Hosts Services Event			
🛔 Change Service   Warehouse Con	nector   Explore ⊗		
■Warehouse Connect <	/warehouseconnector/destinations/NFS/config	Warehouse Connector (Warehouse Connector)	
Warehouse Connector (WAREHOUSE_CO	isChecksumValidationRequired	1	
Warehouse Connector (WAREHOUSE_CO	root		
	subtype	nfs	
II logs	type	hdfs	
III 🗋 rest			
services			
storedproc			
🛙 🗀 sys			
II users			
Warehouseconnector	1		
C config			
C destinations			
II C NFS			
III CI SFTP			
sources			
🗅 stats			
C deviceappliance			
>	1		

e. Restart the respective stream.

## **Configure a Stream**

You can configure the data stream to define the data source and destination combinations.

Make sure that you have:

- Installed the Warehouse Connector service or virtual appliance in your network environment.
- Added the Warehouse Connector service to NetWitness. For more information, see the "Add a Service to a Host" in the *Hosts and Services Getting Started Guide*.
- Configured the data source from which the Warehouse Connector service needs to collect data. For more information, see Configure the Data Source for Warehouse Connector.
- Configured the destination to which the Warehouse Connector service needs to write the collected data. For more information, see <u>Configure the Destination</u>.

#### To configure the stream:

- 1. Create a stream
- 2. Finalize the stream
- 3. Start the stream

#### **Create a Stream**

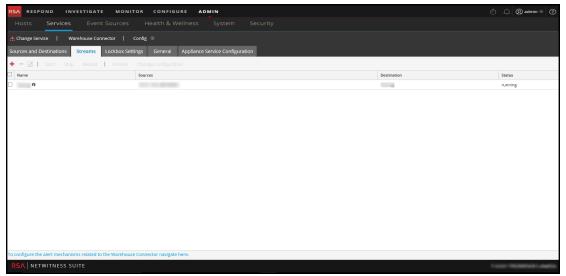
To create a stream:

- 1. Go to **ADMIN** > Services.
- 2. In the Services view, select the added Warehouse Connector service and select  $\diamond$

> View > Config.

The Services Config view of Warehouse Connector is displayed.

3. Click the **Streams** tab.



4. On the Streams tab, click +.

Add Stream			0×
Stream Name * Select Destination *	Choose Destination	🗸	
Select Source *			
□ Name	Address	Port	Session ID
		56004	Enter Session
		56002	Enter Session
			_
		Cance	l Save

- 5. In the Add Stream dialog, perform the following:
  - a. In the Stream Name field, enter a name for the stream.

**Note:** The **Stream Name** field does not support spaces or special characters except underscore (\_).

- b. In the **Select Destination** drop-down menu, select a destination from the list of destinations added to the Warehouse Connector.
- c. In the Select Source field, select sources from the list of sources displayed.
- d. In the Session ID column, enter the last session id.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. e. Click **Save**.

#### **Finalize the Stream**

Make sure that you have created a stream.

To finalize the stream:

- 1. Go to **ADMIN** > **Services**.
- 2. In the Services view, select the added Warehouse Connector service and select  $\diamond$

```
> View > Config.
```

The Services Config view of Warehouse Connector is displayed.

3. On the **Streams** tab, select the stream that you have created.

RSA RESPOND INVESTIGATE MONIT	TOR CONFIGURE ADMIN	Ŏ	∫ admin ⊚ ?
Hosts <b>Services</b> Event Sources			
A Change Service   Warehouse Connector	Config $\odot$		
Sources and Destinations Streams Lockbox Sett	tings General Appliance Service Configuration		
🕂 — 🗹   Start Stop Reload   Finalize			
Name Name	Sources	Destination	Status
θ	:50002	10000	running
To configure the alert mechanisms related to the Warehouse	e Connector navigate here.		
RSA NETWITNESS SUITE			

4. Click Finalize.

#### Start the Stream

Note: If you have deployed a Warehouse Connector Virtual Appliance, make sure that you change the default value of the Maximum Message Hold Count parameter to 800000. For more information, see General Tab Settings.

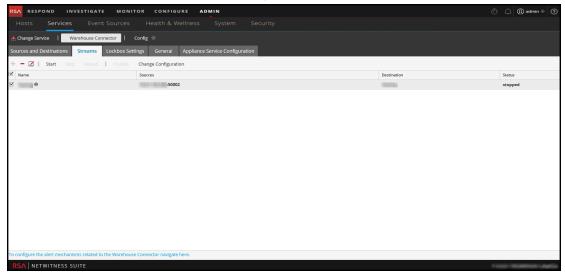
To start the stream:

- 1. Go to **ADMIN> Services**.
- 2. In the Services view, select the added Warehouse Connector service and select

#### > View > Config.

The Services Config view of Warehouse Connector is displayed.

3. On the Streams tab, select the stream that you have created.



4. Click Start.

## **Monitor a Warehouse Connector**

By monitoring a Warehouse Connector, you can automatically generate notifications when critical thresholds concerning Warehouse Connector and its storage have been met.

To monitor a Warehouse Connector:

- 1. Go to **ADMIN** > Services.
- 2. In the Services view, select the added Warehouse Connector service and select  $\textcircled{\circ}$

```
> View > Config.
```

The Services Config view of Warehouse Connector is displayed.

- 3. Click the **Streams** tab.
- 4. At the bottom of the **Streams** tab, click **To configure the alert mechanisms related to the Warehouse Connector navigate here**.

The Warehouse Connector Monitoring page is displayed.

Caution: This page is deprecated and will be removed in a future release.

5. In the **Source or Destination Status** section, select the number of minutes or hours in the **Notify After Failing For** field.

You will receive a notification if the source or destination connection fails for the defined number of minutes or hours.

- 6. In the Stream Status section, perform the following:
  - a. In the **Notify Stopped For** field, define the number of minutes or hours after which you would like to receive a notification when the stream goes offline.
  - b. In the **Disk Is** field, define the limit on the percentage of disk usage after which you would like to receive a notification.
  - c. In the **Source is Behind** field, define the number of sessions. A notification is raised if the source goes behind the defined number of sessions.
  - d. In the **Rejected Folder Size is** field, define the limit on the percentage of folder usage after which would like to receive a notification.
  - e. In the **Number Of Files in Permanent Failure Folder** field, define the limit on the number of files in the permanent failure folder after which you would like to receive a notification.

- 7. In the Notification Type field, perform the following:
  - a. Click **Configure email or distribution list** to configure email so that you can receive notifications in NetWitness. For more information, see the "Configure Email Server and Notification Account" topic in the *System Configuration* guide.
  - b. Click **Configure Syslog and SNMP Trap servers** to configure audit logs. For more information, see the "Configure Syslog and SNMP Settings" topic in the *System Configuration* guide.
  - c. Select the following notification mechanisms as per your requirement:
    - NetWitness Console To get notifications on the NetWitness UI notification toolbar.
    - Email To get email notifications.
    - Syslog Notification To generate syslog events.
    - SNMP Trap Notifications To get audit events as SNMP traps.

# Add Warehouse as a Data Source to Reporting Engine

You must add Warehouse as a data source to Reporting Engine to make this data source available to reports against this Reporting Engine. For more information, see "Add Warehouse as a Data Source to Reporting Engine" topic in the *Reporting Engine Configuration Guide*.

## Analyze a Warehouse Report

The Warehouse modules provide analysts with reports of early indicators of compromise. The following Warehouse reports can be analyzed in NetWitness:

- Suspicious Domains report
- Suspicious DNS Activity report
- Host Profile report

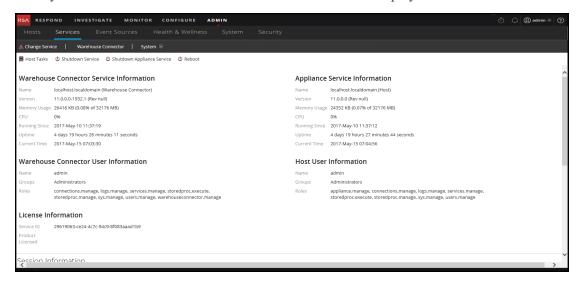
For more information, see "Step 4. Analyze a Warehouse Report" topic in the Warehouse Guide.

# **View the Warehouse Connector Service**

While the information displayed in the Services System view is the same for all types of core services, several options in the toolbar are relevant only for Warehouse Connector.

To access this view:

- 1. Go to **ADMIN** > Services.
- In the Services view, select a Warehouse Connector and select > View > System. The Systems view for the selected Warehouse Connector is displayed.



The following is an example of toolbar options for Warehouse Connectors.



Host Tasks, Shutdown Service, Shutdown Appliance Service or (Shutdown Appliance), and Reboot are common to all services and are described in the *Hosts and Services Getting Started Guide*.

# **Troubleshoot the Warehouse Connector**

The following information suggests the possible issues that NetWitness users may encounter when adding a Warehouse service to the Reporting Engine as a data source for reporting in NetWitness. Look for explanations and solutions in this section.

While adding a Warehouse service to the Reporting Engine as a data source for reporting, you may observe some of the errors listed in this document. Information is provided on how to troubleshoot the errors and add the data source successfully.

New Service				• • ×
Source Type *	WAREHOU	JSE	~	
Warehouse Source *	HiveServe	er2	~	
Name *	PDH2.0-D	CA		
HDFS Path *	/			
Advanced				
Host *				
Port *	10000			
Username *	gpadmin			
Password	*******			
Kerberos Authentication	$\checkmark$			
Server Principal *				
User Principal *				
Kerberos Keytab File *				
Enable Jobs				
Test Connection				
		Cancel	2	Save

The following figure shows the New Service dialog.

For more information, see "Add Warehouse as a Data Source to Reporting Engine" topic in the *Reporting Engine Configuration Guide*.

Error	Possible Solutions
Could not open connection	• Ensure that the HiveServer2 is running on the Host.
to HiveServer	• Check if the port provided can be accessible from the Reporting Engine server.
No Schema found in HDFS path	Ensure that meta avro data file(s) are available in the HDFS path ( <hdfs path="">/rsasoc/v1/sessions/meta) mentioned. The following figure shows an example of the command to check the files in hdfs.</hdfs>
14/12/09 10:31:59 INFO util.Nativ 14/12/09 10:31:59 INFO security.J	fs -lsr /testdata/rsasoc/v1/sessions/meta eCodeLoader: Loaded the native-hadoop library niBasedUnixGroupsMapping: Using JniBasedUnixGroupsMapping for Group resolution 76 2013-08-28 01:09 /testdata/rsasoc/v1/sessions/meta/nwdev-testing.avro
Could not open connection	GSS initiate failed errors will be observed only in the case of
to HiveServer, GSS	Kerberos enabled Hive.
initiate failed	Ensure that the proper keytab file is provided and it should have
	read options for the rsasoc user (user on which the Reporting
	Engine Server runs).
	Ensure that the system time is synchronized between KDC,
	Hadoop (HortonWorks) server, and the Reporting Engine system.

# Manage a Stream and Lockbox

You can manage a stream using the following procedures:

- Edit a Stream
- Reload the Stream
- Specify meta filters for a Stream
- Define muti-valued metas

## Edit a Stream

You can edit a stream to perform the following:

- Add more data sources to the stream.
- Delete existing data sources from the stream.

To edit a stream:

- 1. Go to **ADMIN > Services**.
- 2. In the Services view, select the added Warehouse Connector service and select  $\textcircled{\circ}$

> View > Config.

The Services Config view of Warehouse Connector is displayed.

RSA RESPOND INVESTIGATE MONITOR	CONFIGURE ADMIN			Š @ admin ⊗
A Change Service   Warehouse Connector   Config				
Sources and Destinations Streams Lockbox Settings	General Appliance Service Configuration			
Source Configuration		Destination Configuration		
+ -		+ - 🗵		
Address	Port	□ Name	Туре	Path
10.31.125.245	56004	NFS	nfs	/root/test/kaushal
10.31.125.248	56002	SFTP	sftp	/root/test
RSA   netwitness suite				

- 3. On the Streams tab, click  $\square$ .
- 4. In the Edit Stream dialog, you can perform the following:

• On the Available Sources tab, you can select the available data sources to add to the stream and click Save.

Edit Stream			×
Stream Name			
Destination			
Available Sources Curr	rent Sources		
Name	Address	Port	Session ID
:50004		50004	Enter Session
		Cancel	Save

On the Current Sources tab, you can delete an existing data source from the stream.
 Select the data source and click — .

Edit Stream				×
Stream Name				
Destination				
Available Sources Current Sou	ırces			
—		At least one	e source	is required
□ Name	Address		Port	
:50002			50002	
		Ca	ncel	Save

## **Reload the Stream**

When you reload the stream, the Warehouse Connector updates the schema file for the stream. You should reload the stream whenever you add a new custom meta to the Log Decoder or Decoder.

#### To reload the stream:

- 1. Go to **ADMIN** > **Services**.
- 2. In the Services view, select the added Warehouse Connector service and select  $\textcircled{\circ}$

#### > View > Config.

The Services Config view of Warehouse Connector is displayed.

- 3. On the **Streams** tab, select the stream that you want to reload.
- 4. Click Reload.

# Specify Meta Filters for a Stream

You need to specify the filter for each stream in the export.session.meta.fields parameter in the Explore view of the Warehouse Connector.

The following table lists the values that you can provide as a filter:

Values	Description
*	All the collected metas are written to SAW.
*, metal, meta2	All the metas except the defined metas are written to SAW. For example, Filter:*, ip.src All the metas except ip.src is written to SAW.
meta1, meta2, meta3	Only the defined metas are written to SAW.

**Note:** By default, the following metas are written to Warehouse even if you specify them in the filter:

- ng\_source

- unique id

- time

To specify meta filters for a Stream:

- 1. Go to **ADMIN** > **Services**.
- In the Services view, select a Warehouse Connector services and select > View > Explore.

RSA RESPOND INVESTIGATE	MONITOR CONFIGURE AD	MIN	ँ 🗘 🕅 admin 🛛 🧑
Hosts Services Event			
A Change Service   Warehouse Con	nector   Explore ©		
≡Warehouse Connect <	undefined	Warehouse Connector (Warehouse Connector)	
Warehouse Connector (WAREHOUSE_C	connections		-
□	logs		
	rest		
I C rest	services storedproc		
services	sys		-
12 istoredproc	users		
II 🗋 sys	warehouseconnector		
II 🗋 users	deviceappliance		-
warehouseconnector			
C config			
tats			
C deviceappliance			
< >			
RSA   NETWITNESS SUITE	1		A LEWIS CONTRACTOR OF A LEWIS CONTRACTOR OF A LEWIS CONTRACTOR OF A LEWIS CONTRACTOR OF A LEWIS CONTRACTOR A LE LEWIS CONTRACTOR A LE LE LEWIS CONTRACTOR A L

The Explore view of the Warehouse Connector service is displayed.

- In the options panel, select warehouseconnector > streams > <stream\_name> > loader > config.
- 4. In the export.session.meta.fields parameter, enter the filter.

RSA RESPOND INVESTIGATE	MONITOR CONFIGURE AD	MIN	Š . Ω @ admin ∞ 🥱
A Change Service   Warehouse Con	nector   Explore ©		
≡Warehouse Connect <	/warehouseconnector/streams/ /loader/config	Warehouse Connector (Warehouse Connector)	
	:50002	10231	
Warehouse Connector (WAREHOUSE_C	avro.load.interval	3	
Connections	bulk.copy	0	
II Cogs	destination.online	1	
III 🗀 rest	export.log.enabled	yes	
services	export.rollup	hour	
storedproc	export.session.enabled	yes	
🖾 🗀 sys	export.session.meta.fields	*	
🛙 🗀 users	hold.count	100000	
warehouseconnector	hold.interval	60	
Config	hold.size	512 MB	
C destinations	loader.stats.interval	1	
Sources	page.size	200000	
□ stats	permrejected.number	0	
C streams	rejected.size	0	
Testing	root	/testing	
C1 config	thread.count	4	
I loader	thread.pool.count	3	
	use.compression	deflate	
stats	wait.thread.pool	2	
□ schema ✓			
<	1		
RSA NETWITNESS SUITE			A LUMIN - THREE ADDRESS AND IN A MARKED

5. Restart the stream.

## **Define Multi-valued Metas**

You can also define an existing meta or a custom meta to be treated as multi-valued meta.

To define multi-valued metas:

**Caution:** Defining an existing meta to be treated as multi-valued may change the data type of the meta and cause the associated reports to fail.

- 1. Create a new file with the filename **multivalue-users.xml** in the /etc/netwitness/ng directory.
- 2. Add the following entries:

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<Netwitness>

<MultiValueMetas>

<Meta>NEWMETANAME</Meta>

</MultiValueMetas>

</Netwitness>
```

Where *NEWMETANAME* is the existing meta or a custom meta to be treated as multi-valued meta.

**Caution:** Make sure that you do not add metas that are by default treated as non multivalue.

3. Restart the stream.

# Manage a Lockbox

You can manage a lockbox using the following procedures:

- Change the Lockbox password
- Refresh the Lockbox

To change the Lockbox password:

- 1. Log on to NetWitness.
- 2. Go to **ADMIN** > Services.
- 3. In the Services view, select the added Warehouse Connector service, and select  $\diamond$



> View > Config.

The Services Config view of Warehouse Connector is displayed.

RSA RESPOND INVESTIGATE MONITOR	CONFIGURE ADMIN			ै ⊥़ @ admin ◎ ?
Hosts Services Event Sources Health & Wellness System Security				
Change Service   Warehouse Connector   Confi	g @			
Sources and Destinations Streams Lockbox Settings	General Appliance Service Configuration			
Source Configuration		Destination Configuration		
+ -		+ - 🗹		
Address	Port	Name	Туре	Path
10.31.125.245	56004	NFS	nfs	/root/test/kaushal
10.31.125.248	56002	SFTP	sftp	/root/test
R5A NETWITNESS SUITE				

4. Click the Lockbox Settings tab.

RSA RESPOND INVI	ISTIGATE MONITOR CONFIGURE ADMIN	○ ① <b>①</b> admin ⊗ ⑦
Hosts Services		
🛔 Change Service   Wa	rehouse Connector   Config $\odot$	
Sources and Destinations	Streams Lockbox Settings General Appliance Service Configuration	
Create New Lockbox		
Set the lockbox password. The pass	vord should satisfy lockbox password strength.You will be required to enter this password to perform any lockbox management.	
Lockbox Password	******	
Confirm Lockbox Password	******	
Apply		
Change Lockbox Pas	sword	
Change the lockbox password. You v	vill 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	******	
Apply		
Refresh Lockbox		
Reset the lockbox.You will be require	et to enter current lockbox password.	
Lockbox Password	******	
Apply		
RSA NETWITNESS SU		11100011700200300010001110000000

- 5. In the Change Lockbox Password section, perform the following:
  - a. In the Current Lockbox Password field, enter the current lockbox password.
  - b. In the New Lockbox Password field, enter the new lockbox password.

**Note:** The lockbox password must be at least eight characters in length and it 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.

- c. In the **Confirm New Lockbox Password** field, enter the new lockbox password to confirm.
- d. Click Apply.

The Lockbox password is successfully changed.

To refresh the Lockbox:

- 1. Log on to NetWitness.
- 2. Go to **ADMIN** > **Services**.

3. In the Services view, select the added Warehouse Connector service, and select 🌣 💿

> View > Config.

RESPOND INVESTIGATE MONITOR     Hosts Services Event Sources H     thange Service   Warehouse Connector   Config     purces and Destinations Streams Lockbox Settings     ource Configuration	© General Appliance Service Configuration	Destination Configuration		Ö Ω Ø admin ⊚ Ø
change Service   Warehouse Connector   Config	© General Appliance Service Configuration	Destination Configuration		
ources and Destinations Streams Lockbox Settings	General Appliance Service Configuration	Destination Configuration		
		Destination Configuration		
ource Configuration		Destination Configuration		
+ - ·		+ - 🗵		
Address	Port	Name	Туре	Path
10.31.125.245	56004	NFS NFS	nfs	/root/test/kaushal
10.31.125.248	56002	SFTP	sftp	/root/test
RSA   NETWITNESS SUITE				11000017000010000100000

The Services Config view of Warehouse Connector is displayed.

4. Click the Lockbox Settings tab.

RSA RESPOND INVI	STIGATE MONITOR CONFIGURE ADMIN	ਁ <u></u>
Hosts Services		
🛔 Change Service 🕴 🛛 Wa	rehouse Connector   Config 🐵	
Sources and Destinations	Streams Lockbox Settings General Appliance Service Configuration	
Create New Lockbox		
Set the lockbox password. The passw	vord should satisfy lockbox password strength.You will be required to enter this password to perform any lockbox management.	
Lockbox Password	******	
Confirm Lockbox Password	******	
Apply		
Change Lockbox Pas	sword	
Change the lockbox password. You v	vill 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	*******	
Apply		
Refresh Lockbox		
Reset the lockbox.You will be require	ed to enter current lockbox password.	
Lockbox Password	******	
Apply		
<b>RSA</b> NETWITNESS SU	ITE	1110001794580394611000088

- 5. In the **Refresh Lockbox** section, enter the current lockbox password in the **Lockbox Password** field.
- 6. Click Apply.

The Lockbox is reset.

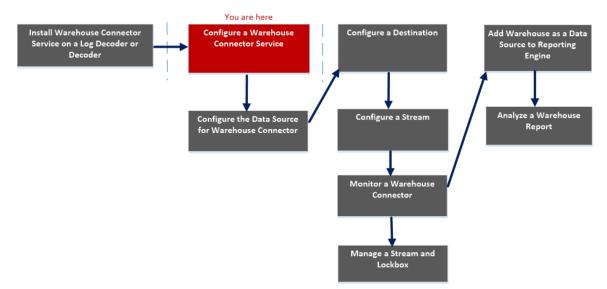
# Warehouse Connector Configuration References

This section contains descriptions of the user interface as well as other reference information.

#### **General Tab Settings**

The General tab displays the general configuration settings for Warehouse Connector service.

## Workflow



## What do you want to do?

Role	I want to	Refer to
Administrator	Install Warehouse Connector Service on a Log Decoder or Decoder	Install Warehouse Connector Service on a Log Decoder or Decoder or Hybrid
Administrator	Configure a Warehouse Connector Service*	<u>Configure a Warehouse Connector</u> <u>Service</u>
Administrator	Configure the Data Source for Warehouse Connector	Configure the Data Source for Warehouse Connector
Administrator	Configure the Destination using NFS, SFTP, WebHDFS.	Configure the Destination Using NFSConfigure the Destination Using SFTPConfigure the Destination Using WebHDFS

Role	I want to	Refer to
Administrator	Configure a Stream	Configure a Stream
Administrator	Monitor a Warehouse Connector	Monitor a Warehouse Connector
Administrator	Add Warehouse as Data Source to Reporting Engine	For more information, see "Add Warehouse as a Data Source to Reporting Engine" in the <i>Reporting Engine Configuration</i> <i>Guide</i> .
Administrator	Analyze a Warehouse Report	For more information, see "Step 4. Analyze a Warehouse Report" in the <i>Warehouse Guide</i> .
Administrator	Manage a Stream and Lockbox*	Manage a Stream and Lockbox

\*You can complete these tasks here.

## **Related topics**

• Configure a Warehouse Connector Service

# **Quick Look**

The following figure shows the General tab on the Warehouse Connector Services Config view. The General tab displays the system configuration parameters for the Warehouse Connector service.

RSA RESPOND INVESTIGATE MONITOR CONFIGURE ADMIN	💍 💭 🕅 admin 👳 😗
Hosts Services Event Sources Health & Wellness System Security	
A Change Service   Warehouse Connector   Config ©	
Sources and Destinations Streams Lockbox Settings General Appliance Service Configuration	
System Configuration	
Name	Config Value
Compression	0
Port	50020
SSL FIPS Mode	
SSL Port	56020
Stat Update Interval	1000
Threads	20
Αφ	ylqc
RSA NETWITNESS SUITE	Turner (Malakitikak) (applied

When you add a Warehouse Connector service, default values are in effect. RSA designed the default values to accommodate most environments and recommends that you do not edit these values because it may adversely affect performance.

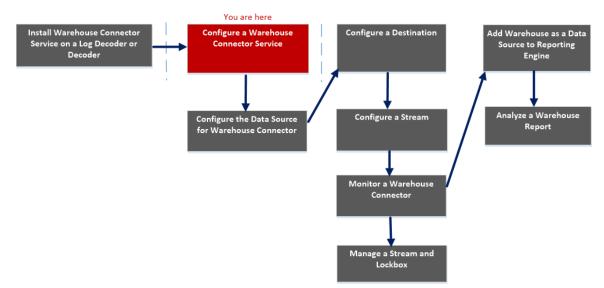
The following table describes the System Configuration parameters:

Name	Config Value
Compression	Determines the minimum amount of bytes before a message is compressed. If set to zero, messages are not compressed.
Port	Determines the port used by the service.          Note: If you change the port number, ensure that you restart the service.
SSL	If enabled, all the data transferred in the network will be encrypted using SSL.
Stat Update Interval	Determines how often (in milliseconds) statistic nodes are updated in the system.
Threads	Determines the number of threads in the thread pool to handle incoming requests.

#### **Appliance Service Configuration Tab Settings**

The Appliance Service Configuration tab displays the appliance configuration settings for Warehouse Connector service. For more information, see "Appliance Service Configuration" topic in the *Hosts and Services Getting Started Guide*.

#### Workflow



## What do you want to do?

Role	I want to	Refer to
Administrator	Install Warehouse Connector Service on a Log Decoder or Decoder	Install Warehouse Connector Service on a Log Decoder or Decoder or Hybrid
Administrator	Configure a Warehouse Connector Service*	<u>Configure a Warehouse Connector</u> <u>Service</u>
Administrator	Configure the Data Source for Warehouse Connector	Configure the Data Source for Warehouse Connector

Role	I want to	Refer to
Administrator	Configure the Destination using NFS, SFTP, WebHDFS.	Configure the Destination Using NFSConfigure the Destination Using SFTPConfigure the Destination Using WebHDFS
Administrator	Configure a Stream	Configure a Stream
Administrator	Monitor a Warehouse Connector	Monitor a Warehouse Connector
Administrator	Add Warehouse as Data Source to Reporting Engine	For more information, see "Add Warehouse as a Data Source to Reporting Engine" in the <i>Reporting Engine Configuration</i> <i>Guide</i> .
Administrator	Analyze a Warehouse Report	For more information, see "Step 4. Analyze a Warehouse Report" in the <i>Warehouse Guide</i> .
Administrator	Manage a Stream and Lockbox*	Manage a Stream and Lockbox

\*You can complete these tasks here.

## **Related topics**

• Configure a Warehouse Connector Service

# **Quick Look**

The following figure shows the different settings on the Appliance Service Configuration tab.

RSA RESPOND INVESTIGATE MONITOR CONFIGURE ADMIN	 (∰ admin ∞ ()
Hosts Services Event Sources Health & Wellness System Security	
Ange Service   Warehouse Connector   Config ©	
Sources and Destinations Streams Lockbox Settings General Appliance Service Configuration	
Name	Config Value
Compression	0
Port	50006
SSL FIPS Mode	
SSL Port	56006
Stat Update Interval	1000
Threads	20
	pply

When you add a Warehouse Connector service, default values are in effect. RSA designed the default values to accommodate most environments and recommends that you do not edit these values because it may adversely affect performance.

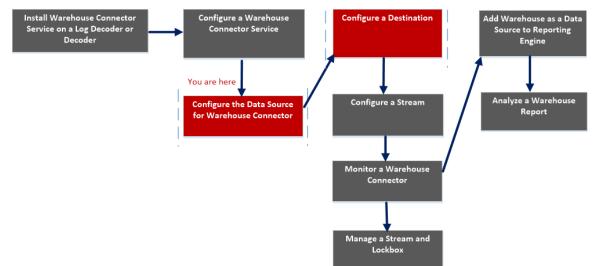
The following table describes the Appliance Service Configuration parameters:

Name	Configuration Value
Compression	Determines the minimum amount of bytes before a message is compressed. If set to zero, messages are not compressed.
Port	Determines the port used by the service.          Note: If you change the port number, ensure that you restart the service.
SSL FIPS Mode	If enabled, all the data transferred in the network will be encrypted using SSL FIPS.
SSL Port	Determines the SSL port used by the service.
Stat Update Interval	Determines how often (in milliseconds) statistic nodes are updated in the system.
Threads	Determines the number of threads in the thread pool to handle incoming requests.

#### **Sources and Destinations Configuration**

The Sources and Destinations tab for a Warehouse Connector in the Services Config view provides a way to manage basic service configuration and configure source and destination.

# Workflow



# What do you want to do?

Role	I want to	Refer to
Administrator	Install Warehouse Connector Service on a Log Decoder or Decoder	Install Warehouse Connector Service on a Log Decoder or Decoder or Hybrid
Administrator	Configure a Warehouse Connector Service	Configure a Warehouse Connector Service
Administrator	Configure the Data Source for Warehouse Connector*	Configure the Data Source for Warehouse Connector
Administrator	Configure the Destination using NFS, SFTP, WebHDFS*	Configure the Destination Using NFSConfigure the Destination Using SFTPConfigure the Destination Using WebHDFS

Role	I want to	Refer to
Administrator	Configure a Stream	Configure a Stream
Administrator	Monitor a Warehouse Connector	Monitor a Warehouse Connector
Administrator	Add Warehouse as Data Source to Reporting Engine	For more information, see "Add Warehouse as a Data Source to Reporting Engine" in the <i>Reporting Engine Configuration</i> <i>Guide</i> .
Administrator	Analyze a Warehouse Report	For more information, see "Step 4. Analyze a Warehouse Report" in the <i>Warehouse Guide</i> .
Administrator	Manage a Stream and Lockbox*	Manage a Stream and Lockbox

\*You can complete these tasks here.

#### **Related topics**

- Configure the Data Source for Warehouse Connector
- Configure the Destination

# **Quick Look**

The following figure shows the Sources and Destinations tab on the Warehouse Connector Services Config view.

Hosts Services Event Sources Health & Wellness System Security    Source Configuration   Source Configuration    Source Configuration <ul> <li>Pert</li> <li>Source Source</li> <li>Source Configuration</li> <li>Pert</li> <li>Source Source</li> <li>Source Source Source</li> <li>Source Source Source</li> <li>Source Source<th>INVESTIGATE MONITOR CONFIGURE ADMIN</th><th></th><th></th><th></th></li></ul>	INVESTIGATE MONITOR CONFIGURE ADMIN			
Sources and Destinations         Streams 1         Lockbox Settings         General         Appliance Service Configuration         2           Sources Configuration         +	Hosts Services Event Sources Health & Wellness System Security			
Source Configuration         Destination Configuration           + -         -           Address         Part           56004         NRFS         nfs	thange Service   Warehouse Connector   Config ⊚			
+ - ∠           Address         Part         Name         Type         Part.           1         5004         NFS         nfs         /root/test/Raudual	ources and Destinations Stream 1 Lockbox Settings General Appliance Service Configuration			
+ - ∠           Address         Part         Name         Type         Part.           1         5004         NFS         nfs         /root/test/Raudual	Source Configuration	Destination Configuration		
S6004     NFS     nfs     /root/test/kaushal	-	-		
	Address Port	Name	Туре	Path
C SEP stp //oot/test		NFS	nfs	/root/test/kaushal
	56002	SFTP	sftp	/root/test

The Sources and Destinations tab includes the following two sections:

1 Source Configuration

2 Destination Configuration

#### **Source Configuration**

The Source Configuration section allows you to configure the data sources from which the Warehouse Connector service needs to collect data.

The following is an example of the Source Configuration section.

Sc	Source Configuration		
+	-		
	Address	Port	
		56004	
	Status - Second	56002	

The Source Configuration section allows you to perform the following:

Features	Description
+	Add the data source.
-	Delete the data source.

#### **Destination Configuration**

The Destination Configuration section allows you to configure the destination to which the Warehouse Connector service needs to write the collected data.

Destination Configuration		
+ - 🗵		
□ Name	Туре	Path
NFS	nfs	/root/test/
SFTP SFTP	sftp	/root/test

The Destination Configuration section allows you to perform the following:

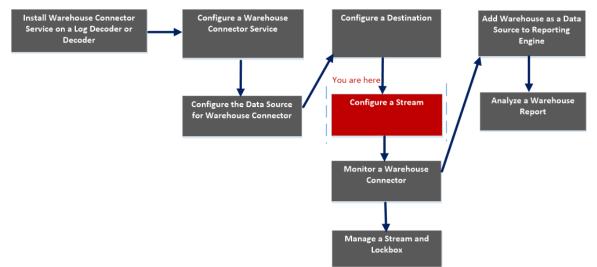
Features	Description
+	Add the destination.

Features	Description
-	Delete the destination.
	Edit the destination.
	<b>Note:</b> You can only edit the SFTP destination type.

## Add Stream Dialog

You can configure and add a stream to a Warehouse Connector in this dialog

## Workflow



## What do you want to do?

Role	I want to	Refer to
Administrator	Install Warehouse Connector Service on a Log Decoder or Decoder	Install Warehouse Connector Service on a Log Decoder or Decoder or Hybrid
Administrator	Configure a Warehouse Connector Service	<u>Configure a Warehouse Connector</u> <u>Service</u>
Administrator	Configure the Data Source for Warehouse Connector	Configure the Data Source for Warehouse Connector
Administrator	Configure the Destination using NFS, SFTP, WebHDFS.	Configure the Destination Using NFSConfigure the Destination Using SFTPConfigure the Destination Using WebHDFS

Role	I want to	Refer to
Administrator	Configure a Stream*	Configure a Stream
Administrator	Monitor a Warehouse Connector	Monitor a Warehouse Connector
Administrator	Add Warehouse as Data Source to Reporting Engine	For more information, see "Add Warehouse as a Data Source to Reporting Engine" in the <i>Reporting Engine Configuration</i> <i>Guide</i> .
Administrator	Analyze a Warehouse Report	For more information, see "Step 4. Analyze a Warehouse Report" in the <i>Warehouse Guide</i> .
Administrator	Manage a Stream and Lockbox*	Manage a Stream and Lockbox

\*You can complete these tasks here.

## **Related Topics**

• Configure a Stream

# **Quick Look**

The following figure is an example with the important features labeled.

roups		Se	ervi	ces 1					
- 🗷 O		+		- 🗹 📔 🐺 Licenses 🛞				💎 <sub>☉</sub> Filter	
me				Name	Licensed	Host	Туре	Version	Actions
∃ All	28		•	Event Stream Analysis	0	localhost.localdomain	Event Stream Analysis	11.0.0.373-1	\$ ⊙
			٠	Event Stream Analytics Server	0	localhost.localdomain	Entity Behavior Analytics	11.0.0.0	\$ ⊙
			٠	Investigate Server	0	localhost.localdomain	Investigate Server	11.0.0.0	•
			٠	Log Collector	0	localhost.localdomain	Log Collector	11.0.0.0-14450.1.e6da2ce	♦ ⊙
			٠	Log Collector	0	localhost.localdomain	Log Collector	11.0.0.0-14450.1.e6da2ce	•
			•	Log Collector	0	localhost.localdomain	Log Collector	11.0.0.0-14450.1.e6da2ce	\$ ⊙
			٠	Log Decoder	0	localhost.localdomain	Log Decoder	11.0.0.0-0	\$ ⊙
			0	Log Decoder	0	localhost.localdomain	Log Decoder		\$ ⊗
			٠	Orchestration Server	0	localhost.localdomain	Orchestration Server	11.0.0.0	\$ ⊙
			•	Reporting Engine	0	localhost.localdomain	Reporting Engine	11.0.0.0-5618.1.b20e69b	•
			٠	Response Server	0	localhost.localdomain	Response Server	11.0.0.0	•
			٠	Security Server	0	localhost.localdomain	Security Server	11.0.0.0	•
			٠	Warehouse Connector	0	localhost.localdomain	Warehouse Connector	System View	>
		M	•	Warehouse Connector	Ø	localbost localdomain	Warehouse Connector	Config Edit	

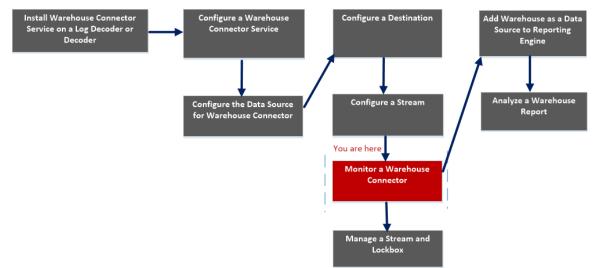
	CONFIGURE ADMIN ealth & Wellness System Security			Ô Ω @ admin ⊗ Ø
Sources and Destinations Streams Lockbox Settings	General Appliance Service Configuration ge Configuration ces		Destination	Status
_				
Add Stream			(B)	×
Stream Name *				
Select Destination *	Choose Destination	<b>v</b>		
Select Source *				
□ Name	Address	Port	Session ID	
		56004	Enter Session	
		56002	Enter Session	
1       Go to ADMIN > S         2       In the services view	S <b>ervices</b> . w, select a Warehouse	Cance Connector serv		
<ul><li>&gt;view&gt;config</li><li>3 In the Streams tab</li></ul>	, click 🕇 to view the	add stream dialo	.a.	
The following table desc	ribes the fields in the A	Add Stream dialo	og:	
Parameter Descri	ption			
	name of the stream. T rs and underscores. It			-
Select Select a Destination	destination from the d	rop-down list.		

Parameter	Description
Select Source	Select a source from the grid at the bottom section of the dialog.
Name	The name of the source.
Address	The address of the source.
Port	The port of the source.
Session ID	The session ID of the source.

#### **Streams Configuration**

The Streams tab for a Warehouse Connector in the Services Config view provides a way to manage stream configuration.

## Workflow



## What do you want to do?

Role	I want to	Refer to
Administrator	Install Warehouse Connector Service on a Log Decoder or Decoder	Install Warehouse Connector Service on a Log Decoder or Decoder or Hybrid
Administrator	Configure a Warehouse Connector Service	<u>Configure a Warehouse Connector</u> <u>Service</u>
Administrator	Configure the Data Source for Warehouse Connector	Configure the Data Source for Warehouse Connector
Administrator	Configure the Destination using NFS, SFTP, WebHDFS.	Configure the Destination Using NFSConfigure the Destination Using SFTPConfigure the Destination Using WebHDFS

Role	I want to	Refer to
Administrator	Configure a Stream*	Configure a Stream
Administrator	Monitor a Warehouse Connector*	Monitor a Warehouse Connector
Administrator	Add Warehouse as Data Source to Reporting Engine	For more information, see "Add Warehouse as a Data Source to Reporting Engine" in the <i>Reporting Engine Configuration</i> <i>Guide</i> .
Administrator	Analyze a Warehouse Report	For more information, see "Step 4. Analyze a Warehouse Report" in the <i>Warehouse Guide</i> .
Administrator	Manage a Stream and Lockbox*	Manage a Stream and Lockbox

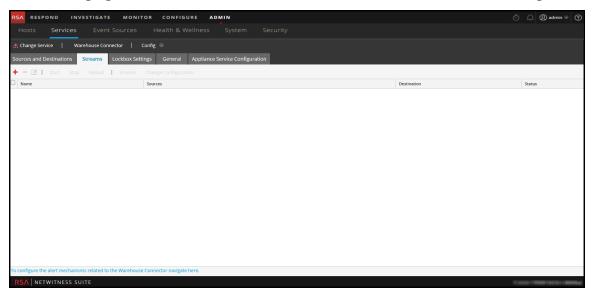
\*You can complete these tasks here.

# **Related topics**

Configure a Stream

# Quick Look

The following figure shows the Streams tab on the Warehouse Connector Services Config view.



The Streams tab allows you to perform the following:

Features	Description
+	Add a stream.
-	Delete a stream.
	Edit the stream.
Start	Start the stream.
Stop	Stop the stream.
Finalize	Finalize the stream.
Reload	Reload the stream. If you have added a new meta or if a new meta is added as part of content update to any of the sources, Log Decoder or Decoder, you need to reload the stream for the meta to be visible in the schema for the Reporting Engine. Reloading a stream does not have any impact on the data, but only the new meta list is fetched from the sources.

The following table describes the fields in the Streams tab:

Parameter	Description
Name	Name of the stream.
Sources	The sources associated with the stream.
Destination	The destinations associated with the stream.
Status	Status of the stream.

#### **Stream Statistics**

You can view the statistics of a configured stream. Click the  $\, \Theta \,$  icon next to the name of the stream.

RSA RESPOND INVESTIGATE MONIT	OR CONFIGURE ADMIN	Ŏ	
Hosts Services Event Sources			
A Change Service   Warehouse Connector   0	Config ©		
Sources and Destinations Streams Lockbox Sett	ings General Appliance Service Configuration		
+ - 🗹   Start Stop Reload   Finalize	Change Configuration		
☑ Name	Sources	Destination	Status
Stream Statistics Stream (Testing) Number of Iles in the permanent rejected fol Rejected fold wage in percentage : 0 Session Rate: 7 Destination (Testing) Source (1031) 125.246-50022) Status: containe Session Behind: 0 Latt Session Read: 16698	ser: 0		running

The following parameters are displayed in the Stream Statistics:

Section	Parameter	Description
Stream		
	Number of files in the permanent rejected folder	Determines the number of files in the permanent rejected folder (named, <b>permfail</b> ) in the Warehouse Connector. The permanent rejected folder contains the files that Warehouse Connector failed to write to the destination.
	Rejected folder usage in percentage	Determines the disk usage of the rejected folder.
	Session Rate	Determines the rate at which the session is processed by the Warehouse Connector for the source.
Destination		
	Status	Indicates the status of the destination.
Source		
	Status	Indicate the status of the source.
	Sessions Behind	Determines that number of sessions that needs to be processed by the Warehouse Connector.

Section	Parameter	Description
	Last Session read	Determines the last session id processed by the Warehouse Connector.

#### **Change Stream Configuration**

You can change configuration of a stream in runtime. In the **Streams** tab, click **Change Configuration** to change the configuration of the selected stream.

Change Configuration :	×
Stream Configuration	
Name	Config Value ~
Aggregation Configuration	
Aggregate max sessions	1000
Aggregation Interval	10
⊟ Loader Settings	
Compress files on disk.	deflate
Export Rollup Interval	hour
Maximum Message Hold Count	100000
Maximum Message Hold Interval (Seconds)	60
Maximum Message Hold Size	512 MB
Page Size	200000
Remote Export Path	/
Session Meta Fields Exported	*
Session Remote Export	
∃ Stream Settings	
Auto Startup	
	Close Apply

You can change the following parameters of the Stream Configuration:

**Note:** If you change the value of any parameter in stream configuration, make sure that you restart the stream.

After upgrading, if the values of Maximum Message Hold Count, Maximum Message Hold Interval and Maximum Message Hold Size are 3000000, 60 and 128 respectively, ensure that you assign the following values to the streams:

- Maximum Message Hold Count 2400000
- Maximum Message Hold Interval 600
- Maximum Message Hold Size 512

You can assign these values by modifying the existing Stream configuration.

Section	Parameter	Description			
	Aggregation Configuration				
	Aggregate max sessions	Determines the maximum number of sessions in a response for an aggregation request from the Warehouse Connector to the source .			
	Aggregation Interval	Determines the time between the responses from the source.			
		Loader Settings			
	Compress files on disk	<ul> <li>Enable to compress files on disk.</li> <li>Supported values: <ul> <li>Deflate - Provides smaller compressed files and good performance while generating reports.</li> <li>Off</li> <li>By default, the parameter is set to deflate.</li> </ul> </li> </ul>			

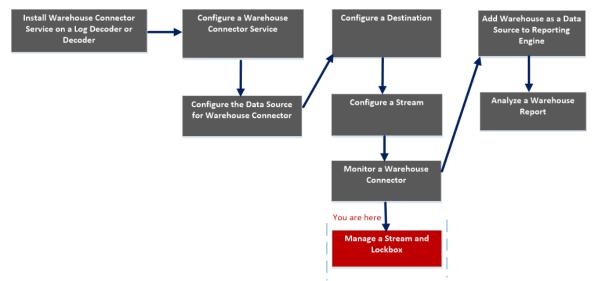
Section	Parameter	Description		
	Export Rollup Interval	Determines the roll-up interval for export files and also the directory structure the Warehouse Connector writes to the destination. For example: If the parameter is set to:		
		Value Directory Structure		
		hour /rsasoc/v1/[logs   sessions]/data/ {year}/{month}/{day}/{hour}		
		<pre>minute /rsasoc/v1/[logs   sessions]/data/ {year}/{month}/{day}/{hour}/ {minute}</pre>		
		day /rsasoc/v1/[logs   sessions]/data/ {year}/{month}/{day}		
		If you change the value of the parameter, ensure that you restart the stream. Recommended value is <b>hour</b> .		
	Maximum Message Hold	Determines the maximum number of sessions to store in the memory before processing.		
	Count	<b>Note:</b> If you have deployed a Warehouse Connector Virtual Appliance, make sure that you change the default value of the parameter to 800000.		
	Maximum Message Hold Interval (Seconds)	Determines the maximum time (in seconds) to hold the sessions in memory before processing.		
	Maximum Message Hold Size	Determines the maximum size for the sessions to store in the memory before processing.		

Section	Parameter	Description
	Remote Export Path	Determines the remote local mount point for HDFS (nfs://) and the location to export the data.
	Page Size	
		Stream Settings
	Auto Startup	Enable to automatically start the stream whenever the Warehouse connector process is restarted. By default, the parameter is set to <b>off</b> .

#### **Lockbox Settings**

The Lockbox Settings tab for a Warehouse Connector in the Services Config view provide a way to manage the lockbox settings.

## Workflow



## What do you want to do?

Role	I want to	Refer to
Administrator	Install Warehouse Connector Service on a Log Decoder or Decoder	Install Warehouse Connector Service on a Log Decoder or Decoder or Hybrid
Administrator	Configure a Warehouse Connector Service*	<u>Configure a Warehouse Connector</u> <u>Service</u>
Administrator	Configure the Data Source for Warehouse Connector	Configure the Data Source for Warehouse Connector

Role	I want to	Refer to
Administrator	Configure the Destination using NFS, SFTP, WebHDFS.	Configure the Destination Using NFSConfigure the Destination Using SFTPConfigure the Destination Using WebHDFS
Administrator	Configure a Stream	Configure a Stream
Administrator	Monitor a Warehouse Connector	Monitor a Warehouse Connector
Administrator	Add Warehouse as Data Source to Reporting Engine	For more information, see "Add Warehouse as a Data Source to Reporting Engine" in the <i>Reporting Engine Configuration</i> <i>Guide</i> .
Administrator	Analyze a Warehouse Report	For more information, see "Step 4. Analyze a Warehouse Report" in the <i>Warehouse Guide</i> .
Administrator	Manage a Stream and Lockbox*	Manage a Stream and Lockbox

\*You can complete these tasks here.

## **Related topics**

- <u>Configure a Warehouse Connector Service</u>
- Manage a Stream and Lockbox

# Quick Look

The following figure shows the Lockbox settings tab on the Warehouse Connector Services Config view.

RSA RESPOND INVI	ESTIGATE MONITOR CONFIGURE <b>ADMIN</b>	
Hosts Services		
Å Change Service   Wa	rehouse Connector   Config 🐵	
Sources and Destinations	Streams Lockbox Settings General Appliance Service Configuration	
Create New Lockbox		
Set the lockbox password. The pass	word should satisfy lockbox password strength.You will be required to enter this password to perform any lockbox management.	
Lockbox Password	******	
Confirm Lockbox Password	A+A+A+A+A	
Apply		
Change Lockbox Pas	sword	
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	R484848A	
Confirm New Lockbox Password	\$\$\$\$\$	
Apply		
Refresh Lockbox		
Reset the lockbox.You will be require	ed to enter current lockbox password.	
Lockbox Password	x4x4x4x4	
Apply		
RSA   NETWITNESS SU		111000110000000000000000000000000000000

The Lockbox Settings tab allows you to set, change, or refresh the lockbox password of the Warehouse Connector.