# NetWitness<sup>®</sup> Platform Version 12.4.0.0

Warehouse Connector Configuration Guide



Platform

## **Contact Information**

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

### Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <u>https://www.rsa.com/en-us/company/rsa-trademarks</u>. Other trademarks are trademarks of their respective owners.

### License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates 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 RSA.

### **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 NetWitness Community. 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

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

### Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

© 2024 RSA Security LLC or its affiliates. All Rights Reserved.

March, 2024

## Contents

Warehouse Connector Configuration	4
How Warehouse Connector Works	4
Install Warehouse Connector Service on a Log Decoder or Decoder or Hybrid	7
Configure a Warehouse Connector Service	8
Configure the Data Source for Warehouse Connector	9
Configure the Data Source	9
Update the Port Number and SSL Settings of the Data Source	10
Configure the Destination 1	2
Configure the Destination Using NFS	14
Configure the Destination Using SFTP	17
Configure the Destination Using WebHDFS	24
Configure a Stream 2	28
Create a Stream	28
Finalize a Stream	30
Start a Stream	31
Monitor a Warehouse Connector 3	62
Add Warehouse as a Data Source to Reporting Engine3	4
Analyze a Warehouse Report3	5
View the Warehouse Connector Service 3	6
Troubleshoot the Warehouse Connector 3	57
Manage a Stream3	;9
Manage a Lockbox 4	5
Warehouse Connector Pre-Upgrade and Post-Upgrade Steps 4	9
Warehouse Connector Configuration References 5	50
General Tab Settings	51
Appliance Service Configuration Tab Settings	54
Sources and Destinations Configuration	57
Add Stream Dialog	60
Streams Configuration	63
Lockbox Settings	70

## **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 the 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**

Warehouse Connector collects data from the data source to store it in the destination. The supported data sources are Log Decoder and Decoder.

### Destination

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

- 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 a single data source and destination or with multiple data sources and a single destination.

The Warehouse Connector:

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

### **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>.

#### Multi-Valued Meta Keys

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**

You can 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 option when 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.

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

The following is an overview on how to install and configure the Warehouse Connector service on Log Decoder or Decoder.

- Configuring the Warehouse Connector service on NetWitness,
- Configuring data sources,
- Destinations,
- Streams for Warehouse Connector,
- Configuring alert notifications on NetWitness.

**Note:** NetWitness Platform has added a Health & Wellness stat for Warehouse Connector to indicate the status of its Lockbox. Also, an out-of-the-box rule has been added so that a Health & Wellness alarm is raised when the Lockbox does not exist or cannot be opened.



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

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

# 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 in to NW Admin server
- Enter the following command on NetWitness Server: warehouse-installer --help The command line interface (CLI) usage descriptions are displayed.
- 3. Install Warehouse Connector service by executing the following command: warehouse-installer --host-key <ID, IP address, hostname or display name of Decoder, Log Decoder, or Hybrid host>
- 4. Restart the Warehouse Connector using following command: service nwwarehouseconnector restart

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

Note: If you have custom-defined host entries in /etc/hosts, make sure to have the same entires in /etc/hosts.user. Run the following command to ensure that the host names are updated in this installation: nw-manage --refresh-host --host-key <ID, IP, hostname or display name of host> For more information, see "Manage Custom Host Entries in /etc/hosts" in the System Maintenance Guide.

## **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.

XNETWITNESS Platform Investigate Respond Users Hosts Files Dashboard Reports	Ö 🗘 로 % ⑦ admin 🗸
HOSTS SERVICES EVENT SOURCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY	
🚠 Change Service   decoder - Warehouse Connector   Config 🐵	
Sources and Destinations Streams Lockbox Settings General Appliance Service Configuration	
Create New Lockbox	
Set the lockbox password. The password should satisfy lockbox password strength. You will be required to enter this password to perform any lockbox management.	
Lockbox Password *******	
Confirm Lockbox Password +++++++	
Apply	
Change Lockbox Password	
Change the lockbox password. You will be required to enter current password and new password. The password should satisfy lockbox password strength.	
Current Lockbox Password *******	
New Lockbox Password *******	
Confirm New Lockbox Password ******	
Apply	
Refresh Lockbox	
Reset the lockbox.You will be required to enter current lockbox password.	
Lockbox Password +++++++	
Apply	

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**

There are two procedures for configuring the data source for the Warehouse Connector:

- 1. First, you must configure the data source.
- 2. Then, you need to update the Port Number and SSL Settings for the Data Source.

## **Configure the Data Source**

To configure the data source:

- 1. Log on to NetWitness.
- 2. Go to (Admin) > Services.
- 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 to the port number or SSL settings of the Warehouse Connect data sources, you can update the changes in Explore view of the Warehouse Connector.

Make sure that:

- You have the changed port number or SSL settings of the data source.
- You have stopped the streams related to the data source that is updated with the port number or SSL settings.

To update the port number or SSL settings:

- 1. Log on to NetWitness.
- 2. Go to **(Admin) > Services**.
- 3. In the Services view, select the added Warehouse Connector service and select > **Explore**.

The Service Explore view of Warehouse Connector is displayed.

KITWITNESS   Platform	Investigate Respond Users Hosts Files Dashboard Reports			admin 🗸
HOSTS SERVICES EVENT SOUR	CES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY			
🚠 Change Service   decoder - Wareh	puse Connector   Explore ©			
Change Service   decoder - Wareh decoder - Warehouse Connector (WARE  Connections  deviceappliance  logs  rest services  services  warehouseconnector  warehouseconnector	Indecoder - Warehouse Connector (WAREHOUSE_CONNECTOR) decoder - Warehouse Connector connections deviceappliance logs rest services storedproc sys users warehouseconnector			
4				

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

	vestigate Respond Users Hosts Files Dashboard Reports	Ō	Ŵ	14	* (	?) admi	n 🗸
HOSTS SERVICES EVENT SOURCES	ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY						
A Change Service   decoder - Warehouse	Connector   Explore $\otimes$						
Connections Connector (WAREH Connectors Connectors Connectors Connectors Connectors Connectors Connectors Connector Connec	decoder - Warehouse Connector  inections  iceappliance is  iceappliance is  iceapce iceace ic						

- 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:

- 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\_ folder>/rsasoc/v1/sessions/data/<year>/<month>/<day>/<hour>/
- /<staging\_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:

- 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.
- In the Services view, select the Warehouse Connector service, and select > View > Config. The Services Config View of Warehouse Connector is displayed.

	ate Respond Us	ers Hosts Files	Dashboard Reports		⊙ ໍ 로 % ⑦ admin ✔
HOSTS SERVICES EVENT SOURCES ENDPOIN		WELLNESS SYSTEM S			
A Change Service   Warehouse Connector   Config					
Sources and Destinations Streams Lockbox Settings	General Appliance Se	rvice Configuration			
Source Configuration			Destination Configuration		
+ -			+ - 🗷		
Name	Address	Port	Name	Туре	Path
logdecoder1 - Log Decoder	1111-12-28	56004	NFS	nfs	/root/test/kaushal
logdecoder2 - Log Decoder	1010103-040	56002	SFTP	sftp	/root/test

- 4. On the Sources and Destinations tab, in the Destination Configuration section, click 🕇.
- 5. In the Add Destination dialog, from the Type drop-down list, select NFS.
- 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 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	1

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:



b. In the Services view, select the added Warehouse Connector service, and select > Explore.

The Explore view of Warehouse Connector is displayed.

KITWITNESS   Platform	Investigate Respond Users Hosts Files Dashboard Reports		? adr	min 🗸
HOSTS SERVICES EVENT SOUR	CES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY			
🚠 Change Service   decoder - Wareh	ouse Connector   Explore ©			
Change Service   decoder - Warehouse <  Change Service   decoder - Warehouse <  Change Service   decoder - Warehouse Connector (WARE Change Service   deviceappliance Change Services Change Service   deviceappliance Change Serviceappliance Change Servicea	buse Connector I Explore			

- 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 isChecksumValidationRequired to 1.

KITWITNESS   Platfo	🗂 Investigate Respond Users Hosts Files Dashboard Reports	ф (	3 %	admin 🗸
HOSTS SERVICES EVENT SOUR				
A Change Service   Warehouse Conr	ector   Explore ⊗			
≡Warehouse Connect <	/warehouseconnector/destinations/NFS/config Warehouse Connector (Warehouse Connector)			
	isChecksumValidationRequired 1			
	root /root/test/kaushal			
	subtype nfs			
	type hdfs			
□				
warehouseconnector				
C config				
destinations				
II CI NFS				
Config				
SFTP				
III 🗀 sources				
C stats				
C 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. Log in 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 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. SSH to the Warehouse Connector.
  - b. Type the following command and press ENTER:
    - \$ OWB\_FORCE\_FIPS\_MODE\_OFF=1 ssh-keygen -t ecdsa -b 521
  - 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 ecdsa):

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.

**Note:** If the SSH key is not generated in the default location (/root/.ssh/id\_ecdsa), you need to configure the destination for warehouse connector through Explore view. For more information, see To configure the destination through Explore view:.

e. Change the directory by entering the following command:

cd /root/.ssh/

f. Move the generated key to the below location:

```
mv ~/.ssh/id_ecdsa ~/.ssh/id_ecdsa.old
```

g. Type the following command and press ENTER:

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

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 ~/.ssh/id\_ecdsa

- j. Copy the generated public key to append to the remote Warehouse host or Hadoop node. ssh-copy-id -i ~/.ssh/id ecdsa.pub root@<destination host ipaddress>
- 2. SSH to remote Warehouse host or Hadoop node as "ssh '<user>@<ip address>", if identity key file is at default location.

or

SSH to remote Warehouse host or Hadoop node as "ssh '<user>@<ip address> -i <identity file path>", If identity key file is not at default location.

3. 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 Warehouse Connector to use SFTP destination

**Note:** If the SSH key is not generated in the default location (/root/.ssh/id\_ecdsa), you need to configure the destination through Explore view. For more information, see <u>To configure the destination</u> through Explore view:

#### To configure the destination through User Interface:

- 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.

	gate Respond Us	ers Hosts Files	Dashboard Reports		Õ ♫ ☞ ‰ ⑦ admin ✔
HOSTS SERVICES EVENT SOURCES ENDPOIN		WELLNESS SYSTEM S	ECURITY		
🚠 Change Service   Warehouse Connector   Config					
Sources and Destinations Streams Lockbox Settings	General Appliance Se	vice Configuration			
Source Configuration			Destination Configuration		
+ -			+ - 🗵		
Name	Address	Port	Name	Туре	Path
logdecoder1 - Log Decoder	0101100100	56004	NFS	nfs	/root/test/kaushal
logdecoder2 - Log Decoder	01010000	56002	SFTP SFTP	sftp	/root/test
1					

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 password-based access.
  - SSH passphrase If you are using SFTP to write data into the destination using SSH key-based 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.

XNETWITNESS   Platform	Investigate Respond Users Hosts Files Dashboard Reports		?) ad	dmin 🗸
HOSTS SERVICES EVENT SOU	RCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY			
A Change Service   decoder - Ware	iouse Connector   Explore 🐵			
decoder - Warehous      Connector (WARE.     Connectors     Connections     Consections     Consections     Consections     Consections     Consections     Consections     Consections     Consections     Consections	/decoder - Warehouse Connector (WAREHOUSE_CONNECTOR) decoder - Warehouse Connector connections deviceappliance logs rest services storedproc			
storedproc     sys     users     warehouseconnector	sys users warehouseconnector			

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.

NOTS     SERVICE     EVENT SOURCES     ENDPOINT SOURCES     HEALTH & WELLNESS     SYSTEM     SERVITY       A, drange Service     Warehouse Connector     Explore ©     Image: Service     Image: Service		orm Investigate Respond U	Jsers Hosts Files Dashboard Reports	Ō.	¢_8	1 %	0	admin 🗸
Anange Service Warehouse Connector     Warehouse Connector     Warehouse Connector (WAREHOUSE, Conector)     Worehouse Connector (WAREHOUSE, Conector)     Momenhotts.file     Possord     Nore     Nore / Conector (WAREHOUSE, Conector)     Momenhotts.file     Possord     Nore / Conector (WAREHOUSE, Conector)     Subsystem     Subsystem </td <td>HOSTS SERVICES EVENT SOUR</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	HOSTS SERVICES EVENT SOUR							
Warehouse Connector,          Avarehouse connector (Warehouse Connector),            Momenhouse Connector (WAREHOUSE, Con         Hommahotts, file           Diags         root         /root/test           Diags         icCnector (WAREHOUSE, Con         /root/test           Diags         isCnector (WAREHOUSE, Con         /root/test           Diags         iscnector (WAREHOUSE, Con         /root/test           Diags         subsys         istner         /root/test           Diages         subsys         subsys         istner           Diages         istner         /root         /root           Diages         istner         /root         /root           Di	A Change Service   Warehouse Conr	nector   Explore ©						
Inst         10.31/20.44.22           B_ierrois         pp         hdfs           B_ierrois         uername         root           B_igs         subope         sftp           B_ierrois         subope         sftp           B_ierrois         subope         sftp           B_ierrois         stp         stp           B	Warehouse Connect <  Warehouse Connector (WAREHOUSE_CO Connections Clogs Clogs	/warehouseconnector/destinations/SFIP/config v known.hosts.file password root isChecksumValidationRequired	Warehouse Connector (Nerehouse Connector) >					
90         000           uerame         root           000000000000000000000000000000000000	□ services	host	10.31.204.44:22					
III jays     subtype     sftp       III jays     sibtype     sftp	storedproc	username	root					
		subtype	sfφ					

e. Restart the respective stream.

To configure the destination through Explore view:

- 1. Go to (Admin) > Services.
- 2. In the Services view, select the added Warehouse Connector service, and select > View
   > Explore.

	Investigate Respond Users Hosts Files Dashboard Reports	Ö	Ω I	10 %	; 0	admin 🗸
HOSTS SERVICES EVENT SOUR	CES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY					
A Change Service   decoder - Wareh	use Connector   Explore ()					
Change Service decoder - Wareh     decoder - Warehouse Connector (WARE     Connections     deviceappliance     logs     conrections     convections     convections	lase Connector   Explore ◎ /decoder - Warehouse Connector (WAREHOUSE_CONNECTOR) decoder - Warehouse Connector connections deviceappliance logs rest services storedproc sys userbouseconnector					

#### The Explore view of Warehouse Connector is displayed.

3. Right click on "warehouseconnector" node and select properties.

NETWITNESS   Platform	Investigate Respond Users Hosts Files	Dashboard Reports	Ö 🗘 🗷 % 🕐 admin 🗸
HOSTS SERVICES EVENT SOU	RCES ENDPOINT SOURCES HEALTH & WELLNESS		
🚠 Change Service   decoder - Wareł	ouse Connector   Explore ©		
單 decoder - Warehous <	Awarehouseconnector	decoder - Warehouse Connector	
	stats		
i stats	Properties for decoder - Warehouse Co add Parameters Message Help Add a source, destination or a stream to this archiver. security:roles: warehouseconnector.manage parameters: source - <string. an="" be="" i<br="" must="" optional,="" value="" {ip-address:the="">Response Output</string.>	DDNECTOR (WAREHOUSE_CONNECTOR) / Wa	> The connection endpoint (ip:port) of a NetWitness

4. Select "add" property and manually enter the below config parameters. name=<destination name> destination=sftp://<destination path> host=<destination host ipaddress:port> type=hdfs port=22 username=<username> password=<password> privKeyFile=<private key file path>

## Aggregate Metas and Raw Logs for a Log Session

To aggregate raw logs and metas from Log Decoder into a single AVRO file instead of two folders.

- 1. Go to **ADMIN** > **Services**.
- Select a Warehouse Connector service and click > View > Explore. The Explore view for the Warehouse Connector is displayed.
- 3. Open warehouseconnector/streams/<stream name>/loader/config and in the right pane, select the export.logAndsession.avro.enabled parameter.
- 4. Change the value to **yes**.
- 5. Restart the service.
- 6. Go to **ADMIN** > **Services**.
- 7. Select a Warehouse Connector service and click **\* View** > **Config**.
- 8. On the Streams tab, select the stream that you want to reload.
- 9. Click Reload.

## **Configure the Destination Using WebHDFS**

Make sure that you have:

- Installed the Warehouse Connector service or virtual appliance in your network environment.
- 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 🔅 🕑 > View

#### > Config.

The Services Config view of Warehouse Connector is displayed.

	ate Respond Us	ers Hosts Files	Dashboard Reports		⊙ ໍ 로 % ⑦ admin ✔
HOSTS SERVICES EVENT SOURCES ENDPOIN			ECURITY		
A Change Service   Warehouse Connector   Config					
Sources and Destinations Streams Lockbox Settings	General Appliance Ser	vice Configuration			
Source Configuration			Destination Configuration		
+ -			+ - 🗵		
Name	Address	Port	Name	Туре	Path
logdecoder1 - Log Decoder	0100100000	56004	NFS	nfs	/root/test/kaushal
logdecoder2 - Log Decoder	0100-020-000	56002	SFTP SFTP	sftp	/root/test

- 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.

WebHDFS	~
	\$
Cancel	Save
	WebHDFS

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		~	
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.

	Investigate Respond Users Hosts Files Dashboard Reports	Ō	¢	R	%	?) a	idmin 🗸
HOSTS SERVICES EVENT SOUR	CES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY						
A Change Service   decoder - Wareh	ouse Connector   Explore ©						
Change Service decoder - Wareh  Change Service decoder - Warehouse  Connections  Connections	Idecader - Warehouse Connector (WAREHOUSE_CONNECTOR) decader - Warehouse Connector Connections deviceappliance logs rest services storedproc sys users warehouseconnector						
(							

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

XNETWITNESS   Platfo	rm Investigate Respond U	lsers Hosts Files Dashboard Reports	친 다. ㄹ % ⑦ admin ✔
HOSTS SERVICES EVENT SOUR	CES ENDPOINT SOURCES HEALTH	& WELLNESS SYSTEM SECURITY	
A Change Service   Warehouse Conr	ector   Explore ⊙		
≡Warehouse Connect <	/warehouseconnector/destinations/NFS/config	Warehouse Connector (Warehouse Connector)	
	isChecksumValidationRequired	1	
	root		
	subtype	nfs	
	type	hdfs	
I users			
warehouseconnector			
C config .			
C destinations			
II CI NFS			
E SFTP			
□ _ sources			
C stats			
C deviceappliance			

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 "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 Configure the Destination.

#### 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.
- In the Services view, select the added Warehouse Connector service and select >View > Config.

The Services Config view of Warehouse Connector is displayed.

3. Click the **Streams** tab.

	🔆 NETWITNESS   Platfoi	rm Investigate Respond	Users Host	s Files [	Dashboard Reports		ö ↓ <b>Ξ %</b>	⑦ admin ✔
	HOSTS SERVICES EVENT SOURCES	ENDPOINT SOURCES HEALTH & WEL	LNESS SYSTEM	SECURITY				
	A Change Service   Warehouse Connector	Config ⊙						
	Sources and Destinations Streams Lockb	box Settings General Appliance Service C	Configuration					
	+ - 🛛   Start Stop Reload   Fin	Sources			Destina	tion	Status	
	<b>0</b>				line and		running	
4.	On the <b>Streams</b> tab, Add Stream Stream Name * Select Destination *	click 🕂 .		~	e×			
	Select Source *							
	Name	Address	Port	Se	ssion ID			
			56004	En	ter Session			
			56002	En	ter Session			
				Cancel	Save			

- 5. In the Add Stream dialog, perform the following steps:
  - 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 a Stream

#### To finalize the stream:

- 1. Go to **(Admin) > Services**.
- 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 Finalize.

## Start a 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**.
- 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**.
- In the Services view, select the added Warehouse Connector service and select > View
   Config.

The Services Config view of Warehouse Connector is displayed.

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

The Warehouse Connector Monitoring view is displayed.

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 Offline 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 report against this Reporting Engine. For more information, see "Add Warehouse as a Data Source to Reporting Engine" 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" 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.

🔆 NETW	ITNESS P	l <mark>atform</mark> Investigate R	espond Users Hosts Files	Dashboard Repo	orts Ö	û ≅ % ? admin ✔
HOSTS S	ERVICES EV		SOURCES HEALTH & WELLNESS			
🚠 Change Ser	vice   deco	oder - Warehouse Connector	System ©			
📕 Host Tasks	😃 Shutdown S	ervice 🖞 Shutdown Appliance S	ervice 🖞 Reboot			
Warehou	se Connecto	or Service Information		Appliance	Service Information	
Name	decoder (Ware	house Connector) UNLICENSED		Name	decoder (Host)	
Version	12.0.0.0 (Rev n	(11)		Version	12.2.0.0 (Rev null)	
Memory Usag	e 31128 KB (0.19	% of 16046 MB)		Memory Usage	30392 KB (0.18% of 16046 MB)	
CPU	3%			CPU	0%	
Running Since	2022-Sep-27 0	9:40:40		Running Since	2022-Sep-27 10:07:53	
Uptime	1 day 3 hours 2	8 minutes 50 seconds		Uptime	1 day 3 hours 2 minutes 42 seconds	
Current Time	2022-Sep-28 1	3:09:30		Current Time	2022-Sep-28 13:10:35	
Warehou	se Connecto	or User Information		Host User	Information	
Name	admin			Name	admin	
Groups	Administrators			Groups	Administrators	
Roles	Roles connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage, warehouseconnector.manage		Roles	appliance.manage, connections.manage, logs.manage, service storedproc.execute, storedproc.manage, sys.manage, users.m	s.manage, anage	
Session Ir	nformation					
Session		User	IP Address		Login Time ^	Active Queries
182		admin	[::1]:53094		2022-Sep-27 09:40:46	0
211		admin	[::1]:53098		2022-Sep-27 09:40:46	0
361		escalateduser	10.125.249.2:33690		2022-Sep-28 06:54:10	0
482		admin	10.125.249.2:33690		2022-Sep-28 12:29:46	0
517		admin	10.125.249.2:35348		2022-Sep-28 12:33:12	0
4						۰.

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		€×3
Source Type *	WAREHOUSE ~	,
Warehouse Source *	HiveServer2 ~	,
Name *	PDH2.0-DCA	
HDFS Path *	/	
Advanced		
Host *		
Port *	10000	
Username *	gpadmin	
Password	******	
Kerberos Authentication		
Server Principal *		
User Principal *		
Kerberos Keytab File *		
Enable Jobs		
Test Connection		
	Cancel	Save

The following figure shows the New Service dialog.

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

Error	Possible Solutions					
Could not open connection to HiveServer	<ul> <li>Ensure that the HiveServer2 is running on the Host.</li> <li>Check if the port provided can be accessible from the Reporting Engine server.</li> </ul>					
No Schema found in HDFS path	Ensure that meta avro data file(s) are available in the HDFS path ( <b>HDFS Path&gt;/rsasoc/v1/sessions/meta</b> ) mentioned. The following figure shows an example of the command to check the files in hdfs.					
<pre>[root@NWAPPLIANCE ~] # hadoop fs -lsr /testdata/rsasoc/v1/sessions/meta 14/12/09 10:31:59 INFO util.NativeCodeLoader: Loaded the native-hadoop library 14/12/09 10:31:59 INFO security.JniBasedUnixGroupsMapping: Using JniBasedUnixGroupsMapping for Group resolution -rwxr-xr-x 3 root root 3076 2013-08-28 01:09 /testdata/rsasoc/v1/sessions/meta/nwdev-testing.avro</pre>						
Could not open connection to HiveServer, GSS initiate failed	GSS initiate failed errors will be observed only in the case of Kerberos enabled Hive. 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.					

## Add SFTP Destination

To add SFTP destination to Warehouse Connector, you need to follow the below steps:

- 1. SSH to NetWitness Host and run the following command to edit ssd\_config file: vi/etc/ssh/sshd\_config file
- 2. Do not comment HostKey/etc/ssh/ssh\_host\_rsa\_key
- 3. You must append KexAlgorithms +diffie-hellman-group14-sha1, diffie-hellmangroup-exchange-sha1
- 4. Run the following command to restart NetWitness Host: systemctl restart sshd
- 5. On Warehouse Connector Host SSH to NetWitness Host and run the following command: ssh -o "HostKeyAlgorithms ssh-rsa" root@<NWhost\_IP> For example, ssh -o "HostKeyAlgorithms ssh-rsa" root@10.10.10.10
- 6. Run the following curl command on Warehouse Connector Host to authenticate: curl -vvvv sftp://root:netwitness@<NWhost\_ip>:22/root/ For example, curl -vvvv sftp://root:netwitness@<10.10.10.10>:22/root/
- 7. You can now add SFTP Destination from UI.

## Manage a Stream

You can manage a stream using the following procedures:

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

## Edit a Stream

You can edit a stream to perform the following:

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

To edit a stream:

- 1. Go to (Admin) > Services.
- In the Services view, select the added Warehouse Connector service and select > View
   > Config.

The Services Config view of Warehouse Connector is displayed.

🔆 NETWITNESS   Platform Investigate Respond Users Hosts Files Dashboard Reports 💍 🗘 🗷 🖄 🕐 admin 🦄										
HOSTS SERVICES EVENT SOURCES ENDP	HOSTS SERVICES EVENT SOURCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY									
A Change Service   Warehouse Connector   Co	At Change Service   Warehouse Connector   Config ©									
Sources and Destinations Streams Lockbox Settings General Appliance Service Configuration										
Source Configuration Destination Configuration										
+ -	+									
Name	Address	Port	Name	Туре	Path					
logdecoder1 - Log Decoder	1010-101-00	56004	NFS	nfs	/root/test/kaushal					
logdecoder2 - Log Decoder	1010-101-00	56002	SFTP SFTP	sftp	/root/test					
•										

- 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	ent 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	irces			
-		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 must reload the stream when you add a new custom meta to the Log Decoder or Decoder.

#### To reload the stream:

- 1. Go to (Admin) > Services.
- 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 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 > Config. The Explore view of the Warehouse Connector service is displayed.

	Investigate Respond Users Hosts Files Dashboard Reports	Ö	¢	8	K (	?) a	admin 🗸
HOSTS SERVICES EVENT SOUR	CES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY						
🚠 Change Service   decoder - Wareh	ouse Connector   Explore 🐵						
Change Service decoder - Wareh decoder - Warehouse Connector (WARE Connections Connect	Vaccoder - Warehouse Connector Varehouse Connector Varehouse Connector Conne						
4							

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

	o <mark>rm</mark> Investigate Respond U	Jsers Hosts Files Dashboard Reports	Ů 슈 콜 ‰ ⑦ admin ✔
HOSTS SERVICES EVENT SOUR	CES ENDPOINT SOURCES HEALTH &	WELLNESS SYSTEM SECURITY	
A Change Service   Warehouse Con	nector   Explore ©		
₩arehouse Connect <	/warehouseconnector/streams/ /loader/config	Warehouse Connector (Warehouse Connector)	
	:50002	10231	
Warehouse Connector (WAREHOUSE_C	avro.load.interval	3	
Connections	bulk.copy	0	
	destination.online	1	
□ ] rest	export.log.enabled	yes	
Services	export.rollup	hour	
storedproc	export.session.enabled	yes	
□ C sys	export.session.meta.fields	*	
users	hold.count	100000	
warehouseconnector	hold.interval	60	
C config	hold.size	512 MB	
destinations	loader.stats.interval	1	
sources	page.size	200000	
🗋 stats	permrejected.number	0	
streams	rejected.size	0	
Testing	root	/testing	
□ config	thread.count	4	
C loader	thread.pool.count	3	
🗋 config	use.compression	deflate	
🗅 stats	wait.thread.pool	2	
🗅 schema			
< > >			

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 multi-value.

3. Restart the stream.

#### View the current schema

You can view the current schema that is used by warehouse connector for writing in AVRO files.

#### To view the current schema:

- 1. Go to **(Admin) > Services**.
- In the Services view, select a Warehouse Connector services and select > View > Explore.
   The Explore view of the Warehouse Connector service is displayed.
- 3. In the options panel, select warehouseconnector > streams > <stream\_name> > config.
- 4. Set the value for refresh.schemanode.enabled parameter to true. By default, this value is set to false.

KITWITNESS   Platfo	orm Investigate Respond Users Ho	sts Files Dashboard Reports 💍 🛱 🗄	z 🔏 🕐 admin 🗸
HOSTS SERVICES EVENT SOUR	RCES ENDPOINT SOURCES HEALTH & WELLNESS		
A Change Service decoder141 - Wa	arehouse Connector   Explore $\odot$		
■ decoder141 - Wareh <	/warehouseconnector/streams/ #2000 config	decoder141 - Warehouse Connector	
	aggregate.nice	true	
services	aggregate.sessions	1000	
storedproc	aggregation.interval	10	
sys	auto.startup	off	
users	destination	/warehouseconnector/destinations/	
warehouseconnector	free.space	1024 MB	
C1 config	handle.multivalue	false	
destinations	heartbeat.error	120	
sources	heartbeat.interval	10	
	max.pending	80	
 ■ ⇔ streams	refresh.schemanode.enabled	true	
	rejected.maxusage	30 A configuration node whose value can alter system behavior	
	sources	/warehouseconnector/sources/10.101.33.141:50004	-
	state	running	
	stream.data.path	/var/netwitness/warehouseconnector/bulk/1P104C	
	stream.id	1589975797421821	
<	stream.startpercent	50	
	•	-	

- 5. Reload the stream. For more information see, <u>Reload the Stream</u>.
- 6. Restart the Warehouse Connector service.
- 7. Go to **(Admin) > Services**.

- 8. In the Services view, select a Warehouse Connector services and select > View > Explore. The Explore view of the Warehouse Connector service is displayed.
- 9. In the options panel, select warehouseconnector > streams > <stream\_name> > schema, to view the current schema.

**Note:** You must to reload the stream every time, before you want to view the current schema or you can add a scheduler to reload the stream automatically at regular intervals as mentioned in step 10.

- 10. (Optional) To reload the stream automatically at regular intervals, follow the below steps.
  - a. Go to **(Admin) > Services**.
  - b. In the Services view, select a Warehouse Connector services and select > View
     > Explore.

The Explore view of the Warehouse Connector service is displayed.

- c. In options panel, select warehouseconnector > sys > config > scheduler. Right click and select properties.
- d. In the property drop down select addInter and in the **Parameters** text box, add "hours=24 pathname=/warehouseconnector/streams/<stream name> msg=reload".

L ·		
	orm Investigate Respond Users Hosts Files Dashboard Reports 💍 🗘 🖃 🎉 ၇ admin	~
HOSTS SERVICES EVENT SOUR	RCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY	
🚠 Change Service   decoder141 - Wa	arehouse Connector   Explore ©	
≡decoder141 - Wareh <	/sys/config/scheduler decoder141 - Warehouse Connector	
decoder141 - Warehouse Connector (WAR		
Connections		
deviceappliance		
🖾 🗀 logs		
🖾 🗀 rest		
services	Properties for decoder 141 - Warehouse Connector (WAREHOUSE_CONNECTOR) /sys/config/scheduler.	×
II Storedproc	addinter v Parameters hours=24 pathname=/warehouseconnector/streams/international msg=reload Send	
■ 🗁 sys	Message Help	
■ 🗁 config	Add a new scheduled task on an interval security.roles svs.manaze	1
🗋 scheduler	parameters:	
C stats	seconds - <uint32, 3155926}="" optional,="" to="" {range:1=""> The number of seconds between executions, must provide one of seconds, minutes or hours</uint32,>	•
tasks	Personal Charter	
🖾 🗋 users	nesponse output	
warehouseconnector		
•		

Note: Standard time format used is hours. You can use seconds or minutes format in lieu of hours.

e. Then click Send.

## Manage a Lockbox

You can change the lockbox password, as well as refresh the lockbox.

## Lockbox Status

**Note:** NetWitness Platform has added a Health & Wellness stat for Warehouse Connector to indicate the status of its Lockbox. Also, an out-of-the-box rule has been added so that a Health & Wellness alarm is raised when the Lockbox does not exist or cannot be opened.

To see the rule details, go to (Admin) > Health & Wellness > Policies > Warehouse Connector and select Warehouse Connector Monitoring Policy.

	Invest	igate	Respond Users Ho	sts Files D	ashboard Rep	ports	🖑 🗘 🗷 % 🕜 admin 🗸
HOSTS SERVICES EVENT SOURC		ENDPOI	NT SOURCES HEALTH	& WELLNESS			
Alarms Monitoring Policies S	System	Stats Brow	vser Event Source Monit	oring Settings	New Health &	Wellness	
Policies + ⊗ - Z   ♥ X > □ ESA Correlation > □ Endpoint Broker Server	R	Warehc ules and su Enable Services Choose the	DUSE CONNECTOR: W ppression schedules of Out-of-ti hosts, services, and groups that	Yarehouse C ne-box policies canno your health policy ap	Connector M t be directly modified plies to.	<b>Ionitoring Policy</b> Duplicate the policy if you wish to so modi	fy them Last Modified: 2019-04-29 03:15:00 PM
D Endpoint Server     1     Host		+ ⊙ -	<b>`</b>		Group		Туре
Integration Server		🗆 All			2		Group
Investigate Server							
► Log Collector		Rules		* ** ******* ** *	an the Matheman Di		everythy statistic the classe evolves to showshold, and thereby it
▶ □ Log Decoder 1		at which the	e alarm clears). After you define	the alarm rule, enabl	e or disable the alarm	i.	sevency, statistic the alarm applies to, threshold, and threshold
Malware Analysis		+ - 2	5				
Crchestration Server		Enable	Name ^	Severity	Category	Statistic	Threshold
Carl Reporting Engine			Lockbox Access Failure	Critical	Lockbox	Lockbox Status	Alarm != 'Ok' for 0 MINUTES
Respond Server			Warehouse Connector Serv	Critical	ProcessInfo	Service State	Alarm != 'started','ready' for 0 MINUTES
Security Server			Warehouse Connector Serv	Critical	ProcessInfo	Service Status	Alarm != started for 0 MINUTES
► Source Server			Warehouse Connector Stre	High	Streams	Stream Behind	Alarm >= 2000000 for 0 MINUTES
▲ ➡ Warehouse Connector			Warehouse Connector Stre	High	Streams	Disk Usage (Pending Destination Load)	Alarm >= 75 for 0 MINUTES
Marahavaa Cannastar Manitar			Warehouse Connector Stre	Critical	Streams	Stream Status	Alarm != 'consuming', 'online' for 10 MINUTES
Warkharch			Warehouse Connector Stre	High	Streams	Number of files in the permanent rej	Alarm >= 300 for 0 MINUTES
• Li workbench 1	*		Warehouse Connector Stre	High	Streams	Rejected folder usage in percentage	Alarm >= 75 for 0 MINUTES

#### To change the Lockbox password:

- 1. Log on to NetWitness.
- 2. Go to **%** (Admin) > Services.
- In the Services view, select a Warehouse Connector service, and select > View > Config.
   The Services Config view of Warehouse Connector is displayed.

NETWITNESS Platform Investigate Respond Users Hosts Files Dashboard Reports 💍 🗘 🖃 🔏 🕐 admin 🗸									
HOSTS SERVICES EVENT SOURCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY									
Sources and Destinations Streams Lockbox Settings	General Appliance Ser	vice Configuration							
Source Configuration Destination Configuration									
+ -			+ - 🗷						
Name	Address	Port	Name	Туре	Path				
logdecoder1 - Log Decoder	1111110-001	56004	NFS	nfs	/root/test/kaushal				
logdecoder2 - Log Decoder	0.0.000	56002	SFTP SFTP	sftp	/root/test				

#### 4. Click the Lockbox Settings tab.

	tform Investigate Respond Users	Hosts Files	Dashboard	Reports			admin 🗸
HOSTS SERVICES EV	ENT SOURCES ENDPOINT SOURCES I	IEALTH & WELLNESS					
A Change Service   dec	der - Warehouse Connector 🛛 Config 💿						
Sources and Destinations	treams Lockbox Settings General A	opliance Service Configu	uration				
Create New Lockbox							
Set the lockbox password. The passw	rd should satisfy lockbox password strength.You will be	required to enter this passv	word to perform a	ny lockbox management.			
Lockbox Password	****						
Confirm Lockbox Password	e de de de de de de de						
Apply							
Change Lockbox Pas	word						
Change the lockbox password. You w	l be required to enter current password and new passw	ord.The password should sa	itisfy lockbox pass	word strength.			
Current Lockbox Password	*****						
New Lockbox Password	****						
Confirm New Lockbox Password	******						
Apply							
Refresh Lockbox							
Reset the lockbox.You will be require	to enter current lockbox password.						
Lockbox Password	****						
Apply							

- 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 X (Admin) > Services.
- In the Services view, select the added Warehouse Connector service, and select > View
   > Config.

The Services Config view of Warehouse Connector is displayed.

🔆 NETWITNESS   Platform Investigate Respond Users Hosts Files Dashboard Reports 💍 🗘 🗃 % 🕜 admin 🗸									
HOSTS SERVICES EVENT SOURCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY									
🚠 Change Service   Warehouse Connector   Config 🐵									
ources and Destinations Streams Lockbox Settings General Appliance Service Configuration									
Source Configuration Destination Configuration									
+ -			+ - 🗵						
Name	Address	Port	Name	Туре	Path				
logdecoder1 - Log Decoder	0101030-000	56004	NFS	nfs	/root/test/kaushal				
logdecoder2 - Log Decoder	0100-00-00	56002	SFTP SFTP	sftp	/root/test				

4. Click the Lockbox Settings tab.

	te Respond Users Hosts Files Dashboard Reports	Ō	_ ₽ ₹	K	?	admin 🗸
HOSTS SERVICES EVENT SOURCES E	NDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY					
A Change Service   decoder - Warehouse Conne	ctor   Config ⊚					
Sources and Destinations Streams Lockbox S	ettings General Appliance Service Configuration					
Create New Lockbox						
Set the lockbox password. The password should satisfy lockbox	password strength.You will be required to enter this password to perform any lockbox management.					
Lockbox Password *******						
Confirm Lockbox Password *******						
Apply						
Change Lockbox Password						
Change the lockbox password. You will be required to enter cur	rent 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 required to enter current lockbox	password.					
Lockbox Password *******						
Apply						

- 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 Pre-Upgrade and Post-Upgrade

## **Steps**

#### **Pre-Upgrade Steps:**

If NFS destination is configured, unmount the configured directory and disable the entry from /*etc/fstab* using the command umount <directory name>.

#### **Post-Upgrade Steps:**

- 1. Create a fresh lockbox key.
- 2. Reauthorize the user account in source configurations using using **Explore** or **REST API**. Reauthorization of source user account is not available in UI. The command to reauthorize the user account from **Explore** is given below:

```
> /warehouseconnector/sources/<source:port> ---> setPass property with
password=<password of the configured user in source>
```

3. Reauthorize the user account in SFTP destination configuration from UI, Explore or REST API. The command to reauthorize the password from Explore is given below:

> /warehouseconnector/destinations/<sftp\_destination> ---> setPass property
with password=<password of the configured user in SFTP destination>

4. If NFS directory mount was removed as part of pre-upgrade step, mount back the same configuration. Additionally, enable back the mount entry in */etc/fstab*.

> mount -t nfs -o nolock,tcp,hard,intr <IP\_Address\_for\_SAW>:/mapr/<clustername> /<directory name>

Where **<IP\_Address\_for\_SAW>** is the IP address of the primary Warehouse appliance in the cluster and **<cluster-name>** is the name provided in the template file.

## Warehouse Connector Configuration References

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

- General Tab Settings
- Appliance Service Configuration Tab Settings
- Sources and Destinations Configuration
- Add Stream Dialog
- Streams Configuration
- Lockbox Settings

## **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*	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 NFS Configure the Destination Using SFTP Configure the Destination Using WebHDFS
Administrator	Configure a Stream	Configure a Stream
Administrator	Monitor a Warehouse Connector	Monitor a Warehouse Connector

Role	I want to	Refer to
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</i> <i>Engine Configuration 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

\*You can perform this task in the current view

### **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.

KITWITNESS Platform Investigate Respond Users Hosts Files Da	shboard Reports Ö 🗘 🗟 % 🕜 admin 🗸
HOSTS SERVICES EVENT SOURCES ENDPOINT SOURCES HEALTH & WELLNESS S	YSTEM SECURITY
A Change Service   decoder - 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	$\mathbf{A}$
SSL Port	56020
Stat Update Interval	1000
Threads	20

Apply

When you add a Warehouse Connector service, default values are in effect. NetWitness designed the default values to accommodate most environments and recommends that you do not modify 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" 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*	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 NFS Configure the Destination Using SFTP Configure the Destination Using WebHDFS
Administrator	Configure a Stream	Configure a Stream
Administrator	Monitor a Warehouse Connector	Monitor a Warehouse Connector

Role	I want to	Refer to
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</i> <i>Engine Configuration 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

\*You can perform this task in the current view

### **Related topics**

• Configure a Warehouse Connector Service

### **Quick Look**

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

XINETWITNESS Platform Investigate Respond Users Hosts Files Dask	nboard Reports 💍 🗘 🗷 % 🕐 admin 🗸							
HOSTS SERVICES EVENT SOURCES ENDPOINT SOURCES HEALTH & WELLNESS SY								
🚠 Change Service   decoder - Warehouse Connector   Config 👳	A Change Service   decoder - 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							

Apply

When you add a Warehouse Connector service, default values are in effect. NetWitness 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
Administrator	Configure a Stream	Configure a Stream
Administrator	Monitor a Warehouse Connector	Monitor a Warehouse Connector

Role	I want to	Refer to
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</i> <i>Engine Configuration 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

\*You can perform this task in the current view

### **Related topics**

- <u>Configure the Data Source for Warehouse Connector</u>
- Configure the Destination

### Quick Look

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

NETWITNESS   Platform Investigate	Respond Users Hosts	Files Das	hboard Reports		) 💭 🖻 % (?) admin 🗸		
HOSTS <u>SERVICES</u> EVENT SOURCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY							
A Change Service   Warehouse Connector   Config							
Sources and Destinations Streams 1 Lockbox Settings	Sources and Destinations Streams 1 Lockbox Settings General Appliance Service Configuration 2						
Source Configuration			Destination Configuration				
+ -			+ - 🗵				
Name	Address	Port	Name	Туре	Path		
logdecoder1 - Log Decoder	101110000	56004	NFS	nfs	/root/test/kaushal		
logdecoder2 - Log Decoder	100000000000000000000000000000000000000	56002	SFTP	sftp	/root/test		

The Sources and Destinations tab includes the following two sections:

Source Configuration
 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.

So	Source Configuration				
+	+ -				
	Name Address Port				
	logdecoder1 - Log Decoder		56004		
	logdecoder2 - Log Decoder		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.

De	Destination Configuration				
+	$+$ $ \square$				
	Name	Туре	Path		
	NFS	nfs	/root/test/		
	SFTP	sftp	/root/test		

The Destination Configuration section allows you to perform the following:

Features	Description	
+	Add the destination.	
=	Delete the destination.	
	Edit the destination.	
<b>Note:</b> You can only edit the SFTP destinatitype.		

## 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	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 NFS Configure the Destination Using SFTP Configure the Destination Using WebHDFS
Administrator	Configure a Stream*	Configure a Stream
Administrator	Monitor a Warehouse Connector	Monitor a Warehouse Connector

Role	I want to	Refer to
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</i> <i>Engine Configuration 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

\*You can perform this task in the current view

## **Related Topics**

• Configure a Stream

## **Quick Look**

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

X NETWITNESS   Platfo	m Investigate Respond Users Hosts Fil	les Dashboard Reports		Ö 🗘 🖻 %	🕐 admin 🗸	
HOSTS SERVICES EVENT SO	IRCES ENDPOINT SOURCES HEALTH & WELLNESS					
Groups	Services					
+ - 1 0	- 13			♥ ⊙ Filter	×	
Name	Name	Licensed Host	Туре	Version	Actions	
⊕ All	3		nespona server		••••••••••••••••••••••••••••••••••••••	
	adminserver - Security Server	adminserver	Security Server	12.1.0.0	•	
	adminserver - Source Server	adminserver	Source Server	12.1.0.0	⇔ ⊙	
	archiver - Archiver	archiver	Archiver	12.2.0.0	⇔ ⊗	
	archiver - Workbench		Workbench	12.1.0.0	<b>☆</b> ⊙	
	broker - Broker		Broker	12.2.0.0	♦ 😒	
	concentrator - Concentrator		Concentrator	12.2.0.0	⇔ ⊘	
	decoder - Decoder		Decoder	12.2.0.0	⇔ ⊗	
	decoder - Warehouse Connector	⊘ decoder	Warehouse Connector	12.0.0.0	⇔ ⊙	
	endpoint - Endpoint Server		Endpoint Server	System View	>	
	endpointbroker - Endpoint Broker Server		Endpoint Broker Server	Config Edit		
	endpointloghybrid - Concentrator	endpointloghybrid	Concentrator 2	Explore Start		
	one endpointloghybrid - Endpoint Server	O endpointloghybrid	Endpoint Server	Logs Stop Security Restart		
	endpointloghybrid - Log Collector		Log Collector	12.1.0.0	<b>\$</b> •	
	endpointloghybrid - Log Decoder		Log Decoder	12.1.0.0	⇔ ⊙	
	esaprimary - Contexthub Server		Contexthub Server	12.1.0.0	<b>⇔</b>	
	<pre>《《   Page 1 of 2   》》   C</pre>			Displa	ying 1 - 25 of 43	
	n Investigate Respond Lisers Hosts File	as Dashboard Peports		Å ∩ <b>⊒ %</b>	<li>admin v</li>	
HOSTS SERVICES EVENTSOURCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY						
A Change Service   decoder - Warehouse Connector   Config 😡						
Sources and Destinations Streams	Sources and Destinations Streams Lockbox Settings General Appliance Service Configuration					
🕂 🚬 🗹 📔 Start Stop Reload	Finalize Change Configuration					
Name 3	Sources		Destination	Statu	s	

Add Stream			• e×
Stream Name *	Choose Destination 🗸		
	Adduces	Dort	Cossion ID
Name	Address	Port	Session ID
		56004	Enter Session
		56002	Enter Session
		_	_
		Canc	el Save

Go to (Admin) > Services<sup>-</sup>
 In the services view, select a Warehouse Connector service and select <sup>\*</sup> ⊙ >view>config

3 In the **Streams** tab, click 🕇 to view the add stream dialog.

The following table describes the fields in the Add Stream dialog:

Parameter	Description
Stream Name	Type the name of the stream. The stream name may only contain alphanumeric characters and underscores. It cannot exceed 20 characters in length.
Select Destination	Select a destination from the drop-down list.
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	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 NFS Configure the Destination Using SFTP Configure the Destination Using WebHDFS
Administrator	Configure a Stream*	Configure a Stream
Administrator	Monitor a Warehouse Connector*	Monitor a Warehouse Connector

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

\*You can perform this task in the current view

## **Related topics**

Configure a Stream

### **Quick Look**

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

	Name	Sources		Destination	Status		
+	+ - 🗹   Start Stop Reload   Finalize Change Configuration						
So	ources and Destinations Streams Lo	ckbox Settings General Appliance	Service Configuration				
#	A. Change Service   logdecoder1 - Warehouse Connector   Config ⊚						
н	OSTS SERVICES EVENT SOURCE	S ENDPOINT SOURCES HEALTH	& WELLNESS SYSTEM SECURITY				
2	NETWITNESS   Platform	Investigate Respond Users	Hosts Files Dashboard Reports		) 🗘 🗷 % 🕐 admin 🗸		

To configure the alert mechanisms related to the Warehouse Connector navigate here.

The Streams tab allows you to perform the following:

Features	Description
+	Add a stream.
-	Delete a stream.

Features	Description
	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  $\bigcirc$  icon next to the name of the stream.

NETWITNESS   Platform Investi	gate Respond Users Hosts Files Dashboard Reports	\$ \$	% 🕜 admin 🗸
HOSTS SERVICES EVENT SOURCES END	POINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY		
A Change Service   Warehouse Connector	⊑onfig ⊙		
Sources and Destinations Streams Lockbox Sett	ings General Appliance Service Configuration		
+ - 🗹   Start Stop Reload   Finalize	Change Configuration		
🗹 Name	Sources	Destination	Status
	:50002	10000	running
Stream (Testing) Number of files in the permanent rejected fold Rejected folder usage in percentage: 0 Session Rate: 7 Destination (Testing) Status: entine Source (10.31.125.24650002) Status: consuming Sessions Behind: 0 Last Session Read : 16698	der: 0		

The following parameters are displayed in the Stream Statistics:

Section	Parameter	Description
Stream		

Section	Parameter	Description	
	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.	
	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	
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.

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	s the time between the responses from the source.	
		Loader Settings	
Compress files on disk	Enable to compress files on disk. Supported values:		
	• Deflate generati	- Provides smaller compressed files and good performance while ng reports.	
	• Off By default,	the parameter is set to <b>deflate</b> .	
Export Rollup Interval	Determines the Wareho For examp If the para	s the roll-up interval for export files and also the directory structure ouse Connector writes to the destination. le: meter is set to:	
	Value	Directory Structure	
	hour	/rsasoc/v1/[logs   sessions]/data/ {year}/{month}/{day}/{hour}	
	minute	/rsasoc/v1/[logs   sessions]/data/ {year}/{month}/{day}/{hour}/ {minute}	
	day	/rsasoc/v1/[logs   sessions]/data/ {year}/{month}/{day}	
	If you char Recommen	nge the value of the parameter, ensure that you restart the stream. Inded value is <b>hour</b> .	
Maximum Message Hold Count	Determines processing.	s the maximum number of sessions to store in the memory before	
	Note: If y make sure	you have deployed a Warehouse Connector Virtual Appliance, 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.		
Remote Export Path	Determines the remote local mount point for HDFS (nfs://) and the location to export the data.		

Parameter	Description
Page Size	Determines the maximum pages.
	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*	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 NFS Configure the Destination Using SFTP Configure the Destination Using WebHDFS
Administrator	Configure a Stream	Configure a Stream
Administrator	Monitor a Warehouse Connector	Monitor a Warehouse Connector

Role	I want to	Refer to
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</i> <i>Engine Configuration 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*	<u>Manage a Stream</u> <u>Manage a Lockbox</u>

\*You can perform this task in the current view

### **Related topics**

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

## **Quick Look**

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

<b>WITNESS</b> PI	latform Investigate Respond Users Hosts Files Dashboard Reports	🖑 💭 🗷 % 🕜 admin 🗸
HOSTS SERVICES EV	VENT SOURCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY	
A Change Service   deco	oder - Warehouse Connector   Config ©	
Sources and Destinations	Streams Lockbox Settings General Appliance Service Configuration	
Create New Lockbox		
Set the lockbox password. The passv	word 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 w	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		

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