RSA NETWITNESS® SUITE

Warehouse Connector構成ガイド

バージョン 11.0

連絡先情報

RSA Link(https://community.rsa.com) では、よくある質問への回答や、既知の問題の解決方法を含むナレッジベースを公開しています。また、製品ドキュメント、コミュニティ ディスカッション、ケース管理なども公開されています。

商標

RSAの商標のリストについては、japan.emc.com/legal/EMC-corporation-trademarks.htm#rsaを参照してください。

使用許諾契約

本ソフトウェアと関連ドキュメントは、EMCが著作権を保有しており、使用許諾契約に従って提供されます。本ソフトウェアと関連ドキュメントの使用と複製は、使用許諾契約の条項に従い、上記の著作権を侵害しない場合のみ許諾されます。本ソフトウェアと関連ドキュメント、およびその複製物を他人に提供することは一切認められません。

本使用許諾契約によって、本ソフトウェアと関連ドキュメントの所有権およびその他の知的財産権が譲渡されることはありません。本ソフトウェアと関連ドキュメントを不正に使用または複製した場合、民事および刑事責任が課せられることがあります。

本ソフトウェアは予告なく変更されることがありますので、あらかじめご承知おきください。

サード パーティ ライセンス

この製品にはRSA以外のサード パーティによって開発されたソフトウェアが含まれます。本製品内のサード パーティ製ソフトウェアに適用される使用許諾契約の内容については、RSA Linkの製品ドキュメント ページで確認できます。本製品を使用することにより、本製品のユーザは、本使用許諾契約の条項に同意したものとみなされます。

暗号技術に関する注意

本製品には、暗号技術が組み込まれています。これらの暗号技術の使用、輸入、輸出は、各国の法律で禁止または制限されています。本製品を使用、輸入、輸出する場合は、各国における使用または輸出入に関する法律に従わなければなりません。

配布

EMC Corporationは、この資料に記載される情報が、発行日時点で正確であるとみなしています。予告なく変更される場合があります。

2月 2018

目次

Warehouse Connectorの仕組み

Warehouse Connectorは、メタやイベントをDecoderおよびLog Decoderから収集して、Hadoopベースの分散コンピューティングシステムにAVRO形式で書き込みます。Warehouse Connectorは、既存のLog DecoderまたはDecoder上のサービスとして設定することができます。

Warehouse Connectorには、次のコンポーネントが含まれます。

- データソース
- 宛先
- データストリーム

データソース

データソースとは、Warehouse Connectorが宛先に格納するデータを収集するサービスです。サポートされるデータソースは、Log DecoderとDecoderのサービスです。Log Decoderはログイベントのみを、Decoderはパケットとメタを収集します。

宛先

宛先は、セキュリティ情報のレポートの収集、管理、有効化を行うためのHadoopベースの分散コンピューティングシステムです。サポートされる宛先は次のとおりです。

- RSA NetWitness Warehouse(MapR) 環境
- HortonWorksデータプラットフォーム
- WebHDFSまたはNFSでマウント可能なHDFSファイルシステムが構成されているHadoopベースの分散コンピューティングシステム
  - 例 : 商用MapR M5 Enterprise Edition for Apache Hadoop

データストリーム

データストリームは、データソースと宛先の論理的な接続です。収集されたデータの異なるサブセットに応じて複数のストリームを使用できます。複数のストリームを設定することで、DecoderとLog Decoderの複数のサービスからのデータを分けて管理できます。複数のデータソースと1つの宛先を使用したストリーム、または1つのデータソースと宛先を使用したストリームを作成できます。

Warehouse Connectorは次を実行します。

- DecoderとLog Decoderからの生のセッション データやログ データを集計する。
- サポートされている宛先(Hadoopベースの環境など) に集計データを転送する。

- スキーマとデータの両方を含む集計データをAVRO形式にシリアライズする。

さらに、Warehouse Connectorは次もサポートします。

メタフィルタ

メタフィルタにより、Warehouseに書き込む必要があるメタキーをフィルタできます。詳細については、「メタフィルタの指定」を参照してください。-

複数値メタキーのサポート

RSA NetWitness Warehouseでは、複数値メタキーがサポートされています。複数値メタキーとは、配列タイプのメタフィールドです。メタキーライブラリを使用して配列タイプのメタフィールドを決定し、正しい配列構文を使ってHIVEクエリを記述することができます。デフォルトでは、次のメタキーは複数値として扱われ、Warehouse Connectorの**/etc/netwitness/ng**にあるファイル**multivalue-bootstrap.xml**で定義されます。

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

チェックサム検証

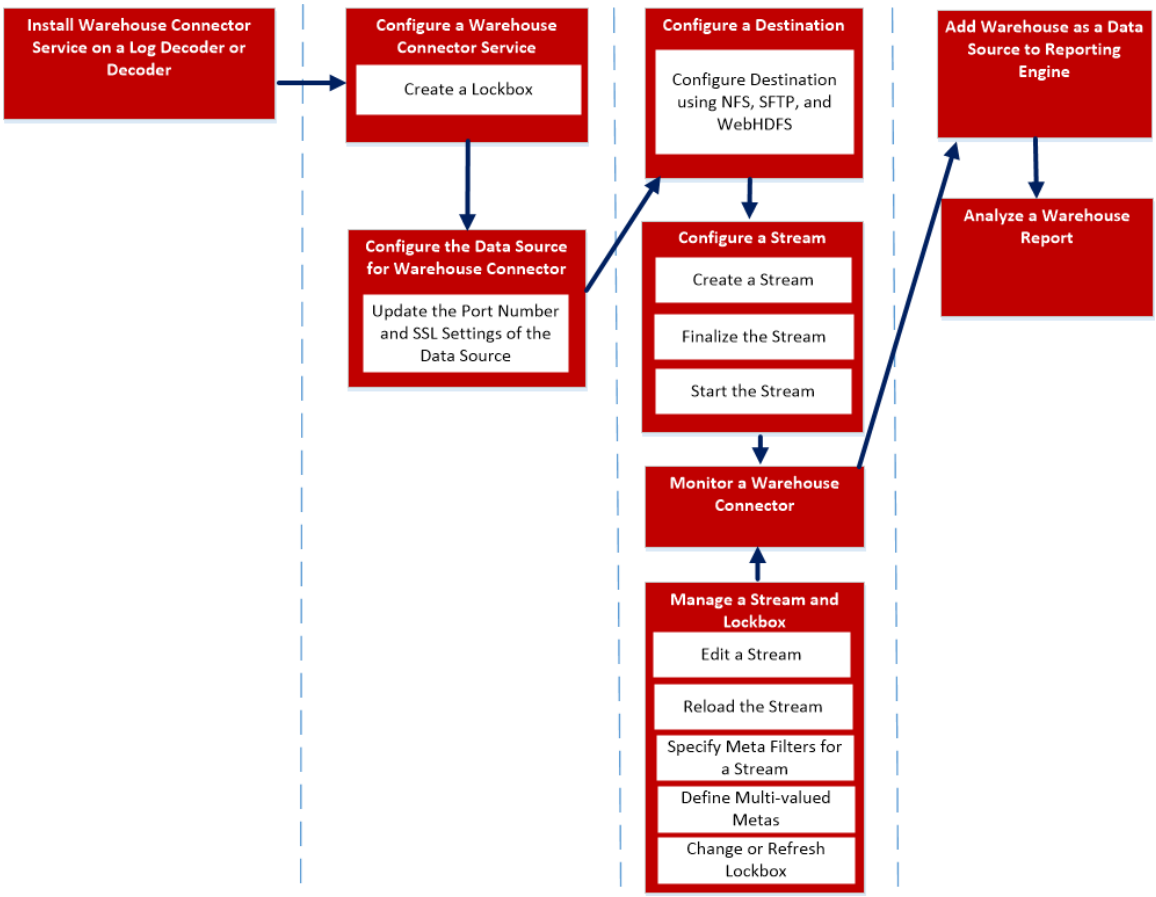
Warehouse Connectorでは、Warehouse Connectorからデータの宛先に転送されるAVROファイルの整合性を検証できます。Warehouse Connectorの構成で、チェックサム検証を有効にする必要があります。

Lockboxのサポート

Lockboxは、Warehouse Connectorが機微データの格納と保護に使用する暗号化ファイルを提供します。Warehouse Connectorを最初に構成するときに、Lockboxのパスワードを指定して、Lockboxを作成する必要があります。

Warehouse Connectorは、既存のLog DecoderまたはDecoderホスト上のサービスとしてWarehouse Connectorを設定することで実装できます。

次に、Log DecoderまたはDecoderでのWarehouse Connectorサービスのインストールと構成、NetWitnessでのWarehouse Connectorサービスの構成、Warehouse Connectorのデータソース、宛先、ストリームの構成、NetWitnessでのアラート通知の構成を行うプロセス全体の概要を示します。



Warehouse Connectorサービスをインストールおよび構成するには、次を実行します。

1. Log DecoderまたはDecoderへのWarehouse Connectorサービスのインストール
2. Warehouse Connectorサービスの構成
3. Warehouse Connectorのデータソースの構成
4. 宛先の構成
5. ストリームの構成
6. Warehouse Connectorの監視
7. Reporting EngineへのWarehouseデータソースの追加
8. Warehouse Reportの分析
9. ストリームとLockboxの管理

Log DecoderまたはDecoderあるいはHybridへのWarehouse Connectorサービスのインストール

Warehouse ConnectorサービスをLog DecoderまたはDecoderあるいはHybridにインストール(新規インストール) するには、次の手順を実行します。

1. Log DecoderまたはDecoderホストにログオンします。
2. NetWitnessサーバで次のコマンドを入力します。

   ```
   warehouse-installer --help
   ```

   コマンド ラインコマンド ライン インタフェース(CLI) の使い方の説明が表示されます。

   注 : 11.0.0.0より後のバージョンに更新されたホストにWarehouse Connectorをインストールする場合は、ホストのバージョンを指定する必要があります。
3. ホストのバージョンを確認するには、次のコマンドを実行します。

   ```
   upgrade-cli-client -list
   ```
4. 次のいずれかのコマンドを実行して、Warehouse Connectorサービスをインストールします。

   ```
   warehouse-installer --host-addr 10.0.0.0 --version 11.0.0.2
   warehouse-installer --host-id 5928b9d8-83be-4143-9602-fa936de5c41e
   warehouse-installer --host-name NW11AdminServer
   ```

   項目の説明 :

   10.0.0.0:ホストのIPアドレス

   11.0.0.2 : ホストのバージョン

   5928b9d8-83be-4143-9602-fa936de5c41e : ホストのID

   NW11AdminServer : ホスト名

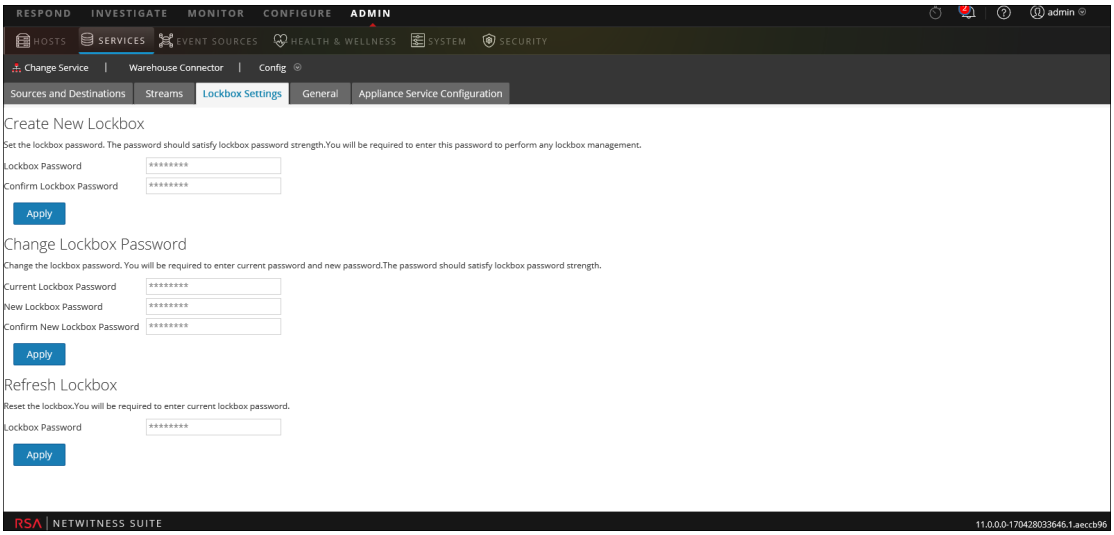
Log DecoderまたはDecoderあるいはHybridにWarehouse Connectorサービスが正常にインストールされます。

Warehouse Connectorサービスの構成

次の手順に従って、Warehouse Connectorサービスを構成できます。

Lockboxのパスワードを設定するには、次の手順を実行します。

1. NetWitnessにログオンします。
2. メイン メニューで、**[管理]＞[サービス]**を選択します。
3. [サービス]ビューで、追加されたWarehouse Connectorサービスを選択して、  **＞[表示]＞[構成]**を選択します。
4. Warehouse Connectorの[サービス]の[構成]ビューで、[**Lockbox設定**]タブをクリックします。



5. [**新しいLockboxの作成**]セクションで、以下の手順に従います。
   a. [**Lockboxのパスワード**]フィールドに、Lockboxの新しいパスワードを入力します。

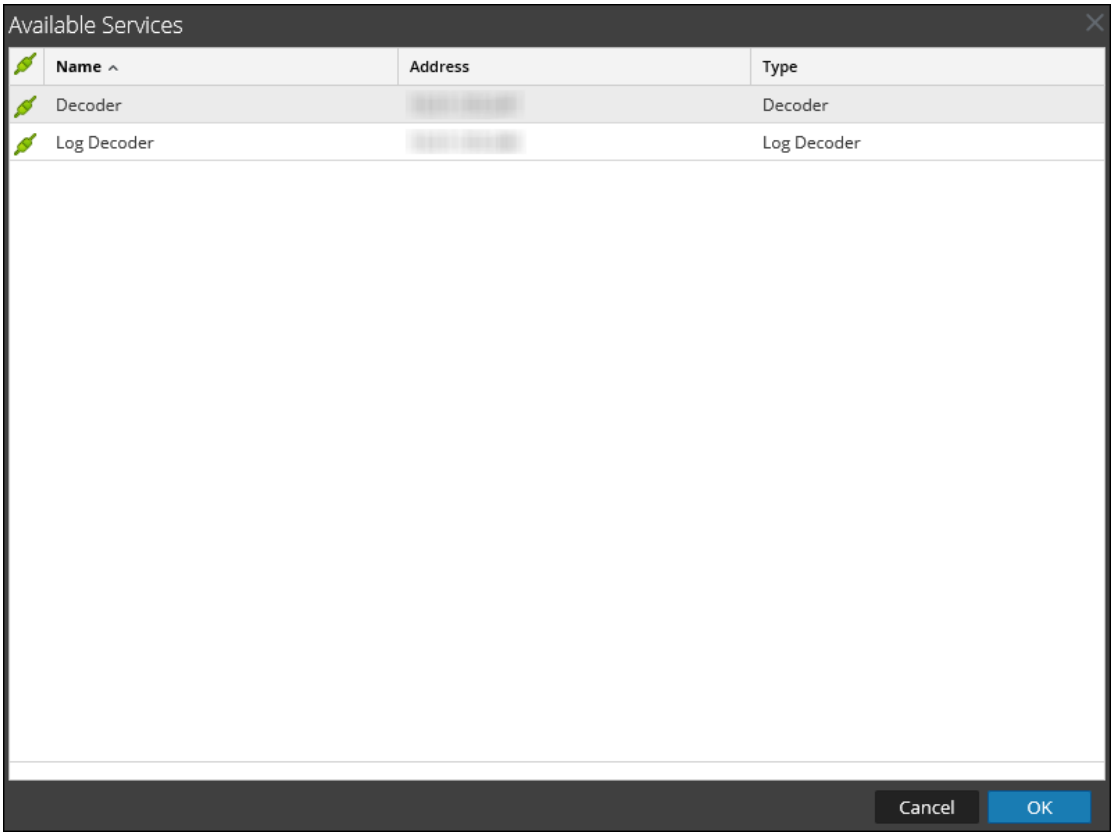
      注：Lockboxのパスワードは、少なくとも8文字の長さを持ち、1つ以上の大文字(A～Z)、1つ以上の小文字(a～z)、1つ以上の数字(0～9)、1つ以上の特殊文字のうち、少なくとも3種類を含む必要があります。

   b. 確認のため、[**Lockboxのパスワードの確認**]フィールドに、追加したLockboxのパスワードを入力します。
   c. **適用**をクリックします。
      Lockboxのパスワードが設定されます。

Warehouse Connectorのデータ ソースの構成

データ ソースを構成するには、次の手順を実行します。

1. NetWitnessにログオンします。
2. メイン メニューで、[**管理**]＞[**サービス**]を選択します。
3. [サービス]ビューで、追加されたWarehouse Connectorサービスを選択して、  ＞[**表示**]＞[**構成**]を選択します。
   Warehouse Connectorサービスの[構成]ビューが表示されます。
4. [**ソースと宛先**]タブの[**ソースの構成**]セクションで、＋をクリックします。



5. [**使用可能なサービス**]ダイアログで、Warehouse Connectorサービスにソースとして追加するLog DecoderまたはDecoderサービスを選択し、[**OK**]をクリックします。
   選択したLog DecoderサービスとDecoderサービスが[**ソースの構成**]セクションに表示されます。

データ ソースのポート番号とSSL設定の更新

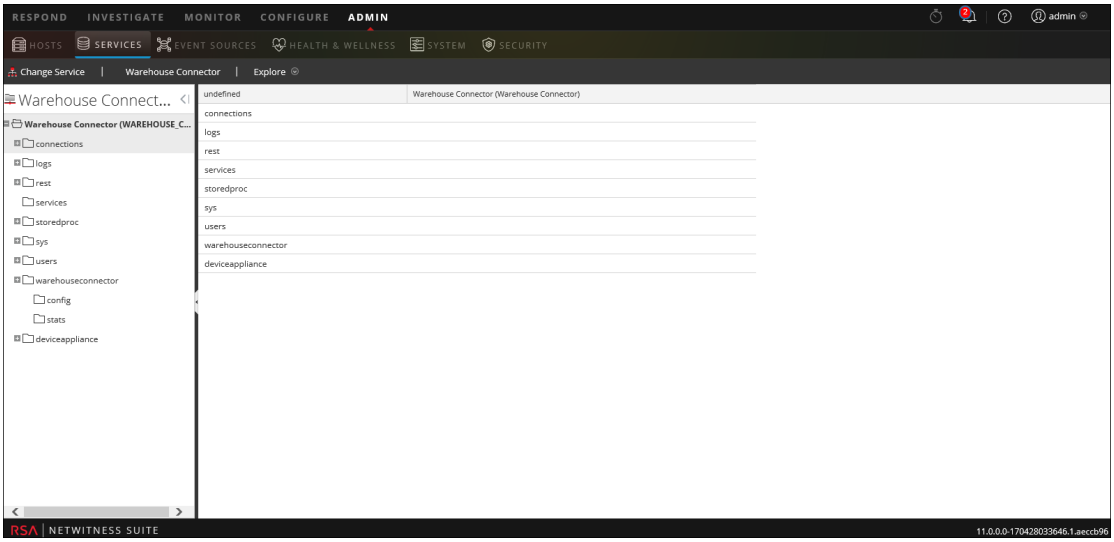
Warehouse Connectorのデータ ソースのポート番号またはSSL設定に変更があった場合、Warehouse Connectorの[エクスプローラ]ビューで、Warehouse Connectorから直接これらの詳細を更新できます。

以下の項目について確認します。

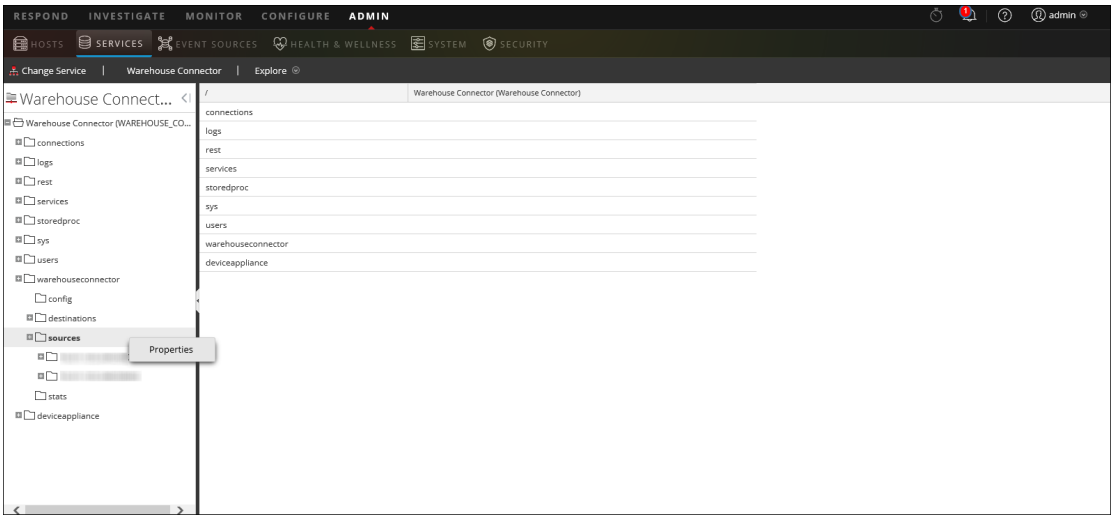
- データ ソースのポート番号またはSSL設定が更新されていること。
- 更新するポート番号またはSSL設定のデータ ソースに関連したストリームを停止すること。

ポート番号またはSSL設定を更新する方法

1. NetWitnessにログオンします。
2. メイン メニューで、**[管理]＞[サービス]**を選択します。
3. [サービス]ビューで、追加されたWarehouse Connectorサービスを選択して、  **＞[表示]＞[エクスプローラ]**を選択します。
   Warehouse Connectorで[サービス]の[エクスプローラ]ビューが表示されます。

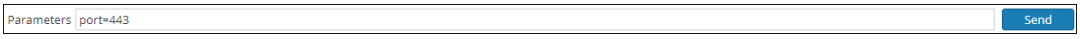


4. **warehouseconnector/sources**に移動し、ソースを右クリックして、[**プロパティ**]をクリックします。
   ソースの[プロパティ]セクションが表示されます。



5. ドロップダウン メニューから、[**update**]を選択します。[パラメータ]フィールドで、次の手順を実行します。

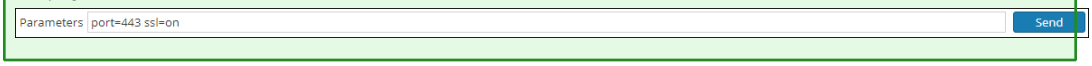
   - ソースのポート番号を更新するには、「`port=<new_source_portnumber>`」を入力して、[**送信**]をクリックします。

   - ソースのSSL設定を更新するには、「`ssl=<new_ssl_settings`」を入力して、[**送信**]をクリックします。

     注：ポート番号とSSL設定を同時に更新するには、パラメータの間にスペースを挿入します。

6. Warehouse Connectorサービスを再開します。
7. ストリームを開始します。

宛先の構成

NFS、SFTP、WebHDFSを使用して宛先を構成することができます。

収集データの書き込み先としてNFSを使用する際にはWarehouse Connectorサービスの宛先を下記の構成にする必要があります。

- RSA NetWitness Warehouse(MapR) 環境
- 商用MapR M5 Enterprise Edition for Apache Hadoop環境

SFTP(Secure File Transfer Protocol) を使用して、リモートの宛先にデータを書き込むようWarehouse Connectorを構成する必要があります。リモートの宛先として、MapRクラスタにNFSNFSマウントさマウントされたリモート サーバ、またはリモート ステージング サーバを使用することができます。

デフォルトでは、Warehouse Connectorはリモートの宛先の次のディレクトリにデータを書き込みます。

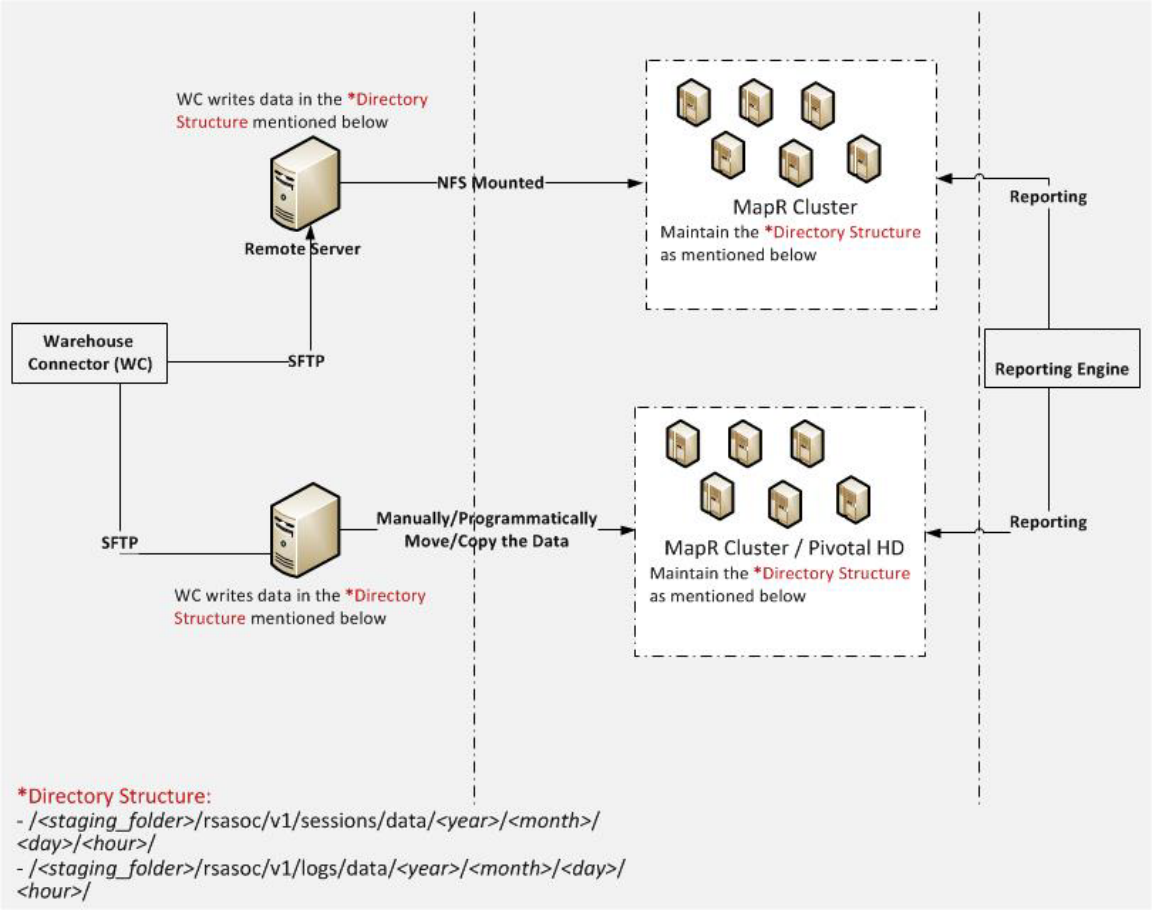
- `/<staging_folder>/rsasoc/v1/sessions/data/<year>/<month>/<day>/<hour>/`
- `/<staging_folder>/rsasoc/v1/logs/data/<year>/<month>/<day>/<hour>/`
  ここで<staging_folder>は、Warehouse Connectorがデータを書き込むリモート サーバのフォルダです。

リモートの宛先としてリモート ステージング サーバを使用している場合は、ディレクトリを次のいずれかの環境に手動でコピーまたは移動する必要があります。

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

Warehouse Connectorが書き込んだデータを使用してレポートを生成するには、Hadoop環境で作成したディレクトリ構造にあわせてWarehouse Connectorでリモートの宛先を指定する必要があります。

次の図では、SFTPを使用して、Warehouse Connectorからリモートの宛先にデータを書き込む方法について説明します。



WebHDFSをサポートするHadoopベースの分散コンピューティングシステムに収集データを書き込むように、Warehouse Connectorサービスを構成する必要があります。

NFSを使用した宛先の構成

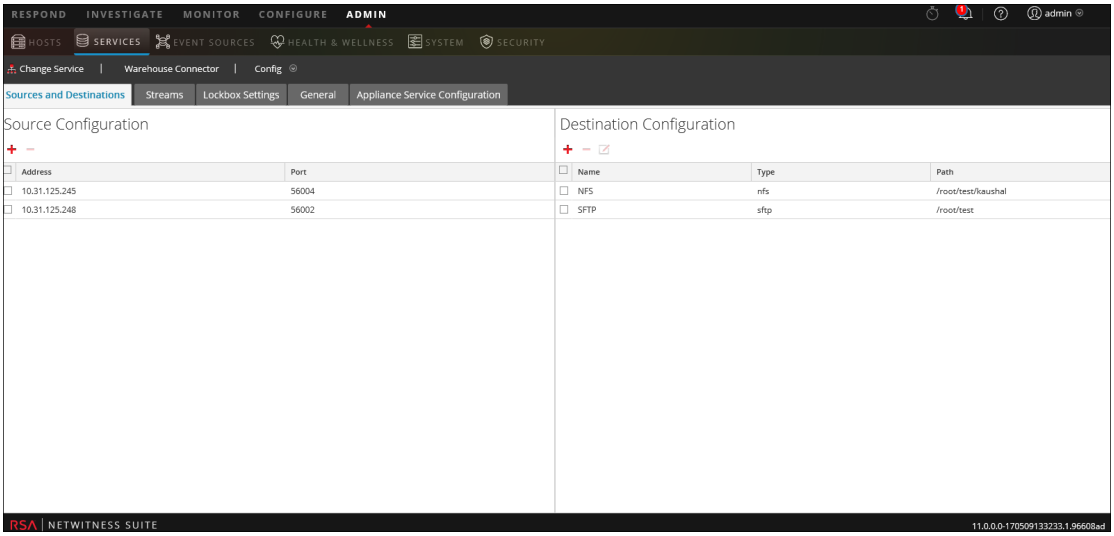
以下の項目について確認します。

- Warehouse Connectorサービスまたは仮想アプライアンスアプライアンスがネットワーク環境にインストールされていること。
- NetWitnessにWarehouse Connectorサービスが追加されている必要があります。詳細については、「*ホストおよびサービス スタート ガイド*」のトピック「ホストへのサービスの追加」を参照してください。
- NFSをWarehouse Connectorで設定します。Warehouse ConnectorにNFSを設定する方法の詳細については、「*Warehouse(MapR) 構成ガイド*」のトピック「Warehouse Connectorでの Warehouseへの書き込みの構成」を参照してください。

NFSを使用して宛先を構成するには、次の手順を実行します。

1. NetWitnessにログオンします。
2. メイン メニューで、**[管理]**>**[サービス]**を選択します。
3. [サービス]ビューで、Warehouse Connectorサービスを選択して、  **>[表示]>[構成]**を選択します。

   Warehouse Connectorの[サービス]の[構成]ビューが表示されます。



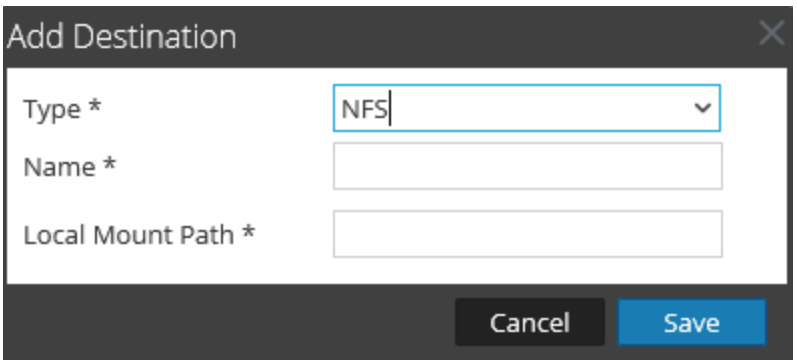
4. [**ソースと宛先**]タブの[**宛先の構成**]セクションで、**+**をクリックします。
5. [**宛先の追加**]ダイアログで、[**タイプ**]ドロップダウン リストから[**NFS**]を選択します。
6. [**名前**]フィールドに、宛先の一意のシンボリック名を入力します。

注 : [**名前**]フィールドでは、アンダースコア(_) を除く特殊文字やスペースはサポートされません。

7. Warehouse Connectorのデータの書き込み先として、ローカルにマウントされたHDFSのディレクトリを[**ローカル マウント パス**]フィールドに入力します。

   次に例を挙げます。
   HDFSのローカル マウント ポイントとして**/saw**が構成されている環境で、RSA NetWitness Warehouse(MapR) に書き込むためにWarehouse Connectorサービスをインストールしたホストにmapr NFSクラスタがマウントされている場合、**/saw**配下に**Ionsaw01**という名前のディレクトリに作成します。これに対応する宛先のローカル マウント パスは**/saw/Ionsaw01**になります。

   詳細については、「*Warehouse(MapR) 構成ガイド*」のトピック「**Warehouse Connectorへの Warehouseのマウント**」を参照してください。



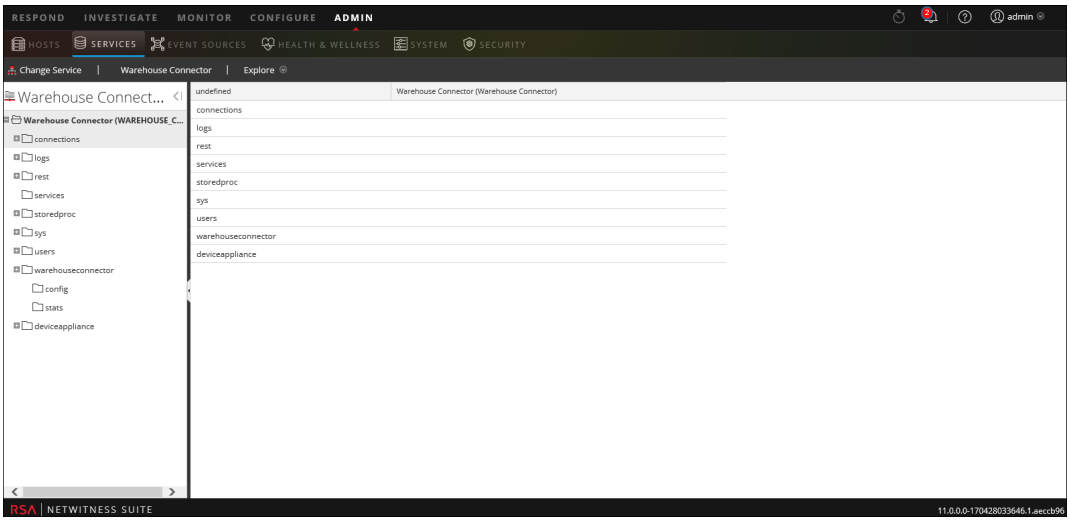
   /sawマウント ポイントは、HDFSのルート パスとして/に対応します。Warehouse Connectorは、HDFSの**/Ionsaw01**にデータを書き込みます。

8. [**保存**]をクリックします。

9. (オプション) チェックサム検証を有効にする場合は、次の手順を実行します。

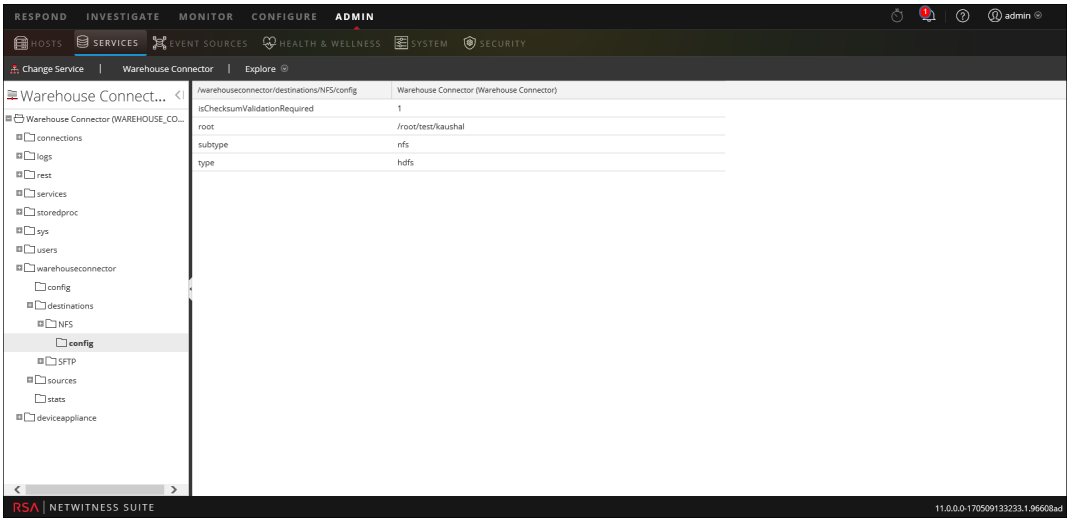
   a. メイン メニューで、[**管理**]＞[**サービス**]を選択します。

   b. [サービス]ビューで、追加されたWarehouse Connectorサービスを選択して、  ＞[**表示**]＞[**エクスプローラ**]を選択します。
      Warehouse Connectorの[エクスプローラ]ビューが表示されます。



c. [オプション]パネルで、**warehouseconnector/destinations/nfs/config**に移動します。

d. パラメータ`isChecksumValidationRequired`を**1**に設定します。



e. ストリームが構成されている場合には、再開します。

SFTPを使用した宛先の構成

以下の項目について確認します。

- Warehouse Connectorサービスまたは仮想アプライアンスアプライアンスがネットワーク環境にインストールされていること。
- NetWitnessにWarehouse Connectorサービスが追加されている必要があります。詳細については、「*ホストおよびサービス スタート ガイド*」のトピック「ホストへのサービスの追加」を参照してください。
- SFTPの宛先タイプを設定する場合、Warehouse Connectorのsshサービス(たとえばsshd) が使用する**/root/.ssh/known_hosts**ファイルに宛先ホストが含まれている必要があります。

Warehouse Connectorホストから宛先を追加

宛先ホストを**/root/.ssh/known_hosts**ファイルに追加するには、Warehouse Connectorホストから、宛先ホストへのセキュアな接続を開始します。

1. Warehouse Connectorにログインします。
2. `ssh root@<SAWIP>`または`ssh username@<SAWIP>`と入力します。
3. [**Yes**]を選択し、パスワードを入力します。
4. **/root/.ssh/known_hosts**ファイルにホスト キーを追加します。

注 : Warehouse Connectorを11.0にアップグレードした環境では、Warehouse Connector上のsshサービス(sshd) が使用する/root/.ssh/known_hostsファイルに宛先ホストが含まれていることを確認します。この手順を実行しないと、Warehouse ConnectorでSFTPを使用して構成されたストリームが開始されません。

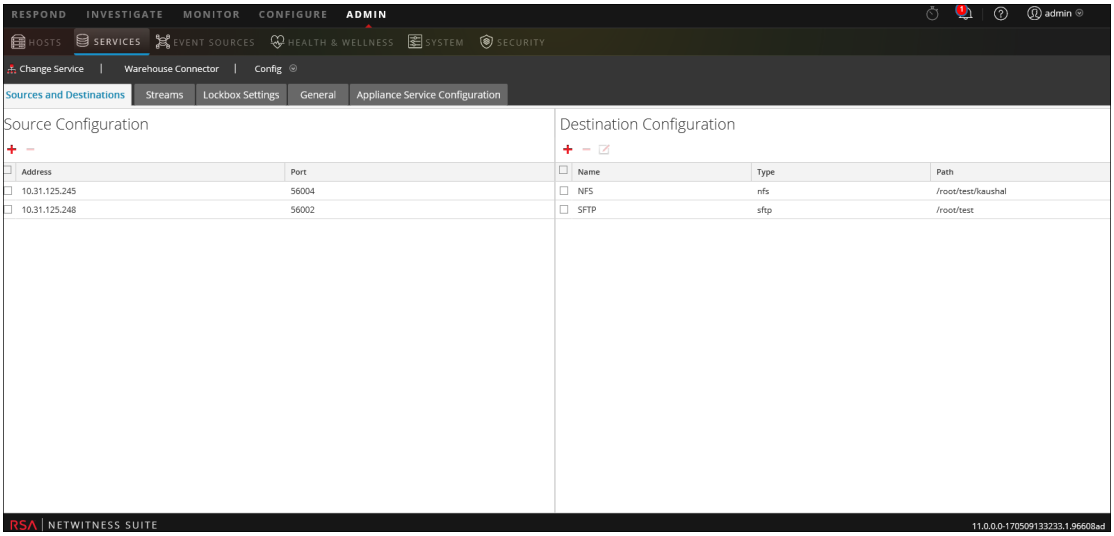
- SFTPを使用し、SSHキー ベースのアクセスで宛先にデータを書き込むには、Warehouse ConnectorとWarehouseホスト(またはHadoopノード) 間にSSHキー ベースのアクセスを構成する必要があります。詳細については、以下の「**SSHキーの構成**」を参照してください。

注 : Warehouse Connectorから宛先に転送されるAVROファイルの整合性を検証するチェックサム検証を有効化する場合は、パスフレーズを設定せずにキーを生成し、Warehouse ConnectorとWarehouseノード間でキーを交換する必要があります。

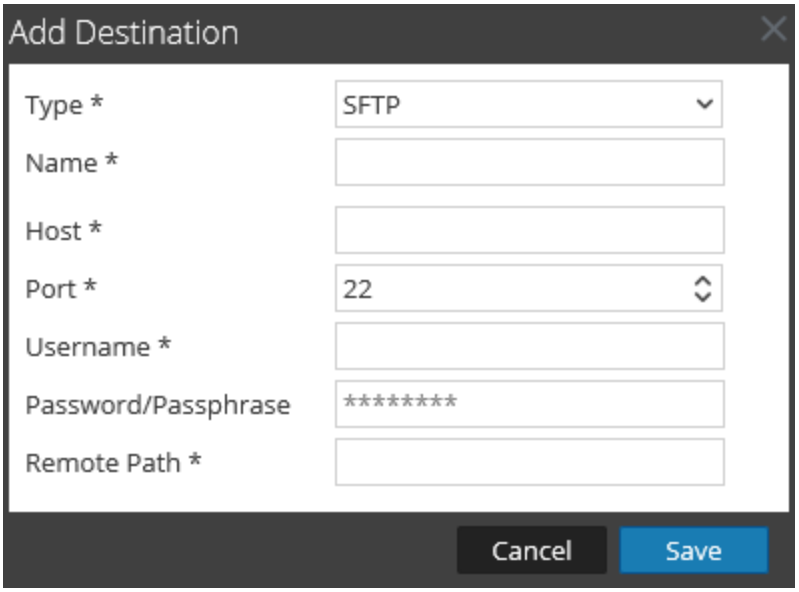
Warehouse Connectorでのリモートの宛先への書き込みの構成

宛先を構成する方法

1. NetWitnessにログオンします
2. メイン メニューで、**[管理]＞[サービス]**を選択します。
3. [サービス]ビューで、追加されたWarehouse Connectorサービスを選択して、  **＞[表示]＞[構成]**を選択します。
   Warehouse Connectorの[サービス]の[構成]ビューが表示されます。



4. **[ソースと宛先]**タブの**[宛先の構成]**セクションで、＋をクリックします。
5. **[宛先の追加]**ダイアログで、**[タイプ]**ドロップダウン リストから**[SFTP]**を選択します。



6. [**名前**]フィールドに、宛先の一意のシンボリック名を入力します。

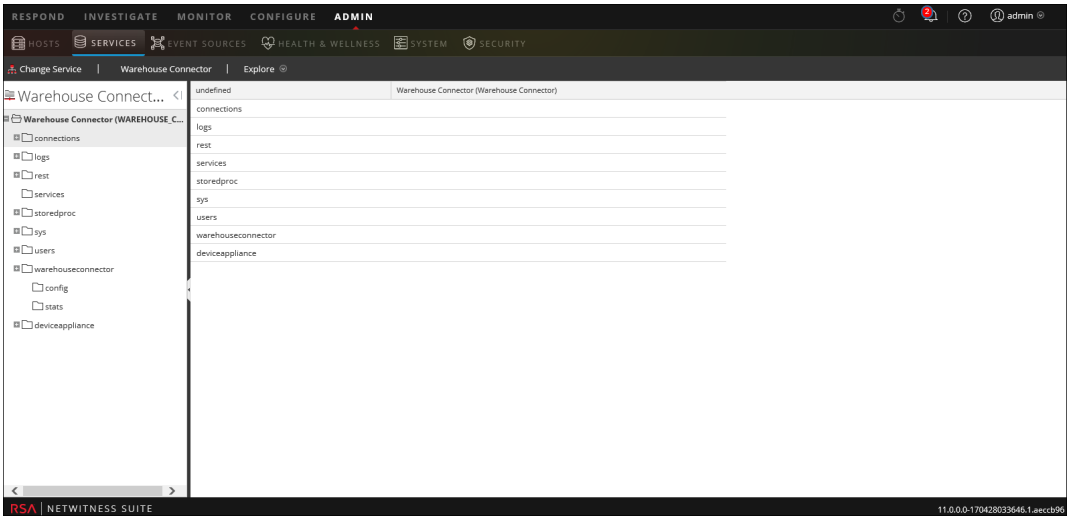
   注:[**名前**]フィールドでは、アンダースコア(_)を除く特殊文字やスペースはサポートされません。

7. [**ホスト**]フィールドに、リモート サーバのIPアドレスを入力します。
8. [**ポート**]フィールドでは、デフォルトのポート22を保持します。
9. [**ユーザ名**]フィールドに、SSHのユーザ名を入力します。

   注:HortonWorks HDの場合、ユーザ名はgpadminであり、パスワード ベースのアクセスの場合はgpadminのパスワードを使用する必要があります。パスフレーズ ベースのアクセスの場合は、gpadminユーザ用のキーの生成に使用するパスフレーズを使用する必要があります。

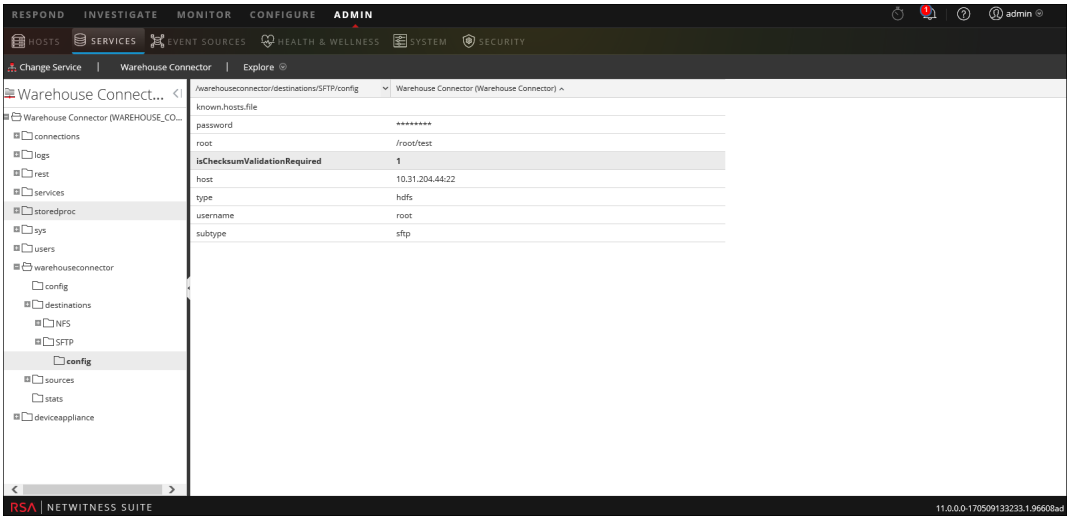
10. [**パスワード/パスフレーズ**]フィールドに、次のいずれかを入力します。
    - SSHパスワード:SFTPを使用し、パスワード ベースのアクセスによって宛先にデータを書き込む場合。
    - SSHパスフレーズ:SFTPを使用し、SSHキー ベースのアクセスによって宛先にデータを書き込む場合)。
11. [**リモート パス**]フィールドに、SFTPサーバ上に存在するディレクトリのパスを入力します。
12. [**保存**]をクリックします。
13. (オプション) チェックサム検証を有効にする場合は、次の手順を実行します。
    a. メイン メニューで、[**管理**]>[**サービス**]を選択します。
    b. [サービス]ビューで、追加されたWarehouse Connectorサービスを選択して、  >[**表示**]>[**エクスプローラ**]を選択します。

Warehouse Connectorの[エクスプローラ]ビューが表示されます。



c. [オプション]パネルで、**warehouseconnector/destinations/sftp/config**に移動します。

d. パラメータ`isChecksumValidationRequired`を**1**に設定します。



e. ストリームが構成されている場合には、再開します。

SSHキーの構成

Warehouse ConnectorとWarehouseホスト(またはHadoopノード)間にSSHキーベースのアクセスを構成するには、次の手順に従います。

1. Warehouse Connector上のデフォルトの場所にSSHキーを生成します。次の手順を実行します。

   a. Warehouse Connectorにログインします。

   b. 次のコマンドを入力し、Enterキーを押します。

```
$ OWB_FORCE_FIPS_MODE_OFF=1 ssh-keygen -t dsa
```

c. 生成されたキーの保存先となるファイルを入力するように求められます。

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

d. キーを保存するファイルを入力して、ENTERキーを押します。

コマンド プロンプトが表示されて、パスフレーズを入力して確認するよう求められます。

注：チェックサム検証と呼ばれる機能を有効にして、Warehouse Connectorから宛先に転送されるAVROファイルの検証を行う場合、**パスフレーズ**を設定しないようにします。次のステップe、f、g、hは実行しません。

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

公開キーが生成され、指定した場所に保存されます。

e. 次のコマンドを入力して、ディレクトリを変更します。

```
cd /root/.ssh/
```

f. 生成されたキーを次の場所に移します。

```
mv id_dsa id_dsa.old
```

g. 次のコマンドを入力し、Enterキーを押します。

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

コマンド プロンプトが表示されて、パスフレーズを入力して確認するよう求められます。

h. 暗号化パスフレーズを入力します。

i. 次のコマンドを使用してファイル権限を変更します。

```
chmod 600 id_dsa
```

2. 生成された公開鍵を、リモートのWarehouseホストか、Hadoopノードの次の場所にあるauthorized keys listに追加します：`~/.ssh/authorized_keys`

注：公開鍵をHadoopノードにコピーします。公開鍵をコピーするときは、追加するWebHDFSの宛先に関する情報を使用して、ユーザのログイン詳細を提供します。

Warehouse ConnectorとWarehouseノードまたはHadoopノードとの間でセキュアな通信が確立されます。

WebHDFSを使用した宛先の構成

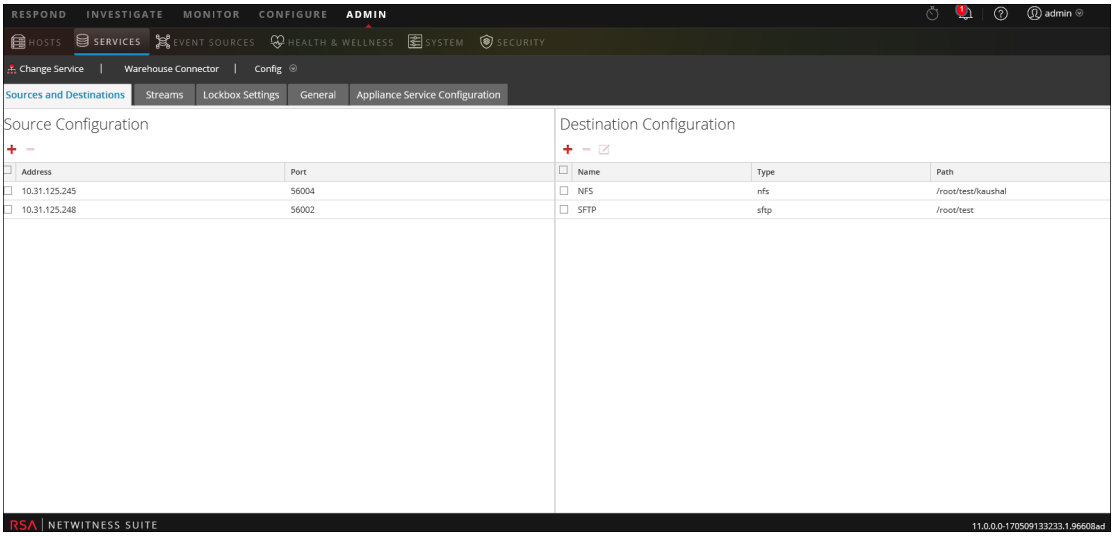
以下の項目について確認します。

- Warehouse Connectorサービスまたは仮想アプライアンスアプライアンスがネットワーク環境にインストールされていること。
- NetWitnessにWarehouse Connectorサービスが追加されている必要があります。詳細については、「*ホストおよびサービス スタート ガイド*」のトピック「ホストへのサービスの追加」を参照してください。
- WarehouseノードとWarehouse Connectorのホスト名(または完全修飾ドメイン名)とIPアドレスがDNSサーバに追加されていることを確認します。DNSサーバが構成されていない場合は、WarehouseノードとWarehouse Connectorのホスト名(または完全修飾ドメイン名)とIPアドレスを、Warehouse Connectorサービスがインストールされているホストのファイルに追加します。
- Warehouse ConnectorとWarehouseクラスタとの間にKerberos認証が必要な場合、次を実行します。
  - Kerberosキー配布センター(KDC)サーバがネットワーク環境で構成済みで、Kerberos KeytabファイルがWarehouse Connectorをインストールしたホストにコピーされていることを確認します。
  - Kerberos認証がWarehouseクラスターで有効になっていることを確認します。
- Warehouse Connectorから宛先に転送されるAVROファイルの整合性を検証するためにチェックサム検証を有効にする場合、パスフレーズを設定せずにキーを生成し、Warehouse ConnectorとWarehouseノードとの間でキーの交換を行います。Warehouse ConnectorとWarehouseホスト(またはHadoopノード)間にSSHキーベースのアクセスを構成する必要があります。詳細については、「SFTPを使用した宛先の構成」の「SSHキーの構成」を参照してください。

Warehouse Connectorでのリモートの宛先への書き込みの構成

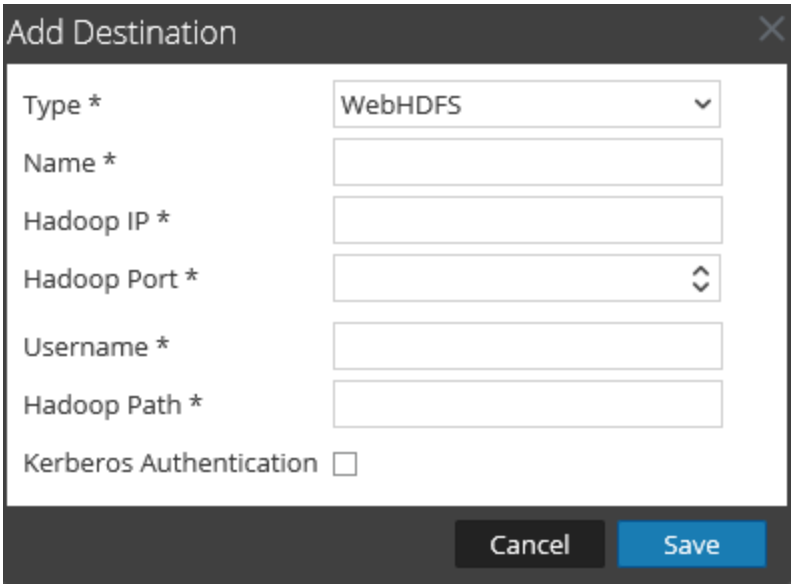
宛先を構成する方法

1. NetWitnessにログオンします。
2. メイン メニューで、**[管理]＞[サービス]**を選択します。
3. [サービス]ビューで、追加されたWarehouse Connectorサービスを選択して、  **＞[表示]＞[構成]**を選択します。
   Warehouse Connectorの[サービス]の[構成]ビューが表示されます。



4. **[ソースと宛先]**タブの[**宛先の構成**]セクションで、＋をクリックします。

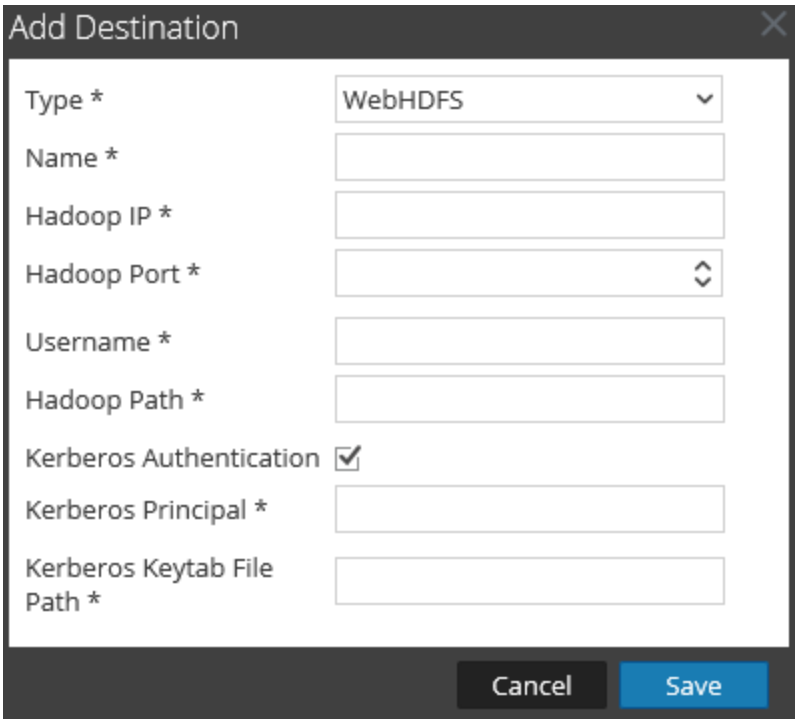
5. [**宛先の追加**]ダイアログで、ドロップダウンリストから[**WebHDFS**]を選択します。



6. [**名前**]フィールドに、宛先の一意のシンボリック名を入力します。

   注:[**名前**]フィールドでは、アンダースコア(_)を除く特殊文字やスペースはサポートされません。

7. [**Hadoop IP**]フィールドに、WarehouseクラスタのNameNode IPアドレスを入力します。
8. [**Hadoopポート**]フィールドに、NameNode Webユーザインタフェースで使用するベースポートを入力します。
9. [**ユーザ名**]フィールドに、Warehouse Connectorのデータ書き込み先となるWarehouseのディレクトリの所有者を入力します。
10. [**Hadoopパス**]フィールドに、Warehouse Connectorのデータ書き込み先となるWarehouseのディレクトリのパスを入力します。
11. Warehouse ConnectorがKerberos認証を使って安全にWarehouseと通信するには、[**Kerberos認証**]チェックボックスをオンにします。



次の手順を実行します。

a. [**Kerberosプリンシパル**]フィールドで、Kerberos認証に使用されるKDCプリンシパルを入力します。

b. [**Kerberosキータブ ファイル パス**]フィールドで、Warehouse ConnectorのKerberos キータブ ファイルのパスを入力します。

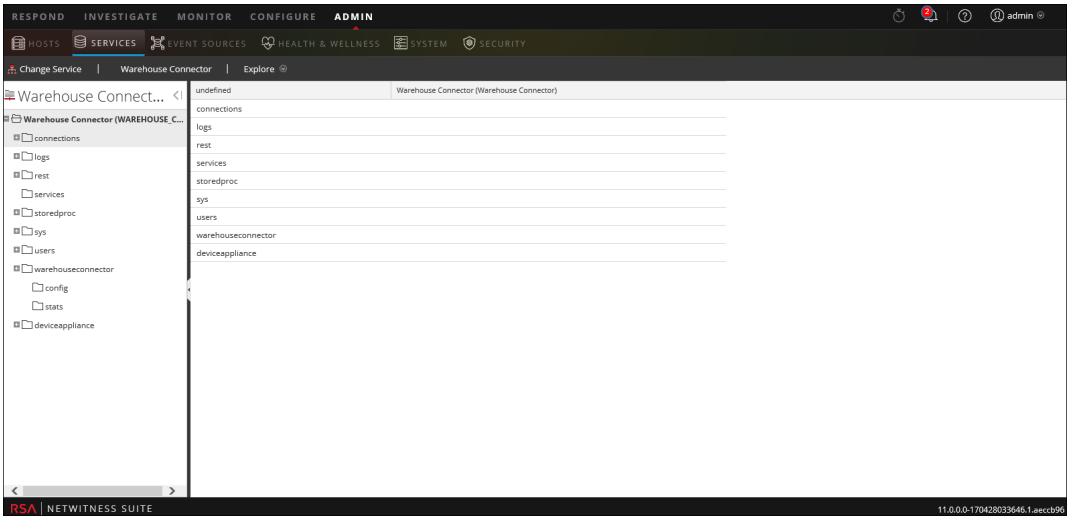
12. [**保存**]をクリックします。

13. (オプション) チェックサム検証を有効にする場合は、次の手順を実行します。

a. メイン メニューで、[**管理**]>[**サービス**]を選択します。

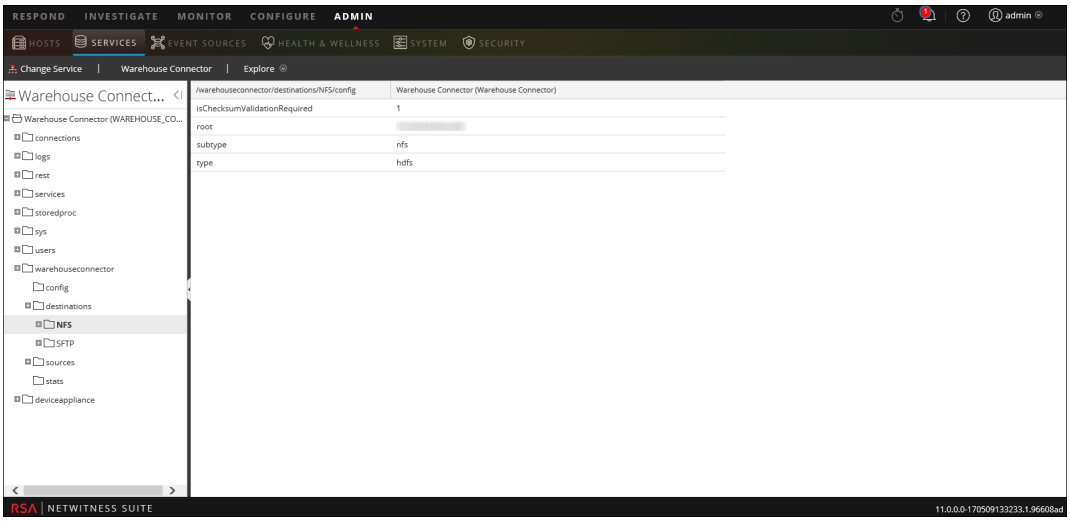
b. [サービス]ビューで、追加されたWarehouse Connectorサービスを選択して、  >[**表示**]>[**エクスプローラ**]を選択します。

Warehouse Connectorの[エクスプローラ]ビューが表示されます。



c. [オプション]パネルで、**warehouseconnector/destinations/webhdfs/config**に移動します。

d. パラメータ`isChecksumValidationRequired`を**1**に設定します。



e. ストリームが構成されている場合には、再開します。

ストリームの構成

データストリームの構成で、データソースと宛先の組み合わせを定義できます。

以下の項目について確認します。

- Warehouse Connectorサービスまたは仮想アプライアンスアプライアンスがネットワーク環境にインストールされていること。
- NetWitnessにWarehouse Connectorサービスが追加されている必要があります。詳細については、「*ホストおよびサービス スタート ガイド*」の「ホストへのサービスの追加」を参照してください。
- Warehouse Connectorサービスがデータの収集元として使用するデータソースを構成済みであること。詳細については、「Warehouse Connectorのデータソースの構成」を参照してください。
- 収集データの書き込み先としてWarehouse Connectorサービスが使用する宛先を構成済みであること。詳細については、「宛先の構成」を参照してください。

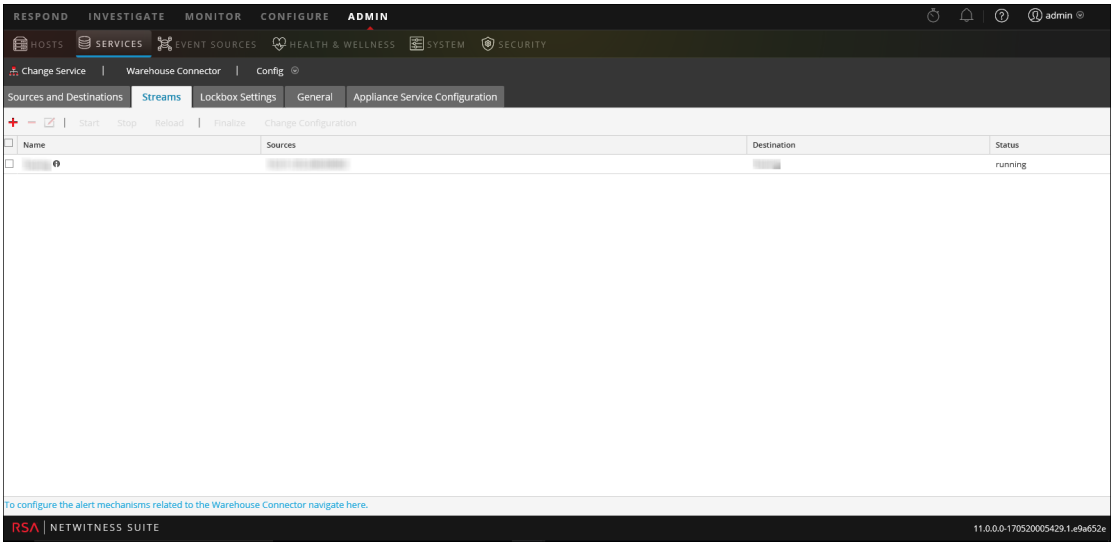
ストリームを構成するには、次の手順を実行します。

1. ストリームの作成
2. ストリームのファイナライズ
3. ストリームの開始

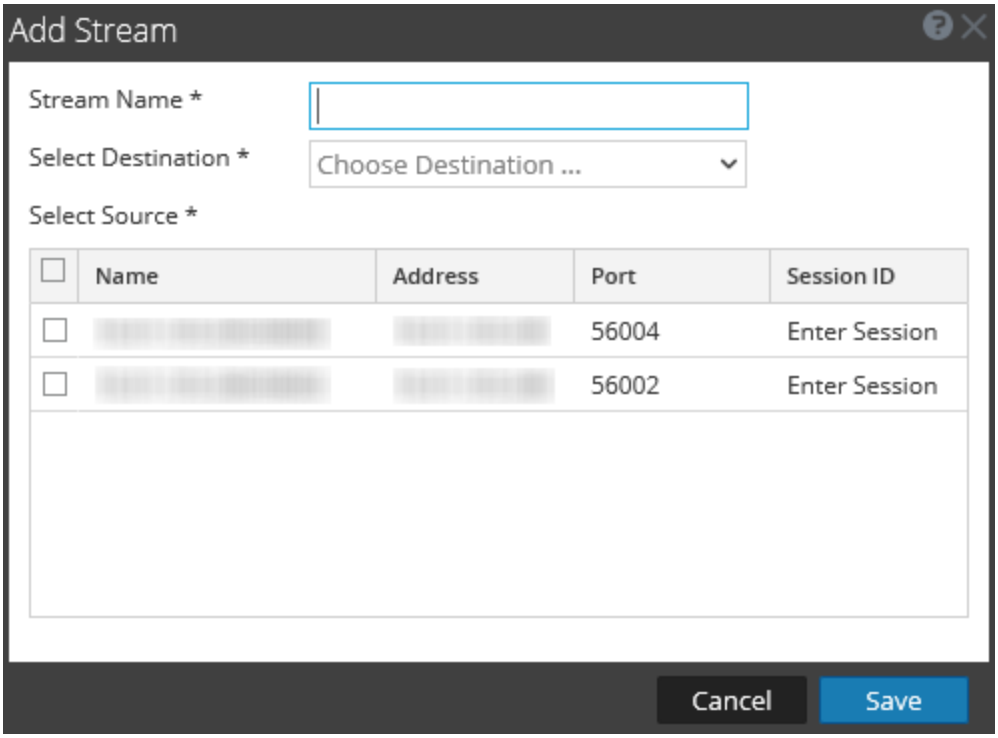
ストリームの作成

ストリームを作成するには、次の手順を実行します。

1. メイン メニューで、[**管理**]＞[**サービス**]を選択します。
2. [サービス]ビューで、追加されたWarehouse Connectorサービスを選択して、  ＞[**表示**]＞[**構成**]を選択します。
   Warehouse Connectorの[サービス]の[構成]ビューが表示されます。
3. [**ストリーム**]タブをクリックします。



4. [**ストリーム**]タブで、➕をクリックします。



5. [**ストリームの追加**]ダイアログで、以下の手順に従います。

   a. [**ストリーム名**]フィールドに、ストリームの名前を入力します。

   > **注**：[**ストリーム名**]フィールドでは、アンダースコア(_)を除くスペースや特殊文字はサポートされません。

   b. [**宛先の選択**]ドロップダウンメニューで、Warehouse Connectorに追加されている宛先のリストから宛先を選択します。

   c. [**ソースの選択**]フィールドで、表示されたソースのリストから目的のソースを設定します。

   d. [**セッションID**]列に、最終セッションIDを入力します。
   セッションIDを指定した場合は、そのセッションから集計が開始されます。セッションIDを空白のままにした場合は、現在のセッションから集計が開始されます。

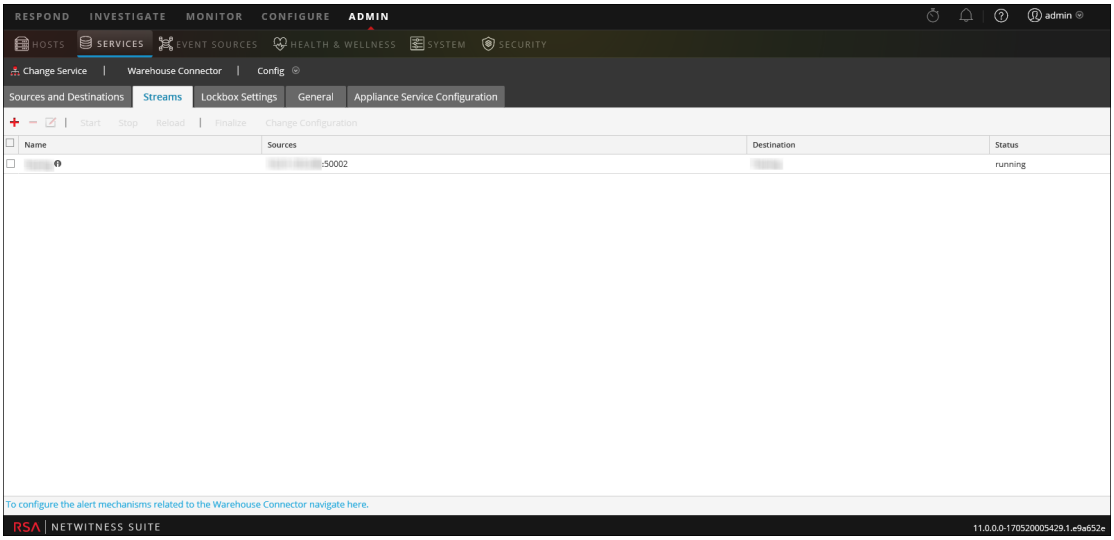
   e. [**保存**]をクリックします。

ストリームのファイナライズ

ストリームがすでに作成済みであること。

ストリームをファイナライズする方法

1. メイン メニューで、[**管理**]＞[**サービス**]を選択します。
2. [サービス]ビューで、追加されたWarehouse Connectorサービスを選択して、  ＞[**表示**]＞[**構成**]を選択します。
   Warehouse Connectorの[サービス]の[構成]ビューが表示されます。
3. [**ストリーム**]タブで、作成したストリームを選択します。



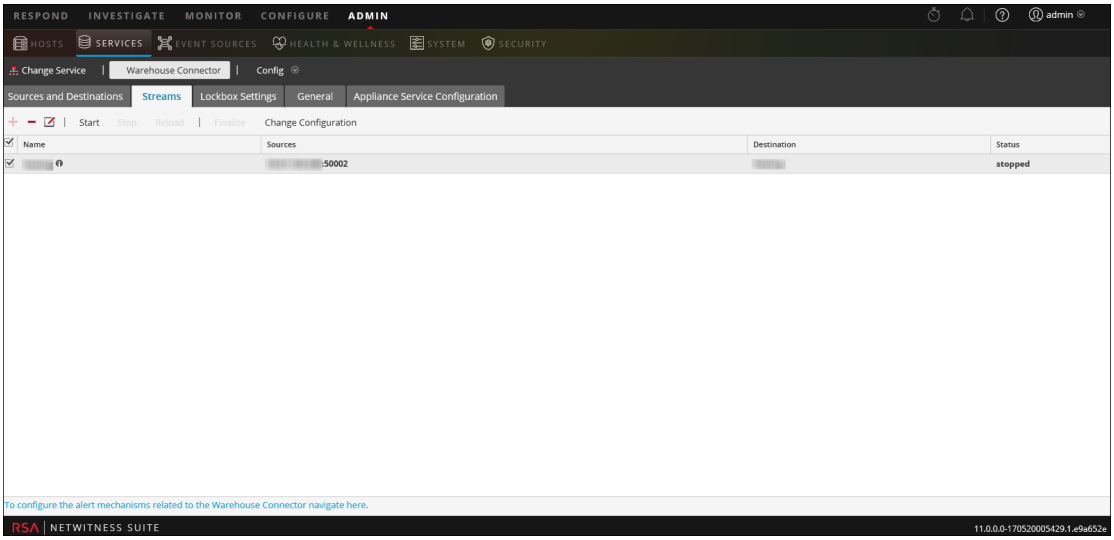
4. [**ファイナライズ**]をクリックします。

ストリームの開始

注：Warehouse Connector仮想アプライアンスアプライアンスを導入している場合は、`Maximum Message Hold Count`パラメータのデフォルト値を800000に変更していることを確認します。詳細については、「[全般]タブの設定」を参照してください。

ストリームを開始するには、次の手順を実行します。

1. メイン メニューで、**[管理]＞[サービス]**を選択します。
2. [サービス]ビューで、追加されたWarehouse Connectorサービスを選択して、  **＞[表示]＞[構成]**を選択します。
   Warehouse Connectorの[サービス]の[構成]ビューが表示されます。
3. **[ストリーム]**タブで、作成したストリームを選択します。



4. **[開始]**をクリックします。

Warehouse Connectorの監視

Warehouse Connectorを監視することで、Warehouse Connectorとそのストレージに関する重要な閾値を超える条件が発生した場合に、自動的に通知を生成できます。

Warehouse Connectorを監視するには、次の手順を実行します。

1. メイン メニューで、**[管理]>[サービス]**を選択します。
2. [サービス]ビューで、追加されたWarehouse Connectorサービスを選択して、  **>[表示]>[構成]**を選択します。
   Warehouse Connectorの[サービス]の[構成]ビューが表示されます。
3. **[ストリーム]**タブをクリックします。
4. **[ストリーム]**タブの下にある**[Warehouse Connectorに関連するアラートを構成するには、ここに移動します]**をクリックします。
   [Warehouse Connectorモニタリング]ページが表示されます。

注意:このページは廃止予定で、将来のリリースでは削除されます。

5. **[ソースまたは宛先のステータス]**セクションで、**[次の時間失敗したら通知]**フィールドで時間および時間の単位(分または時間)を選択します。
   ソースまたは宛先の接続に障害が発生し、定義した時間が経過した場合に、通知が送信されます。
6. **[ストリーム ステータス]**セクションで、次の手順を実行します。
   a. **[次の時間停止している場合に通知]**フィールドで、ストリームがオフラインになってから通知が送信されるまでの時間および時間の単位(分または時間)を定義します。
   b. **[ストレージ]**フィールドで、使用済み(%)の制限を定義します。超過した場合に通知が送信されます。
   c. **[ソース遅延]**フィールドで、セッションの数を定義します。定義した数のセッションでソースが未処理となった場合に通知が発生します。
   d. **[拒否フォルダ サイズ]**フィールドで、フォルダの使用量(%)の制限を定義します。超過した場合に通知が送信されます。
   e. **[永続的な失敗フォルダ内ファイル数]**フィールドで、永続的な失敗フォルダ内のファイル数の制限を定義します。超過した場合に通知が送信されます。

7. [**通知のタイプ**]フィールドで、次の手順を実行します。

   a. [**メール サーバ設定を構成します**]をクリックして、NetWitnessの通知を受信できるようにメールを構成します。詳細については、「*システム構成構成ガイド*」のトピック「**メール サーバおよび通知アカウントの構成**」を参照してください。

   b. 監査ログを設定するには、[**SyslogサーバおよびSNMPトラップ サーバを構成します**]をクリックします。詳細については、「*システム構成構成ガイド*」のトピック「**SyslogおよびSNMP設定の構成**」を参照してください。

   c. 必要に応じて、次の通知メカニズムを選択します。

   - **NetWitnessコンソール**: NetWitness UI通知ツールバーで通知を受信します。
   - [**メール**]: 通知をメールで受信します。
   - [**Syslog通知**]: Syslogイベントを生成します。
   - [**SNMPトラップ通知**]: SNMPトラップとして監査イベントを受信します。

Reporting EngineへのWarehouseデータ ソースの追加

Reporting Engineに対するレポートとアラートにこのデータ ソースを利用できるようにするには、Reporting EngineへのWarehouseデータ ソースを追加する必要があります。詳細については、「*Reporting Engine構成ガイド*」のトピック「**Reporting EngineへのWarehouseデータ ソースの追加**」を参照してください。

Warehouseレポートの分析

Warehouseモジュールでは、セキュリティ侵害の兆候を早期に示すレポートがアナリストに提供されます。NetWitnessでは、次のWarehouseレポートを分析できます。

- 不審なドメイン レポート
- 不審なDNSアクティビティ レポート
- ホスト プロファイル レポート

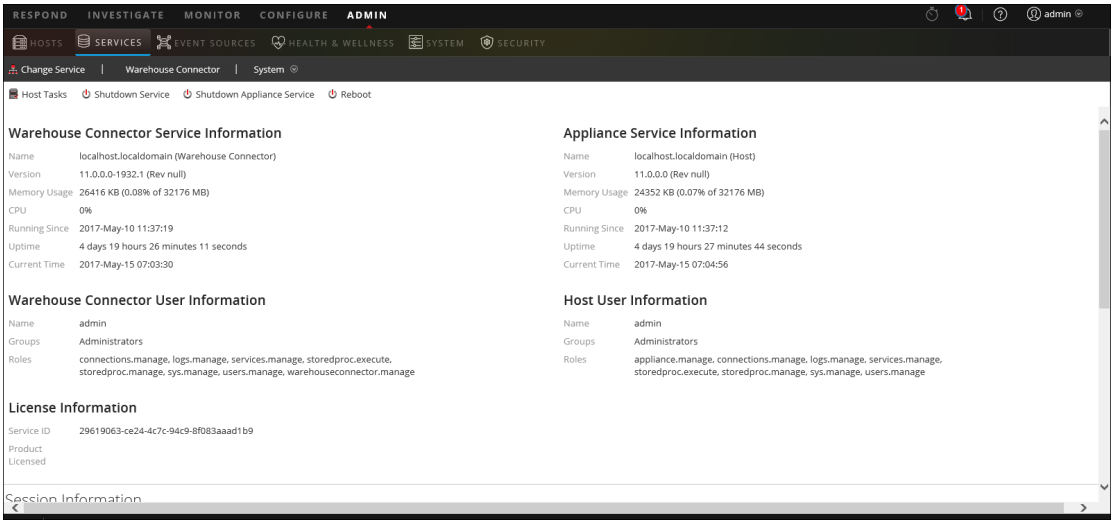
詳細については、「*Warehouseガイド*」の「**ステップ4.Warehouseレポートの分析**」トピックを参照してください。

Warehouse Connectorサービスの表示

[サービス]の[システム]ビューに表示される情報はすべてのタイプのコア サービスで共通ですが、ツールバーにあるいくつかのオプションではWarehouse Connectorのみで提供されているものがあります。

このビューにアクセスするには、次の手順を実行します。

1. メイン メニューで、**[管理]＞[サービス]**を選択します。
2. [サービス]ビューで、Warehouse Connectorサービスを選択して、  **＞[表示]＞[システム]**を選択します。
   選択したWarehouse Connectorの[システム]ビューが表示されます。



次の図は、Warehouse Connectorのツールバー オプションの例です。

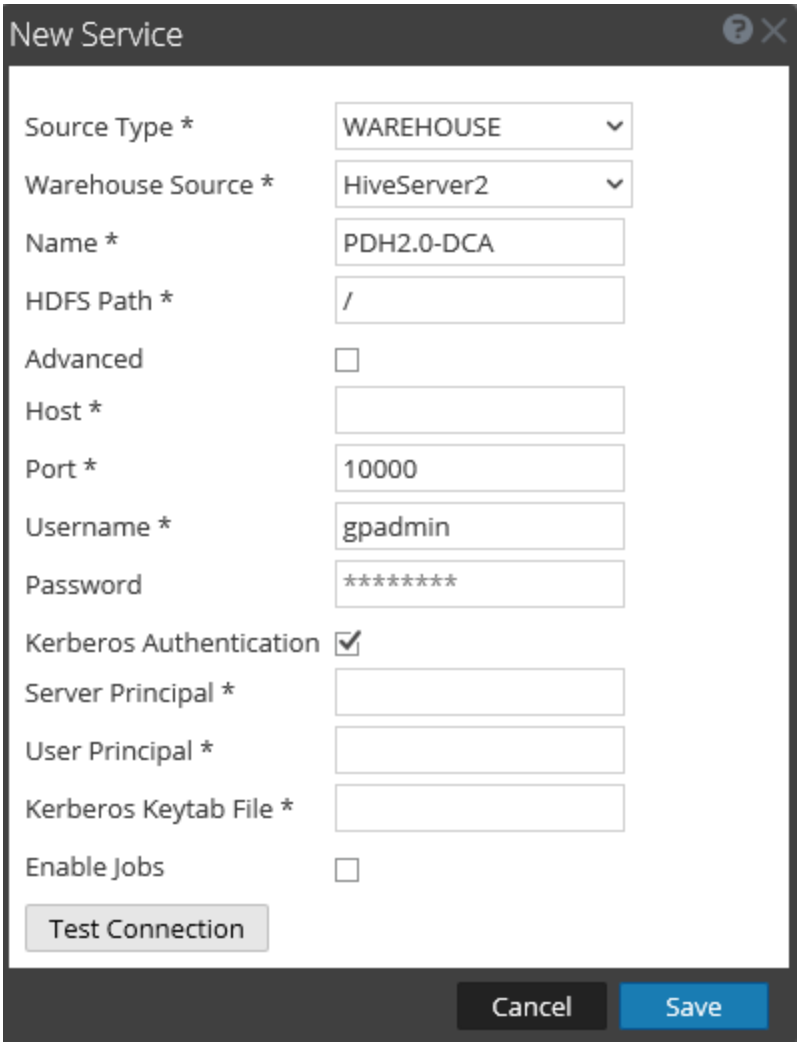
ツールバーのオプションとして、ホスト タスク、サービスのシャットダウン、Applianceサービスのシャットダウン、再起動はすべてのサービスで共通です。これらについては、「*ホストおよびサービス スタート ガイド*」を参照してください。

Warehouse Connectorのトラブルシューティング

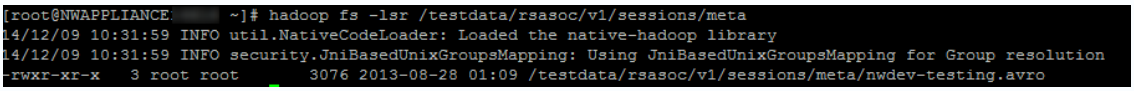
次の情報では、NetWitnessでのレポート作成用データソースとしてWarehouseサービスをReporting Engineに追加する際にNetWitnessで発生する可能性のある問題を提示します。このセクションで解決策を確認してください。

Warehouseサービスをレポート作成用データソースとしてReporting Engineに追加しようとすると、このドキュメントに示すエラーが発生する場合があります。ここでは、これらのエラーをトラブルシューティングしてデータソースを正しく追加する方法について説明します。

次の図に[新しいサービス]ダイアログを示します。



詳細については、「*Reporting Engine構成ガイド*」のトピック「**Reporting EngineへのWarehouseデータソースの追加**」を参照してください。

エラー	有効な解決策
HiveServerとの接続を開くことができませんでした	• HiveServer2がホストで実行されていることを確認します。 • 指定されたポートにReporting Engineサーバからアクセスできるかどうかを確認します。
HDFSパスでスキーマが見つかりません	指定されたHDFSパス (**<HDFS Path>/rsasoc/v1/sessions/meta**) でメタAvroデータファイルが使用可能であることを確認します。 次の図は、HDFSでファイルをチェックするコマンドの例を示しています。
	
HiveServerとの接続を開くことができず、GSSを開始できませんでした	GSS開始失敗エラーは、Kerberos対応のHiveの場合にのみ発生します。 正しいキータブファイルが指定され、rsasocユーザ(Reporting Engineサーバの実行に使用されるユーザ) の読み取りオプションが設定されていることを確認します。 システム時刻がKDC、Hadoop(HortonWorks) サーバ、Reporting Engineシステムの間で同期化されていることを確認します。

ストリームとLockboxの管理

次の手順を使用して、ストリームを管理できます。

- ストリームの編集
- ストリームの再ロード
- ストリームのメタフィルタの指定
- 複数値メタの定義

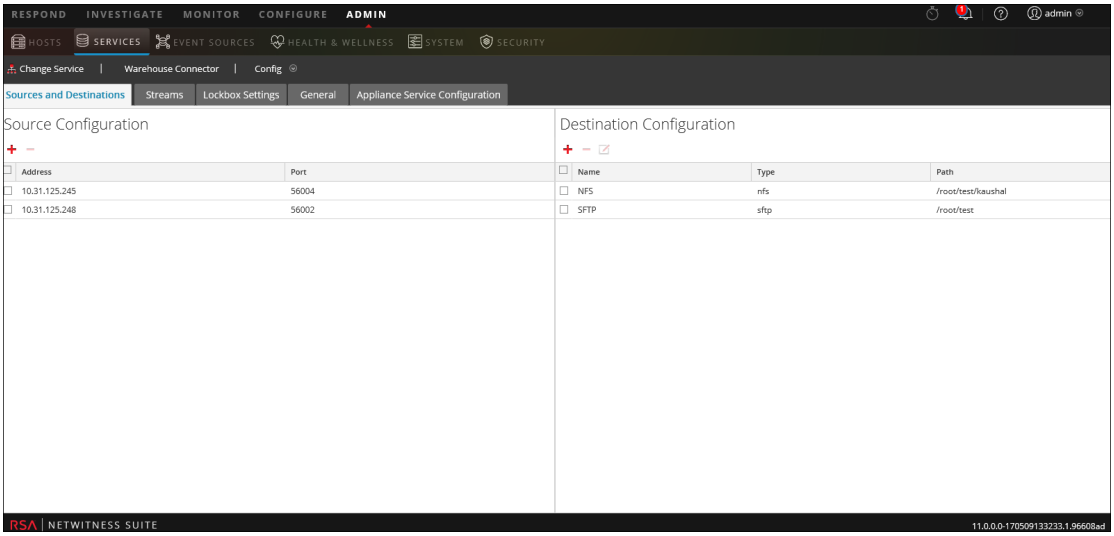
ストリームの編集

ストリームを編集することで次の操作を実行できます。

- データソースをストリームに追加します。
- 既存のデータソースをストリームから削除します。

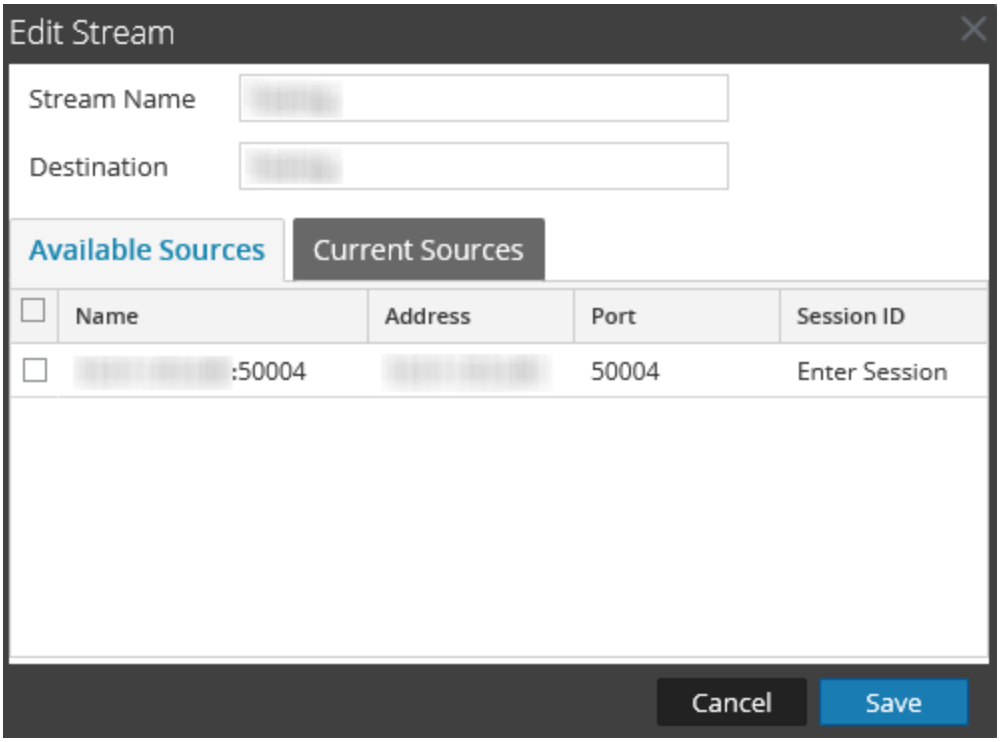
ストリームを編集するには、次の手順を実行します。

1. メインメニューで、[**管理**]＞[**サービス**]を選択します。
2. [サービス]ビューで、追加されたWarehouse Connectorサービスを選択して、  ＞[**表示**]＞[**構成**]を選択します。
   Warehouse Connectorの[サービス]の[構成]ビューが表示されます。

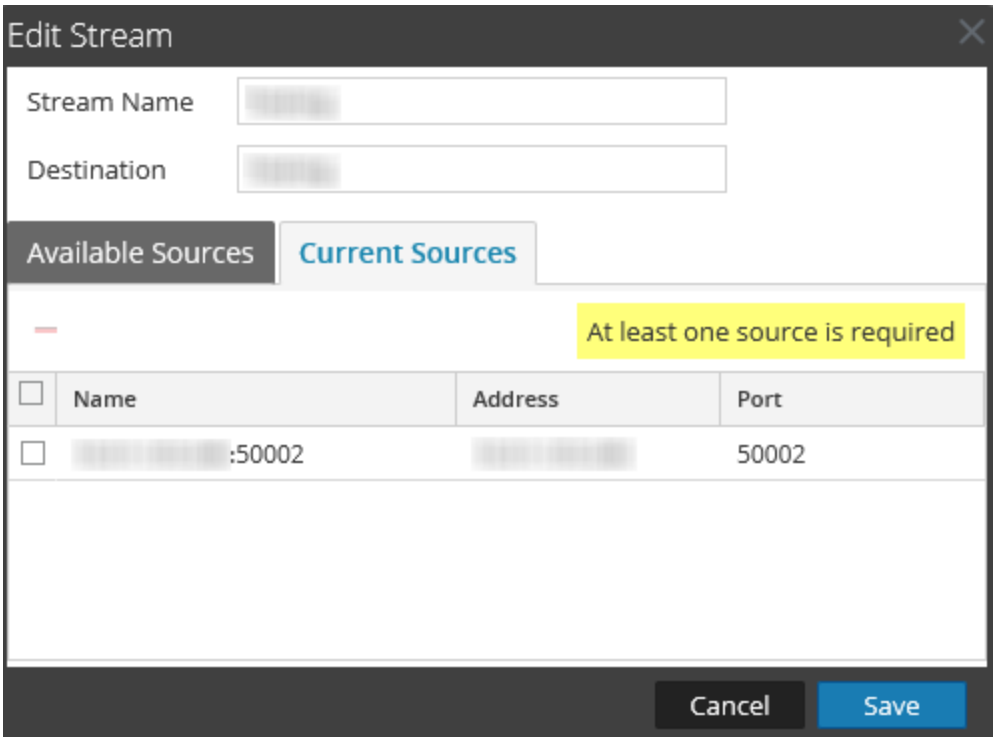


3. [**ストリーム**]タブで、  をクリックします。
4. [**ストリームの編集**]ダイアログでは、次の操作を実行できます。

- [**使用可能なソース**]タブで、使用可能なデータソースを選択してストリームに追加できます。[**保存**]をクリックします。



- [**現在のソース**]タブで、既存のデータソースをストリームから削除できます。データソースを選択し、 をクリックします。



ストリームの再ロード

ストリームを再ロードすると、Warehouse Connectorによってそのストリームのスキーマファイルが更新されます。新しいカスタムメタをLog DecoderまたはDecoderに追加した場合は必ず、ストリームを再ロードする必要があります。

ストリームを再ロードするには、次の手順を実行します。

1. メインメニューで、[**管理**]＞[**サービス**]を選択します。
2. [サービス]ビューで、追加されたWarehouse Connectorサービスを選択して、 ＞[**表示**]＞[**構成**]を選択します。
   Warehouse Connectorサービスの[構成]ビューが表示されます。
3. [**ストリーム**]タブで、再ロードするストリームを選択します。
4. [**再ロード**]をクリックします。

ストリームのメタフィルタの指定

Warehouse Connectorの[エクスプローラ]ビューで、ストリームごとに`export.session.meta.fields`パラメータでフィルタを指定する必要があります。

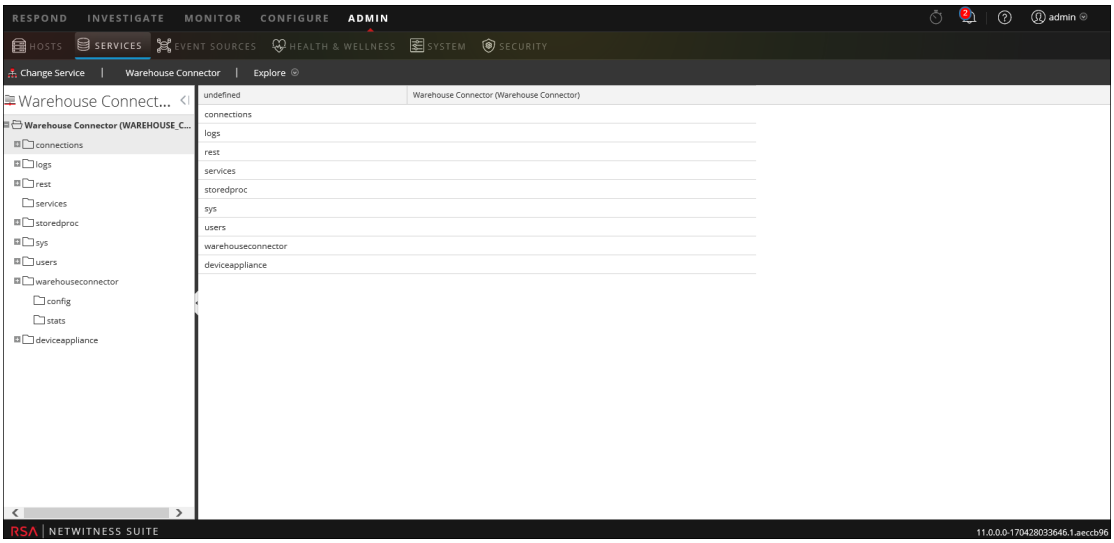
フィルタとして指定できる値を次の表に示します。

値	説明
*	収集されたすべてのメタが宛先に書き込まれます。
*, *meta1*, *meta2*	定義されているメタ以外、すべてのメタが宛先に書き込まれます。 たとえば、 **Filter:**`*,ip.src` この場合は`ip.src`を除くすべてのメタがSAWに書き込まれます。
meta1, meta2, meta3	定義されているメタのみ宛先に書き込まれます。

注:次のメタについては、フィルタを指定したとしても、デフォルトで宛先に書き込まれます。
- ng_source
- unique_id
- time

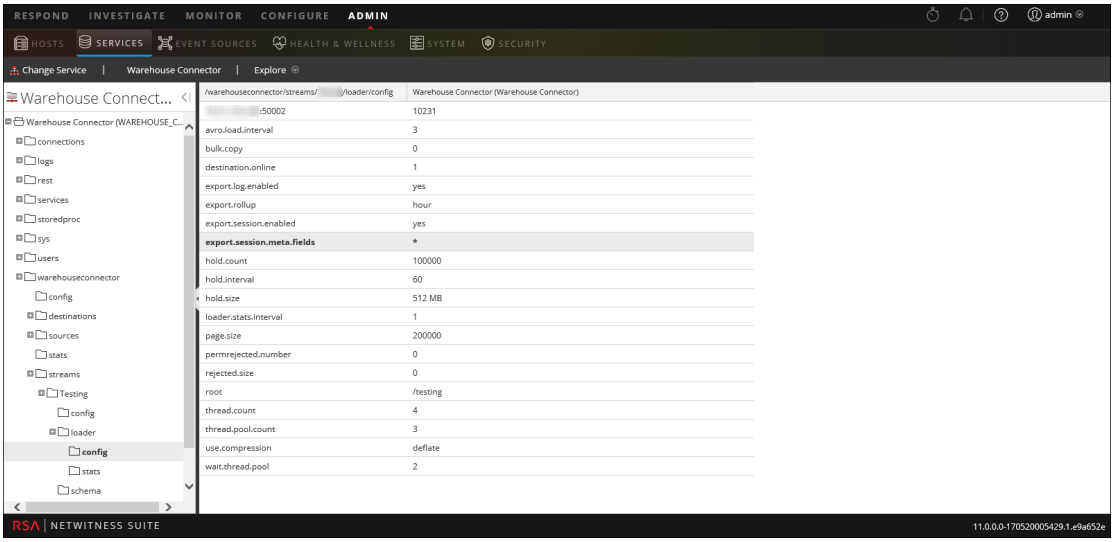
ストリームのメタフィルタを指定するには、次の手順を実行します。

1. メインメニューで、**[管理]**>**[サービス]**を選択します。
2. [サービス]ビューでWarehouse Connectorサービスを選択し、  >**[表示]**>**[エクスプローラ]**を選択します。
   Warehouse Connectorサービスの[エクスプローラ]ビューが表示されます。



3. [オプション]パネルで、[**warehouseconnector**]＞[**streams**]＞[**<stream_name>**]＞[**loader**]＞[**config**]を選択します。

4. `export.session.meta.fields`パラメータで、フィルタを入力します。



5. ストリームを再開します。

複数値メタの定義

既存のメタまたはカスタム メタを、複数値メタとして処理されるように定義することもできます。

複数値メタを定義するには、次の手順を実行します。

注意：既存のメタを複数値メタとして処理されるように定義すると、メタのデータ タイプが変わり、関連付けられているレポートが失敗する場合があります。

1. **/etc/netwitness/ng**ディレクトリに、ファイル名 **multivalue-users.xml**で新しいファイルを作成します。
2. 次のエントリーを追加します。

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

<Netwitness>
    <MultiValueMetas>
<Meta>NEWMETANAME</Meta>
    </MultiValueMetas>
</Netwitness>
```

ここで*NEWMETANAME*は複数値のメタとして扱われる既存のメタまたはカスタム メタです。

注意：デフォルトで非複数値として扱われるメタは追加しないでください。

3. ストリームを再開します。

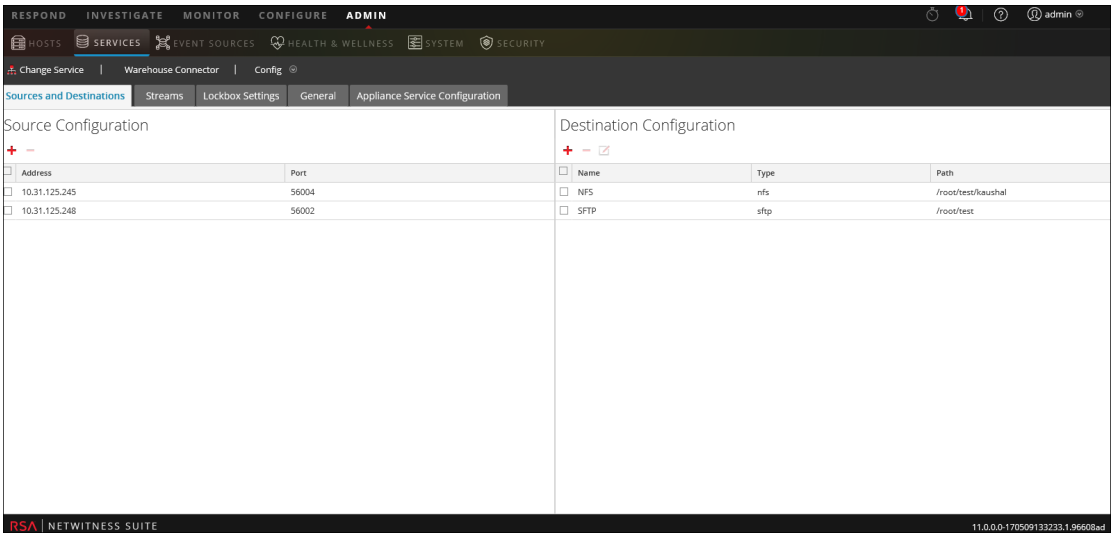
Lockboxの管理

次の手順を使用して、Lockboxを管理できます。

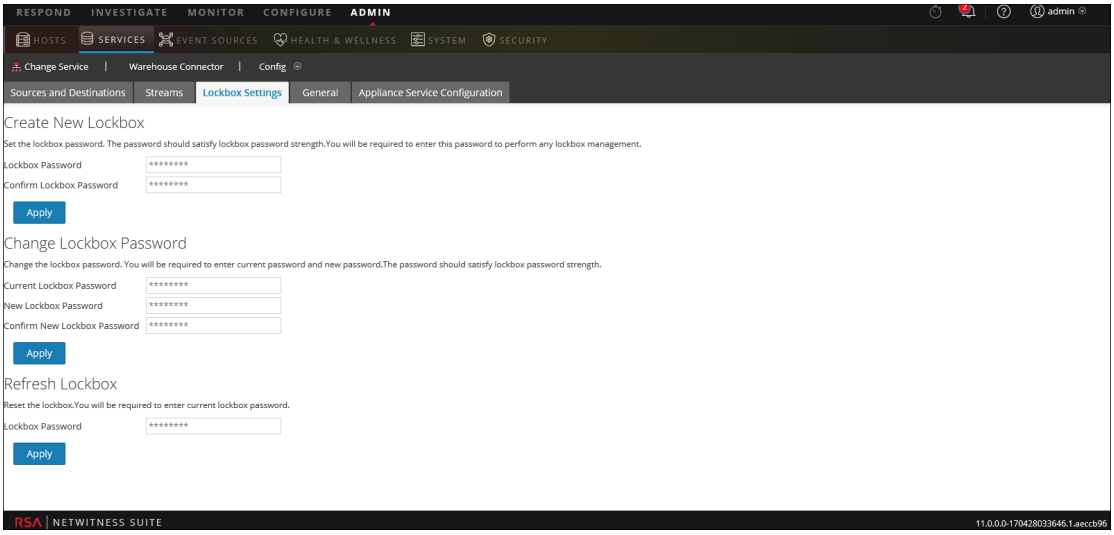
- Lockboxのパスワードの変更
- Lockboxの更新

Lockboxのパスワードを変更するには、次の手順を実行します。

1. NetWitnessにログオンします。
2. メイン メニューで、**[管理]＞[サービス]**を選択します。
3. [サービス]ビューで、追加されたWarehouse Connectorサービスを選択して、  **＞[表示]＞[構成]**を選択します。
   Warehouse Connectorの[サービス]の[構成]ビューが表示されます。



4. [**Lockbox設定**]タブをクリックします。



5. [**Lockboxのパスワードの変更**]セクションで、次の操作を行います。

   a. [現在のLockboxのパスワード]フィールドに、現在のLockboxのパスワードを入力します。

   b. [**新しいLockboxのパスワード**]フィールドに、新しいLockboxのパスワードを入力します。

   > **注**：Lockboxのパスワードは、少なくとも8文字の長さを持ち、1つ以上の大文字(A～Z)、1つ以上の小文字(a～z)、1つ以上の数字(0～9)、1つ以上の特殊文字のうち、少なくとも3種類を含む必要があります。

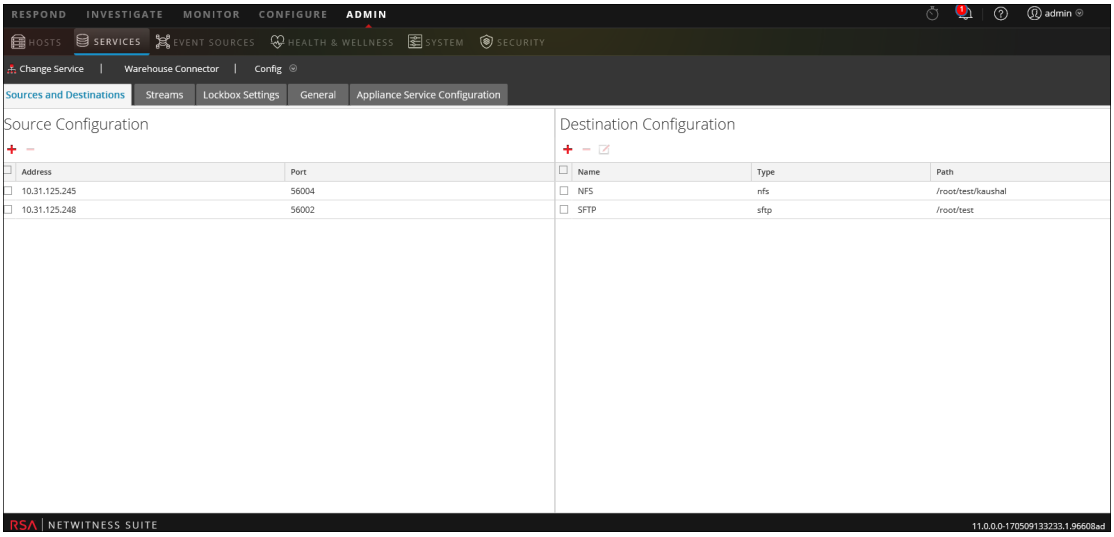
   c. 確認のため、[**新しいLockboxのパスワードの確認**]フィールドに、Lockboxの新しいパスワードを入力します。

   d. [**適用**]をクリックします。
   Lockboxのパスワードが正常に変更されます。

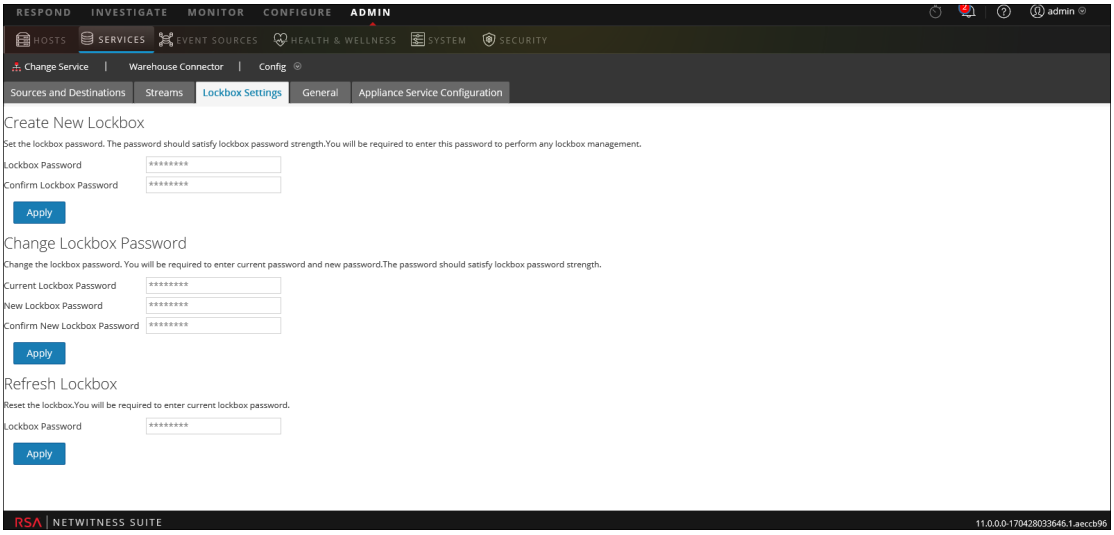
Lockboxを更新するには、次の手順を実行します。

1. NetWitnessにログオンします。
2. メイン メニューで、[**管理**]＞[**サービス**]を選択します。
3. [サービス]ビューで、追加されたWarehouse Connectorサービスを選択して、  ＞[**表示**]＞[**構成**]を選択します。

Warehouse Connectorの[サービス]の[構成]ビューが表示されます。



4. [**Lockbox設定**]タブをクリックします。



5. [**Lockboxの更新**]セクションで、現在のLockboxのパスワードを[**Lockboxのパスワード**]フィールドに入力します。
6. [**適用**]をクリックします。
   Lockboxがリセットされます。

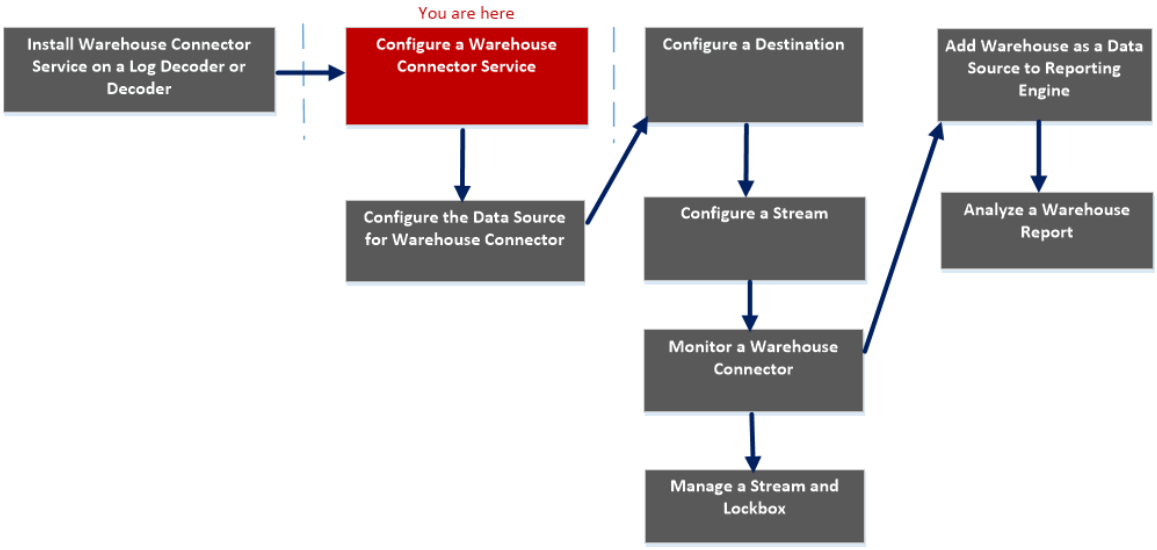
Warehouse Connectorの構成の参考情報

このセクションでは、ユーザ インタフェースに関する説明とその他の参考情報を示しています。

[全般]タブの設定

[全般]タブには、Warehouse Connectorサービスの全般的な構成設定が表示されます。

ワークフロー



実行したいことは何ですか?

ロール	実行したいこと	参照先
管理者	Log DecoderまたはDecoderへのWarehouse Connectorサービスのインストール	Log DecoderまたはDecoderあるいはHybridへのWarehouse Connectorサービスのインストール
管理者	Warehouse Connectorサービスの構成*	Warehouse Connectorサービスの構成
管理者	Warehouse Connectorのデータソースの構成	Warehouse Connectorのデータソースの構成
管理者	NFS、SFTP、WebHDFSを使用した宛先の構成。	NFSを使用した宛先の構成 SFTPを使用した宛先の構成 WebHDFSを使用した宛先の構成
管理者	ストリームの構成	ストリームの構成

ロール	実行したいこと	参照先
管理者	Warehouse Connectorの監視	Warehouse Connectorの監視
管理者	Reporting EngineへのWarehouseデータ ソースの追加	詳細については、「*Reporting Engine構成ガイド*」の「Reporting EngineへのWarehouseデータ ソースの追加」を参照してください。
管理者	Warehouse Reportの分析	詳細については、「ステップ4. Warehouseレポートの分析」(「*Warehouseガイド*」) を参照してください。
管理者	ストリームとLockboxの管理*	ストリームとLockboxの管理

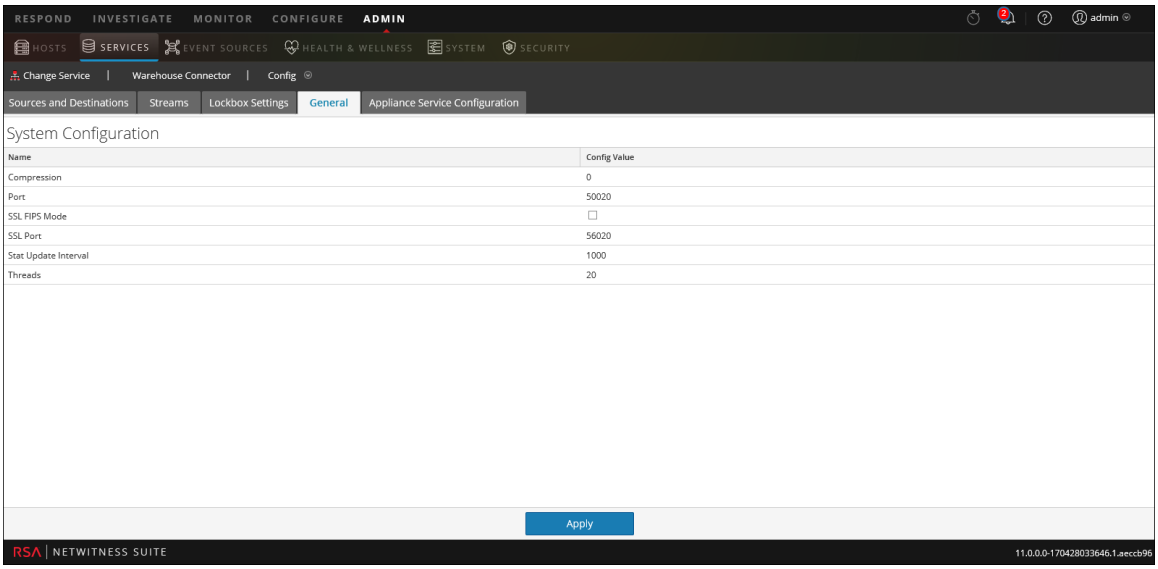
*これらのタスクはここで実行できます。

関連トピック

- Warehouse Connectorサービスの構成

クイック ビュー

次の図は、Warehouse Connectorの[サービス]の[構成]ビューにある[全般]タブを示します。[全般]タブには、Warehouse Connectorサービスのシステム構成パラメータが表示されます。



Warehouse Connectorサービスを追加すると、デフォルト値が有効になります。RSAでは、デフォルト値でほとんどの環境に対応できるように設計しています。これらの値を編集するとパフォーマンスに影響を及ぼす可能性があるため、編集しないことを推奨します。

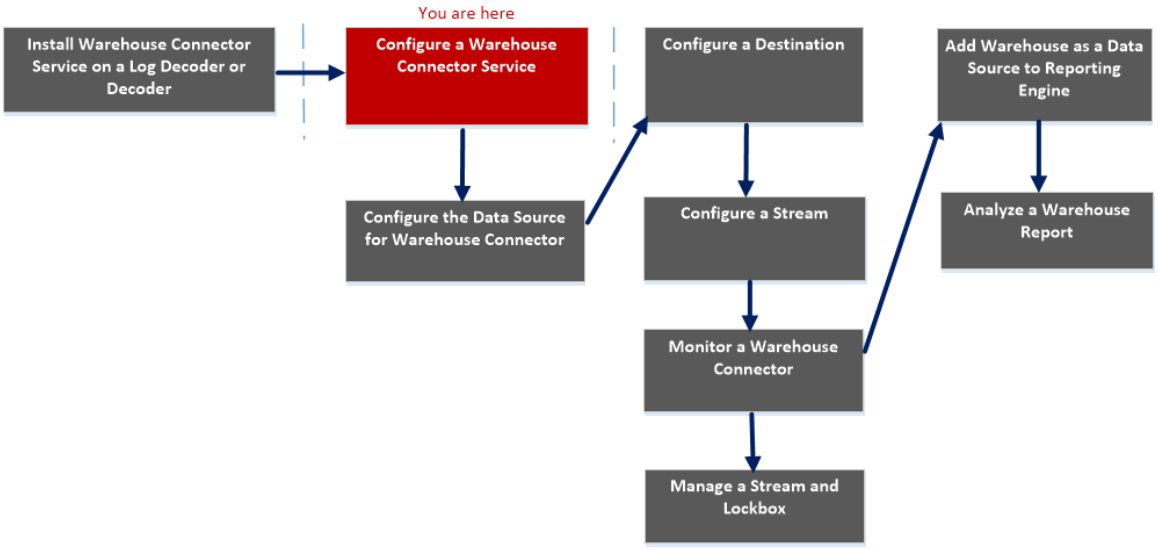
次の表に、システム構成パラメータの説明を示します。

名前	構成
Compression	メッセージが圧縮されるかどうかの分岐点となるバイト数を指定します。ゼロに設定した場合、メッセージは圧縮されません。
Port	サービスに使用されるポートを指定します。 **注**:ポート番号を変更した場合は必ず、サービスを再起動してください。
SSL	有効にした場合、ネットワークで転送されるすべてのデータがSSLで暗号化されます。
Stat Update Interval	システムで統計ノードが更新される頻度(ミリ秒単位)を指定します。
Threads	着信リクエストを処理するスレッド プール内のスレッド数を指定します。

[Applianceサービス構成]タブの設定

[Applianceサービス構成]タブには、Warehouse Connectorサービスのアプライアンスの構成設定が表示されます。詳細については、「*ホストおよびサービス スタート ガイド*」のトピック「**Applianceサービス構成**」を参照してください。

ワークフロー



実行したいことは何ですか?

ロール	実行したいこと	参照先
管理者	Log DecoderまたはDecoderへのWarehouse Connectorサービスのインストール	Log DecoderまたはDecoderあるいはHybridへのWarehouse Connectorサービスのインストール
管理者	Warehouse Connectorサービスの構成*	Warehouse Connectorサービスの構成
管理者	Warehouse Connectorのデータ ソースの構成	Warehouse Connectorのデータ ソースの構成
管理者	NFS、SFTP、WebHDFSを使用した宛先の構成。	NFSを使用した宛先の構成 SFTPを使用した宛先の構成 WebHDFSを使用した宛先の構成

ロール	実行したいこと	参照先
管理者	ストリームの構成	ストリームの構成
管理者	Warehouse Connectorの監視	Warehouse Connectorの監視
管理者	Reporting EngineへのWarehouseデータソースの追加	詳細については、「*Reporting Engine構成ガイド*」の「Reporting EngineへのWarehouseデータソースの追加」を参照してください。
管理者	Warehouse Reportの分析	詳細については、「ステップ4. Warehouseレポートの分析」(「*Warehouseガイド*」) を参照してください。
管理者	ストリームとLockboxの管理*	ストリームとLockboxの管理

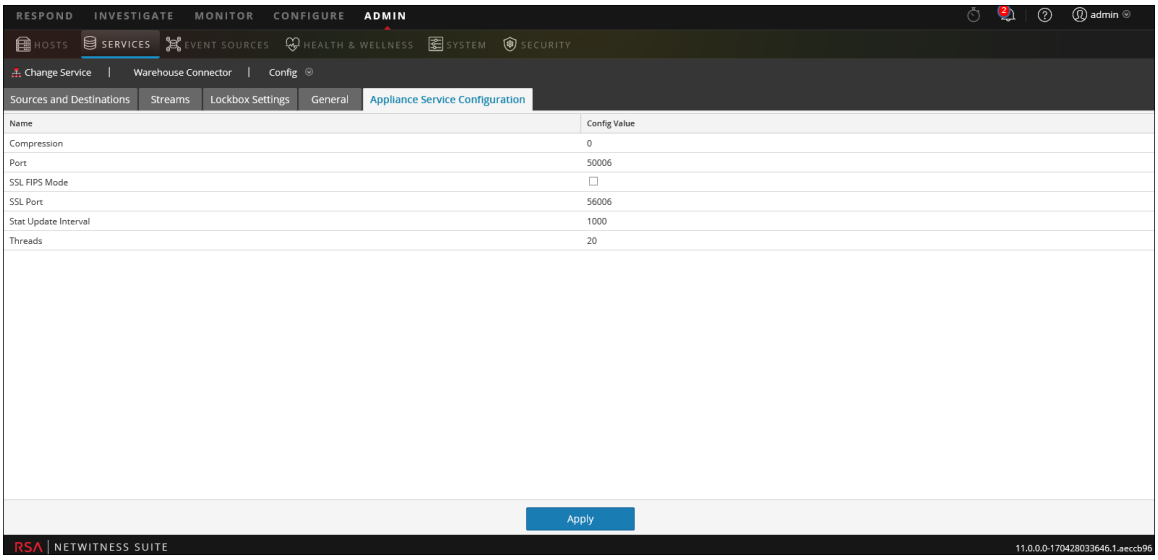
*これらのタスクはここで実行できます。

関連トピック

- Warehouse Connectorサービスの構成

クイックビュー

次の図は、[Applianceサービス構成]タブのさまざまな設定を示しています。



Warehouse Connectorサービスを追加すると、デフォルト値が有効になります。RSAでは、デフォルト値でほとんどの環境に対応できるように設計しています。これらの値を編集するとパフォーマンスに影響を及ぼす可能性があるため、編集しないことを推奨します。

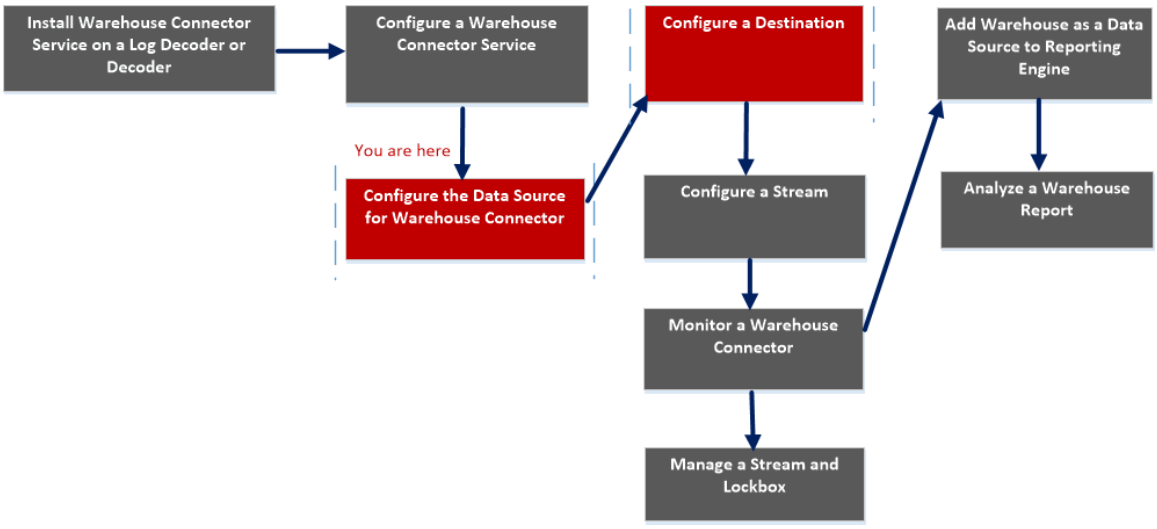
次の表に、Applianceサービス構成パラメータの説明を示します。

名前	構成値
Compression	メッセージが圧縮されるかどうかの分岐点となるバイト数を指定します。ゼロに設定した場合、メッセージは圧縮されません。
Port	サービスに使用されるポートを指定します。 **注**:ポート番号を変更した場合は必ず、サービスを再起動してください。
SSL FIPS Mode	有効にした場合、ネットワークで転送されるすべてのデータがSSL FIPSで暗号化されます。
SSL Port	サービスに使用されるSSLポートを指定します。
Stat Update Interval	システムで統計ノードが更新される頻度(ミリ秒単位)を指定します。
Threads	着信リクエストを処理するスレッド プール内のスレッド数を指定します。

[ソースと宛先]の構成

[サービス]の[構成]ビューにあるWarehouse Connectorの[ソースと宛先]タブでは、基本的なサービスの構成を管理し、ソースと宛先を構成する方法が提供されています。

ワークフロー



実行したいことは何ですか?

ロール	実行したいこと	参照先
管理者	Log DecoderまたはDecoderへのWarehouse Connectorサービスのインストール	Log DecoderまたはDecoderあるいはHybridへのWarehouse Connectorサービスのインストール
管理者	Warehouse Connectorサービスの構成	Warehouse Connectorサービスの構成
管理者	Warehouse Connectorのデータソースの構成*	Warehouse Connectorのデータソースの構成
管理者	NFS、SFTP、WebHDFSを使用した宛先の構成*	NFSを使用した宛先の構成 SFTPを使用した宛先の構成 WebHDFSを使用した宛先の構成
管理者	ストリームの構成	ストリームの構成

ロール	実行したいこと	参照先
管理者	Warehouse Connectorの監視	Warehouse Connectorの監視
管理者	Reporting EngineへのWarehouseデータソースの追加	詳細については、「*Reporting Engine構成ガイド*」の「Reporting EngineへのWarehouseデータソースの追加」を参照してください。
管理者	Warehouse Reportの分析	詳細については、「ステップ4. Warehouseレポートの分析」(「*Warehouseガイド*」)を参照してください。
管理者	ストリームとLockboxの管理*	ストリームとLockboxの管理

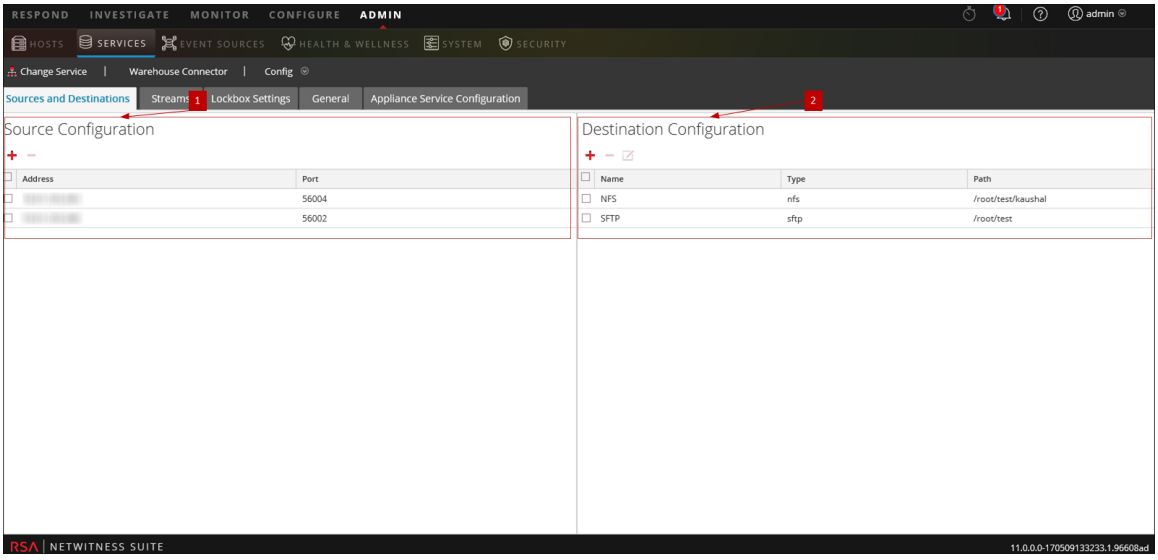
*これらのタスクはここで実行できます。

関連トピック

- Warehouse Connectorのデータソースの構成
- 宛先の構成

クイックビュー

次の図は、Warehouse Connectorの[サービス]の[構成]ビューにある[ソースと宛先]タブを示します。



[ソースと宛先]タブには、次の2つのセクションがあります。

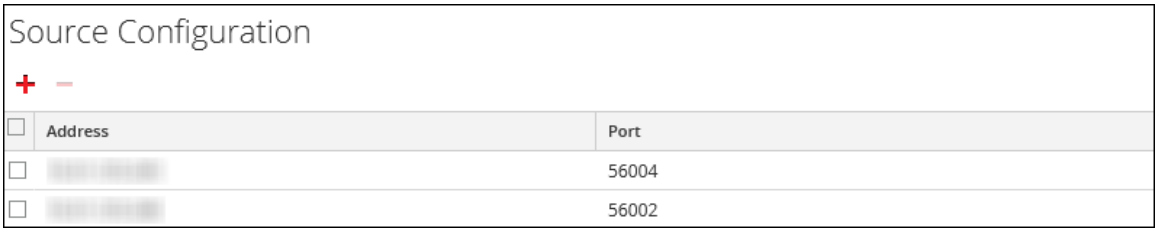
1 ソースの構成

2 宛先の構成

ソースの構成

Warehouse Connectorサービスがデータの収集元として使用するデータソースは、[ソースの構成]セクションで構成できます。

[ソースの構成]セクションの例を次に示します。

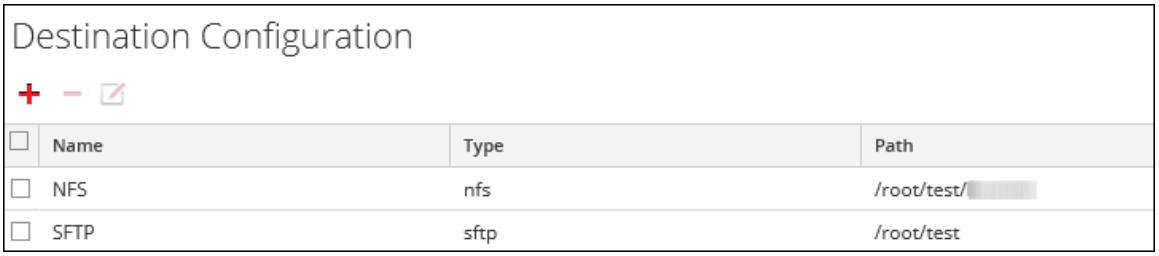


[ソースの構成]セクションでは、次の操作を実行できます。

機能	説明
+	データソースを追加します。
−	データソースを削除します。

宛先の構成

Warehouse Connectorサービスが収集データの書き込み先として使用する宛先は、[宛先の構成]セクションで構成できます。



[宛先の構成]セクションでは、次の操作を実行できます。

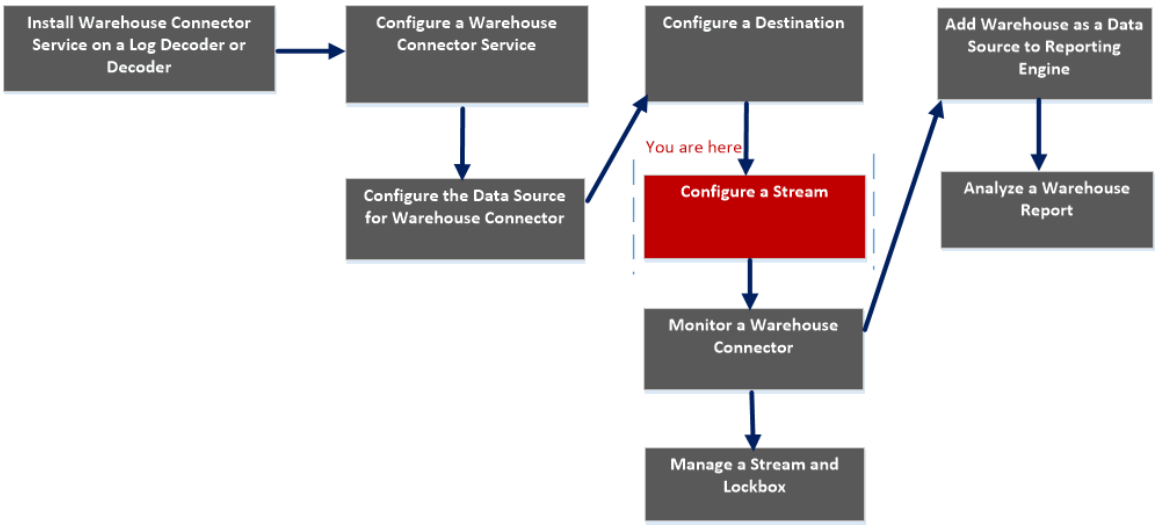
機能	説明
+	宛先を追加します。
−	宛先を削除します。

機能	説明
	宛先を編集します。 **注**:SFTPの宛先タイプのみを編集できます。

[ストリームの追加]ダイアログ

このダイアログでは、ストリームを構成し、Warehouse Connectorに追加できます。

ワークフロー



実行したいことは何ですか?

ロール	実行したいこと	参照先
管理者	Log DecoderまたはDecoderへのWarehouse Connectorサービスのインストール	Log DecoderまたはDecoderあるいはHybridへのWarehouse Connectorサービスのインストール
管理者	Warehouse Connectorサービスの構成	Warehouse Connectorサービスの構成
管理者	Warehouse Connectorのデータソースの構成	Warehouse Connectorのデータソースの構成
管理者	NFS、SFTP、WebHDFSを使用した宛先の構成。	NFSを使用した宛先の構成 SFTPを使用した宛先の構成 WebHDFSを使用した宛先の構成
管理者	ストリームの構成*	ストリームの構成

ロール	実行したいこと	参照先
管理者	Warehouse Connectorの監視	Warehouse Connectorの監視
管理者	Reporting EngineへのWarehouseデータ ソースの追加	詳細については、「*Reporting Engine構成ガイド*」の「Reporting EngineへのWarehouseデータ ソースの追加」を参照してください。
管理者	Warehouse Reportの分析	詳細については、「ステップ4. Warehouseレポートの分析」(「*Warehouseガイド*」) を参照してください。
管理者	ストリームとLockboxの管理*	ストリームとLockboxの管理

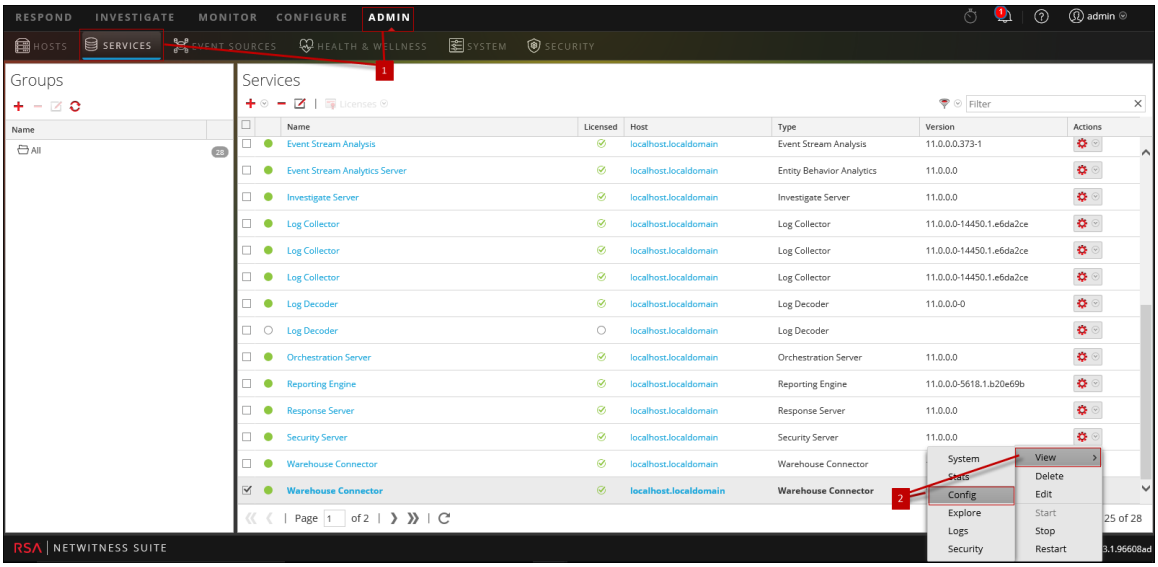
*これらのタスクはここで実行できます。

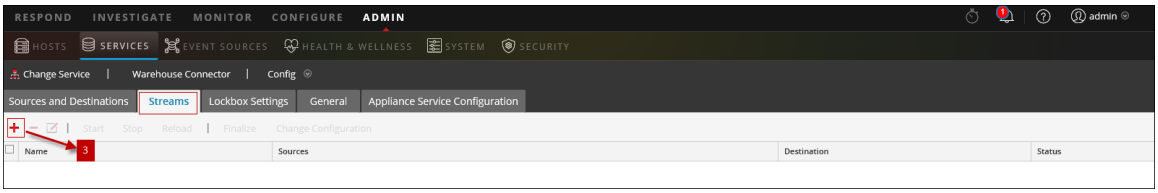
関連トピック

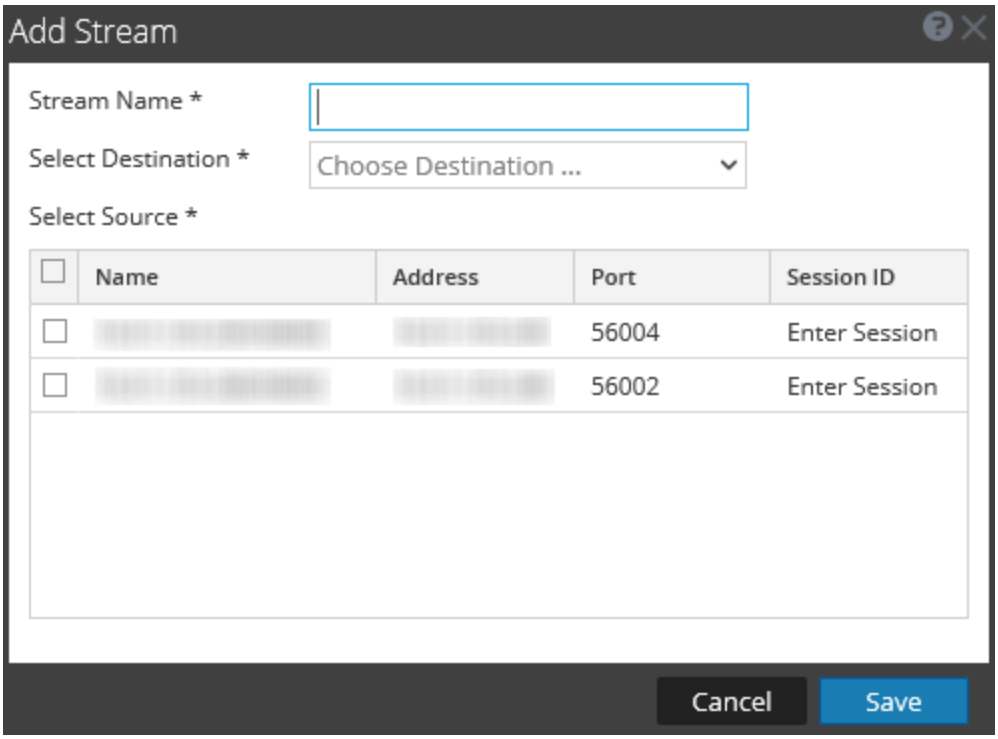
- ストリームの構成

クイック ビュー

次の図は、重要な機能にラベル付けされた例です。







1 メイン メニューで、[**管理**]＞[**サービス**]を選択します。

2 [**サービス**]ビューで、Warehouse Connectorサービスを選択し、  ＞[**表示**]＞[**構成**]を選択します。

3 [**ストリーム**]タブで、＋をクリックして[ストリームの追加]ダイアログを表示します。

次の表で、[ストリームの追加]ダイアログの各フィールドについて説明します。

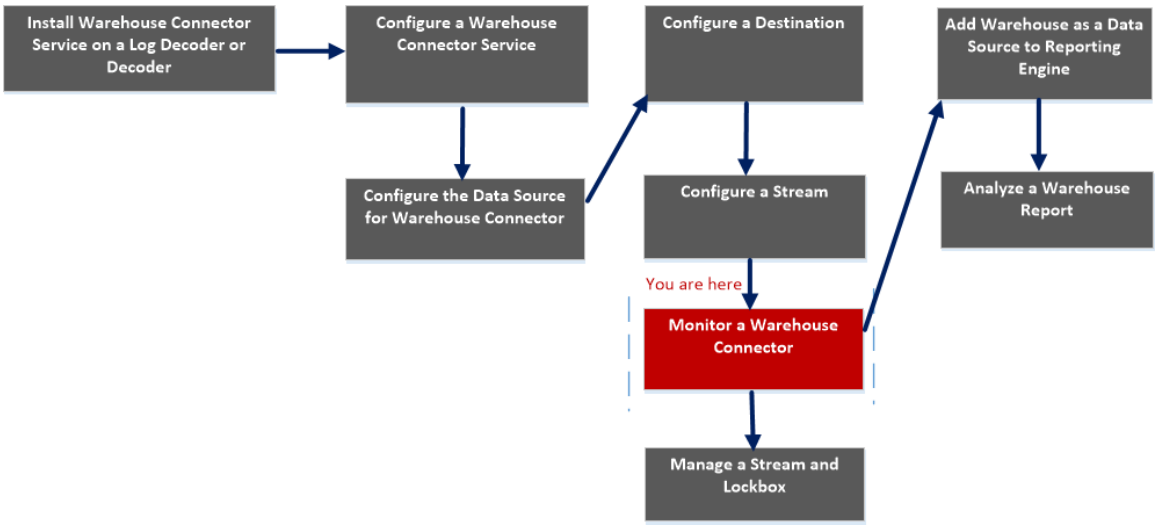
パラメータ	説明
ストリーム名	ストリームの名前を入力します。ストリーム名に使用できるのは、英数字とアンダースコアのみです。また、20文字を超えることはできません。
宛先の選択	ドロップダウン リストから宛先を選択します。

パラメータ	説明
ソースの選択	ダイアログの下部のグリッドからソースを選択します。
名前	ソースの名前。
アドレス	ソースのアドレス。
ポート	ソースのポート。
セッションID	ソースのセッションID。

ストリーム構成

[サービス]の[構成]ビューにあるWarehouse Connectorの[ストリーム]タブでは、ストリーム構成を管理する方法が提供されています。

ワークフロー



実行したいことは何ですか?

ロール	実行したいこと	参照先
管理者	Log DecoderまたはDecoderへのWarehouse Connectorサービスのインストール	Log DecoderまたはDecoderあるいはHybridへのWarehouse Connectorサービスのインストール
管理者	Warehouse Connectorサービスの構成	Warehouse Connectorサービスの構成
管理者	Warehouse Connectorのデータソースの構成	Warehouse Connectorのデータソースの構成
管理者	NFS、SFTP、WebHDFSを使用した宛先の構成。	NFSを使用した宛先の構成 SFTPを使用した宛先の構成 WebHDFSを使用した宛先の構成
管理者	ストリームの構成*	ストリームの構成

ロール	実行したいこと	参照先
管理者	Warehouse Connectorの監視*	Warehouse Connectorの監視
管理者	Reporting EngineへのWarehouseデータ ソースの追加	詳細については、「*Reporting Engine構成ガイド*」の「Reporting EngineへのWarehouseデータ ソースの追加」を参照してください。
管理者	Warehouse Reportの分析	詳細については、「ステップ4. Warehouseレポートの分析」(「*Warehouseガイド*」) を参照してください。
管理者	ストリームとLockboxの管理*	ストリームとLockboxの管理

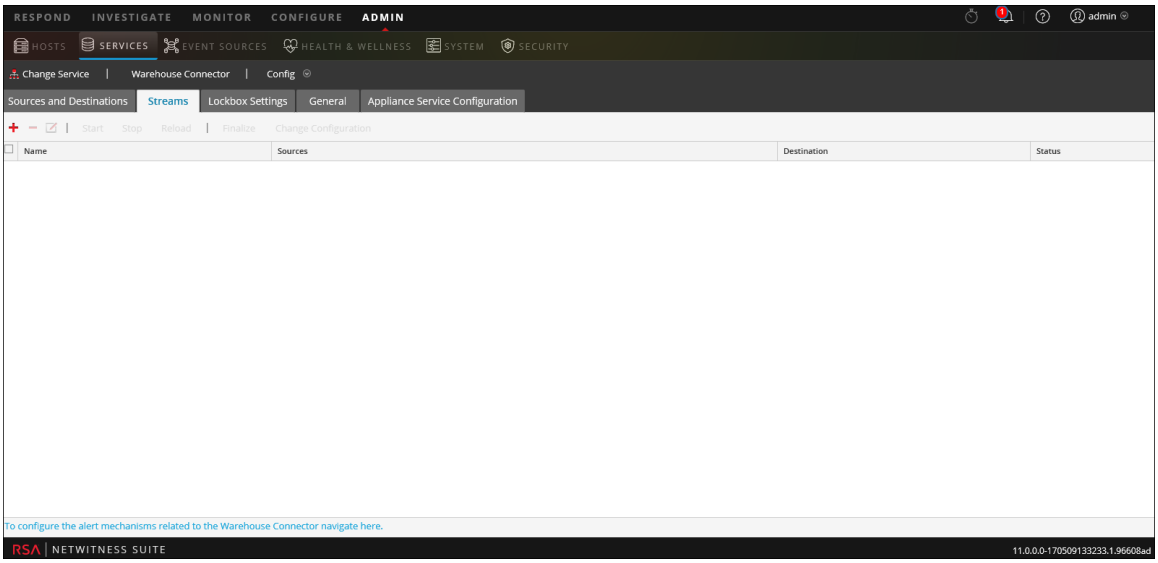
*これらのタスクはここで実行できます。

関連トピック

ストリームの構成

クイック ビュー

次の図は、Warehouse Connectorの[サービス]の[構成]ビューにある[ストリーム]タブを示します。



[ストリーム]タブでは、次の操作を実行できます。

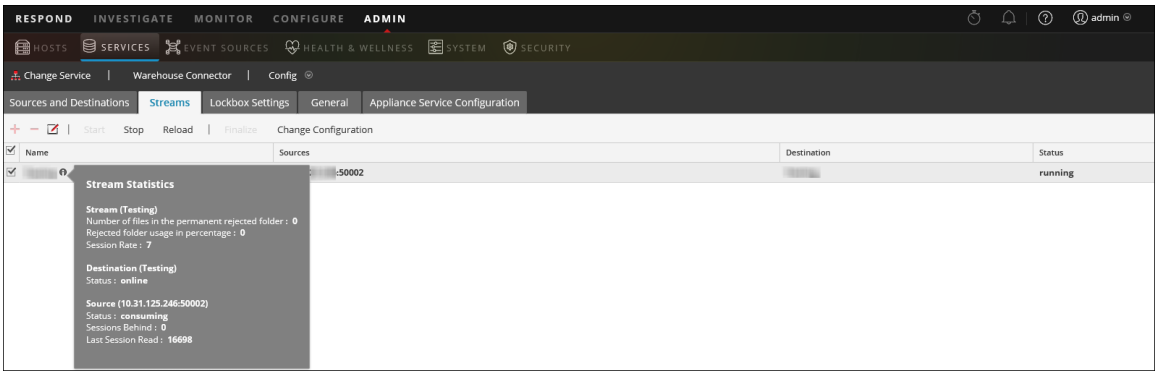
機能	説明
+	ストリームを追加します。
−	ストリームを削除します。
	ストリームを編集します。
Start	ストリームを開始します。
Stop	ストリームを停止します。
Finalize	ストリームをファイナライズします。
Reload	ストリームを再ロードします。 新しいメタを追加した場合や、コンテンツの更新の一環として新しいメタがいずれかのソース(Log DecoderまたはDecoder) に追加された場合、Reporting Engineのスキーマにそのメタを表示するためには、ストリームを再ロードする必要があります。ストリームを再ロードしても、ソースから新しいメタリストがフェッチされるだけであり、データには一切影響はありません。

次の表で、[ストリーム]タブの各フィールドについて説明します。

パラメータ	説明
名前	ストリームの名前。
ソース	ストリームに関連づけられたソース。
宛先	ストリームに関連づけられた宛先。
ステータス	ストリームのステータス。

ストリームの統計情報

構成したストリームの統計を表示できます。ストリーム名の隣の ⓘ アイコンをクリックします。



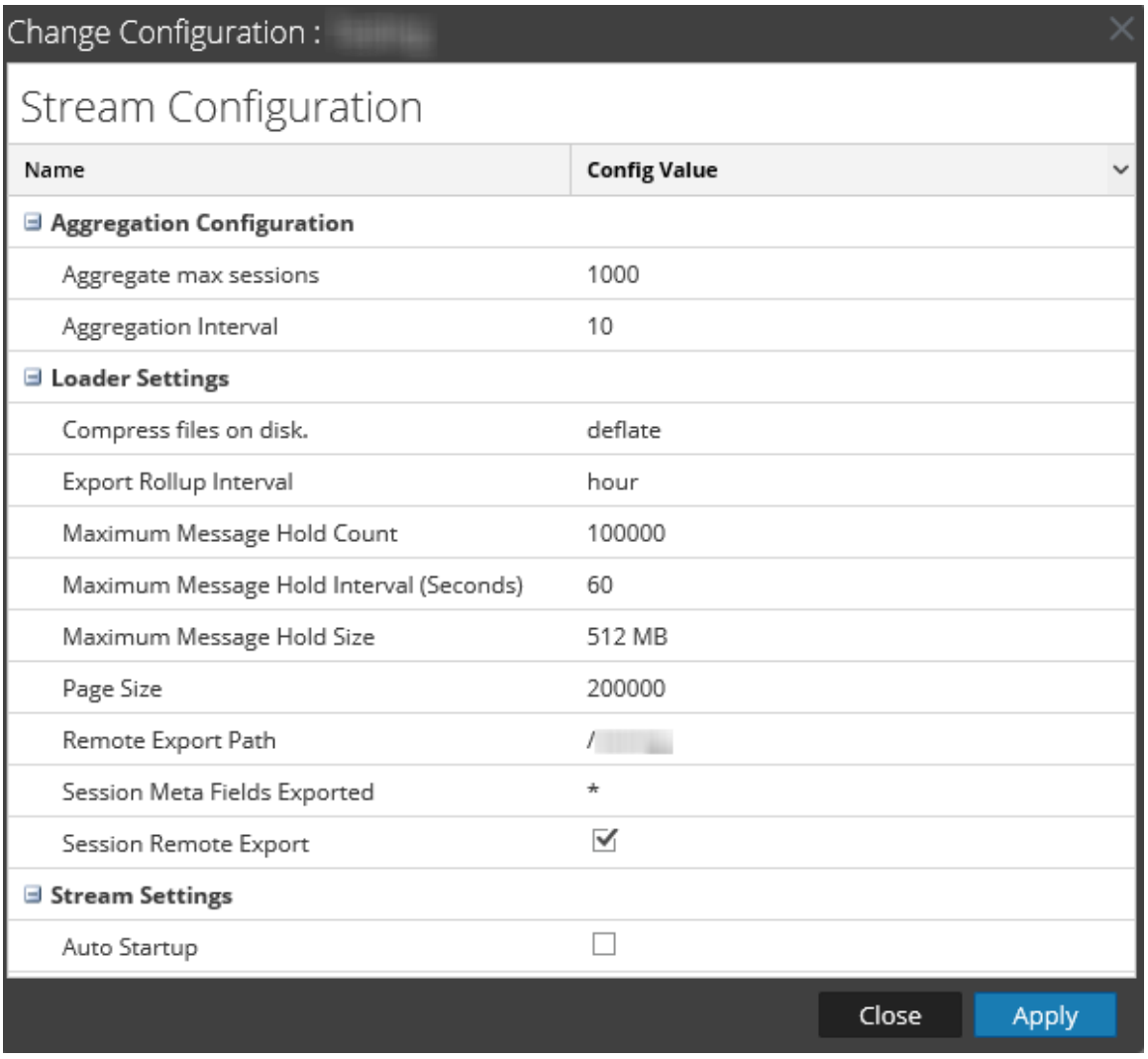
次のパラメータがストリームの統計情報に表示されます。

セクション	パラメータ	説明
ストリーム		
	永続的な拒否フォルダ内ファイル数	Warehouse Connectorの永続的な拒否フォルダ(フォルダ名 : **permfail**) のファイル数が表示されます。永続的な拒否フォルダには、Warehouse Connectorが宛先に書き込むことができなかったファイルが含まれます。
	拒否フォルダの使用率(%)	拒否フォルダのディスク使用率が表示されます。
	セッション レート	Warehouse Connectorが処理するソースのセッションのレートが表示されます。
宛先		
	ステータス	宛先のステータスを示します。
ソース		
	ステータス	ソースのステータスを示します。

セクション	パラメータ	説明
	未処理のセッション数	Warehouse Connectorが処理する必要があるセッション数が表示されます。
	最終読み取りセッション	Warehouse Connectorが処理した最終のセッションIDが表示されます。

ストリーム構成の変更

ストリームの構成は実行中に変更できます。[**ストリーム**]タブで、[**構成の変更**]をクリックして、選択したストリームの構成を変更します。



ストリームの構成について、次のパラメータを変更できます。

注:ストリームの構成でパラメータの値を変更した場合は、ストリームを再開する必要があります。

アップグレードされた環境で、最大メッセージ保持数、最大メッセージ保持間隔、最大メッセージ保持サイズの値がそれぞれ3000000、60、128になっている場合、ストリームに次の値を割り当てる必要があります。

- 最大メッセージ保持数:2400000
- 最大メッセージ保持間隔:600
- 最大メッセージ保持サイズ:512

既存のストリーム構成を変更することで、これらの値を割り当てることができます。

セクション	パラメータ	説明
	集計の構成	
	集計最大セッション数	Warehouse Connectorからソースに対して集計リクエストを行う際の応答における最大セッション数を指定します。
	集計間隔	ソースからの応答の間隔を指定します。
	ローダー設定	
	ディスク上のファイルを圧縮	ディスク上のファイルを圧縮する場合に有効化します。 サポートされる値は次のとおりです。 • Deflate:ファイルを圧縮し、レポートを生成する際に、優れたパフォーマンスを提供します。 • Off デフォルトで、パラメータは**deflate**に設定されます。

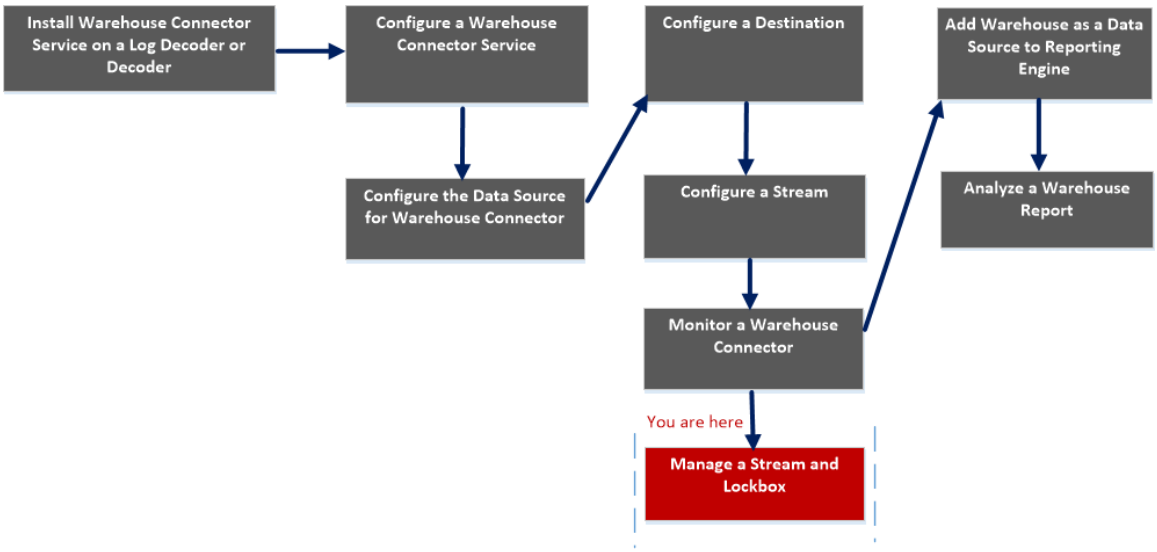
セクション	パラメータ	説明
	エクスポート ロールアップ間隔	エクスポート ファイルのロールアップ間隔、およびWarehouse Connectorが宛先に書き込むディレクトリ構造を指定します。 次に例を示します。パラメータが次のように設定された場合 : **Value** **ディレクトリ構造** hour /rsasoc/v1/[logs | sessions]/data/{year}/{month}/{day}/{hour} minute /rsasoc/v1/[logs | sessions]/data/{year}/{month}/{day}/{hour}/{minute} day /rsasoc/v1/[logs | sessions]/data/{year}/{month}/{day} パラメータの値を変更した場合は、ストリームを再開する必要があります。 推奨値は[**hour**]です。
	最大メッセージ保持数	処理前にメモリに格納するセッションの最大数を指定します。 **注 :** Warehouse Connector仮想アプライアンスアプライアンスを導入している場合は、パラメータのデフォルト値を800000に変更していることを確認します。
	最大メッセージ保持間隔(秒)	処理前にセッションをメモリに保持する最大期間(秒)を指定します。
	最大メッセージ保持サイズ	処理前にメモリに格納するセッションの最大サイズを指定します。

セクション	パラメータ	説明
	リモート エクスポート パス	HDFSのリモート ローカル マウント ポイント (nfs://) とデータのエクスポート先を指定します。
	ページ サイズ	
ストリーム設定		
	自動開始	有効にすると、Warehouse Connectorプロセスが再起動されるたびにストリームが自動的に開始されます。デフォルトで、パラメータは**off**に設定されます。

Lockbox設定

サービスの[構成]ビューにあるWarehouse Connectorの[Lockbox設定]タブでは、lockboxの設定を管理する方法を提供します。

ワークフロー



実行したいことは何ですか?

ロール	実行したいこと	参照先
管理者	Log DecoderまたはDecoderへのWarehouse Connectorサービスのインストール	Log DecoderまたはDecoderあるいはHybridへのWarehouse Connectorサービスのインストール
管理者	Warehouse Connectorサービスの構成*	Warehouse Connectorサービスの構成
管理者	Warehouse Connectorのデータソースの構成	Warehouse Connectorのデータソースの構成
管理者	NFS、SFTP、WebHDFSを使用した宛先の構成。	NFSを使用した宛先の構成 SFTPを使用した宛先の構成 WebHDFSを使用した宛先の構成
管理者	ストリームの構成	ストリームの構成

ロール	実行したいこと	参照先
管理者	Warehouse Connectorの監視	Warehouse Connectorの監視
管理者	Reporting EngineへのWarehouseデータ ソースの追加	詳細については、「*Reporting Engine構成ガイド*」の「Reporting EngineへのWarehouseデータ ソースの追加」を参照してください。
管理者	Warehouse Reportの分析	詳細については、「ステップ4. Warehouseレポートの分析」(「*Warehouseガイド*」) を参照してください。
管理者	ストリームとLockboxの管理*	ストリームとLockboxの管理

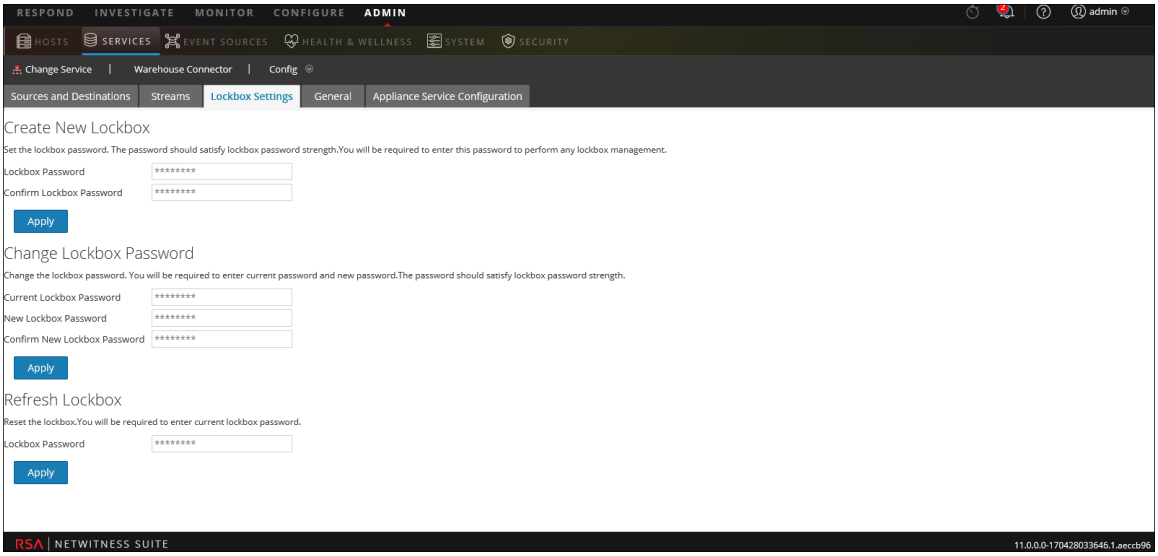
*これらのタスクはここで実行できます。

関連トピック

- Warehouse Connectorサービスの構成
- ストリームとLockboxの管理

クイック ビュー

次の図は、Warehouse Connectorの[サービス]の[構成]ビューにある[Lockbox設定]タブを示します。



[Lockbox設定]タブでは、Warehouse ConnectorのLockboxのパスワードを設定、変更、更新することができます。