RSA NETWITNESS® SUITE

Archiver Configuration Guide

for Version 11.0

Contact Information

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

Trademarks

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

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, 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 EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

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

October 2017

Contents

Archiver Overview

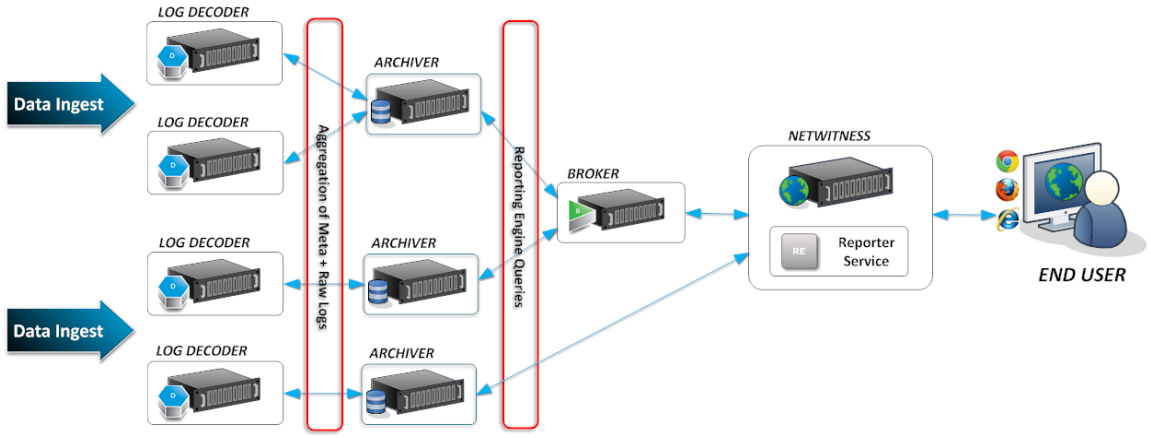
This guide provides detailed instructions on how to configure Archiver in your network, additional procedures that are used at other times, and reference materials that describe the user interface for configuring Archiver in your network.

The NetWitness Suite Archiver is an appliance that enables long-term log archiving by indexing and compressing log data and sending it to Archiving storage. The Archiving storage is then optimized for long-term data retention and compliance reporting.

Archiver stores raw logs and log meta from Log Decoders for long-term retention and it uses Direct-Attached Capacity (DAC) for storage.

Note: Raw packets and packet meta are not stored in the Archiver.

The following figure depicts the architecture of a NetWitness Suite network that implements the Archiver.



Configuring an Archiver

The NetWitness Suite Archiver is an appliance that enables long-term log archiving by indexing and compressing log data and sending it to Archiving storage. The Archiving storage is then optimized for long-term data retention and compliance reporting.

Archiver stores raw logs and log meta from Log Decoders for long-term retention and it uses Direct-Attached Capacity (DAC) for storage.

Note: Raw packets and packet meta are not stored in the Archiver.

Prerequisites

Ensure that you have:

- Installed the Archiver host in your network environment.
- Installed and configured Log Decoder version 11.0.0.0 in your network environment.

If you want to configure multiple Archiver or Concentrator services as a group and share the aggregation tasks between them, refer to **Group Aggregation** in the *Deployment Guide*.

Workflow

This workflow illustrates the end-to-end installation and configuration process for an Archiver.

The following table describes the basic steps for configuring an Archiver.The tasks must be completed in the sequence they are given.

Configuration Step	Description
Add the Archiver Service	Provides information on how to add an Archiver service to the Archiver host and apply a license to it.
Add Log Decoder as a Data Source to Archiver	Provides instructions on how to add a Log Decoder to an Archiver.

Configuration Step	Description
Configure Archiver Storage and Log Retention	Provides instructions on how to configure storage and log retention on an Archiver.
Add Archiver as a Data Source to Reporting Engine	Provides instructions on how to add an Archiver as a data source to Reporting Engine to generate reports for the data collected by an Archiver.
Configure Archiver Monitoring	Provides instructions on how to configure the alert mechanism related to Archiver storage.

Add the Archiver Service

In order to add an Archiver service, ensure that you have installed an Archiver host on which you want to run the Archiver service. See the **Step 1: Add or Update Host** topic in the *Host and Services Getting Started Guide* for the procedure that explains how to add a host.

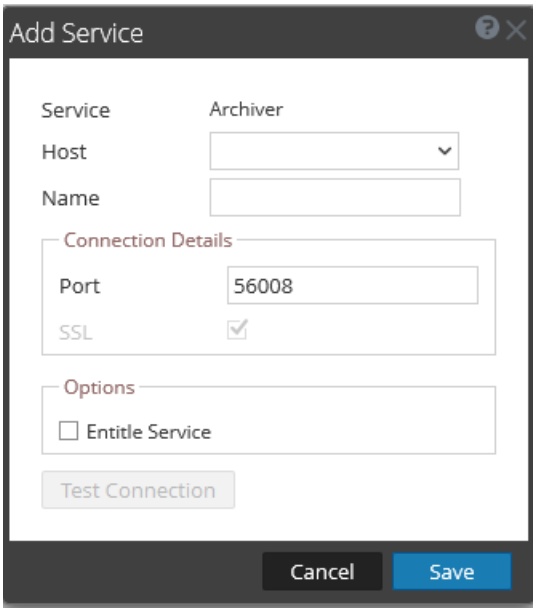
After you install an Archiver host, you need to add an Archiver service an apply a license to it, as explained in the following procedure.

Note: This procedure is only required if you do not have the Archiver service installed.

Perform the following steps to add the Archiver service:

1. Go to **ADMIN > Services**.
2. In the **Services** panel toolbar, select + > **Archiver**.

   The Add Service dialog is displayed.



3. Provide the following details.

Field	Description
Host	Select a host from the drop-down menu.
Name	Type a name for the service.
Port	Default port is 50008.

Field	Description
SSL	Select **SSL** if you want NetWitness Suite to communicate with the service using SSL. The security of data transmission is managed by encrypting information and providing authentication with SSL certificates. **Note:** If you select SSL, ensure SSL is enabled in the System Configuration panel.
Username	(Optional) Type the username for the service.
Password	(Optional) Type the password for the service.
Entitle Service	Select if you want to apply the entitlements currently configured to this service. For more information, see the **Entitlement Capability Implementation** topic in the *Licensing Guide*.

4. Click **Test Connection** to determine if NetWitness Suite connects to the service.
5. When the result is successful, click **Save**.

   The added service is now displayed in the services panel.

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

6. Apply license to the Archiver service.

   Refer to the **Synchronize NetWitness Server** topic in the *Licensing Guide* for details on the procedure to activate (apply a license to) the Archiver service.

Add Log Decoder as a Data Source to Archiver

In order to add a Log Decoder as a data source to Archiver, you need to have installed the Archiver host in your network environment, installed and configured a Log Decoder in your network environment, and added the Archiver host to NetWitness Suite and make sure the Archiver service shows as active and licensed.

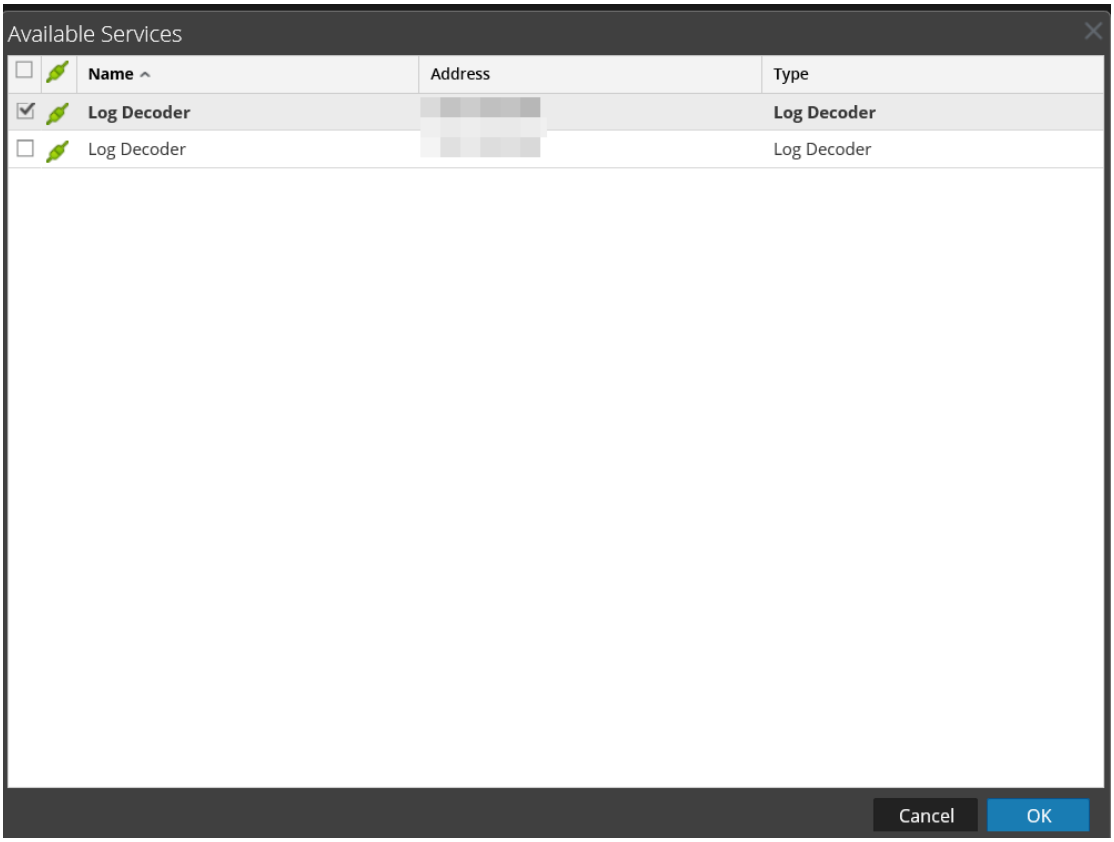
Add Log Decoder as a Data Source to Archiver

To add a Log Decoder as a data source to an Archiver:

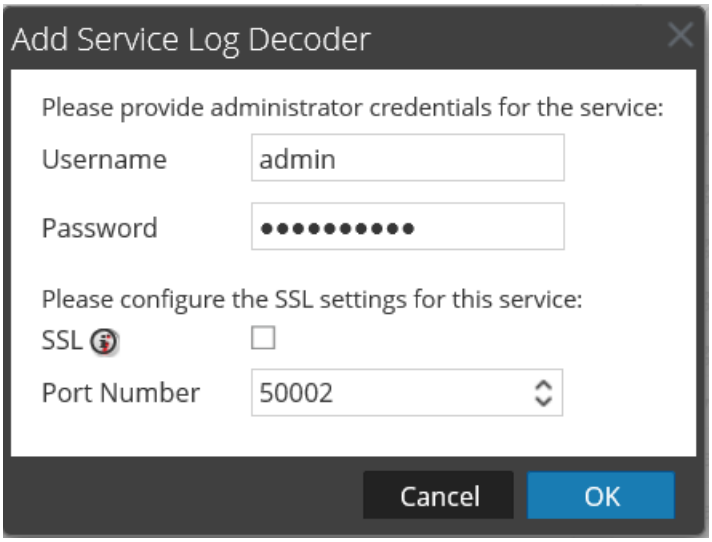
1. Go to **ADMIN > Services**.
2. Select the Archiver service.
3. In the  **Actions** column, select **View > Config**.

   The Services Config view of Archiver is displayed.
4. On the **General** tab, in the **Aggregate Services** panel, click +.

   The Available Services dialog is displayed.



5. Select the Log Decoder service to add as a data source to the Archiver and click **OK**.
6. If the Log Decoder is using the trust model, an Add Service dialog is displayed.



7. Type the username and password for the Log Decoder, and configure the SSL settings.
8. Click **OK**.
   The selected Log Decoder service is listed in the **Aggregate Services** panel.

Archiver Meta Settings Considerations

To maximize retention time, the meta items and index of the Archiver have been reduced (when compared to the Concentrator) to support common reporting needs. This means that, by default, you may not be able to run all of the reports you run on the Concentrator on the Archiver. You can view a list of the current meta and index items used by the Archiver in the following locations:

- **Explorer view**: The **/archiver/devices/<logdecoder>/config/options** path in the **metaInclude** field shows the current list of meta items.
- **Config view > Files tab**: The **index-archiver.xml** shows the default index configuration. The **index-archiver-custom.xml** shows any modifications.

The meta items and index of the Archiver can be customized to support customer specific reporting needs, however this will require additional storage, CPU resources, and Memory resources to support, and may impact retention time. As more meta items are added to the Archiver, the maximum aggregation rate will decrease, and the time to execute reports will increase.

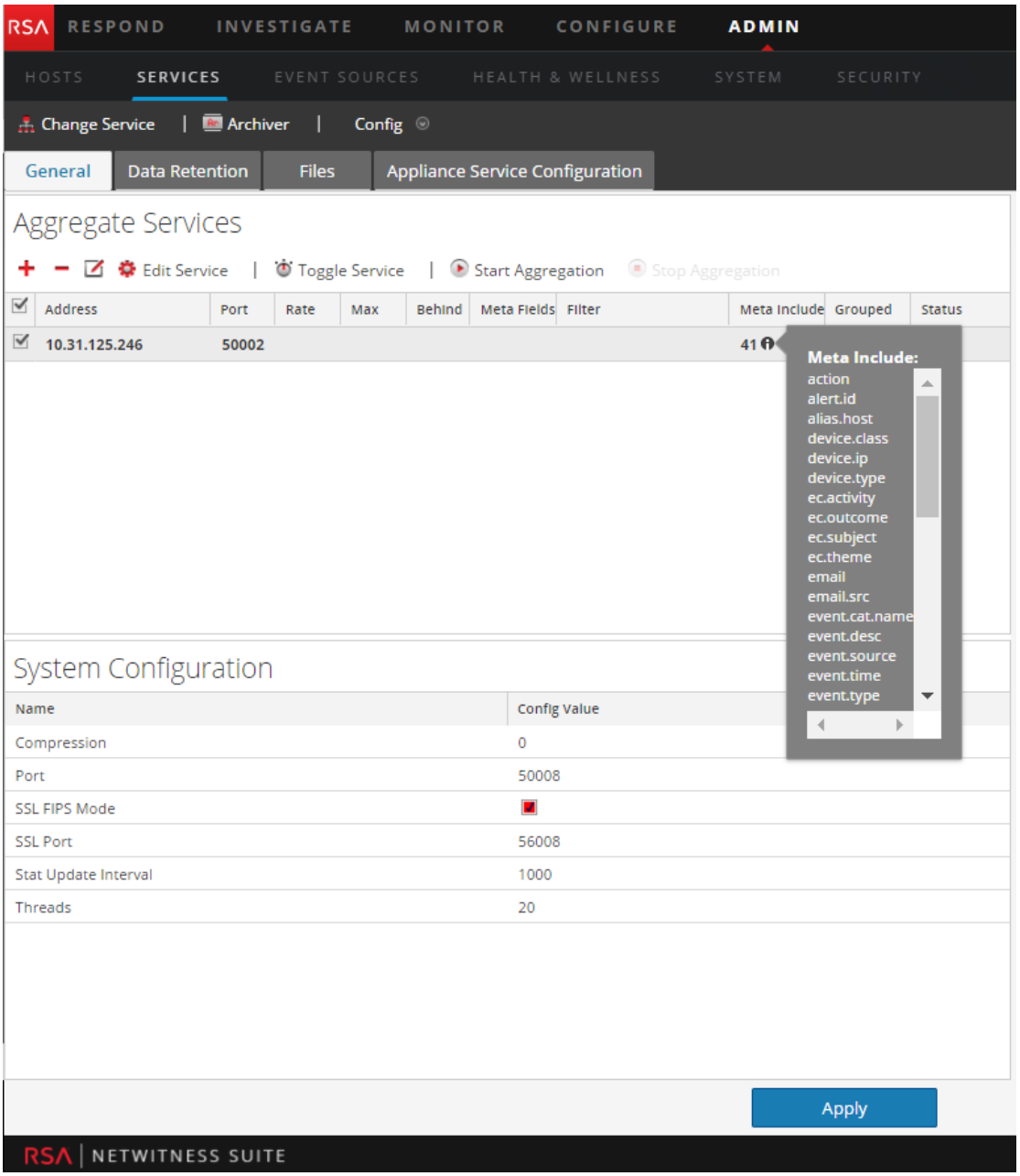
See (Optional) Configure Meta Filters for Aggregation and (Optional) Add Index Entries for Archiver Reporting for additional details.

(Optional) Configure Meta Filters for Aggregation

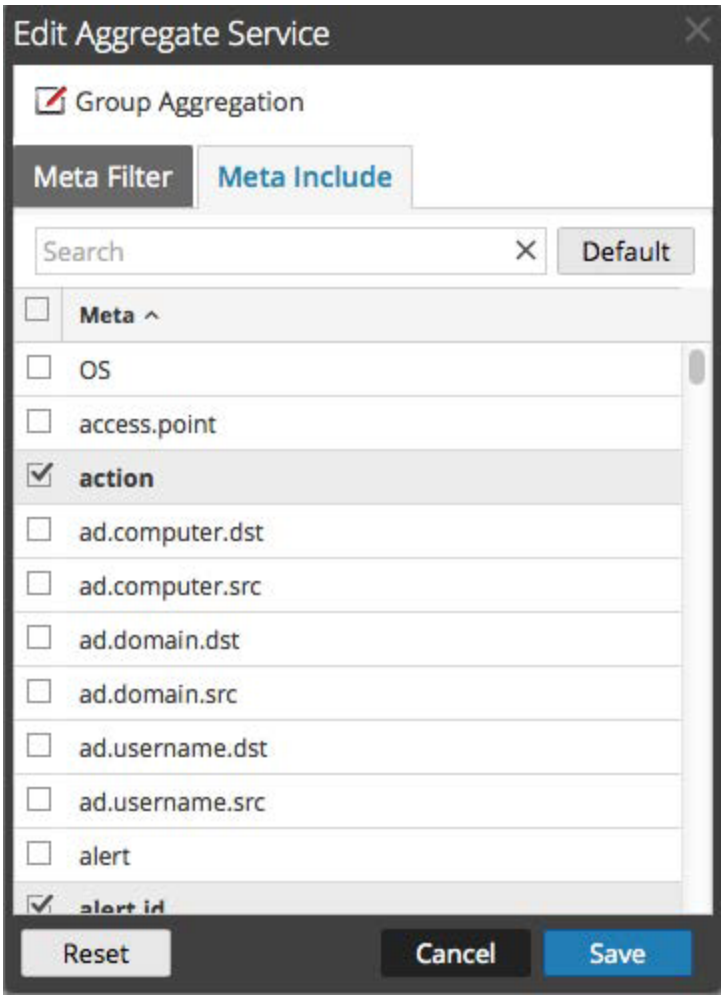
Follow this procedure to view and add additional meta items to the Archiver.

Caution: Adding meta or indexes will require additional storage, CPU resources, and Memory resources to support, and may impact retention time. As more meta items are added to the Archiver, the maximum aggregation rate will decrease, and the time to execute reports will increase.

1. To view the current meta items, in the **Aggregate Services** panel, select the Log Decoder service and click in the **Meta Include** field.



2. To add additional meta items, select the Log Decoder service and click  .



3. In the Edit Aggregate Service dialog, select the meta items to include in the Meta Include list. For example, you may want to consider including ip.srcport, tcp.srcport, udp.srcport, msg, url, query, bytes, alias.host, ip.dst, ip.dstport, ip.src, tcp.dstport, megabytes, time, event.desc, and word.
4. Click **Save** and then click **Apply**.
5. See (Optional) Add Index Entries for Archiver Reporting below for information on how to index the additional meta keys.

(Optional) Add Index Entries for Archiver Reporting

Caution: Adding meta or indexes will require additional storage, CPU resources, and Memory resources to support, and may impact retention time. As more meta items are added to the Archiver, the maximum aggregation rate will decrease, and the time to execute reports will increase.

The Archiver's default index configuration only includes value indexes for these keys:

- time
- decoder source (did)
- destination user account (user.dst),
- alert ID (alert.id)
- device IP (device.ip)
- source IP address (ip.src)
- destination IP address (ip.dst)
- event description (event.desc)
- device class (device.class)
- medium
- object name (obj.name)
- word

For information on customizing this list, see **Index Customization** in the *Core Database Tuning Guide*.

Configure Archiver Storage and Log Retention

This topic provides instructions for Administrators to configure storage and log retention on an Archiver.

For compliance reasons, it is often necessary to retain some logs longer than other logs. Some logs are legally sensitive and cannot be retained for a long period of time. Other logs have a requirement to be retained for years. In addition to compliance, some logs are useful for historic forensics and other logs have little to no security or operationally relevant value and can be deleted after a short time.

Because business requirements vary, NetWitness Suite enables you to configure Collections, which are log retention sets for storing log data. For each collection, you can specify how much of the total storage space to use and how many days to retain the logs in the collection. To specify the type of logs to put in the collection, you define retention rules to associate with the collections. Retention rules for all of your collections execute sequentially in an order that you define.

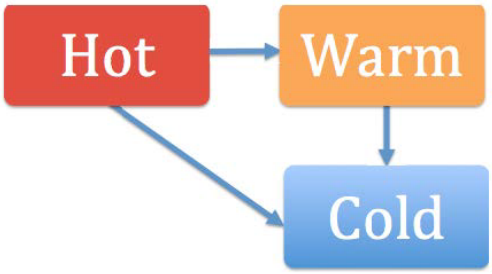
To do this, you must first define the total physical storage space for your collections. NetWitness Suite enables you to define three types of storage:

- **Hot Tier Storage**: This storage contains log data that is in active use as part of the business process. Users can access these logs faster than other types of storage and they can use these logs for reporting and other tasks. Hot storage is usually Direct-Access Capacity (DAC) or SAN storage.
- **Warm Tier Storage**: (Optional) This storage contains older log data aggregated by Archiver. Log data access is slower than hot storage. Users can also use these logs for reporting and other tasks. Warm storage is usually Network Attached Storage (NAS).
- **Cold Tier Storage**: (Optional) This storage contains the oldest log data that is either required for the operation of the business or mandated by regulatory requirements. The logs are offline and Archiver cannot access these logs for reporting or other tasks. However, if you want to access this log data, you can restore it to the collections created on the Archiver service and then use it for reporting. Cold storage is usually offline storage, such as NAS, or temporary storage before archiving to tape. Once data moves to the Cold Tier, that data is no longer managed by Archiver. Once moved, it is incumbent on external processes to back it up or manage that Cold Tier space such that it does not reach 100% capacity. If capacity is reached, this will cause the Archiver to stop aggregation until the problem is fixed.

Archivers are preconfigured to use available hot storage and a default log collection, so you do not have to configure Archiver storage and log retention if you do not have complex log retention requirements.

Logs can move from one type of storage to another in the following ways:

- Hot Storage > Cold Storage
- Hot Storage > Warm Storage > Cold Storage



When a collection reaches its retention limits for hot and warm storage, NetWitness Suite deletes the log data from hot or warm storage. With cold storage configured, a copy goes into cold storage before the logs are deleted from hot or warm storage. For example, if you have a collection with Hot Storage of 1 TB, Warm Storage of 1 TB, and Cold Storage enabled, when the log data reaches 1 TB of hot storage, the oldest log data moves to warm storage. When the log data in warm storage reaches 1 TB, the oldest log data from warm storage is copied to cold storage before it is removed from warm storage.

For Hot and Warm Storage, size and retention period settings for a collection can override each other based on which criterion (size or time) is satisfied first. For example, if you have a collection with Hot Storage of 1 TB, no Warm or Cold Storage, and a Retention period of 20 days, if the Log data exceeds 1 TB after 11 days, the oldest logs over 1 TB are deleted even though the collection has a 20 day retention period.

After you create hot, warm, and cold storage, you configure your log retention storage collections. You can specify the maximum size of the Hot and Warm Storage for the collection, whether to use Cold Storage, the number of days to retain the logs in the collection, the data compression, and whether to use a hash algorithm to be able to verify the data integrity of the files being saved.

After configuring your collections, you define retention rules for your collection. These rules specify the type of logs to be stored in the collection. Each collection must have at least one retention rule associated with it in order to store log data.

Procedure

Perform the following tasks in the order shown to configure storage and log retention.

Task	Reference
1. Configure total hot, warm, and cold storage.	Refer to Configure Hot, Warm, and Cold Storage.

Task	Reference
2. Configure log retention storage collections.	Refer to Configure Log Storage Collections.
3. Define retention rules for the collections and determine the order of execution of the overall list of retention rules.	Refer to Define Retention Rules.

Configure Hot, Warm, and Cold Storage

This topic provides instructions for Administrators on how to configure total hot, warm, and cold storage on an Archiver.

An Archiver host has hot storage pre-configured to the defaults. Administrators can configure total hot, warm, and cold storage to meet their specific business requirements. An Archiver must have total hot storage configured, but warm and cold storage configurations are optional. NetWitness Suite does not manage cold storage.

Prerequisites

Ensure that you have:

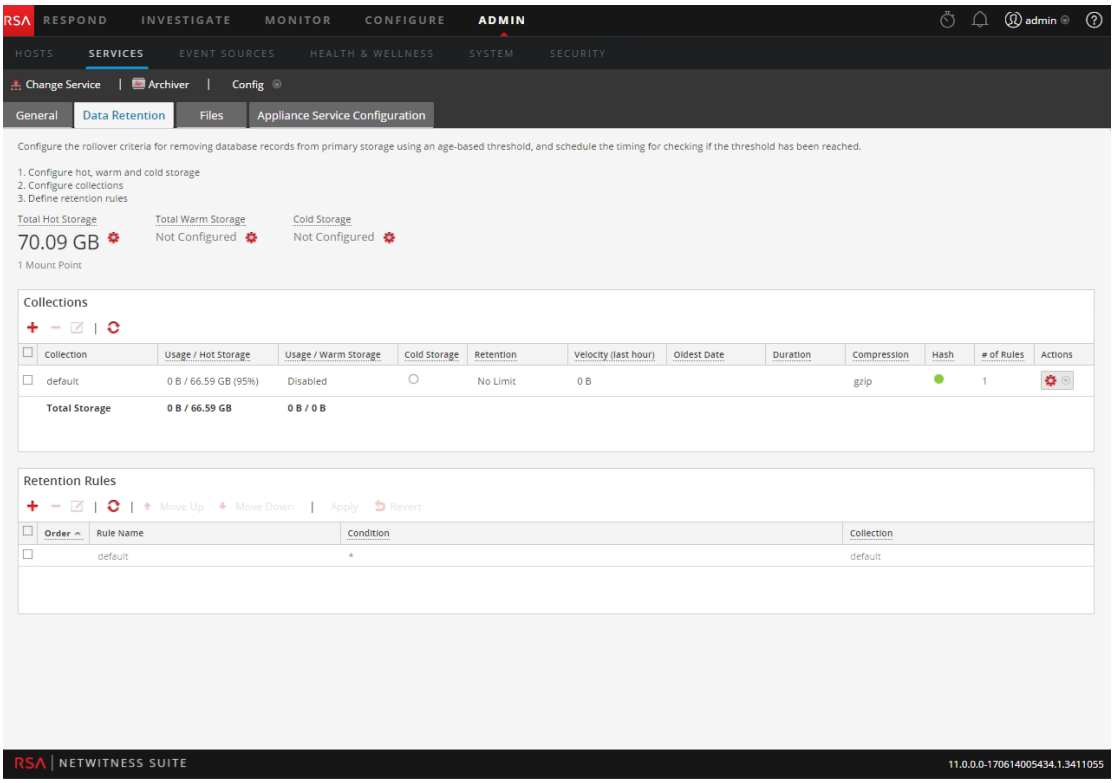
1. Installed the Archiver host in your network environment.
2. Installed and configured Log Decoder in your network environment.
3. Added Archiver as a Core service to your NetWitness Suite deployment.
4. Added Log Decoder services as a data source for Archiver.
5. Installed and configured a DAC or other physical storage in your network environment.
6. Determined your log retention and storage requirements.

Procedures

Configure Total Hot Storage for an Archiver

1. Go to **ADMIN > Services**.
2. Select the Archiver service and  **> View > Config**.

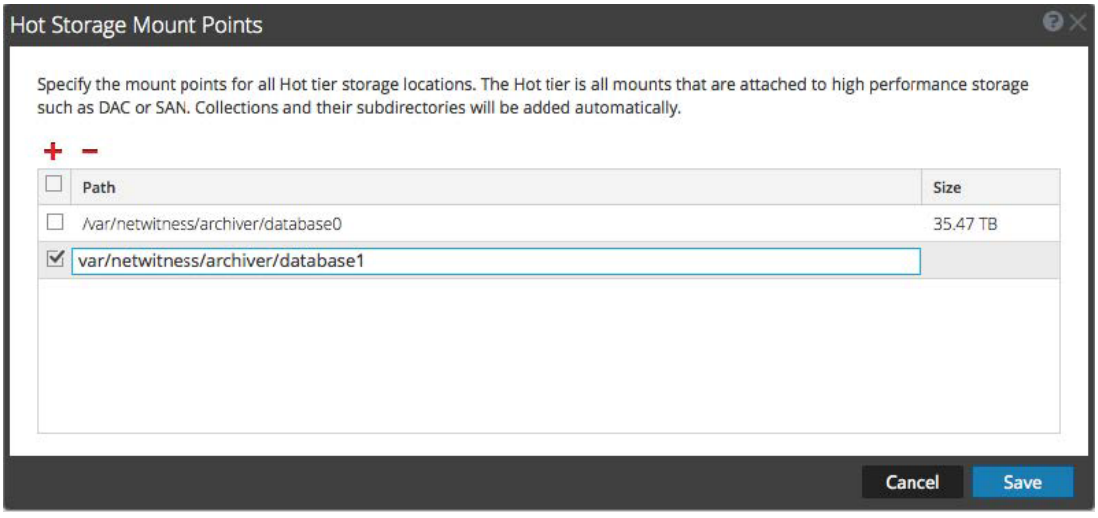
   The Services Config view of Archiver is displayed.
3. On the **Data Retention** tab, in the **Total Hot Storage** section, click  to configure total hot storage.



4. In the **Hot Storage Mount Points** dialog, add the mount points attached to the Archiver host that you want to include in Total Hot Storage.

   These are the paths to high performance storage, such as DAC storage and SAN. Do not add collections or subdirectories to the mount points.

   To add a mount point, click + and type the path to the mount point.



5. Verify that your mount point paths are correct and click **Save**.

   NetWitness Suite will automatically create metadb, packetdb, sessiondb, and index

directories for each collection defined on the Archiver:
<storageLocation>/<CollectionName>/metadb
<storageLocation>/<CollectionName>/packetdb
<storageLocation>/<CollectionName>/sessiondb
<storageLocation>/<CollectionName>/index

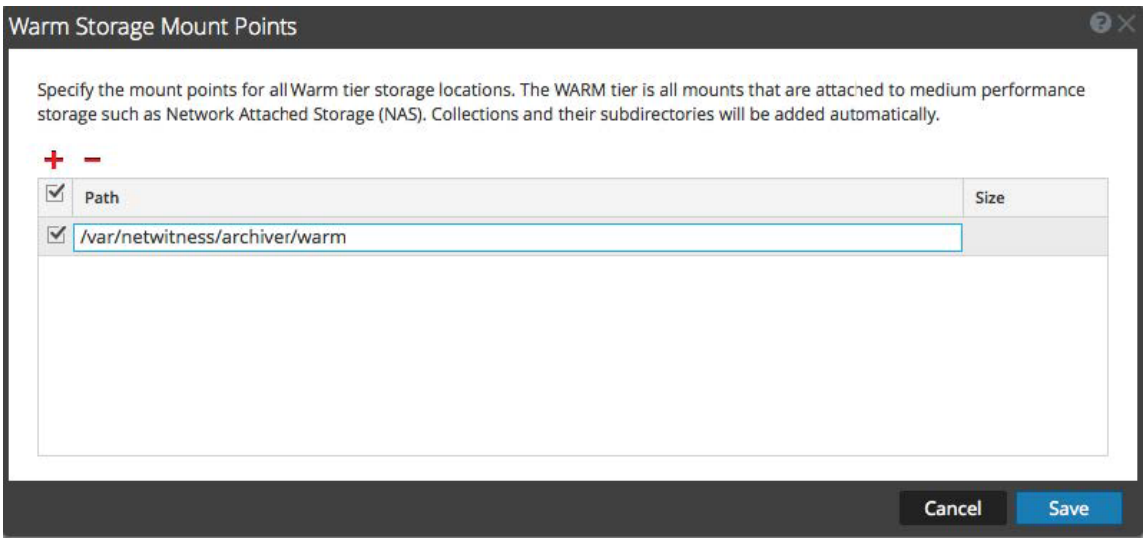
For example, if your mount point is /var/netwitness/archiver, then the following directories will be created for each of your collections:
/var/netwitness/archiver/<CollectionName>/metadb
/var/netwitness/archiver/<CollectionName>/packetdb
/var/netwitness/archiver/<CollectionName>/sessiondb
/var/netwitness/archiver/<CollectionName>/index

After the Archiver service is restarted, data will start being saved to your defined collections. Ensure that your log retention collections are correct before restarting the Archiver service.

Caution: After data has been saved to a mount point, it cannot be removed from the user interface.

Configure Total Warm Storage for an Archiver

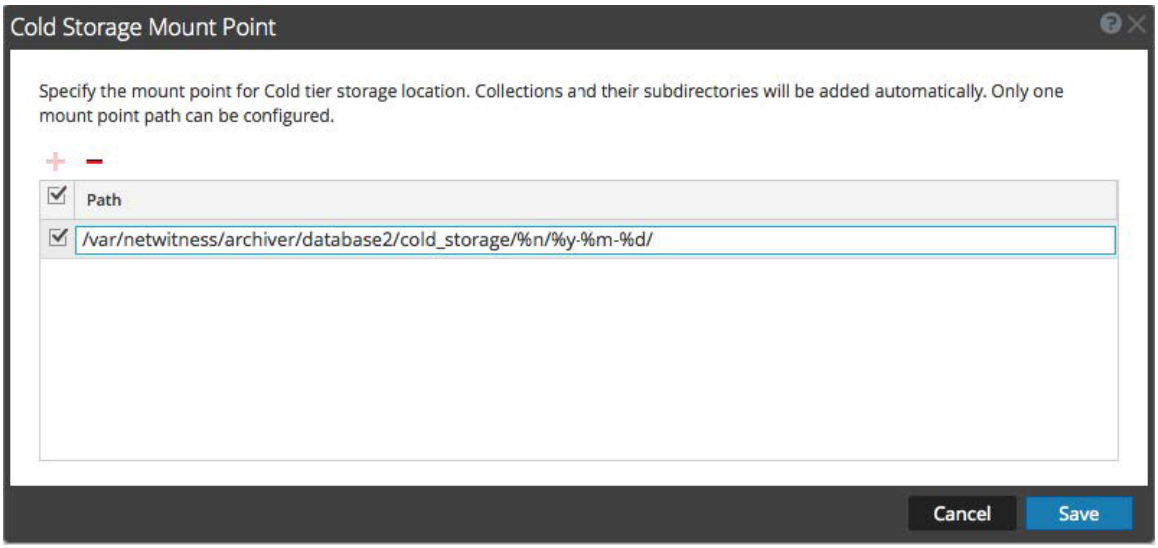
(Optional) The procedure to configure Total Warm Storage for an Archiver is the same as for Total Hot Storage, except that you click  in the Total Warm Storage section and add the mount points that you want to use for warm storage, which are the physical paths to warm storage, such as Network Attached Storage (NAS).



Configure Total Cold Storage for an Archiver

(Optional) The procedure to configure Total Cold Storage for an Archiver is the same as for Total Hot Storage, except that you click in the Total Cold Storage section and you add only one mount point for cold storage. NetWitness Suite does not manage cold storage.

You must include the collection name format specifier `%n` somewhere in the cold storage mount point path name to avoid filename collisions between collections.



The following format specifiers are allowed in the path:

Format Specifier	Description
%n	collection name (required)
%y	year the data moved to cold storage
%m	month
%d	day
%h	hour
%##r	block of hours for the current day. For example, if you want three 8 hour blocks, you can set it to %8r. The first 8 hours of the day returns 0, the second 8 hours returns 1, and last 8 hours of the day returns 2.

Changes take effect immediately.

For example, if you have a collection named **compliance** and you create the following cold storage path:

```
/sa-cold-storage/%n/%y-%m-%d/
```

NetWitness Suite creates a directory each day with the following format:

/sa-cold-storage/compliance/2015-11-20/

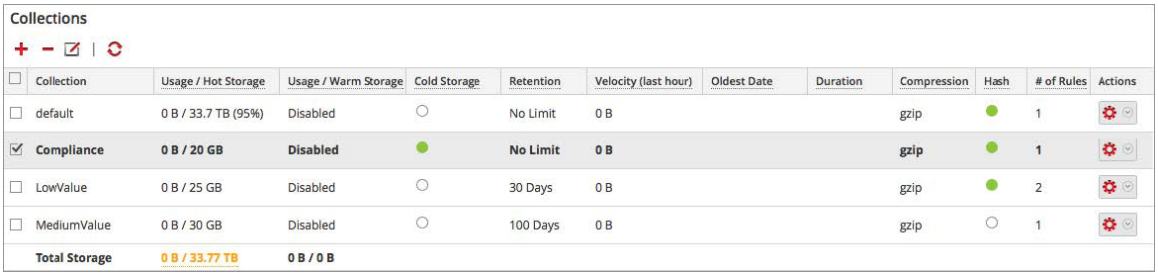
Hot, Warm, and Cold Tier Storage Features

The following table describes features of the Hot, Warm, and Cold Tier Storage dialogs.

Feature	Description
	Adds a mount point.
	Removes a mount point. You cannot delete a mount point that is in use unless you delete the associated collections.
	Select the mount points that you want to include for the Total Hot, Warm, and Cold Storage. You can only select one mount point for Total Cold Storage.
Mount Point	Shows the path to the attached physical storage. For example: **/var/netwitness/archiver/database0**, which is the location of the hot storage DAC. Do not add collections or subdirectories to the mount points. NetWitness Suite will automatically create metadb, packetdb, sessiondb, and index directories for each collection defined on the Archiver: <storageLocation>/<CollectionName>/metadb <storageLocation>/<CollectionName>/packetdb <storageLocation>/<CollectionName>/sessiondb <storageLocation>/<CollectionName>/index For example, if your hot storage mount point is /var/netwitness/archiver, then the following directories will be created for each of your collections: /var/netwitness/archiver/<CollectionName>/metadb /var/netwitness/archiver/<CollectionName>/packetdb /var/netwitness/archiver/<CollectionName>/sessiondb /var/netwitness/archiver/<CollectionName>/index For Cold Storage, you must include the collection name format specifier `%n` somewhere in the cold storage mount point path name to avoid filename collisions between collections.
Storage Size	Shows the size of the attached storage. The Data Retention tab shows the total amount of storage for your reference.

Collections

The Collections section lists all of your storage collections along with Total Storage for Hot and Warm Storage.



Collections Features

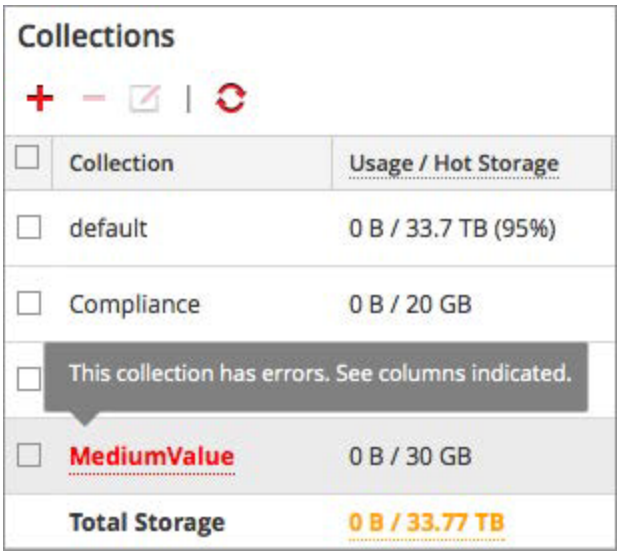
The following table describes the icons and columns of the Collections section. You can hide some of the columns based on your requirements.

Feature	Description
	Opens the Collections dialog, in which you can add a storage collection.
	Removes the selected collection. Deleting the collection permanently removes all stored data from the collection, but the empty data directories remain.
	Opens the Collections dialog, in which you can edit the selected collection.
	Refreshes collection information.
	Selects a collection. For example, you can select a collection for editing or removal.
Collection	Shows the name of your collection, such as Default, Compliance, MediumValue, and LowValue. You can create multiple collections with different criteria for retaining logs. If you do not create any collections, the Default collection is used. If a collection has errors, the collection name and the columns with errors appear in red text.

Feature	Description
Usage / Hot Storage	Shows the current hot storage usage and the maximum hot storage for the collection. When the size of the logs reach the maximum hot storage amount, the logs are removed or they roll to the next available storage tier (warm or cold).
Usage / Warm Storage	Shows the current warm storage usage and the maximum warm storage for the collection. When the size of the logs reach the maximum warm storage amount, the logs are removed or they roll to available cold storage.
Cold Storage	Indicates whether cold storage is enabled or disabled. A solid colored green circle indicates that cold storage is enabled ( ). An blank white circle indicates that cold storage is disabled.
Retention	Shows the number of days that logs are retained before being removed or optionally moved to cold storage. No Limit indicates that log retention is not restricted by a specified number of days. For Hot and Warm Storage, size and retention period settings for a collection can override each other based on which criterion (size or time) is satisfied first.
Velocity (last hour)	Shows the number of logs captured over the last hour.
Oldest Date	Shows the date and time of the last log capture.
Duration	Shows how may days ago that the last log was captured. For example: 20 days.
Compression	Shows the compression type used for the meta and raw data in the collection.
Hash	Shows whether hash is enabled or disabled. When enabled, the hash algorithm is used to ensure the data integrity of the files being saved. By default, the only data being hashed is raw logs and the hash files are saved in the same directory as data.

Feature	Description
# of Rules	Shows the number of rules applied to the collection. Define at least one rule for each collection. A collection without any associated rules shows a zero in red text as a warning: The collection name also appears in red text, which indicates an error in the collection. **Caution:** If a collection does not have a rule, no logs will ever go into that collection.
Actions	Enables you to see the rules associated with a collection in the Retention Rule section when you select <actions button> **> Select Rules**. In the Retention Rule section, you can change the overall priority of the collection rules.
Total Storage	Shows the current total hot storage usage and the maximum total hot storage at the bottom of the **Usage / Hot Storage** column. It also shows the current total warm storage usage and the maximum total warm storage at the bottom of the **Usage / Warm Storage** column.

Any errors in the collection appear in red text. A dotted underline indicates that a tooltip is available with information about the error.



Collections that have editing disabled (grayed out) also have tooltips that provide information on the problem.

Retention Rules

The Retention Rules section lists all of the retention rules used for your storage collections listed in the order of rule execution.

The following table describes the features of the Retention Rule section.

Feature	Description
	Opens the Rule Definition dialog, in which you can add a retention rule to use in a storage collection.
	Removes the selected retention rule. In order for your log collections to gather and store log data, you must associate them with at least one retention rule.
	Opens the Rule Definition dialog, in which you can edit the selected retention rule.
	Refreshes retention rule information.
 Move Up	Moves the selected retention rule up in the Retention Rule priority list. Retention Rule order is very important. NetWitness Suite evaluates the the retention rules for all of the collections in numerical order by the number listed in the Order column in the Retention Rule section. You can also use drag and drop to reorder retention rules.
 Move Down	Moves the selected retention rule down in the Retention Rule priority list. Retention Rule order is very important. NetWitness Suite executes the retention rules for all of the collections in numerical order by the number listed in the Order column in the Retention Rule section.
Apply	Saves the rule order change.
 Revert	Reverts the rule order change.
	Selects or shows a selected retention rule.
Order	Shows the order of a rule in the overall list of retention rules.

Feature	Description
Rule Name	Shows the name of rule, such as ComplianceDevices and GeneralWindowsLogs.
Condition	Shows the conditions for the rule. These conditions specify the type of logs to include in the collection. Define Retention Rules presents the guidelines for all queries and rule conditions in Core services.
Collection	Shows Collection name and how many days that the collection is retained. For example: MediumValue (30 Days)

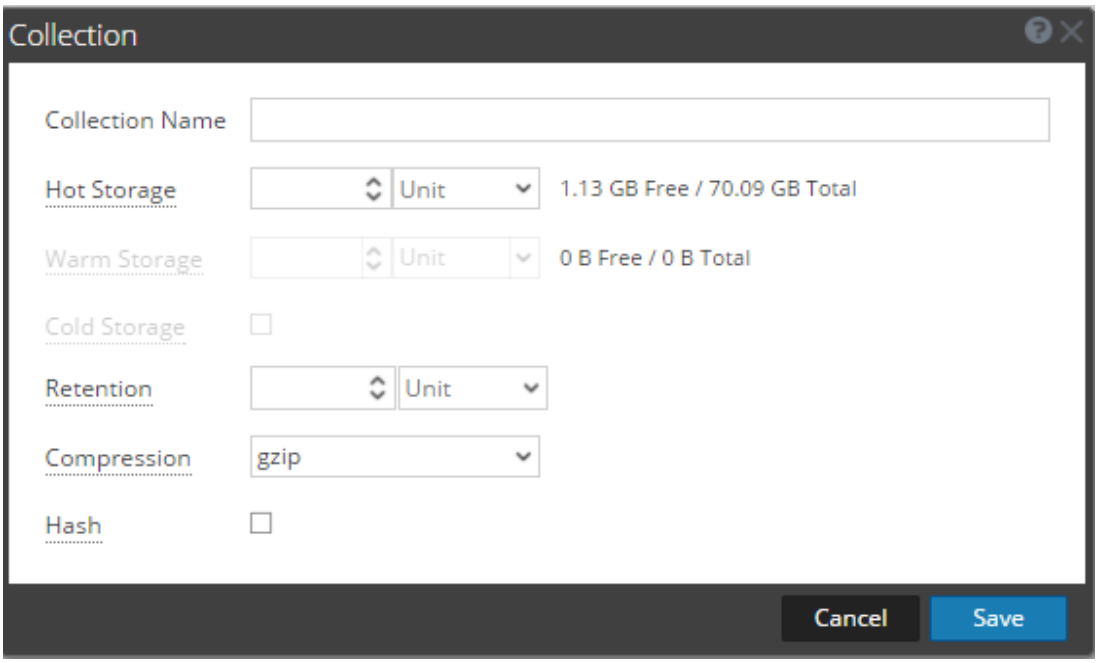
Collection Dialog

On the ADMIN > Services > Config view > Data Retention tab of an Archiver, Administrators can define the criteria for log retention and storage. In the Collection dialog, which is accessible from the Collections section, you can define individual storage collections to use for different log types. For example, you may want to create collections for compliance reasons or to selectively retain critical logs.

Procedures related to this dialog box are described in Configure Archiver Storage and Log Retention and Configure Log Storage Collections.

To access the Collection dialog:

1. Select **ADMIN > Services**.
2. Select an Archiver service and  **>View > Config**.
3. In the Services Config view for the service, click the **Data Retention** tab.
4. In the **Collections** section, click  to add or edit the rule.
   The Collection dialog is displayed.



The following table describes the fields in the Collection dialog.

Field	Description
Collection Name	Specify a name for your collection, such as Compliance, MediumValue, or LowValue.
Hot Storage	Specify the maximum size or percentage of hot storage to use for this collection. The free space available to use for hot storage and the total hot storage are shown next to this field. When the size of the logs reach the maximum hot storage size, the logs are removed or they roll to the next available storage tier (warm or cold).
Warm Storage	(Optional) Specify the maximum size or percentage of warm storage to use for this collection. The free space available to use for warm storage and the total warm storage are shown next to this field. When the size of the logs reach the maximum warm storage size, the logs are removed or they roll to available cold storage.

Field	Description
Cold Storage	(Optional) Specify whether to use cold storage for this collection. If you use cold storage for the collection, logs outside of the specified size and retention limits roll over to cold storage. If you do not use cold storage, logs outside of the specified size and retention limits are removed.
Retention	(Optional) Specify the number of days that logs are retained before they are removed or rolled over to cold storage. For Hot and Warm Storage, size and retention period settings for a collection can override each other based on which criterion (size or time) is satisfied first.
Compression	Specify the type of compression to use for meta and raw logs in the collection. You can compress the meta and raw logs using GZIP or LZMA to save space. GZIP is very fast at compressing and decompressing, but it does not compress as well as LZMA. LZMA offers better compression at a cost of decompression speed (roughly three times slower than GZIP). Compression ratios are highly dependent on your data. The default compression is GZIP.
Hash	Specify whether to enable or disable hash. When enabled, the hash algorithm is used to verify the data integrity of the files being saved. By default, the only data being hashed is raw logs and the hash files are saved in the same directory as

Note: When decreasing collection storage allocations or lowering retention time, it may take several minutes to hours for the data to move and space to become available depending on the amount of moving (rolling) data. The default times are every 20 minutes for a size roll and every six hours for a time roll.

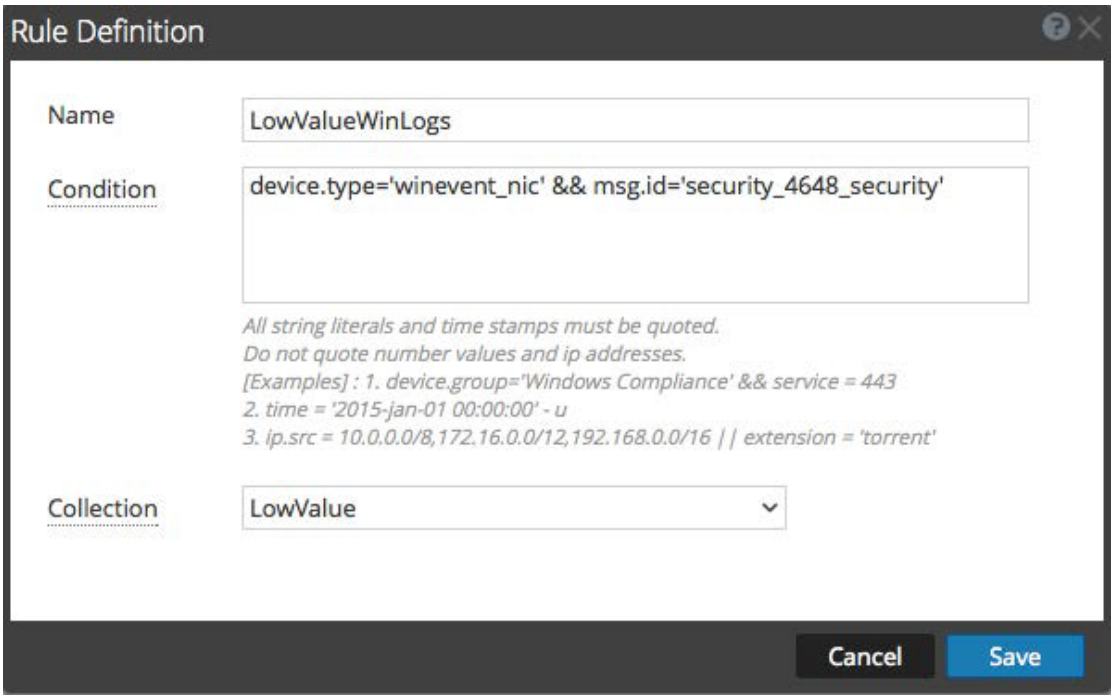
Rule Definition Dialog

In the ADMIN > Services > Config view > Data Retention tab of an Archiver, Administrators can define the criteria for log retention and storage. In the Rule Definition dialog, which is accessible from the Retention Rules section, you can define retention rules to use for your storage collections.

Procedures related to this dialog box are described in Configure Archiver Storage and Log Retention and .Define Retention Rules

To access the Rule Definition dialog:

1. Select **ADMIN > Services**.
2. Select an Archiver service and **>View > Config**.
3. In the Services Config view for the service, click the **Data Retention** tab.
4. In the **Retention Rule** section, click + or ✎.
   The Rule Definition dialog is displayed.



The following table describes fields in the Rule Definition dialog.

Field	Description
Name	Specify a unique name for your retention rule. For example: ComplianceDevices
Condition	Specify the conditions for the type of logs that you want to include in the collection. All sting literals and time stamps must be quoted. Do not quote number values and IP addresses. For example: device.group='PCI Devices' || device.group='HIPPA Devices'
Collection	Select the collection on which you want to apply this rule. For example: Compliance

Next Step

Configure log storage collections.

Configure Log Storage Collections

This topic provides instructions for Administrators on how to configure log storage collections on an Archiver.

NetWitness Suite enables you to define individual storage collections for different log types. You can specify the maximum size of the Hot and Warm Storage space used by the collection, whether to use offline storage (Cold Storage), the number of days to retain the logs in the collection, the data compression, and whether to use a hash algorithm to be able to verify the data integrity of the files being saved. You should create collections based on your log retention storage requirements. Each collection that you create must be associated with at least one retention rule.

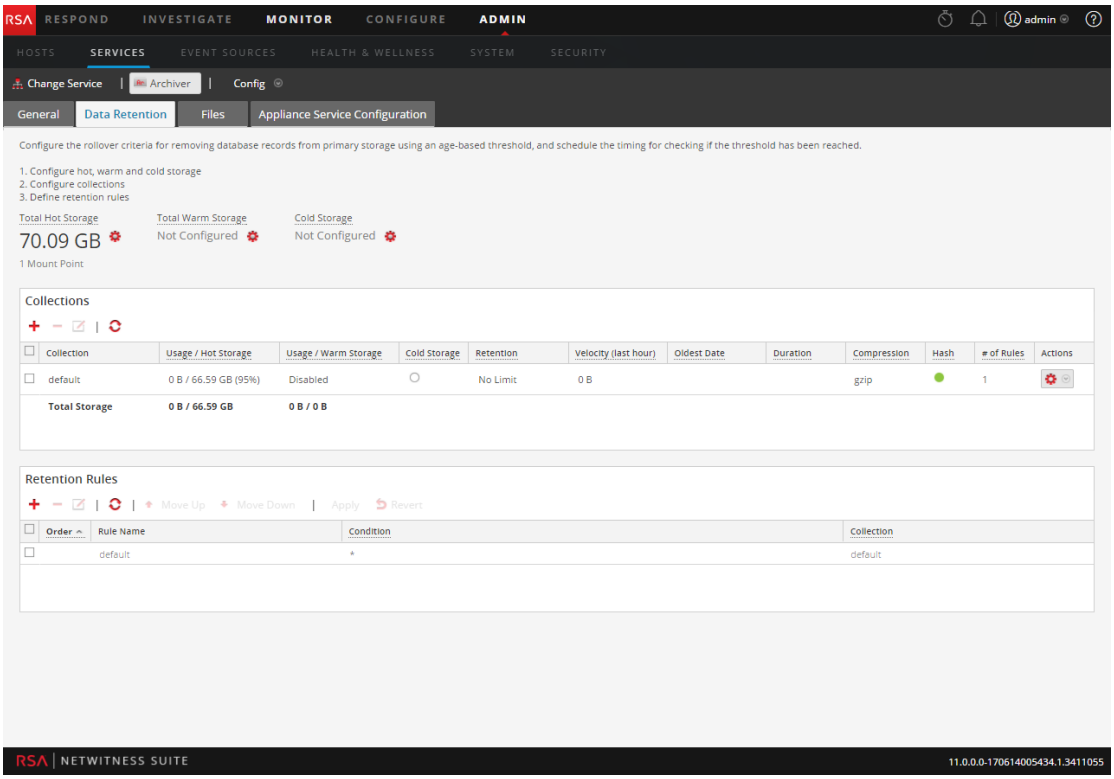
Prerequisites

Before you configure your log retention storage collections, configure total hot, warm, and cold storage.

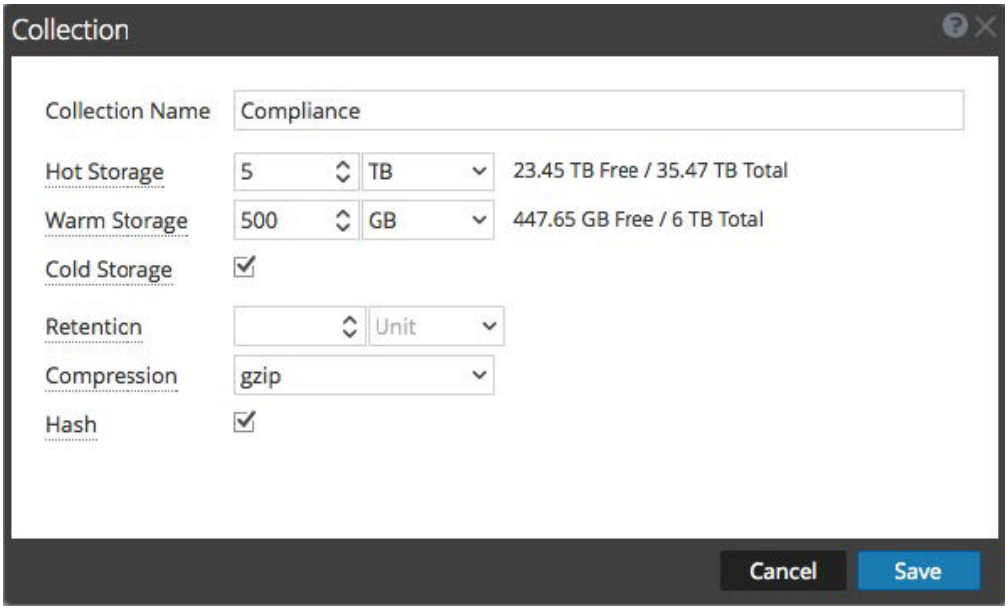
Configure a Log Storage Collection

To configure a log retention storage collection on an Archiver:

1. Go to **ADMIN > Services**.
2. Select the Archiver service and  **> View > Config**.
   The Services Config view of Archiver is displayed.
3. On the **Data Retention** tab, in the **Collections** section, click  to add a collection.
   (If you decide to make changes to an existing collection, you can select the collection and click  to change the settings.)



The **Collection** dialog is displayed.



4. Configure the collection as described in the following table.

Field	Description
Collection Name	Specify a unique name for your collection, such as Compliance, MediumValue, or LowValue.
Hot Storage	Specify the maximum size or percentage of hot storage to use for this collection. The free space available to use for hot storage and the total hot storage is shown next to this field.
Warm Storage	(Optional) Specify the maximum size or percentage of warm storage to use for this collection. The free space available to use for warm storage and the total warm storage is shown next to this field.
Cold Storage	(Optional) Specify whether to use cold storage for this collection. If you use cold storage for the collection, logs outside the storage limits are copied to cold storage before they are deleted from hot or warm storage.
Retention	(Optional) Specify the number of days that logs are retained before they are removed or rolled over to cold storage. For Hot and Warm Storage, size and retention period settings for a collection can override each other based on which criterion (size or time) is satisfied first.
Compression	Specify the type of compression to use for meta and raw logs in the collection. You can compress the meta and raw logs using GZIP or LZMA to save space. GZIP is very fast at compressing and decompressing, but it does not compress as well as LZMA. LZMA offers better compression at a cost of decompression speed (roughly three times slower than GZIP). Compression ratios are highly dependent on your data. The default compression is GZIP.
Hash	Specify whether to enable or disable hash. When enabled, the hash algorithm is used to verify the data integrity of the files being saved. By default, the only data being hashed is raw logs and the hash files are saved in the same directory as data.

5. Click **Save**.
   Any errors in the collection appear in red text. A dotted underline indicates that a tooltip is available with information about the error. Your collection name appears in red text until at least one retention rule is defined for your collection.

If you have a collection with editing disabled (grayed out), look at the associated tooltip for more information.

Note: When decreasing collection storage allocations or lowering retention time, it may take several minutes to hours for the data to move and space to become available depending on the amount of moving (rolling) data. The default times are every 20 minutes for a size roll and every six hours for a time roll.

Next Step

Define retention rules for your collections.

Define Retention Rules

Administrators can define and order retention rules for log storage collections on an Archiver. Retention rules specify the type of logs to be stored in the collection. For your log collections to gather and store log data, you must associate them with at least one retention rule. When you configure a retention rule, you specify a condition and a collection for that rule. The condition (rule definition) determines the type of logs stored in that collection.

For the condition, you can use anything that works in a regular query `where` clause.

For example, to get logs from compliance services, you can use the following condition:

```
device.group='PCI Devices' || device.group='HIPPA Devices'
```

After you define the retention rules for your collections, it is important that you specify the order of your retention rules. NetWitness Suite evaluates the retention rules for all of the collections in numerical order by the number listed in the Order column in the Retention Rule section of the Data Retention tab of the Archiver (ADMIN > Services Config view).

Caution: Rule order is very important. It determines the priority for evaluating the log data for storage retention.

Prerequisites

Before you configure your retention rules:

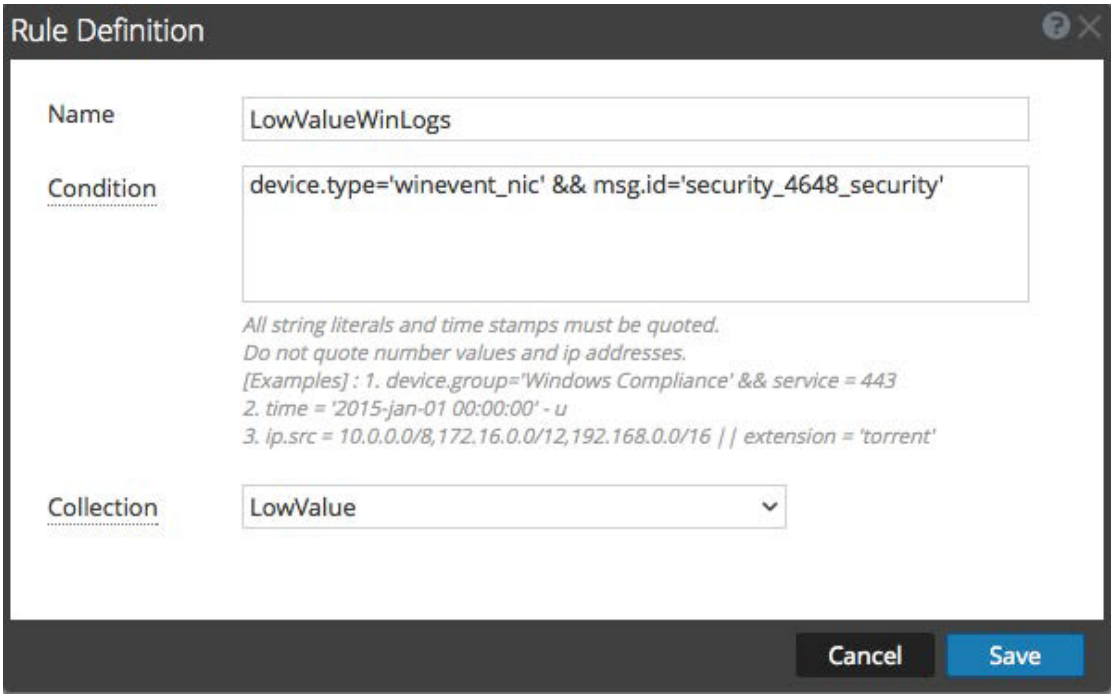
- Configure total hot, warm, and cold storage
- Configure log storage collections

Procedures

Define a Retention Rule for a Collection

1. Go to **ADMIN > Services**.
2. Select the Archiver service and  **> View > Config**.
   The Services Config view of Archiver is displayed.
3. On the **Data Retention** tab, in the **Retention Rule** section, click  .

The **Rule Definition** dialog is displayed.



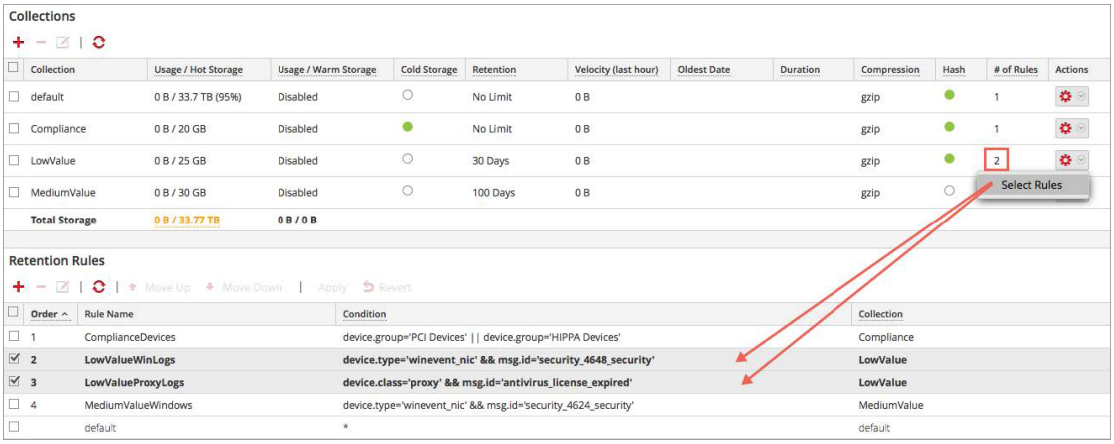
4. Configure the fields in the Rule Definition dialog as described in the following table:

Field	Description
Rule Name	Specify a unique name for your retention rule. It cannot include spaces. For example: LowValueWinLogs
Condition	Specify the conditions for the type of logs that you want to include in the collection. All string literals and time stamps must be quoted. Do not quote number values and IP addresses. For example: `device.type='winevent_nic' && msg.id='security_4648_security'`
Collection	Select the collection on which you want to apply this rule. For example: LowValue.

5. Click **Save**.

   The retention rule that you define becomes associated with the collection you selected. On the **Data Retention** tab, in the **Collections** section, you can click  > **Select Rules** in

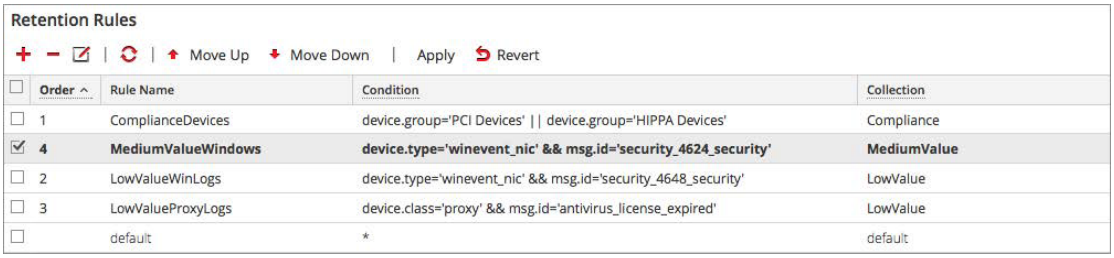
the **Actions** column for the selected collection to view the retention rules associated with the collection in the **Retention Rule** section.



Specify the Order of your Retention Rules

To prioritize the complete list of all of your retention rules:

1. In the **Retention Rule** section of the **Data Retention** tab, select a retention rule and use drag and drop (or select **Move Up** and **Move Down**) to change its order in the priority list.



2. Click **Apply** to save the order of the retention rules.

Caution: Rule order is very important. It determines the priority for evaluating the log data for storage retention.

Next Step

Add Archiver as a Data Source to Reporting Engine.

Add Archiver as a Data Source to Reporting Engine

This topic provides instructions on how to add Archiver Archiver as a data source to Reporting Engine to generate reports for the data collected by Archiver.

Prerequisites

Ensure that you have:

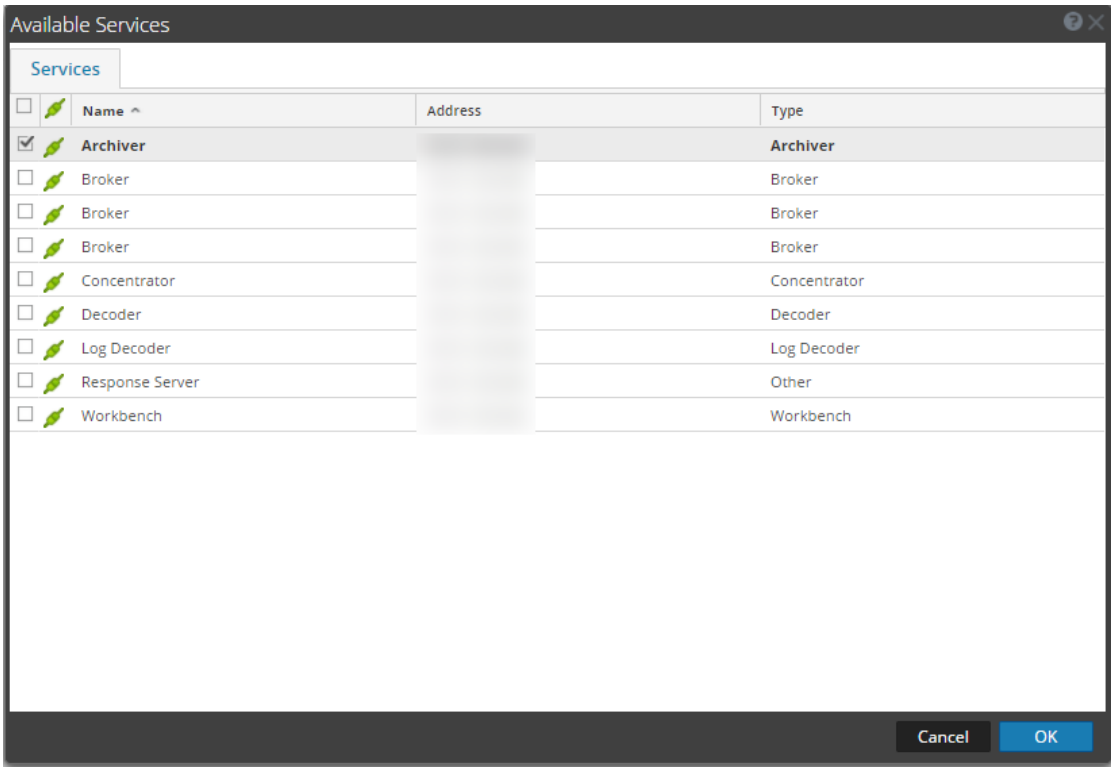
1. Installed the Archiver host in your network environment.
2. Installed and configured a Log Decoder Decoder in your network environment.
3. Verified that Reporting Engine and Archiver services are active.

Procedure

To associate an Archiver data source with Reporting Engine:

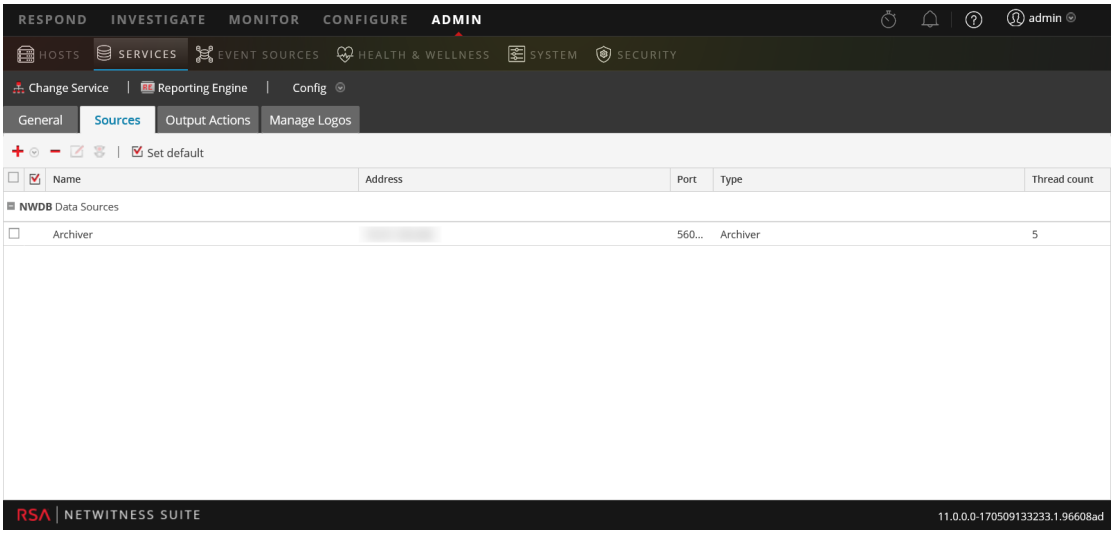
1. Go to **ADMIN > Services**.
2. In the **Services** panel, select a **Reporting Engine** service.
3. In the **Actions** column, select **View > Config**.
4. Select the **Sources** tab.
5. Click + and select **Available Services**.

   The Available Services dialog is displayed.



6. Select the Archiver that you want to add as data source to the Reporting Engine and click **OK**.
7. In the Service Information dialog, type the username and password for the Archiver.
8. Click **OK**.

   The selected Archiver is listed in the NWDB Data Sources category.



You can now create reports on the data collected by Archiver.

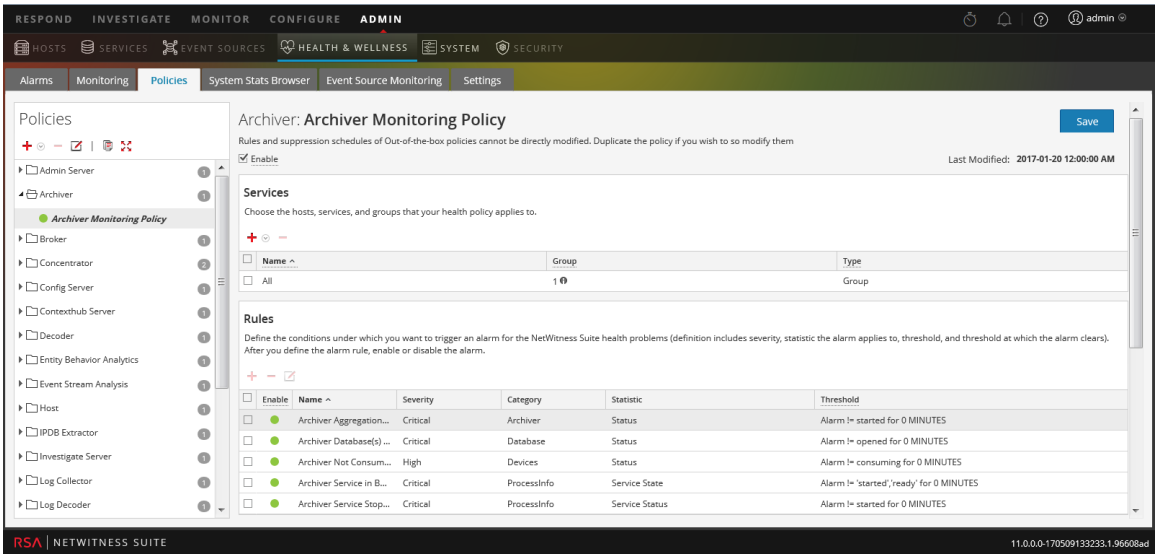
Next Step

Configure alerts for archive storage.

Configure Archiver Monitoring

Health & Wellness enables you to automatically generate notifications when critical thresholds are met.

Review the Health & Wellness policies for Archiver and Host in the Health & Wellness Policies section. Make updates as required.



For detailed information, see **Manage Policies** in the *System Maintenance* guide.

Additional Archiver Configuration

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

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

Topics

Configuring Data Backup and Restore

This topic provides information on the Data Backup and Restore feature for an Archiver. You can use this feature to back up Archiver data and retrieve the backed up data.

You can back up the data in the following ways:

- Use scripts to copy files from cold storage backup folders onto an offline storage.
- Use backup software to copy files from cold storage backup folders onto an offline storage.
- Run EMC Networker or other backup software on Archiver and have it do daily incremental backup of the database files.

Note: For details on the procedure to back up data using Networker, see the *Administration Guide for Networker*.

Once you have the data backup, you have to perform the following tasks to restore the backed up data that is installed on the Archiver.

Action	Description
1. Restore your data to a location accessible by the Archiver.	Refer to Create Collection
2. Create a collection in Archiver that uses that location.	Refer to the **Manage Collections** topic in the *Workbench Configuration Guide*.
3. Add the Archiver service as a data source on Reporting Engine to generate reports for the data restored on the Archiver service.	Refer to Add Archiver as a Data Source to Reporting Engine

Add Archiver Service

The NetWitness Suite Archiver service enables you to create collections with restored data from Archiver offline (cold) storage. This procedure is only required if you do not have the Archiver service installed.

Prerequisites

Make sure you have added an Archiver host and applied a license to it.

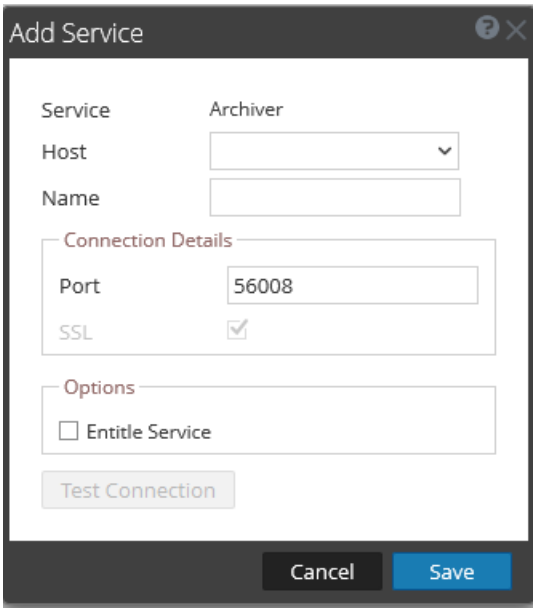
Procedure

Note: This procedure is only required if you do not have Archiver service installed.

Perform the following steps to add the Archiver service:

1. Go to **ADMIN > Services**.
2. In the **Services** panel, select + **>Archiver**.

   The Add Service dialog is displayed, as shown below.



3. Provide the following details.

Field	Description
Host	Select an Archiver host from the drop-down menu.
Name	Type a name for the service.
Port	Default port is 50007.
SSL	Select **SSL** if you want NetWitness Suite to communicate with the service using SSL. The security of data transmission is managed by encrypting information and providing authentication with SSL certificates. **Note:** If you select SSL, ensure SSL is enabled in the System Configuration panel.
Username	(Optional) Type the username for the service.
Password	(Optional) Type the password for the service.

4. Click **Test Connection** to determine if NetWitness Suite connects to the service.
5. When the result is successful, click **Save**.
   The added service is now displayed in the Services panel.

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

Create Collection

This topic provides information on how to create a collection on an Archiver service.

You can create a collection using data restored from the backed-up data or an existing subset of data. When you recover the backed-up data, you have to place it in the collection folder created on the Archiver service to enable you to generate the required reports for the retrieved data. For example, if you have backed up the data using EMC Networker at <*location*>, you can use the restore options in Networker to restore the backed-up data to the collection folder created on the Archiver service. For restore procedure using EMC Networker, see the *Administration Guide for Networker*.

Prerequisites

Ensure that you have:

- Archiver service installed on an Archiver host.
- Ensure the Archiverservice has enough space to hold the collection.

- The backed-up data placed in a known location on your local host, if you are creating a collection using the data restored from the backed-up data.

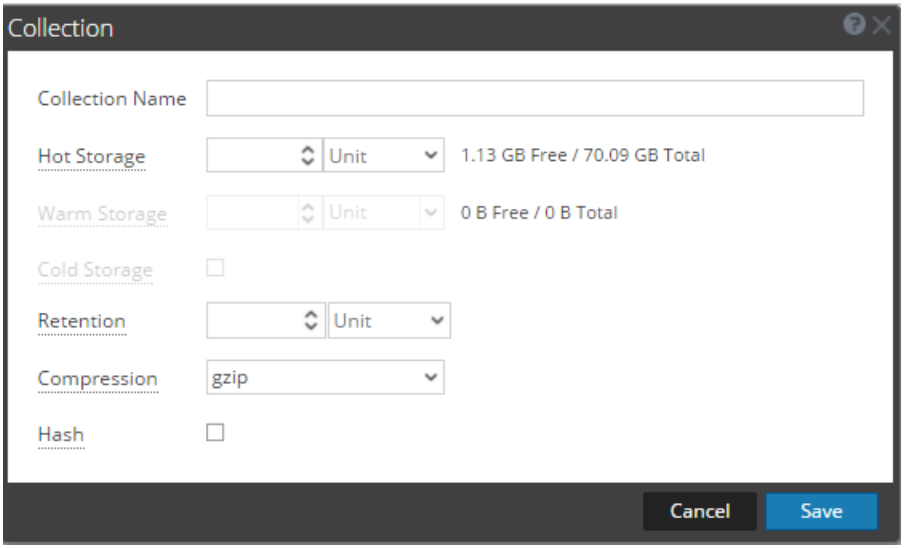
Procedure

The Data Retentions tab enables Administrators to restore and save data that is restored from a backup or from an existing set of data.

Note: The Administrator can point the source path to the location of the database files and the restore command copies them to the Archiver. The Administrator needs to mount those directories to the Archiver before a restoration collection can be created.

To create a collection using data restored from the backed-up data or existing subset of data:

1. Go to **ADMIN > Services > Archiver**.
2. From the **Services** grid, select **>View > Config**.
   The **General** tab is displayed.
3. Select the **Data Retentions** tab and click + in the **Collections** panel to add a collection.
   The **Collection** dialog is displayed.



5. Provide the following information:
   - **Collection Name:** Name of the Archiver collection that you want to restore.
   - **Hot Storage:**Enter the number of Archiver database files and unit size (either Gigabytes or Terabytes) that have been moved from cold storage.
   - **Retention:** Select the number of days or hours that you want to store the collection.
   - **Compression:** Select the compression type for the collection.

6. Click **Save** to restore the collection.

   Note: Target is the location where the collection is created.

   Note: If the source path provided to create the restoration collection does not exist, the following error message is displayed:
   "The source path does not exist '/xxx/xxx/'."
   If there is insufficient storage to restore your collection, the following error is displayed:
   "Error during disk space checking. Insufficient disk space in location '/xxx/xxx'."

   The Schedule Job dialog is displayed with the following message:
   "Restoring data into a new collection. Check the jobs page for progress."

7. Click **Jobs**  icon in the top right area of the main menu to expand the list of restoration collection jobs with their current status.

Note: When restoring a collection, the larger the dataset that you have to restore, the longer the restoration will take. If you are restoring a collection containing hundreds of gigabytes or more, restoration may take several hours.

Add Archiver Service as a Data Source to Reporting Engine

This topic provides instructions on how to add the Archiver service as a data source to Reporting Engine to generate reports for the data restored onto the Archiver.

Prerequisites

Ensure that you have:

- Installed the Archiver service on the Archiver host.
- Added a collection on the Archiver service.

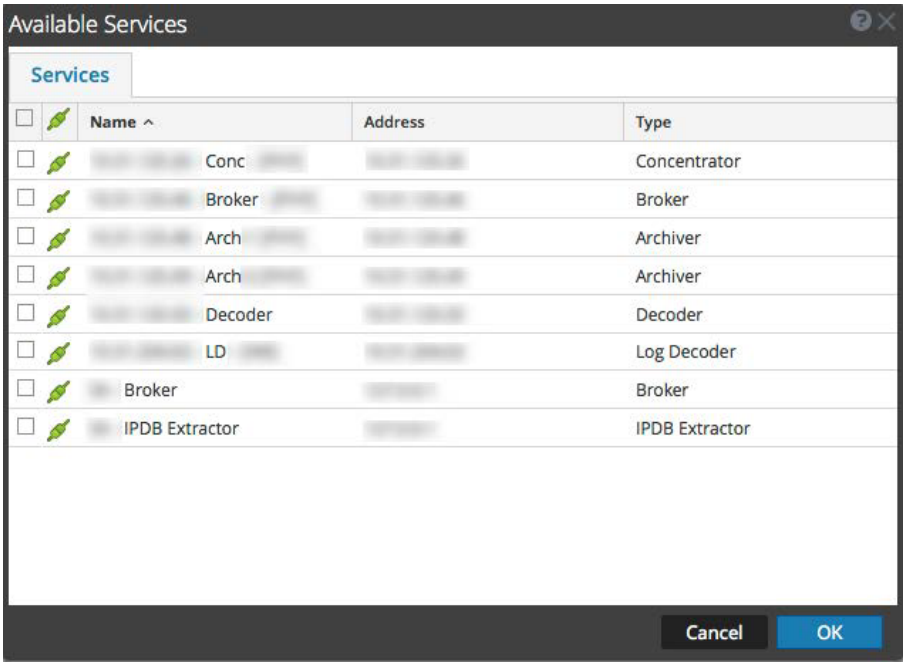
Procedure

Perform the following steps to add the Archiver service as a data source to Reporting Engine:

1. Select **ADMIN > Services**.
2. In the **Services** panel, select a Reporting Engine service.
3. In the **Actions** column, select **View > Config**.
4. Select the **Sources** tab.

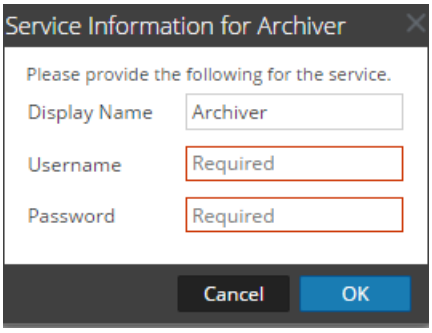
5. Click + and select **Available Services**.

   The Available Services dialog is displayed.



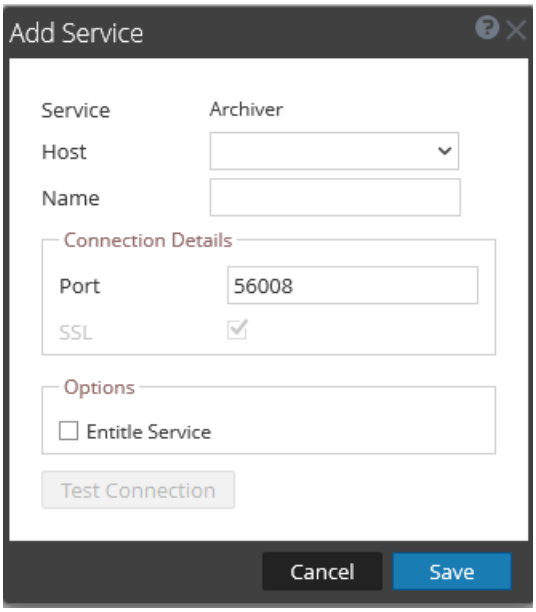
6. Select the Archiver service and click **OK**.

   If the Archiver service is using a Trust Model, the Service Information dialog for the selected service is displayed with the username and password fields required. If the service is not using a Trust Model, these fields will be optional.



7. Type the username and password for admin credentials for the service.

8. Click **OK**.
   The Add Service dialog is displayed.



9. Select a host from the drop-down list and click **Save**.
   The Archiver service is now added as a data source to the Reporting Engine and is listed in the NWDB Data Sources list.

Note: This procedure has to be performed for each collection.

An Administrator can create and delete Workbench collections. and view Workbench statistics and logs. This topic provides all of these procedures and an example procedure for restoring a collection for Reporting and Investigation.

- Mount Archiver Directories
- Create a Collection
- Delete a Collection
- Investigate a Collection
- View Workbench Collection Statistics
- View Workbench Logs

Mount Archiver Directories

If data is in offline storage or cold-tier storage, you need to mount the Archiver directories in order to restore the data for reporting and investigation purposes:

1. Go to **ADMIN > Services**.
2. Select an **Archiver** from the Services grid and select  **> View > Explore**.
   The Explorer view for the Archiver is displayed
3. Right-click on the **Database** node in left-hand tree and select **Database** properties to open them in the right-hand panel.
4. Run the **manifest** command for a time range, for example, 2015-April-01 to 2015-April-10.
   The search returns all files that need to be restored for the selected query.

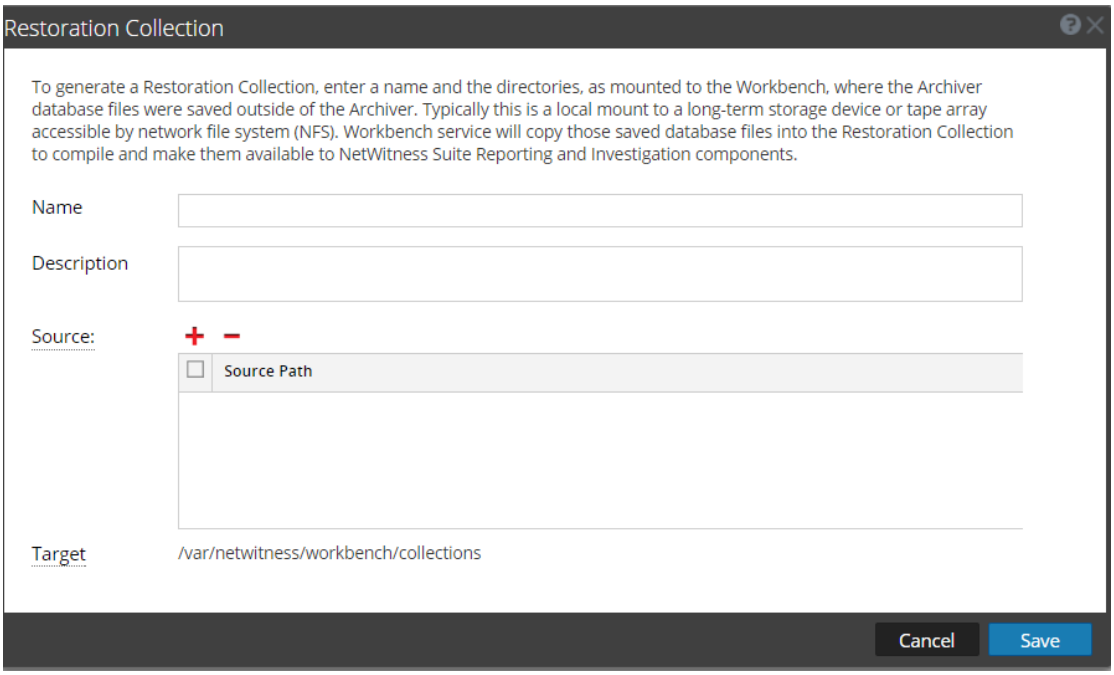
Create a Collection

Administrators can create collections of restored data from a backup or from an existing set of data.

Note: You can point the source path to the location of the database files and the restore command copies them to the Archiver. You need to mount those directories to the Archiver (where the Workbench is installed) before a restoration collection can be created.

To create a collection using data restored from the backed up data or existing subset of data:

1. Go to **ADMIN> Services.**
2. In the Services view, select a **Workbench**, then select  **> View > Config**.
   The Services Config view is displayed with the General tab open.
3. Click the **Collections** tab.
   The Collections grid is displayed.
4. Click + in the toolbar.
   The Restoration Collection dialog is displayed.



5. Provide the following information:

   - **Name:** Name of the Workbench collection that you want to restore.
   - **Source:** Location where the Archiver database files have been moved from cold storage.

   Note: Target is the location where the collection is created.

6. Click **Save** to restore the collection.

   Note: If the source path provided to create the restoration collection does not exist, the following error message is displayed:

   ```
   The source path does not exist '/xxx/xxx/'.
   ```

   If there is insufficient storage to restore your collection, the following error is displayed:

   ```
   Error during disk space checking. Insufficient disk space in location '/xxx/xxx'.
   ```

   The Schedule Job dialog is displayed with the following message:

   ```
   Restoring data into a new collection. Check the jobs page for progress.
   ```

7. Click the **Jobs** icon  in the NetWitness Suite toolbar to expand the list of restoration collection jobs with their current status.

Note: Restoring a collection that is larger than 550 GB may take several hours to process.

Delete a Collection

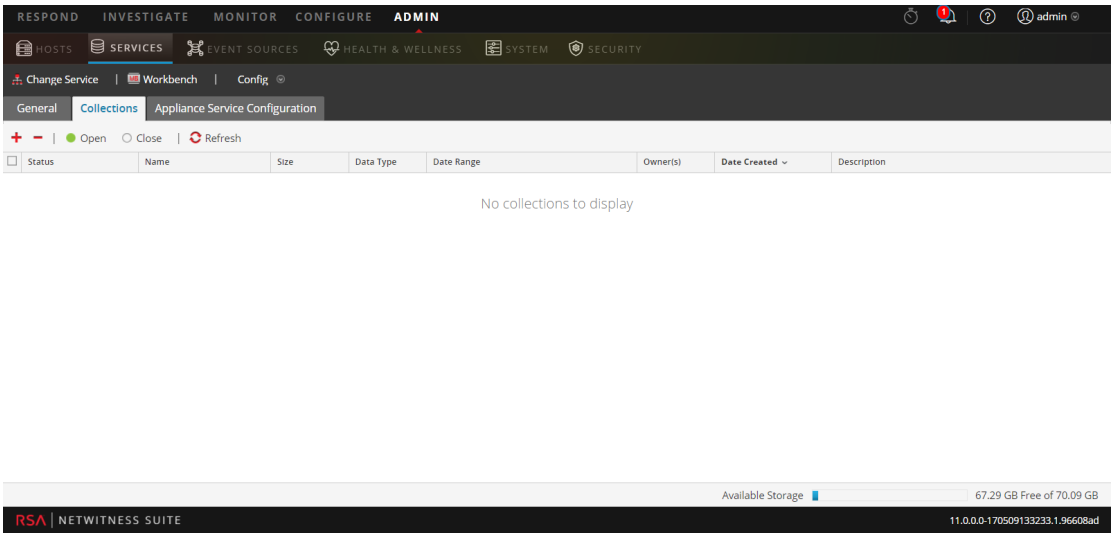
Administrators can delete collections from the Workbench service.

Perform the following steps to delete a collection:

1. Go to **ADMIN > Services.**
2. From the Services view, select a **Workbench** and click  **> View > Config**.

   The Services Config view opens with the General tab displayed.
3. Select the **Collections** tab.

   The Collections grid is displayed.



4. In the Collections grid, select the collection that you want to delete.
5. Click from the toolbar.

   A warning dialog requests confirmation.
6. If you want to delete the collection, click **Yes**.

   The collection is removed from the Workbench service.

Example Procedure: How to Restore a Collection for Reporting and Investigation

The following steps illustrate how to restore data for reporting and investigation purposes that is in offline storage or cold-tier storage. In the following example, data is restored for the time range beginning on 2015-April-01 through 2015-April-10.

To restore data for reporting and investigation purposes:

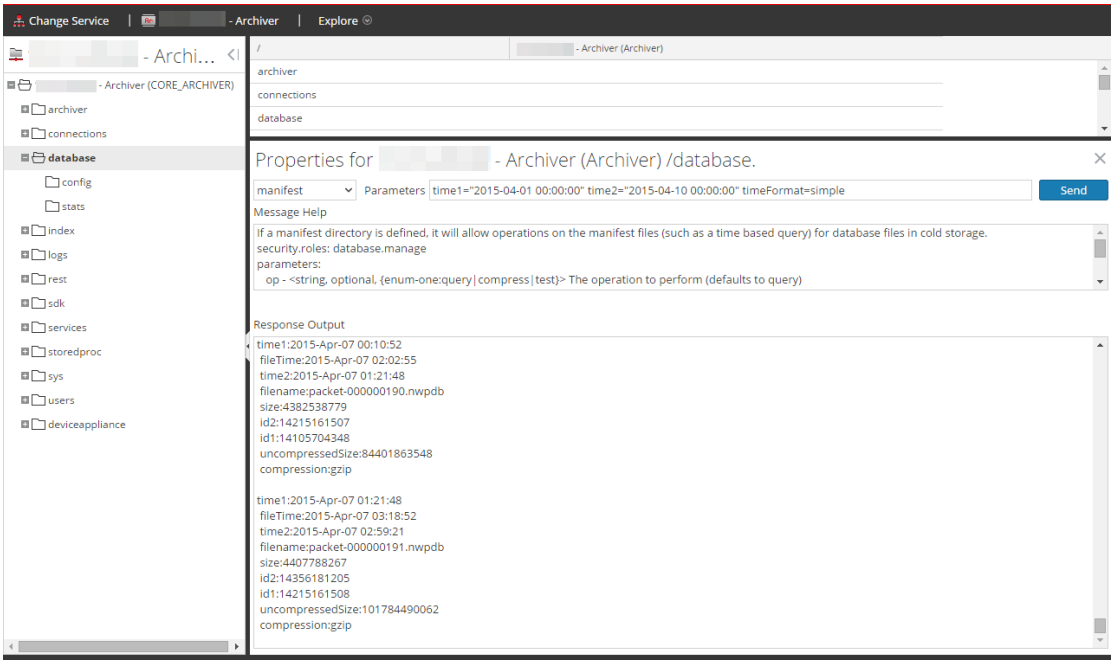
1. Go to **ADMIN > Services**.
2. Select the **Archiver**from the Services grid.
3. Navigate to the Explorer view of the Archiver appliance by selecting  **> View > Explore**.

   The Explorer view for Archiver is displayed
4. Right click on **Database** node in left-hand tree and select **Database** properties to open them in the right-hand panel.
5. Run the **manifest** command for the selected time range 2015-April-01 to 2015-April-10.

   The search returns all files that need to be restored for your selected query.

   Example Search:

   ```
   time1="2015-04-01 00:00:00" time2="2015-04-10 00:00:00"
   timeFormat=simple
   ```



6. Go to **ADMIN > Services**.
7. In the Services view, select a **Archiver**, then select  **> View > Config**.

   The Services Config view is displayed with the General tab open.
8. Select the **Collections tab.**
9. Create a restoration collection with the source path pointing to files listed in the manifest command output.

10. Save the collection.
    After successfully creating a collection, you can use this collection for reporting and investigation purposes.

Investigate a Collection

To perform an investigation on an Archiver collection:

1. Select **Investigate**.
   The Investigate dialog is displayed.
2. Click the **Collections** tab in the Investigate dialog.
3. Select an Archiver service in the left panel.
4. Select the collection you want to investigate in the right panel.
5. Click **Navigate**.

The Navigate view is displayed showing data pertaining to the Archiver collection that you selected.

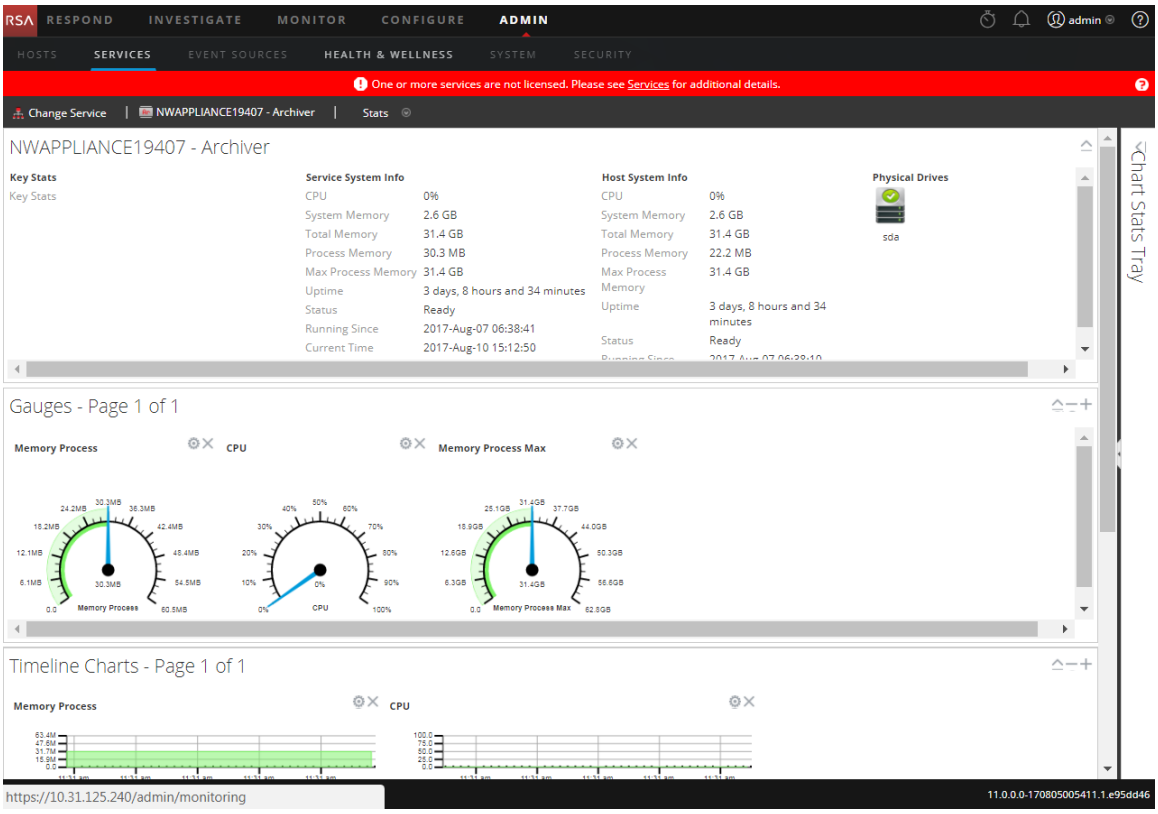
Note: For detailed information about using Investigation, see *Investigation and Malware Analysis*.

View Archiver Collection Statistics

The same statistics available for other services are provided for the Archiver service. The Services Stats view displays key statistics and system information that pertain to your selected Archiver service. The information is displayed in several different sections within the Stats view: Archiver, Gauges, Timeline Charts and Chart Stats Tray. The Chart Stats Tray lists all available statistics for the Archiver. Any statistic in the Chart Stats Tray can be displayed in a gouge or a timeline chart.

Perform the following steps to view Archiver statistics:

1. Go to **ADMIN > Services**.
2. In the Services view, select an Archiver, then select  **> View > Stats**.
   The Services Stats view is displayed.



Note: For more information about Archiver statistics, see the *Host and Services Getting Started Guide*.

View Archiver Logs

Perform the following steps to view logs on an Archiver service:

1. Go to **ADMIN > Services.**
2. In the Services view, select a **Archiver**, then select  **> View > Logs**.
   The Services Logs grid is displayed.

Note: For information about viewing and configuring audit logs, see the topic **Configure Global Audit Logging** in the *System Configuration Guide* .

Add Archiver Service as a Data Source to Broker

Adding the Archiver service as a data source to Broker is useful when you have more than one collection and you want a report on the archived data. To do this, you can add more than one collection as a downstream service to a Broker and then generate a report on it.

Prerequisites

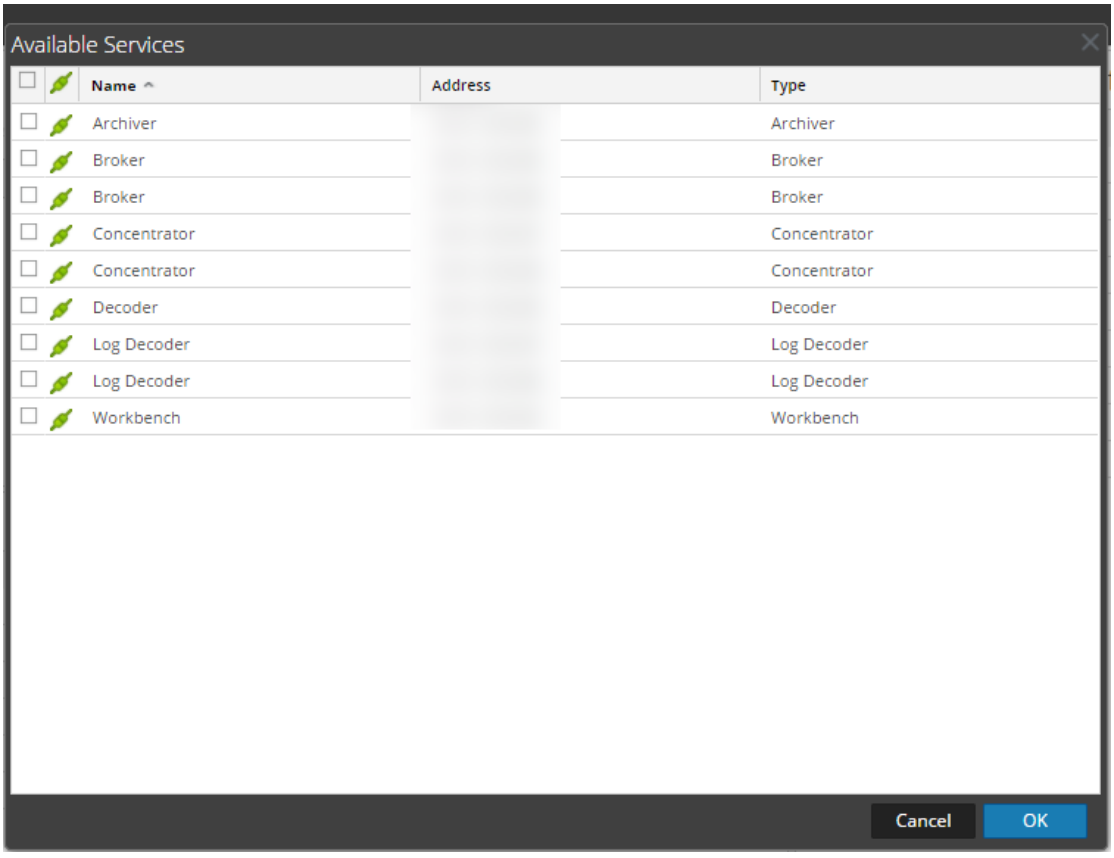
Ensure that you have:

- Installed the Archiver service on the Archiver host.
- Added a collection on the Archiver service.

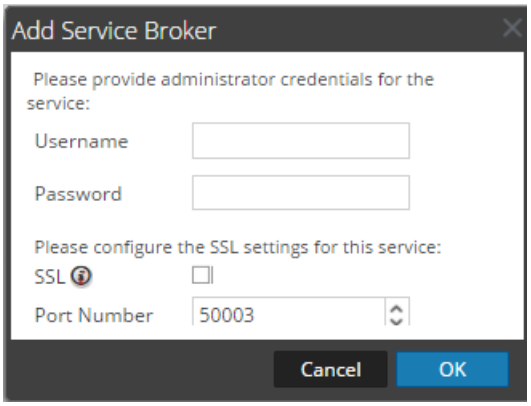
Procedure

To add an Archiver service as a data source on the Broker:

1. Select **ADMIN > Services**.
2. In the **Services** panel, select a Broker service.
3. In the **Actions** column, select > **View** > **Config**.
   The Config view is displayed with the General tab open.
4. In the **Aggregate Services** section, click +.
   The Available Services dialog is displayed.

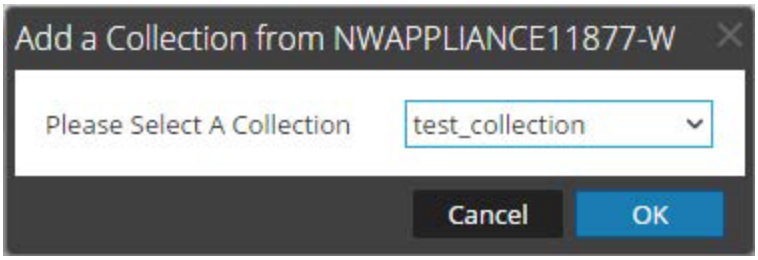


6. Select the Broker service and click **OK**.
7. If the Archiver service is using a Trust Model, a Service Information dialog for the selected service is displayed.



8. Type the username and password for admin credentials for the service.
9. Click **OK**.

   The Add Collection dialog is displayed.



10. Select a collection from the drop-down list and click **OK**.

    The Archiver service is now added as a data source to the Broker.

Note: This procedure has to be performed for each collection.

Retrieve Hash Information

Archiver provides a command, **hashInfo**, which you can use to retrieve the hash information for each session, meta, and packet database that meets the session list or date range criteria. The hash information retrieved is in the form of a list of string parameters, each string parameter corresponding to the hash information for a single database file. You can retrieve the hash information of the database files using the Archiver Service Explore view or REST interface of the Archiver service. The hash information thus retrieved is used to compare the database files in the original location and the exported location to validate data integrity.

The following table lists the criteria that you can use to retrieve the hash files from the database.

Criteria	Description
sessions	You can retrieve the hash information of the database files by specifying the sessions that exist or read from the session database to determine the associated meta and packet id required to determine which meta and packet database files are needed to retrieve the hash information. **For example:** sessions=100 - Retrieves the hash information of all database files that contain the constituent components(session, meta, content) of session 100. sessions=100,500000 - Retrieves the hash information of all database files that contain the constituent components(session, meta, content) of session 100 and 500000
beginDate	You can specify a begin date as a filter against the database files. This finds the hash information for the files created after the specified date. The begin date specified has to be in the format YYYY-MM-DD HH:MM:SS.
endDate	You can specify an end date as a filter against the database files. This finds the hash information for the files created before the specified date. The end date specified has to be in the format YYYY-MM-DD HH:MM:SS **For example:** beginDate: “2014-Mar-25 05:52:00” endDate=”2014-Mar-27 05:52:00” – Retrieves the hash information of all the database files in between March 25, 2014 and March 27, 2014 in the specified time range on those days.

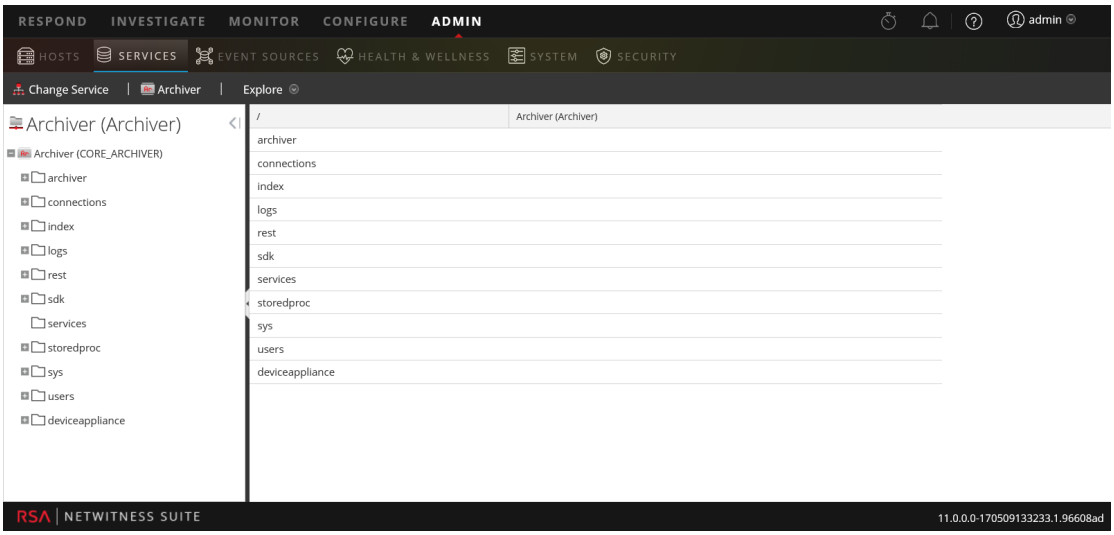
Criteria	Description
directories	By default, the hash information files are stored with the database files they were created for. You can also store the hash information file in different location by defining multiple locations in the hash.dir configuration parameter. You can define the location as a filter and retrieve the hash information files for the configured location. **For example:** directories="/home/hash" – Retrieves the hash information of the database files from the location /home/hash

Procedure

To retrieve hash information of the database files:

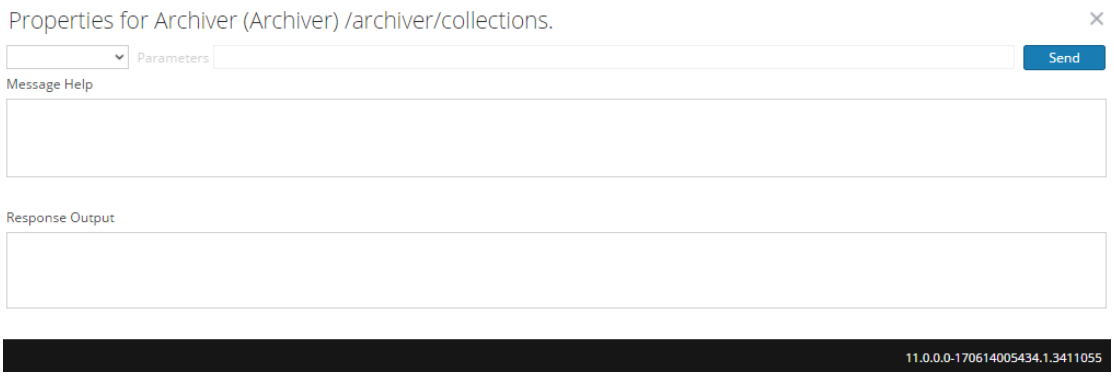
1. Select **ADMIN > Services**.
2. Select an Archiver service.
3. In the **Actions** column, select **View > Explore**.

   The Explore view of the Archiver service is displayed.



4. In the node tree, right-click on **archiver** and select **Properties**.

   The Properties dialog is displayed.



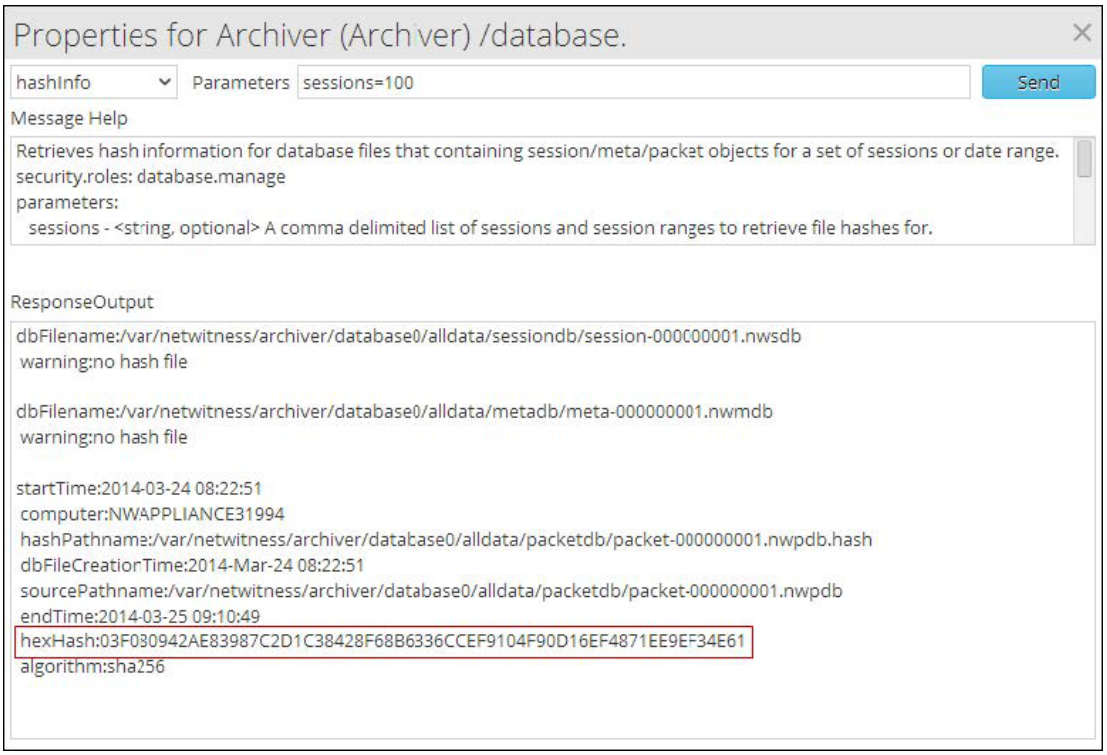
5. In the drop-down menu, select **hashInfo**.
6. In the **Parameters** field, type the criteria that you want to use to retrieve the hash information from the database.
7. Click **Send**.

   The output of the command is displayed in the ReponseOutput textbox. In the output, the hash information is shown in the hexHash parameter. You can use this hash information to verify data integrity manually.

Examples

Retrieve the hash information of the database files for the sessions that exist.
Criteria: sessions=100

Output

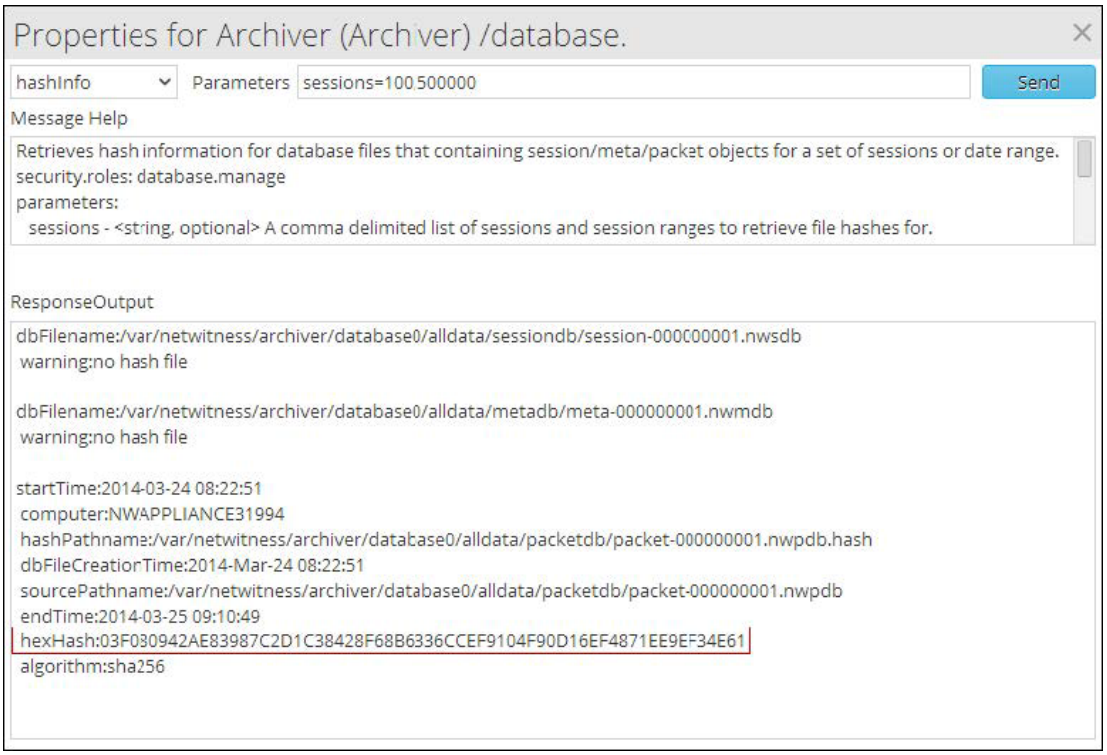


The hash information shown in the hexHash parameter is retrieved and you can use this to verify data integrity manually for session 100.

Retrieve the hash information of the database files for the session ranges that exist.

Criteria: sessions=100,500000

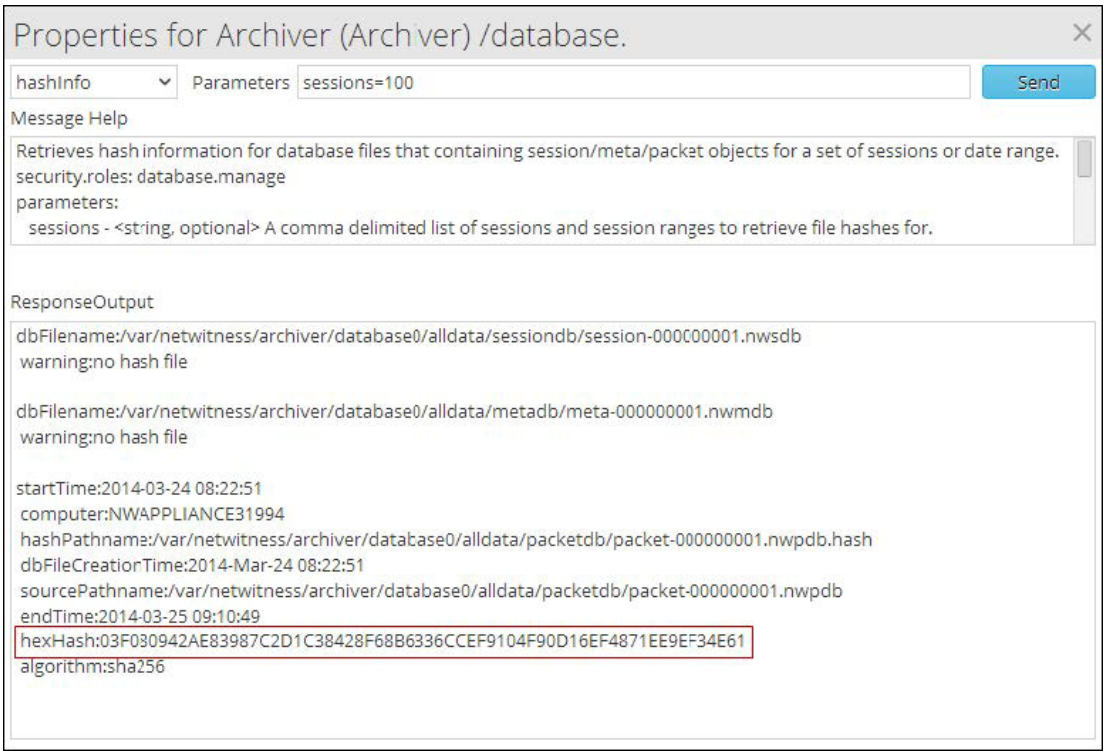
Output



The hash information shown in the hexHash parameter is retrieved and you can use this to verify data integrity manually for session range 100 - 500000

Retrieve the hash information of the database files created in the specified date range
Criteria: beginDate="2017-Mar-25 05:52:15" endDate="2017-Mar-27 05:52:15"

Output



The hash information shown in the hexHash parameter is retrieved and you can use this to verify data integrity manually for the date range specified.

References

This topic is a collection of references, which describe the user interface for Archiver in NetWitness Suite.

Topics

Archiver Collection Dialog

On the Administration > Services > Config view > Data Retention tab of an Archiver, Administrators can define the criteria for log retention and storage. In the Collection dialog, which is accessible from the Collections section, you can define individual storage collections to use for different log types. For example, you may want to create collections for compliance reasons or to selectively retain critical logs.

Workflow

This workflow illustrates the end-to-end installation and configuration process for an Archiver.

What do you want to do?

Role	I want to...	Show me how...
Administrator	Configure Archiver Collections	Configure Archiver Storage and Log Retention

Related Topics

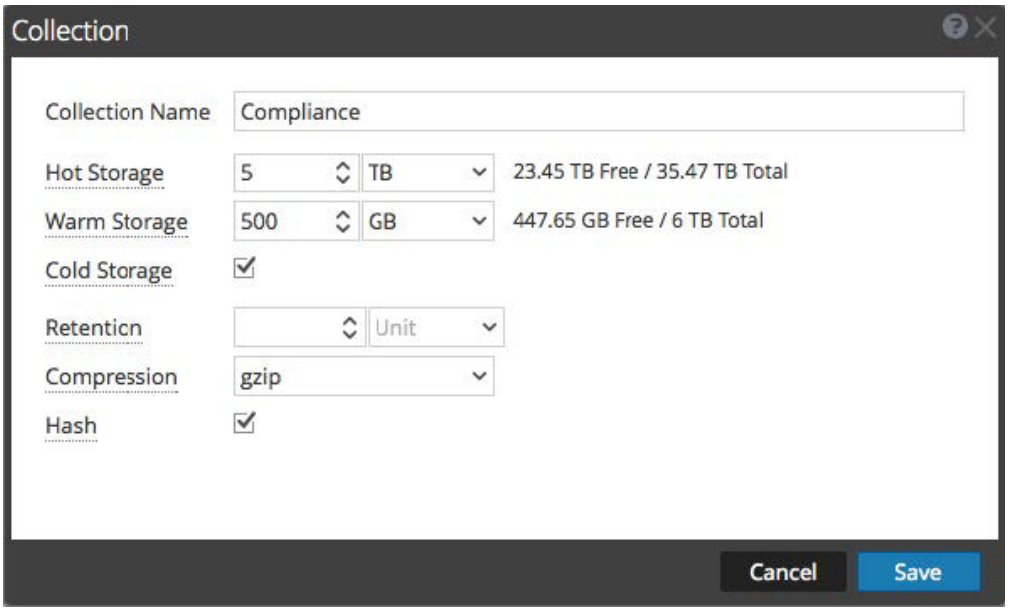
Configure Archiver Storage and Log Retention

Quick Look

To access the Collection dialog:

1. Go to ADMIN > Services.
2. Select an Archiver service and >  View > Config.
3. In the Services Config view for the service, click the Data Retention tab.
4. In the Collections section, click +.

   The Collection dialog is displayed.



Note: When decreasing collection storage allocations or lowering retention time, it may take several minutes to hours for the data to move and space to become available depending on the amount of moving (rolling) data. The default times are every 20 minutes for a size roll and every six hours for a time roll.

The following table describes the fields in the Collection Dialog.

Field	Description
Collection Name	Specify a name for your collection, such as Compliance, MediumValue, or LowValue.
Hot Storage	Specify the maximum size or percentage of hot storage to use for this collection. The free space available to use for hot storage and the total hot storage are shown next to this field. When the size of the logs reach the maximum hot storage size, the logs are removed or they roll to the next available storage tier (warm or cold).
Warm Storage	(Optional) Specify the maximum size or percentage of warm storage to use for this collection. The free space available to use for warm storage and the total warm storage are shown next to this field. When the size of the logs reach the maximum warm storage size, the logs are removed or they roll to available cold storage.

Field	Description
Cold Storage	(Optional) Specify whether to use cold storage for this collection. If you use cold storage for the collection, logs outside of the specified size and retention limits roll over to cold storage. If you do not use cold storage, logs outside of the specified size and retention limits are removed.
Retention	(Optional) Specify the number of days that logs are retained before they are removed or rolled over to cold storage. For Hot and Warm Storage, size and retention period settings for a collection can override each other based on which criterion (size or time) is satisfied first.
Compression	Specify the type of compression to use for meta and raw logs in the collection. You can compress the meta and raw logs using GZIP or LZMA to save space. GZIP is very fast at compressing and decompressing, but it does not compress as well as LZMA. LZMA offers better compression at a cost of decompression speed (roughly three times slower than GZIP). Compression ratios are highly dependent on your data. The default compression is GZIP.
Hash	Specify whether to enable or disable hash. When enabled, the hash algorithm is used to verify the data integrity of the files being saved.

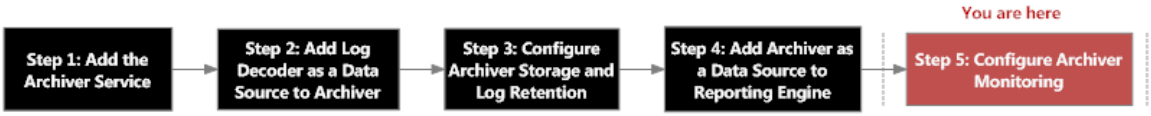
Archiver Services Config View - General Tab

The General tab for an Archiver in the Services Config view helps manage basic service configuration, configure the aggregate service, and configure the aggregation process between an Archiver and the aggregate service.

To access the General tab, go to ADMIN > Services, select an Archiver service, then select View > Config.

Workflow

This workflow illustrates the end-to-end installation and configuration process for an Archiver.



Configuring the aggregate service (whose data is consumed and aggregated) includes:

- Adding, editing, and deleting Archivers as aggregate services
- Toggling an aggregate service online and offline
- Monitoring statistics for aggregate services
- Starting and stopping aggregation

Configuring the aggregation process includes setting:

- Aggregation autostart
- Timing and performance parameters, such as the number of sessions per round of aggregation and time between rounds
- The timing of attempts to restart, reconnect, or take offline a non-responsive aggregate service

What do you want to do?

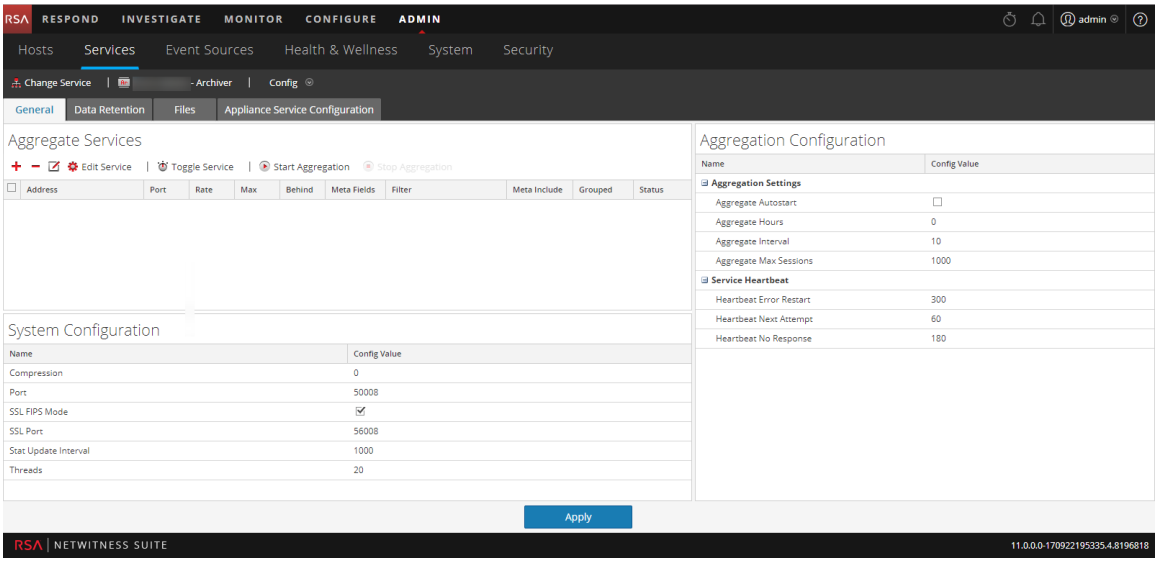
Role	I want to...	Show me how...
Administrator	Start and Stop aggregation Add, edit, delete, and toggle an aggregate service	Aggregate Services Section
Administrator	Manage System Configuration	System Configuration Section

Related Topics

Configure Archiver Monitoring

Quick Look

This is an example of the General tab.



These are the three major sections in the General tab for Archivers:

- Aggregate Services
- System Configuration
- Aggregation Configuration

Aggregate Services Section

The Aggregate Services section provides a way to start and stop aggregation, as well as add, edit, delete, and toggle an aggregate service. This is an example of the Aggregate Services section for a Concentrator.

The Aggregate Services section toolbar offers these options.

Option	Description
+	Opens a dialog in which you can add a Concentrator, Decoder, or Log Decoder as an aggregate service.
−	Removes the selected aggregate service.
	Opens a dialog to edit **Meta Fields** and **Filter** values.

Option	Description
Start Aggregation	When aggregation has been stopped or has not started, starts aggregating data from the online service in the list using the rules defined for the service.
Stop Aggregation	When aggregation is in progress, stops aggregation on the Broker or Concentrator. This stops all services and flushes the index, which may take several minutes to complete. It is necessary to stop aggregate services in order to perform various administrative procedures.
Toggle Service	Toggles the state of a service between offline and online. Only data from online service is consumed during aggregation.

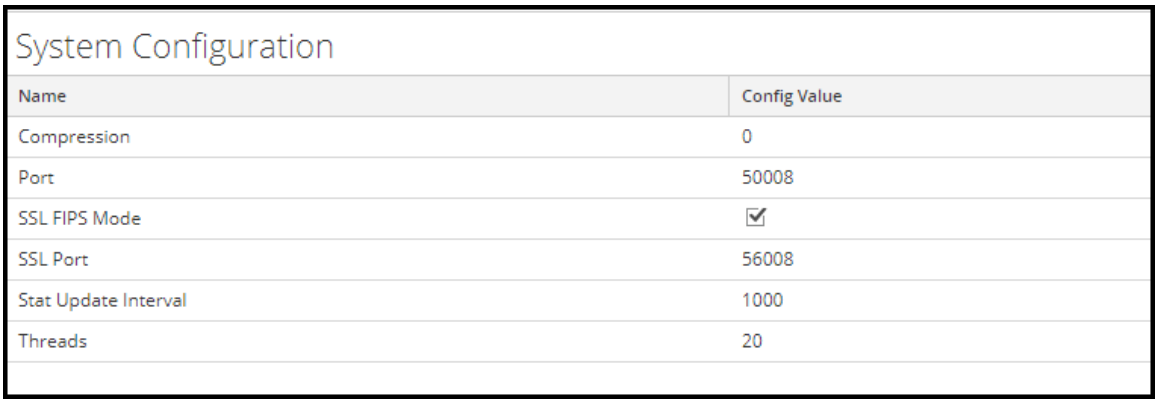
The Aggregate Services section list has these columns.

Column	Description
Address	Lists the address of the service.
Port	Lists the port on which the service listens. The default ports are: • 50001 for Log Collectors • 50002 for Log Decoders • 50003 for Brokers • 50004 for Decoders • 50005 for Concentrators • 50007 for other services
Rate	Lists the number of metadata objects being written to the database per second. Values are rolling average samples over a short time period (10 seconds). After capture stops, the rate is reset to **0**.

Column	Description
Max	Lists the maximum number of metadata objects written to the database per second since capture started. Values are rolling average samples over a short time period (10 seconds). After capture stops, **Max** continues to show the maximum value during capture.
Behind	Lists the number of sessions on the service that need to be aggregated.
Collection	For Brokers only, indicates the collection that was selected when the Analyst Workbench service was added to the Aggregate Services section.
Meta Fields	For Concentrators only, lists the types of metadata being consumed by the aggregate service.
Filter	For Concentrators only, lists any filter being applied to the metadata being consumed by the aggregate service.
Meta Include	For Concentrators only, lists the number of types of meta included in the aggregate service.
Grouped	Whether or not the aggregate service is part of a group.
Status	Lists the current status of the service: • online = available to provide data for consumption by the Broker or Concentrator • offline = not available to provide data for consumption by the Broker or Concentrator • consuming = providing data for consumption by the Broker or Concentrator

System Configuration Section

The System Configuration section manages service configuration for a service. When a service is first added, default values are in effect. You can edit these values to tune performance.



System Configuration

Name	Config Value
Compression	0
Port	50008
SSL FIPS Mode	☑
SSL Port	56008
Stat Update Interval	1000
Threads	20

The System Configuration section has these parameters.

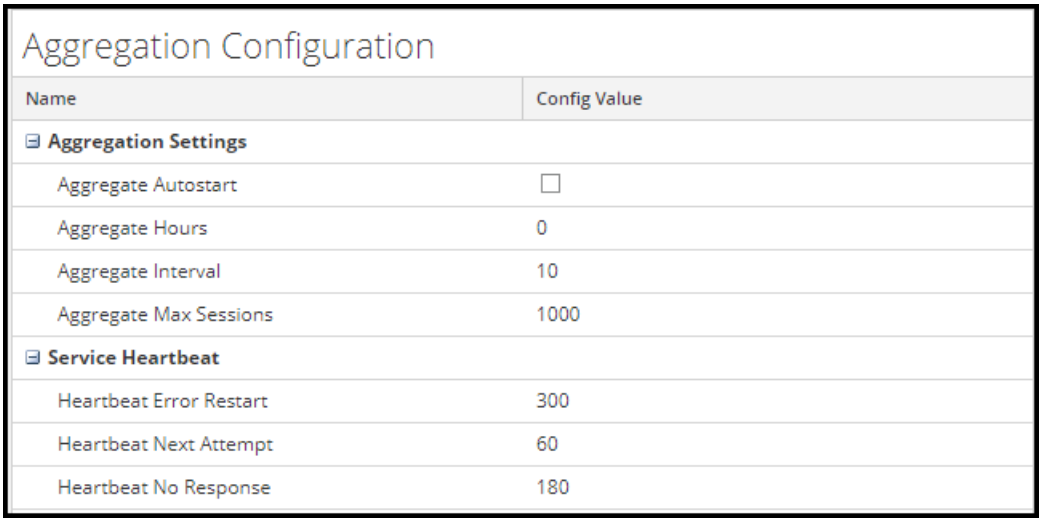
Parameter	Description
Compression	The minimum number of bytes that must be transmitted per response before compression. A setting of **0** disables compression. The default value is **0**. A change in value is effective immediately for all subsequent connections.
Port	The port on which the service listens. The default ports are: • 50001 for Log Collectors • 50002 for Log Decoders • 50003 for Brokers • 50004 for Decoders • 50005 for Concentrators • 50007 for other services
SSL FIPS Mode	When enabled (**on**), the security of data transmission is managed by encrypting information and providing authentication with SSL certificates. The default value is **off**.
SSL Port	Indicates the SSL port.
Stat Update Interval	The number of milliseconds between statistic updates on the system. Lower numbers cause more frequent updates and can slow down other processes. The default value is **1000**. A change in value is effective immediately.

Parameter	Description
Threads	The number of threads in the thread pool to handle incoming requests. A setting of **0** lets the system decide. The default value is **15**. A change takes effect on service restart.

Aggregation Configuration Section

The Aggregation Configuration section provides configuration settings that affect various aspects of the aggregation process. When you click **Apply**, the changes are saved; however, not all settings take effect immediately. The tables for Aggregation Settings and Service Heartbeat provide details.

Caution: Do not edit any of these settings without guidance from Customer Support.

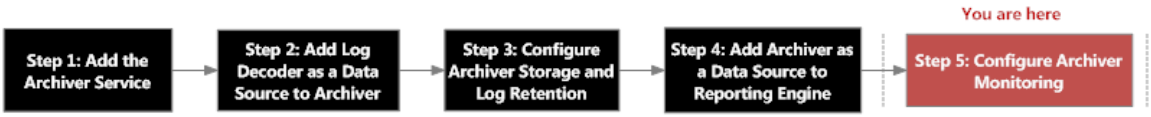


Archiver Service Configuration

This topic lists and describes the available configuration settings for RSA NetWitness Suite Archivers.

Workflow

This workflow illustrates the end-to-end installation and configuration process for an Archiver



What do you want to do?

Role	I want to...	Show me how...
Administrator	Configure Archiver settings.	/archiver/config
Administrator	Configure Database settings.	/database/config
Administrator	Configure Index settings.	/index/config
Administrator	Configure Logs settings.	/logs/config
Administrator	Configure REST settings.	/rest/config
Administrator	Configure SDK settings.	/sdk/config
Administrator	Configure Services settings.	/services/<service name>/config
Administrator	Configure System settings.	/sys/config

Related Topics

- For more information on configuring Database settings, refer to the "Database Configuration Nodes" topic in the *RSA NetWitness Core Database Tuning Guide.)*
- For more information on configuring Index settings, refer to the "Index Configuration Nodes" topic in the *RSA NetWitness Core Database Tuning Guide.*

- For more information on configuring SDK settings, refer to the "SDK Configuration Nodes" topic in the *RSA NetWitness Core Database Tuning Guide*.

Data Retention Tab - Archiver

From the Admin > Services > Config view > Data Retention tab of an Archiver, Administrators can define the criteria for log retention and storage.

Workflow

This workflow illustrates the end-to-end installation and configuration process for an Archiver. From the Data Retention Tab you can configure hot, warm, and cold storage along with configuring multiple storage collections for data retention.

What do you want to do?

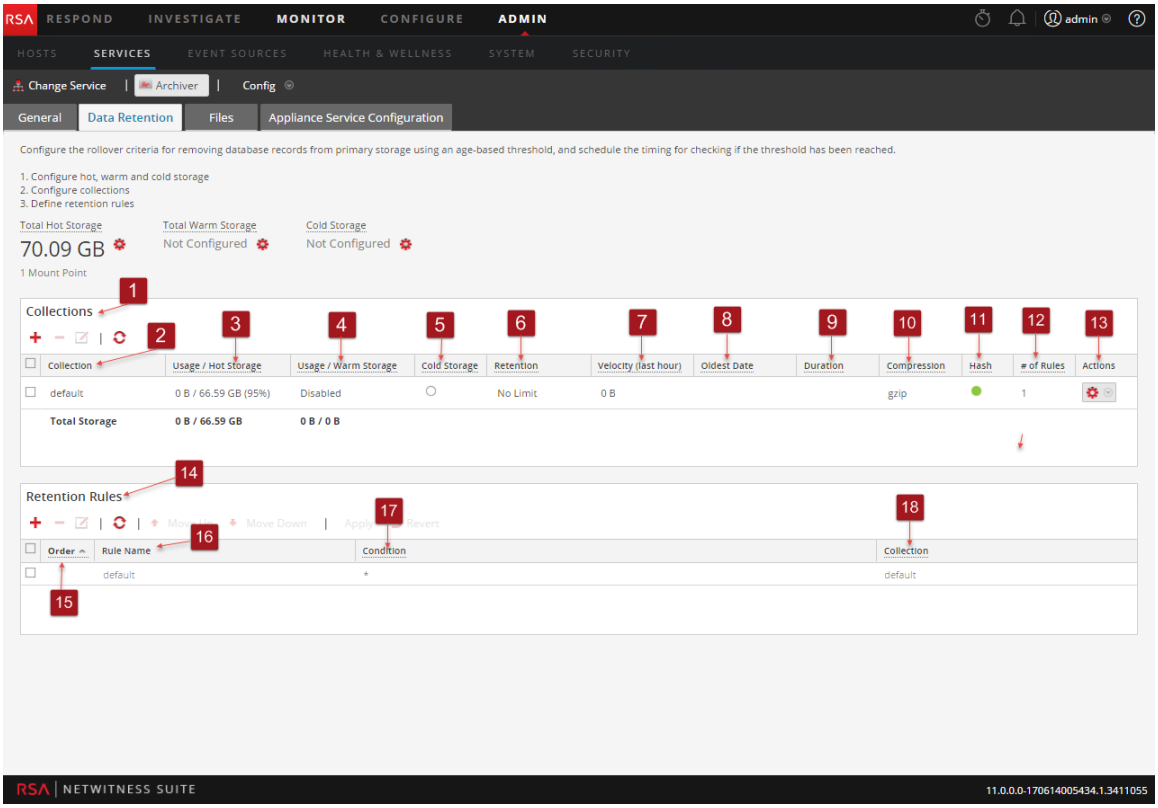
Role	I want to...	Show me how...
Administrator	Configure Total Hot Storage	Configure Hot, Warm, and Cold Storage
Administrator	Configure Total Warm Storage (Optional)	Configure Hot, Warm, and Cold Storage
Administrator	Configure Total Cold Storage (Optional)	Configure Hot, Warm, and Cold Storage
Administrator	Configure Collections	Configure Log Storage Collections
Administrator	Configure Retention Rules	Define Retention Rules

Related Topics

- Configure Hot, Warm, and Cold Storage
- Configure Archiver Storage and Log Retention
- Define Retention Rules

Quick Look

As an Administrator, you can configure hot, warm, and cold storage as well as multiple storage collections with different locations and criteria for retaining logs. For example, you can create a Compliance collection that stores logs for a specific time period as required by government regulations. You can create another collection that stores low value logs in hot storage with a much shorter retention period. The flexibility of these collections enables you to have significantly less overall storage requirements.



1	Displays the Collections panel with the Data Retention tab open.
2	Allows you to sort the collections in ascending or descending order.
3	Displays the allocated hot storage space for the collection, as well as the approximate current usage.
4	Displays the allocated warm storage space for the collection, as well as the approximate current usage.
5	Displays whether the collection uses cold storage for long-term backup.
6	Displays the time range used to determine when data is moved to cold storage or discarded.
7	Displays the amount of data written to the collection during the past hour.

8	Displays the date of the oldest data stored in the collection.
9	Displays the approximate age of the oldest data stored in the collection.
10	Displays the compression type used in collection storage.
11	Displays whether or not hashes are used when storing data in the collection.
12	Displays the number of retention rules that use this collection for storing data.
13	Displays the Actions drop-down menu.
14	Displays the Retention Rules panel.
15	Displays the order in which Retention Rules are evaluated in the execution chain.
16	Displays the name of the Retention Rule.
17	Data that satisfies this condition is stored in the corresponding collection.
18	Displays the collection used to store the data that satisfies this particular rule condition.

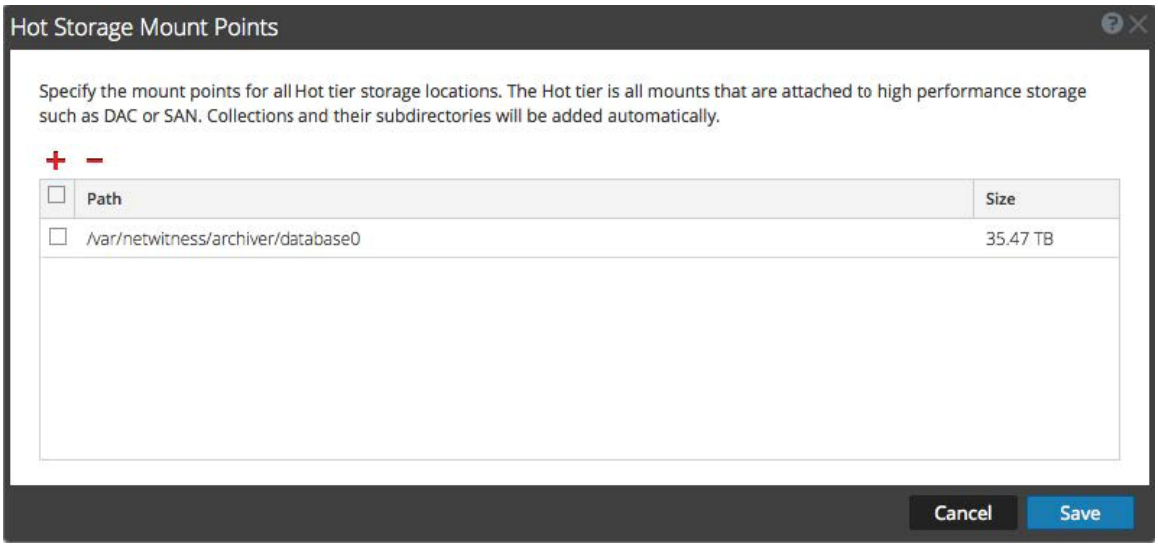
Total Hot, Warm, and Cold Storage

The Total Hot Storage section shows the total amount of Hot storage available and the number of hot storage mount points. The Total Hot Storage section shows the total amount of Warm storage available and the number of warm storage mount points. The Total Cold Storage section shows the total amount of Cold storage and the remaining free space available in Cold storage.

Hot, Warm, and Cold Storage Mount Points Dialogs

In the Hot, Warm, and Cold Storage Mount Points dialogs, you can specify the mount points for your storage locations. You can specify portions of this storage to use for your log storage collections.

To access the Hot, Warm, and Cold Storage Mount Points dialogs, click the icon near the respective section.

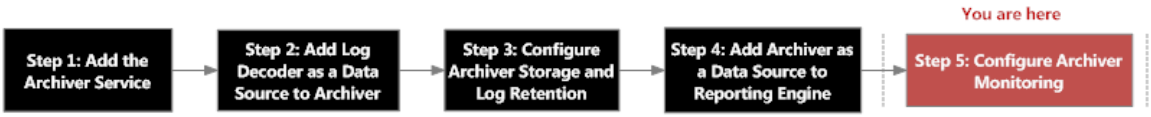

Hot Storage Mount Points
Specify the mount points for all Hot tier storage locations. The Hot tier is all mounts that are attached to high performance storage such as DAC or SAN. Collections and their subdirectories will be added automatically.
Path
Size
/var/netwitness/archiver/database0
35.47 TB
Cancel
Save

Services Config View - Archiver

The Services Config view (ADMIN > Services > select Archiver service and select >View > Config) provides a way to manage basic service configurations, configure aggregate services, configure log retention and storage, edit service configuration files, and configure the appliance service for an Archiver.

Workflow

This workflow illustrates the end-to-end installation and configuration process for an Archiver.



What do you want to do?

Role	I want to...	Show me how...
Administrator	*Add a Log Decoder as an aggregate service.	Click + in the Aggregate Services section.
Administrator	*Remove the selected aggregate service.	Click − in the Aggregate Services section.
Administrator	*Edit Meta Fields and Filter values of the aggregate service.	Click ✎ in the Aggregate Services section. You can specify the type of metadata that the Archiver consumes from this service. You can also specify a rule to filter data that the Archiver consumes from this service.

Role	I want to...	Show me how...
Administrator	*Communicate with the Archiver.	Click Edit Service in the Aggregate Services section. This enables you to enter the administrator credentials of the selected aggregate service so that it can communicate with the Archiver.
Administrator	*Toggle the state of a service between offline and online.	Click Toggle Service in the Aggregate Services section.
Administrator	*Aggregate data using the rules defined for the service.	Click Start Aggregation in the Aggregate Services section. Note that it is necessary to start aggregate service after aggregation has been stopped.
Administrator	*Stop aggregation on the Archiver.	Click Stop Aggregation in the Aggregate Services section. This stops all services and flushes the index, which may take several minutes to complete. It is necessary to stop aggregate services in order to perform various administrative procedures.

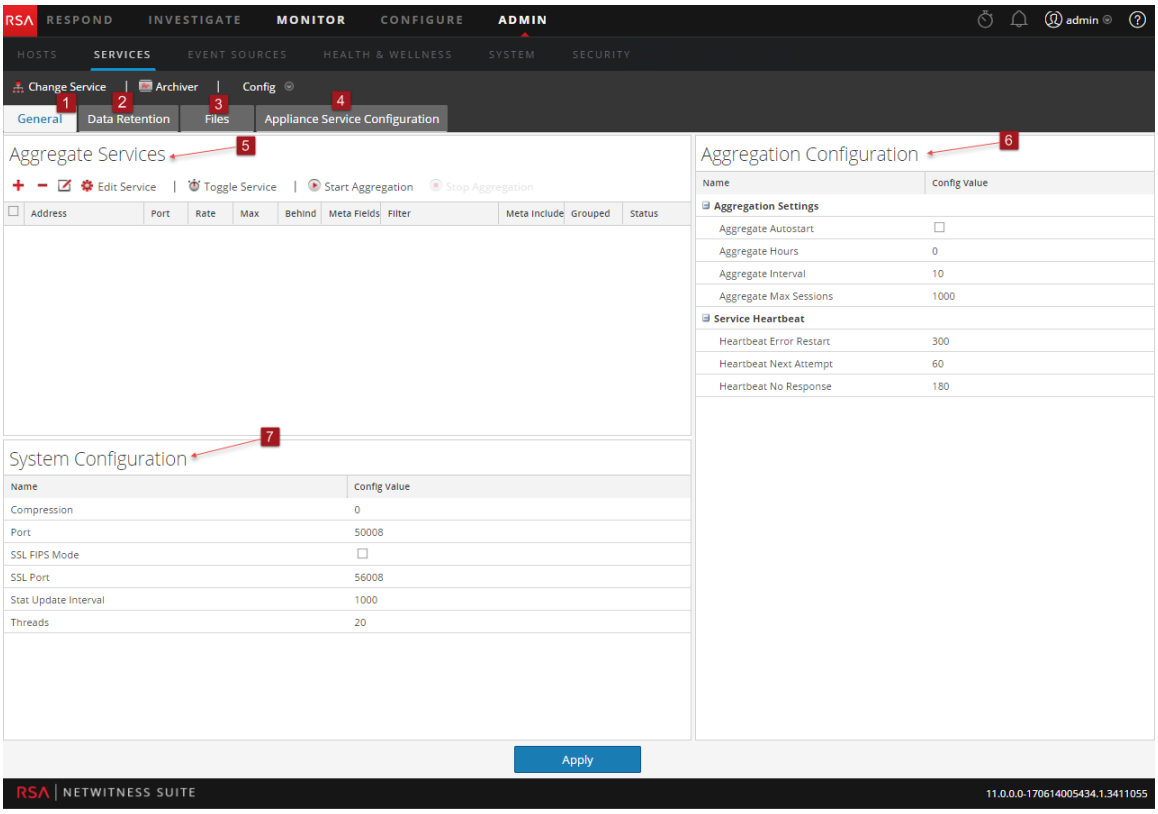
*You can perform this task in the current view.

Related Topics

- Add Log Decoder as a Data Source to Archiver
- Configure Archiver Monitoring
- Configure Log Storage Collections

Quick Look

The Services Config view has four tabs and three panels.



1	General tab provides a way to manage basic Archiver service configuration.
2	Data Retention tab provides a way to view and edit collections and retention rules.
3	Files tab allows you to edit enables you to edit the service configuration files for the Archiver as text files
4	Appliance Service Configuration tab provides a way to configure an Archiver service.
5	Aggregate Services panel provides a way to start and stop aggregation, as well as add, edit, delete, and toggle an aggregate service.
6	Aggregation Configuration panel provides configuration settings that affect various aspects of the aggregation process.
7	System Configuration panel provides a way to manage service configuration for an Archiver service.

General

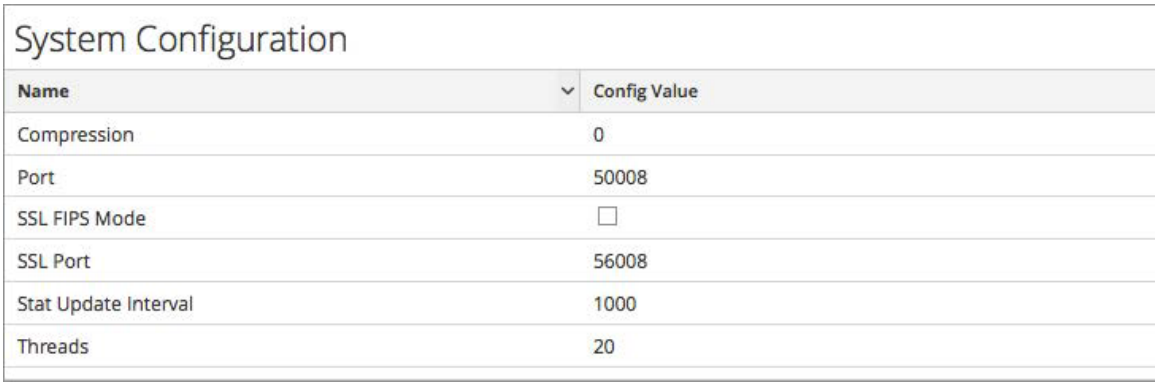
The General tab contains the following sections:

- Aggregate Services
- System Configuration
- Aggregation Configuration

Aggregate Services

The Aggregate Services section provides a way to start and stop aggregation, as well as add, edit, delete, and toggle an aggregate service.

System Configuration

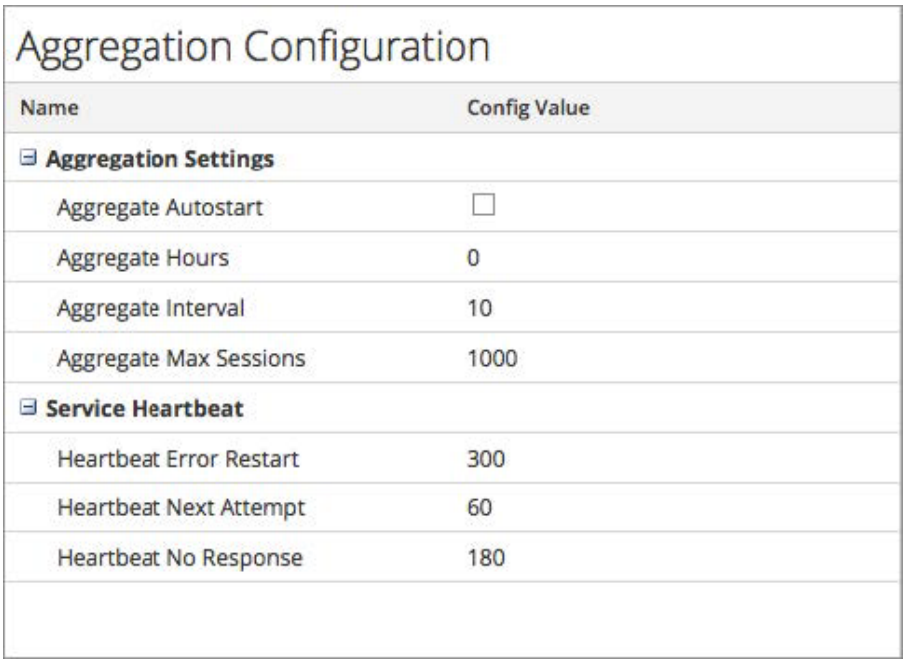


When you add an Archiver service, default values are in effect. RSA designed the default values to accommodate most environments and recommends that you do not edit these values because it may adversely affect performance. The following table describes the System Configuration parameters.

Task	Description
Compression	Determines the minimum amount of bytes before a message is compressed. If set to zero, messages are not compressed.

Task	Description
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.
SSL Port	Indicates the port used for encrypting 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.

Aggregation Configuration



The Aggregation Configuration section contains the following sections:

- Aggregation Settings
- Service Heartbeat

Aggregation Settings

The Aggregations Settings section has the following parameters.

Parameter	Description
Aggregate Autostart	If enabled, data aggregation will automatically restart after a service restart.
Aggregate Hours	Determines the maximum number of hours a service is allowed to start aggregation.
Aggregate Interval	Determines the minimum number of milliseconds before another round of aggregation is requested.
Aggregate Max Sessions	Determines the number of sessions to aggregate on each round.

Service Heartbeat

The Service Heartbeat section has the following parameters.

Parameters	Description
Heartbeat Error Restart	Determines the number of seconds to wait after a service error before attempting a service reconnect.
Heartbeat Next Attempt	Determines the number of seconds to wait before attempting a service reconnect.
Heartbeat No Response	Determines the number of seconds to wait before taking unresponsive service to offline.

Files

The **Files** tab in the Service Config view enables you to edit the service configuration files for the Archiver as text files. The files available to edit vary depending upon the type of service being configured.

The following files are common to all core services:

- Service index file
- NetWitness file
- Crash reporter file
- Scheduler file
- Feed definitions file

For more information on the **Files** tab, see the "Files Tab" topic in the *Host and Services Getting Started Guide*.