RSA NETWITNESS® SUITE

ログ収集の構成ガイド

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

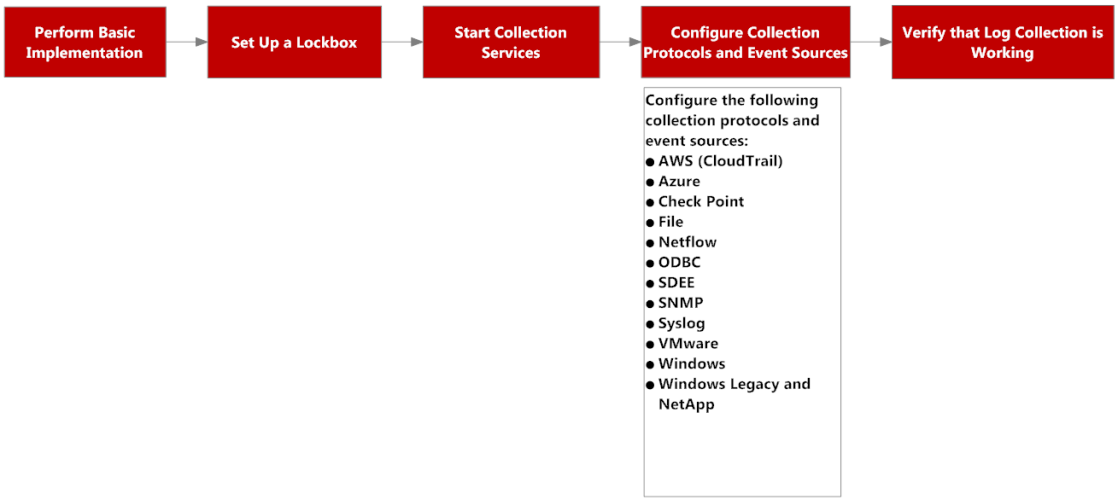
ログ収集について

このガイドでは、次を含むイベント ソースのログ収集を設定および構成する手順の概要とサブタスクについて説明します。

- ログ収集の機能とその仕組みの概要、および概要レベルの導入図を示します。
- イベント収集の開始方法。
- より複雑な構成で導入するための手順の掲載場所。
- 収集プロトコルの開始方法。
- ログ収集を構成するためのユーザ インタフェースの説明。
- ログ収集の問題をトラブルシューティングするためのツールや、全般的なトラブルシューティングの手順のリスト。
- 使用中の環境におけるログ収集の精査とカスタマイズに関する方法。
- 個別の収集プロトコルの構成方法。手順については、各ログ収集セクションを参照してください。

ワークフロー

このワークフローでは、ログ収集機能によるイベント収集の開始に必要な基本タスクを示しています。



手順の概要

これらは、ログを収集する際に従う必要がある概要レベルの手順です。

I. ローカルCollectorおよびリモートCollectorをRSA NetWitness Suiteに追加します。

Log Decoder上(つまりローカルCollector)でLog Collectorをローカルに設定します。組織の要件に従って、任意の数のリモートの設置場所にLog Collector(リモートCollectorとして機能する)を設定できます。詳細については、「基本的な実装」を参照してください。

II. Liveからの最新のコンテンツをダウンロードします。Liveで提供されるコンテンツは定期的に更新されるため、このタスクは定期的に実行してください。

LIVEは、RSA NetWitness® Suiteのコンテンツ管理システムで、ここから最新のコンテンツをダウンロードします。ログ収集に関するコンテンツには、次の2つのリソースタイプがあります。

- **RSA Log Collector**: イベント ソース タイプの収集を可能にするコンテンツ。
- **RSA Log Device**: サポートされる最新のイベント ソースParser。

Liveのコンテンツをサブスクライブすることもできます。詳細については、「*Live サービス管理ガイド*」を参照してください。

III. 設定(Lockboxと証明書のセットアップ)を構成します。

詳細については、「Lockbox設定」と「証明書の構成」を参照してください。

IV. イベント ソースを構成します。

ログ情報をRSA NetWitness Suiteに送信するように、ネットワーク上のすべてのイベント ソースを構成します。新しいイベント ソースを追加したら、必ずこの手順も実行する必要があります。イベント ソースの構成ガイドはすべて、RSA Linkの「RSA Supported Event Sources」に掲載されています。

V. 構成されたプロトコルのサービスを開始および停止します。RSA NetWitness Suiteに追加する新しいイベント ソースに応じて、サービスの停止と再開が必要になる場合があります。

VI. ログ収集が動作していることを確認します。

新しいイベント ソースをセットアップりたり、新しい収集プロトコルを追加したら、必ず適切なログがRSA NetWitness Suiteに送信されていることを確認する必要があります。

ログ収集アーキテクチャ

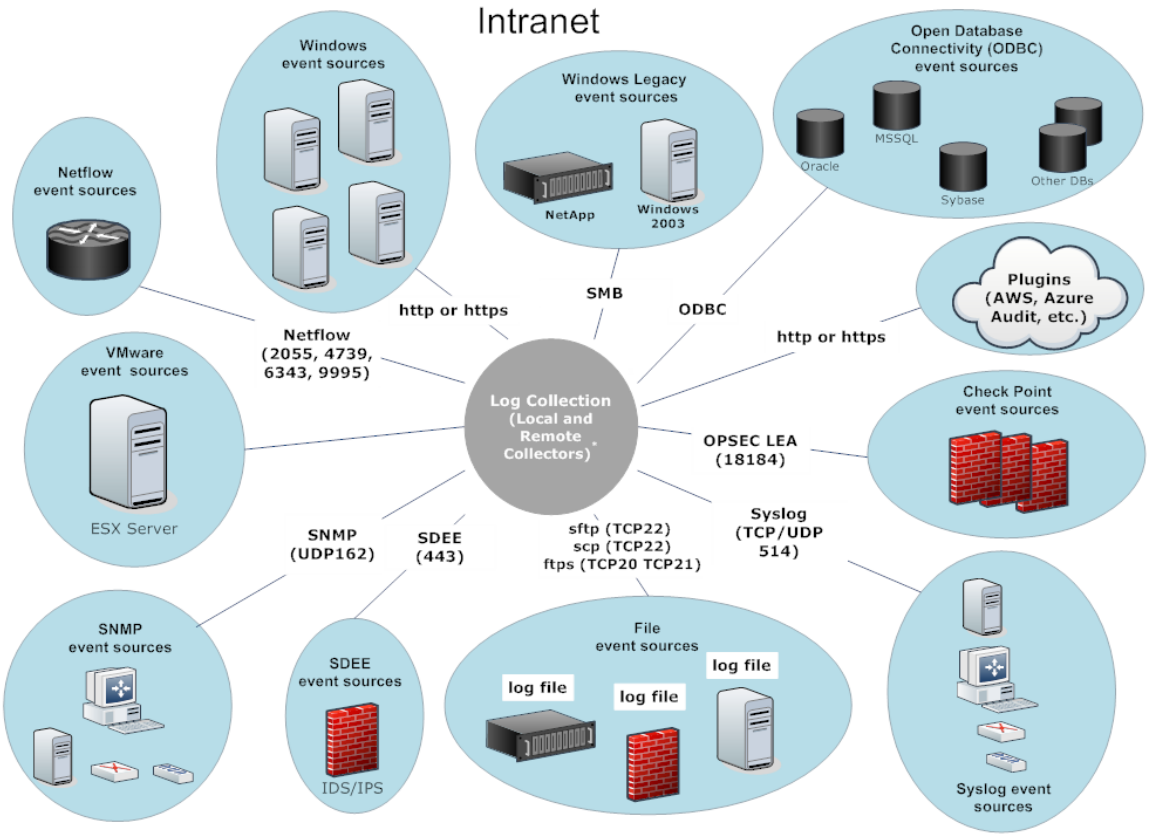
このトピックでは、NetWitness Suiteでのログ収集の実行方法について説明します。

ログ収集の導入方法

組織のニーズに従って、ログ収集を導入できます。これには、複数の設置場所にまたがるログ収集の導入、さまざまなイベント ソースからのデータ収集が含まれます。こうした設定を実装するには、1つ以上のリモートCollectorとローカルCollectorをセットアップします。

ログ収集のコンポーネント

次の図に、NetWitness Suite Log Collectorを通じたイベント収集に関わるすべてのコンポーネントを示します。



*In Log Collection, Remote Collectors send events to the Local Collector and the Local Collector sends events to the Log Decoder.

ローカルCollectorおよびリモートCollector

次の図に、ローカルCollectorおよびリモートCollectorがすべての場所からイベントを収集する方法を示します。

このようなシナリオでは、WindowsやODBCなどの各種プロトコルからのログ収集は、リモートCollectorとLog Collectorサービスの両方で実行されます。ログ収集がローカルCollectorによって行われた場合、ローカルの導入シナリオと同様に、Log Decoderサービスに転送されます。収集がリモートCollectorによって行われた場合、これらがローカルCollectorに転送される方法は2つあります。

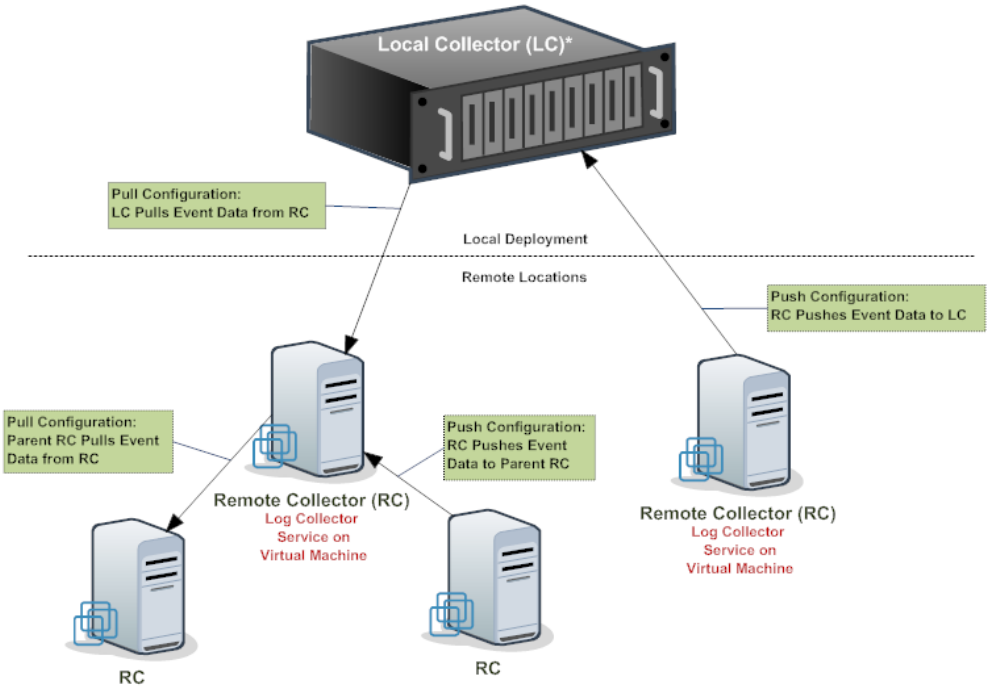
- **プル構成**：ローカルCollectorから、イベントをプルするリモートCollectorを選択する。
- **プッシュ構成**：リモートCollectorから、イベントをプッシュするローカルCollectorを選択する。

注：通常の用途はプッシュです。プルは、環境内にDMZがある場合に使用できます。より安全なネットワークセグメントに接続するために、安全性の低いネットワークセグメントは使用できません。プルでは、安全なネットワーク内のLog Collector(またはVirtual Log Collector)が安全性の低いネットワーク内のVLCへの接続を開始され、ログは接続ルールを破ることなく転送されます。

イベント データをローカルCollectorにプッシュするように1つ以上のリモートCollectorを構成するか、あるいは1つ以上のリモートCollectorからイベント データをプル受信するようにローカルCollectorを構成することができます。

さらに、構成可能なリモートCollectorのチェーンを設定することができます。

- 1つのリモートCollectorにイベント データをプッシュする1つ以上のリモートCollector。
- 1つ以上のリモートCollectorからイベント データをプル受信する1つのリモートCollector。



* The Local Collector (LC) is the Log Collector service on the Log Decoder appliance.

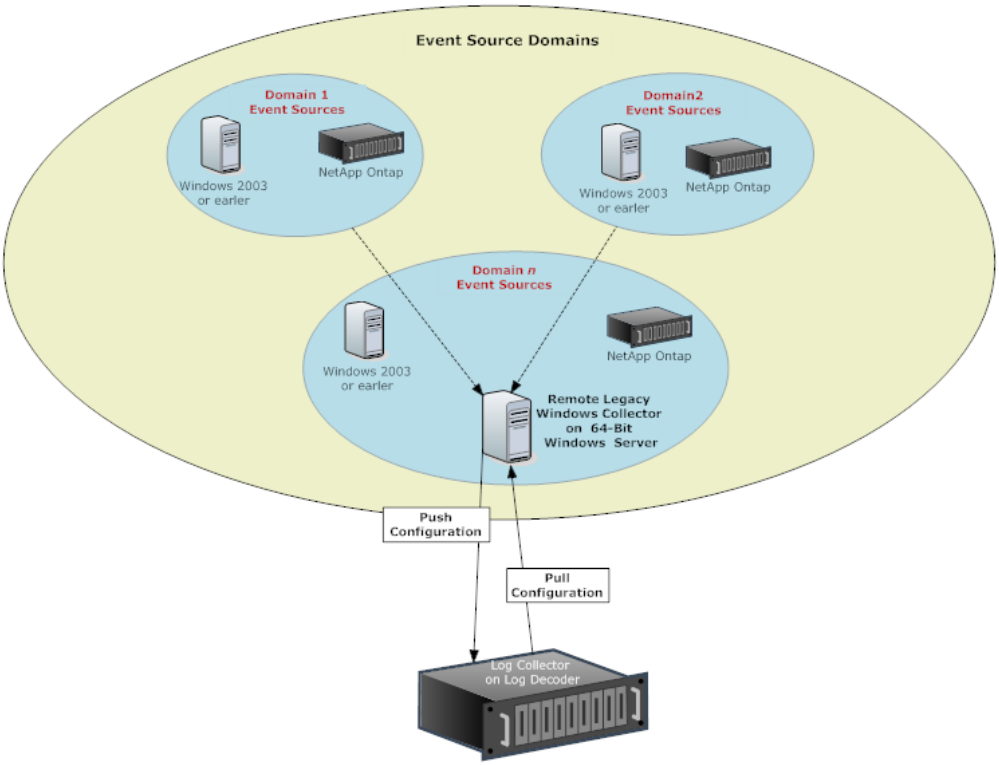
Windows Legacy リモート Collector

RSA NetWitness® Suite Windows Legacy Collectorは、Windowsドメインにインストールできる Microsoft Windowsベースのリモート Log Collector(RC) です。

次のソースからの収集がサポートされます。

- Windows 2003以前のイベント ソース
- NetApp ONTAPホストのevtファイル

次の図に、Windows Legacyイベント ソースからイベントを収集するために必要な導入環境を示します。


Event Source Domains
Domain 1
Event Sources
Windows 2003
or earlier
NetApp Ontap
Domain2
Event Sources
Windows 2003
or earlier
NetApp Ontap
Domain n
Event Sources
Windows 2003
or earlier
NetApp Ontap
Remote Legacy
Windows Collector
on 64-Bit
Windows Server
Push
Configuration
Pull
Configuration
Log Collector
on Log Decoder

構成

基本的な実装

このトピックでは、ローカルCollectorおよびリモートCollectorの初期設定の方法について説明します。

前提条件

Log Decoderが設定されていることを確認する

- データの収集が開始している。
- 最新のコンテンツがロードされている。
- 適切なライセンスが供与されている。

ローカルCollectorおよびリモートCollectorの役割

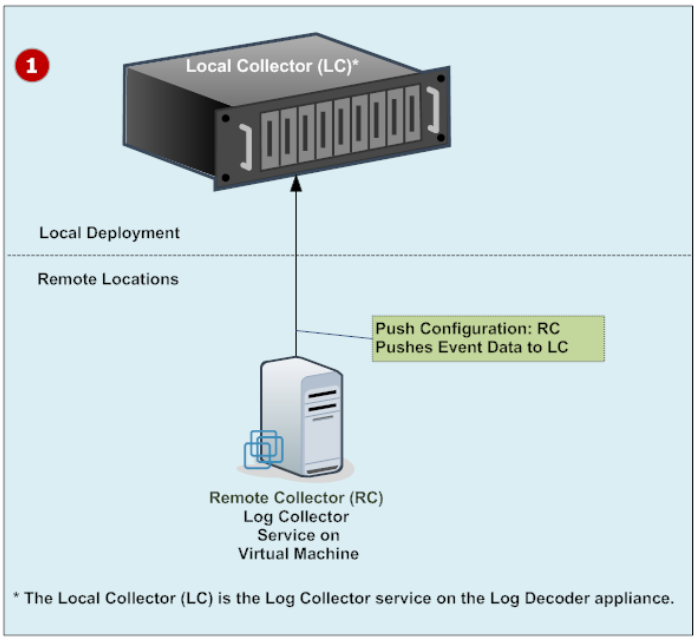
ローカルCollector(LC) は、Log Decoderホスト上で実行されるLog Collectorサービスです。ローカルへの導入シナリオでは、Log CollectorサービスはLog Decoderホスト上にLog Decoderサービスとともに導入されます。WindowsやODBCなどの各種プロトコルからのログ収集はLog Collectorサービスで実行され、イベントはLog Decoderサービスに転送されます。ローカルCollectorは、収集されたすべてのイベント データをLog Decoderサービスに送信します。

非Syslogイベントを収集するためには少なくとも1つのローカルCollectorが必要です。

リモートCollector(RC) は、スタンドアロンの仮想マシン上で実行されるLog Collectorサービスで、VLC(Virtual Log Collector) とも呼ばれます。リモートCollectorはオプションで、収集したイベントをローカルCollectorに送信する必要があります。リモートCollector導入環境は、リモートロケーションからログを収集する必要がある場合に最適です。リモートCollectorは、ログを圧縮および暗号化してからローカルCollectorに送信します。

ログ収集の導入および構成

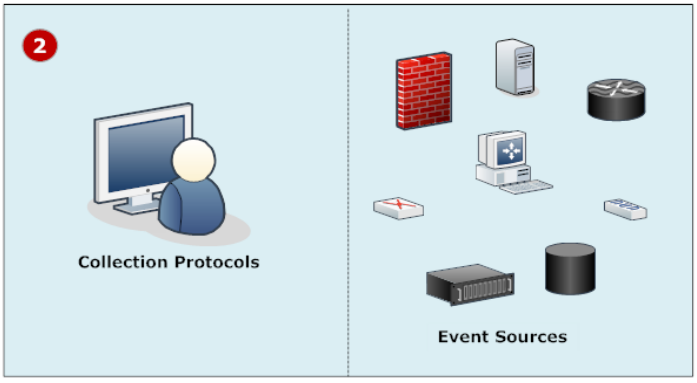
次の図に、ログ収集を導入および構成する前の基本的なタスクを示します。ログ収集を導入するには、ローカルCollectorを設定する必要があります。1つまたは複数のリモートCollectorを導入することもできます。ログ収集を導入した後は、NetWitness Suiteでイベント ソースを構成する必要があります。次の図は、ローカルCollectorと、ローカルCollectorにイベントをプッシュする1つのリモートCollectorを示しています。



1 Local CollectorとRemote Collectorを設定します。

ローカルCollectorは、Log Decoderホストで実行されているLog Collectorサービスです。

リモートCollectorは、仮想マシンまたはリモートのWindowsサーバ上で実行されるLog Collectorサービスです。



2 イベント ソースを構成します。

- NetWitness Suiteで収集プロトコルを構成します。
- 各イベント ソースとNetWitness SuiteLog Collectorの通信を構成します。

NetWitness SuiteへのローカルCollectorとリモートCollectorの追加

ローカルCollectorとリモートCollectorをNetWitness Suiteに追加するには、次の手順を実行します。

1. **[管理]＞[サービス]**に移動します。
2. +をクリックし、メニューから[**Log Collector**]を選択します。

   [**サービスの追加**]ダイアログボックスが表示されます。
3. **Log Collector**サービスの詳細を定義します。
4. [**接続のテスト**]を選択して、ローカルまたはリモートCollectorが追加されたことを確認します。

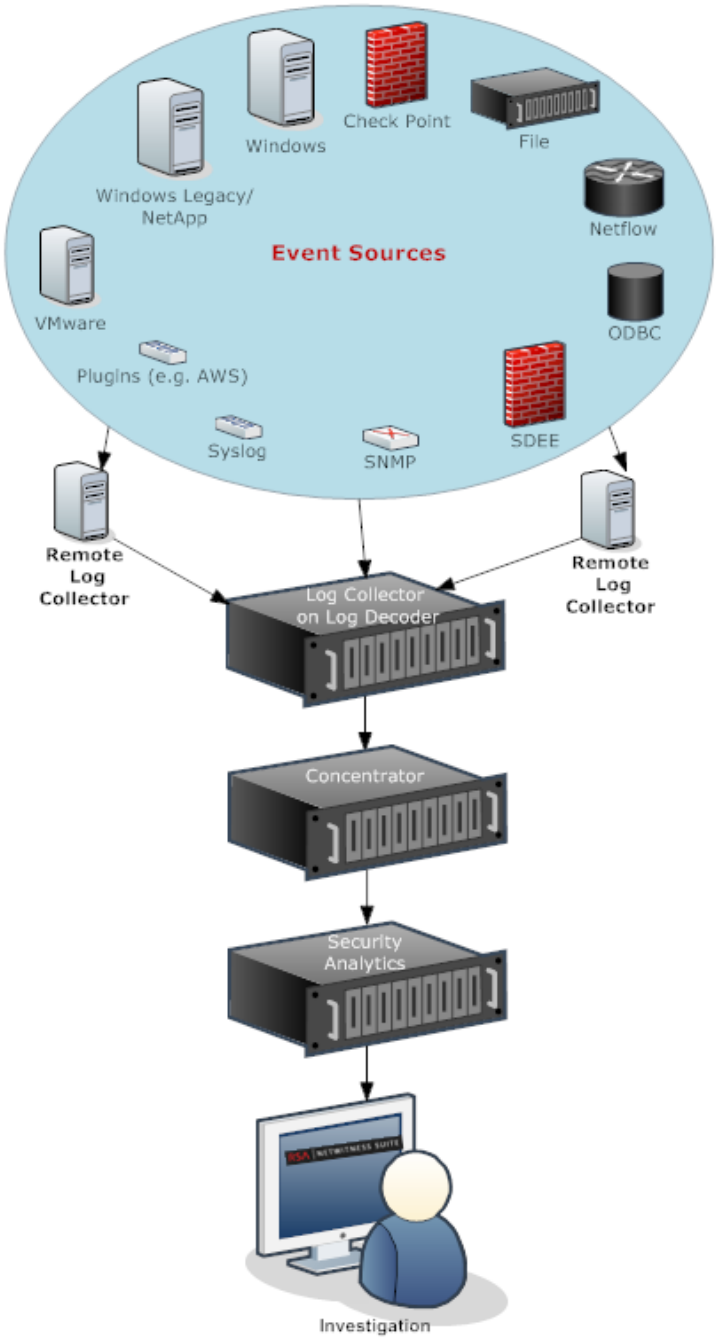
ログ収集の構成

[サービス]ビューでパラメータを定義するLog Collectorとして、ローカルCollector(LC) またはリモートCollector(RC) を選択します。次の図に、[サービス]ビューを表示し、Log Collectorサービスを選択して、サービスの構成パラメータ インタフェースを表示する方法を示します。

1. **[管理]＞[サービス]**に移動します。
2. [Log Collector]サービスを選択します。
3. [**アクション**]の下の  をクリックし、[**表示**]＞[**構成**]を選択して、ログ収集の構成パラメータのタブを表示します。
4. [**全般**]タブで、全般的なログ収集パラメータを定義します。
5. 次に、
   - ローカルCollectorの場合、NetWitness Suiteは、[**リモートCollector**]タブを表示します。このタブで、ローカルCollectorがイベントをプル受信するリモートCollectorを選択します。
   - リモートCollectorの場合、NetWitness Suiteは、[**ローカルCollector**]タブを表示します。このタブで、リモートCollectorがイベントをプッシュする先のローカルCollectorを選択します。
6. [**ファイル**]タブで、構成ファイルをテキスト ファイルとして編集します。
7. [**イベント ソース**]タブで、収集プロトコル パラメータを定義します。
8. [設定]タブで、Lockbox、暗号化キー、証明書を定義します。
9. [**Applianceサービス構成**]タブで、Applianceサービスのパラメータを定義します。

データフロー図

Log Collectorサービスによって収集されたログデータを使用して、組織内のシステムの稼働状態の監視および調査を実施します。次の図は、NetWitness Suiteのログ収集からInvestigation (調査) までのデータフローを示しています。



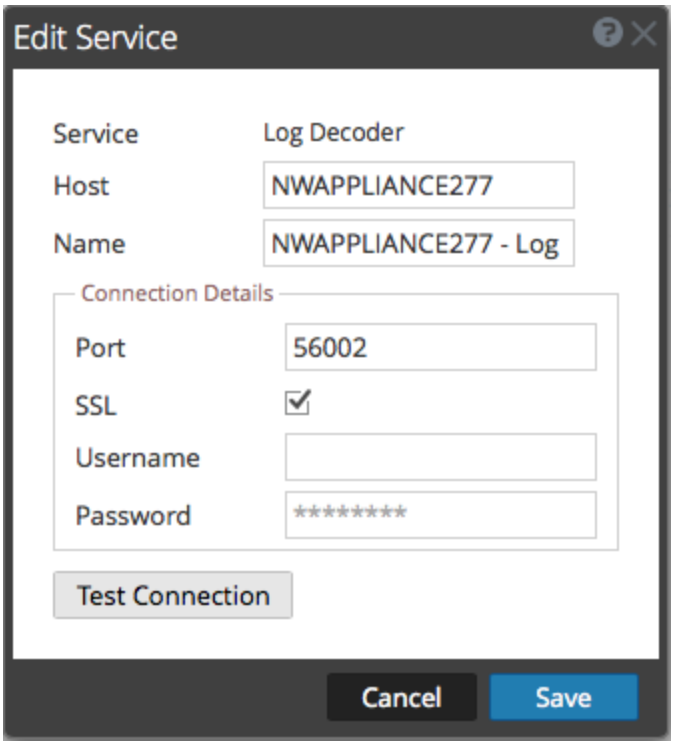
ローカルCollectorおよびリモートCollectorのプロビジョニング

NetWitness Suiteサーバは、アプライアンスにLog Decoderサービスがあるかどうかを確認します。Log Decoderサービスがある場合、ローカルCollectorになります。Log Decoderサービスがない場合、リモートCollectorになります ローカルLog Collectorにはイベントの宛先があり、デフォルトでローカルLog Decoderサービスになります。リモートCollectorにはイベントの宛先はありません。NWサーバサーバはLegacy Windows Collectorをリモートとして識別します。

ローカルCollectorまたはリモートCollectorを編集するには、次の手順を実行します。

1. **[管理]**>**[サービス]**に移動します。
2. [**サービス**]ビューで、ツールバーのを選択します。

   [**サービスの編集**]ダイアログが表示されます。



3. [**サービスの編集**]ダイアログで、次の情報を指定します。

フィールド	説明
サービス	サービスのタイプとしてLog Collectorを選択します。
ホスト	Log Decoderホストを選択します。
名前	サービスに割り当てる名前を入力します。

フィールド	説明
ポート	デフォルト ポートは、平文の場合は50001、SSL暗号化の場合は56001です。
SSL	NetWitness Suiteとホストの通信にSSLを使用する場合は、[**SSL**]を選択します。暗号化とSSL証明書による認証によってデータ転送のセキュリティが実装されます。
ユーザ名(オプション)	ローカルCollectorのユーザ名を入力します。
パスワード(オプション)	ローカルCollectorのパスワードを入力します。

4. NetWitness Suiteからサービスへの接続を確認するには、[**接続のテスト**]をクリックします。
5. テストに成功したら、[**保存**]をクリックします。

   テストが失敗した場合は、サービスの情報を編集し、再試行します。

ローカルCollectorおよびリモートCollectorの構成

このトピックでは、ローカルCollectorおよびリモートCollectorを構成する方法について説明します。

ログ収集を導入する場合、各種イベント ソースからログ イベントを収集するようにLog Collectorを構成する必要があります。Log Collectorを構成することで、これらのイベントをLog Decoderホストに安全かつ確実に配信できます。配信されたイベントはホストでパースされ、今後の解析のために保存されます。

イベント データをローカルCollectorにプッシュするように1つ以上のリモートCollectorを構成するか、あるいは1つ以上のリモートCollectorからイベント データをプル受信するようにローカルCollectorを構成することができます。

このトピックでは、以下の項目について説明します。

- リモートCollectorからイベントをプル受信するためのローカルCollectorの構成
  リモートCollectorからローカルCollectorのイベントをプル受信する場合、ローカルCollectorの[構成]ビューにある[リモートCollector]タブで設定を行います。
- ローカルCollectorにイベントをプッシュするためのリモートCollectorの構成
  リモートCollectorからローカルCollectorにイベントをプッシュする場合、リモートCollectorの[構成]ビューにある[ローカルCollector]タブで設定を行います。プッシュ構成では、次の内容も構成できます。

- リモートCollectorでのフェールオーバーローカルCollectorの構成

  ローカルCollectorで構成される宛先を設定します。 プライマリローカルCollectorに接続できない場合、リモートCollectorは、宛先内の各ローカルCollectorに対して、成功するまで接続を試行します。

- レプリケーションの構成

  複数の宛先グループへのレプリケーションを設定します。これにより、NetWitnessは、各グループにイベント データをレプリケートします。宛先グループの1つに接続できない場合でも、他の宛先グループにデータがレプリケートされている場合、必要なデータをリカバリできます。

- 特定のプロトコルのログ ルーティングの構成

  プロトコル タイプに応じて特定のロケーションにイベント データを転送する、宛先グループ内の複数の宛先を設定します。

- リモートCollectorのチェーンの構成

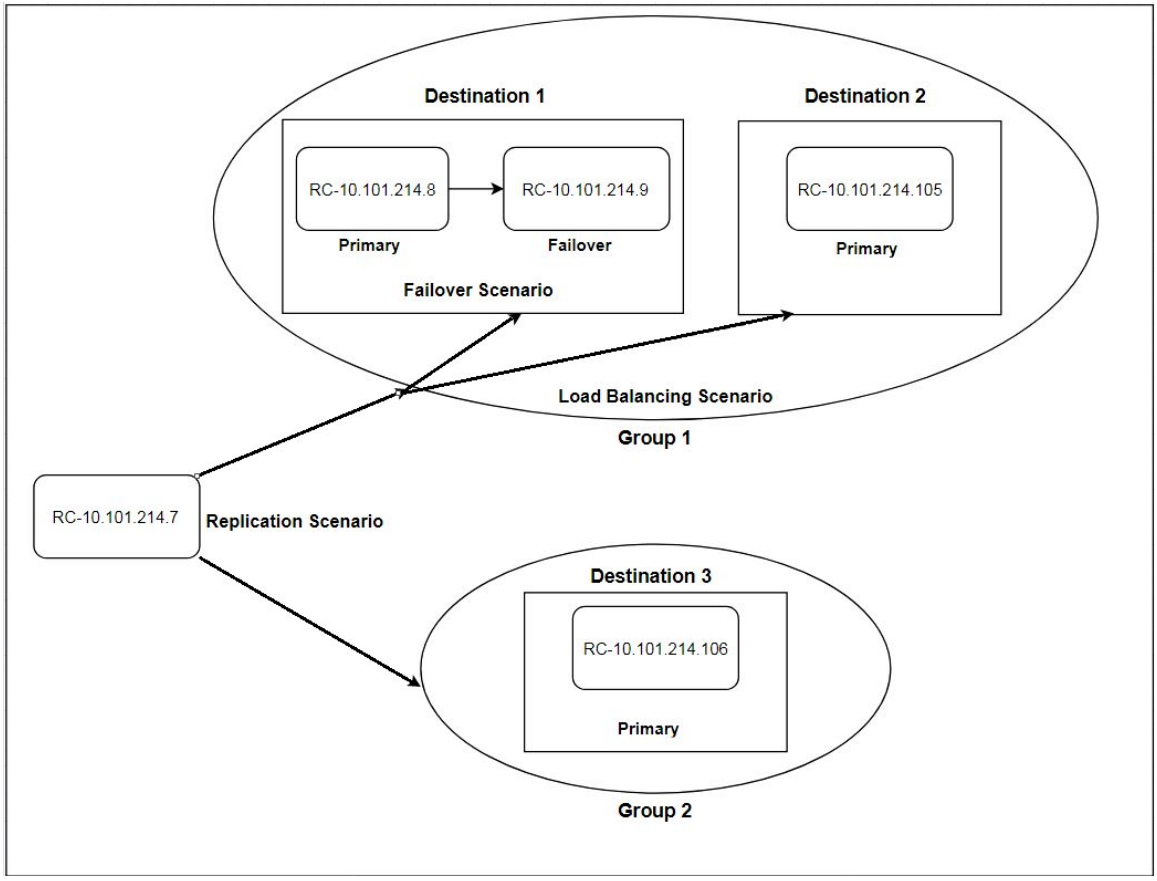
  イベント データをローカルCollectorにプッシュするように1つ以上のリモートCollectorを構成するか、1つ以上のリモートCollectorからイベント データをプル受信するようにローカルCollectorを構成することができます。

  - 1つのリモートCollectorにイベント データをプッシュする1つ以上のリモートCollector。
  - 1つ以上のリモートCollectorからイベント データをプル受信する1つのリモートCollector。

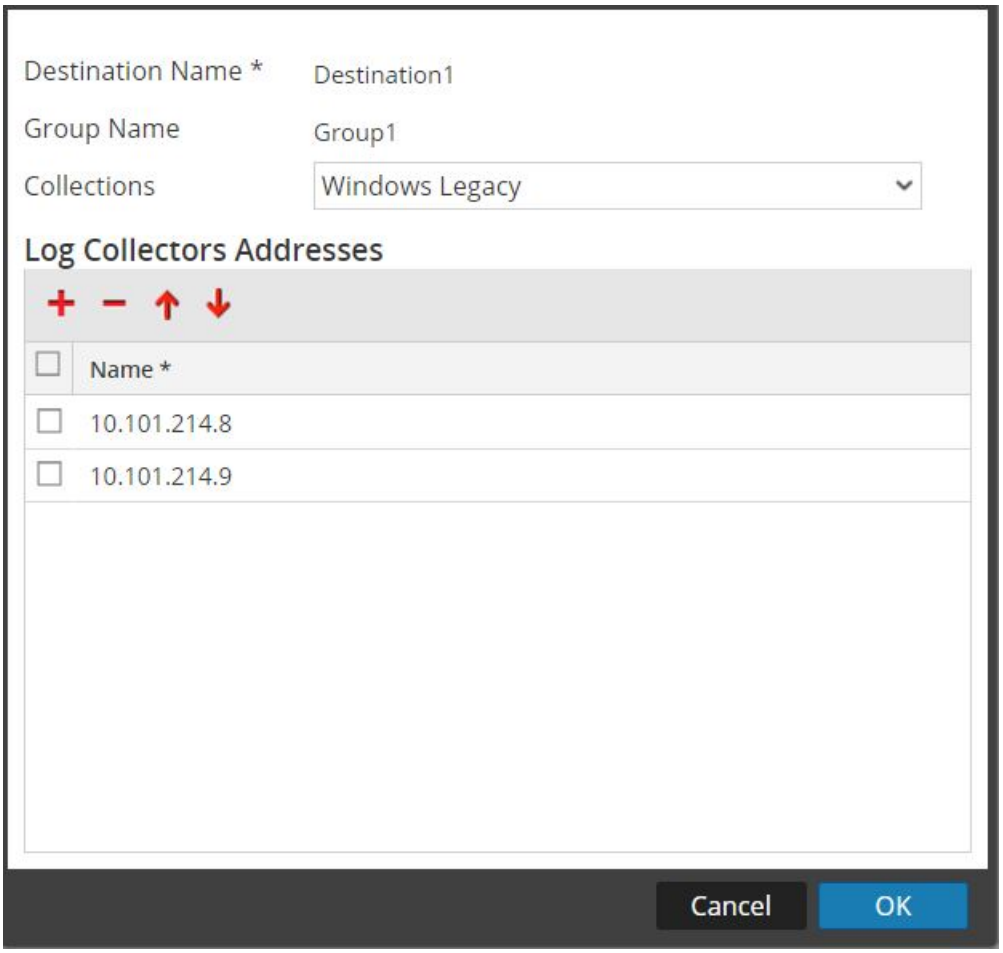
フェールオーバー、レプリケーション、ロード バランシング

このセクションでは、RSA NetWitness Suiteでのフェールオーバー、レプリケーション、ロード バランシングの動作方法について説明します。

次の図は、ロード バランシング、フェールオーバー、レプリケーション用に構成されたリモートCollectorを示しています。

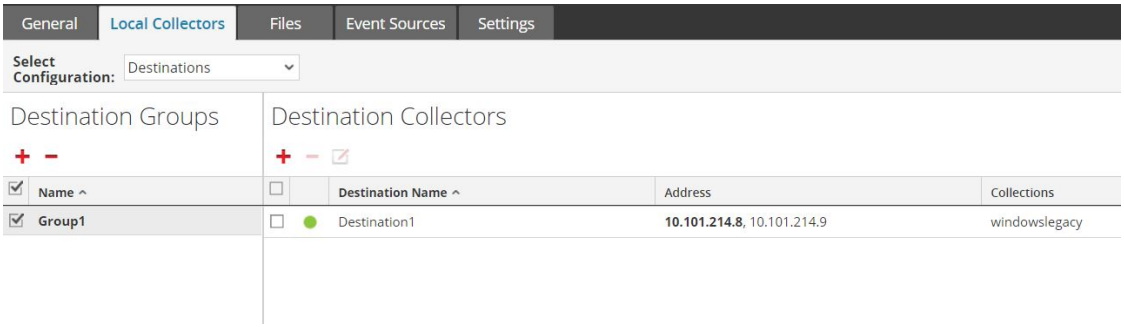


- **フェールオーバー**は、同じ宛先に複数のコレクターを設定することで実現されます。宛先1には、プライマリコレクターと、2番目のフェールオーバー コレクターがあります。これは、NetWitness Suiteで複数のLog Collectorを同じ宛先に追加することで実行されます。



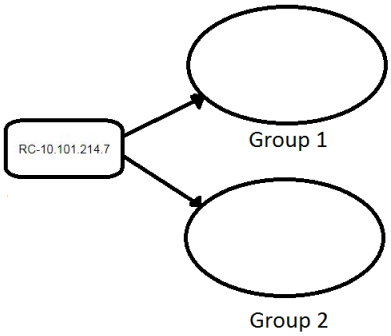
10.101.214.8が最初に表示されているため、これがプライマリコレクターとなり、10.101.214.9はフェールオーバーとなります。10.101.214.9をプライマリにするには、上矢印を使用して順序を変更します。

以下では、2つのコレクターの両方が宛先1の一覧に表示されていることが分かります。プライマリ(10.101.214.8) は、太字で表示されています。

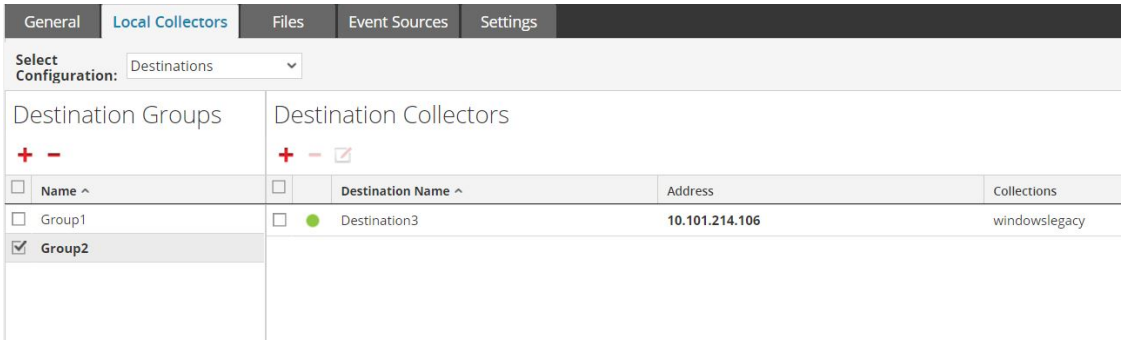


- **レプリケーション**は、複数の宛先グループを設定することで実現されます。各グループには、

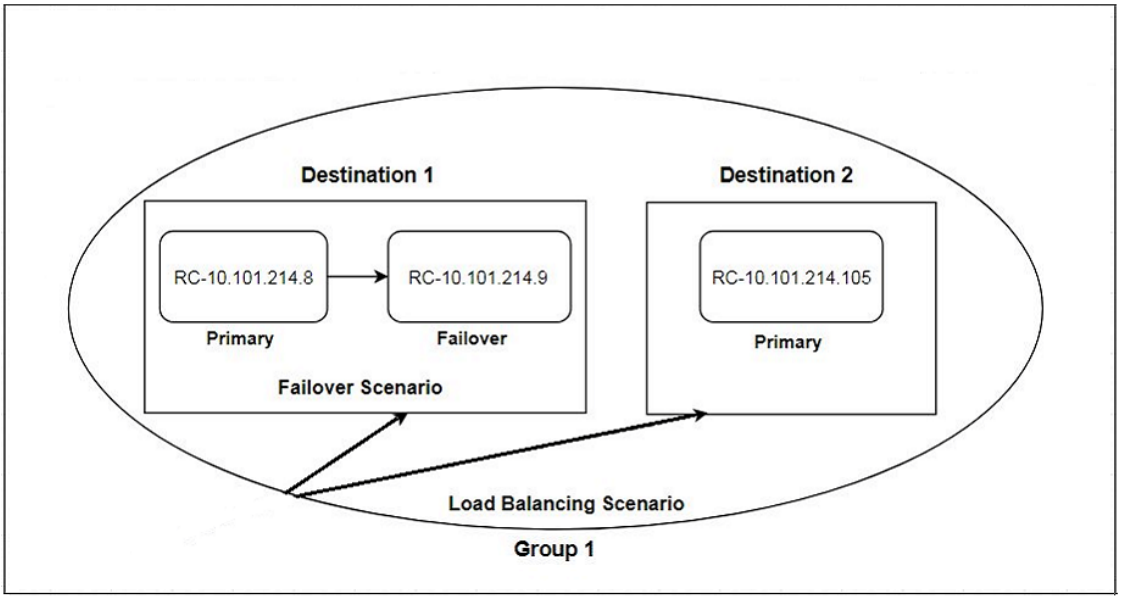
メッセージ データのセット全体があります。



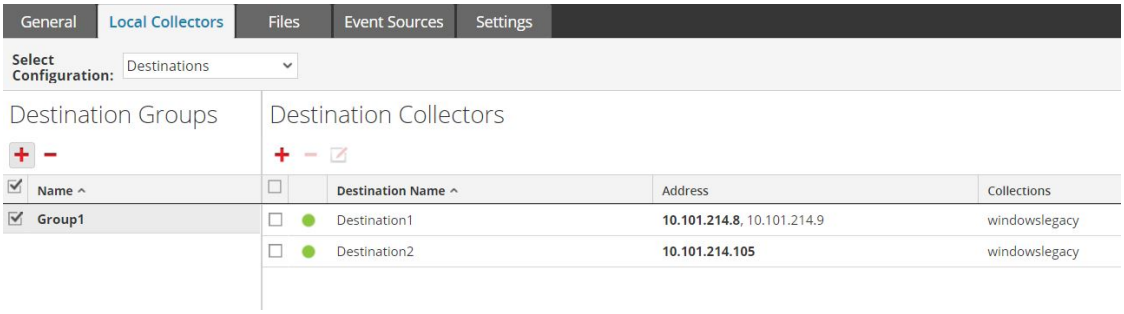
次の画面では、メッセージ データがグループ1とグループ2のコレクターに送信されていることが分かります。



- **ロード バランシング**は、1つのグループ内に複数の宛先を設定することで実現されます。



次の画面では、グループ1が、宛先1および宛先2の2つの宛先を持つことが分かります。メッセージ データは、グループ内の宛先間で均等に分割されます。



宛先が2つの場合、各宛先は、メッセージ データの半分を使用します。宛先が3つの場合、全メッセージ データの3分の1を使用します。宛先を追加し続けると、各宛先のコレクターに対する負荷がさらに削減されます。

注：特定のプロトコルのイベント データが特定の宛先に送信されるようにログのルーティングを設定することもできます。

ローカルCollectorまたはリモートCollectorの構成

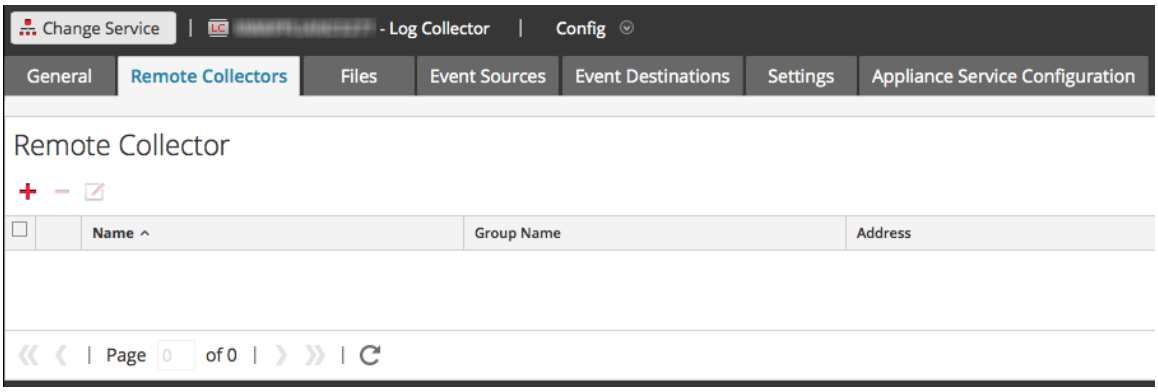
[サービス]ビューで導入パラメータの定義の対象となるLog Collector(ローカルCollectorまたはリモートCollector) を選択します。次の手順は、[サービス]ビューのナビゲーション方法、ローカルCollectorまたはリモートCollectorの選択方法、サービスの導入パラメータ インタフェースの表示方法を示しています。

ローカルCollectorまたはリモートCollectorを構成するには、次の手順を実行します。

1. **管理＞[サービス]**に移動します。
2. [Local Log Collection]または[Remote Log Collection]サービスを選択します。
3. [アクション]で、⚙＞**[表示]＞[構成]**を選択して、ログ収集の構成パラメータのタブを表示します。
4. ステップ2での選択内容に応じて
   - ローカルCollectorを選択した場合、[**リモートCollector**]タブが表示されます。このタブで、ローカルCollectorがイベントをプル受信するリモートCollectorを選択します。
   - リモートCollectorを選択した場合、[**ローカルCollector**]が表示されます。このタブで、リモートCollectorがイベントをプッシュする先のローカルCollectorを選択します。

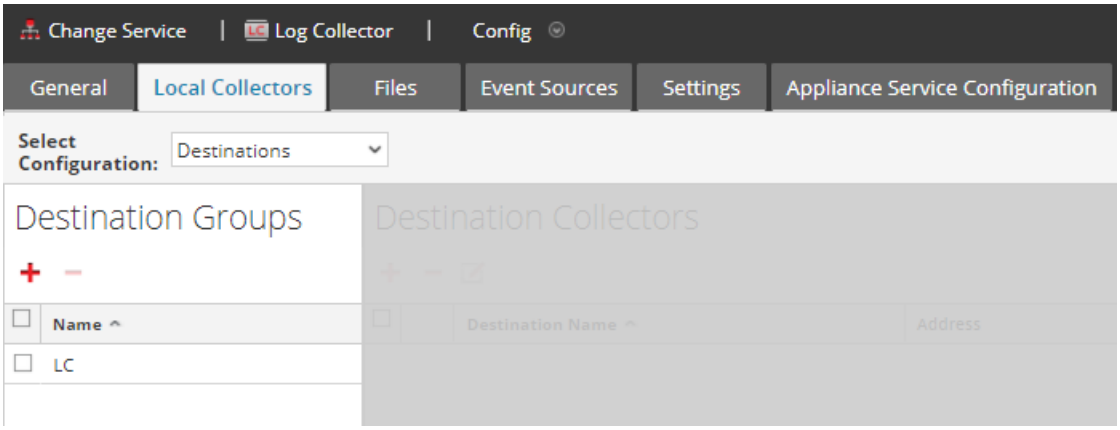
[リモートCollector]タブ

次の図は、ローカルCollectorで[**リモートCollector**]タブを設定し、リモートCollectorからイベントをプル受信する構成を示しています。**[管理]＞[サービス]**でローカルCollectorを選択した場合に、このタブがNetWitness Suiteに表示されます。

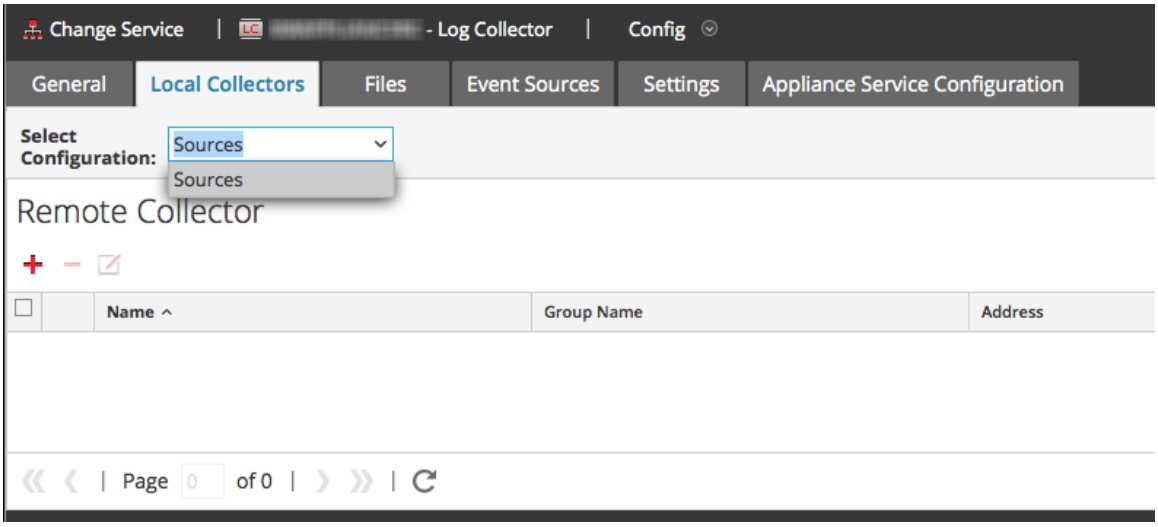


リモートCollectorの[ローカルCollector]タブ

次の図は、リモートCollectorの[**ローカルCollector**]タブを設定し、ローカルCollectorまたは別のリモートCollectorにイベントをプッシュする構成を示しています。



次の図は、リモートCollectorで[リモートCollector]タブを設定し、リモートCollectorからイベントをプル受信する構成を示しています。[**管理**]>[**サービス**]でリモートCollectorを選択した場合に、このタブがNetWitness Suiteに表示されます。



パラメータ

「 リモートCollector/ローカルCollectorの構成パラメータ 」

フェールオーバーローカルCollectorの構成

このトピックでは、リモートCollectorでフェールオーバー ローカルCollectorまたはリモートCollectorを設定する方法について説明します。

フェールオーバー ローカルCollectorの設定

プライマリ ローカルCollectorが何らかの理由でダウンした場合にRSA NetWitness® Suiteが代わりに使用するフェールオーバー ローカルCollectorを設定することができます。

1. **[管理]＞[サービス]**に移動します。
2. [**サービス**]で、リモートCollectorサービスを選択します。
3. [**アクション**]の下の をクリックし、**[表示]＞[構成]**を選択します。

   [サービス]の[構成]ビューが表示され、[**Log Collector全般**]タブが開きます。
4. [**ローカルCollector**]タブを選択します。
5. [**宛先グループ**]パネル セクションで、 を選択します。

   [リモートの宛先の追加]ダイアログが表示されます。
6. 宛先グループを設定し、プライマリ ローカルCollectorを選択します(**LC-PRIMARY**など) 。
7. [宛先グループ]パネルでグループ(**Primary_Standby_LCs**など) を選択し、 をクリックします。

   選択したグループが[ローカルCollector]パネルに表示されます。
8. フェールオーバー ローカルCollectorを追加します(**LC-STANDBY**など) 。

   次の例は、新たに追加されたプライマリとフェールオーバーのローカルCollectorを示しています。プライマリ ローカルCollectorが[**アクティブ**]として、フェールオーバー ローカルCollectorが[**スタンバイ**]として表示されています。アクティブなローカルCollector(**LC-PRIMARY**など) がハイライト表示されます。
9. (オプション) それぞれのリモートの宛先に対し、ローカルCollectorを追加するか、削除するか、その順序を変更します。

   a. をクリックして、Log Collectorをリモートの宛先のフェールオーバーとして追加します。

   b. リモートの宛先に接続するとき、リモートCollectorは、リスト内の各ローカルCollectorに対し、接続に成功するまで上から順に接続を試行します。

c. 接続の順序を変更するには、ローカルCollectorを選択し、(上下の矢印ボタン) を使用します。

d. リストから削除するには、ローカルCollectorを1つ以上選択し、 をクリックします。

選択したローカルCollectorが[Log Collector]セクションに追加されます。リモートCollectorがデータの収集を開始すると、これらのLog Collectorにデータをプッシュします。

フェールオーバー リモートCollectorの設定

プライマリリモートCollectorが何らかの理由でダウンした場合にRSA NetWitness® Suiteが代わりに使用するフェールオーバー リモートCollectorを設定することができます。

1. **[管理]＞[サービス]**に移動します。
2. [**サービス**]で、リモートCollectorサービスを選択します。
3. [**アクション**]の下の をクリックし、**[表示]＞[構成]**を選択します。

   [サービス]の[構成]ビューが表示され、[**Log Collector全般**]タブが開きます。
4. [**ローカルCollector**]タブを選択します。
5. [**構成の選択**]ドロップダウン メニューで[**ソース**]を選択します。
6. をクリックして[**ソースの追加**]ダイアログを表示します。
7. フェールオーバー用リモートCollectorを定義して、[**OK**]をクリックします。

パラメータ

「 リモートCollector/ローカルCollectorの構成パラメータ 」

レプリケーションの構成

このトピックでは、リモートCollectorから送信するイベント データをレプリケートする方法について説明します。

複数の宛先グループを指定すると、各グループにイベント データをレプリケートできます。

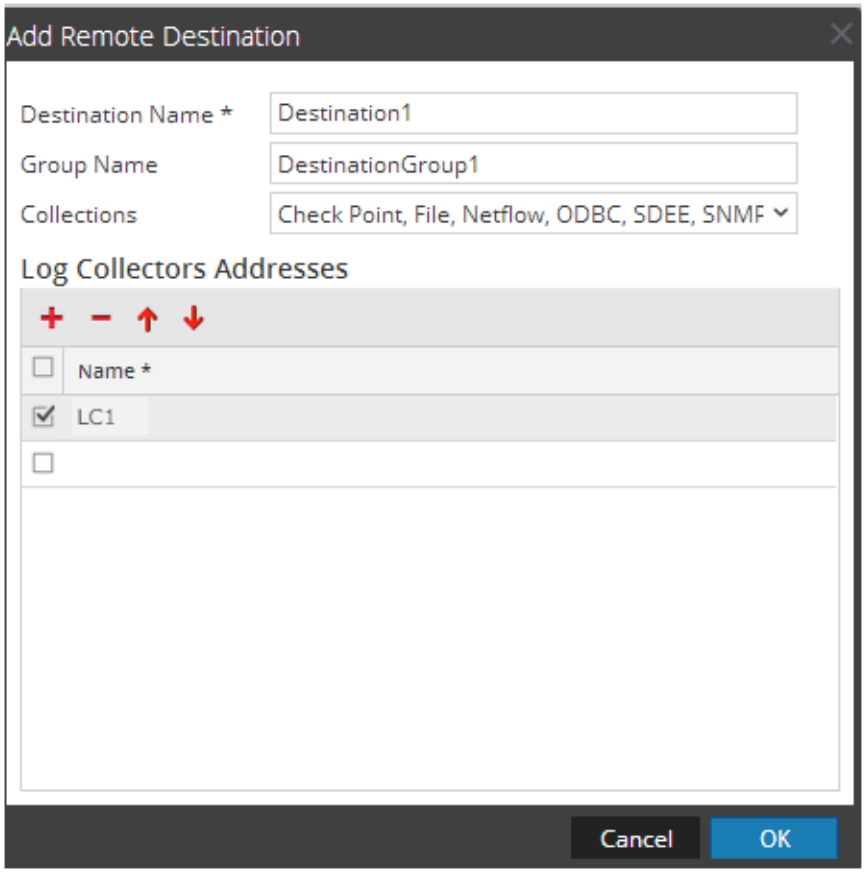
複数のローカルCollectorにイベント データをレプリケートするには、次の手順を実行します。

1. **[管理]＞[サービス]**に移動します。
2. リモート ログ収集サービスを選択します。
3. [アクション]で、 **＞[表示]＞[構成]**を選択します。

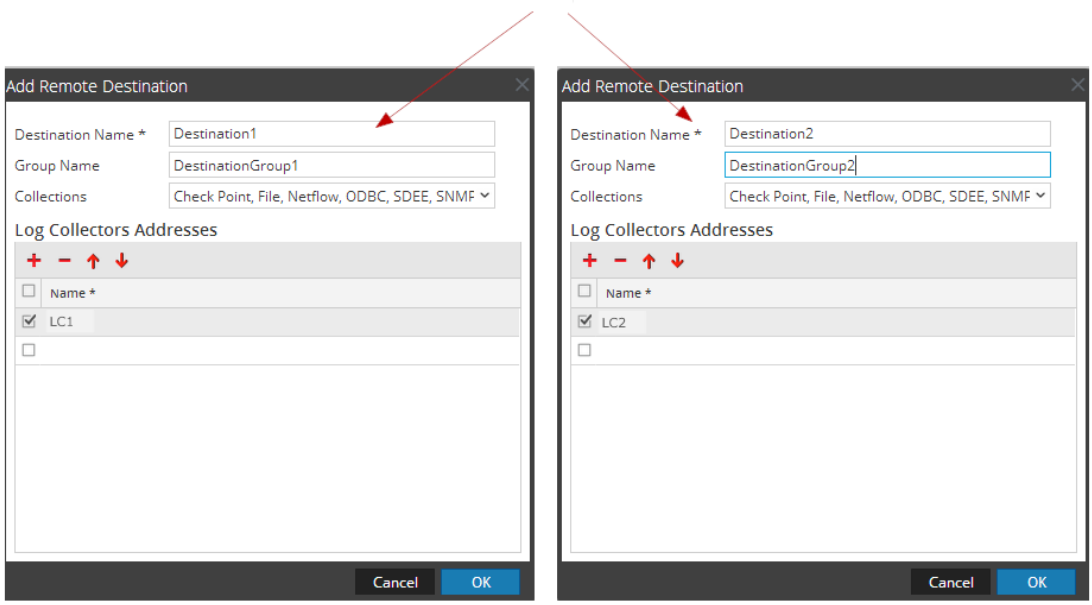
   [サービス]の[構成]ビューが表示され、[**Log Collector全般**]タブが開きます。
4. [**ローカルCollector**]タブを選択します。
5. [**宛先グループ**]パネル セクションで、

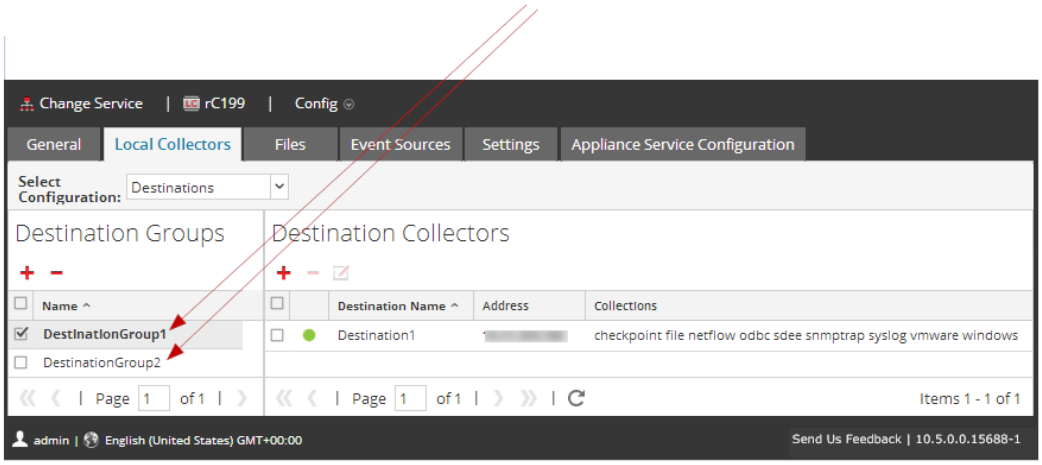
+をクリックします。

[**リモートの宛先の追加**]ダイアログが表示されます。



6. ローカルCollectorごとに個別の宛先を設定し、対象のローカルCollectorにイベント メッセージをプッシュするプロトコルを指定します。次の例は、**Check Point**、**ファイル**、**Netflow**、**ODBC**、**SDEE**、**SNMP**、**Syslog**、**Windows**の各収集プロトコルを指定して2つの宛先ローカルCollector(**Destination1**および**Destination2**) を追加する方法を示しています。





a. [**宛先名**]に名前を入力します。

b. [**グループ名**]に名前を入力します。グループ名を入力しない場合は、宛先名がグループ名として使用されます。

c. ドロップダウンリストで収集プロトコルを選択します。

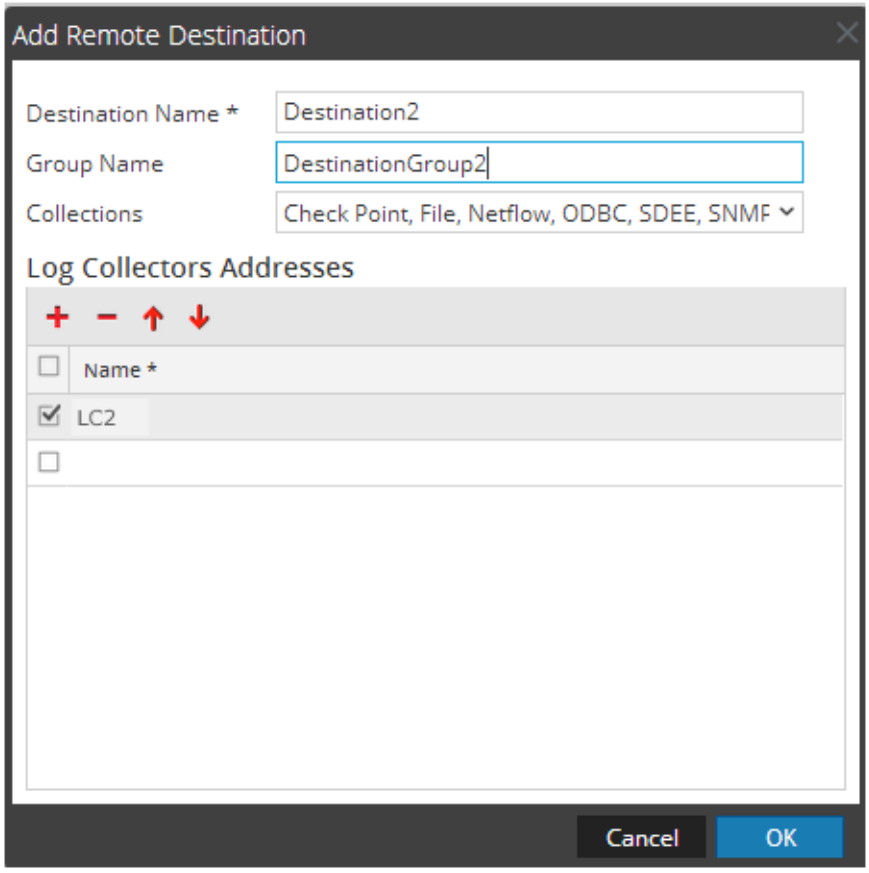
d. ローカルCollectorを選択します(**LC1**など) 。

e. [**OK**]をクリックします。

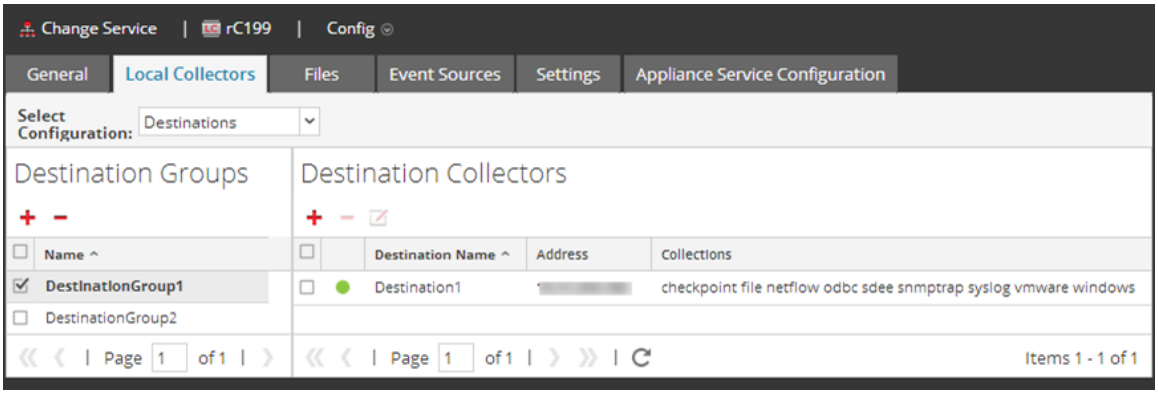
f. [**宛先グループ**]パネルで新しいグループ(**DestinationGroup2**など) を選択し、[**ローカルCollector**]パネルで＋をクリックします。

g. [**ローカルCollector**]パネルで、＋をクリックし、次の図に示すとおり[**リモートの宛先の追**

加]ダイアログを完了します。



Check Point、ファイル、Netflow、ODBC、SDEE、SNMP、Syslog、Windowsの各収集プロトコルが2つのローカルCollector(**LC1**および**LC2**) に送信されます。両方のローカルCollectorがアクティブになり、イベント データを収集します。



リモートCollectorのチェーンの構成

このトピックでは、リモートCollector(VLCとも呼ばれます) のチェーンを設定する方法について説明します。

イベント データをリモートCollectorにプッシュするように1つ以上のリモートCollectorを設定するか、1つ以上のリモートCollectorからイベント データをプル受信するようにリモートCollectorを構成することができます。

- **データをプッシュするリモートCollector。**リモートCollectorから他のリモートCollectorまたはローカルCollectorにデータをプッシュします。
- **データをプル受信するリモートCollector。**1つのリモートCollectorを使用して、1つ以上のリモートCollectorからデータをプル受信します。

イベント データをリモートCollectorにプッシュ送信するためのリモートCollectorの構成

リモートCollectorは、リモートCollectorにイベント データをプッシュ送信するように構成できます。

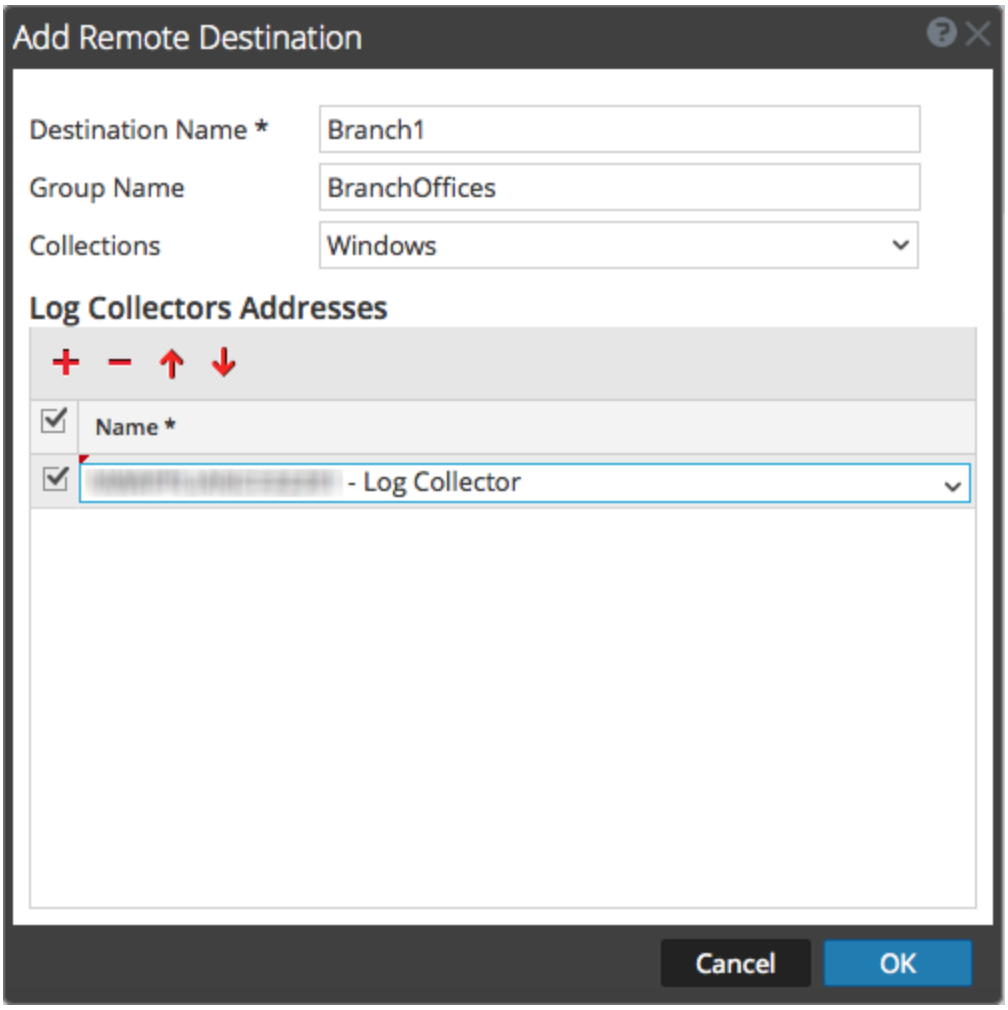
指定したリモートCollectorにイベントをプッシュ送信するようにリモートCollectorを構成する

1. **[管理]＞[サービス]**に移動します。
2. [**サービス**]で、**リモートCollector**を選択します。
3. [アクション]で、  **＞[表示]＞[構成]**を選択して、ログ収集に関する構成パラメータのタブを表示します。

   Log Collector[サービス]の[構成]ビューが表示され、[**Log Collector全般**]タブが開きます。
4. [**ローカルCollector**]タブを選択します。
5. [**構成の選択**]ドロップダウン メニューで[**宛先**]を選択します。
6. [**宛先グループ**]パネル セクションで、  を選択します。

   [**リモートの宛先の追加**]ダイアログが表示されます。
7. 次の手順で**宛先グループ**を設定します。
   a. **宛先名**を入力します。
   b. (オプション) **グループ名を入力します**。グループ名を空白にした場合、[宛先名]に指定した値がNetWitness Suiteによって設定されます。
   c. [**コレクション**]ドロップダウン リストから、1つ以上の収集プロトコルを選択します。

d. [**Log Collectorのアドレス**]で+をクリックし、リモートCollectorを選択します。



注:収集プロトコルを選択しなかった場合、リモートCollectorは、すべての収集プロトコルをリモートCollectorにプッシュ送信します。

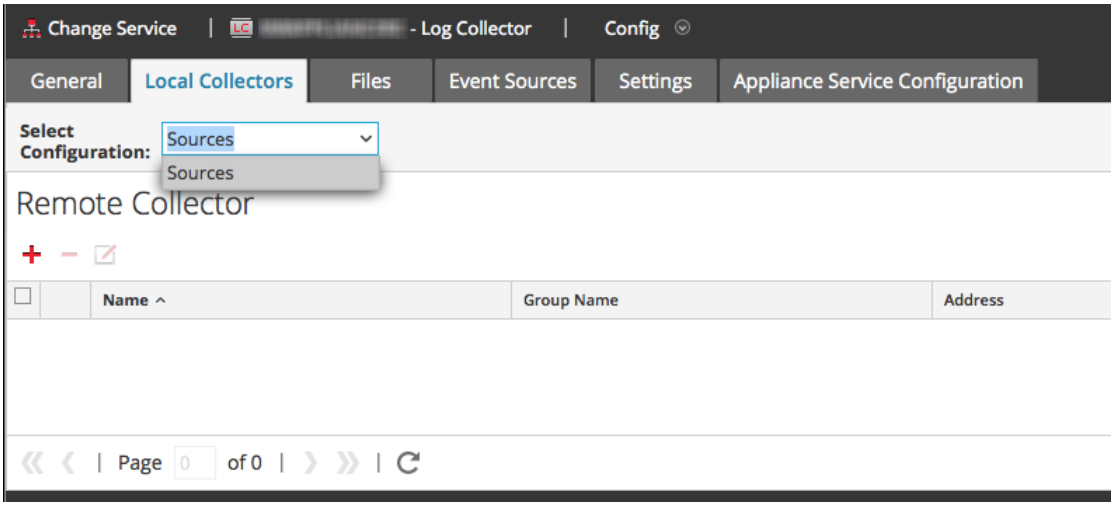
イベント データをリモートCollectorからプル受信するためのリモートCollectorの構成

指定したリモートCollectorからイベントをプル受信するように、選択したリモートCollectorを構成

1. [**管理**]>[**サービス**]に移動します。
2. [**サービス**]で、**リモートCollector**を選択します。
3. [アクション]で、⚙>[**表示**]>[**構成**]を選択して、ログ収集に関する構成パラメータのタブを表示します。

   [**サービス**]の[**構成**]ビューが表示され、[**Log Collector全般**]タブが開きます。
4. [**ローカルCollector**]タブを選択します。

5. [**構成の選択**]ドロップダウン メニューで[**ソース**]を選択します。



6. [**リモートCollector**]パネルで、**+**を選択します。

   [**ソースの追加**]ダイアログが表示されます。

7. [**ソースの追加**]ダイアログで、次の手順を実行します。

   a. 1つ以上の収集プロトコルを選択します。
   収集プロトコルを選択しなかった場合、リモートCollectorは、すべての収集プロトコルをリモートCollectorからプル受信します。

   b. [**OK**]をクリックします。

   [リモートCollector]セクションにリモートCollectorが追加されます。Log Collectorがデータの収集を開始すると、このリモートCollectorからイベント データがプルされます。

リモートCollectorのローカルCollector帯域幅へのスロットリング

イベント データ送信時の帯域幅を調節し、リモートCollectorからローカルCollectorへの送信時や、Message Broker間での送信時の速度を制御して、パフォーマンスを改善できます。帯域幅の調整を設定するには、Linuxのカーネルのフィルタリングとiptables機能を構成します。

この機能は、プッシュ型とプル型の両方のリモートCollector構成で使用できます。**/opt/netwitness/bin**にある**set-shovel-transfer-limit.sh**シェル スクリプトにより、使用するポートに関係するiptableとカーネル フィルタの構成を自動化できます。

このトピックでは、**set-shovel-transfer-limit.sh**シェル スクリプトを使用してリモートCollectorをローカルCollector帯域幅にスロットリングする方法を説明します。次のセクションで構成されています。

- **set-shovel-transfer-limit.sh**シェル スクリプトコマンド ライン ヘルプ。

  注：設定する必要があるフィルタ値は、リモートLog Collectorがイベントをローカルcollectorに送信するレートによって異なります。

- フィルタを4,096 kbpsに設定する例。

Set Shovel Transfer Limitスクリプトのコマンド ライン ヘルプ

`-h`コマンドを発行し、`set-shovel-transfer-limit.sh` シェル スクリプトのヘルプを表示します。

```
cd /opt/netwitness/bin
./set-shovel-transfer-limit.sh
```

使用法：

```
code>set-shovel-transfer-limit.sh -s|-c|-d|[-i interface] [-r
rate]
```

各項目の意味は次のとおり。

- -c = clear existing
- -d = display filter
- -s = set new values
- -i = interfaceはネットワーク インタフェースの名前。デフォルト値は**eth0**
- -r = rateは帯域幅速度。デフォルト値は**256kbps**

帯域幅およびレートは以下の単位で指定できます。

- **nolimit**：スロットリングを無効にする
- **kbit**：1秒あたりのキロビット数
- **mbit**：1秒あたりのメガビット数
- **kbps**：1秒あたりのキロバイト数
- **mbps**：1秒あたりのメガバイト数
- **bps**：1秒あたりのバイト数

フィルタを4,096 kbpsに設定

この例ではフィルタを4,096 kbpsに設定します。

```
[root@<hostname> bin]# ./set-shovel-transfer-limit.sh -s -r
4096kbit
```

```
RATE=4096kbit
 PORTNUMBER=5671
 DEVICE_INTERACE=eth0

iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK
]

Current/new values...

iptables -t mangle -n -v -L
 Chain PREROUTING (policy ACCEPT 2 packets, 161 bytes)
 pkts bytes target  prot opt in  out  source
destination

Chain INPUT (policy ACCEPT 2 packets, 161 bytes)
 pkts bytes target prot opt in out   source          destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target prot opt in out   source          destination

Chain OUTPUT (policy ACCEPT 2 packets, 248 bytes)
 pkts bytes target prot opt in out   source          destination
     0    0 MARK   tcp -- *    eth0     0.0.0.0/0     0.0.0.0/0
multiport dports 5671 MARK set 0xa
     0    0 MARK   tcp -- *    eth0     0.0.0.0/0    0.0.0.0/0
multiport sports 5671 MARK set 0xa

Chain POSTROUTING (policy ACCEPT 2 packets, 248 bytes)
 pkts bytes target prot opt in out   source          destination

tc -s -d class show dev eth0
 class htb 1:1 root rate 10000Kbit ceil 10000Kbit burst 1600b/8
mpu 0b overhead 0b cburst 1600b/8 mpu 0b overhead 0b level 7
 Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
 lended: 0 borrowed: 0 giants: 0
 tokens: 20000 ctokens: 20000

class htb 1:2 parent 1:1 prio 0 quantum 51200 rate 4096Kbit ceil
4096Kbit burst 1599b/8 mpu 0b overhead 0b cburst 1599b/8 mpu 0b
overhead 0b level 0
 Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
 lended: 0 borrowed: 0 giants: 0
 tokens: 48828 ctokens: 48828
```

Lockbox設定

このトピックでは、Lockboxのセキュリティ設定を構成する方法について説明します。

Lockboxとは

Lockboxは、アプリケーションに関連する機密情報を格納するために使用される暗号化ファイルです。NetWitness Suite Lockboxには、Log Collectorの暗号化キーが格納されます。

暗号化キーは、すべてのイベント ソース パスワードとイベント ブローカー パスワードを暗号化するために使用されます。

Lockboxを作成するとき、Lockboxのパスワードを定義する必要があります。

データの収集中、Log Collectorはユーザによるパスワードの指定が不要なモードでLockboxを運用します(Log Collectorは代わりにホスト システムのフィンガープリントを使用します) 。

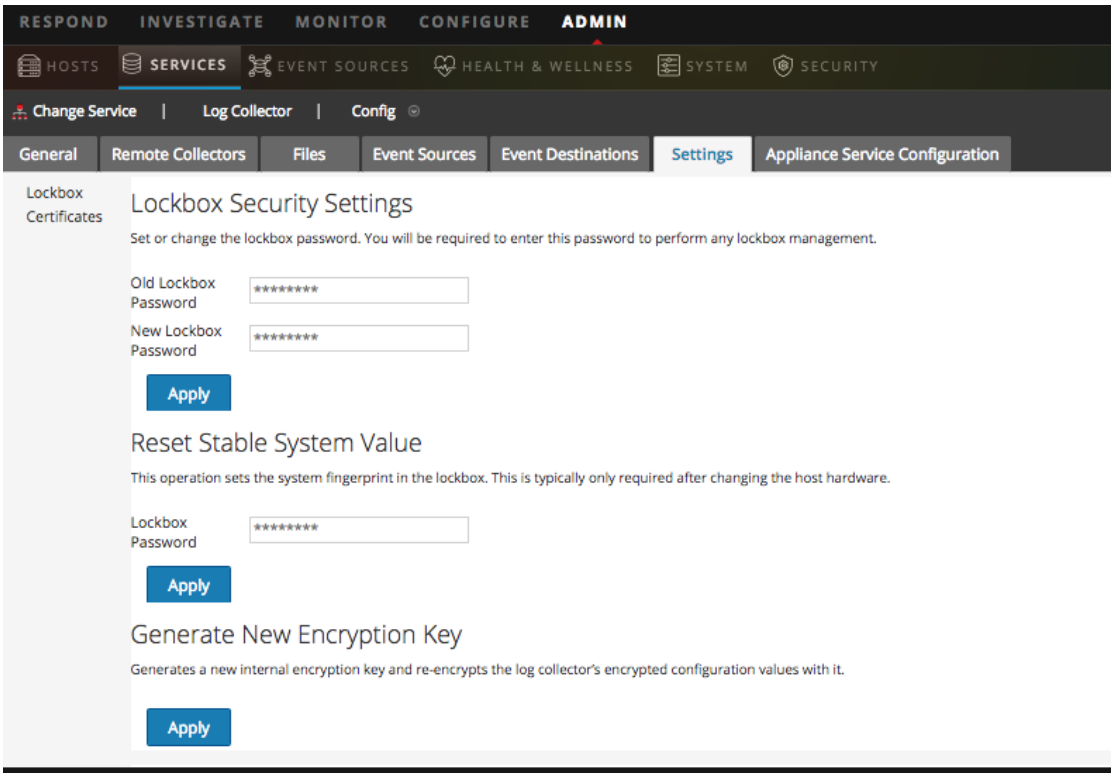
Lockboxのセキュリティ設定は次のとおりです。

機能	説明
古いLockboxのパスワード	初めてLockboxを設定する場合、このフィールドは空白です。NetWitness Suiteは、[新しいLockboxのパスワード]に入力して[適用]をクリックした後、このフィールドに値を表示します。
新しいLockboxのパスワード	新しいLockboxのパスワードです。Lockboxのセキュリティを最大限に高めるために、パスワードの長さを8文字以上にして、数字、大文字、#や!などの記号を少なくとも1つ含めます。
適用	[**適用**]をクリックして、Lockboxのパスワードを保存します。

Lockbox設定

Lockboxを設定するには、次のようにパスワードを設定する必要があります。

1. [**管理**]＞[**サービス**]に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、＞[**表示**]＞[**構成**]を選択して、ログ収集に関する構成パラメータのタブを表示します。
4. [**設定**]タブをクリックします。



5. オプション パネルで、[**Lockbox**]を選択してLockboxの設定を構成します。
6. [**Lockboxのセキュリティ設定**]で、[**新しいLockboxのパスワード**]フィールドにパスワードを入力し、[**適用**]をクリックします。

収集サービスの開始

収集サービスが停止したときは、再度開始することが必要な場合があります。また、収集サービスの自動開始を有効化することもできます。

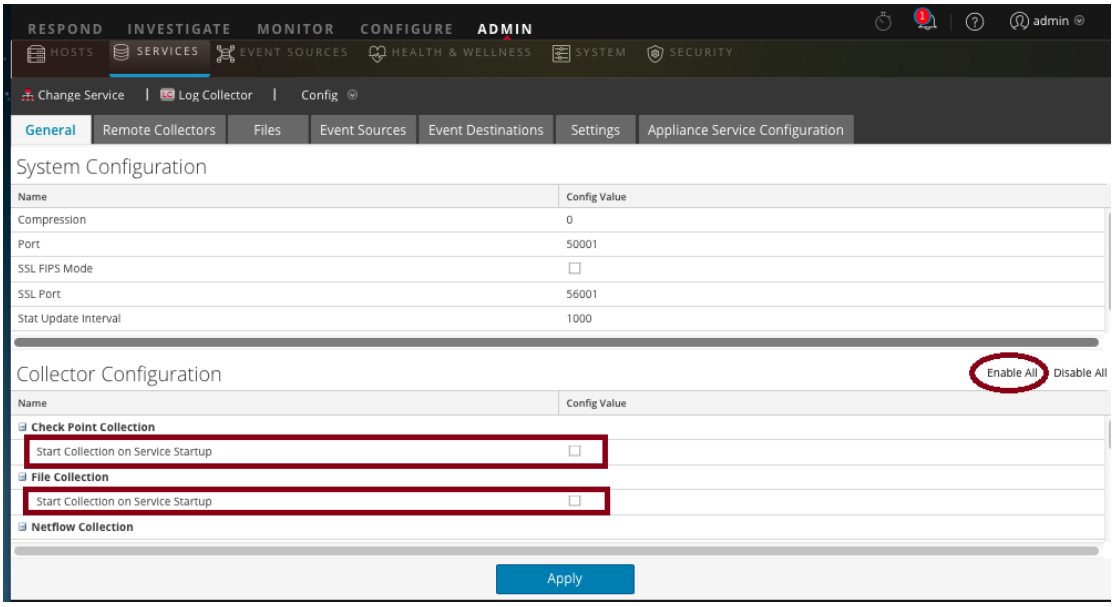
収集サービスの開始

1. [**管理**]＞[**サービス**]に移動します。
2. Log Collectorサービスを選択して、[**アクション**]の下の  をクリックします。
3. [**表示**]＞[**システム**]をクリックします。
4. [**収集**]＞[***サービス***](例：**ファイル**)を選択して、[**開始**]をクリックします。

収集サービスの自動開始の有効化

1. [**管理**]＞[**サービス**]に移動します。
2. Log Collectorサービスを選択して、[**アクション**]の下の  をクリックします。
3. [**表示**]＞[**構成**]をクリックします。

   [全般]タブが表示されます。
4. [Collector構成]パネルで、自動的に開始する個々の収集サービスに対して[**サービス起動時に収集を開始**]を選択します。または、すべての収集サービスを自動的に開始するには[**すべて有効化**]を選択します。



5. [**適用**]をクリックすると変更が有効になります。

ログ収集の動作確認

このトピックでは、ログ収集が正しく設定されていることを確認する方法を説明します。

以下の方法で、ログ収集が動作していることを確認します。

- [**管理**]＞[**ヘルスモニタ**]ビューの[イベント ソース モニタリング]タブにイベント アクティビティが表示されていることを確認します。
- 構成した収集プロトコルについて、[**調査**]＞[**イベント**]ビューの[**詳細**]列にある[**device.type**]フィールドに、Parserの値が記録されていることを確認します。

収集プロトコルが正しく設定されていることを確認するステップについては、それぞれの収集プロトコルのトピックを参照してください。

証明書の構成

証明書は、Log Collectorにトラスト ストアを作成して管理します。Log Collectorはこれらのトラスト ストアを参照して、イベント ソースが信頼できるかを判定します。

証明書の追加

証明書を追加するには:

1. **[管理]**>**[サービス]**に移動します。
2. [**サービス**]グリッドで**Log Collector**サービスを選択します。
3. [**アクション**]の下の  をクリックし、**[表示]**>**[構成]**を選択します。
4. [**設定**]タブをクリックします。
5. オプション パネルで、[**証明書**]を選択します。
6. **証明書**ツール バーの  をクリックします。

   [**証明書の追加**]ダイアログが表示されます。
7. [**参照**]をクリックし、ローカル ディレクトリやネットワークから証明書(***.PEM**) を選択します。
8. パスワードを指定します(必要な場合) 。
9. [**保存**]をクリックします。

[証明書]パネル

次の表で、[証明書]パネルで使用可能なボタンと列について説明します。

フィールド	説明
	証明書とパスワードを追加できる[証明書の追加]ダイアログが開きます。
	選択した証明書を削除します。
	証明書を選択します。
トラスト ストア名	トラスト ストアの名前を表示します。
証明書の識別名	証明書の識別名を表示します。

フィールド	説明
証明書のパスワード名	チェック ポイントのイベント ソースについてのみ、証明書のパスワード名を表示します。

[証明書の追加]ダイアログ

次の表は、[**証明書の追加**]ダイアログで使用できるパラメータについて説明しています。

フィールド	説明
トラスト ストア名	トラスト ストア名を入力します。
ファイル	[参照]をクリックして、ネットワークから証明書ファイル(*.PEMファイル) を選択します。
パスワード	この証明書のパスワードを指定します。
閉じる	証明書を追加せずに、ダイアログを閉じます。
保存	証明書が追加されます。

ログ収集の基礎

ログ収集の仕組み

Log Collectorサービスは、組織内のIT環境にあるイベント ソースからログを収集して他のNetWitness Suiteコンポーネントに転送します。ログは、メタ データとともに格納され、調査やレポートに使用することができます。

イベント ソースとは、サーバ、スイッチ、ルータ、ストレージ アレイアレイ、オペレーティング システム、ファイアウォールなど監視対象となるネットワーク上の資産を指します。多くの場合、IT部門がLog Collectorサービスにログを送信するためにイベント ソースを構成し、NetWitness Suite管理者は、イベント ソースをポーリングしてログを取得するためにLog Collectorサービスを構成します。Log Collectorは、元の形式のまますべてのログを受信します。

収集プロトコル

RSA NetWitness Suiteは、さまざまなイベント ソースからログを収集できます。特定のイベント ソースに対してログ収集を構成している場合、まず、ログの収集に使用するプロトコルを理解する必要があります。

収集プロトコル	説明
Check Point	OPSEC LEAを使用してCheck Pointイベント ソースからイベントを収集します。OPSEC LEAは、ログの抽出を容易にするためのCheck Point Operations Security Log Export APIです。詳細については、「NetWitness SuiteでのCheck Pointイベント ソースの構成」を参照してください。
ファイル	ログ ファイルからイベントを収集します。イベント ソースはログ ファイルを生成します。このファイルは、セキュアなファイル転送方式を使用してLog Collectorサービスに転送されます。 詳細については、「NetWitness Suiteでのファイル イベント ソースの構成」を参照してください。
Netflow	Netflow v5およびNetflow v9からイベントを受け入れます。詳細については、「NetWitness SuiteでのNetflowイベント ソースの構成」を参照してください。
ODBC	ODBC(Open Database Connectivity) ソフトウェア インタフェースを使用して、イベント ソースとして構成されたデータベースの監査データからイベントを収集します。詳細については、「NetWitness SuiteでのODBCイベント ソースの構成」を参照してください。

収集プロトコル	説明
プラグイン	プラグイン収集は、他の言語で記述された外部スクリプトを使用してイベントを収集するための一般的な収集フレームワークです。RSAは、現在AWS(Amazon Web Services) CloudTrailとMicrosoft Azureに対する収集機能を提供します。 • **AWS** AWS(Amazon Web Services) CloudTrailからイベントを収集します。CloudTrailイベントには、アカウントのAWS APIコールが記録されます。詳細については、「NetWitness SuiteでのAWS(CloudTrail) イベント ソースの構成」を参照してください。 • **Azure** Microsoft Azureからイベントを収集します。詳細については、「NetWitness SuiteでのAzureイベント ソースの構成」を参照してください。 お客様はこのフレームワークを使用して、独自の収集プロトコルを開発できます。
SDEE	IDS(侵入検知システム) およびIPS(侵入防止サービス) のメッセージを収集します。 詳細については、「NetWitness SuiteでのSDEEイベント ソースの構成」を参照してください。
SNMPトラップ	SNMPトラップを収集します。詳細については、「NetWitness SuiteでのSNMPイベント ソースの構成」を参照してください。
Syslog	Syslogメッセージを発行するイベント ソースからのメッセージを収集します。詳細については、「リモートCollectorに対するSyslogイベント ソースの構成」を参照してください。 **注 :** Syslogの収集はローカルLog Collectorに対して構成しないでください。リモートCollectorに対してのみ、Syslogの収集を構成する必要があります。
VMware	VMware仮想インフラストラクチャからのイベントを収集します。詳細については、「NetWitness SuiteでのVMwareイベント ソースの構成」を参照してください。
Windows	Microsoft Windows イベントAPIをサポートするWindowsマシンからのイベントを収集します。Windows NT 6.0系(Microsoft Windows VistaとWindows Server 2008) のオペレーティング システムでサポートされている、イベント ログとトレースのフレームワークを使用します。詳細については、「NetWitness SuiteでのWindowsイベント ソースの構成」を参照してください。

収集プロトコル	説明
Windows Legacy	次のソースからのイベントを収集します。 • Windows 2000やWindow 2003などWindowsの古いバージョン。RSA enVisionでの収集用に構成されたWindowsイベント ソースからデータを収集でき、再構成を行う必要はありません。 • NetApp ONTAPアプライアンス イベント ソース。NetApp .evtファイルを収集してパースできます。 • 詳細については、「Windows Legacy収集およびNetApp収集の構成」を参照してください。 **注：SALegacyWindowsCollector-*version-number.exe*を使用して、NetWitness Suite Windows Legacy Collectorを物理または仮想のWindows Server 2008 R2 SP1 64ビット版にインストールします。**

基本的な手順

基本的な手順は、サポートされているすべての収集プロトコルで同じです。

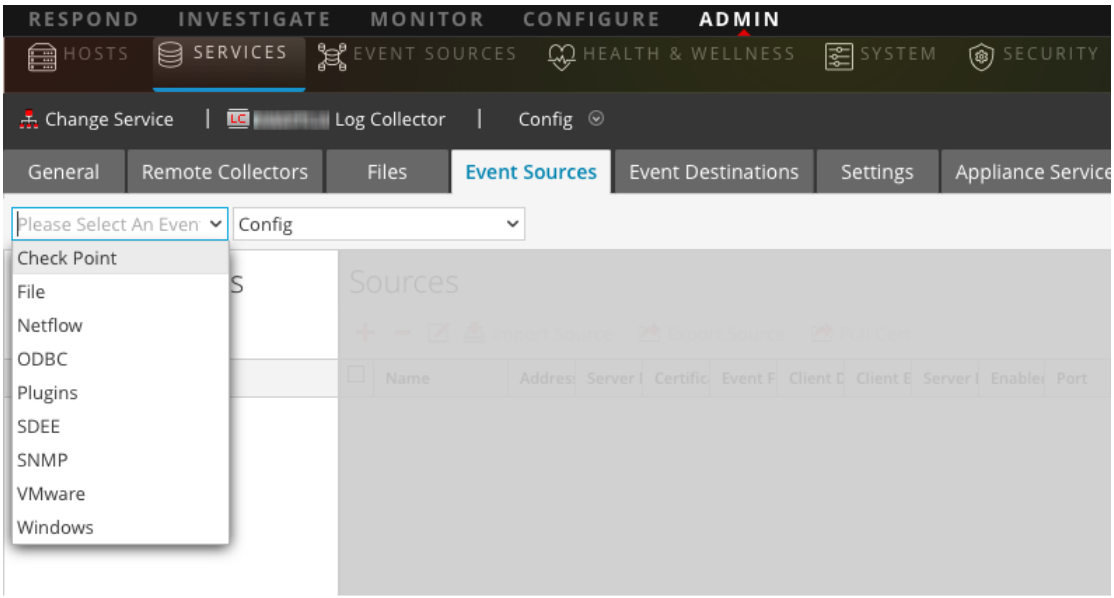
1. **収集対象のイベント ソースを設定します。** サポート対象の各イベント ソースの構成ドキュメントが、RSA Linkの「RSA Supported Event Sources」領域で入手できます。
   a. RSA Linkの「RSA Supported Event Sources」領域に移動します。
   b. イベント ソースに対応する手順を検索します。
      「Overview」ページには現在サポートされているすべてのイベント ソースに加え、収集方法、デバイス クラス、サポートされるバージョンに関する情報が一覧表示されます。
   c. イベント ソースに対応する構成手順をダウンロードし、それらに従ってください。
2. **RSA NetWitness Suiteで収集を構成します。** イベント ソース構成ガイドには、これらの手順が記載されています。ただし、このガイドには、イベント ソースで使用される収集方法に基づいた手順も記載されています。詳細については、「収集プロトコル」を参照してください。
3. **収集方法に対応するサービスを開始します。** 通常、この収集方法を使用する最初のイベント ソースに対してのみこの作業を行う必要があります。たとえば、初めてファイルの収集を使用するイベント ソースを構成するときに、NetWitness Suiteでファイル サービスを開始する必要がある場合があります。
4. **イベント ソースに対して収集が機能しているか確認します。**

以下では、ステップ2、3、および4について詳しく説明します。

RSA NetWitness Suiteでの収集の構成

イベント ソースを構成するプロセスは、それらのソースが使用する収集方法によって異なります。ただし、これらのプロセスは非常に似ていることに注意してください。次の手順は一般的な手順です。個別の収集方法の詳細については、それぞれの特定の収集方法の詳細について説明するトピックに記載されています。

1. NetWitness Suiteメニューから**[管理]**>**[サービス]**に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、⚙>**[表示]**>**[構成]**を選択して、ログ収集に関する構成パラメータのタブを表示します。
4. **[イベント ソース]**タブをクリックします。



5. **Log Collectorの[イベント ソース]**タブで、ドロップダウン メニューから収集方法を選択します。
6. **[イベント カテゴリ]**パネル ツールバーで、➕をクリックします。

   [使用可能なイベント ソース タイプ]ダイアログ ボックスが表示されます。
7. イベント ソース タイプを選択し、**[OK]**をクリックします。

   新しく追加されたイベント ソース タイプが[イベント カテゴリ]パネルに表示されます。
8. **[イベント カテゴリ]**パネルで新しいタイプを選択し、[ソース]ツールバーで➕をクリックします。

   [ソースの追加]ダイアログが表示されます。

9. 指定可能なパラメータの値を入力します。

   構成している特定の収集方法の「パラメータ」セクションを参照してください。

10. [**OK**]をクリックします。

収集方法に対応するサービスの開始

収集方法に対応するサービスを開始するには、次の手順を実行します。

1. [**管理**]＞[**サービス**]に移動します。
2. **Log Collector**を選択し、  ＞[**表示**]＞[**システム**]を選択します。
3. [**収集**]＞[*protocol*]＞[**開始**]をクリックします。

   ここで*protoco*は、**Netflow**などの開始するプロトコルです。

イベント ソースに対して収集が機能しているか確認します。

Netflow収集の稼働状況は、[**管理**]＞[**ヘルスモニタ**]＞[**イベント ソース モニタリング**]タブで確認できます。

イベント ソースに対して収集が機能しているか確認するには、次の手順を実行します。

1. [**管理**]＞[**ヘルスモニタ**]に移動します。
2. [**イベント ソース モニタリング**]タブをクリックします。
3. グリッドで、[**Log Decoder**]、[**イベント ソース**]、[**イベント ソース タイプ**]を確認します。
4. イベント ソースの[**件数**]列で、収集がイベントを受信していることを確認します。

Collectorのイベント フィルタの構成

このトピックでは、すべての収集プロトコルを対象としたイベント フィルタの作成方法と管理方法について説明します。

注：Syslogの収集はローカルLog Collectorに対して構成することはできません。リモートCollectorに対してのみ、Syslogの収集を構成する必要があります。詳細な構成情報については、「ローカルCollectorおよびリモートCollectorの構成」を参照してください。

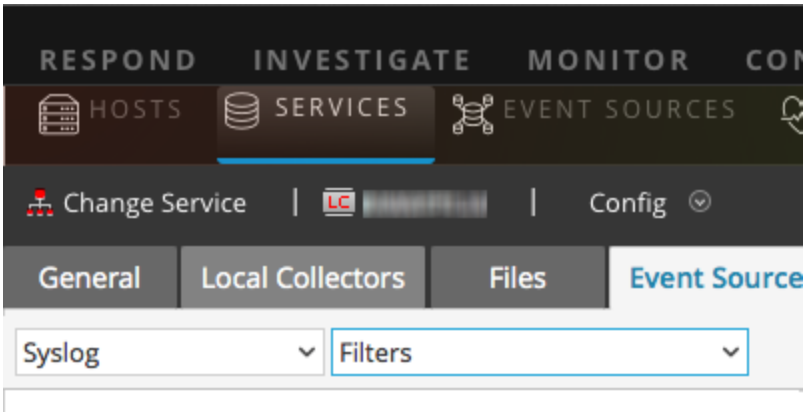
イベント フィルタの構成

イベント ソースを構成するには、次の手順を実行します。

1. [**管理**]＞[**サービス**]に移動します。
2. [Log Collector]サービスを選択します。

3. [アクション]で、**[表示]＞[構成]**を選択して、ログ収集に関する構成パラメータのタブを表示します。
4. [**イベント ソース**]タブをクリックします。
5. [**イベント ソース**]タブで、ドロップダウン メニューから任意の収集方法や[**フィルタ**]を選択します。

   次の画面に、選択した**Syslog**を示します。

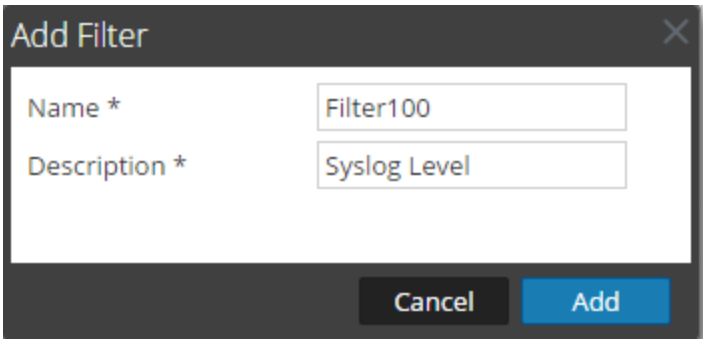


注：Syslogの構成はリモートCollectorでのみ利用可能です。ローカルCollectorサービスを使用している場合、**Syslog**をドロップダウン メニューから選択することはできません。

   [**フィルタ**]ビューでは、選択された収集方法(ある場合)に対して構成されているフィルタを表示します。

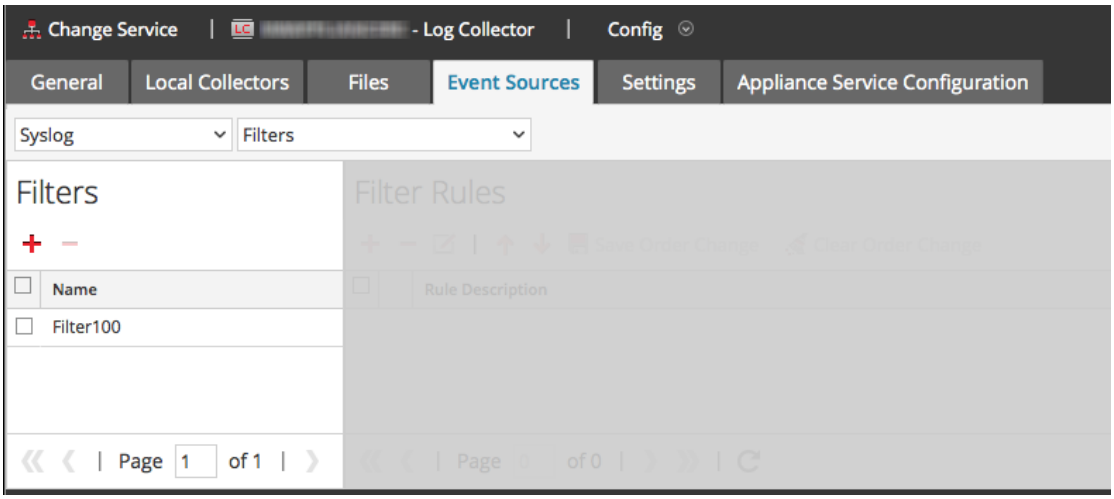
6. [**フィルタ**]パネルのツールバーで＋をクリックします。

   [**フィルタの追加**]ダイアログが表示されます。



7. 新しいフィルタの名前と説明を入力して[**追加**]をクリックします。

   [**フィルタ**]パネルに新しいフィルタが表示されます。

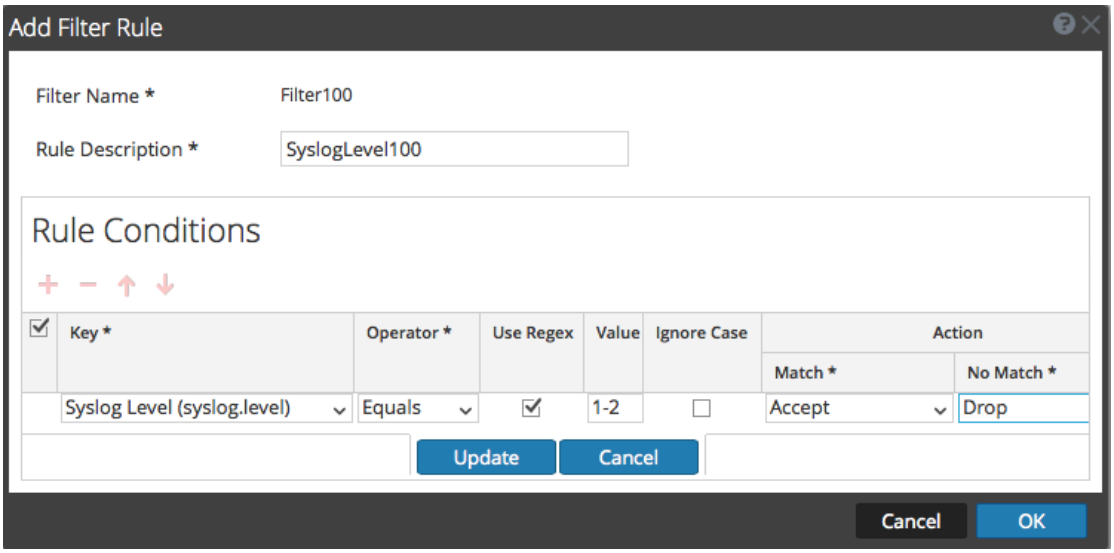


8. [**フィルタ**]パネルで新しいフィルタを選択し、[**フィルタ ルール**]パネルのツールバーで+をクリックします。

   [**フィルタ ルールの追加**]ダイアログが表示されます。

9. [**ルールの条件**]の下の+をクリックします。

10. ルールのパラメータを追加し、[**更新**]>[**OK**]をクリックします。



NetWitness Suiteにより、定義されたルールを使用してフィルタが更新されます。

注：ルールは、アクション タイプが処理を中止したり、最後のルールがチェックされるまで上から順に処理されます。デフォルトの動作では、一致が検出されない場合はルールを受け入れます。

次の表では、フィルタ ルールを追加するためのパラメータについて説明します。

イベント フィルタ ルールの「キー」パラメータ

[キー]フィールドの値は、フィルタに適用される収集メソッドによって異なります。

収集方法	[キー]フィールドの値
チェックポイント、ファイル、Netflow、プラグイン、SDEE SNMP とVMware	• すべてのデータ フィールド • イベント ソース タイプ • イベント ソース名 • ソースIP • RAWイベント
ODBC	• すべてのデータ フィールド • イベント ソース タイプ • イベント ソース名 • ソースIP • メッセージID • メッセージ レベル
Syslog	• すべてのデータ フィールド • イベント ソース タイプ • イベント ソース名 • ソースIP • Syslogレベル • RAWイベント

収集方法	[キー]フィールドの値
Windows	• すべてのデータ フィールド • イベント ソース タイプ • イベント ソース名 • ソースIP • イベントID • プロバイダー • チャネル • コンピューター • UserName • ドメイン名
Windows Legacy	• すべてのデータ フィールド • イベント ソース タイプ • イベント ソース名 • ソースIP • イベントID

その他のイベント フィルタ ルール パラメータ

次の表では、イベント フィルタ ルールを作成するために利用可能なその他すべてのフィールドについて説明します。

フィールド	説明
演算子	有効な値は次のとおりです。 • Contains • Equal
Regexの使用	(オプション) Regexを使用する場合に、選択します。

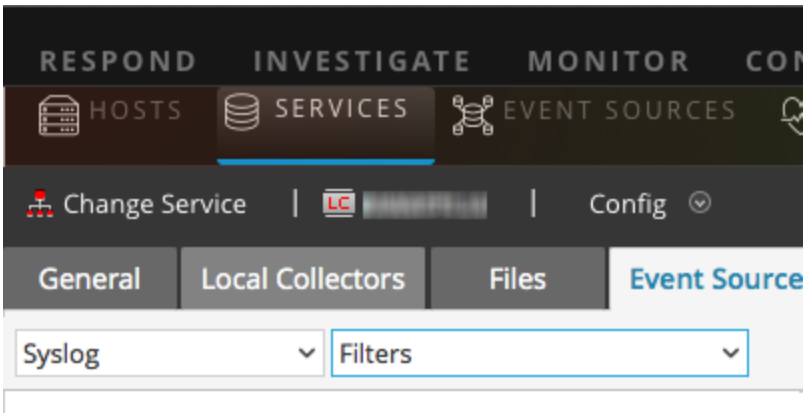
フィールド	説明
値	条件を構成するためのキーの値を指定します。 たとえば、キーに**Syslogレベル**を選択している場合、この値はSyslogレベルを表す数値になります。
大文字と小文字を区別しない	(オプション) 大文字と小文字を区別しないときに選択します。
アクション	一致した場合、Accept(許可)、Drop(ドロップ)、Next Condition(次の条件)、Next Rule(次のルール)のいずれかのアクションを選択できます。 • **許可**:提供されているIDに一致するイベントがイベント ログに含まれ、Systems AnalyticsのUIに表示されます。 • **ドロップ**:提供されているIDに一致するイベントはイベント ログに含まれず、UIに表示されません。 • **次の条件**:フィルタは一致するIDをもつイベントを無視し、次のルール条件に移動します。 • **次のルール**:フィルタは一致するIDをもつイベントを無視し、次のルールに移動します。 一致しない場合、Accept(許可)、Drop(ドロップ)、Next Condition(次の条件)、Next Rule(次のルール)のいずれかのアクションを選択できます。

フィルタ ルールの変更

イベント ソースを変更するには、次の手順を実行します。

1. **[管理]>[サービス]**に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、**[表示]>[構成]**を選択して、ログ収集に関する構成パラメータのタブを表示します。
4. [**イベント ソース**]タブをクリックします。
5. [**イベント ソース**]タブで、ドロップダウン メニューから任意の収集方法や[**フィルタ**]を選択します。

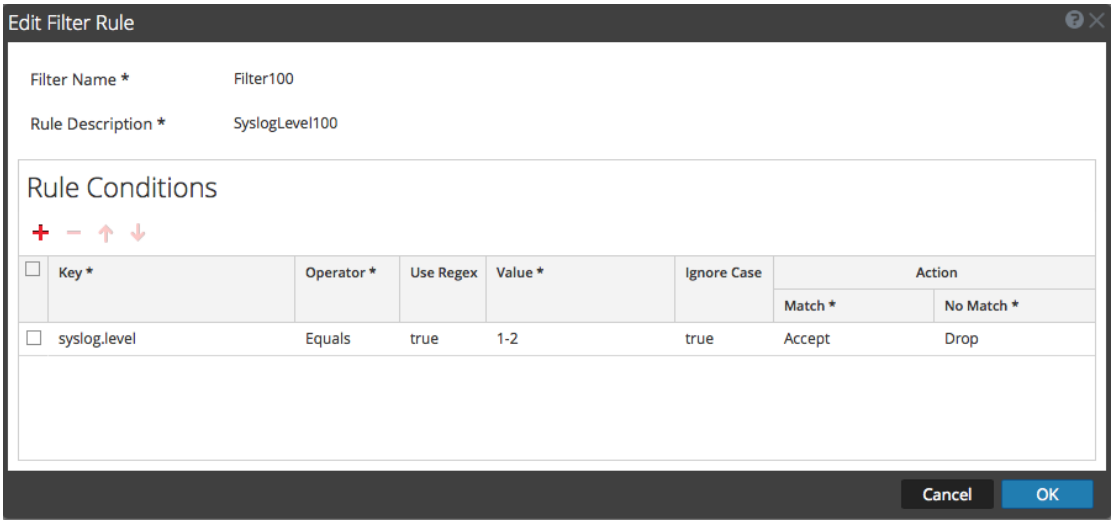
   次の画面に、選択した**Check Point**を示します。



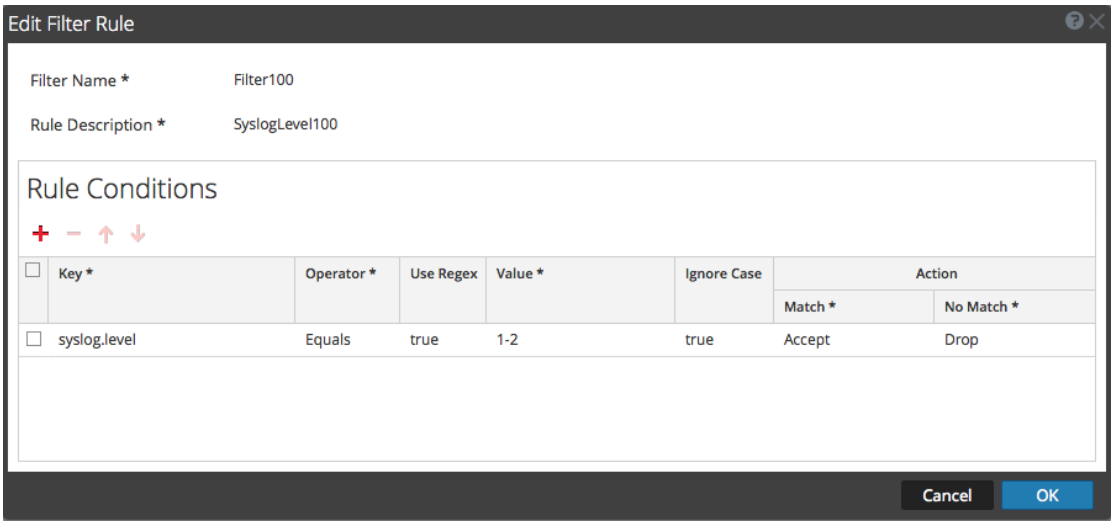
[**フィルタ**]ビューでは、選択された収集方法(ある場合)に対して構成されているフィルタを表示します。

6. [**フィルタ ルール**]リストで、ルールを選択し、をクリックします。

   [**フィルタ ルールの編集**]ダイアログが表示されます。



7. 変更するルール条件を選択します。



8. 変更が必要なパラメータを変更し、[**更新**]＞[**OK**]をクリックします。

NetWitness Suiteにより、選択したフィルタ ルールにパラメータの変更が適用されます。

イベント ソースの一括でのインポート、エクスポート、編集、テスト

このトピックでは、イベント ソースのインポート、エクスポート、編集、テストを一括で行う方法について説明します。

一括エクスポート オプションを使用すると、現在設定されているイベント ソースの詳細をエクスポートして格納できます。これらのデータは、現在の設定で問題が発生し、以前のイベント ソース データが必要になった場合に一括でインポートできます。

ある特定の変更が必要な複数のイベント ソースがある場合は、一括編集機能を使用できます。すべてのソースを選択して一度に編集オプションを適用できるため、個別に変更を適用せずに済みます。

イベント ソースの一括インポート

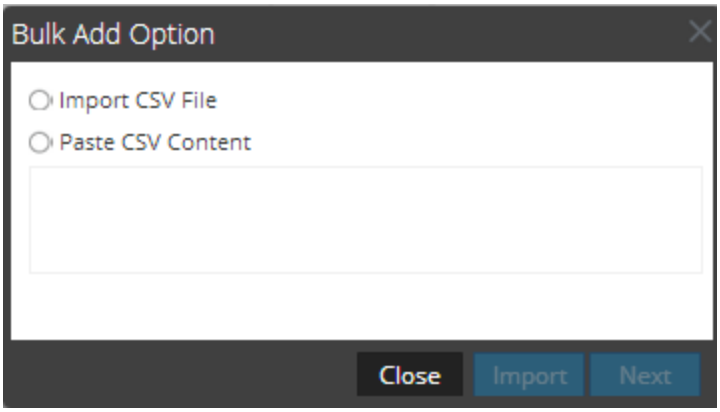
警告: 表計算プログラムを使用して、エクスポートされたイベント ソースのCSVファイルを編集する場合、数値や日付など一部のデータ フィールドが表計算プログラムのネイティブ フィールド タイプに再フォーマットされることがあります。この場合、一部のデータ フィールドの内容や形式が不正であるため、この情報を再インポートするときに問題が発生することがあります。この問題を回避するには、CSVファイルを表計算プログラムにインポートするときに、すべてのデータ フィールドをテキスト値として指定します。

複数のイベント ソースを一度にインポートするには、次の手順を実行します。

1. [**管理**]＞[**サービス**]に移動します。
2. [Log Collector]サービスを選択します。

3. [アクション]で、  **>[表示]>[構成]**を選択して、ログ収集に関する構成パラメータのタブを表示します。
4. [**イベント ソース**]タブをクリックします。
5. **Check Point、ファイル、Netflow、ODBC、プラグイン、SDEE、(リモートCollectorの場合Syslog)、VMware、Windows、Windows Legacy**のいずれかを選択します(SNMPにはインポート機能はありません)。
6. [**ソース**]パネルのツールバーで、[**ソースのインポート**]をクリックします。

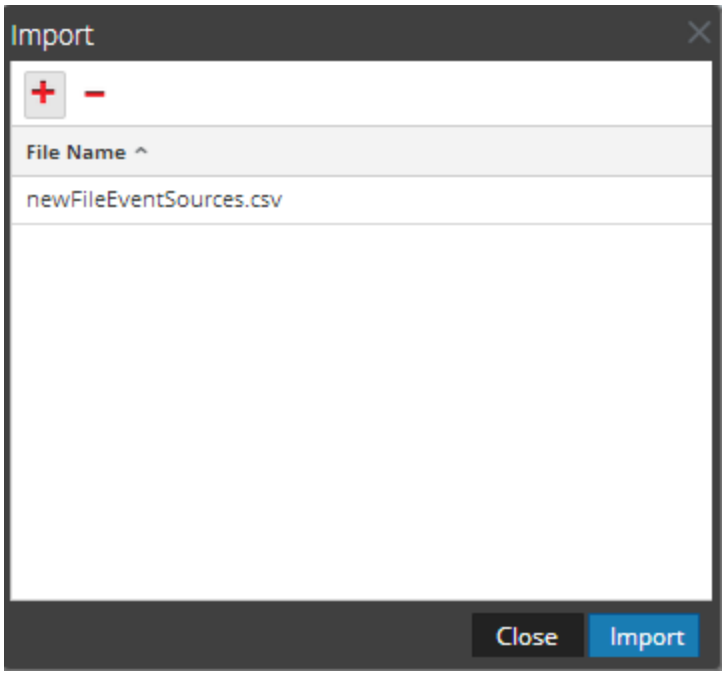
   [**一括追加オプション**]ダイアログが表示されます。



7. [**CSVファイルのインポート**]または[**CSVコンテンツの貼り付け**]のいずれかを選択します。選択した項目に応じて、以下のいずれかの手順を実行します。
   - CSVファイルのインポート。
     a. **次へ**をクリックします。

        [**インポート**]ダイアログが表示されます。

     b. [**追加**]をクリックし、ネットワークから**.csv**ファイルを選択します。

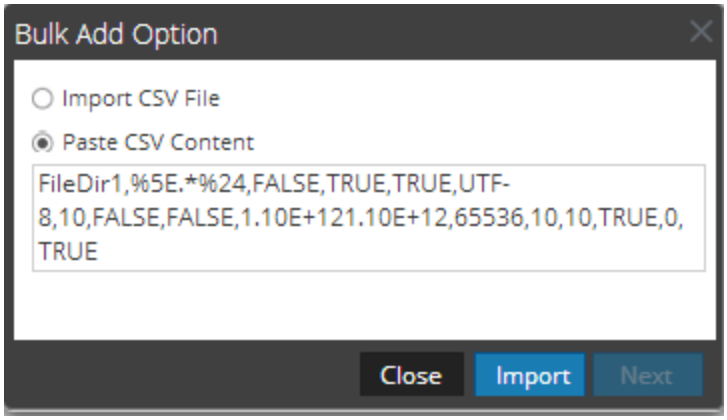


c. [**インポート**]をクリックします。

イベント ソース リストにイベント ソースが追加されます。

- CSVコンテンツの貼り付け

a. **.csv**ファイルのコンテンツをコピーし、それらをダイアログに貼り付けます。



b. [**インポート**]をクリックします。

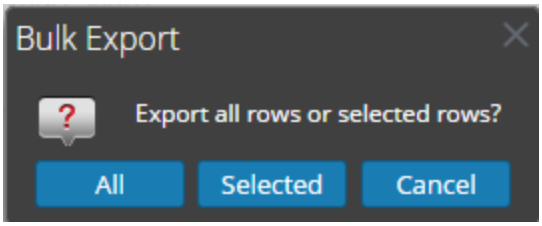
イベント ソース リストにイベント ソースが追加されます。

イベント ソースの一括エクスポート

警告: 表計算プログラムを使用して、エクスポートされたイベント ソースのCSVファイルを編集する場合、数値や日付など一部のデータ フィールドが表計算プログラムのネイティブ フィールド タイプに再フォーマットされることがあります。この場合、一部のデータ フィールドの内容や形式が不正であるため、この情報を再インポートするときに問題が発生することがあります。この問題を回避するには、CSVファイルを表計算プログラムにインポートするときに、すべてのデータ フィールドをテキスト値として指定します。

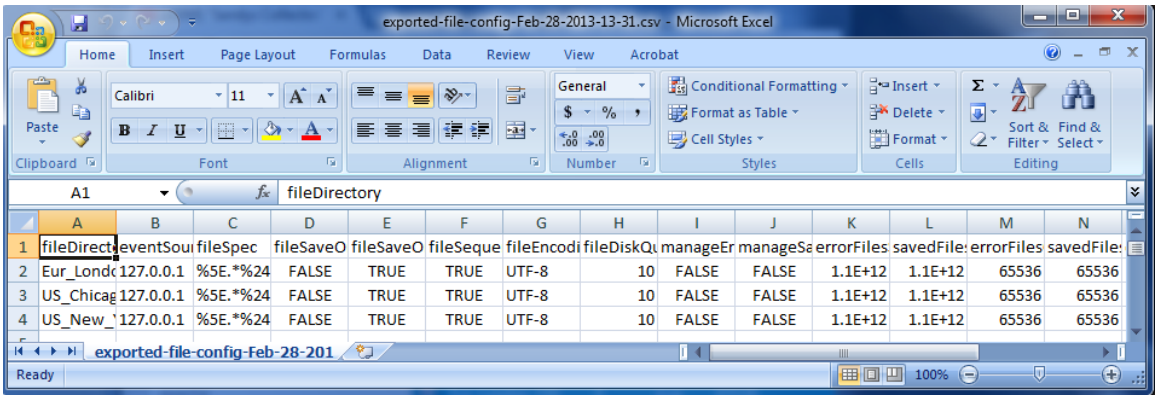
1. **[管理]**>**[サービス]**に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、  >**[表示]**>**[構成]**を選択して、ログ収集に関する構成パラメータのタブを表示します。
4. [**イベント ソース**]タブをクリックします。
5. **Check Point**、**ファイル**、**Netflow**、**ODBC**、**プラグイン**、**SDEE**、(**リモートCollectorの場合 Syslog**)、**VMware**、**Windows**、**Windows Legacy**のいずれかを選択します(SNMPにはエクスポート機能はありません)。
6. [**ソース**]パネルで、1つまたは複数のイベント ソースを選択し、[**ソースのエクスポート**]をクリックします。

   [**一括エクスポート**]ダイアログが表示されます。



7. 選択内容に基づいて、以下のようになります。
   - [**すべて**]を選択すると、NetWitness Suiteによってすべてのイベント ソースがタイム スタンプ付きのCSVファイルにエクスポートされます。
   - [**選択済み**]を選択すると、選択したイベント ソースがNetWitness Suiteによってタイム スタンプ付きのCSVファイルにエクスポートされます。
   - [**キャンセル**]を選択すると、NetWitness Suiteでエクスポートがキャンセルされます。

   以下に、リストから選択したイベント ソースで作成されるタイム スタンプ付きのCSVファイルの例を示します。

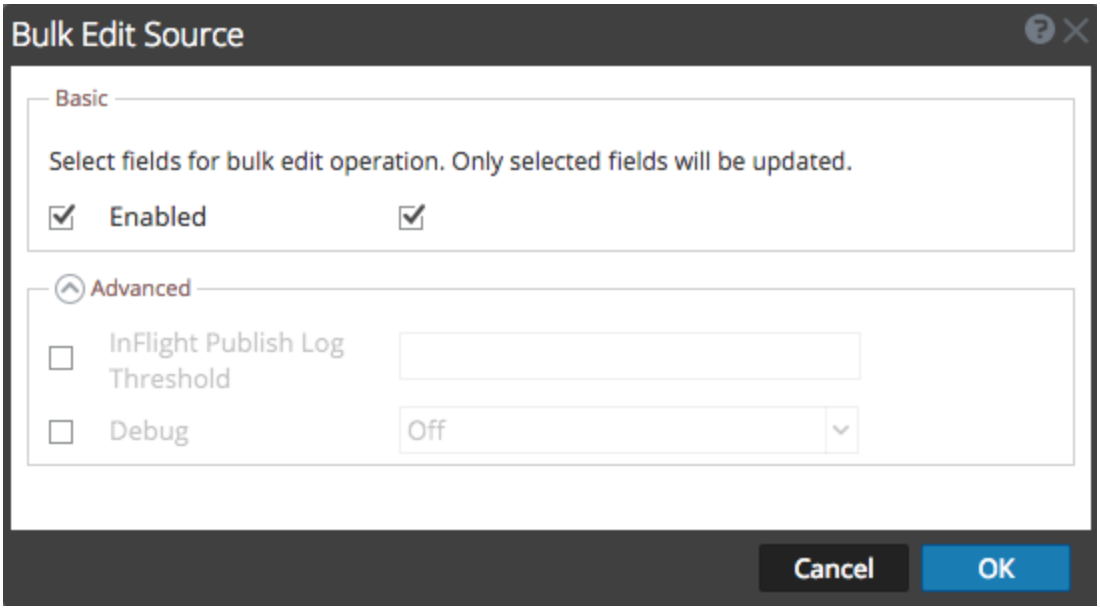


イベント ソースの一括編集

複数のイベント ソースを一度に編集するには、次の手順を実行します。

1. Log Collectorの[**イベント ソース**]タブで、**Check Point**、**ファイル**、**Netflow**、**ODBC**、**プラグイン**、**SDEE**、**Syslog**、**VMware**、**Windows**、**Windows Legacy**のいずれかを選択します(SNMPには編集機能はありません)。
2. [**ソース**]パネルで、複数のイベント ソースを選択し、(編集アイコン)をクリックします。

   選択したイベント ソースに該当する**一括編集**ダイアログが表示されます。次の図は、ファイル イベント ソースのパラメータの[**ソースの一括編集**]ダイアログの例を示しています。



3. 変更するフィールド(たとえば、[**デバッグ**])の左にあるチェックボックスをオンにします。
4. 選択したパラメータを変更します(たとえば、[デバッグ]の[**Off**]を[**On**]に変更します)。
5. [**OK**]をクリックします。

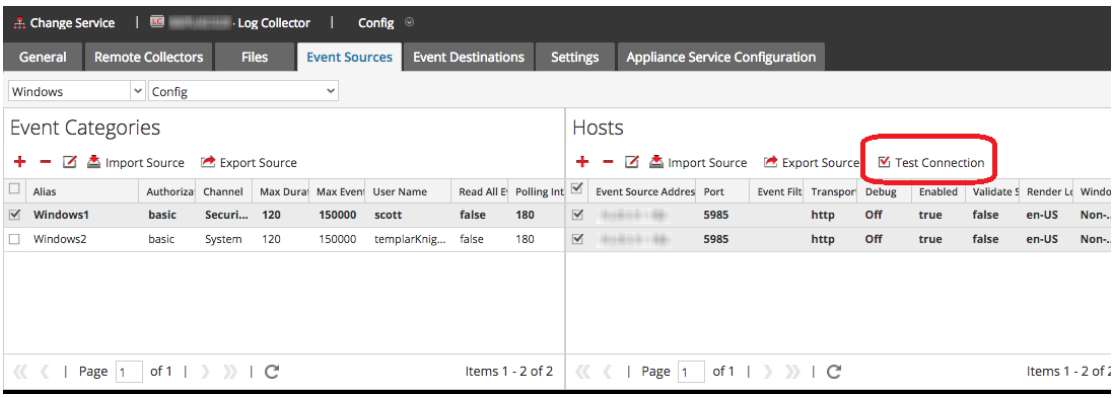
NetWitness Suiteにより、選択されているすべてのイベント ソースに同じパラメータ値の変更が適用されます。

イベント ソースへの接続の一括テスト

複数のイベント ソースへの接続を一度にテストするには、次の手順を実行します。

1. **[管理]＞[サービス]**に移動します。
2. [**サービス**]グリッドで、**Log Collector**サービスを選択します。
3. [アクション]で、  **＞[表示]＞[構成]**を選択して、ログ収集に関する構成パラメータのタブを表示します。
4. [**イベント ソース**]タブで[**プラグイン**]、[**ODBC**]、[**Windows**]のいずれかを選択します(その他のプロトコルには接続の一括テスト機能はありません) 。
5. 次の1つまたは複数を選択します。
   - [**プラグ イン**]または[**ODBC**]の[**ソース**]パネルのソース
   - [**Windows**]の[**ホスト**]パネルにあるホスト

   [**接続のテスト**]ボタンが有効になります。



6. Test Connection をクリックします。

   [**一括接続テスト**]ダイアログが表示され、各ソースでのテストのステータスが示されます。ステータスは、待機中、テスト中、成功、失敗のいずれかです。

   完了する前にテストで[閉じる]を選択した場合、テストは停止し、[**一括接続テスト**]ダイアログが閉じます。

テストが完了すると、その結果が[**一括接続テスト**]ダイアログに表示されます。

関連項目

イベント ソース モジュール([管理] > [イベント ソース]) を使用して、通常CMDBからインポートされるイベント ソースのグループを作成し、それらのグループに基づいてイベント ソースを監視できます。詳細については、「*イベント ソース管理ガイド*」の次のトピックを参照してください:

- イベント ソースのインポート
- イベント ソースのエクスポート
- イベント ソース属性の一括編集

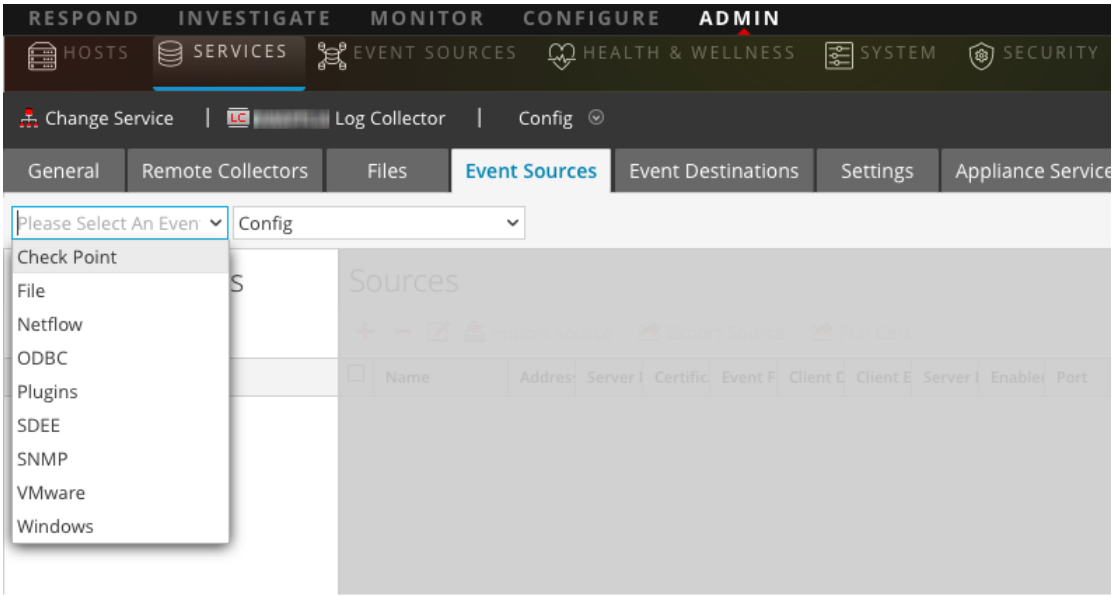
収集プロトコルおよびイベント ソースの構成

このトピックでは、収集プロトコルと、収集プロトコルを使用したイベント ソースの構成方法について説明します。

[イベント ソース]タブを使用してログ収集パラメータを設定し、イベント ソースからイベント データを収集するようにLog Collectorを構成します。

収集プロトコルを構成するには、次の手順を実行します。

1. NetWitness Suiteメニューから[**管理**]＞[**サービス**]に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、⚙＞[**表示**]＞[**構成**]を選択して、ログ収集に関する構成パラメータのタブを表示します。
4. [**イベント ソース**]タブをクリックします。



5. 収集プロトコル(例 : [**ファイル**]) を選択してから[**構成**]を選択します。
6. ＋をクリックして、イベント ソースを選択します。
7. 新しく追加されたカテゴリを選択し、＋をクリックします。
8. イベント ソースのパラメータを指定します。詳細については、個々の収集プロトコルのトピックを参照してください。

次のガイドでは、NetWitness Suiteの収集プロトコルと関連するイベント ソースの構成方法について詳細に説明します。 各ガイドには、収集プロトコルでサポートされるイベント ソースの構成手順のインデックスが付いています。

個々の収集プロトコルを構成するには、次のトピックを参照してください。

- 「NetWitness SuiteでのAWS(CloudTrail) イベント ソースの構成」
- 「NetWitness SuiteでのAzureイベント ソースの構成」
- 「NetWitness SuiteでのCheck Pointイベント ソースの構成」
- 「NetWitness Suiteでのファイル イベント ソースの構成」
- 「NetWitness SuiteでのNetflowイベント ソースの構成」
- 「NetWitness SuiteでのODBCイベント ソースの構成」
  - 「DSN(データ ソース名) の構成」
  - 「ODBC収集用のカスタムのTypespecの作成」
  - 「ODBCイベント ソース構成パラメータ」
  - 「ODBC DSNイベント ソース構成パラメータ」
- 「NetWitness SuiteでのSDEEイベント ソースの構成」
- 「NetWitness SuiteでのSNMPイベント ソースの構成」
- 「リモートCollectorに対するSyslogイベント ソースの構成」
- 「NetWitness SuiteでのVMwareイベント ソースの構成」
- 「NetWitness SuiteでのWindowsイベント ソースの構成」
- 「Windows Legacy収集およびNetApp収集の構成」
  - 「Windows Legacy Collectorの設定」
  - 「Windows LegacyおよびNetAppイベント ソースの構成」
  - 「トラブルシューティング: Windows LegacyおよびNetApp Collection」

NetWitness SuiteでのAWS(CloudTrail) イベント ソースの構 成

このトピックでは、AWS(Amazon Web Services) CloudTrailからイベントを収 集 する、AWS収 集 プロトコルを構 成 する方 法 について説 明します。

注 : AWSプラグインは、AWS CloudTrailログからの収 集 だけを指し、S3バケット(任 意 のディレクトリ下) にある任 意 のログからの収 集 のことは指しません。AWS CloudTrailログはJSON形 式 で送 信 されます。この形 式 については、AWSのドキュメント (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference.html) で詳しく説 明されています。

AWS収 集 の仕 組 み

Log Collectorサービスは、AWS(Amazon Web Services) CloudTrailからイベントを収 集 します。CloudTrailは、アカウントのAWS API呼 び出しを記 録 します。イベントには、API呼 び出し元 のID、APIコールの時 刻 、API呼 び出し元 のソースIPアドレス、リクエスト パラメータ、AWSサービスによって返 されるレスポンス構 成 要 素 が含 まれます。CloudTrailイベントによって提 供 されるAWS API呼 び出し履 歴 により、セキュリティ分 析 、リソース変 更 トラッキング、コンプライアンス監 査 を実 行 できます。CloudTrailでは、ログ ファイルの保 存 と配 布 にAmazon S3を使 用 します。NetWitness Suiteは、クラウド(S3バケット) からログ ファイルをコピーし、ファイルに含 まれているイベントをLog Collectorに送 信 します。

導 入 のシナリオ

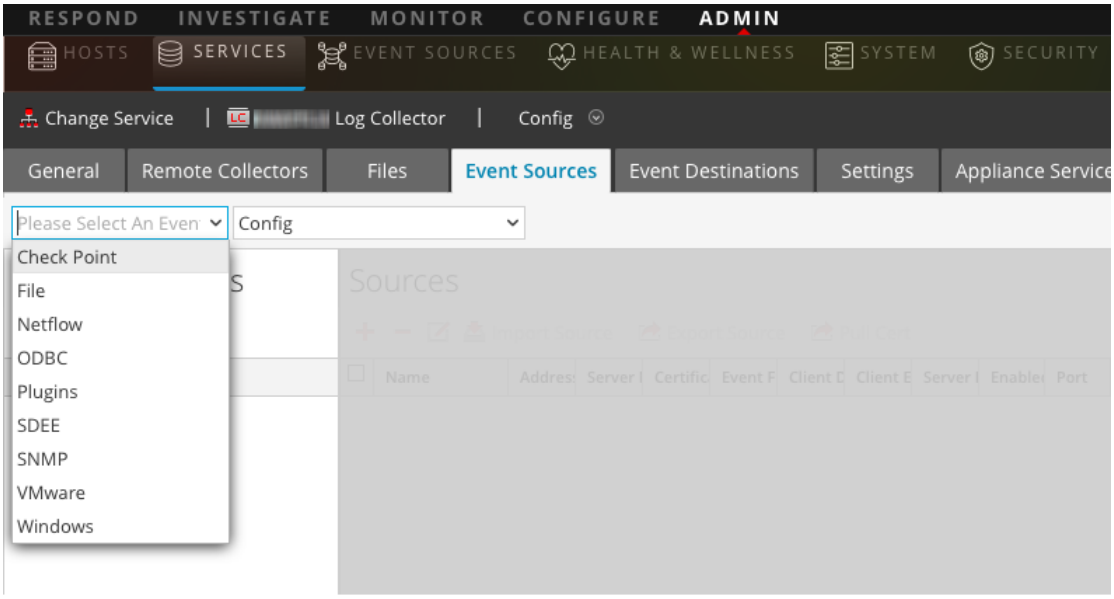
次 の図 に、NetWitness SuiteにAWS収 集 プロトコルを導 入 する方 法 を示します。

構成

AWS(CloudTrail) イベント ソースを構成するには、次の手順を実行します。

1. NetWitness Suiteメニューから[**管理**]＞[**サービス**]に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、⚙＞[**表示**]＞[**構成**]を選択して、ログ収集に関する構成パラメータのタブを表示します。

4. [**イベント ソース**]タブをクリックします。



5. [**イベント ソース**]タブで、ドロップダウン メニューから[**プラグイン**]と[**構成**]を選択します。
6. [**イベント カテゴリー**]パネル ツールバーで、 + をクリックします。

   [**使用可能なイベント ソース タイプ**]ダイアログが表示されます。
7. **cloudtrail**を選択し、[**OK**]をクリックします。

   新しく追加されたイベント ソース タイプが[**イベント カテゴリー**]パネルに表示されます。
8. [**イベント カテゴリ**]パネルで新しいタイプを選択し、[**ソース**]ツールバーで + をクリックします。

   [**ソースの追加**]ダイアログが表示されます。
9. パラメータ値を定義します。詳細については、以下の「AWSパラメータ」を参照してください。
10. [**接続のテスト**]をクリックします。

    テストの結果がダイアログ ボックスに表示されます。テストが失敗した場合は、デバイスまたはサービスの情報を編集し、再試行します。

    Log Collectorでは、約60秒後にテストの結果を返します。制限時間を超えると、テストがタイムアウトになり、NetWitness Suiteはエラー メッセージを表示します。
11. テストが正常に実行された場合は、[**OK**]をクリックします。

    新しいイベント ソースが[**ソース**]パネルに表示されます。

AWSパラメータ

次の表に、AWSコレクションで使用できる構成パラメータについて説明します。

パラメータ	説明
パラメータ	**説明**
	基本
名前*	イベント ソースの名前です。
有効化 	イベント ソース構成を有効化して収集を開始するには、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。
アカウントID*	S3バケットのアカウント識別コード

パラメータ	説明
S3バケット名*	AWS(CloudTrail) S3バケットの名前。 Amazon S3バケットの名前は、バケットを作成したAWS (CloudTrail) のリージョンには関係なく、グローバルに一意です。名前はバケットの作成時に指定します。 バケット名はDNSの命名規則に従う必要があります。DNSに準拠したバケット名の規則は次のとおりです。 • バケット名は3文字以上63文字以下の長さの文字列とする。 • バケット名は1つ以上のラベルを連結したものとする。隣接するラベルはピリオド1文字「.」で区切る。バケット名には小文字、数字、ハイフンを使用できる。各ラベルの最初と最後の文字は、小文字また数字とする。 • バケット名をIPアドレスのような形式で指定してはならない(たとえば192.168.5.4) など。 **有効な**バケット名の例を次に示します。 • **myawsbucket** • **my.aws.bucket** • **myawsbucket.1** **無効な**バケット名の例を次に示します。 • **.myawsbucket**: バケット名の先頭にはピリオド「.」を使用できません。 • **myawsbucket.** : バケット名の末尾にもピリオド「.」は使用できません。 • **my..examplebucket**: ラベルの間のピリオドは1つしか使用できません。
アクセスキー*	S3バケットへのアクセスに使用するキー。アクセスキーはAWSサービスAPIに対して安全なRESTリクエストまたはクエリプロトコルリクエストを作成するために使用します。アクセスキーの詳細は、Amazon Web Servicesサポート サイトの「Manage User Credentials」を参照してください。

パラメータ	説明
シークレット キー*	S3バケットへのアクセスに使用するシークレット キー。
リージョン*	S3バケットのリージョン。**us-east-1**がデフォルト値です。
リージョン エンドポイント	AWS CloudTrailホスト名を指定します。たとえば、us-eastリージョンのAWSパブリック クラウド では、リージョン エンドポイントは s3.amazonaws.comです。詳細については、http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_regionを参照してください。このパラメータは AWSガバメントまたはプライベート クラウドからCloudTrailログを収集するために必要です。
プロキシを使用	[**プロキシを使用する**]を有効にして、AWSサーバのプロキシを設定します。デフォルトでは無効です。
プロキシ サーバ	AWSサーバにアクセスするために接続するプロキシ名を入力します。
プロキシ ポート	AWSサーバにアクセスするプロキシ サーバに接続するポート番号を入力 します。
プロキシ ユーザ	プロキシ サーバを使用して認証するユーザ名を入力します。
プロキシ パスワード	プロキシ ポートを使用して認証するユーザのパスワードを入力します。
開始日*	その時点のタイムスタンプから指定日数分過去にさかのぼって、AWS(CloudTrail) コレクションを開始します。デフォルト値は0で、当日から開始します。範囲は0～89日です。
ログ ファイル プレフィックス	収集処理するファイルのプレフィックス。 **注**：CloudTrailサービス側の設定でプレフィックスを指定した場合は、このパラメータにも必ず同じプレフィックスを入力してください。
詳細	

パラメータ	説明
デバッグ	**注意**:イベント ソースに問題が発生し、その問題を調査する必要がある場合にのみ、デバッグを有効に(このパラメータを「On」または「Verbose」に設定)します。デバッグを有効にすると、Log Collectorのパフォーマンスに影響があります。 イベント ソースのデバッグ記録を有効または無効にします。 有効な値は次のとおりです。 • **Off** = (デフォルト) 無効 • **On** = 有効 • **Verbose** = verboseモードで有効になります。スレッド情報とソース コンテキスト情報をメッセージに追加します。 このパラメータは、イベント収集の問題をデバッグまたは監視するような状況で使用するよう設計されています。パフォーマンスへの影響を最小限にするために、デバッグのVerboseモードは、監視するイベント ソース数が限定された環境で設定するようにしてください。 この値を変更すると、変更はすぐに反映されます(再起動は不要です)。
コマンド引数	スクリプトに追加する引数。
ポーリング間隔	ポーリングの間隔(秒)です。デフォルト値は60です。 たとえば、60と指定すると、Collectorは、イベント ソースへのポーリングを60秒ごとに実行します。直前のポーリング サイクル(収集)がまだ完了していない場合、そのサイクルが完了するまで待機します。ポーリング中のイベント ソースが多数ある場合、スレッドがビジーになるため、ポーリングが開始するまでに60秒より長くかかる場合があります。
SSLが有効	SSLを使用して通信する場合は、このチェックボックスをオンにします。暗号化とSSL証明書による認証によってデータ転送のセキュリティが実装されます。 このチェックボックスは、デフォルトでオンになっています。

パラメータ	説明
接続のテスト	このダイアログで指定した構成パラメータが正しいことを検証します。 たとえば、このテストでは次の項目を検証します。 • このダイアログで指定した認証情報を使用してNetWitnessがAWSのS3バケットと接続できるか。 • NetWitnessがバケットからログファイルをダウンロードできるか(バケットにログファイルが全くない場合にはテストは失敗しますが、そのような可能性はほとんどありません)。
キャンセル	AWS(CloudTrail) を追加せずにダイアログを閉じます。
OK	現在のパラメータ値を新しいAWS(CloudTrail) として追加します。

NetWitness SuiteでのAzureイベント ソースの構成

このトピックでは、Azure収集プロトコルを構成する方法について説明します。Microsoft Azureは、Microsoftが管理するデータ センターのグローバル ネットワークを通じてアプリケーションとサービスを構築、導入、管理するためのクラウド コンピューティング プラットフォームおよびインフラストラクチャです。

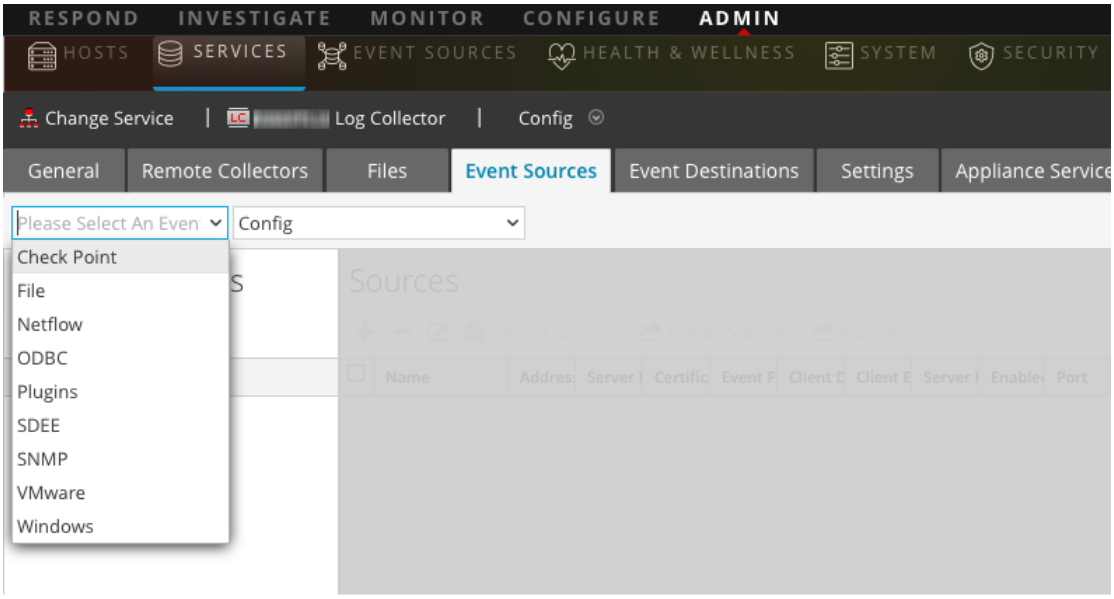
NetWitness Suiteでの構成

イベント ソースとしてのAzureの構成に関する詳細については、RSAリンクから利用できる「Azureのイベント ソース構成ガイド」を参照してください。

Azureのイベント ソースを構成するには、次の手順を実行します。

1. NetWitness Suiteメニューから[**管理**]>[**サービス**]に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、[ ]>[**表示**]>[**構成**]を選択して、ログ収集に関する構成パラメータのタブを表示します。

4. [**イベント ソース**]タブをクリックします。



5. [**イベント ソース**]タブで、ドロップダウン メニューから[**プラグイン**]と[**構成**]を選択します。
6. [**イベント カテゴリ**]パネル ツールバーで、 + をクリックします。

   [**使用可能なイベント ソース タイプ**]ダイアログが表示されます。
7. [**azureaudit**]を選択して[**OK**]をクリックします。

   新しく追加されたイベント ソース タイプが[**イベント カテゴリ**]パネルに表示されます。
8. [**イベント カテゴリ**]パネルで新しいタイプを選択し、[**ソース**]ツールバーで + をクリックします。

   [**ソースの追加**]ダイアログが表示されます。
9. パラメータ値を定義します。詳細については、以下の「Azureパラメータ」を参照してください。
10. [**接続のテスト**]をクリックします。

    テストの結果がダイアログ ボックスに表示されます。テストが失敗した場合は、デバイスまたはサービスの情報を編集し、再試行します。

    Log Collectorでは、約60秒後にテストの結果を返します。制限時間を超えると、テストがタイムアウトになり、NetWitness Suiteはエラー メッセージを表示します。
11. テストが正常に実行された場合は、[**OK**]をクリックします。

    新しいイベント ソースが[**ソース**]パネルに表示されます。

Azureパラメータ

このトピックでは、Azureイベント ソース構成パラメータについて説明します。

注:アスタリスク(*) が付いている項目は必須です。

基本パラメータ

名前	説明
名前*	英数字からなる、分かりやすいソースの名前を入力します。この値を使用するのは、このスクリーンで名前を表示するときだけです。
有効	イベント ソース構成を有効化して収集を開始するには、このチェックボックスをオンにします。このチェックボックスはデフォルトでオンになっています。
クライアントID*	クライアントIDは、Azureアプリケーション構成タブにあります。表示されるまで下にスクロールします。
クライアント シークレット*	イベント ソースを構成している場合、キーを作成して、有効期間を選択したときに、クライアント シークレットが表示されます。 表示されるのは1回のみで、後で取得することはできないので、必ず保存してください。
APIリソース ベースURL*	「`https://management.azure.com/`」を入力します。最後のスラッシュ(/) を必ず含めてください。
フェデレーション メタデータ エンドポイント*	使用するAzureアプリケーションで、[**エンドポイントの表示**]ボタン(ウィンドウの下部) をクリックします。 同じ文字列で始まる多くのリンクがあります。URLを比較し、それらのほとんどの先頭にある共通文字列を見つけます。この共通文字列が、ここで入力する必要のあるエンドポイントです。
サブスクリプションID*	Microsoft Azureのダッシュボードで確認できます。左側のリストの下部にあるサブスクリプションをクリックします。
テナント ドメイン*	Active Directoryに移動し、ディレクトリをクリックします。テナント ドメインはURLで、**manage.windowsazure.com/**の直後に続く文字列です。テナント ドメインは、**.com**までを含む文字列です。
リソース グループ名*	Azureでは、左側のナビゲーション ペインペインで、リソース グループを選択し、使用するグループを選択します。
開始日*	収集を開始する日付を選択します。デフォルトは設定当日です。
接続のテスト	このダイアログで指定された構成パラメータをチェックして、正しいことを確認します。

詳細パラメータ

[**詳細**]の横にある をクリックして、必要に応じて、拡張パラメータを表示し、編集します。

名前	説明
ポーリング間隔	ポーリングの間隔(秒)です。デフォルト値は**180**です。 たとえば、180と指定すると、Collectorは、イベント ソースへのポーリングを180秒ごとに実行します。ポーリング サイクル(収集)が進行中である場合、Collectorは、そのサイクルが完了するまで待機します。ポーリング中のイベント ソースが多数ある場合、スレッドがビジーになるため、ポーリングが開始するまでに180秒より長くかかる場合があります。
ポーリング最大継続時間	ポーリング サイクルの最大継続時間(秒)です。値ゼロは制限がないことを示します。
ポーリング最大イベント数	ポーリング サイクルごとのイベントの最大値(ポーリング サイクルごとに収集されるイベント数)です。
ポーリング最大アイドル時間	ポーリング サイクルの最大継続時間(秒)です。値ゼロは制限がないことを示します。
コマンド引数	スクリプトの起動に追加するオプションの引数です。
デバッグ	**注意**:イベント ソースに問題が発生し、その問題を調査する必要がある場合にのみ、デバッグを有効に(このパラメータを「On」または「Verbose」に設定)します。デバッグを有効にすると、Log Collectorのパフォーマンスに影響があります。 **注意**:イベント ソースのデバッグ記録を有効または無効にします。有効な値は次のとおりです。 • **Off** = (デフォルト)無効 • **On** = 有効 • **Verbose** = verboseモードで有効になります。スレッド情報とソース コンテキスト情報をメッセージに追加します。 このパラメータは、イベント収集の問題をデバッグまたは監視するような状況で使用するよう設計されています。この値を変更すると、変更はすぐに反映されます(再起動は不要です)。パフォーマンスへの影響を最小限にするために、デバッグのVerboseモードは、監視するイベント ソース数が限定された環境で設定するようにしてください。

NetWitness SuiteでのCheck Pointイベント ソースの構成

このトピックでは、Check Pointイベント ソースからイベントを収集するCheck Point収集プロトコルの構成方法について説明します。

このプロトコルは、OPSEC LEAを使ってCheck Pointイベント ソースからイベントを収集します。OPSEC LEAは、ログの抽出を容易にするためのCheck Point Operations Security Log Export APIです。

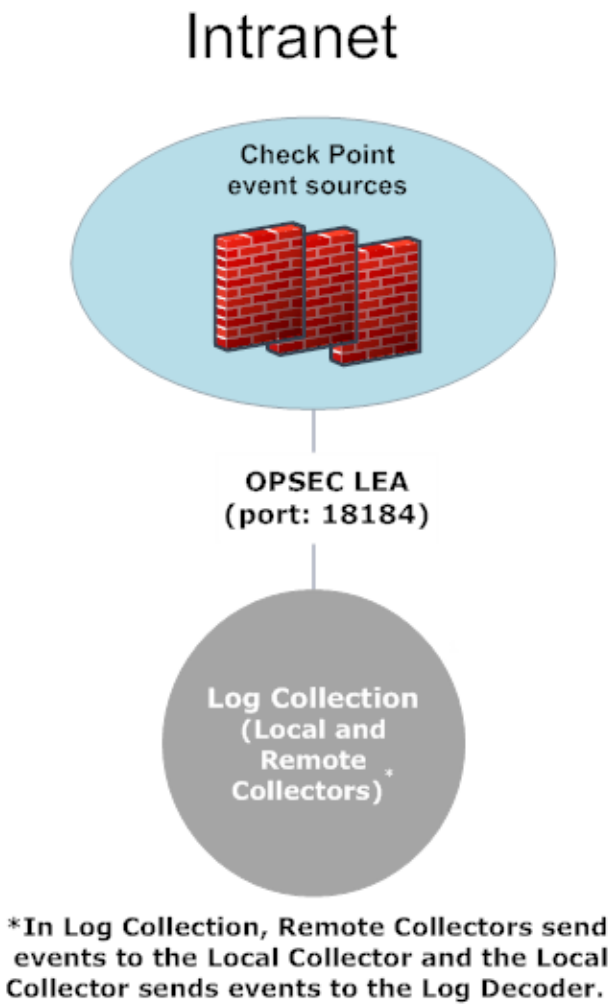
Check Point収集の仕組み

Log Collectorサービスは、OPSEC LEAを使用してCheck Pointイベント ソースからイベントを収集します。OPSEC LEAは、ログの抽出を容易にするためのCheck Point Operations Security Log Export APIです。

注 : OPSEC LEA(Log Export API) は、SHA-256またはSHA-1証明書を使用して構成されたCheck Pointイベント ソースからのログ抽出をサポートしています。

導入のシナリオ

次の図は、NetWitness SuiteでCheck Point収集プロトコルを導入する方法について示しています。

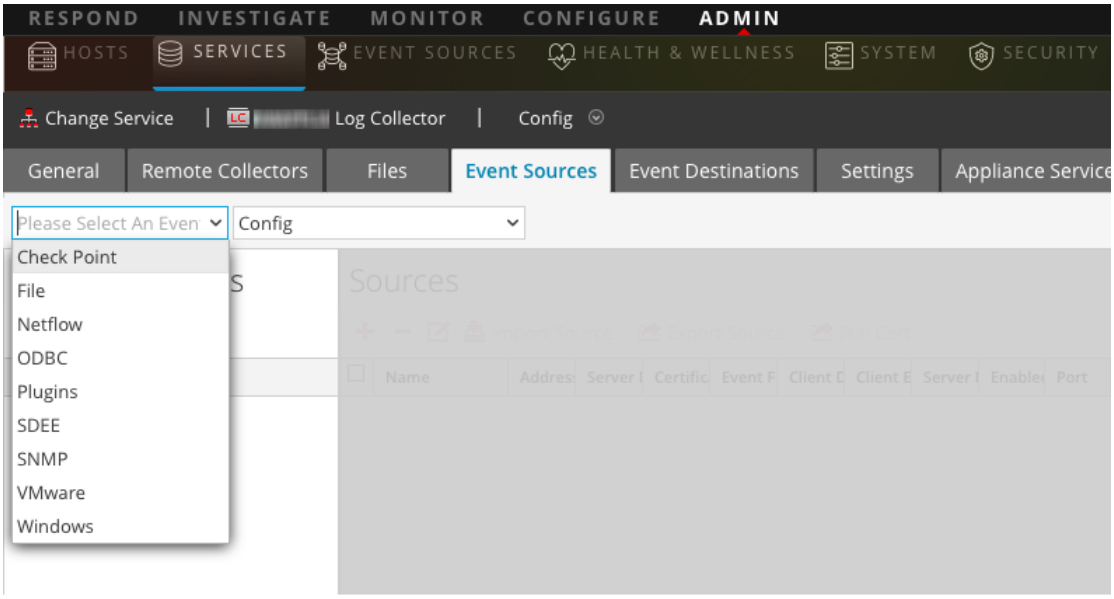


NetWitness Suiteでの構成

Check Pointイベント ソースを構成するには、次の手順を実行します。

1. NetWitness Suiteメニューから[**管理**]＞[**サービス**]に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、⚙＞[**表示**]＞[**構成**]を選択して、ログ収集に関する構成パラメータのタブを表示します。

4. [**イベント ソース**]タブをクリックします。



5. [**イベント ソース**]タブで、ドロップダウン メニューから[**Check Point/構成**]を選択します。
6. [**イベント カテゴリ**]パネル ツールバーで、 をクリックします。

   [**使用可能なイベント ソース タイプ**]ダイアログが表示されます。
7. Check Pointイベント ソース タイプを選択し、[**OK**]をクリックします。

   新しく追加されたイベント ソース タイプが[**イベント カテゴリ**]パネルに表示されます。
8. [**イベント カテゴリ**]パネルで新しいタイプを選択し、[**ソース**]ツールバーで をクリックします。

   [**ソースの追加**]ダイアログが表示されます。
9. パラメータ値を定義します。詳細については、下の「Check Point**パラメータ**」を参照してください。
10. [**接続のテスト**]をクリックします。

    テストの結果がダイアログ ボックスに表示されます。テストが失敗した場合は、デバイスまたはサービスの情報を編集し、再試行します。

    Log Collectorでは、約60秒後にテストの結果を返します。制限時間を超えると、テストがタイムアウトになり、NetWitness Suiteはエラー メッセージを表示します。
11. テストが正常に実行された場合は、[**OK**]をクリックします。

    新しいイベント ソースが[**ソース**]パネルに表示されます。

Check Pointパラメータ

このセクションでは、Check Pointイベント ソースの構成パラメータについて説明します。

基本パラメータ

パラメータ	説明
名前*	イベント ソースの名前です。
アドレス*	Check PointサーバのIPアドレスです。
サーバ名*	Check Pointサーバの名前です。
証明書	転送モードがhttpsである場合に使用するセキュア接続の証明書名です。このパラメータを設定する場合、[設定]タブで作成した証明書トラスト ストアに証明書が存在する必要があります。 ドロップダウン リストから証明書を選択します。Check Pointイベント ソース証明書のファイルの命名規則は、**checkpoint_*name-of-event-source***です。
クライアント識別	Check Pointサーバのクライアント識別名を入力します。
クライアント エンティティ名	Check Pointサーバのクライアント エンティティ名を入力します。
サーバ識別	Check Pointサーバのサーバ識別名を入力します。
有効化	イベント ソース構成を有効化して収集を開始するには、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。

パラメータ	説明
証明書の受信	初めて証明書の受信を行う場合は、このチェックボックスをオンにします。 証明書を受信すると、その証明書がトラスト ストアで使用可能になります。
証明書サーバアドレス	証明書が格納されているサーバのIPアドレス。デフォルトは、イベント ソース アドレスです。
パスワード	初回に[証明書の受信]チェックボックスをオンにした場合にのみアクティブになります。証明書を受信するにはパスワードが必要です。パスワードは、Check Pointサーバ上のCheck PointにOPSECアプリケーションを追加するときに作成されるアクティベーション キーです。

Check Point収集の拡張パラメータ値の決定

Check Pointイベント ソースへの接続を開いておくタイミングとイベント ボリュームを指定する(一時的に接続を開く)と、システム リソースの使用量を抑えることができます。RSA NetWitness Suiteはデフォルトで次の接続パラメータを使用して、一時的な接続を確立します。

- ポーリング間隔 = **180**(3分)
- ポーリング最大継続時間 = **120**(2分)
- ポーリング最大イベント数 = **5000**(ポーリング間隔あたり5000イベント)
- ポーリング最大アイドル時間 = **0**

Check Pointのイベント ソースから大量のイベントが発生する場合、収集を停止するまで接続を開いておく(持続的な接続を使用する) ように設定することをお勧めします。この設定によって、チェック ポイント収集において大量のログを生成するイベント ソースから生成されるイベント収集の速度を維持できます。永続的な接続によって、収集の再開や接続の遅延が回避され、Check Point収集がイベント生成よりも遅延することを防ぎます。

Check Pointイベント ソースに対する永続的な接続を確立するには、次のパラメータに値を設定します。

- ポーリング間隔 = **-1**
- ポーリング最大継続時間 = **0**

- ポーリング最大イベント数 = **0**
- ポーリング最大アイドル時間 = **0**

パラメータ	説明
ポート	Log Collectorが接続するCheck Pointサーバのポート番号です。 デフォルト値は18184です。
ログの収集タイプ	収集するログのタイプを選択します。 有効な値は次のとおりです。 • **監査**: 監査イベントを収集します。 • **セキュリティ**: セキュリティ イベントを収集します。 監査イベントとセキュリティ イベントの両方を収集する場合、同じイベント ソースを新たに作成する必要があります。たとえば、最初に[監査]を選択したイベント ソースを作成し、このイベント ソースのためにトラスト ストアから証明書を受信します。次に、別のイベント ソースとして、[ログの収集タイプ]で[セキュリティ]を選択し、その他は同一のパラメータ値を持つイベント ソースを作成する場合、最初のパラメータ セットを設定したときに受信した同じ証明書を[証明書]で選択します。[証明書の受信]が選択されていないことを確認します。
ログの収集開始点	Check Pointイベント ソースを設定すると、NetWitnessは現在のログ ファイルからイベントを収集します。有効な値は次のとおりです。 • **現在**: 現在の時点からログを収集します(現在のログ ファイルの現時点から) 。 • **最初から**: 現在のログ ファイルの最初からログを収集します。 このパラメータ値で「最初から」を選択すると、現在のログ ファイルでイベントを保持している期間に応じて、収集されるデータの量が非常に多くなることがあります。このオプションは、最初のコレクション セッションに対してのみ有効なことに注意してください。

パラメータ	説明
ポーリング間隔	ポーリングの間隔(秒) です。デフォルト値は**180**です。 たとえば、180と指定すると、Collectorは、イベント ソースへのポーリングを180秒ごとに実行します。直前のポーリング サイクル(収集)がまだ完了していない場合、そのサイクルが完了するまで待機します。ポーリング中のイベント ソースが多数ある場合、スレッドがビジーになるため、ポーリングが開始するまでに180秒より長くかかる場合があります。
ポーリング最大継続時間	ポーリング サイクルの最大継続時間(サイクルがどれだけ続行されるか) (秒) です。
ポーリング最大イベント数	ポーリング サイクルごとのイベントの最大値(ポーリング サイクルごとに収集されるイベント数) です。
ポーリング最大アイドル時間	ポーリング サイクルの、秒単位のアイドル時間です。0は制限がないことを示します。デフォルト値は> **300**です。
フォワーダ	フォワーダとしてCheck Pointサーバを有効または無効にします。デフォルトでは無効です。
ログ タイプ(名前と値のペア)	名前と値の形式のイベント ソースのログです。デフォルトでは無効です。

パラメータ	説明
デバッグ	**注意**:イベント ソースに問題が発生し、その問題を調査する必要がある場合にのみ、デバッグを有効に(このパラメータをOnまたはVerboseに設定)します。デバッグを有効にすると、Log Collectorのパフォーマンスに影響があります。 イベント ソースのデバッグ ログ記録を有効および無効にします。 有効な値は次のとおりです。 • **Off** = (デフォルト) 無効 • **On** = 有効 • **Verbose** = verboseモードで有効になります。スレッド情報とソース コンテキスト情報をメッセージに追加します。 このパラメータは、イベント収集の問題をデバッグまたは監視するような状況で使用するよう設計されています。パフォーマンスへの影響を最小限にするために、デバッグのVerboseモードは、監視するイベント ソース数が限定された環境で設定するようにしてください。 この値を変更すると、変更はすぐに反映されます(再起動は不要です)。

Check Point収集の稼働状況の確認

次の手順では、**[管理]**>**[ヘルスモニタ]**>**[イベント ソース モニタリング]**タブからCheck Point収集の稼働状況を確認する方法を示しています。

1. **[管理]**>**[ヘルスモニタ]**ビューから**[イベント ソース モニタリング]**タブにアクセスします。
2. **[イベント ソース タイプ]**列で**checkpointfw1**を検索します。
3. **[カウント]**列を確認し、Check Point収集がイベントを受信していることを確認します。

次の手順では、**[調査]**>**[イベント]**ビューからCheck Point収集の稼働状況を確認する方法を示します。

1. **[調査]**>**[イベント]**ビューにアクセスします。
2. **[デバイスの調査]**ダイアログでCheck Pointイベントを集計しているLog Decoder(**LD1**など)を選択します。
3. **[詳細]**列の**[device.type]**フィールドでCheck Pointイベント ソースParser(**checkpointfw1**など)を検索し、Check Point収集がイベントを受信していることを確認します。

注 : VSX Checkpointファイアウォール サーバからのログがLog Collector Checkpointサービスによって収集されている場合、ログのVSX IPを**ip.orig**メタに変換するには、VSXホスト名とVSX IPアドレスをLog Collectorの`/etc/hosts`ファイルに追加する必要があります。

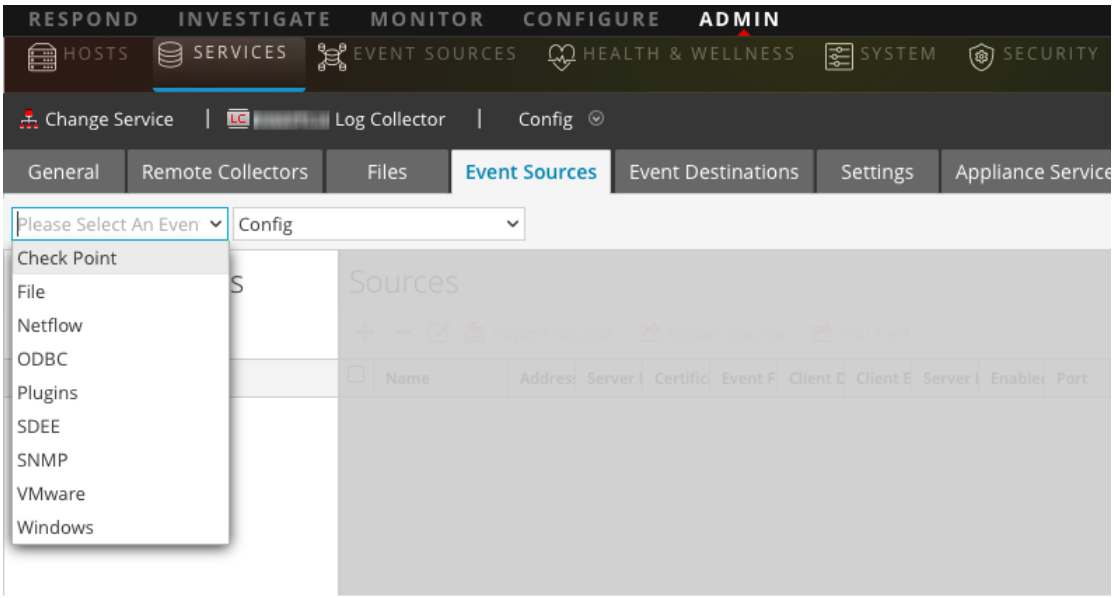
NetWitness Suiteでのファイル イベント ソースの構成

このトピックでは、ファイル収集プロトコルを構成する方法について説明します。

ファイル イベント ソースの構成

ファイル イベント ソースを構成するには、次の手順を実行します。

1. NetWitness Suiteメニューから[**管理**]＞[**サービス**]に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、 ＞[**表示**]＞[**構成**]を選択して、ログ収集に関する構成パラメータのタブを表示します。
4. [**イベント ソース**]タブをクリックします。



5. [**イベント ソース**]タブで、ドロップダウン メニューから[**ファイル/構成**]を選択します。
6. [**イベント カテゴリ**]パネル ツールバーで、 をクリックします。
   [**使用可能なイベント ソース タイプ**]ダイアログが表示されます。
7. ファイル イベント ソース タイプを選択し、[**OK**]をクリックします。
   新しく追加されたイベント ソース タイプが[**イベント カテゴリ**]パネルに表示されます。

8. [**イベント カテゴリ**]パネルで新しいタイプを選択し、[**ソース**]ツールバーで + をクリックします。

   [**ソースの追加**]ダイアログが表示されます。

9. **格納先ディレクトリ**名、およびその他の必要なパラメータを入力します。詳細については、下の「ファイル収集のパラメータ」を参照してください。

10. 公開鍵を取得し、それをダイアログ ボックスに入力するには、次の手順を実行します。

    a. 次のコマンドを実行して、イベント ソースから公開鍵を選択し、コピーします。**cat ~/.ssh/id_rsa.pub**

    b. 公開鍵を[**イベント ソースSSHキー**]フィールドにペーストします。

11. [**OK**]をクリックします。

変更を反映させるには、ファイル収集を再起動する必要があります。

ファイル収集の停止と再開

ファイル収集を使用する新しいイベント ソースを追加した後は、NetWitness Suiteファイル収集サービスを停止して再開する必要があります。これは、新しいイベント ソースにキーを追加するために必要となります。

ファイル収集のパラメータ

次の表に、ファイル収集のソース パラメータの説明を示します。

名前	説明
	基本
格納先ディレクトリ名*	ファイル イベント ソースがそのファイルを格納するディレクトリ(たとえば、**Eur_London100**) 。有効な値は、次の正規表現に従う文字列です。 **[_a-zA-Z][_a-zA-Z0-9]*** ファイル ディレクトリ名は文字で始まる必要があり、数字、文字、下線などが続きます。このパラメータは、イベント データの収集を始めた後は変更できません。 コレクションを作成した後、Log Collectorはcollectionディレクトリの下に、work、save、errorの各サブ ディレクトリを作成します。
アドレス*	イベント ソースのIPアドレス。有効な値は、**IPv4アドレス**、**IPv6アドレス**、ドメインの完全修飾名を含む**ホスト名**です。

名前	説明
収集するファイルの形式 (regex)	正規表現で指定します。たとえば、^.*$ではすべてを処理します。
ファイル エンコーディング	ファイルで多言語対応が必要な場合にファイルのエンコーディングを指定します。ファイルのエンコーディング方式を入力します。次の例は有効な方式です。 • UTF-8(デフォルト) • UCS-16LE • UCS-16BE • UCS-32LE • UCS-32BE • SHIFT-JIS • EBCDIC-US
有効化	イベント ソース構成を有効化して収集を開始するには、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。
拡張	
エンコード変換エラー無視	エンコード変換エラーと無効なデータを無視する場合は、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。 **注意**:これにより、パースと変換のエラーが発生する可能性があります。

名前	説明
ファイルディスククォータ	[**エラー時に保存**]および[**成功時に保存**]パラメータ設定に関係なく、ファイルの保存を停止するタイミングを決定します。たとえば、値が10の場合、使用可能なディスクが10%未満になると、Log Collectorはファイルの保存を停止し、推定される通常収集処理のために十分なスペースを確保します。 **注意**:使用可能なディスクとは、ベースとなるcollectionディレクトリがマウントされているパーティションを指します。Log Collectorサーバに10 TBのディスク サイズがあり、2 TBがベースのcollectionディレクトリに割り当て済みの場合、この値を10に設定すると、ログ収集は残りのスペースが0.2 TB(2 TBの10%) 未満になると停止します。10 TBの10%ではありません。 有効な値の範囲は**0**～**100**です。デフォルト値は**10**です。
シーケンシャル処理	シーケンシャル処理フラグ: • 収集した順にイベント ソース ファイルを処理する場合は、このチェックボックスをオンにします(デフォルト) 。 • 並列でイベント ソース ファイルを処理する場合は、このチェックボックスをオフにします。
エラー時に保存	エラー フラグが発生した場合にファイルを保存します。Log Collectorでエラーが発生したときに**eventsource collection**ファイルを保持する場合は、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。
成功時に保存	処理フラグの完了後に**eventsource collection**ファイルを保存します。ファイルの処理後にeventsource collectionファイルを保存する場合は、このチェックボックスをオンにします。このチェックボックスは、デフォルトではオンになっていません。
イベント ソースSSH キー	このイベント ソースのファイルのアップロードに使用するSSH公開キーです。キーの生成手順については、「SFTP Agentのインストールと更新ガイド」の「*イベント ソースでの鍵ペアの生成およびLog Collectorへの公開鍵のインポート*」を参照してください。 **注**:ファイル収集が停止した場合に、authorized_keysファイルが、このパラメータで追加または変更されたSSH公開キーに、NetWitness Suiteで自動的に更新されることはありません。公開キーを更新するには、ユーザがファイル収集を再開する必要があります。 このパラメータでは、ファイル収集が実行されていなくても、複数のファイル イベント ソースについて公開キーの値を追加または変更できますが、NetWitness Suiteでファイル収集が再開されるまでは、**authorized_keys**ファイルが更新されません。

名前	説明
エラーファイルの管理	デフォルトで、Log Collectorは[**ファイル ディスク クォータ**]パラメータを使用して、ディスクがエラー ファイルでフルにならないようにします。このパラメータを[**有効**]に設定すると、次のいずれかを指定できます。 • [**エラー ファイルのサイズ**]パラメータでエラー ファイルに割り当てる最大容量を指定します。 • [**エラー ファイル数**]パラメータでエラー ファイルの最大数を指定します。 削減量の割合を指定することもできます。このパラメータを指定すると、最大値に達したときに指定された割合でファイルが削減されます。 エラー ファイルを管理する場合は、このチェックボックスをオンにします。このチェックボックスは、デフォルトではオンになっていません。
エラーファイルのサイズ	[**エラー ファイルの管理**]および[**エラー時に保存**]パラメータが[有効]に設定されている場合のみ設定できます。 NetWitness Suiteがどれだけのエラー ファイルを保存するかを指定します。指定する値は、errorディレクトリにあるすべてのファイルの最大合計サイズです。 有効な値の範囲は**0～281474976710655**です。これらの値は、**KB**単位、**MB**単位、**GB**単位のいずれかで指定します。デフォルト値は**100 MB**です。このパラメータを変更した場合、収集を再開するまで、またはLog Collectorのサービスを再起動するまで有効になりません。
エラーファイル数	[**エラー ファイルの管理**]および[**エラー時に保存**]パラメータが[有効]に設定されている場合のみ設定できます。errorディレクトリで許可されるエラー ファイルの最大数を指定します。有効な値の範囲は**0～65536**です。デフォルト値は**65536**です。 このパラメータを変更した場合、収集を再開するまで、またはLog Collectorのサービスを再起動するまで有効になりません。
エラーファイルの削減量	ファイルが最大サイズまたは最大数に達したときに、Log Collectorサービスが削除するエラー ファイルのサイズまたは数の割合を指定します。サービスは、最初に最も古いファイルから削除します。 有効な値の範囲は**0～100**です。デフォルト値は**10**です。

名前	説明
保存ファイルの管理	保存ファイルを管理する場合は、このチェックボックスをオンにします。このチェックボックスは、デフォルトではオンになっていません。 デフォルトで、Log Collectorは[**ファイル ディスク クォータ**]パラメータを使用して、ディスクが保存ファイルでフルにならないようにします。このチェックボックスをオンにすると、次のいずれかを指定できます。 • [**保存ファイルのサイズ**]パラメータで保存ファイルに割り当てる最大容量を指定します。 • [**保存ファイル数**]パラメータで保存ファイルの最大数を指定します。 削減量の割合を指定することもできます。このパラメータを指定すると、最大値に達したときに指定された割合でファイルが削減されます。
保存ファイルのサイズ	[**保存ファイルの管理**]および[**成功時に保存**]パラメータが[有効]に設定されている場合のみ設定できます。 saveディレクトリに格納するすべてのファイルの最大合計サイズを指定します。有効な値の範囲は**0～281474976710655**です。これらの値は、**KB**単位、**MB**単位、**GB**単位のいずれかで指定します。デフォルト値は**100 MB**です。 このパラメータを変更した場合、収集を再開するまで、またはLog Collectorのサービスを再起動するまで有効になりません。
保存ファイル数	[**保存ファイルの管理**]および[**成功時に保存**]パラメータが[有効]に設定されている場合のみ設定できます。saveディレクトリで許可されるエラーファイルの最大数を指定します。有効な値の範囲は**0～65536**です。デフォルト値は**65536**です。 このパラメータを変更した場合、収集を再開するまで、またはLog Collectorのサービスを再起動するまで有効になりません。
保存されたファイルの削減量	ファイルが最大サイズまたは最大数に達したときに、Log Collectorサービスが削除する保存ファイルのサイズまたは数の割合を指定します。サービスは、最初に最も古いファイルから削除します。 有効な値の範囲は**0～100**です。デフォルト値は**10**です。

名前	説明
デバッグ	**注意**:イベント ソースに問題が発生し、その問題を調査する必要がある場合にのみ、デバッグを有効に(このパラメータを「**On**」または「**Verbose**」に設定)します。デバッグを有効にすると、Log Collectorのパフォーマンスに影響が生じる場合があります。 イベント ソースのデバッグ記録を有効または無効にします。 有効な値は次のとおりです。 • **Off** = (デフォルト) 無効 • **On** = 有効 • **Verbose** = verboseモードで有効になります。スレッド情報とソース コンテキスト情報をメッセージに追加します。 このパラメータは、イベント収集の問題をデバッグまたは監視するような状況で使用するよう設計されています。パフォーマンスへの影響を最小限にするために、デバッグのVerboseモードは、監視するイベント ソース数が限定された環境で設定するようにしてください。 この値を変更すると、変更はすぐに反映されます(再起動は不要です)。
キャンセル	イベント ソースを追加または保存せずに、ダイアログを閉じます。
OK	イベント ソースを追加または保存します。

NetWitness SuiteでのNetflowイベント ソースの構成

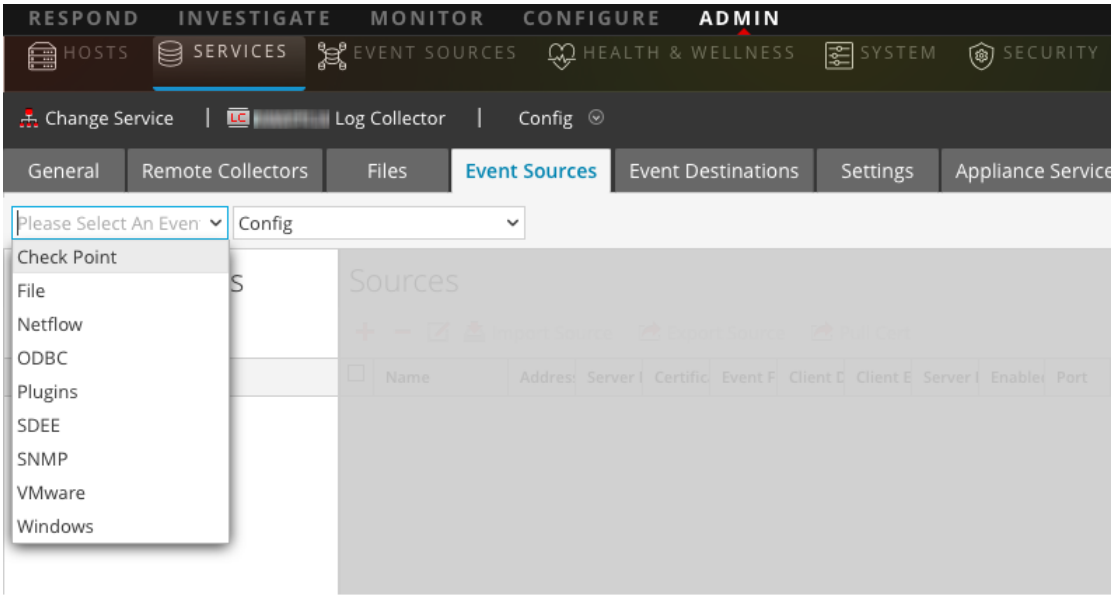
このトピックでは、Netflow収集プロトコルを構成する方法について説明します。

Netflowイベント ソースの構成

Netflowイベント ソースの構成するには、次の手順を実行します。

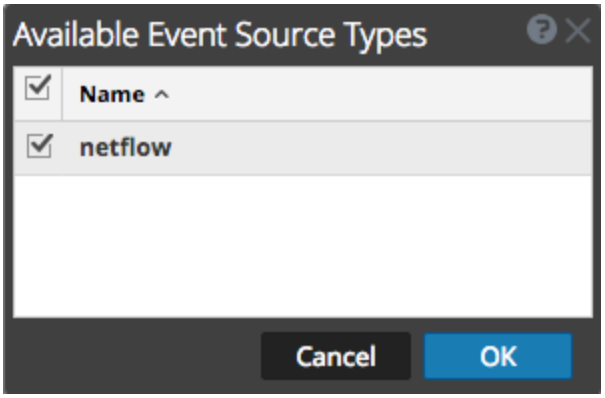
1. NetWitness Suiteメニューから[**管理**]>[**サービス**]に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、[ ]>[**表示**]>[**構成**]を選択して、ログ収集に関する構成パラメータのタブを表示します。

4. [**イベント ソース**]タブをクリックします。



5. [**イベント ソース**]タブで、ドロップダウン メニューから[**Netflow/構成**]を選択します。
6. [**イベント カテゴリ**]パネル ツールバーで、 + をクリックします。

   [**使用可能なイベント ソース タイプ**]ダイアログが表示されます。
7. **netflow**のイベント ソース タイプを選択し、[**OK**]をクリックします。



   新しく追加されたイベント ソース タイプが[**イベント カテゴリ**]パネルに表示されます。
8. [**イベント カテゴリ**]パネルで新しいタイプを選択し、[**ソース**]ツールバーで + をクリックします。

   [**ソースの追加**]ダイアログが表示されます。
9. [**ポート**」フィールドにポート番号を入力して、[有効]チェックボックスがオンになっていることを確認します。

注 : NetWitness Suiteがデフォルトでファイアウォールの2055、4739、6343、9995のポートを開きます。 必要な場合は、Netflow用に他のポートを開きます。

その他のパラメータの詳細については、以下の「Netflow収集のパラメータ」を参照してください。

10. [**OK**]をクリックします。

新しいイベント ソースがリストに表示されます。

Netflow収集のパラメータ

次の表に、Netflow収集のソース パラメータの説明を示します。

名前	説明
	基本
ポート	Netflowイベント ソースを構成するポート番号を指定します。 NetWitness Suiteはデフォルトでは、Netflow用ポート2055、4739、6343、9995を開きます。必要な場合は、Netflow用に他のポートを開きます。
有効化	イベント ソース構成を有効化して収集を開始するには、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。
	拡張
インフライト公開ログ閾値	この閾値に達すると、イベント フローの問題を解決するのに役立つログ メッセージがNetWitness Suiteによって生成されます。この閾値には、現在イベント ソースからNetWitness Suiteに流れているnetflowイベント メッセージのサイズを指定します。 有効な値は次のとおりです。 • **0**(デフォルト) : ログ メッセージは無効化されます。 • **100-100000000** - 指定した数のNetflowイベントがこのLog Collectorで処理されると、ログ メッセージが生成されます。 たとえば、この値を「100」に設定すると、特定のバージョン(V5またはV9) のNetflowイベントが100件処理された時点で、NetWitness Suiteによりログ メッセージが生成されます。

名前	説明
デバッグ	**注意**:イベント ソースに問題が発生し、その問題を調査する必要がある場合にのみ、デバッグを有効に(このパラメータを「On」または「Verbose」に設定)します。デバッグを有効にすると、Log Collectorのパフォーマンスに影響が生じる場合があります。 イベント ソースのデバッグ記録を有効または無効にします。 有効な値は次のとおりです。 • **Off** = (デフォルト) 無効 • **On** = 有効 • **Verbose** = verboseモードで有効になります。スレッド情報とソース コンテキスト情報をメッセージに追加します。 このパラメータは、イベント収集の問題をデバッグまたは監視するような状況で使用するよう設計されています。パフォーマンスへの影響を最小限にするために、デバッグのVerboseモードは、監視するイベント ソース数が限定された環境で設定するようにしてください。 この値を変更すると、変更はすぐに反映されます(再起動は不要です)。
キャンセル	イベント ソースを追加または保存せずに、ダイアログを閉じます。
OK	イベント ソースを追加または保存します。

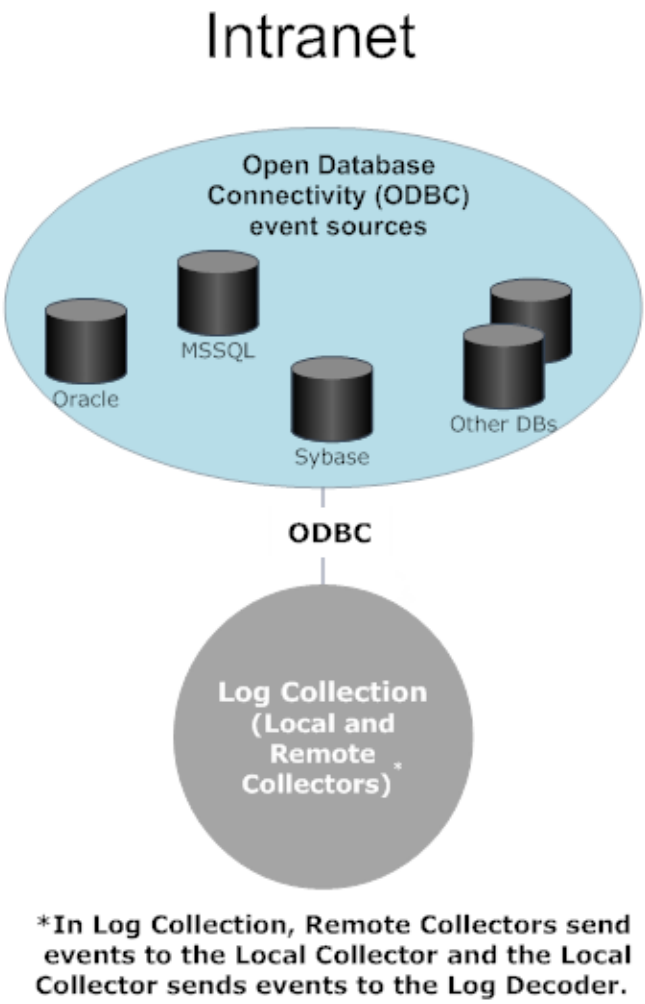
ODBC

NetWitness SuiteでのODBCイベント ソースの構成

このトピックでは、ODBC収集プロトコルの構成方法について説明します。ODBC収集プロトコルでは、ODBC(Open Database Connectivity)ソフトウェア インタフェースを使用して、データベースに監査データを格納するイベント ソースのイベントを収集します。

導入のシナリオ

次の図に、NetWitness SuiteにODBC収集プロトコルを導入する方法を示します。



ODBCイベント ソースの構成

ODBCイベント ソースを構成するには、イベント ソース タイプを構成し、DSNテンプレートを選択する必要があります。

DSNの構成

次の手順では、既存のDSNテンプレートからDSNを追加する方法について説明します。DSNに関連するその他の手順については、「DSN(データ ソース名) の構成」を参照してください。

DSN(データ ソース名) を構成します。

1. [**管理**]＞[**サービス**]に移動します。
2. [**サービス**]グリッドで、**Log Collector**サービスを選択します。
3. [**アクション**]の下の  をクリックし、[**表示**]＞[**構成**]を選択します。
4. Log Collectorの[**イベント ソース**]タブで、ドロップダウン メニューから[**ODBC/DSN**]を選択し

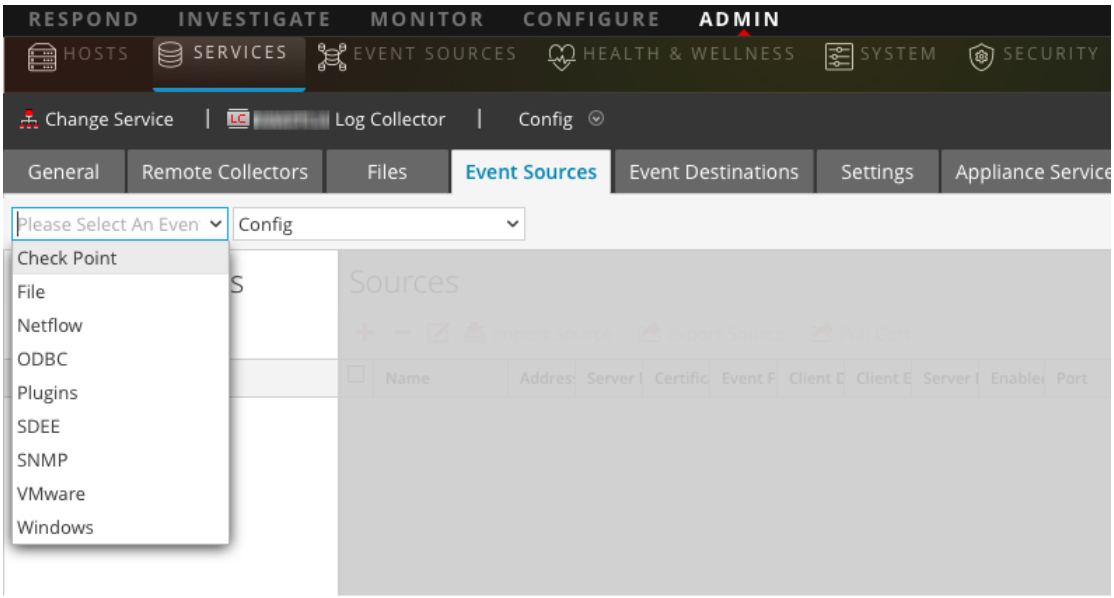
ます。

5. 既存のDSNがある場合は、DSNパネルに表示されます。
6. +をクリックして[**DSNの追加**]ダイアログを開きます。
7. ドロップダウン メニューからDSNテンプレートを選択し、DSNの名前を入力します (ODBCイベント ソース タイプを設定するときに、この名前を使用します)。必要に応じて、Manage Templatesをクリックしてテンプレートを追加または削除します。
8. パラメータを入力し、[**保存**]をクリックします。

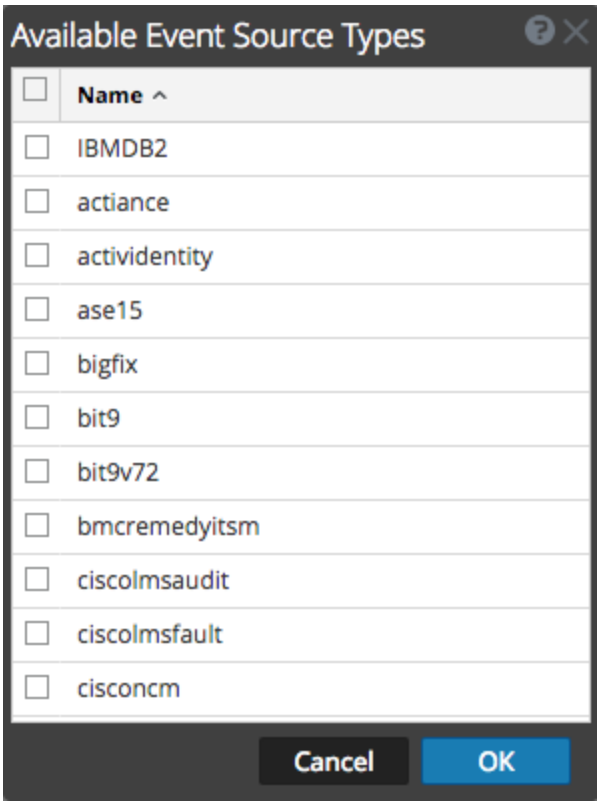
イベント ソース タイプの追加

ODBCイベント ソース タイプを構成するには、次の手順を実行します。

1. [**管理**]>[**サービス**]に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、>[**表示**]>[**構成**]を選択して、ログ収集に関する構成パラメータのタブを表示します。
4. [**イベント ソース**]タブをクリックします。



5. [**イベント ソース**]タブで、ドロップダウン メニューから[**ODBC/構成**]を選択します。
6. [**イベント カテゴリ**]パネル ツールバーで、+をクリックします。
   [**使用可能なイベント ソース タイプ**]ダイアログが表示されます。

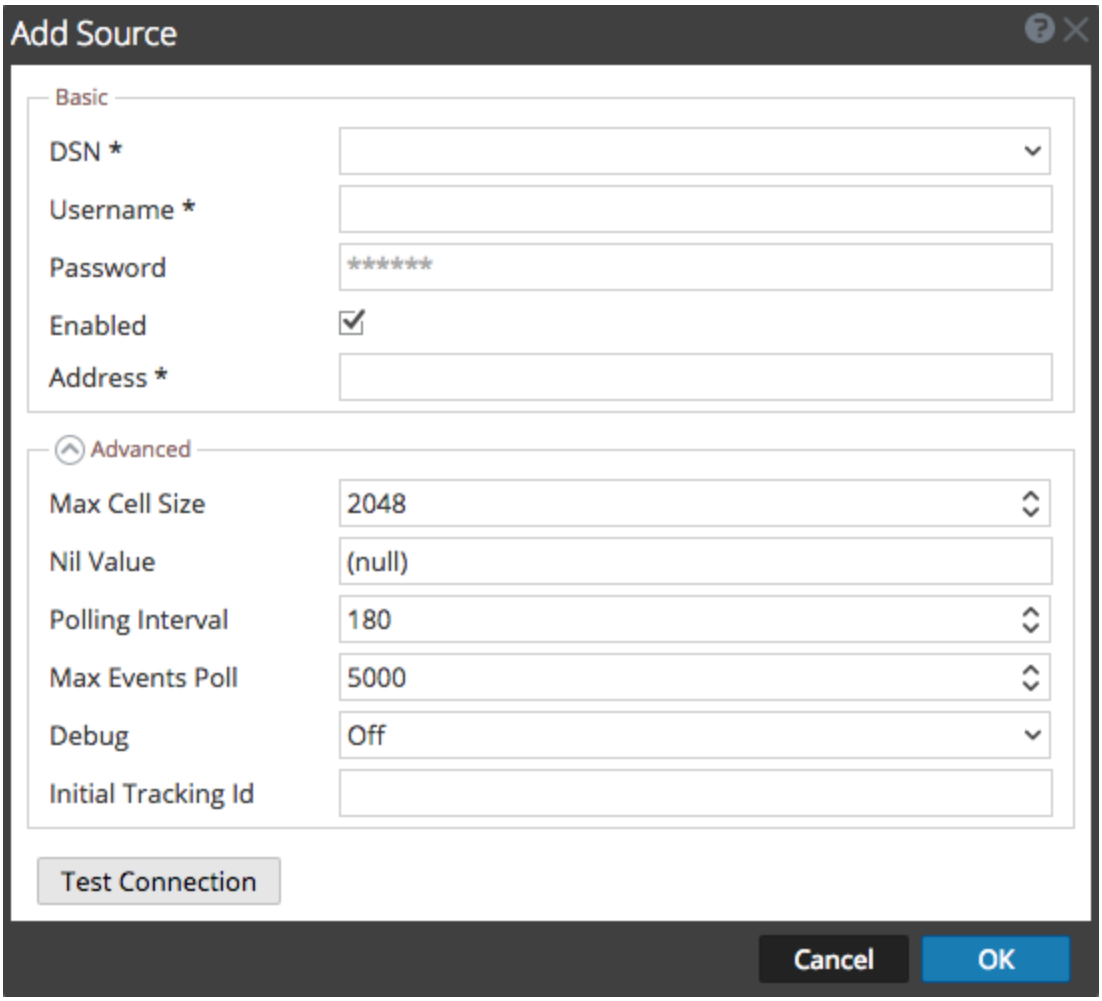


7. イベント ソースのカテゴリ(例 : **mssql**) を選択し、[**OK**] をクリックします。

   新しく追加されたイベント ソース タイプが[**イベント カテゴリ**] パネルに表示されます。

8. [**イベント カテゴリ**] パネルで新しいタイプを選択し、[**ソース**] ツールバーで + をクリックします。

   [**ソースの追加**] ダイアログが表示されます。



9. ドロップダウン リストからDSNを選択し、必要に応じて他のパラメータを指定または変更して［**OK**］をクリックします。
10. ［**接続のテスト**］をクリックします。

    テストの結果がダイアログ ボックスに表示されます。テストが失敗した場合は、DSN情報を編集し、再試行します。

    注：Log Collectorでは、約60秒後にテストの結果を返します。制限時間を超えると、テストがタイムアウトになり、NetWitness Suiteサーバはエラー メッセージを表示します。

11. テストが正常に実行された場合は、［**OK**］をクリックします。

新たに定義したDSNが［**ソース**］パネルに表示されます。

ODBC収集のパラメータ

次の表に、ODBC収集のソース パラメータの説明を示します。

DSN(データ ソース名) の構成

このトピックでは、ODBCによるデータ収集のためのDSNを作成および管理するための方法について説明します。

はじめに

ODBC(Open Database Connectivity) イベント ソースを登録するには、データ ソース名 (DSN) が必要です。ODBCイベント ソースの構成に必要なパラメータ(値 ペア)を設定して、DSNを定義する必要があります。

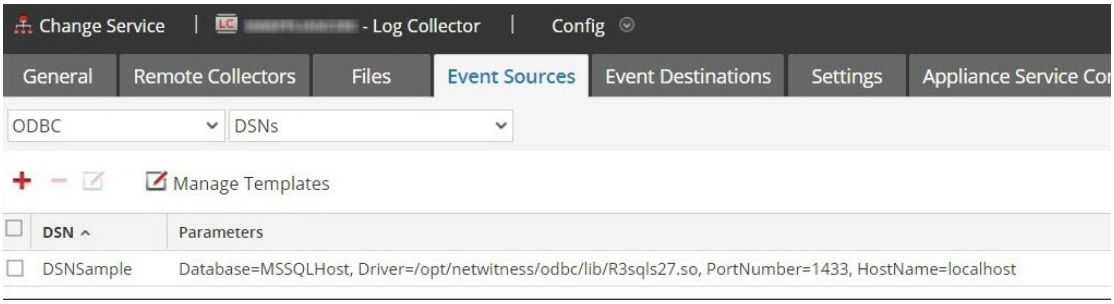
[DSN] パネルへの移動

DSNまたはDSNテンプレートを追加または編集するには、最初に適切な画面に移動します。

DSNテンプレート パネルに移動するには、次の手順に従います。

1. **[管理] > [サービス]** へ進みます。
2. [**サービス**] グリッドで**Log Collector**サービスを選択します。
3. [**アクション**] の下の をクリックし、**[表示] > [構成]** を選択します。
4. Log Collectorの[**イベント ソース**] タブで、ドロップダウン メニューから[**ODBC/DSN**] を選択します。

   追加されたDSNがある場合は、**DSN**パネルに表示されます。



この画面では、次のアクションを実行できます。

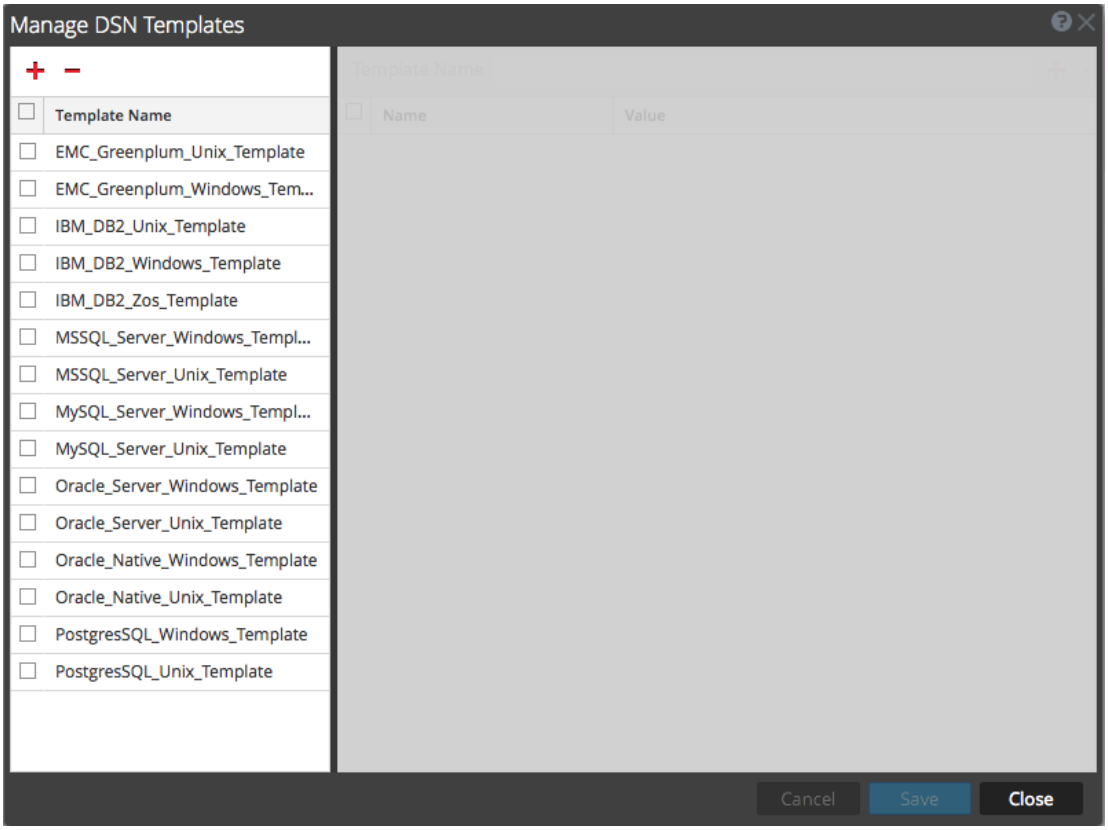
- 新しいDSNテンプレートの追加
- 既存のテンプレートからのDSNの追加
- 既存のDSNテンプレートを編集してDSNを追加
- DSNまたはDSNテンプレートの削除

新しいDSNテンプレートの追加

ニーズに合う定義済みDSNテンプレートがない場合は、次の処理手順を使用してDSNテンプレートを追加します。

1. [DSN]パネルで Manage Templates をクリックします。

   [**DSNテンプレートの管理**]ダイアログが表示されます。



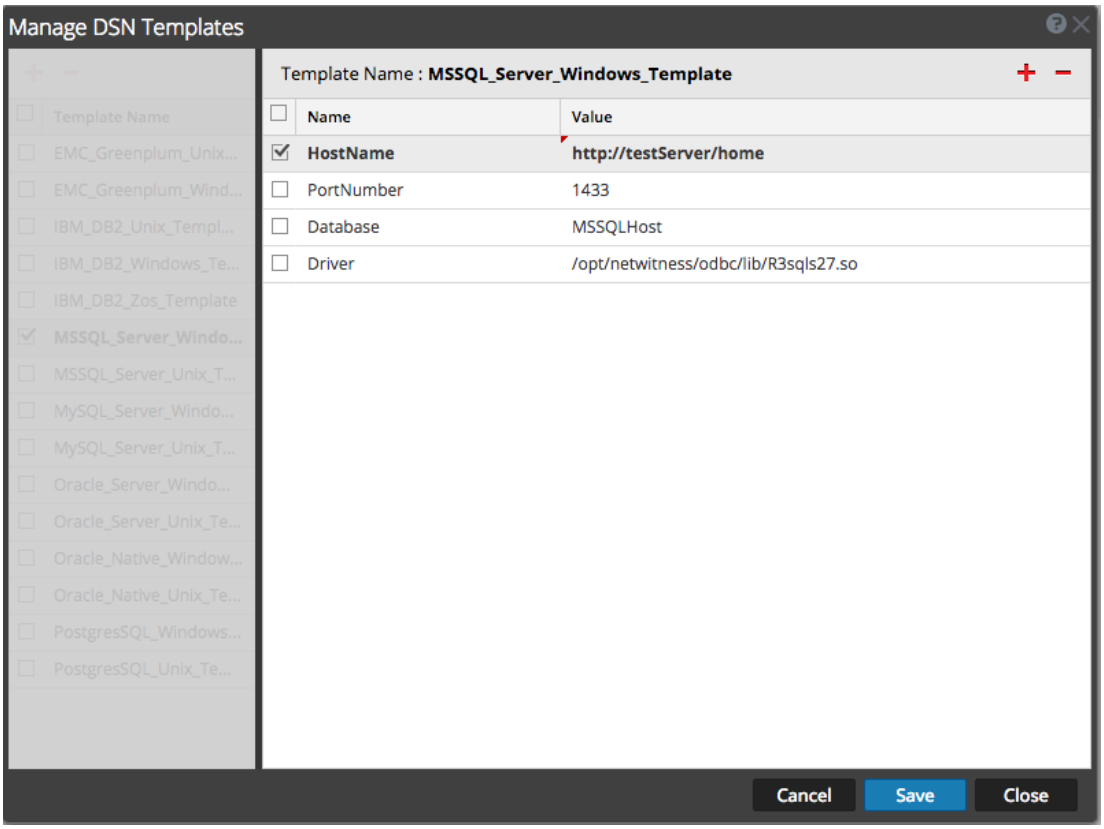
   注:左側パネルには、新しいDSNを追加するときに使用できるデフォルトのテンプレートが用意されています。

2. + をクリックします。

   右パネルがアクティブになります。

3. テンプレート名を指定して、右パネルの + をクリックしてパラメータを追加します。

4. パラメータを指定します。[**保存**]をクリックします。



新しいDSNテンプレートが[**DSNテンプレートの管理**]リストに追加されます。

既存のテンプレートからのDSNの追加

既存のテンプレートを選択し、ニーズに合わせてパラメータを設定できます。

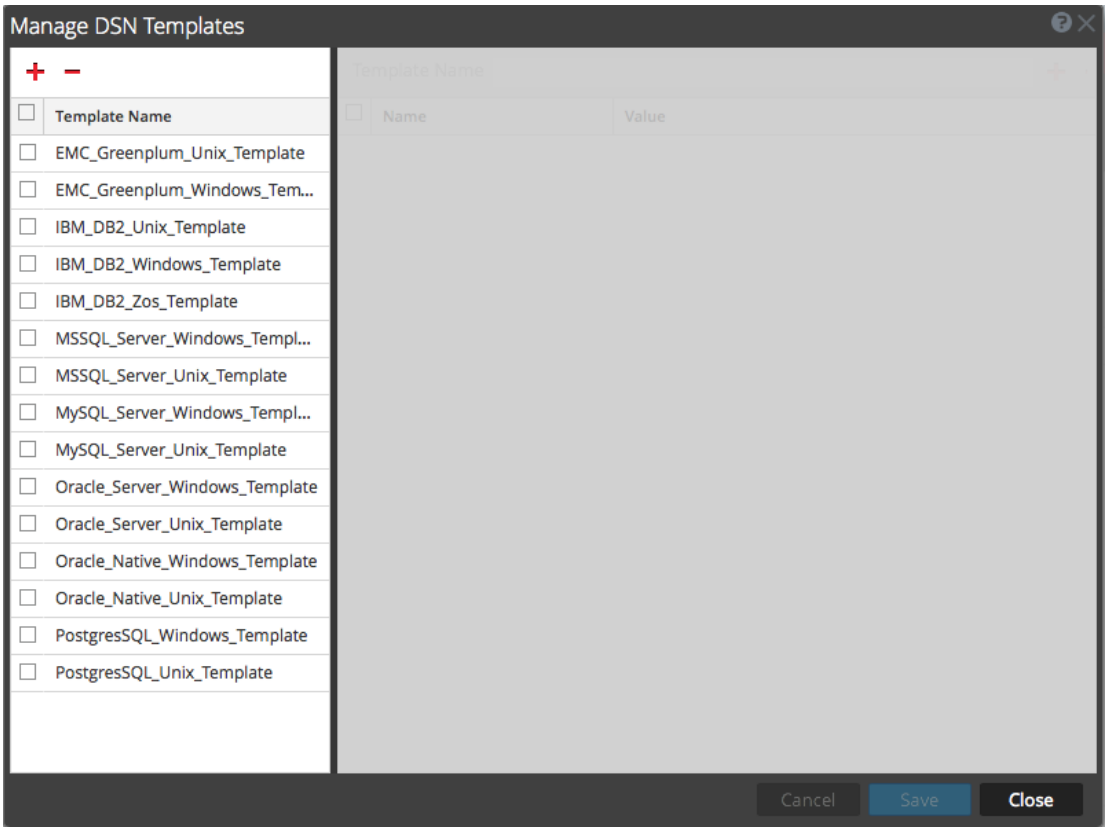
1. [DSN]パネルで + をクリックし、[DSNの追加]ダイアログボックスを開きます。
   既存のDSNを示す(存在する場合)[**DSNの追加**]ダイアログが表示されます。
2. ドロップダウンメニューからDSNテンプレートを選択し、DSNの名前を入力します(ODBCイベントソースタイプを設定する場合にこの名前を使用します)。
3. パラメータを入力し、[**保存**]をクリックします。

DSNがDSNのリストに追加されます。

既存のDSNテンプレートを編集して新しいDSNを追加

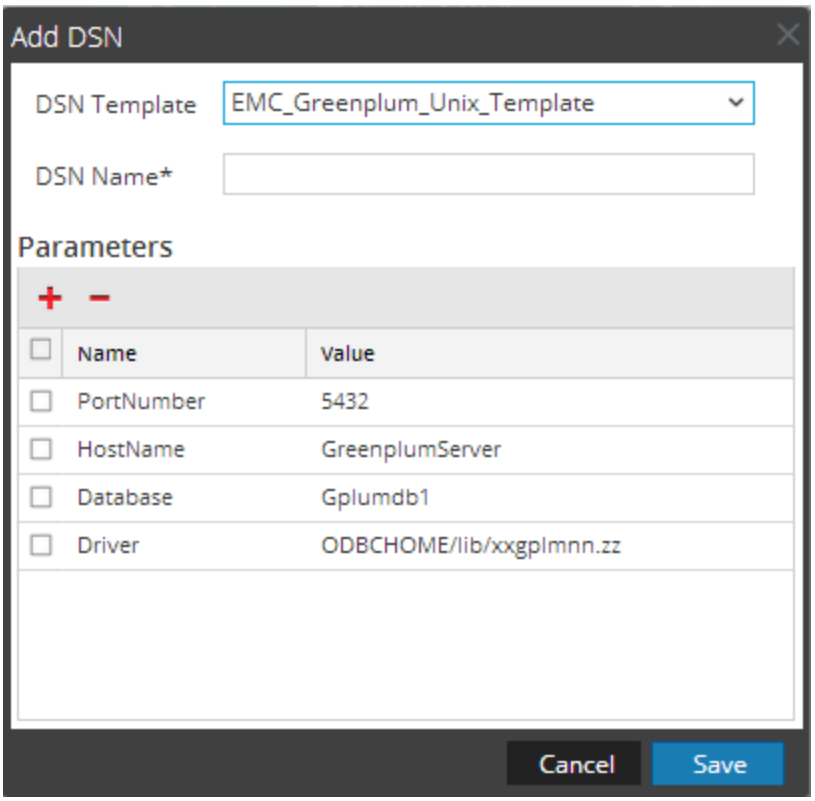
ニーズに合わせて既存のDSNテンプレートを更新してDSNを追加できます。

1. [DSN]パネルで Manage Templates をクリックします。
   [**DSNテンプレートの管理**]ダイアログが表示されます。



2. 変更する既存のテンプレートを選択します。

   右側のパネルが有効になり、選択したテンプレートのデフォルト パラメータが表示されます。



3. [**DSN名**]フィールドで名前を指定します。
4. デフォルトのパラメータを追加、削除、編集します。
5. 必要なパラメータのセットを作成したら[**保存**]、[**閉じる**]の順にクリックします。
6. ドロップダウン メニューから更新した[DSNテンプレート]を選択し、DSNの名前を入力します(ODBCイベント ソース タイプを設定する場合にこの名前を使用します)。
7. パラメータを入力し、[**保存**]をクリックします。

DSNがDSNのリストに追加されます。

DSNまたはDSNテンプレートの削除

不要になったDSNまたはDSNテンプレートは、システムから削除することができます。

既存のDSNを削除するには、次の手順に従います。

1. [DSN]パネルで既存のDSNを選択します。
2. ーをクリックします。

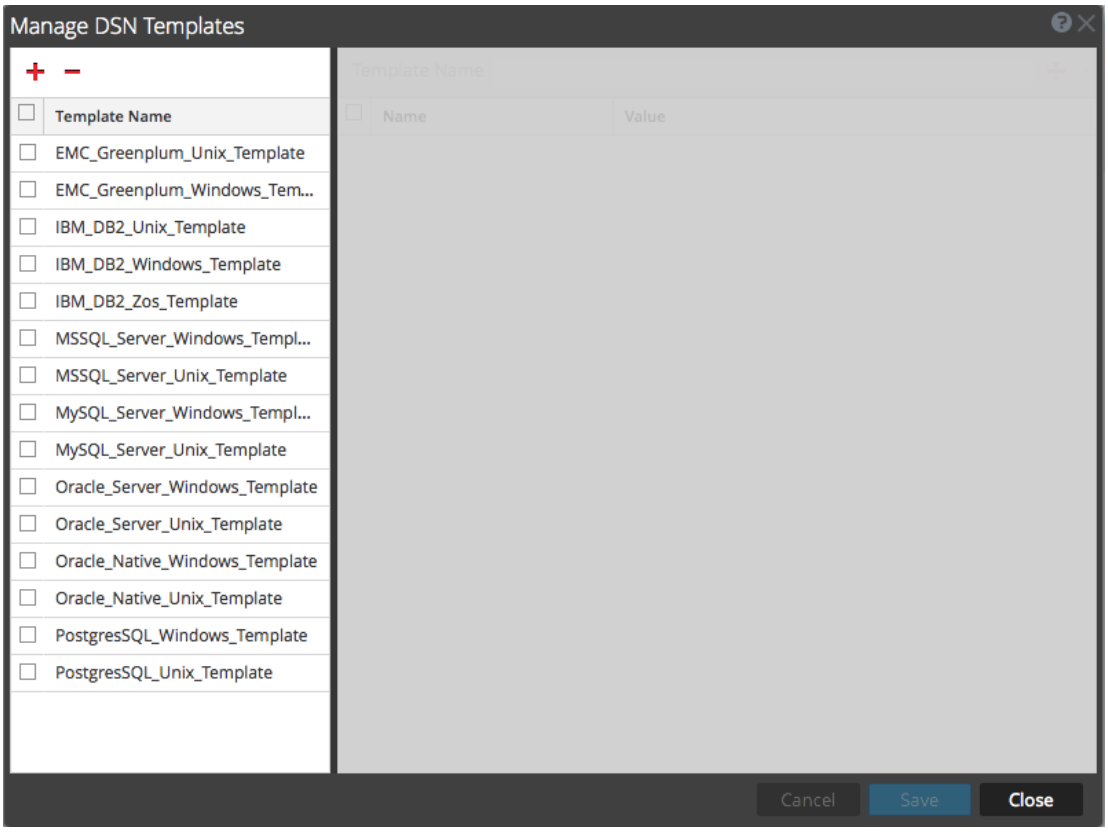
   DSNを削除するかどうかを確認する警告メッセージが表示されます。
3. DSNを削除するには、[**はい**]をクリックします。または、削除をキャンセルするには、[**いいえ**]をクリックします。

削除を確定した場合、選択したDSNがシステムから削除されます。

既存のDSNテンプレートを削除するには、次の手順に従います。

1. [DSN]パネルで Manage Templates をクリックします。

   [**DSNテンプレートの管理**]ダイアログが表示されます。



2. [DSN]パネルで既存のDSNテンプレートを選択します。
3. ー をクリックします。

   DSNテンプレートを削除するかどうかを確認する警告メッセージが表示されます。

4. DSNテンプレートを削除するには、[**はい**]をクリックします。または、削除をキャンセルするには、[**いいえ**]をクリックします。

削除を確定した場合、選択したDSNテンプレートがシステムから削除されます。

ODBC収集用のカスタムのTypespecの作成

このトピックでは、Log CollectorのカスタムTypespecを作成する方法について説明します。トピックには次の項目が含まれます。

- カスタムTypespecの作成手順
- ODBC収集Typespec構文
- ODBC収集Typespecファイルのサンプル

カスタムTypespecの作成

カスタムTypespecファイルを作成するには、次の手順を実行します。

1. SFTPクライアント(たとえば、WinSCP)を開き、Log CollectorまたはリモートLog Collectorに接続します。
2. **/etc/netwitness/ng/logcollection/content/collection/odbc**に移動して、既存のファイル(たとえば、**bit9.xml**)をコピーします。
3. 要件に応じてファイルを変更します。詳細については、「ODBC収集Typespec構文」を参照してください。
4. ファイルの名前を変更し、同じディレクトリに保存します。
5. Log Collectorを再起動します。

注: Log Collectorを再起動するまで、NetWitness Suiteに新しいイベント ソース タイプは表示されません。

ODBC収集Typespec構文

以下の表は、typespecパラメータについての説明です。

パラメータ	説明
name	ODBCイベント ソースの表示名(たとえば、**actividentity**)。NetWitness Suiteでは、**[表示]>[構成]>[イベント ソース]**タブの**[ソース]**パネルにこの名前が表示されます。 有効な値は英数字の文字列です。-(ダッシュ)、_(下線)、またはスペースは使用できません。この名前は、フォルダ内のすべてのtypespecファイル全体にわたり一意である必要があります。
type	イベント ソース タイプ: **odbc**。この行は変更しないでください。
prettyName	イベント ソースのユーザ定義名。nameと同じ値(たとえば、apache)を使用するか、もっと分かりやすい名前を使用することができます。
version	このtypespecファイルのバージョン。デフォルト値は1.0です。
author	typespecファイルの作成者。author-nameは、自分の名前に置き換えてください。

パラメータ	説明
description	イベント ソースの正式な説明。formal-descriptionは、イベント ソースの実際の説明に置き換えてください。
	<device>セクション
parser	このオプションのパラメータにはログ パーサの名前が含まれています。この値は、このイベント ソースからログを解析するときに、指定したログ パーサを使用するようLog Decoderを強制します。 **注**:使用するログ パーサが不明である場合は、このフィールドを空白のままにします。
name	ODBCイベント ソースの名前(たとえば、**ActivIdentity ActivCard AAA Server**)。
maxVersion	イベント ソースのバージョン番号(たとえば、**6.4.1**)。
description	イベント ソースの説明。
	<collection>セクション
odbc	`<odbc>`の下の構文は、イベントの収集および処理に使用されます。`<query>`タグを追加することで、同じイベントソース タイプに対して複数のクエリを指定できます。
query	このセクションには、イベント ソースから情報を収集するために使用するクエリの詳細を記述します。
tag	変換時にイベントに追加するプレフィックス タグ(たとえば、**ActivIdentity**)。
outputDelimiter	フィールドを区切るために使用する区切り文字を指定します。次のいずれかの値を指定します。 • ||(パイプ) • ^(キャレット) • ,(コンマ) • :(コロン) • **0x20**(スペースを表します)
interval	イベントとイベントの間の秒数を指定します。デフォルト値は**60**です。

パラメータ	説明
dataQuery	SQL-syntaxには、ODBCイベントソースのデータベースからデータを取得するクエリを指定します。例： `SELECT acceptedrejected, servername, serveripa, sdate, millisecond, suid, groupname, ipa, reason, info1, info2, threadid FROM A_AHLOG WHERE sdate > '%TRACKING%' ORDER BY sdate`
maxTrackingQuery	データセットからのログの収集を開始するために、データセット内の起点を特定するイベントの最初の収集に使用するクエリ。最初の収集の実行後、**maxTracking**値がリセットまたは変更されるまで、このクエリは使用されなくなります。例： `SELECT MAX(Event_Id) from ExEvents`
trackingColumn	ODBC Collectorが新たなイベントを収集する際に使用するトラッキング列の名前。

ODBC収集Typespecファイルのサンプル

次のサンプルは、IBM ISS SiteProtectorイベント ソースのためのtypespecファイルです。

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

   <name>siteprotector4_x</name>
   <type>odbc</type>
   <prettyName>SITEPROTECTOR4_X</prettyName>
   <version>1.0</version>
   <author>Administrator</author>
   <description>Collects events from SiteProtector</description>

   <device>
      <name>Internet Security Systems, Inc. RealSecure SiteProtector v 2.0</name>
      <maxVersion>2.0</maxVersion>
      <description></description>
      <parser>iss</parser>
   </device>

   <configuration>
   </configuration>

   <collection>
      <odbc>
```

```
         <query>
            <tag></tag>
            <outputDelimiter></outputDelimiter>
            <interval></interval>
            <dataQuery></dataQuery>
            <maxTrackingQuery></maxTrackingQuery>
            <trackingColumn></trackingColumn>
            <levelColumn></levelColumn>
            <eventIdColumn></eventIdColumn>
            <addressColumn></addressColumn>
         </query>
      </odbc>
   </collection>
</typespec>
```

次のサンプルは、Bit9 Security Platformイベント ソースのためのtypespecファイルです。

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

   <name>bit9</name>
   <type>odbc</type>
   <prettyName>BIT9</prettyName>
   <version>1.0</version>
   <author>Administrator</author>
   <description>Bit9 Events</description>

   <device>
      <name>Bit9</name>
      <parser>bit9</parser>
   </device>

   <configuration>
   </configuration>

   <collection>
      <odbc>
         <query>
            <tag>BIT9</tag>
            <outputDelimiter>||</outputDelimiter>
            <interval>10</interval>
            <dataQuery>
```

```
            SELECT
            Timestamp,
            Event_Id,
            Computer_Id,
            File_Catalog_Id,
            Root_File_Catalog_Id,
            Priority,
            Type,
            Subtype,
            IP_Address,
            User_Name,
            Process,
            Description
            FROM
            ExEvents
            WHERE
            Event_Id > '%TRACKING%'
            </dataQuery>
            <trackingColumn>Event_Id</trackingColumn>
            <maxTrackingQuery>SELECT MAX(Event_Id) from
ExEvents</maxTrackingQuery>
            <eventIdColumn></eventIdColumn>
         </query>
      </odbc>
   </collection>
</typespec>
```

ODBC収集のトラブルシューティング

収集の実行中にODBC Collectorのログ情報、警告、エラー メッセージを確認し、ODBC収集の監視と問題のトラブルシューティングを行うことができます。

各ODBCログ メッセージには次の項目が含まれます。

- タイム スタンプ
- カテゴリ: `debug`、`info`、`warning`、または`failure`
- 収集方法 = `OdbcCollection`
- ODBCイベントソース タイプ(GOTS-name) = イベント ソースで構成したGeneric ODBC Type Specificationの名前。
- 完了または試行した収集ファンクション(たとえば、`[processing]`)

- ODBCイベントソース名 (DSN名) = イベント ソースで構成したデータ ソース名。
- 説明(たとえば、Log Collectorが収集したイベントの数)
- トラッキングID = 対象となるデータベース テーブルのLog Collectorの位置。

次の例は、ODBCイベントが正常に収集されたときに記録されるメッセージです。

```
2014-July-25 17:21:25 info (OdbcCollection) : [event-source]
[processing] [event-source] Published 100 ODBC events: last tracking
id: 2014-July-25 13:22:00.280
```

次の例は、ODBCイベントが正常に収集されなかったときに記録されるメッセージです。

ログメッセージ	`timestamp failure (OdbcCollection: [event-source] [processing] [event-source-type] Failed during doWork: Unable to prepare statement: state: S0002; error-code:208; description: [RSA] [ODBC-driver] [event-source-type] Invalid object name 'object-name'.`
考えられる原因	ODBCドライバまたはターゲット データベースにアクセスする際にODBC収集が失敗しました。
解決策	イベント ソースのDSNと値のペアを確認します。

NetWitness SuiteでのSDEEイベント ソースの構成

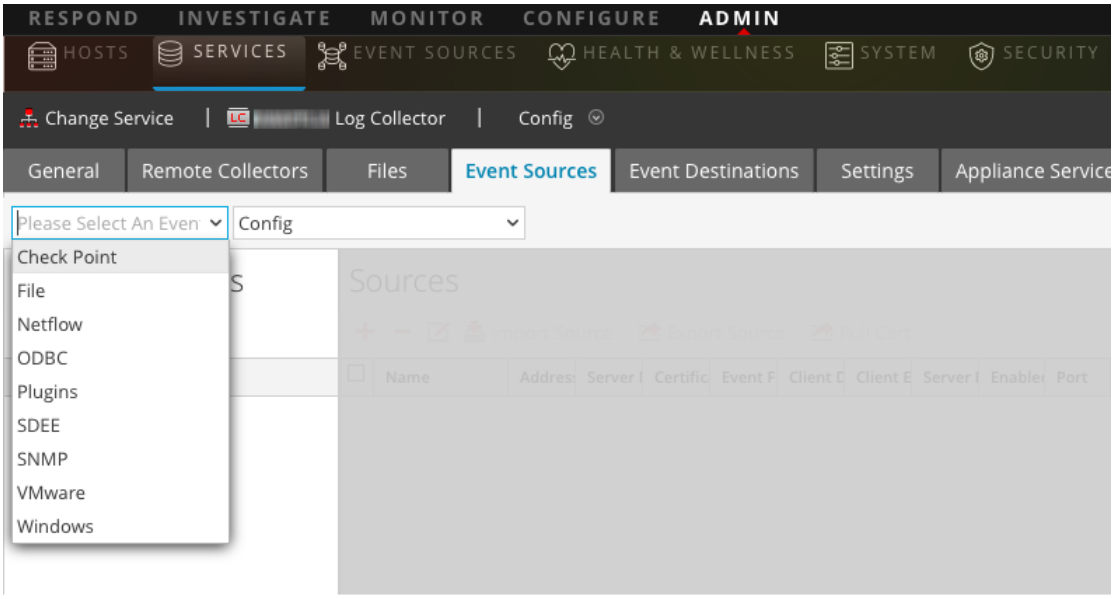
このトピックでは、SDEE収集プロトコルを構成する方法について説明します。

SDEEイベント ソースの構成

SDEEイベント ソースを追加するには、次の手順を実行します。

1. **[管理]＞[サービス]**に移動します。
2. [Log Collector]サービスを選択します。

3. [アクション]で、 > [**表示**] > [**構成**]を選択して、ログ収集に関する構成パラメータのタブを表示します。
4. [**イベント ソース**]タブをクリックします。



5. [**イベント ソース**]タブで、ドロップダウン メニューから[**SDEE/構成**]を選択します。

   [イベント カテゴリ]パネルに、構成済みのSDEEイベント ソースが表示されます(存在する場合)。

6. [**イベント カテゴリ**]パネル ツールバーで、 をクリックします。

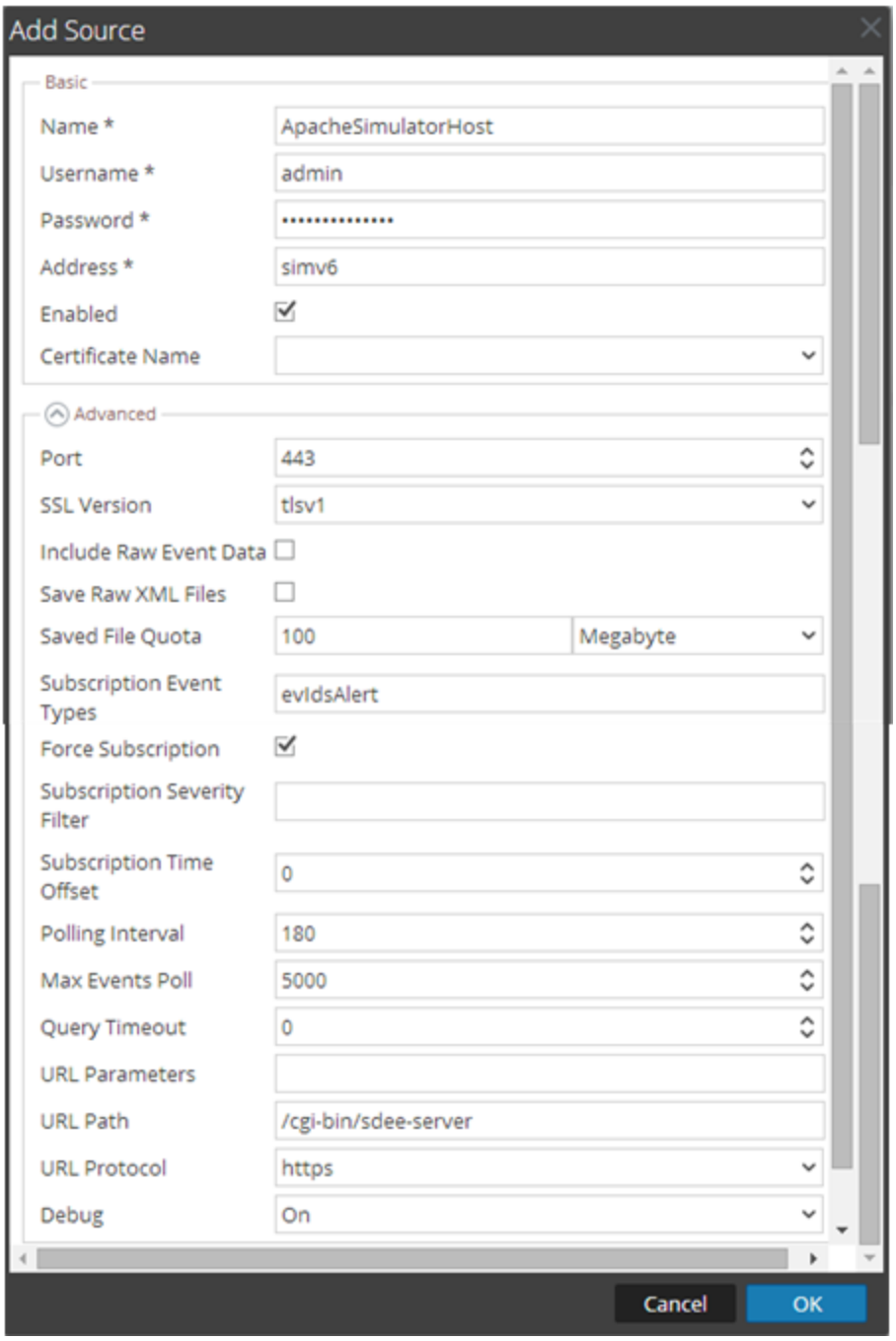
   [**使用可能なイベント ソース タイプ**]ダイアログが表示されます。

7. イベント ソース タイプを選択し、[**OK**]をクリックします。

   新しく追加されたイベント ソース タイプが[**イベント カテゴリ**]パネルに表示されます。

8. [イベント カテゴリ]パネルで追加したイベント ソース タイプを選択し、[ソース]パネルのツールバーで + をクリックします。

   [ソースの追加]ダイアログが表示されます。



9. 名前、ユーザ名、アドレス、パスワードを追加し、その他の必要なパラメータを入力して、[**OK**]をクリックします。

NetWitness SuiteでのSNMPイベント ソースの構成

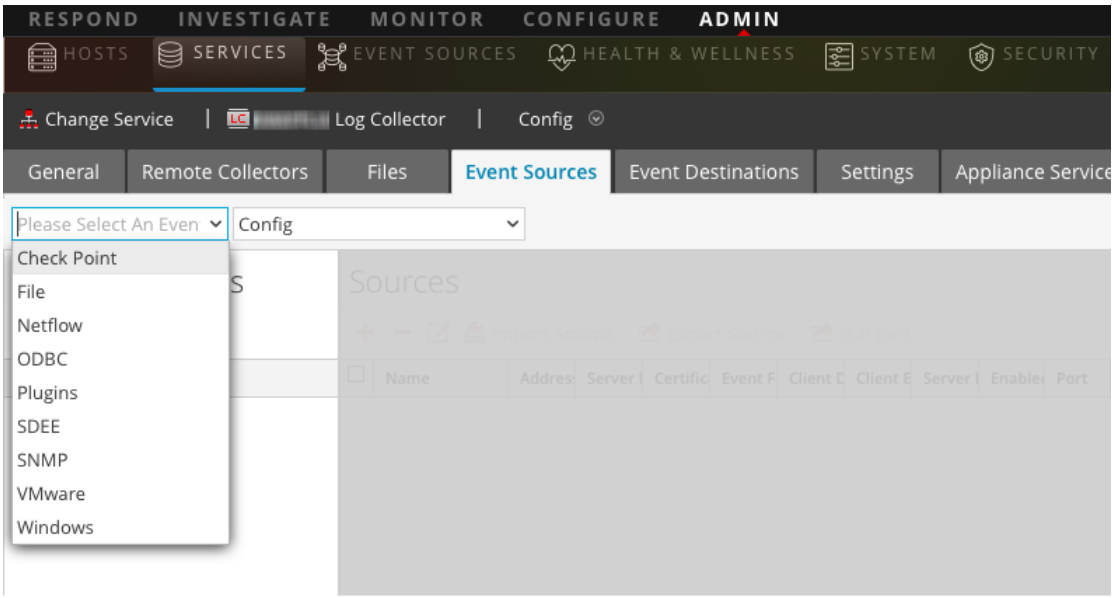
このトピックでは、SNMP収集プロトコルを構成する方法について説明します。

SNMPトラップ イベント ソースの構成

SNMPイベント ソースを追加するには、次の手順を実行します。

注：以前に**snmptrap**タイプを追加している場合は、このタイプを再度追加することはできません。このタイプを編集するか、ユーザを管理することはできます。

1. NetWitness Suiteメニューから[**管理**]＞[**サービス**]に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、 ＞[**表示**]＞[**構成**]を選択して、ログ収集に関する構成パラメータのタブを表示します。
4. [**イベント ソース**]タブをクリックします。



5. [**イベント ソース**]タブで、ドロップダウン メニューから[**SNMP/構成**]を選択します。
6. [**イベント カテゴリ**]パネル ツールバーで、 をクリックします。
   [**使用可能なイベント ソース タイプ**]ダイアログが表示されます。
7. **snmptrap**イベント ソース タイプを選択し、[**OK**]をクリックします。
   新しく追加されたイベント ソース タイプが[**イベント カテゴリ**]パネルに表示されます。
8. [イベント カテゴリ]パネルで[**snmptrap**]を選択します。

9. [ソース]パネルで[**snmptrap**]を選択してから、編集アイコン( ) をクリックしてパラメータを編集します。
10. 変更する必要があるいずれかのパラメータを更新し、[**OK**]をクリックします。

(オプション) SNMPユーザの構成

SNMPv3を使用している場合は、次の手順に従ってSNMP v3ユーザを更新および維持します。

SNMP v3ユーザの構成

1. [**管理**]>[**サービス**]に移動します。
2. [**サービス**]グリッドで、**Log Collector**サービスを選択します。
3. [**アクション**]の下の をクリックし、[**表示**]>[**構成**]を選択します。The SNMP v3 User panel is displayed with the existing users, if any.
4. Log Collectorの[**イベント ソース**]タブで、[**SNMP/SNMP v3ユーザ マネージャ**]をドロップダウン メニューから選択します。

   既存のユーザが存在する場合、[SNMP v3ユーザ]パネルに表示されます。
5. をクリックして[**SNMPユーザの追加**]ダイアログを開きます。
6. ダイアログに必要なパラメータを入力します。使用可能なパラメータは次のとおりです。

SNMPユーザ パラメータ

次の表では、SNMP v3ユーザを作成する際に入力する必要のあるパラメータについて説明します。

パラメータ	説明
ユーザ名*	ユーザの名前(厳密にはSNMP用語でsecurity name)です。 [**ユーザ名**]と[**エンジンID**]の組み合わせは一意になる必要があります(たとえば、**logcollector**)。
エンジンID	(オプション) イベント ソースのエンジンのIDです。この収集サービスにSNMP v3トラップを送信するすべてのイベント ソースについて、送信イベント ソースのユーザ名とエンジンIDを追加する必要があります。 SNMPv3のInformメッセージを送信するイベントソースでは、エンジンIDを空白にして、ユーザ名のみを追加する必要があります。

パラメータ	説明
認証タイプ	(オプション) 認証プロトコルプロトコルを指定できます。有効な値は、以下のとおりです。 • **なし**(デフォルト):このサービスに送信されるトラップには、**noAuthNoPriv**のセキュリティレベルしか使用できません • **SHA**: Secure Hash Algorithm • **MD5**: Message Digest Algorithm。**使用不可:FIPSモードで実行されているLog Collectorと競合するため、MD5を選択しないでください。**
認証パスフレーズ	[**認証タイプ**]を設定しない([なし]に設定)場合には設定しません。認証パスフレーズです。
プライバシータイプ	(オプション) プライバシープロトコルです。このパラメータは、認証タイプパラメータが設定されている場合にのみ設定できます。有効な値は、以下のとおりです。 • **None**(デフォルト) • **AES**:高度暗号化標準 • **DES**:データ暗号化標準**使用不可:FIPSモードで実行されているLog Collectorと競合するため、DESを選択しないでください。**
プライバシーパスフレーズ	[**プライバシータイプ**]を設定しない([なし]に設定)場合には設定しません。プライバシーパスフレーズ。
閉じる	SNMP v3ユーザを追加しないか、パラメータに対する変更を保存せずに、ダイアログを閉じます。
保存	SNMP v3ユーザパラメータを追加するか、パラメータに対する変更を保存します。

リモートCollectorに対するSyslogイベントソースの構成

このトピックでは、Log CollectorLog CollectorにSyslogイベントソースを構成する方法について説明します。

Syslogの収集はローカルLog Collectorに対して構成しないでください。リモートCollectorに対してのみ、Syslogの収集を構成する必要があります。

Syslogイベント ソースの構成

注：必要な作業は、Syslogを使用してその出力をRSA NetWitness Suiteに送信するイベント ソースを初めて設定するときに、Syslog収集を構成するだけです。

Syslog用にLog DecoderまたはリモートLog Collectorのいずれかを構成する必要があります。両方を構成する必要はありません。

Syslog収集用にLog Decoderを構成するには、以下の手順を実行します。

1. **[管理]＞[サービス]**に移動します。
2. [サービス]グリッドでLog Decoderを選択し、アクション メニューから＞**[表示]＞[システム]**を選択します。
3. 表示されるアイコンに応じて、次のいずれかを実行します。
   - Start Capture が表示された場合は、アイコンをクリックしてSyslogの収集を開始します。
   - Stop Capture が表示された場合は、何もする必要はありません。このLog Decoderはすでにsyslogを収集しています。

リモートLog CollectorでSyslogの収集を構成するには、次の手順を実行します。

1. **[管理]＞[サービス]**に移動します。
2. [サービス]グリッドで、リモートLog Collector選択し、アクション メニューから＞＞**[表示]＞[イベント ソース]**を選択します。
3. ドロップダウン メニューから、[**Syslog/構成**]を選択します。

   [イベント カテゴリ]パネルに、構成済みのSyslogイベント ソースが表示されます(存在する場合)。
4. [イベント カテゴリ]パネル ツールバーで、＋をクリックします。

   [使用可能なイベント ソース タイプ]ダイアログが表示されます。
5. [**syslog tcp**]または[**syslog udp**]のいずれかを選択します。組織のニーズに応じて、いずれか一方または両方を設定できます。
6. [イベント カテゴリ]パネルで新しいタイプを選択し、[ソース]パネルのツールバーで＋をクリックします。

   [ソースの追加]ダイアログが表示されます。
7. ポートとして「**514**」を入力し、[**有効**]を選択します。必要に応じて、オプションで任意の拡張パラメータを構成します。

   [**OK**]をクリックして変更内容を承認し、ダイアログ ボックスを閉じます。

1つまたは両方のsyslogタイプを構成すると、Log DecoderまたはリモートLog Collectorは、すべての使用可能なイベント ソースからこれらのタイプのメッセージを収集します。そのため、RSA NetWitness Suiteでさらに構成を行う必要なく、Syslogイベント ソースのシステムへの追加を続行できます。

Syslogパラメータ

次の表に、Syslogの構成で使用できるパラメータについて説明します。

名前	説明
	基本
	拡張
OK	イベント ソースを追加または保存します。
キャンセル	イベント ソースを追加または保存せずに、ダイアログを閉じます。
ポート *	デフォルトのポートは**514**です。
インフライト公開ログ閾値	この閾値に達すると、イベント フローの問題を解決するのに役立つログ メッセージがNetWitnessによって生成されます。この閾値には、現在イベント ソースからNetWitnessに流れているSyslogイベント メッセージのサイズを指定します。 有効な値は次のとおりです。 • **0**(デフォルト) : ログ メッセージは無効化されます • **100～100000000**: 現在イベント ソースからNetWitnessに流れているSyslogイベント メッセージが100から100,000,000バイトの範囲内であるとき、ログ メッセージが生成されます。
最大レシーバ数	収集されたSyslogイベントの処理に使用される最大レシーバ リソース数です。 デフォルト値は**2**です。

名前	説明
デバッグ	**注意**：イベント ソースに問題が発生し、その問題を調査する必要がある場合にのみ、デバッグを有効に(このパラメータをOnまたはVerboseに設定) します。デバッグを有効にすると、Log Collectorのパフォーマンスに影響があります。 イベント ソースのデバッグ記録を有効または無効にします。 有効な値は次のとおりです。 • **Off** = (デフォルト) 無効 • **On** = 有効 • **Verbose** = verboseモードで有効になります。スレッド情報とソース コンテキスト情報をメッセージに追加します。 このパラメータは、イベント収集の問題をデバッグまたは監視するような状況で使用するよう設計されています。パフォーマンスへの影響を最小限にするために、デバッグのVerboseモードは、監視するイベント ソース数が限定された環境で設定するようにしてください。 この値を変更すると、変更はすぐに反映されます(再起動は不要です) 。
イベント フィルタ	フィルタを選択します。 フィルタの定義方法に関する説明は、「Collectorのイベント フィルタの構成」を参照してください。
有効	イベント ソース構成を有効化して収集を開始するには、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。

NetWitness SuiteでのVMwareイベント ソースの構成

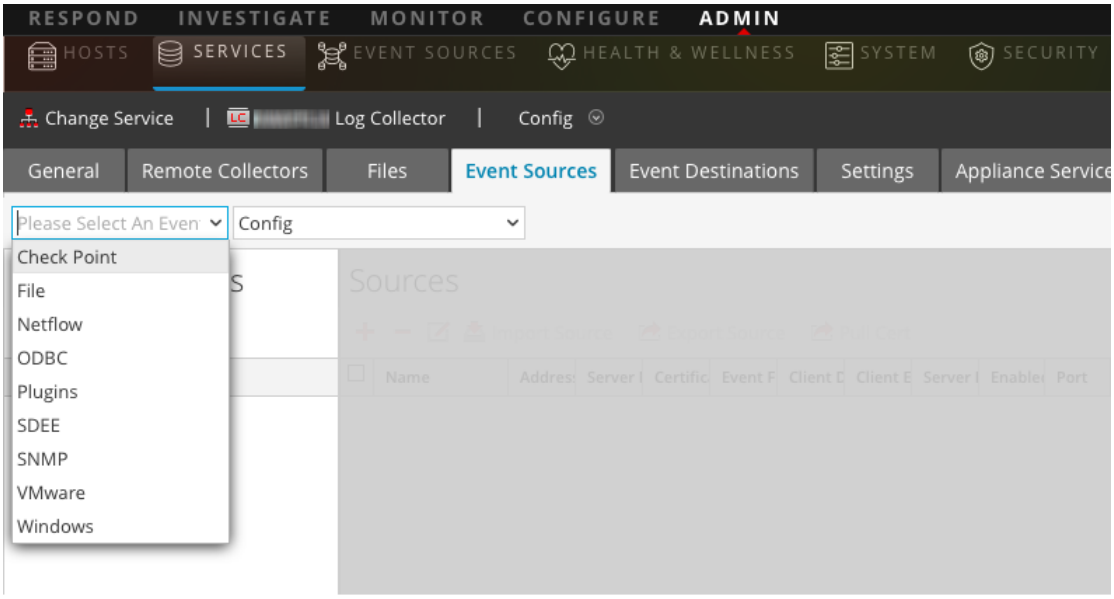
このトピックでは、VMware収集プロトコルの構成方法について説明します。

VMwareイベント ソースの構成

VMwareイベント ソースを追加するには、次の手順を実行します。

1. **[管理]＞[サービス]**に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、[ ]＞**[表示]**＞**[構成]**を選択して、ログ収集に関する構成パラメータのタブを表示します。

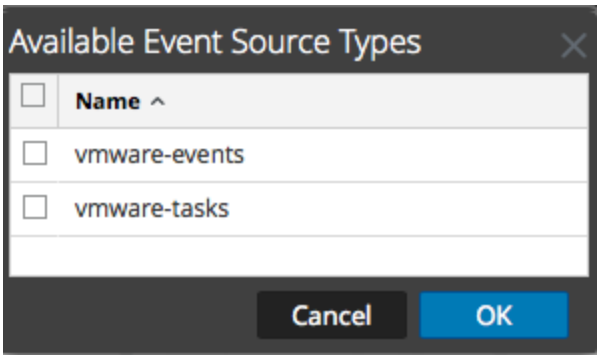
4. [**イベント ソース**]タブをクリックします。



5. Log Collectorの[**イベント ソース**]タブで、ドロップダウン メニューから[**VMware/構成**]を選択します。

   [イベント カテゴリ]パネルに、構成済みのVMwareイベント ソースが表示されます(存在する場合)。

6. [ ]をクリックして、[**使用可能なイベント ソース タイプ**]ダイアログを開きます。



7. [使用可能なイベント ソース タイプ]ダイアログで**vmware-events**または**vmware-tasks**を選択し、[**OK**]をクリックします。

   VMwareの使用可能なイベント ソース タイプは次のとおりです。

   - **vmware-events**: vmware-eventsを構成して、vCenter ServerとVMware ESX/VMware ESXi Serverからイベントを収集します。
   - **vmware-tasks**: (オプション) vmware-tasksを設定して、vCenter Serverからタスクを収集します。

8. [イベント カテゴリ]パネルで新しいタイプを選択し、[ソース]ツールバーで[+]をクリックします。
9. 名前、ユーザ名、パスワードを追加し、修正が必要なその他のパラメータを変更します。

注意:ユーザ名の一部としてドメイン名を入力する場合は、セパレーターとして二重のバックスラッシュを使用する必要があります。たとえば、ドメイン|ユーザ名がcorp\smithjの場合、**corp\\smithj**と指定します。

10. [**OK**]をクリックして、変更内容を保存します。

NetWitness SuiteでのWindowsイベント ソースの構成

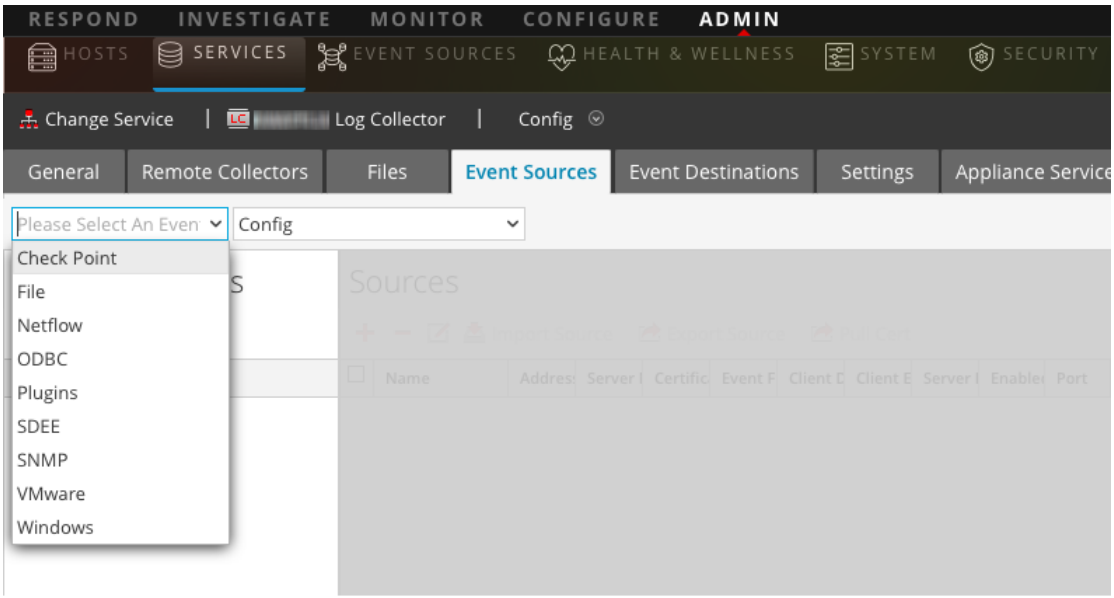
このトピックでは、Windows収集プロトコルを構成する方法について説明します。

Windowsイベント ソースの構成

RSA NetWitness Suiteで、Kerberosレルムを構成し、Windowsイベント ソース タイプを追加する必要があります。

Windows収集のKerberosレルムを構成するには、次の手順を実行します。

1. **[管理]＞[サービス]**に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、⚙＞**[表示]＞[構成]**を選択して、ログ収集に関する構成パラメータのタブを表示します。
4. [**イベント ソース**]タブをクリックします。



5. ドロップダウン メニューから[**Windows/Kerberosレルム**]を選択します。
6. [Kerberosレルム構成]パネルのツールバーで、 をクリックして新しいレルムを追加します。

   [Kerberosドメインの追加]ダイアログが表示されます。
7. 以下のガイドラインを使用して、パラメータを入力します。

パラメータ	詳細
Kerberosレルム名	レルム名をすべて大文字で入力します。たとえば、DSNETWORKING.COM。[マッピング]パラメータにはさまざまなレルム名が自動的に入力されることに注意してください。
KDCホスト名	ドメイン コントローラの名前を入力してください。ここでは、完全修飾名を使用***しないでください***。DCのホスト名のみです。 **注**:Log Collectorは必ず、企業のDNSサーバのDNSクライアントとして構成してください。そうしないと、Log CollectorはKerberosレルムの検索方法を認識できません。
管理サーバ	(オプション) FQDN形式のKerberos管理サーバ名。

8. [**保存**]をクリックしてKerberosドメインを追加します。

Windowsイベント ソースを追加するには、次の手順を実行します。

1. [**管理**]>[**サービス**]に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、 >[**表示**]>[**構成**]を選択して、ログ収集に関する構成パラメータのタブを表示します。
4. [**イベント ソース**]タブをクリックします。
5. Log Collectorの[**イベント ソース**]タブで、ドロップダウン メニューから[**Windows/構成**]を選択します。

   [イベント カテゴリ]パネルに、構成済みのVMwareイベント ソースが表示されます(存在する場合)。

次に、現在の画面から続行し、Windowsイベントのカテゴリとタイプを追加します。

Windowsイベント タイプを構成するには、次の手順を実行します。

1. ドロップダウン メニューから、[**Windows/構成**]を選択します。
2. [イベント カテゴリ]パネル ツールバーで、

+ をクリックしてソースを追加します。

[ソースの追加]ダイアログが表示されます。

3. 以下のガイドラインを使用して、パラメータを入力します。

パラメータ	詳細
エイリアス	分かりやすい名前を入力します。
認証方法	[**ネゴシエート**]を選択します。
チャネル	Windows収集を使用しているほとんどのイベント ソースについては、[**セキュリティ**]、[**システム**]、および[**アプリケーション**]チャネルから収集します。
ユーザ名	NetWitnessとの通信用に以前設定したWindowsユーザ アカウントのアカウント名を入力します。ドメインを含む完全なアカウント名を入力する必要があることに注意してください。たとえば、**rsalog@DSNETWORKING.COM**。
パスワード	ユーザ アカウントの適切なパスワードを入力します。
サイクルごとの最大イベント数	オプションです。RSAでは、この値を0(すべてを収集) に設定することを推奨します。
ポーリング間隔	オプションです。ほとんどのユーザにとっては、値**60**で適切に動作します。

4. [**OK**]をクリックしてソースを追加します。

新しく追加されたWindowsイベント ソースが[イベント カテゴリ]パネルに表示されます。

5. [イベント カテゴリ]パネルで新しいイベント ソースを選択します。

[**ホスト**]パネルがアクティブ化されます。

6. [ホスト]パネル ツールバーで、+ をクリックします。

7. 以下のガイドラインを使用して、パラメータを入力します。

パラメータ	詳細
イベント ソース アドレス	WindowsホストのIPアドレスを入力します。
ポート	デフォルト値の**5985**をそのまま使用します。
転送モード	**http**と入力します。
有効	このボックスを必ずオンにします。

8. [**接続のテスト**]をクリックします。

注: Windowsサービスが実行されていない場合でも、接続テストを正常に実行できる必要があります。

前述のいずれかのステップの詳細については、「NetWitness Suiteユーザ ガイド」の次のヘルプトピックを参照してください。

- 「Configure Windows Collection」: https://community.rsa.com/docs/DOC-43410
- 「Microsoft WinRM Configuration Guide」: https://community.rsa.com/docs/DOC-58163
- 「Test and Troubleshoot Microsoft WinRM Guide」: https://community.rsa.com/docs/DOC-58164

Windows Legacy収集およびNetApp収集の構成

この**Windows Legacy**プロトコルでは、Windows Legacy(Windows 2003以前のイベント ソース)からのイベントおよびNetApp ONTAPイベント ソースからのCIFS監査イベントを収集します。

Windows Legacy収集プロトコルを構成する前に、Windows Legacyをリモート Collectorとして設定するためのローカルCollectorを導入する必要があります。

Legacy WindowsおよびNetApp Collectionの仕組み

Windows Legacy収集プロトコルを使用して、次のソースからイベントを収集するようNetWitness Suiteを構成します。

- 以前のバージョンのMicrosoft Windowsイベント ソース(Window 2003またはそれ以前のイベント ソース)
- NetAppイベント ソース

Windows 2003またはそれ以前のイベント ソース

Legacy Windowsイベント ソースとは、以前のバージョンのWindows(Windows 2000、Windows 2003など) のイベント ソースを指します。 Windows Legacy収集プロトコルでは、enVisionでイベントを収集していたWindowsイベント ソースからイベントを収集できます。再構成を行う必要はありません。これらのイベント ソースは、[windows]タイプのイベント ソースとして設定します。

NetAppイベント ソース

Data ONTAPを実行しているNetAppアプライアンスは、Windows Serverに似たネイティブ監査フレームワークをサポートします。NetAppイベント ソースを構成すると、この監査フレームワークは、Windows .evtファイル形式で監査イベントを生成および保存します。Windows Legacyコレクション プロトコルは、NetApp .evtファイルからのイベント収集をサポートします。 これらのイベント ソースは、[netapp_evt]タイプのイベント ソースとして設定します。

NetApp Data ONTAPアプライアンスは、CIFS監査イベントを生成し、ファイル名にタイムスタンプが含まれる形式で.evtファイルとして定期的に保存するように構成されています。詳細については、RSAリンクの「Network Appliance Data ONTAP Event Source Configuration Guide」を参照してください。この収集プロトコルでは、最後に処理された.evtファイルのファイル名のタイムスタンプを保存して、収集ステータスを追跡します。

NetApp固有のパラメータ

[ソースの追加/編集]ダイアログで管理するほとんどのパラメータは、Windows Legacyイベント ソースとNetAppイベント ソースの両方で共通しています。

次の2つのパラメータは、NetAppイベント ソースに固有のものです。

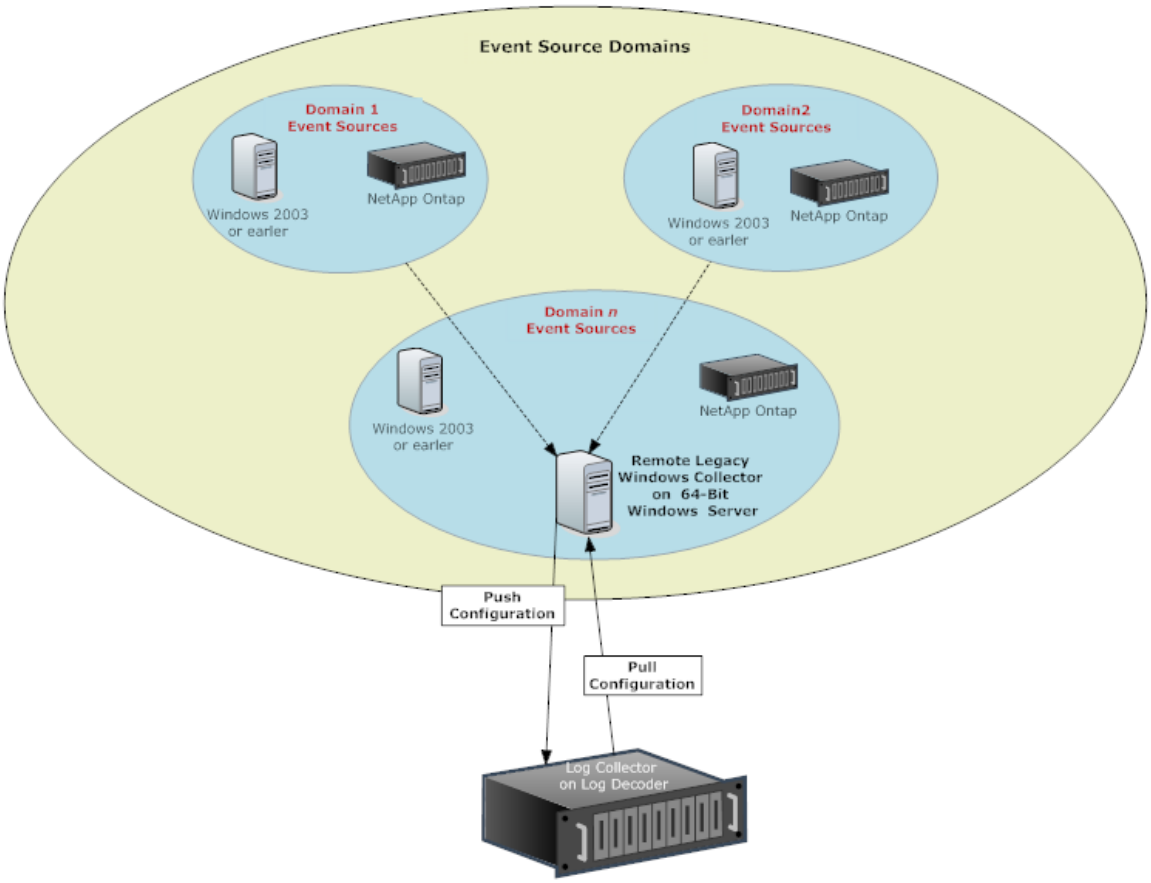
- [**イベント ディレクトリ パス**] : NetAppアプライアンスは、イベント データを生成し、それをNetAppアプライアンス上の共有可能なディレクトリ内の.evtファイルに保存します。NetWitness Suiteでは、[イベント ディレクトリ パス]パラメータにこのディレクトリ パスを指定する必要があります。
- [**イベント ファイル プレフィックス**] : [イベント ディレクトリ パス]と同様に、NetWitness Suiteがこのデータを処理できるように、NetWitness Suiteではイベント データ.evtファイルのプレフィックスを指定する必要があります(たとえば、adtlog.) 。

それぞれのポーリング サイクルにおいて、NetWitness Suiteは、[イベント ディレクトリ パス]パラメータと[イベント ファイル プレフィックス]パラメータで指定したNetApp共有パスの**.evt**ファイルを参照します。NetWitness Suiteでは以下の処理を行います。

- event-file-prefix.YYMMDDhhmmss.evt形式に一致するファイルを昇順でソートします。
- 最後に処理されたファイルのタイムスタンプを使用して、処理が必要なファイルを判定します。部分的に処理されたファイルが見つかった場合、NetWitness Suiteはすでに処理済みのイベントをスキップします。

導入のシナリオ

Windows Legacy収集プロトコルでは、Windows 2003以前とNetApp ONTAPアプライアンスのイベント ソースからイベント データが収集されます。Windows Legacy リモートCollectorは、イベント ソースドメイン内の物理環境または仮想環境の64ビットWindows 2008 Serverにインストールされたサ Legacy Windows Collectorです。



Windows Legacy Collectorの設定

このトピックでは、Windows Legacy環境でWindows Legacy Collectorをインストールまたはアップグレードするために必要な実行ファイルについて説明します。

NWLegacyWindowsCollector-11.*version-number.exe*を使用して、NetWitness Suiteの Windows Legacy Collectorを物理または仮想のWindows Server 2008 R2 SP1 64ビット版にインストールします。**NWLegacyWindowsCollector-11.*version-number.exe***はRSAリンクからダウンロードします。Windows Legacy収集のインストールまたはアップグレード方法の詳細については、「*NetWitness 11.x Windows Legacy Collection Upgrade & Installation Instructions*」を参照してください。

注：インストール処理中は、MMC(Microsoft管理コンソールコンソール) を閉じる必要があります。

Windows LegacyおよびNetAppイベント ソースの構成

このトピックでは、NetWitness SuiteでWindows Legacyイベント ソースを構成する方法について説明します。

Windows Legacy収集プロトコルでは、Windows 2003以前とNetAppのイベント ソースからイベント データが収集されます。

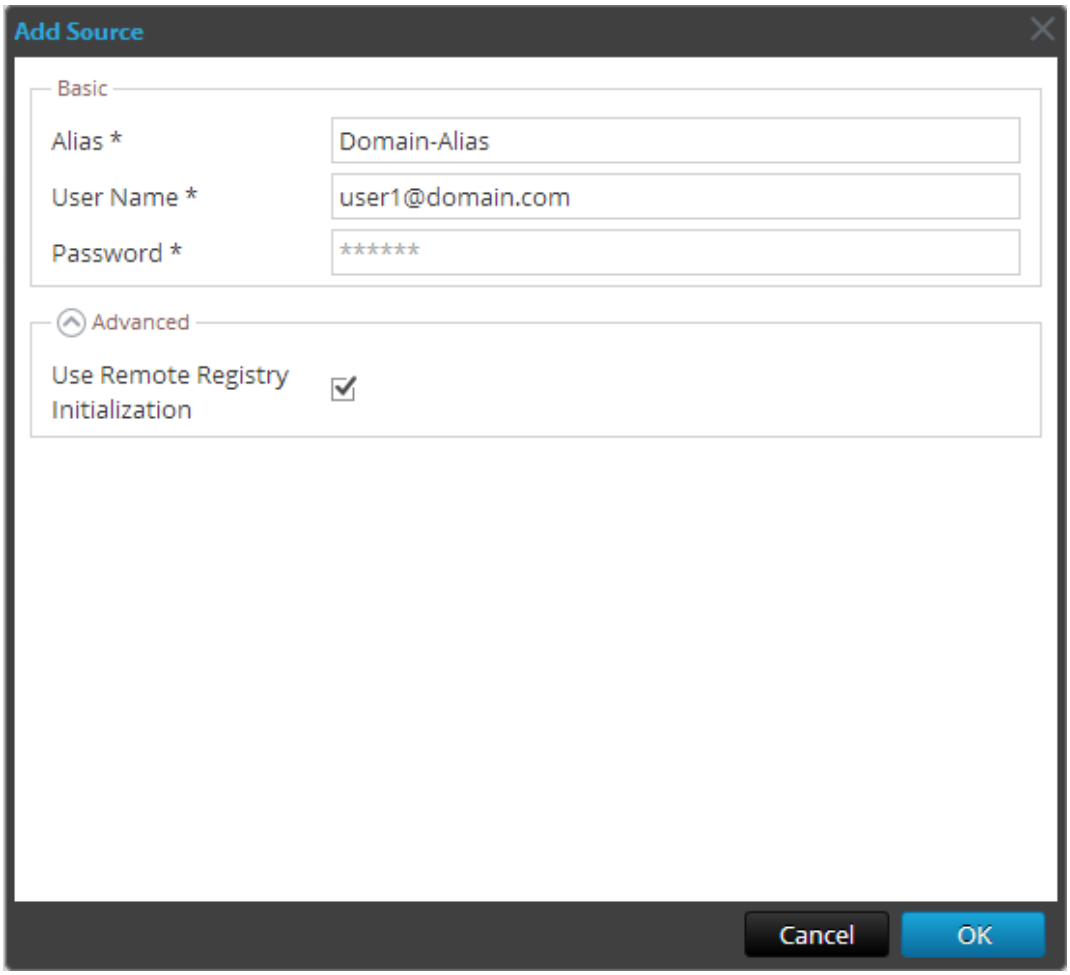
前提条件

Windows Legacyイベント ソースを構成する前に、次のことを確認してください。

1. NetWitness Suite Windows Legacyリモート Collectorが、物理環境または仮想環境の64ビットWindows 2008 Serverにインストールされていること。
2. このWindows LegacyリモートCollectorをNetWitness Suiteに追加していること。

Windows Legacyイベント ソースを追加するには、次の手順を実行します

1. NetWitness Suiteメニューで**[管理]**>**[サービス]**を選択して、[サービス]ビューにアクセスします。
2. [**サービス**]グリッドで、**Windows Legacy Log Decoder**サービスを選択します。
3. [アクション]で、  >**[表示]**>**[構成]**を選択して、ログ収集に関する構成パラメータのタブを表示します。
4. [**イベント ソース**]タブをクリックします。
5. [**イベント ソース**]タブで、ドロップダウン メニューから次のいずれかのオプションを選択します。
   - Windows Legacy/Windows。
   - Windows Legacy/NetApp。
6. エイリアスを構成します。
   a. [**イベント カテゴリ**]パネル ツールバーで、  をクリックします。
   [**ソースの追加**]ダイアログが表示されます。
   b. パラメータに必要な値を指定し、[**OK**]をクリックします。



注：デフォルトでは、[**リモート レジストリ**]が選択されています。詳細については、以下の「リモート レジストリ アクセス」を参照してください。

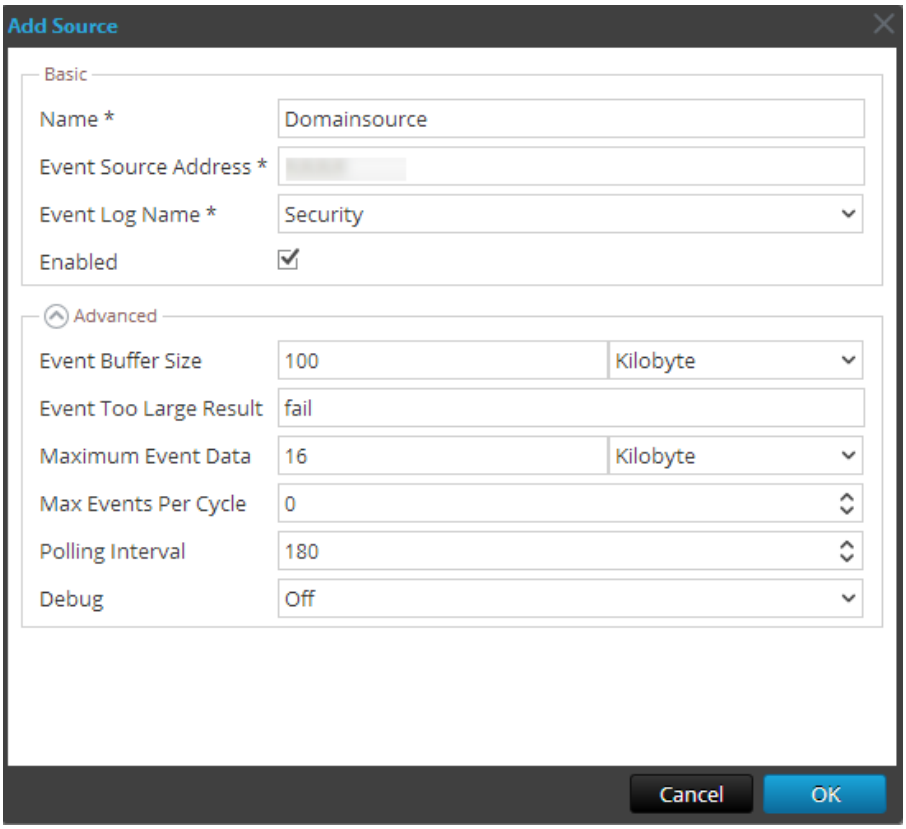
新しく追加された**windows**イベント ソース タイプが[イベント カテゴリ]パネルに表示されます。

7. イベント ソースを追加するには、次の手順を実行します。

   a. [**イベント カテゴリ**]パネルで新しいエイリアスを選択し、[**ソース**]パネルのツールバーで ✚ をクリックします。

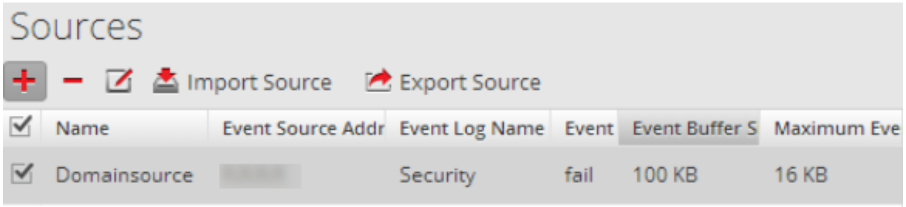
   [**ソースの追加**]ダイアログが表示されます。

   b. イベント ソースのパラメータに必要な値を指定し、[**OK**]をクリックします。



詳細については、以下の「Windows Legacy構成パラメータ」を参照してください。

新しく追加されたWindowsイベント ソースが[**イベント カテゴリ**]パネルに表示されます。



リモート レジストリ アクセス

Windows Legacy Collectorでは、データ収集の前にイベント ソースの初期確認が実行されます。デフォルトで、Windows Legacy Collectorは、WMI(Windows Management Instrumentation) を使用してこの初期確認を実行します。リモート レジストリ アクセスを有効にした場合、Windows Legacy Collectorはイベント ソースを確認するためにリモート レジストリ クエリを実行します。

Windows Legacy構成パラメータ

次の表では、Windows Legacyイベント ソースのパラメータについて説明します。

機能	説明
	基本
名前 *	イベント ソースの名前。有効な値は、「**[_a-zA-Z] [_a-zA-Z0-9]***」の範囲の名前です。ハイフン「-」を名前の一部として使用できます。
イベント ソース アドレス *	イベント ソースのIPアドレス。有効な値は、IPv4アドレス、IPv6アドレス、ドメインの完全修飾名を含むホスト名です。NetWitness Suiteではデフォルトは**127.0.0.1**になります。 Log Collectorは、重複エントリーを避けるために、ホスト名を小文字に変換します。
イベント ログ名	**System**、**Application**、**Security**など、イベント データの収集元となるイベント ログの名前です。 チャネルの例を示します。 • **System**: システム サービス アカウント(インストールされたシステム サービス) 上で稼働するアプリケーション、またはドライバ、さらにはシステムの稼働状態に関するイベントを出力するコンポーネントやアプリケーションなどに関するイベントです。 • **Application**: すべてのユーザ レベル アプリケーションに関するイベントです。このチャネルはセキュリティが設定されていないため、どのアプリケーションからもアクセスすることができます。ある特定のアプリケーションの情報が膨大な場合、アプリケーション固有のチャネルを定義する必要があります。 • **Security**: Windows Local Security Authority専用に使われるWindows監査ログ(イベント ログ) 。
有効	このイベント ソースからイベントを収集するには、このチェックボックスをオンにします。このチェックボックスをオフにすると、Log Collectorはこのイベント ソースからイベントを収集しません。

機能	説明
イベントディレクトリパス	NetApp **.evtまたは.evtx**ファイルのディレクトリパス。これはUNCパスでなければなりません。 NetAppは、イベント データを生成し、これをNetAppアプライアンス上の共有可能ディレクトリに.evtまたは.evtxファイルとして保存します。 • それぞれのポーリング サイクルにおいて、Log Collectorは、[**イベント ディレクトリ パス**] パラメータと[**イベント ファイル プレフィックス**] パラメータで指定したNetApp共有パスの.evtファイルを参照します。Log Collectorでは以下の処理を行います。 ◦ event-file-prefix.**YYMMDDhhmmss.evt**形式に一致するファイルを昇順でソートします。 ◦ 最後に処理されたファイルのタイムスタンプを使用して、処理が必要なファイルを判定します。部分的に処理されたファイルが見つかった場合、Log Collectorはすでに処理済みのイベントをスキップします。 • それぞれのポーリング サイクルにおいて、Log Collectorは、[**イベント ディレクトリ パス**] パラメータと[**イベント ファイル プレフィックス**] パラメータで指定したNetApp共有パスの**.evtx**ファイルを参照します。Log Collectorでは以下の処理を行います。 ◦ **event-file-prefix.YYMMDDhhmmssms.evtx**形式に一致するファイルを昇順でソートします。 ◦ 最後に処理されたファイルのタイムスタンプを使用して、処理が必要なファイルを判定します。部分的に処理されたファイルが見つかった場合、Log Collectorはすでに処理済みのイベントをスキップします。
イベントファイルプレフィックス	**イベント ディレクトリ パス**に保存された**.evt**ファイルのプレフィックス(たとえば、**adtlog**.) 。
拡張	

機能	説明
イベントバッファサイズ	各リクエストについてLog Collectorがイベント ソースから受信するデータの最大サイズ。 有効な値は**0～100** MBの範囲の数値です。この値は**KB**単位で指定します。
バッファを超えるイベント	イベント バッファに対してイベントが大きすぎる場合の動作をLog Collectorに対して指定します。
最大イベントデータ	出力に含めるイベント データの最大サイズ。有効な値は**0～511キロバイト**の範囲の数値です。この値は**KB**単位または**MB**単位で指定します。 • 1 KB～100 MB • 0 = イベント データは出力に含められません。
サイクルごとの最大イベント数	ポーリング サイクルごとのイベントの最大値(ポーリング サイクルごとに収集されるイベント数)です。
ポーリング間隔	ポーリングの間隔(秒)です。デフォルト値は**180**です。 たとえば、180と指定すると、Collectorは、イベント ソースへのポーリングを180秒ごとに実行します。直前のポーリング サイクル(収集)がまだ完了していない場合、そのサイクルが完了するまで待機します。ポーリング中のイベント ソースが多数ある場合、スレッドがビジーになるため、ポーリングが開始するまでに180秒より長くかかる場合があります。

機能	説明
デバッグ	**注意**:イベント ソースに問題が発生し、その問題を調査する必要がある場合にのみ、デバッグを有効に(このパラメータを「On」または「Verbose」に設定)します。デバッグを有効にすると、Log Collectorのパフォーマンスに影響が生じる場合があります。 イベント ソースのデバッグ記録を有効または無効にします。有効な値は次のとおりです。 • **Off** = (デフォルト) 無効 • **On** = 有効 • **Verbose** = Verboseモードが有効になります。スレッド情報やソース コンテキスト情報をメッセージに追加します。 このパラメータは、イベント収集の問題をデバッグまたは監視するような状況で使用するよう設計されています。この値を変更すると、変更はすぐに反映されます(再起動は不要です)。パフォーマンスへの影響を最小限にするために、デバッグのverboseモードは、監視するイベント ソース数が限定された環境で設定するようにしてください。
キャンセル	Windows Legacyイベント ソースを追加せずにダイアログを閉じます。
OK	現在のパラメータ値を新しいイベント ソースとして追加します。

トラブルシューティング:Windows LegacyおよびNetApp Collection

このトピックでは、LWC(Windows Legacy収集)で発生する可能性のある問題と推奨される解決策について説明します。

注:一般的に、SSLを無効にすることで安定的にログ メッセージを受信できるようになる場合があります。

プロトコルの再開に関する問題

問題	考えられる原因	解決策
Windows Legacy収集プロトコルを再開したが、NetWitness Suiteがイベントを受信しない。	logcollectorサービスが停止しています。	**logcollector**サービスを再開します。 1. **Windows Legacyリモート Collector**にログインします。 2. **[スタート]＞[管理ツール]＞[タスクスケジューラ]**の順にクリックし、**[タスクスケジューラ ライブラリ]**をクリックします。 3. 右側のパネルで、**restartnwlogcollector**タスクを見つけ、このタスクが実行中であることを確認します。 4. 実行中でない場合は、**restartnwlogcollector**を右クリックし、**[実行]**を選択します。

インストールに関する問題

MessageBroker.logに次のいずれかのメッセージが記録されている場合は、問題が発生している可能性があります。

ログメッセージ	「rabbitmq」が含まれるすべてのメッセージ
考えられる原因	RabbitMQサービスが実行されていない可能性があります。 ポート**5671**が開いていない可能性があります。
解決策	RabbitMQサービスが実行されていることを確認します。 ポート**5671**が開いていることを確認します。
ログメッセージ	Error: Adding logcollector user account. Error: Adding administrator tag to logcollector account. Error: Adding Adding logcollection vhost.

	Error: Setting permissions to logcollector account in all vhosts.
考えられる原因	インストーラがユーザとvhostを作成しようとしたときに**rabbitmq-server**が実行されていませんでした。

解決策	**RabbitMQ**サービスが実行されていることを確認し、次のコマンドを手動で実行します。
	`rabbitmqctl -q add_user logcollector netwitness`
	`rabbitmqctl -q set_user_tags logcollector administrator`
	`rabbitmqctl -q add_vhost logcollection`
	`rabbitmqctl -q set_permissions -p / logcollector ".*" ".*" ".*"`
	`rabbitmqctl -q set_permissions -p logcollection logcollector ".*" ".*" ".*"`

Windows Legacyフェデレーション スクリプトに関する問題

フェデレーション スクリプト ログに次のいずれかのメッセージが記録されている場合は、問題が発生している可能性があります。

問題	考えられる現象	解決策
フェデレーション スクリプトが開始されたが、LWCサービスが停止した。	NetWitness Suiteのログには、Windows Legacy Collectorとの接続失敗の例外が示されます。	この問題は、Windows Legacyサービスを再開すると、自動的に修正されます。

問題	考えられる現象	解決策

LWCは実行しているが、RabbitMQサービスがダウンするか、再起動される。	Windows Legacy側のフェデレーション ログ ファイルには、ダウンしているRabbitMQサービスに関するエラー メッセージが表示されます。
	確認するログ ファイルは次の場所にあります。**C:\NetWitness\ng\logcollector**
	RabbitMQが実行されていない場合は、次のエラー メッセージがログに記録されます。
	`"Unable to connect to node logcollector@localhost: nodedown"`
	次の診断メッセージが表示されます。
	`attempted to contact: [logcollector@localhost]`
	`logcollector@localhost:`
	`* connected to epmd (port 4369) on localhost`
	`* epmd reports: node 'logcollector' not running at all other nodes on localhost: ['rabbitmqctl-4084']`
	`* suggestion: start the node`
		LWCで**federation.bat**スクリプトを手動で実行します。
		federate.batスクリプトを手動で実行するには、次のステップを実行します。
		1. Windows Legacyインスタンスがインストールされている**C:\Program Files\NwLogCollector**フォルダに移動します。
		2. このフォルダにある**federate.bat**ファイルを見つけます。このファイルを選択して右クリックします。
		3. [**管理者として実行**]を選択します。
		4. ログ ファイルを監視するには、**federate.bat**スクリプトが実行している間に**C:\NetWitness\ng\logcollector\federate.log**に移動します。
		注：スクリプトが実行している間にログ ファイルにエラーが表示されないことを確認します。

NetWitness Suite側でRabbitMQサービスがダウンする。	NetWitness Suiteユーザ インタフェース ページが機能していません。	RabbitMQサービスを再開します。

問題	考えられる現象	解決策
お客様がヘルスモニタの通知を受け取る、または次のようなヘルスモニタのアラームが表示される。「Communication failure between Master NetWitness Suite Host and a Remote Host」と表示され、リモートIPとしてLWCホストが示される。	**federate.bat**スクリプトが正常に実行されていません。	**federate.bat**スクリプトが正しく実行されなかった場合は、前述のように手動で実行します。

参考情報

AWSパラメータ

このトピックでは、AWS(Amazon Webサービス) 環境にリモート ログ収集サービス(VLC) を導入するための、AWS収集の構成パラメータの概要について説明します。

実行したいことは何ですか?

ロール	実行したいこと	ドキュメント
管理者	AWS収集のパラメータの構成。	NetWitness SuiteでのAWS (CloudTrail) イベント ソースの構成

ワークフロー

このワークフローでは、ログ収集機能を介してイベントの収集を開始するために必要な基本タスクを示しています。

関連トピック

- NetWitness SuiteでのAWS(CloudTrail) イベント ソースの構成

次の表に、AWSコレクションで使用できる構成パラメータについて説明します。

パラメータ	説明
パラメータ	**説明**
	基本
名前*	イベント ソースの名前です。

パラメータ	説明
有効化 	イベント ソース構成を有効化して収集を開始するには、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。
アカウントID*	S3バケットのアカウント識別コード
S3バケット名*	AWS(CloudTrail) S3バケットの名前。 Amazon S3バケットの名前は、バケットを作成したAWS (CloudTrail) のリージョンには関係なく、グローバルに一意です。名前はバケットの作成時に指定します。 バケット名はDNSの命名規則に従う必要があります。DNSに準拠したバケット名の規則は次のとおりです。 • バケット名は3文字以上63文字以下の長さの文字列とする。 • バケット名は1つ以上のラベルを連結したものとする。隣接するラベルはピリオド1文字「.」で区切る。バケット名には小文字、数字、ハイフンを使用できる。各ラベルの最初と最後の文字は、小文字また数字とする。 • バケット名をIPアドレスのような形式で指定してはならない(たとえば192.168.5.4) など。 **有効な**バケット名の例を次に示します。 • **myawsbucket** • **my.aws.bucket** • **myawsbucket.1** **無効な**バケット名の例を次に示します。 • **.myawsbucket**: バケット名の先頭にはピリオド「.」を使用できません。 • **myawsbucket.** : バケット名の末尾にもピリオド「.」は使用できません。 • **my..examplebucket**: ラベルの間のピリオドは1つしか使用できません。

パラメータ	説明
アクセスキー*	S3バケットへのアクセスに使用するキー。アクセスキーはAWSサービスAPIに対して安全なRESTリクエストまたはクエリプロトコルリクエストを作成するために使用します。アクセスキーの詳細は、Amazon Web Servicesサポート サイトの「Manage User Credentials」を参照してください。
シークレット キー*	S3バケットへのアクセスに使用するシークレット キー。
リージョン*	S3バケットのリージョン。**us-east-1**がデフォルト値です。
リージョン エンドポイント	AWS CloudTrailホスト名を指定します。たとえば、us-eastリージョンのAWSパブリック クラウド では、リージョン エンドポイントは s3.amazonaws.comです。詳細については、http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_regionを参照してください。このパラメータは AWSガバメントまたはプライベート クラウドからCloudTrailログを収集するために必要です。
プロキシを使用	[**プロキシを使用する**]を有効にして、AWSサーバのプロキシを設定します。デフォルトでは無効です。
プロキシ サーバ	AWSサーバにアクセスするために接続するプロキシ名を入力します。
プロキシ ポート	AWSサーバにアクセスするプロキシ サーバに接続するポート番号を入力 します。
プロキシ ユーザ	プロキシ サーバを使用して認証するユーザ名を入力します。
プロキシ パスワード	プロキシ ポートを使用して認証するユーザのパスワードを入力します。
開始日*	その時点のタイムスタンプから指定日数分過去にさかのぼって、AWS(CloudTrail) コレクションを開始します。デフォルト値は0で、当日から開始します。範囲は0～89日です。

パラメータ	説明
ログ ファイル プレフィックス	収集処理するファイルのプレフィックス。 **注**：CloudTrailサービス側の設定でプレフィックスを指定した場合は、このパラメータにも必ず同じプレフィックスを入力してください。
	詳細
デバッグ	**注意**：イベント ソースに問題が発生し、その問題を調査する必要がある場合にのみ、デバッグを有効に(このパラメータを「On」または「Verbose」に設定) します。デバッグを有効にすると、Log Collectorのパフォーマンスに影響があります。 イベント ソースのデバッグ記録を有効または無効にします。 有効な値は次のとおりです。 • **Off** = (デフォルト) 無効 • **On** = 有効 • **Verbose** = verboseモードで有効になります。スレッド情報とソース コンテキスト情報をメッセージに追加します。 このパラメータは、イベント収集の問題をデバッグまたは監視するような状況で使用するよう設計されています。パフォーマンスへの影響を最小限にするために、デバッグのVerboseモードは、監視するイベント ソース数が限定された環境で設定するようにしてください。 この値を変更すると、変更はすぐに反映されます(再起動は不要です) 。
コマンド引数	スクリプトに追加する引数。

パラメータ	説明
ポーリング間隔	ポーリングの間隔(秒) です。デフォルト値は60です。 たとえば、60と指定すると、Collectorは、イベント ソースへのポーリングを60秒ごとに実行します。直前のポーリング サイクル(収集) がまだ完了していない場合、そのサイクルが完了するまで待機します。ポーリング中のイベント ソースが多数ある場合、スレッドがビジーになるため、ポーリングが開始するまでに60秒より長くかかる場合があります。
SSLが有効	SSLを使用して通信する場合は、このチェックボックスをオンにします。暗号化とSSL証明書による認証によってデータ転送のセキュリティが実装されます。 このチェックボックスは、デフォルトでオンになっています。
接続のテスト	このダイアログで指定した構成パラメータが正しいことを検証します。 たとえば、このテストでは次の項目を検証します。 • このダイアログで指定した認証情報を使用してNetWitnessがAWSのS3バケットと接続できるか。 • NetWitnessがバケットからログ ファイルをダウンロードできるか(バケットにログ ファイルが全くない場合にはテストは失敗しますが、そのような可能性はほとんどありません) 。
キャンセル	AWS(CloudTrail) を追加せずにダイアログを閉じます。
OK	現在のパラメータ値を新しいAWS(CloudTrail) として追加します。

Azureパラメータ

Microsoft Azureは、Microsoftが管理するデータ センターのグローバル ネットワークを通じてアプリケーションとサービスを構築、導入、管理するためのクラウド コンピューティング プラットフォームおよびインフラストラクチャです。

ワークフロー

このワークフローでは、ログ収集機能を介してイベントの収集を開始するために必要な基本タスクを示しています。

実行したいことは何ですか?

ロール	実行したいこと	ドキュメント
管理者	Azureイベント ソースのパラメータの構成。	NetWitness SuiteでのAzureイベント ソースの構成

関連トピック

- NetWitness SuiteでのAzureイベント ソースの構成

Azureイベント ソース構成パラメータ

このトピックでは、Azureイベント ソース構成パラメータについて説明します。

注: アスタリスク(*) が付いている項目は必須です。

基本パラメータ

名前	説明
名前*	英数字からなる、分かりやすいソースの名前を入力します。この値を使用するのは、このスクリーンで名前を表示するときだけです。
有効	イベント ソース構成を有効化して収集を開始するには、このチェックボックスをオンにします。このチェックボックスはデフォルトでオンになっています。
クライアントID*	クライアントIDは、Azureアプリケーション構成タブにあります。表示されるまで下にスクロールします。

名前	説明
クライアント シークレット*	イベント ソースを構成している場合、キーを作成して、有効期間を選択したときに、クライアント シークレットが表示されます。 表示されるのは1回のみで、後で取得することはできないので、必ず保存してください。
APIリソース ベースURL*	「`https://management.azure.com/`」を入力します。最後のスラッシュ(/) を必ず含めてください。
フェデレーション メタデータ エンドポイント*	使用するAzureアプリケーションで、[**エンドポイントの表示**]ボタン(ウィンドウの下部) をクリックします。 同じ文字列で始まる多くのリンクがあります。URLを比較し、それらのほとんどの先頭にある共通文字列を見つけます。この共通文字列が、ここで入力する必要のあるエンドポイントです。
サブスクリプション ID*	Microsoft Azureのダッシュボードで確認できます。左側のリストの下部にあるサブスクリプションをクリックします。
テナント ドメイン*	Active Directoryに移動し、ディレクトリをクリックします。テナント ドメインはURLで、**manage.windowsazure.com/**の直後に続く文字列です。テナント ドメインは、**.com**までを含む文字列です。
リソース グループ名*	Azureでは、左側のナビゲーション ペインペインで、リソース グループを選択し、使用するグループを選択します。
開始日*	収集を開始する日付を選択します。デフォルトは設定当日です。
接続のテスト	このダイアログで指定された構成パラメータをチェックして、正しいことを確認します。

詳細パラメータ

[**詳細**]の横にある⌄をクリックして、必要に応じて、拡張パラメータを表示し、編集します。

名前	説明
ポーリング間隔	ポーリングの間隔(秒) です。デフォルト値は**180**です。 たとえば、180と指定すると、Collectorは、イベント ソースへのポーリングを180秒ごとに実行します。ポーリング サイクル(収集) が進行中である場合、Collectorは、そのサイクルが完了するまで待機します。ポーリング中のイベント ソースが多数ある場合、スレッドがビジーになるため、ポーリングが開始するまでに180秒より長くかかる場合があります。

名前	説明
ポーリング最大継続時間	ポーリング サイクルの最大継続時間(秒) です。値ゼロは制限がないことを示します。
ポーリング最大イベント数	ポーリング サイクルごとのイベントの最大値(ポーリング サイクルごとに収集されるイベント数) です。
ポーリング最大アイドル時間	ポーリング サイクルの最大継続時間(秒) です。値ゼロは制限がないことを示します。
コマンド引数	スクリプトの起動に追加するオプションの引数です。
デバッグ	**注意**:イベント ソースに問題が発生し、その問題を調査する必要がある場合にのみ、デバッグを有効に(このパラメータを「On」または「Verbose」に設定) します。デバッグを有効にすると、Log Collectorのパフォーマンスに影響があります。 **注意**:イベント ソースのデバッグ記録を有効または無効にします。有効な値は次のとおりです。 • **Off** = (デフォルト) 無効 • **On** = 有効 • **Verbose** = verboseモードで有効になります。スレッド情報とソース コンテキスト情報をメッセージに追加します。 このパラメータは、イベント収集の問題をデバッグまたは監視するような状況で使用するよう設計されています。この値を変更すると、変更はすぐに反映されます(再起動は不要です) 。パフォーマンスへの影響を最小限にするために、デバッグのVerboseモードは、監視するイベント ソース数が限定された環境で設定するようにしてください。

Check Pointパラメータ

Check Point収集プロトコルは、OPSEC LEAを使ってCheck Pointイベント ソースからイベントを収集します。OPSEC LEAは、ログの抽出を容易にするためのCheck Point Operations Security Log Export APIです。

ワークフロー

このワークフローでは、ログ収集機能を介してイベントの収集を開始するために必要な基本タスクを示しています。

実行したいことは何ですか?

ロール	実行したいこと	ドキュメント
管理者	Check Pointのパラメータの構成。	NetWitness SuiteでのCheck Pointイベント ソースの構成

関連トピック

- NetWitness SuiteでのCheck Pointイベント ソースの構成

Check Point収集構成パラメータ

基本パラメータ

パラメータ	説明
名前*	イベント ソースの名前です。
アドレス*	Check PointサーバのIPアドレスです。
サーバ名*	Check Pointサーバの名前です。

パラメータ	説明
証明書	転送モードがhttpsである場合に使用するセキュア接続の証明書名です。このパラメータを設定する場合、[設定]タブで作成した証明書トラスト ストアに証明書が存在する必要があります。 ドロップダウン リストから証明書を選択します。Check Pointイベント ソース証明書のファイルの命名規則は、**checkpoint_*name-of-event-source***です。
クライアント識別	Check Pointサーバのクライアント識別名を入力します。
クライアント エンティティ名	Check Pointサーバのクライアント エンティティ名を入力します。
サーバ識別	Check Pointサーバのサーバ識別名を入力します。
有効化	イベント ソース構成を有効化して収集を開始するには、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。
証明書の受信	初めて証明書の受信を行う場合は、このチェックボックスをオンにします。 証明書を受信すると、その証明書がトラスト ストアで使用可能になります。
証明書サーバ アドレス	証明書が格納されているサーバのIPアドレス。デフォルトは、イベント ソース アドレスです。
パスワード	初回に[証明書の受信]チェックボックスをオンにした場合にのみアクティブになります。証明書を受信するにはパスワードが必要です。パスワードは、Check Pointサーバ上のCheck PointにOPSECアプリケーションを追加するときに作成されるアクティベーション キーです。

Check Point収集の拡張パラメータ値の決定

Check Pointイベント ソースへの接続を開いておくタイミングとイベント ボリュームを指定する(一時的に接続を開く) と、システム リソースの使用量を抑えることができます。RSA NetWitness Suiteはデフォルトで次の接続パラメータを使用して、一時的な接続を確立します。

- ポーリング間隔 = **180**(3分)
- ポーリング最大継続時間 = **120**(2分)
- ポーリング最大イベント数 = **5000**(ポーリング間隔あたり5000イベント)
- ポーリング最大アイドル時間 = **0**

Check Pointのイベント ソースから大量のイベントが発生する場合、収集を停止するまで接続を開いておく(持続的な接続を使用する) ように設定することをお勧めします。この設定によって、チェック ポイント収集において大量のログを生成するイベント ソースから生成されるイベント収集の速度を維持できます。永続的な接続によって、収集の再開や接続の遅延が回避され、Check Point収集がイベント生成よりも遅延することを防ぎます。

Check Pointイベント ソースに対する永続的な接続を確立するには、次のパラメータに値を設定します。

- ポーリング間隔 = **-1**
- ポーリング最大継続時間 = **0**
- ポーリング最大イベント数 = **0**
- ポーリング最大アイドル時間 = **0**

パラメータ	説明
ポート	Log Collectorが接続するCheck Pointサーバのポート番号です。 デフォルト値は18184です。

パラメータ	説明
ログの収集タイプ	収集するログのタイプを選択します。 有効な値は次のとおりです。 • **監査**: 監査イベントを収集します。 • **セキュリティ**: セキュリティ イベントを収集します。 監査イベントとセキュリティ イベントの両方を収集する場合、同じイベント ソースを新たに作成する必要があります。たとえば、最初に[監査]を選択したイベント ソースを作成し、このイベント ソースのためにトラスト ストアから証明書を受信します。次に、別のイベント ソースとして、[ログの収集タイプ]で[セキュリティ]を選択し、その他は同一のパラメータ値を持つイベント ソースを作成する場合、最初のパラメータ セットを設定したときに受信した同じ証明書を[証明書]で選択します。[証明書の受信]が選択されていないことを確認します。
ログの収集開始点	Check Pointイベント ソースを設定すると、NetWitnessは現在のログ ファイルからイベントを収集します。有効な値は次のとおりです。 • **現在**: 現在の時点からログを収集します(現在のログ ファイルの現時点から)。 • **最初から**: 現在のログ ファイルの最初からログを収集します。 このパラメータ値で「最初から」を選択すると、現在のログ ファイルでイベントを保持している期間に応じて、収集されるデータの量が非常に多くなることがあります。このオプションは、最初のコレクション セッションに対してのみ有効なことに注意してください。
ポーリング間隔	ポーリングの間隔(秒)です。デフォルト値は**180**です。 たとえば、180と指定すると、Collectorは、イベント ソースへのポーリングを180秒ごとに実行します。直前のポーリング サイクル(収集)がまだ完了していない場合、そのサイクルが完了するまで待機します。ポーリング中のイベント ソースが多数ある場合、スレッドがビジーになるため、ポーリングが開始するまでに180秒より長くかかる場合があります。
ポーリング最大継続時間	ポーリング サイクルの最大継続時間(サイクルがどれだけ続行されるか)(秒)です。

パラメータ	説明
ポーリング最大イベント数	ポーリング サイクルごとのイベントの最大値(ポーリング サイクルごとに収集されるイベント数) です。
ポーリング最大アイドル時間	ポーリング サイクルの、秒単位のアイドル時間です。0は制限がないことを示します。デフォルト値は> **300**です。
フォワーダ	フォワーダとしてCheck Pointサーバを有効または無効にします。デフォルトでは無効です。
ログ タイプ(名前と値のペア)	名前と値の形式のイベント ソースのログです。デフォルトでは無効です。
デバッグ	**注意 :** イベント ソースに問題が発生し、その問題を調査する必要がある場合にのみ、デバッグを有効に(このパラメータをOnまたはVerboseに設定) します。デバッグを有効にすると、Log Collectorのパフォーマンスに影響があります。 イベント ソースのデバッグ ログ記録を有効および無効にします。 有効な値は次のとおりです。 • **Off** = (デフォルト) 無効 • **On** = 有効 • **Verbose** = verboseモードで有効になります。スレッド情報とソース コンテキスト情報をメッセージに追加します。 このパラメータは、イベント収集の問題をデバッグまたは監視するような状況で使用するよう設計されています。パフォーマンスへの影響を最小限にするために、デバッグのVerboseモードは、監視するイベント ソース数が限定された環境で設定するようにしてください。 この値を変更すると、変更はすぐに反映されます(再起動は不要です) 。

ファイル パラメータ

このトピックでは、ファイル収集構成パラメータについて説明します。

ワークフロー

このワークフローでは、ログ収集機能を介してイベントの収集を開始するために必要な基本タスクを示しています。

実行したいことは何ですか?

ロール	実行したいこと	ドキュメント
管理者	ファイル収集のソース パラメータの構成。	NetWitness Suiteでのファイル イベント ソースの構成

関連トピック

- NetWitness Suiteでのファイル イベント ソースの構成

ファイル収集イベントのソース パラメータ

次の表に、ファイル収集のソース パラメータの説明を示します。

名前	説明
	基本
格納先ディレクトリ名 *	ファイル イベント ソースがそのファイルを格納するディレクトリ(たとえば、**Eur_London100**) 。有効な値は、次の正規表現に従う文字列です。 **[_a-zA-Z][_a-zA-Z0-9]*** ファイル ディレクトリ名は文字で始まる必要があり、数字、文字、下線などが続きます。このパラメータは、イベント データの収集を始めた後は変更できません。 コレクションを作成した後、Log Collectorはcollectionディレクトリの下に、work、save、errorの各サブ ディレクトリを作成します。

名前	説明
アドレス*	イベント ソースのIPアドレス。有効な値は、**IPv4アドレス**、**IPv6アドレス**、ドメインの完全修飾名を含む**ホスト名**です。
収集するファイルの形式 (regex)	正規表現で指定します。たとえば、^.*$ではすべてを処理します。
ファイル エンコーディング	ファイルで多言語対応が必要な場合にファイルのエンコーディングを指定します。ファイルのエンコーディング方式を入力します。次の例は有効な方式です。 • UTF-8(デフォルト) • UCS-16LE • UCS-16BE • UCS-32LE • UCS-32BE • SHIFT-JIS • EBCDIC-US
有効化	イベント ソース構成を有効化して収集を開始するには、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。
拡張	
エンコード変換エラー無視	エンコード変換エラーと無効なデータを無視する場合は、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。 **注意**:これにより、パースと変換のエラーが発生する可能性があります。

名前	説明
ファイル ディスク クォータ	[**エラー時に保存**]および[**成功時に保存**]パラメータ設定に関係なく、ファイルの保存を停止するタイミングを決定します。たとえば、値が10の場合、使用可能なディスクが10%未満になると、Log Collectorはファイルの保存を停止し、推定される通常収集処理のために十分なスペースを確保します。 **注意**:使用可能なディスクとは、ベースとなるcollectionディレクトリがマウントされているパーティションを指します。Log Collectorサーバに10 TBのディスク サイズがあり、2 TBがベースのcollectionディレクトリに割り当て済みの場合、この値を10に設定すると、ログ収集は残りのスペースが0.2 TB(2 TBの10%) 未満になると停止します。10 TBの10%ではありません。 有効な値の範囲は**0～100**です。デフォルト値は**10**です。
シーケンシャル処理	シーケンシャル処理フラグ: • 収集した順にイベント ソース ファイルを処理する場合は、このチェックボックスをオンにします(デフォルト) 。 • 並列でイベント ソース ファイルを処理する場合は、このチェックボックスをオフにします。
エラー時に保存	エラー フラグが発生した場合にファイルを保存します。Log Collectorでエラーが発生したときに**eventsource collection**ファイルを保持する場合は、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。
成功時に保存	処理フラグの完了後に**eventsource collection**ファイルを保存します。ファイルの処理後にeventsource collectionファイルを保存する場合は、このチェックボックスをオンにします。このチェックボックスは、デフォルトではオンになっていません。
イベント ソースSSH キー	このイベント ソースのファイルのアップロードに使用するSSH公開キーです。キーの生成手順については、「SFTP Agentのインストールと更新ガイド」の「*イベント ソースでの鍵ペアの生成およびLog Collectorへの公開鍵のインポート*」を参照してください。 **注**:ファイル収集が停止した場合に、authorized_keysファイルが、このパラメータで追加または変更されたSSH公開キーに、NetWitness Suiteで自動的に更新されることはありません。公開キーを更新するには、ユーザがファイル収集を再開する必要があります。 このパラメータでは、ファイル収集が実行されていなくても、複数のファイル イベント ソースについて公開キーの値を追加または変更できますが、NetWitness Suiteでファイル収集が再開されるまでは、**authorized_keys**ファイルが更新されません。

名前	説明
エラーファイルの管理	デフォルトで、Log Collectorは[**ファイル ディスク クォータ**]パラメータを使用して、ディスクがエラー ファイルでフルにならないようにします。このパラメータを[**有効**]に設定すると、次のいずれかを指定できます。 • [**エラー ファイルのサイズ**]パラメータでエラー ファイルに割り当てる最大容量を指定します。 • [**エラー ファイル数**]パラメータでエラー ファイルの最大数を指定します。 削減量の割合を指定することもできます。このパラメータを指定すると、最大値に達したときに指定された割合でファイルが削減されます。 エラー ファイルを管理する場合は、このチェックボックスをオンにします。このチェックボックスは、デフォルトではオンになっていません。
エラーファイルのサイズ	[**エラー ファイルの管理**]および[**エラー時に保存**]パラメータが[有効]に設定されている場合のみ設定できます。 NetWitness Suiteがどれだけのエラー ファイルを保存するかを指定します。指定する値は、errorディレクトリにあるすべてのファイルの最大合計サイズです。 有効な値の範囲は**0**～**281474976710655**です。これらの値は、**KB**単位、**MB**単位、**GB**単位のいずれかで指定します。デフォルト値は**100 MB**です。このパラメータを変更した場合、収集を再開するまで、またはLog Collectorのサービスを再起動するまで有効になりません。
エラーファイル数	[**エラー ファイルの管理**]および[**エラー時に保存**]パラメータが[有効]に設定されている場合のみ設定できます。errorディレクトリで許可されるエラー ファイルの最大数を指定します。有効な値の範囲は**0**～**65536**です。デフォルト値は**65536**です。 このパラメータを変更した場合、収集を再開するまで、またはLog Collectorのサービスを再起動するまで有効になりません。
エラーファイルの削減量	ファイルが最大サイズまたは最大数に達したときに、Log Collectorサービスが削除するエラー ファイルのサイズまたは数の割合を指定します。サービスは、最初に最も古いファイルから削除します。 有効な値の範囲は**0**～**100**です。デフォルト値は**10**です。

名前	説明
保存ファイルの管理	保存ファイルを管理する場合は、このチェックボックスをオンにします。このチェックボックスは、デフォルトではオンになっていません。 デフォルトで、Log Collectorは[**ファイル ディスク クォータ**]パラメータを使用して、ディスクが保存ファイルでフルにならないようにします。このチェックボックスをオンにすると、次のいずれかを指定できます。 • [**保存ファイルのサイズ**]パラメータで保存ファイルに割り当てる最大容量を指定します。 • [**保存ファイル数**]パラメータで保存ファイルの最大数を指定します。 削減量の割合を指定することもできます。このパラメータを指定すると、最大値に達したときに指定された割合でファイルが削減されます。
保存ファイルのサイズ	[**保存ファイルの管理**]および[**成功時に保存**]パラメータが[有効]に設定されている場合のみ設定できます。 saveディレクトリに格納するすべてのファイルの最大合計サイズを指定します。有効な値の範囲は**0～281474976710655**です。これらの値は、**KB**単位、**MB**単位、**GB**単位のいずれかで指定します。デフォルト値は**100 MB**です。 このパラメータを変更した場合、収集を再開するまで、またはLog Collectorのサービスを再起動するまで有効になりません。
保存ファイル数	[**保存ファイルの管理**]および[**成功時に保存**]パラメータが[有効]に設定されている場合のみ設定できます。saveディレクトリで許可されるエラーファイルの最大数を指定します。有効な値の範囲は**0～65536**です。デフォルト値は**65536**です。 このパラメータを変更した場合、収集を再開するまで、またはLog Collectorのサービスを再起動するまで有効になりません。
保存されたファイルの削減量	ファイルが最大サイズまたは最大数に達したときに、Log Collectorサービスが削除する保存ファイルのサイズまたは数の割合を指定します。サービスは、最初に最も古いファイルから削除します。 有効な値の範囲は**0～100**です。デフォルト値は**10**です。

名前	説明
デバッグ	**注意**:イベント ソースに問題が発生し、その問題を調査する必要がある場合にのみ、デバッグを有効に(このパラメータを「**On**」または「**Verbose**」に設定)します。デバッグを有効にすると、Log Collectorのパフォーマンスに影響が生じる場合があります。 イベント ソースのデバッグ記録を有効または無効にします。 有効な値は次のとおりです。 • **Off** = (デフォルト) 無効 • **On** = 有効 • **Verbose** = verboseモードで有効になります。スレッド情報とソース コンテキスト情報をメッセージに追加します。 このパラメータは、イベント収集の問題をデバッグまたは監視するような状況で使用するよう設計されています。パフォーマンスへの影響を最小限にするために、デバッグのVerboseモードは、監視するイベント ソース数が限定された環境で設定するようにしてください。 この値を変更すると、変更はすぐに反映されます(再起動は不要です)。
キャンセル	イベント ソースを追加または保存せずに、ダイアログを閉じます。
OK	イベント ソースを追加または保存します。

ログ収集サービスの[システム]ビュー

Log Collectorには、Log Decoderホスト上で稼働するサービス(ローカルCollectorとも呼ばれます) と、リモートからローカルCollectorにイベントを送信するリモートCollectorがあります。Log CollectorはLog Decoderと同様の方法で構成および管理されます。

ログ収集サービスの[システム]ビューにアクセスするには、管理＞[サービス]に移動し、Log Collectorサービスを選択してから、[表示]＞[システム]を選択します。

ワークフロー

このワークフローでは、ログ収集機能を介してイベントの収集を開始するために必要な基本タスクを示しています。

実行したいことは何ですか?

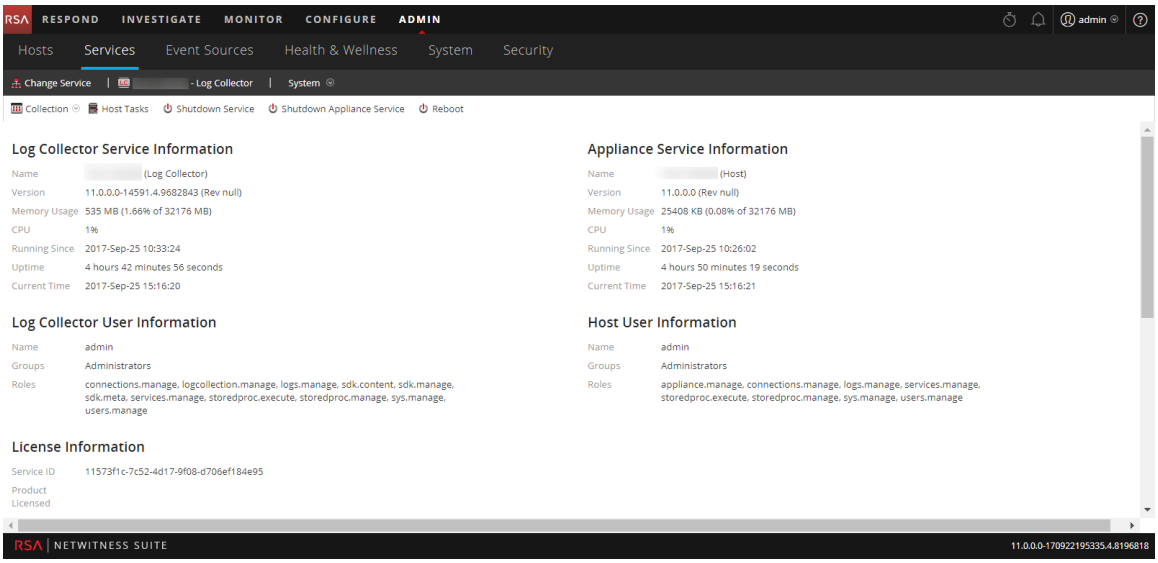
ロール	実行したいこと	ドキュメント
管理者	停止中のプロトコルのイベントデータ収集の開始。	収集サービスの開始
管理者	実行中のプロトコルのイベントデータ収集の停止。	収集サービスの開始

関連トピック

- 収集サービスの開始

簡単な説明

Log Collectorサービスの情報ツールバーから、[収集]アイコンを使用してイベント データを管理し、停止したプロトコルのイベント データを開始したり、開始したプロトコルのデータ収集を停止することができます。[ホスト タスク]アイコンからは、実行するタスクを選択できます。また、サービスの情報ツールバーからサービスをシャットダウンすることや、サービスを再起動することもできます。


RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
Hosts
Services
Event Sources
Health & Wellness
System
Security
Change Service
- Log Collector
System
Collection
Host Tasks
Shutdown Service
Shutdown Appliance Service
Reboot
Log Collector Service Information
Name (Log Collector)
Version 11.0.0.0-14591.4.9682843 (Rev null)
Memory Usage 535 MB (1.66% of 32176 MB)
CPU 1%
Running Since 2017-Sep-25 10:33:24
Uptime 4 hours 42 minutes 56 seconds
Current Time 2017-Sep-25 15:16:20
Appliance Service Information
Name (Host)
Version 11.0.0.0 (Rev null)
Memory Usage 25408 KB (0.08% of 32176 MB)
CPU 1%
Running Since 2017-Sep-25 10:26:02
Uptime 4 hours 50 minutes 19 seconds
Current Time 2017-Sep-25 15:16:21
Log Collector User Information
Name admin
Groups Administrators
Roles connections.manage, logcollection.manage, logs.manage, sdk.content, sdk.manage, sdk.meta, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage
Host User Information
Name admin
Groups Administrators
Roles appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage
License Information
Service ID 11573f1c-7c52-4d17-9f08-d706ef184e95
Product Licensed
RSA | NETWITNESS SUITE
11.0.0.0-170922195335.4.8196818

ODBCイベント ソース構成パラメータ

このトピックでは、ODBC収集プロトコルの構成方法について説明します。ODBC収集プロトコルでは、ODBC(Open Database Connectivity) ソフトウェア インタフェースを使用して、データベースに監査データを格納するイベント ソースのイベントを収集します。

ODBC構成パラメータへのアクセス

ODBCイベント ソース構成パラメータにアクセスするには、次の手順を実行します。

1. NetWitness Suiteメニューから[**管理**]＞[**サービス**]に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、[**表示**]＞[**構成**]を選択して、ログ収集に関する構成パラメータのタブを表示します。

   Log Collectorの[**構成**]ビューが表示され、[**全般**]タブが開きます。
4. [**イベント ソース**]タブをクリックして、ドロップダウン メニューから[**ODBC/構成**]を選択します。

ワークフロー

このワークフローでは、ログ収集機能を介してイベントの収集を開始するために必要な基本タスクを示しています。

実行したいことは何ですか?

ロール	実行したいこと	ドキュメント
管理者	ODBCパラメータの表示または更新。	NetWitness SuiteでのODBCイベント ソースの構成

関連トピック

- NetWitness SuiteでのODBCイベント ソースの構成
- DSN(データ ソース名) の構成

- ODBC収集のトラブルシューティング
- ODBC収集用のカスタムのTypespecの作成

データソース名 (DSN) パラメータ

[ソース] パネルを使用すると、DSN(データソース名) パラメータのレビュー、追加、変更、削除を行えます。

[ソース] パネル

ODBC DSNは、ODBCエンドポイントに接続する方法をLog Collectorに指定します。ODBCドライバやODBCエンドポイントのホスト名やポートなどの情報を使用してデータソース名を構成する場合に、ODBC DSNを参照します。

ODBC DSNは、名前と値のペアのシーケンスです。Sybase、Microsoft SQL Server、Oracleなど、特定のODBCデータソースタイプに対する有効な名前については、「Progress DataDirect Document Library」の「*DataDirect Connect Series for ODBC User's Guide*」と「*DataDirect Connect Series for ODBC User's Guide*」を参照してください。

ツールバー

次の表に、ツールバーオプションの説明を示します。

オプション	説明
	[ソースの追加] ダイアログが開きます。このダイアログで、[イベントカテゴリー] パネルで選択したイベントソースタイプ用のイベントソースを追加します。
	選択したイベントソースを削除します。
	ソースを編集します。[ソースの編集] ダイアログが開きます。このダイアログで、選択したイベントソースの構成パラメータを変更します。 複数のイベントソースが選択されている場合、選択したファイルディレクトリのパラメータ値を編集できる[ソースの一括編集] ダイアログを開きます。 イベントソースのインポート、エクスポート、一括編集の詳細な手順については、「*ログ収集の構成ガイド*」を参照してください。

オプション	説明
Import DSN	[一括追加オプション]ダイアログが開きます。このダイアログで、CSV(コンマ区切り)ファイルから一括でソースをできます。[一括追加オプション]ダイアログには、2つのインポート オプションがあります。 イベント ソースのインポート、エクスポート、一括編集の詳細な手順については、「*ログ収集の構成ガイド*」を参照してください。
Export DSN	選択したソースのパラメータを含む.csvファイルを作成します。 イベント ソースのインポート、エクスポート、一括編集の詳細な手順については、「*ログ収集の構成ガイド*」を参照してください。
Test Connection	選択されたODBCデータベースの構成パラメータを検証します。 イベント ソースへの接続を一括テストする詳細な手順については、「*ログ収集の構成ガイド*」を参照してください。

[DSNの追加]または[DSNの編集]ダイアログ

このダイアログでは、選択されたイベント ソースを追加または編集します。

名前	説明
	基本
DSN*	イベント収集の対象となるデータベースを定義するデータ ソース名(DSN)です。ドロップダウン リストから既存のDSNを選択します。詳細については、「ODBC DSN イベント ソース構成パラメータ」を参照してください。
ユーザー名*	データベースに接続するためにデータ ソース名が使用するユーザー名です。イベント ソースを作成するとき、ユーザー名を指定する必要があります。
パスワード	データベースに接続するためにデータ ソース名が使用するパスワードです。 **注意**:パスワードは内部的に暗号化され、暗号化された形式で表示されます。
Enabled	イベント ソース構成を有効化して収集を開始するには、このチェックボックスをオンにします。このチェックボックスはデフォルトでオンになっています。
アドレス*	ODBCでは、このフィールドは使用されません。 Log CollectorはODBC.iniファイルで指定されたアドレスを使用します。

名前	説明
	詳細
最大セルサイズ	Log Collectorがデータベースの1つのセルから取り出せるデータの最大サイズ(バイト単位) です。デフォルト値は**2048**です。
Nil値	データベースのセルからNILが返された場合にLog Collectorが表示する文字列です。デフォルト値 : “”(null) 。
ポーリング間隔	ポーリングの間隔(秒) です。デフォルト値は**180**です。 たとえば、180と指定すると、Collectorは、イベント ソースへのポーリングを180秒ごとに実行します。ポーリング サイクル(収集) が進行中である場合、Collectorは、そのサイクルが完了するまで待機します。ポーリング中のイベント ソースが多数ある場合、スレッドがビジーになるため、ポーリングが開始するまでに180秒より長くかかる場合があります。
ポーリング最大イベント数	ポーリング サイクルごとのイベントの最大値(ポーリング サイクルごとに収集されるイベント数) です。
デバッグ	**注意** : イベント ソースに問題が発生し、その問題を調査する必要がある場合にのみ、デバッグを有効に(このパラメータをOnまたはVerboseに設定) します。デバッグを有効にすると、Log Collectorのパフォーマンスに影響があります。 イベント ソースのデバッグ記録を有効または無効にします。有効な値は次のとおりです。 • **Off** = (デフォルト) 無効 • **On** = 有効 • **Verbose** = verboseモードで有効になります。スレッド情報とソース コンテキスト情報をメッセージに追加します。 このパラメータは、イベント収集の問題をデバッグまたは監視するような状況で使用するよう設計されています。この値を変更すると、変更はすぐに反映されます(再起動は不要です) 。パフォーマンスへの影響を最小限にするために、デバッグのVerboseモードは、監視するイベント ソース数が限定された環境で設定するようにしてください。

名前	説明
初期トラッキングID	収集が開始されていない場合にLog Collectorがこのイベント ソースに割り当てる初期IDコードです。このパラメータに値がない場合、Log Collectorはテーブルの最後から収集を始め、そこから追加されていくレコードを収集します。デフォルト値は ""(null) です。
ファイル名	Microsoft SQL Serverイベント ソースでのみ設定するパラメータで、トレース ファイル ディレクトリの場所(たとえば、**C:\MyTraceFiles**) を指定します。 適切な設定でディレクトリを作成する方法の詳細については、RSA Secure Care Online(SCOL) にある「RSA Microsoft SQL Server Event Source Configuration Guide」を参照してください。
接続のテスト	このダイアログで指定された構成パラメータをチェックして、正しいことを確認します。
キャンセル	ソースを追加または変更せずにダイアログを閉じます。
OK	DNSのパラメータを追加または変更します。

ODBC DSNイベント ソース構成パラメータ

ODBC(Open Database Connectivity) イベント ソースを登録するには、データ ソース名 (DSN) が必要です。ODBCイベント ソースの構成に必要なパラメータ(値ペア)を設定して、DSNを定義する必要があります。

ODBC構成パラメータへのアクセス

ODBCイベント ソース構成パラメータにアクセスするには、次の手順を実行します。

1. NetWitness Suiteメニューで**[管理]＞[サービス]**を選択して、[サービス]ビューにアクセスします。
2. [Log Collector]サービスを選択します。
3. [アクション]で、**[表示]＞[構成]**を選択して、ログ収集に関する構成パラメータのタブを表示します。

   Log Collectorの**[構成]**ビューが表示され、**[全般]**タブが開きます。
4. **[イベント ソース]**タブをクリックして、ドロップダウン メニューから**[ODBC/DSN]**を選択します。

ワークフロー

このワークフローでは、ログ収集機能を介してイベントの収集を開始するために必要な基本タスクを示しています。

実行したいことは何ですか?

ロール	実行したいこと	ドキュメント
管理者	ODBCデータ ソース名のDSN構成パラメータの構成。	DSN(データ ソース名) の構成

関連トピック

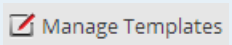
- NetWitness SuiteでのODBCイベント ソースの構成
- DSN(データ ソース名) の構成

ODBC DSN構成パラメータ

このトピックでは、DSN(データ ソース名) の構成パラメータについて説明します。

[DSN]パネル

[DSN]パネルでは、ODBCイベント ソース用に、DSNおよびDSNの名前と値のペアを追加、削除、編集できます。

機能	説明
	[DSNの追加]ダイアログが表示され、DSNとそのパラメータを定義できます。
	選択したDSNを削除します。
	[DSNの編集]ダイアログが表示され、選択したDSNの名前と値のペアを編集できます。
	[DSNテンプレートの管理]ダイアログが表示されます。このダイアログでは、DSNの名前/値ペアのテンプレートを追加または削除できます。
	DSNを選択します。
DSN	追加したDSNの名前です。
パラメータ	<name-value for="" p="" pairs="" the=""> </name-value>

[DSNの追加]または[DSNの編集]ダイアログ

このダイアログでは、DSNを追加または変更します。

機能	説明
XMLテンプレート	事前に定義されたDSN値の名前/値ペアのテンプレートを選択します。

機能	説明
DSN名*	DSNの名前を追加します。 DSN名は追加した後には編集できません。 この値はODBC.iniファイルのDSNエントリーに対応する必要があります。有効な値は、次の形式の文字列です。 `[_a-zA-Z][_a-zA-Z0-9]*` ファイルディレクトリ名は文字で始まる必要があり、数字、文字、下線などが続きます(たとえば、**oracle_executive_compensation**) 。
パラメータ	+ 行を追加して、パラメータの名前と値のペアを定義できるようにします。 − 選択したパラメータの名前と値のペアを削除します。 パラメータの名前と値のペアを選択します。 名前 : パラメータ名を入力または変更します。 値 : パラメータ名に関連づける値を入力または変更します。
キャンセル	DSNおよびその名前と値のペアを保存しないか、名前と値のペアに対する変更を保存せずに、ダイアログを閉じます。
保存	DSNおよびその名前と値のペアを追加するか、名前と値のペアに対する変更を保存します。

[DSNテンプレートの管理]ダイアログ

このダイアログでは、DSNの名前/値ペアのテンプレートを追加または削除できます。

機能	説明
テンプレート選択パネル	
+	テンプレートの追加パネルが開きます。このパネルでは、DSNの名前/値ペアのテンプレートを追加できます。
−	選択したテンプレートを削除します。
	削除または変更するテンプレートを選択します。
テンプレートの追加パネル	

機能	説明
	値ペアの行を追加します。
	値ペアの行を削除します。
	値ペアの行を選択します。
名前	パラメータ名を入力します。
値	パラメータ名に関連付ける値を入力します。
キャンセル	ダイアログで行った変更を取り消します。
保存	DSNおよびその名前と値のペアを追加するか、名前と値のペアに対する変更を保存します。
閉じる	DSNおよびその名前と値のペアを保存しないか、名前と値のペアに対する変更を保存せずに、ダイアログを閉じます。

リモートCollector/ローカルCollectorの構成パラメータ

ログ収集を導入する場合、各種イベント ソースからログ イベントを収集するようにLog Collectorを構成する必要があります。Log Collectorを構成することで、これらのイベントをLog Decoderホストに安全かつ確実に配信できます。配信されたイベントはホストでパースされ、今後の解析のために保存されます。

このトピックでは、[サービス]の[構成]ビュー> [リモートCollector]/[ローカルCollector]タブの機能について説明します。

ワークフロー

このワークフローでは、ログ収集機能を介してイベントの収集を開始するために必要な基本タスクを示しています。

実行したいことは何ですか?

ロール	実行したいこと	ドキュメント
管理者	ローカルCollectorの追加または削除	ローカルCollectorおよびリモートCollectorの構成
管理者	リモートCollectorの追加または削除。	ローカルCollectorおよびリモートCollectorの構成

関連トピック

- ローカルCollectorおよびリモートCollectorのプロビジョニング
- ローカルCollectorおよびリモートCollectorの構成

サービスの[構成]ビュー

ログ収集パラメータはすべて、[サービス]の[構成]ビューで管理されます。このガイドで説明する導入パラメータの管理は、[**リモート/ローカルCollector**]タブで実施します。

- ローカルCollectorを構成している場合、NetWitness Suiteに[**リモートCollector**]タブが表示され、リモートCollectorからイベントをプルするようにローカルCollectorを構成することができま

す。

- リモートCollectorを構成している場合、NetWitness Suiteに[**ローカルCollector**]タブが表示され、ローカルCollectorにイベントをプッシュするようにリモートCollectorを構成できます。

[リモートCollector]タブ

ローカルCollectorの[リモートCollector]パネルでは、ローカルCollectorがイベントをプルするリモートCollectorを追加または削除することができます。

列	説明
	ローカルCollectorがイベントをプルするリモートCollectorを選択するための[**ソースの追加**]ダイアログが表示されます。
	リモートCollectorの[ローカルCollector]パネルからリモートCollectorを削除します。
	選択されたリモートCollectorの[**ソースの編集**]ダイアログを表示します。
	リモートCollectorを選択します。
名前	リモートCollectorの名前です。ローカルCollectorはここからイベントをプルします。
アドレス	リモートCollectorのIPアドレスです。ローカルCollectorはこのアドレスからイベントをプルします。
コレクション	リモートCollectorがローカルCollectorにプッシュする収集プロトコルを選択します。 プロトコルの任意の組み合わせを選択できます。プロトコルを選択しなかった場合、NetWitness Suiteによってすべてのプロトコルが選択されます。

[ローカルCollector]タブ

リモートCollectorの[ローカルCollector]パネルでは、リモートCollectorからイベントをプッシュするローカルCollectorを追加または削除することができます。

[**構成の選択**]ドロップダウンメニューで[**ソース**]または[**宛先**]を選択します。

- [**宛先**]を選択すると、[**リモートの宛先の追加**]ダイアログが表示されます。
- [ソース]を選択すると、[**ソースの追加**]ダイアログが表示されます。

次の表は、[ソースの追加]ダイアログについて説明しています。

列	説明
	ローカルCollectorがイベントをプルするリモートCollectorを選択するための[**ソースの追加**]ダイアログが表示されます。
	リモートCollectorの[ローカルCollector]パネルからリモートCollectorを削除します。
	選択されたリモートCollectorの[**ソースの編集**]ダイアログを表示します。
	リモートCollectorを選択します。
名前	リモートCollectorの名前です。ローカルCollectorはここからイベントをプルします。
アドレス	リモートCollectorのIPアドレスです。ローカルCollectorはこのアドレスからイベントをプルします。

次の表は、[Local Collector]パネルについて説明しています。

列	説明
	選択されたグループの[**リモートの宛先の追加**]ダイアログを表示します。リモートCollectorがイベントをプッシュするローカルCollectorをこのグループに追加します。
	宛先Log Collectorをグループから削除します。
	選択された宛先ローカルCollectorの[**リモートの宛先の編集**]ダイアログを表示します。
	宛先ローカルCollectorを選択します。
宛先名	宛先ローカルCollectorの名前を表示します。
アドレス	ローカルCollectorの宛先のIPアドレスを表示します。

列	説明
コレクション	ローカルCollectorがリモートCollectorからプルする収集プロトコルを選択します。 プロトコルの任意の組み合わせを選択できます。プロトコルを選択しなかった場合、NetWitness Suiteによってすべてのプロトコルが選択されます。

[ログ収集]タブ

このトピックでは、[ログ収集]ビューで使用可能なタブについて説明します。

[ログ収集]ビューへのアクセス

1. NetWitness Suiteメニューから**[管理]**>**[サービス]**に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、**[表示]**>**[構成]**を選択して、ログ収集に関する構成パラメータのタブを表示します。

   Log Collectorの**[構成]**ビューが表示され、[**全般**]タブが開きます。
4. 対応するパラメータの表示または更新に使用可能なタブのいずれかを選択します。

使用可能なタブ

[管理]>[サービス]ビューを使用して、ログ収集パラメータを管理します。次のタブがあります。

- [**全般**]タブ: Log Collectorサービスと各収集プロトコルの操作を制御する詳細パラメータを構成します。詳細については、「ログ収集の[全般]タブ」を参照してください。
- [**リモートCollector**]: このタブは、リモートCollectorを設定するときに使用します。詳細については、「ローカルCollectorおよびリモートCollectorの構成」を参照してください。
- [**ファイル**]: Log Collectorの構成ファイルを編集するためのインタフェースを提供します。
- [**イベント ソース**]: このタブは、イベント ソースの収集を構成するときに使用します。詳細については、「ログ収集の[イベント ソース]タブ」を参照してください
- [**イベントの宛先**]: Log Collectorサービスの[構成]ビューの[イベントの宛先]タブは、Log Collectionで収集されたイベント データの宛先を構成するときに使用します。詳細については、「ログ収集の[イベントの宛先]タブ」を参照してください。

- **[設定]**: Lockboxのセキュリティ設定および証明書管理のためのパラメータが含まれています。
- [**Applianceサービス構成**]: RSA NetWitness Suite Core Applianceサービスの構成パラメータが含まれています。

[**ファイル**]タブと[**Applianceサービス構成**]タブの構成パラメータについては、「*ホストおよびサービスの構成ガイド*」でそれぞれのタブに関する情報を参照してください。

ログ収集の[全般]タブ

このトピックでは、Log Collectorのサービスの[構成]ビュー>[全般]タブの機能について説明します。

ログ収集の[全般]タブにアクセスするには、次の手順を実行します。

1. NetWitness Suiteメニューから**[管理]>[サービス]**に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]の下の  をクリックし、**[表示]>[構成]**を選択します。

   Log Collectorの**[構成]**ビューが表示され、**[全般]**タブが開きます。

ワークフロー

このワークフローでは、ログ収集機能を介してイベントの収集を開始するために必要な基本タスクを示しています。

実行したいことは何ですか?

ロール	実行したいこと	ドキュメント
管理者	必要に応じて、[システム構成]パネルでシステム構成パラメータを調整します。	基本的な実装

ロール	実行したいこと	ドキュメント

管理者	• Log Collectorの[構成]パネルで、イベント ソース タイプごとのログ収集の自動開始を構成します。
	  • Check Point
	  • ファイル
	  • Netflow
	  • ODBC
	  • プラグイン(AWS CloudTrail、Azure Audit)
	  • SDEE
	  • SNMP
	  • VMware
	  • Windows
	  • Windows Legacy
		• NetWitness SuiteでのCheck Pointイベント ソースの構成
		  • NetWitness Suiteでのファイル イベント ソースの構成
		  • NetWitness SuiteでのODBC イベント ソースの構成
		  • NetWitness SuiteでのAWS (CloudTrail) イベント ソースの構成
		  • NetWitness SuiteでのSDEE イベント ソースの構成
		  • NetWitness SuiteでのNetflowイベント ソースの構成
		  • NetWitness SuiteでのODBC イベント ソースの構成
		  • NetWitness SuiteでのAWS (CloudTrail) イベント ソースの構成
		  • NetWitness SuiteでのSNMP イベント ソースの構成
		  • NetWitness SuiteでのVMwareイベント ソースの構成
		  • NetWitness SuiteでのWindowsイベント ソースの構成
		  • Windows Legacy収集およびNetApp収集の構成

関連トピック

- NetWitness SuiteでのAWS(CloudTrail) イベント ソースの構成
- NetWitness SuiteでのCheck Pointイベント ソースの構成

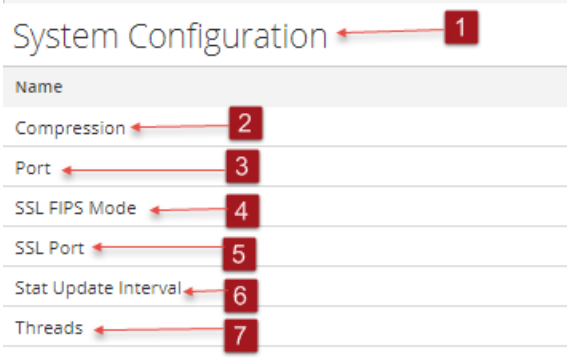
- NetWitness Suiteでのファイル イベント ソースの構成
- NetWitness SuiteでのNetflowイベント ソースの構成
- NetWitness SuiteでのODBCイベント ソースの構成
- NetWitness SuiteでのSDEEイベント ソースの構成
- NetWitness SuiteでのSNMPイベント ソースの構成
- リモートCollectorに対するSyslogイベント ソースの構成
- NetWitness SuiteでのVMwareイベント ソースの構成
- NetWitness SuiteでのWindowsイベント ソースの構成
- Windows Legacy収集およびNetApp収集の構成

簡単な説明

RSA NetWitness Suite管理者は、ログをCollectorに送信するようにイベント ソースを構成する必要があります。イベント ソースが構成されると、そのイベント ソースは、イベント ソースのポーリングを行い、ログを取得して、イベント データをNetWitness Suiteに送信します。

[システム構成]パネル

[システム構成]パネルでは、NetWitness Suiteサービスのサービス構成を管理します。サービスが最初に追加されたときには、デフォルト値が設定されています。これらの値を編集して、パフォーマンスを調整できます。これらのパラメータの説明については、[**全般**]タブを参照してください。

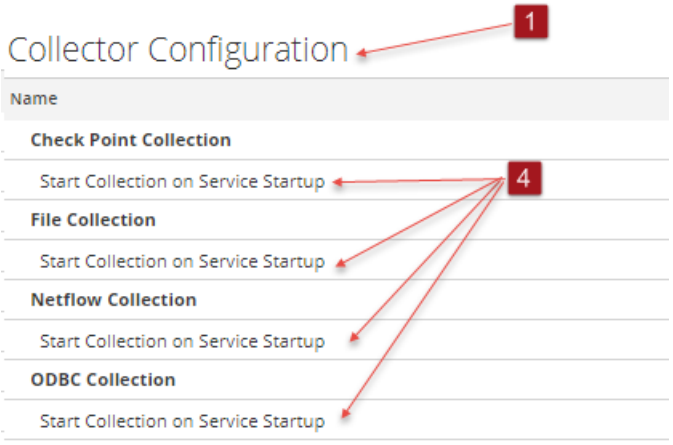


1	[システム構成]パネルでは、NetWitness Suiteサービスのサービス構成を管理します。
2	[Compression]:転送時にデータの圧縮が行われる最小バイト数。0に設定すると、圧縮が無効になります。デフォルト値は**0**です。 値を変更すると、それ以降のすべての接続に即座に反映されます。
3	ポート:サービスがリッスンするポート。ポートは次のとおりです。

	• 50001(Log Collector用) • 50002(Log Decoder用) • 50003(Broker用) • 50004(Decoder用) • 50005(Concentrator用) • その他のサービスでは50007が使用されます
4	SSL FIPSモード:SSL設定を有効にすると、暗号化とSSL証明書による認証によってデータ転送のセキュリティが実装されます。デフォルト値は**オフ**です。
5	SSLポート:サービスがリッスンするNetWitness Suite Core SSLポート。ポートは次のとおりです。 • 56001(Log Collector用) • 56002(Log Decoder用) • 56003(Broker用) • 56004(Decoder用) • 56005(Concentrator用) • その他のサービスでは56007が使用されます
6	統計情報の更新間隔:システムで統計情報を更新する間隔(ミリ秒)。数字を低く設定すると更新がより頻繁になりますが、他のプロセスのパフォーマンスが低下する可能性があります。デフォルト値は**1000**です。 値の変更は即座に反映されます。
7	スレッド: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。0に設定すると、システムが値を設定します。デフォルト値は15です。 変更はサービスの再起動後に有効になります。

[Collector構成]パネル

[Collector構成]パネルでは、イベント ソース タイプごとにログ収集の自動開始を有効化できます。



1	[Collector構成]パネルでは、イベント ソース タイプごとにログ収集の自動開始を有効化できます。
2	[すべて有効化]は、すべてのイベント タイプで自動収集を有効化します。 **すべて有効化**：Log Collectorサービスが開始すると、すべてのイベント タイプのログの収集を開始します。
3	[すべて無効化]は、すべてのイベント タイプで自動収集を無効化します。 **すべて無効化**：(デフォルト) 明示的に収集を開始するまで、すべてのイベント タイプでイベント データを受信しません。
4	[サービス起動時に収集を開始]は、イベント ソース タイプごとに、Log Collectorサービスの開始時にログ収集を自動開始するかどうかを設定します。有効な値は次のとおりです。 • 選択済み = Log Collectorサービスが開始すると、ログの収集を開始します。 • 未選択 = (デフォルト) 明示的に収集を開始するまで、イベント データを収集しません。
5	**適用**：[**適用**]をクリックして、パラメータ値への変更を保存します。

ログ収集の[イベントの宛先]タブ

Log Collectorサービスの[構成]ビューの[イベントの宛先]タブは、Log Collectorで収集されたイベント データの宛先を構成するときに使用します。

- Log Decoder
- Identity Feed

前提条件

Identity Feedを作成するには、次の構成を実装する必要があります。

- Identity Feedイベント プロセッサーを持つLog Collectorサービス
- Windows収集が構成および有効化されているLog Collectorサービス

注: Identity Feedの作成方法と調査方法の詳細については、「*Liveリソース管理ガイド*」の「Identity Feedの作成」を参照してください。

ワークフロー

このワークフローでは、ログ収集機能を介してイベントの収集を開始するために必要な基本タスクを示しています。

実行したいことは何ですか?

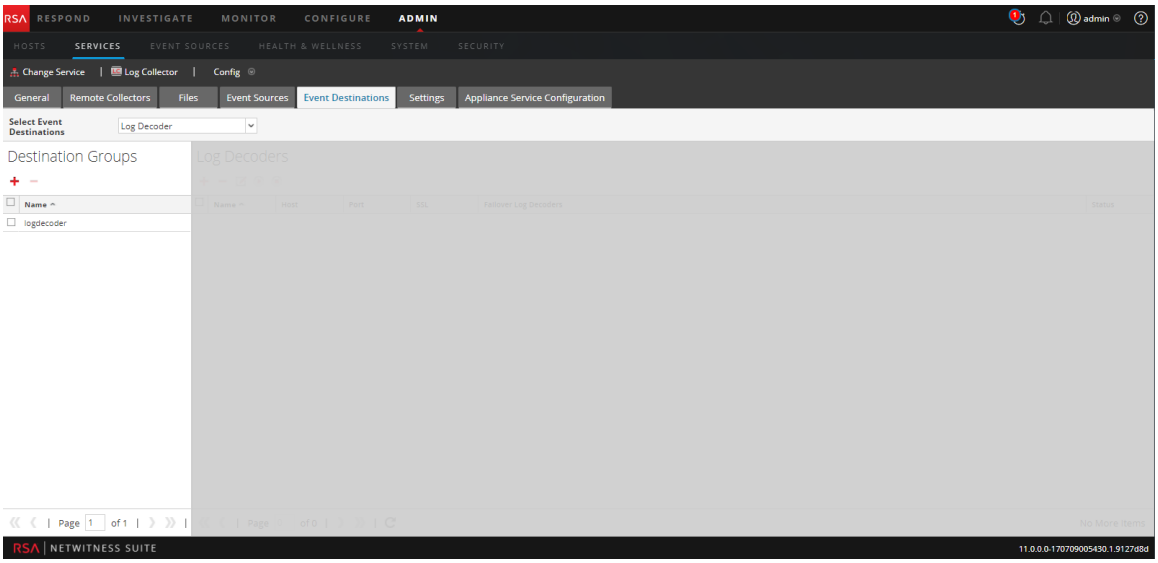
ロール	実行したいこと	ドキュメント
管理者	Log Collectorによって収集されたイベント データの宛先の構成	次の手順を参照してください。

関連トピック

- 「*Liveリソース管理ガイド*」の「**Identity Feedの作成**」トピックを参照してください。

簡単な説明

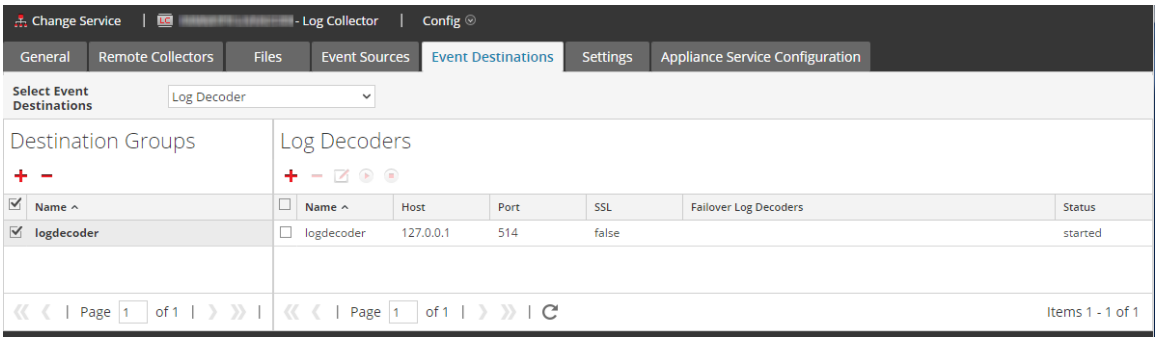
Log Collectorサービスの[構成]ビューの[イベントの宛先]タブでは、Log Collectorで収集されたイベント データの宛先を構成できます。

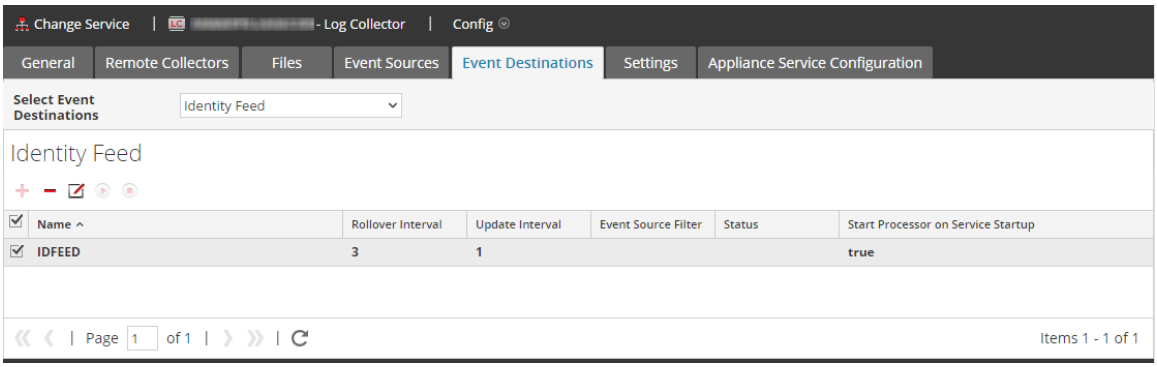


このビューへのアクセスに必要な権限は、[サービスの管理]です。

1. **管理＞[サービス]**に移動します。
2. [Log Collector]サービスを選択します。
3. [アクション]で、 ＞**[表示]＞[構成]**を選択して、ログ収集に関する構成パラメータのタブを表示します。
4. [**イベントの宛先**]タブをクリックします。
5. [**イベントの宛先の選択**]ドロップダウンメニューで、次を実行します。
   - [**Log Decoder**]を選択して、Log Collectorが収集したイベントデータの宛先をLog Decoderに設定します。

     注：Log Decoderサービスは[宛先Log Decoderの追加]ダイアログから選択する必要がありますが、残りの構成は自動的に行われます。
   - [**Identity Feed**]を選択して、Log CollectorLog Collectorが収集したイベントデータの宛先をIdentity Feedに設定します。




Change Service
- Log Collector
Config
General
Remote Collectors
Files
Event Sources
Event Destinations
Settings
Appliance Service Configuration
Select Event Destinations
Identity Feed
Identity Feed
Name
Rollover Interval
Update Interval
Event Source Filter
Status
Start Processor on Service Startup
IDFEED
3
1
true
Page 1 of 1
Items 1 - 1 of 1

ログ収集の[イベント ソース]タブ

[イベント ソース]タブを使用して、AWS(CloudTrail) 、Check Point、ファイル、ODBC、SDEE、SNMP、Syslog、SNMP、VMware、Windows、Windows Legacyの各イベント ソースを構成します。

[イベント ソース]タブにアクセスするには、管理＞[サービス]＞ログ収集サービスを選択＞[表示]＞[構成]＞[イベント ソース]に移動します。

ワークフロー

このワークフローでは、ログ収集機能を介してイベントの収集を開始するために必要な基本タスクを示しています。

実行したいことは何ですか?

ロール	実行したいこと	ドキュメント
管理者	AWS(CloudTrail) イベント ソースの構成。	NetWitness SuiteでのAWS (CloudTrail) イベント ソースの構成
管理者	CheckPointイベント ソースの構成。	NetWitness SuiteでのCheck Pointイベント ソースの構成
管理者	ファイル イベント ソースの構成。	NetWitness Suiteでのファイル イベント ソースの構成
管理者	ODBCイベント ソースの構成。	NetWitness SuiteでのODBCイベント ソースの構成
管理者	SDEEイベント ソースの構成。	NetWitness SuiteでのSDEEイベント ソースの構成
管理者	SNMPイベント ソースの構成。	NetWitness SuiteでのSNMPイベント ソースの構成
管理者	Syslogイベント ソースの構成。	リモートCollectorに対するSyslogイベント ソースの構成

ロール	実行したいこと	ドキュメント
管理者	VMwareイベント ソースの構成。	NetWitness SuiteでのVMware イベント ソースの構成
管理者	Windowsイベント ソースの構成。	NetWitness SuiteでのWindows イベント ソースの構成
管理者	Windows Legacyイベント ソースの構成。	Windows Legacy収集および NetApp収集の構成

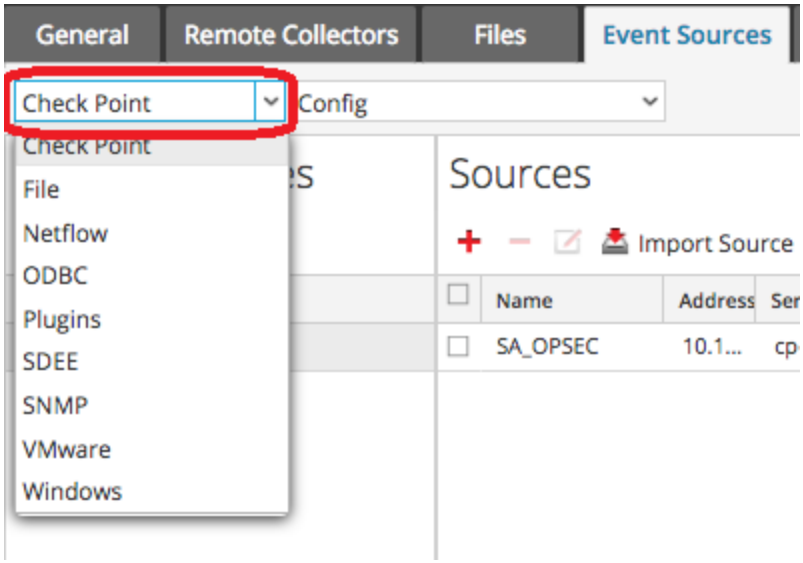
関連トピック

- NetWitness SuiteでのAWS(CloudTrail) イベント ソースの構成
- NetWitness SuiteでのCheck Pointイベント ソースの構成
- NetWitness Suiteでのファイル イベント ソースの構成
- NetWitness SuiteでのODBCイベント ソースの構成
- NetWitness SuiteでのSDEEイベント ソースの構成
- NetWitness SuiteでのSNMPイベント ソースの構成
- リモートCollectorに対するSyslogイベント ソースの構成
- NetWitness SuiteでのVMwareイベント ソースの構成
- NetWitness SuiteでのWindowsイベント ソースの構成
- Windows Legacy収集およびNetApp収集の構成

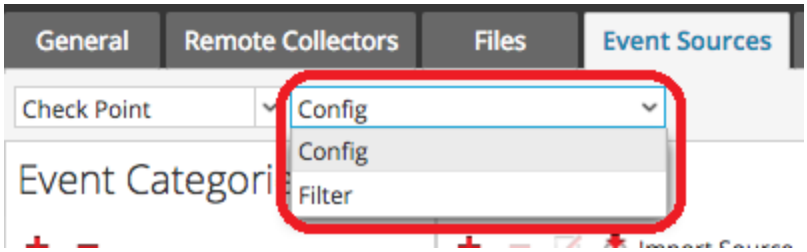
簡単な説明

[構成]ビューには、2つのドロップダウン メニューがあります。

- 一番左のメニューには、使用可能なすべての収集プロトコルが表示されています。



- 一番右のメニューには2つの選択肢があります。[**構成**]と[**フィルタ**]です。



[イベント ソース]タブの[構成]ビューには、[イベント カテゴリー]と[ソース]の2つのパネルがあります。

注:[フィルタ]メニュー アイテムの詳細については、「Collectorのイベント フィルタの構成」を参照してください。

イベント ソース タイプ メニュー

Log Collectorの[イベント ソース]タブには、収集プロトコルとそのプロトコルに関連するパラメータを選択するための、2つのボックスから成るドロップダウン メニューがあります。

左側のボックスでは、次のいずれかのプロトコルを選択します。Check Point、ファイル、ODBC、プラグイン、SDEE、SNMP、SNMP、VMware、Windows、Windows Legacy。

右側のボックスでは、次の設定を選択します。

- 左側のドロップダウンで選択したタイプの一般的なイベント ソース パラメータを構成するには、[構成]を選択します。 すべてのタイプの[構成]パネルでは、ツールバーに次のオプショ

ンが用意されています。

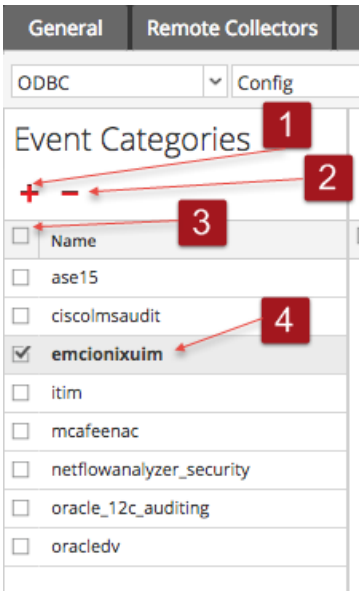
- 追加、編集、削除
- インポート(ソースのインポート、DSNのインポート)
- エクスポート(ソースのエクスポート、DSNのエクスポート)

- ODBC、SNMP、Windowsを選択した場合:
  - ODBC:DSNの構成
  - SNMP:SNMP v3ユーザ マネージャ
  - Windows:Kerberosレルム構成

オプションを選択すると構成パネルが表示され、イベント ソースの収集パラメータを構成できます。構成パネルはイベント ソースごとに少しづつ異なります。各イベント ソースごとのパラメータは個別のセクションで説明します。

[イベント カテゴリー]パネル

収集プロトコルを選択すると、[イベント カテゴリ]パネルにその収集プロトコル用に構成したすべてのイベント ソースが表示されます。たとえば、次のイメージは、構成済みのODBCイベント ソースを示しています。



[イベント カテゴリー]パネルでは、イベント ソース タイプを追加または削除できます。

1 イベント ソースを追加します。[使用可能なイベント ソース タイプ]ダイアログを表示します。このダイアログで、パラメータを定義するイベント ソース タイプを選択します。

2 選択したイベント ソース タイプを[イベント カテゴリー]パネルから削除します。

3 イベント ソース タイプを選択します。

4 追加したイベント ソース タイプの名前を表示します。

[ソース] パネル

[ソース] パネルには、選択したイベント ソース タイプのパラメータの値が表示されます。詳細については、個々の収集プロトコルのトピックを参照してください。

ログ収集の[設定]タブ

[設定]タブでは、次の操作を実行できます。

- Lockbox設定
- Stable System Valueのリセット
- 証明書の管理

注意: Log Collectorがインストールされているホスト名がインストール後に変更された場合、Log Collectorはイベント ソースからのイベントの収集に失敗します。ホスト名が変更された場合はStable System Valueをリセットする必要があります。

ログ収集の[設定]タブにアクセスするには、管理 > [サービス]に移動します。[サービス]グリッドで、Log Collectorサービスを選択します。[アクション]の下の[Actions menu cropped]をクリックし、[表示] > [構成]を選択します。

ワークフロー

このワークフローでは、ログ収集機能を介してイベントの収集を開始するために必要な基本タスクを示しています。

実行したいことは何ですか?

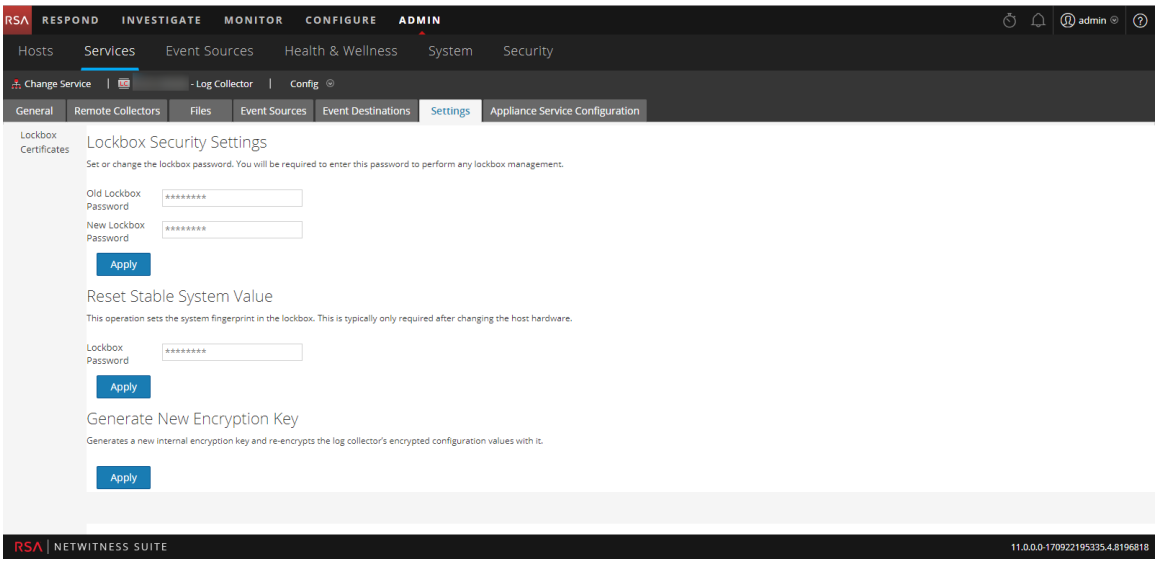
ロール	実行したいこと	ドキュメント
管理者	Lockboxの設定を管理するためのLockboxの設定。	Lockbox設定
管理者	証明書の追加または削除。	証明書の構成

関連トピック

- 「*Liveリソース管理ガイド*」の「Identity Feedの作成」トピックを参照してください。

簡単な説明

これは[設定]タブの例です。


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
Hosts
Services
Event Sources
Health & Wellness
System
Security
Change Service
- Log Collector
Config
General
Remote Collectors
Files
Event Sources
Event Destinations
Settings
Appliance Service Configuration
Lockbox Certificates
Lockbox Security Settings
Set or change the lockbox password. You will be required to enter this password to perform any lockbox management.
Old Lockbox Password
New Lockbox Password
Apply
Reset Stable System Value
This operation sets the system fingerprint in the lockbox. This is typically only required after changing the host hardware.
Lockbox Password
Apply
Generate New Encryption Key
Generates a new internal encryption key and re-encrypts the log collector's encrypted configuration values with it.
Apply
RSA | NETWITNESS SUITE
11.0.0.0-170922195335.4.8196818

ログ収集のトラブルシューティング

このトピックでは、ログ収集のトラブルシューティングの形式と内容について説明します。NetWitness Suiteは、Log Collectorの問題または潜在的な問題を次の2つの方法で通知します。

- ログ ファイル。
- [ヘルスモニタ]ビュー。

ログ ファイル

特定のイベント ソース収集プロトコルに問題がある場合は、問題の調査のためにデバッグ ログをレビューします。各イベント ソースには、このログの収集を有効化できるデバッグパラメータがあります(パラメータをOnまたはVerboseに設定します) 。

注意: 該当するイベント ソースに問題が発生し、その問題を調査する必要がある場合にのみ、デバッグを有効にします。デバッグを常に有効化すると、Log Collectorのパフォーマンスに悪影響があります。

ヘルスモニタの監視

ヘルスモニタの監視によって潜在的なハードウェアおよびソフトウェアの問題をタイムリーに認識し、システム停止を避けることができます。RSAでは、サービスが効率的に動作し、各種の統計値が構成した閾値に近づいていないことを確認するために、Log Collectorの統計フィールドを監視することを推奨します。**[管理]＞[ヘルスモニタ]**ビューに表示される次の統計値を監視できます。

トラブルシューティングの例

RSA NetWitness Suiteは、ログ ファイルに次のタイプのエラー メッセージを返します。

ログ メッセージ	`timestamp failure (LogCollection) Message-Broker Statistics: ...`
	`timestamp failure (AMQPClientBaseLogCollection): ...`
	`timestamp failure (MessageBrokerLogReceiver): ...`

考えら	Log Collectorがメッセージ ブローカーに到達できません。メッセージ ブローカーが次のいずれかの状態である可能性があります。

れる原因	• 実行を停止した。 • 接続設定が正しくない。

解決策	1. <use the="the" systemctl="systemctl" command="command" on="on" console="console" to="to" check="check" status="status" of="of" message="message" broker="broker" shell="shell" console.="console.">returns the following if the message broker is not running:</use>
	`prompt$ systemctl status rabbitmq-server`
	`rabbitmq start/running, process 10916`
	2. [エクスプローラ]ビューでイベント ブローカー ノードのRabbitMQ Message Broker を起動します。