



RSA NetWitness Endpoint統合ガイド

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せん。予告なく変更される場合があります。

2月 2018

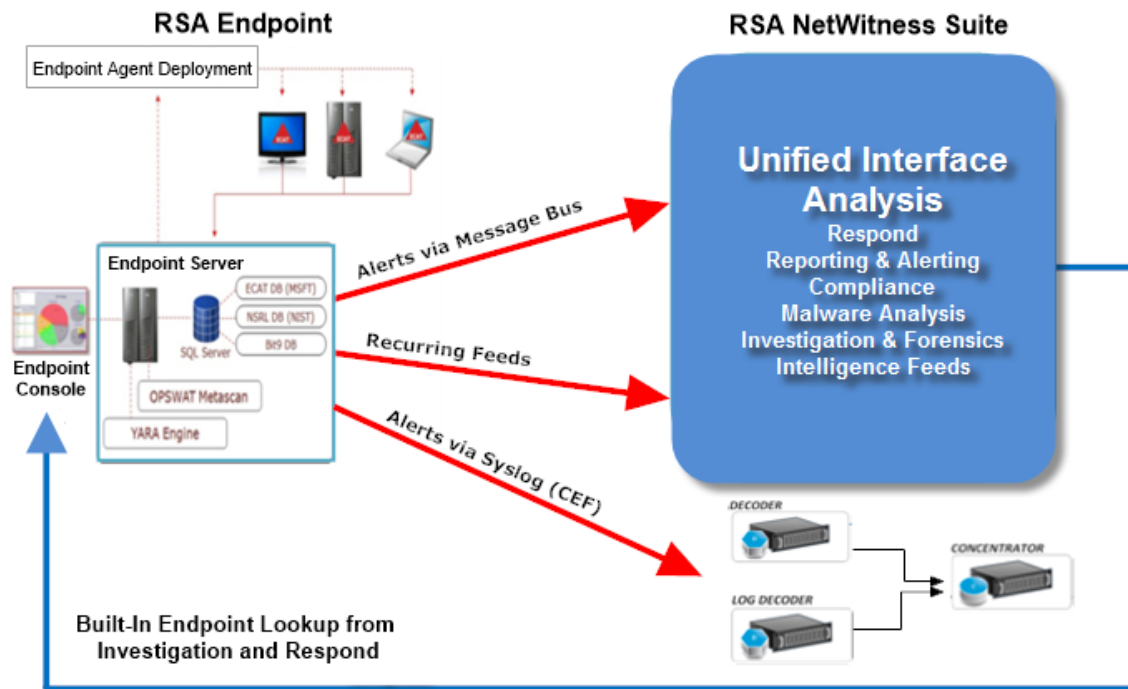
目次

RSA NetWitness Endpointの統合	4
統合オプション	4
ビルトインNetWitness Endpointルックアップ	4
統合方法	5
NetWitness Endpointメタの統合	5
NetWitness Endpointのアラートと侵害インジケータ	6
メッセージパス経由のNetWitness EndPointアラートの構成	7
NetWitness Endpointアラートを転送するNetWitness Endpointの構成	8
繰り返しFeedを通じたNetWitness Endpointからのコンテキストデータの構成	11
NetWitness SuiteのNetWitness Endpoint Feedの有効化	12
NetWitness EndpointのSSL証明書のエクスポート	15
NetWitness Suite Concentratorサービスの構成	16
NetWitness Suiteでの繰り返しカスタムFeedタスクの構成	17
Log DecoderへのSyslog経由のEndpointアラートの構成	21
NetWitness SuiteへのSyslog出力を送信するNetWitness Endpointの構成	22
table-map-custom.xmlでのテーブルマッピングの編集	23
NetWitness Suite Concentratorサービスの構成	26

RSA NetWitness Endpointの統合

RSA NetWitness Endpoint 4.3.0.4、4.3.0.5、または4.4を使用しているRSAのお客様は、NetWitness EndpointとRSA NetWitness Suiteをいくつかの方法で統合できます。このガイドは、RSA NetWitness Suiteバージョン11.0を対象としています。

統合オプション



ビルトインNetWitness Endpointルックアップ

アナリストがブラウザでNetWitness Suiteにアクセスしているコンピューターに、RSA NetWitness Endpoint UI(ユーザ インタフェース) がインストールされている場合、NetWitness Suite InvestigationとNetWitness Suite Respondに組み込まれたNetWitness Endpointルックアップ機能によって、次のメタ キーで右クリックすればNetWitness Endpointコンソール サーバにアクセスできます。IPアドレス(ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip)、host (alias-host, domain.dst)、client、file-hash)。詳細については、「調査およびマルウェア解析ユーザガイド」の「メタ キーの外部ルックアップの起動」トピックおよび「NetWitness Respondユーザガイド」の「[アラート]ビュー」トピックを参照してください。

ビルトインParserであるNetWitness EndpointまたはCEFを使用し、かつInvestigationで使用されるデフォルトのメタ キーをカスタマイズしていない場合、エンドポイント ルックアップの為にNetWitness Suiteを構成する必要はありません。詳細については、「調査およびマルウェア解析 ユーザガイド」の「Investigationでのデフォルト メタ キーの管理と適用」トピックを参照してください。

注:例外としては、Investigationのデフォルト メタ キーの表示設定を編集して、NetWitness Suiteをカスタマイズしたり、メタ キーをtable-map-custom.xmlファイルに追加したり、NetWitness Endpoint Feedをカスタマイズする場合があります。「システム構成ガイド」の「コンテキスト メニューのカスタム アクションの追加」トピックで説明されているように、構成によっては、[管理] > [システム]ビューから、NetWitness Endpoint/ルックアップのコンテキスト メニューにカスタムメタ キーを追加する必要があります。

統合方法

RSA NetWitness Endpoint 4.3.0.4、4.3.0.5、または4.4のコンソール サーバがWindowsホストにインストールされ、NetWitness EndpointとNetWitness Suiteが管理者によって適切に構成されている場合、NetWitness Endpoint分析データの3つの追加統合が可能です。

RSA NetWitness Endpointの統合方法は以下のとおりです。

- メッセージ バス経由のEndPointアラートの構成
- 繰り返しFeedを通じたEndpointからのコンテキスト データの構成
- Log DecoderへのSyslog経由のEndpointアラートの構成

メッセージ バス経由のNetWitness RespondへのEndpointアラートの構成。この統合では、Endpointアラートをメッセージ バス経由でRespondに転送する機能が提供されます。

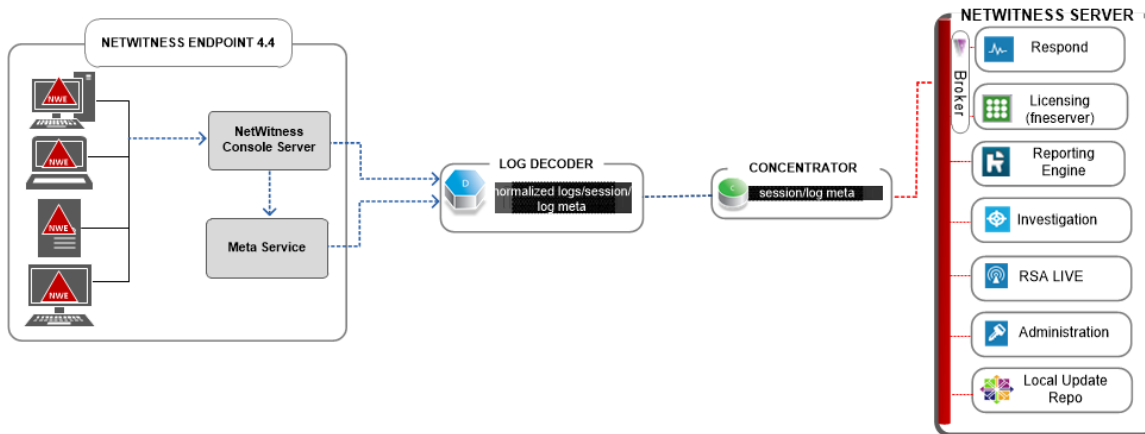
NetWitness Suite Liveの繰り返しFeedを通じたEndpointからのコンテキスト データこの統合では、たとえば、ホスト オペレーティング システム、MACアドレス、HOCスコア、ログやパケット データに存在しないその他のデータなどのコンテキスト情報を使用して、NetWitness Suite Investigationに表示されるセッションにより豊富な情報を付加することができます。

NetWitness Suite Log DecoderへのSyslog(CEF) 経由のNetWitness Endpointアラート。この統合では、Syslog経由でEndpointイベントを転送したり、イベントをNetWitness Suiteエコシステム内の他のログまたはパケット メタデータと関連づける機能を提供します。

NetWitness Endpointメタの統合

NetWitness EndpointのメタとRSA NetWitness Suiteとの統合により、両方の製品を使用しているお客様は、これらの製品を1つのユーザ インタフェースでより簡単に利用できます。次の図は、NetWitness EndpointとNetWitness Suiteの統合を示しています。NetWitness Endpointのメタデータは、NetWitness Endpointエージェントが導入されているすべてのコンピューターから収集および公開された後に、NetWitness Suite Log Decoderに送信されます。

メタは関連づけられているNetWitness Suite ConcentratorおよびNetWitness Suite調査にも表示できます。



NetWitness Endpointのアラートと侵害インジケータ

NetWitness Endpoint IOC(セキュリティ侵害インジケータ)は、NetWitness Endpointがスキャン対象のホストにおけるマルウェアの存在を判断するために、収集されたNetWitness Endpointスキャンデータに対して実行するデータベースクエリです。RSA NetWitness Endpoint 4.1.2以降には、ユーザが有効化しアラート対象としてマークできるIOCが同梱されています。RSA NetWitness Endpointは、データベースに収集されて格納される新しいスキャンデータに対してIOCクエリを定期的に行います。IOCクエリにマッチするデータが検知された場合、これはセキュリティ侵害の可能性を示しており、このイベントをユーザに報告したり、外部システムにアラートとして送信することができます。

アラートには次のタイプがあります。

- マシンアラート: このアラートは、対象のマシンが疑わしいことを示します。
- モジュールアラート: このアラートは、ファイル、DLL、実行ファイルなどのモジュールが疑わしいことを示します。対象のモジュールに関する詳細情報も含まれています。
- イベントアラート: このアラートは、前述のカテゴリに属さないその他の疑わしいアクティビティがNetWitness Endpointで検知されたことを示します。

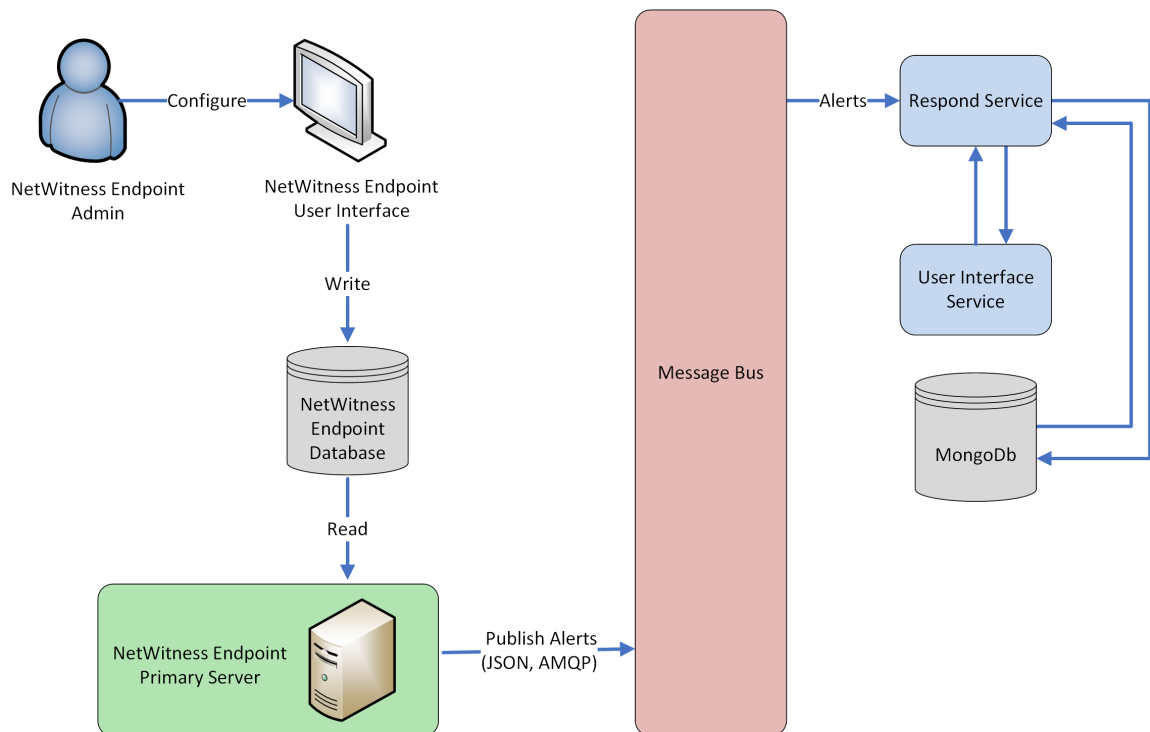
これらのアラートタイプはそれぞれNetWitness Suiteに送信できます。

メッセージ バス経由のNetWitness EndPointアラートの構成

ここでは、NetWitness EndpointとNetWitness Suiteを統合するのに必要な手順を紹介します。この手順を完了すると、NetWitness SuiteのRespondコンポーネントによってNetWitness Endpointアラートが収集され、[対応]>[アラート]ビューに表示されるようになります。

注: NetWitness Respondの統合に関して、RSAはNetWitness Endpointのバージョン4.3.0.4、4.3.0.5、または4.4をサポートします。詳細については、「*NetWitness Endpointユーザガイド*」の「RSA NetWitness Suite Integration」トピックを参照してください。

次の図は、NetWitness Suiteの[対応]の[インシデント リスト]ビューへのNetWitness Endpointアラートの流れと、[対応]>[アラート]ビューでの表示を示しています。



前提条件

以下の条件を満たしていることを確認します。

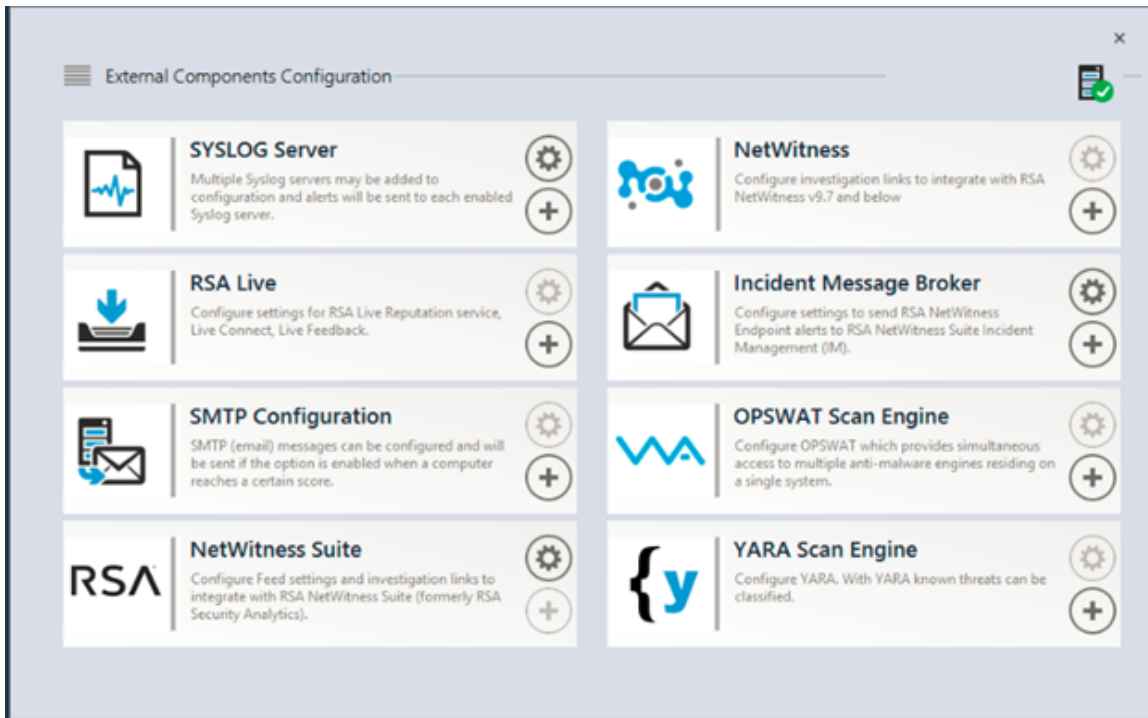
- Respondサービスがインストールされ、NetWitness Suite 11.0で実行されていること。
- NetWitness Endpoint 4.3.0.4、4.3.0.5、4.4 がインストールされ、実行されていること。

NetWitness Endpointアラートを転送するNetWitness Endpointの構成

メッセージパス経由でアラートをNetWitness Suiteのユーザインターフェイスに送信するようにNetWitness Endpointを構成するには、次の手順を実行します。

1. NetWitness Endpointユーザインターフェイスで、[構成]>[監視と外部コンポーネント]をクリックします。

[外部コンポーネントの構成]ダイアログが表示されます。



- a. リストされているコンポーネントから[インシデント メッセージ ブローカー]を選択し、+をクリックして新しいIM brokerを追加します。
2. 次のフィールドを入力します。
 - a. **インスタンス名** : IM brokerを識別する一意の名前を入力します。
 - b. **サーバのホスト名/IPアドレス**: IM brokerのホストDNSまたはIPアドレスを入力します (NetWitnessサーバ)。
 - c. **ポート番号** : デフォルトのポートは5671です。
 3. [保存]をクリックします。
 4. C:\Program Files\RSA\ECAT\ServerのConsoleServer.exe.configファイルに移動します。
 5. 次のように、ファイルの仮想ホスト構成を変更します。


```
<add key="IMVirtualHost" value="/rsa/system" />
```


注: NetWitness Suite 11.0では、仮想ホストは「rsa/system」です。バージョン10.6.x以下では、仮想ホストとは「rsa/sa」です。

6. APIサーバとコンソールサーバを再起動します。
7. Respondアラート用にSSLを設定するには、NetWitness EndpointプライマリコンソールサーバでSSL通信を設定する次の手順を実行します。
 - a. ローカルコンピュータの個人証明書ストアから(秘密鍵を選択せずに) NetWitness EndpointのCA証明書を.CER形式(Base-64でエンコードされたX.509)でエクスポートします。
 - b. NetWitness EndpointのCA証明書を使用して、NetWitness Endpointのクライアント証明書を生成します(CN名を「ecat」に設定する必要があります)。


```
makecert -pe -n "CN=ecat" -len 2048 -ss my -sr LocalMachine -a sha1 -sky exchange -eku 1.3.6.1.5.5.7.3.2 -in "NweCA" -is MY -ir LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -cy end -sy 12 client.cer
```

注: 前述のコードサンプルで、以前のバージョンからEndpointバージョン4.3にアップグレードし、新しい証明書を生成していない場合、「NweCA」の代わりに「EcatCA」を使用する必要があります。
 - c. ステップbで生成したクライアント証明書の拇印をメモしておきます。次に示すように、ConsoleServer.Exe.ConfigファイルのIMBrokerClientCertificateThumbprintセクションに、クライアント証明書の拇印の値を入力します。


```
<add key="IMBrokerClientCertificateThumbprint" value="896df0efacf0c976d955d5300ba0073383c83abc"/>
```
8. NetWitnessサーバで、.CER形式のNetWitness Endpoint CA証明書ファイルをインポートフォルダにコピーします。


```
/etc/pki/nw/trust/import
```
9. 次のコマンドを発行して、必要なChef実行を開始します。


```
orchestration-cli-client --update-admin-node
```

 これにより、すべての証明書がトラストストアに追加されます。
10. RabbitMQサーバを再起動します。


```
systemctl restart rabbitmq-server
```

 NetWitness Endpointアカウントは自動的にRabbitMQで利用可能になります。
11. /etc/pki/nw/ca/nwca-cert.pemファイルと/etc/pki/nw/ca/ssca-cert.pemファイルをNetWitnessサーバからインポートし、それらをEndpointサーバの信頼できるルート証明書ストアに追加します。

トラブルシューティング

このセクションでは、メッセージ バス経由でNetWitness Endpointのアラートを構成するときに発生する可能性のある問題の解決方法を提案します。

既知の問題	解決策
管理ノードでオーケストレーションに失敗する。	EcatCA証明書の内容を/etc/rabbitmq/ssl/truststore.pemにコピー&ペーストし、Rabbitmqサービスを再起動する必要があります。

繰り返しFeedを通じたNetWitness Endpointからのコンテキスト データの構成

RSA NetWitness EndpointのデータをRSA NetWitness Suiteで構成し、NetWitness Endpointからのコンテキスト データをDecoderおよびLog Decoderセッションに提供することができます。この構成では、コンテキスト メタ値の他、NetWitness Suiteエコシステムのその他のメタデータとの相関を構築するときに使用できるインスタントIOCアラートが追加されます。

管理者は、NetWitness Suite Liveの繰り返しFeedを介してNetWitness Endpointからのシステムスキャン コンテキスト データを使用するようにNetWitness Suiteを構成できます。この統合により、DecoderまたはLog Decoderからのセッションに対して、NetWitness Suite Investigationにコンテキスト情報が表示されるようになります。これらの情報には、ホスト オペレーティングシステム、MACアドレス、IIOCスコアなど、DecoderまたはLog Decoderからのセッションのログまたはパケット データには存在しないデータが含まれます。

注:この機能は、パケットDecoderを使用する環境を対象にしていますが、繰り返しFeedはLog Decoderにも実装できます。

注意:多数のNetWitness Endpointホストがある環境では、繰り返しFeedを使用することで、NetWitness Suiteの収集デバイス(DecoderおよびLog Decoder)のパフォーマンスが低下する場合があります。

前提条件

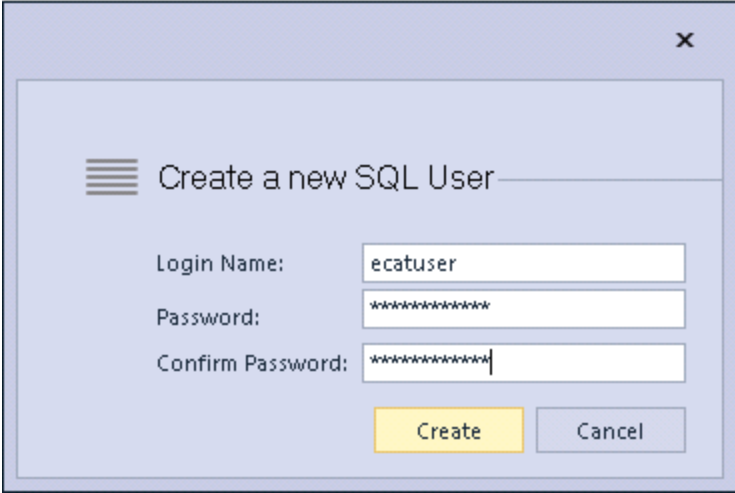
- バージョン4.3.0.4、4.3.0.5、または4.4のNetWitness Endpointコンソール サーバとNetWitness サーババージョン10.4以上がインストールされていること。
- バージョン11.0のRSA DecoderおよびConcentratorがネットワーク内のNetWitnessサーバに接続されていること。

繰り返しFeedを通じたNetWitness Endpointからのコンテキスト データを構成するには、次の手順を実行します。

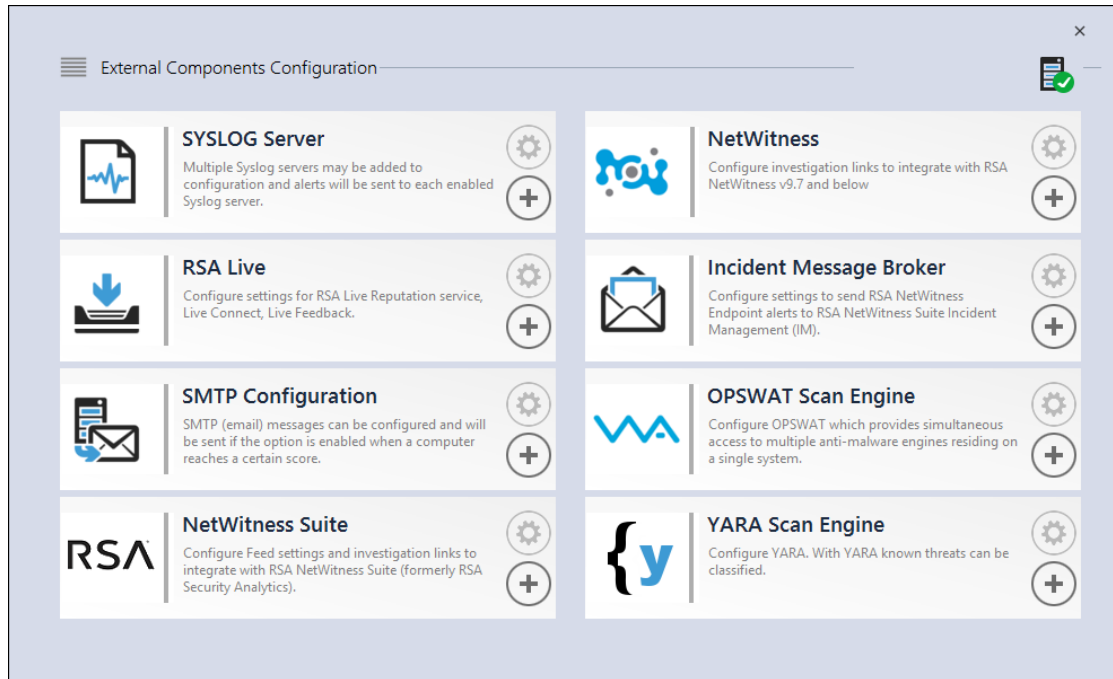
- NetWitness Endpointユーザ インタフェースでNetWitness SuiteのNetWitness Endpoint Feedを有効化します。
- NetWitness Endpointコンソール サーバからNetWitness Endpoint CA証明書をエクスポートし、NetWitness Suiteトラストストアにインポートします。
- NetWitness Suite Concentratorサービスを構成して、インデックスを作成するメタキーを定義します。
- NetWitness Suite Liveで繰り返しFeedを作成します。

NetWitness SuiteのNetWitness Endpoint Feedの有効化

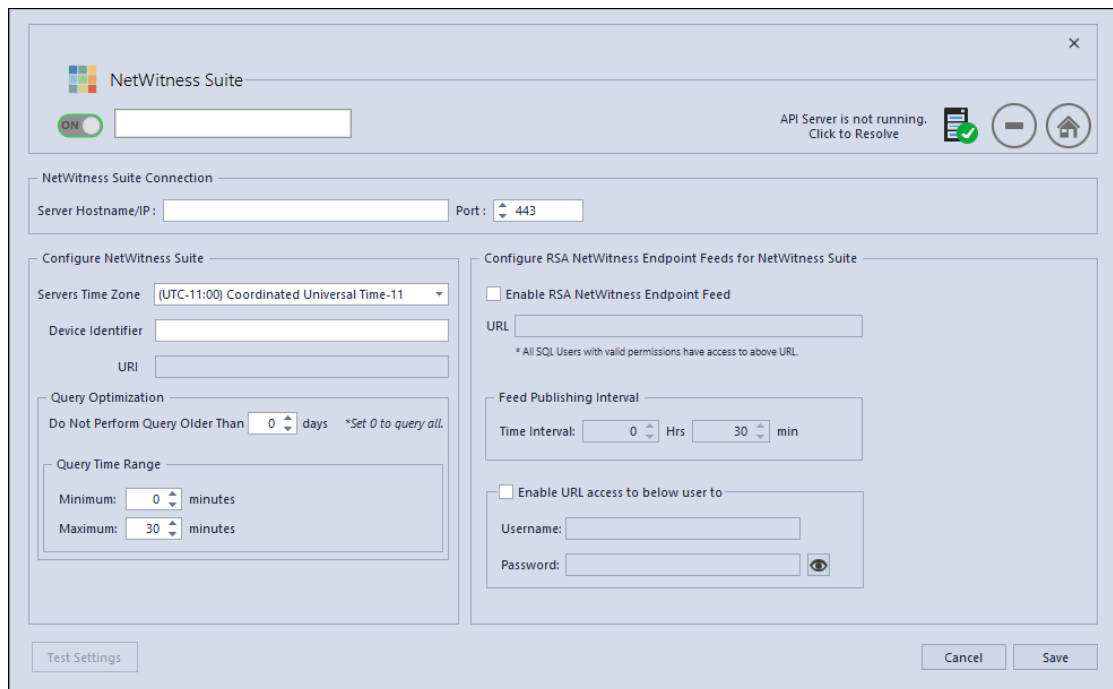
1. NetWitness Endpointのユーザ インタフェースで、SQLユーザをNetWitness Endpointに作成します。
 - a. NetWitness Endpointのユーザ インタフェースを開き、適切な認証情報を使用してログオンします。
 - b. メニュー バーで、[構成]>[ユーザとロールの管理]を選択し、ペインを右クリックして[SQLユーザの作成]を選択します。
[新しいSQLユーザの作成]ダイアログが表示されます。



- c. [ログイン名]と[パスワード]を入力し、[作成]をクリックします。
2. メニュー バーから[構成]>[外部コンポーネントの監視]を選択します。
[外部コンポーネントの構成]ダイアログが表示されます。



3. NetWitness Suiteで、+をクリックします。
[NetWitness Suite]ダイアログが表示されます。



4. [NetWitness Suite]パネルの[オン]に、NetWitness Suiteコンポーネントを識別するための名前を入力します。

5. [NetWitness Suiteの接続]パネルで、次の手順を実行します。
 - a. [サーバホスト名/IP]フィールドに、NetWitnessサーバのホスト名またはIPアドレスを入力します。
 - b. [ポート]フィールドに、ポート番号を入力します。デフォルトでは、ポート番号は443です。
6. [NetWitness Suiteの構成]パネルで、次の手順を実行します。
 - a. [サーバのタイムゾーン]フィールドで、ドロップダウンリストからコンポーネントのタイムゾーンを選択します。
 - b. [デバイス識別子]フィールドにNetWitness Suite ConcentratorデバイスのIDを入力します。

注:[調査]>[ナビゲート]<ConcentratorまたはBrokerの名前>でConcentratorまたはBrokerを検索すると、NetWitness Suiteのデバイスの識別子が見つかります。デバイスの識別子は、URL内の「investigation」の後の数字です。たとえば、URLがhttps://<IP address>investigation/319/navigate/valuesの場合、デバイスの識別子は319です。

[保存]をクリックすると、[URI]フィールドが設定されます。

7. [クエリの最適化]パネルの[古いクエリを実行しない]フィールドに、クエリ期間の制限を日数で入力します。この機能を無効にする場合は、「0」を入力します。
8. [クエリ時間範囲]パネルで、次の手順を実行します。
 - a. [最小値]フィールドに、最小のクエリ時間範囲を分単位で入力します。この値を使用して、NetWitness Suiteに送信される時間範囲を自動的に増加させます。これにより、NetWitness Endpointエージェントの報告された時刻がNetWitness Endpointの時刻とわずかに異なる場合、クエリが肯定的な応答を返すようになります。
 - b. [最大値]フィールドに、時間範囲の制限を分単位で入力します。この値を使用して、NetWitness Suiteに送信される時間範囲が自動的に制限されるため、クエリがNetWitnessサーバを過負荷にすることはありません。
9. [NetWitness SuiteのRSA NetWitness Endpoint Feedの構成]パネルで、次の手順を実行します。
 - a. [RSA NetWitness Endpoint Feedを有効化]を選択します。
 - b. [URL]フィールドで、SQLユーザ名とパスワード(ステップ1で構成した)を入力し、Feedの場所にアクセスします。

[保存]をクリックすると、[URL]フィールドが設定されます。

- c. Feedが発行される頻度の時間間隔を入力します。
10. [Feedの発行間隔]パネルの[時間間隔]フィールドで、Feedが発行される頻度を示す時間の間隔を時間と分で選択します。
11. [次のユーザのURLアクセスを有効化]パネルで、NetWitness Endpointユーザの[ユーザ名]と[パスワード]を入力します。
12. [保存]をクリックします。
Feedが作成されます。

NetWitness EndpointのSSL証明書のエクスポート

注: Java 8のサポートはNetWitness Suite 10.5に対して追加されたため、この手順は10.5以上にのみ適用されます。それより前のバージョンのNetWitness Suiteを使用している場合は、このガイドで該当するバージョンを参照してください。

NetWitness Endpointコンソール サーバからNetWitness Endpoint CA証明書をエクスポートし、それをNetWitness Suiteホストにコピーするには、次の手順を実行します。

1. NetWitness Endpointコンソールにログオンします。
2. MMCを開きます。
3. コンピューター アカウント用の証明書スナップインを追加します。
4. EcatCAという名前の証明書をエクスポートします。
 - a. 秘密鍵なしでエクスポートします。
 - b. DERエンコード バイナリX.509(.CER)形式でエクスポートします。
 - c. EcatCA.cerという名前を付けます。
5. NetWitness Endpoint CA証明書をNetWitness Suiteホストにコピーします。
 - NetWitness Endpoint 4.3.0.4、4.3.0.5、4.4の新規インストールの場合：
`scp NweCA.cer root@<sa-machine>:.`
 - 以前のバージョンからNetWitness Endpoint 4.3.0.4または4.3.0.5へのアップグレードの場合：
`scp EcatCA.cer root@<sa-machine>:.`
6. NetWitness Endpoint CA証明書をNetWitness Suiteトラスト ストアにインポートするには、次の手順を実行します。

- a. 次のコマンドを使用して、NetWitness SuiteにインストールされているJavaバージョンを確認します。

```
java -version
```

openjdkバージョンが表示されます。たとえば、openjdkバージョンは「1.8.0_71」です。

- b. JDKパラメータを設定するには、javaディレクトリに移動します。以下のコマンドを実行します。

- JDK=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64/jre/

- NetWitness Endpointの新規インストールの場合：

```
$JDK/bin/keytool -import -v -trustcacerts -alias nweca -file  
~/NweCA.cer -keystore $JDK/lib/security/cacerts -storepass changeit
```

- 以前のバージョンからのNetWitness Endpointのアップグレードの場合：

```
$JDK/bin/keytool -import -v -trustcacerts -alias ecatca -file  
~/EcatCA.cer -keystore $JDK/lib/security/cacerts -storepass  
changeit
```

証明書更新の確認のプロンプトが表示されたら、「Yes」と入力します。

7. NetWitness Suiteホストで、次のいずれかを実行します。

- NetWitness Endpoint 4.3.0.4、4.3.0.5、4.4の新規インストールの場合は、`/etc/hosts`を編集し、このファイルに次の行を追加して、NetWitness Endpointコンソール サーバのIPアドレスをNweServerCertificateという名前にマップします。

```
<ip-address-ecat-cs> NweServerCertificate
```

- 以前のバージョンからNetWitness Endpoint 4.3.0.4または4.3.0.5へのアップグレードの場合は、`/etc/hosts`を編集し、このファイルに次の行を追加して、アップグレードしたNetWitness Endpointコンソール サーバのIPアドレスをecatserverexportedという名前にマップします。

```
<ip-address-ecat-cs> ecatserverexported
```

8. NetWitness Suiteを再起動するには、次のコマンドを実行します。

```
service jetty restart
```

NetWitness Suite Concentratorサービスの構成

1. NetWitness Suiteにログオンし、[管理]>[サービス]に移動します。
2. リストからConcentratorを選択して、[表示]>[構成]を選択します。
3. [ファイル]タブを選択し、[編集するファイル]ドロップダウンメニューから、`index-concentrator-custom.xml`を選択します。

4. 次のNetWitness Endpointメタ キーをファイルに追加し、[適用]をクリックします。このファイルにはXMLセクションがすでに含まれることに注意してください。例を次に示します。構成と値がFeed定義に含まれる列名に一致することを確認してください。ここで、

descriptionは、NetWitness Suite Investigationで表示されるメタ キー名です。

levelは「IndexValues」です。

nameは、繰り返しFeedを定義する際にNetWitness Suiteが使用するCSVファイルの列名と一致します(次の「NetWitness Suiteでの繰り返しカスタムFeedタスクの構成」の表を参照してください)。

```
<key description="Gateway" format="Text" level="IndexValues"
name="gateway" valueMax="250000" defaultAction="Open"/>

<key description="Risk Number" format="Float64" level="IndexValues"
name="risk.num" valueMax="250000" defaultAction="Open"/>

<key description="Strans Addr" format="Text" level="IndexValues"
name="stransaddr" valueMax="250000" defaultAction="Open"/>

<key description="Domain" format="Text" level="IndexValues"
name="domain" valueMax="250000" defaultAction="Open"/>

<key description="User Account" format="Text" level="IndexValues"
name="username" valueMax="250000" defaultAction="Open"/>

<key description="Ecat Connectiontime" format="Text"
level="IndexValues" name="ecat.ctime" valueMax="250000"
defaultAction="Open"/>

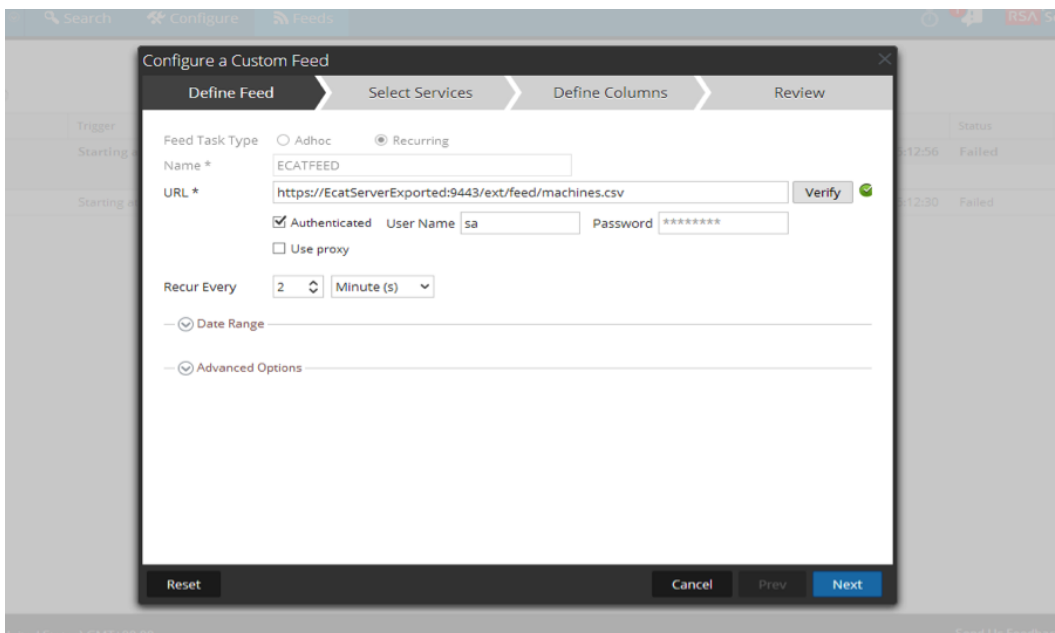
<key description="Ecat Scantime" format="Text" level="IndexValues"
name="ecat.stime" valueMax="250000" defaultAction="Open"/>
```

5. Concentratorを再起動起動して、カスタム キーの更新をアクティブ化します。

NetWitness Suiteでの繰り返しカスタムFeedタスクの構成

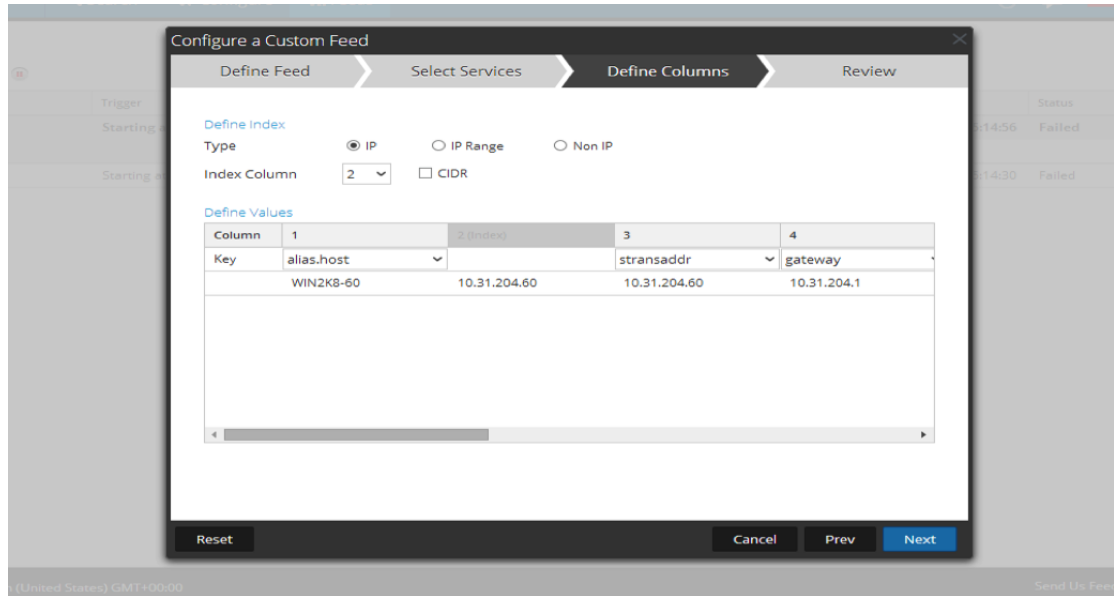
1. NetWitness Suiteにログオンし、[構成]>[カスタムFeed]に移動します。
[Feed]ビューが表示されます。
2. ツールバーで、**+**をクリックします。
[Feedの構成]ダイアログが表示されます。
3. [Feedの構成]ダイアログで、[カスタムFeed]を選択して[次へ]をクリックします。
カスタムFeedの構成ウィザードが表示され、[Feedの定義]フォームが開きます。

4. [Feedの定義]で、次の操作を実行します。
 - a. [Feedタスクタイプ]フィールドで[繰り返し]を選択します。
 - b. [名前]フィールドに、Feedの名前を入力します。たとえば、EndpointFeedなどです。
 - c. [URL]フィールドで、NetWitness EndpointがインストールされているWindowsサーバのURLとホスト名を入力します。
 - NetWitness Endpoint 4.3.0.4、4.3.0.5、4.4の新規インストールの場合は、`https://NweServerCertificate:9443/api/v2/feed/machines.csv`というURLを使用します。
 - 以前のバージョンからNetWitness Endpoint 4.3.0.4または4.3.0.5へのアップグレードの場合は、`https://ecatserverexported:9443/api/v2/feed/machines.csv`というURLを使用します。
 - d. [認証情報]チェックボックスをオンにし、前述の「`{{SA}}`のECAT Feedの有効化」でメモに記録したユーザ名とパスワードを入力します。
 - e. [検証]をクリックして、NetWitness SuiteがWebリソースにアクセスできることを確認します。
 - f. スケジュールを定義し、[次へ]をクリックします。



5. [サービスの選択]タブで、Feedを使用するDecoderまたはグループを選択します。[次へ]をクリックします。

6. [列の定義]タブで、次の表に従って列名を入力し、Feedを保存します。



次の表に、NetWitness Endpoint Feed用のCSVファイルの列を示します。

列	名前	説明	NetWitness Suiteでの列名(メタキー名)
1	MachineName	Windowsエージェントのホスト名	alias.host
2	LocalIp	IPv4アドレス	IPタイプ(インデックス付き列)
3	RemoteIp	ルーターで検出されるリモートIP	stransaddr
4	GatewayIp	ゲートウェイのIP	gateway
5	MacAddress	MACアドレス	eth.src
6	OperatingSystem	Windowsエージェントで使用されているオペレーティングシステム	OS
7	AgentID	ホストのAgent ID(Agentに割り当てられた一意のID)	client
8	ConnectionUTCTime	エージェントが最後にNetWitness Endpointサーバに接続した時刻	ecat.ctime

列	名前	説明	NetWitness Suiteでの列名(メタキー名)
9	Source Domain	Domain	domain.src
10	ScanUTC time	エージェントが前回スキャンされた時刻	ecat.stime
11	UserName	クライアント マシンのユーザ名	username
12	Machine Score	エージェントのスコア	risk.num

注: この表では、推奨されるインデックス設定は、LocalIpです。ただし、DHCPサーバによってNetWitness EndpointエージェントPCのLocalIpが割り当てられるが、DHCPリースの有効期限が切れている場合、およびIPが別のPCに再割り当てされる場合は、Feedによって作成されるメタデータが不適切になります。このリスクを回避するには、localIPアドレスの代わりに、マシン名またはMACアドレスをFeedのインデックスとして使用します。たとえば、MACアドレスを使用する場合は、次の図に示されている値を入力できます。

Configure a Custom Feed

Define Feed > Select Services > Define Columns > Review

Define Index

Type: IP IP Range Non IP

Index Column: 5 Service Type: [dropdown] Truncate Domain

Callback Key (5): eth.src

Define Values

Column	1	2	3	4	5 (index)	6	7
Key	alias.host	ip.src	stransaddr	gateway	OS	client	

結果

インデックス付けされた値 (ip.src) が一致したときに、FeedデータをNetWitness Suiteで表示する場合は、該当するメタデータが、Investigation、Reporting、Alertingの各インタフェースに表示されるようになります。

Log DecoderへのSyslog経由のEndpointアラートの構成

RSA NetWitness SuiteでRSA NetWitness Endpoint データの使用を構成してSyslog経由でNetWitness EndpointアラートをLog Decoderセッションに提供します。これにより、NetWitness Suite Investigation、Alerts、Reporting Engineで使用するメタデータが生成されます。

ログを収集および集計しているNetWitness Suiteネットワーク環境において、NetWitness EndpointとNetWitness Suiteとを統合し、NetWitness EndpointイベントをCEF(Common Event Format)形式のSyslogメッセージでLog Decoderにプッシュし、NetWitness Suite Investigation、Alerts、Reporting Engineで使用可能なメタデータを生成できます。この統合のユースケースはSIEM環境の統合と言えます。この統合によってイベントの一元管理が実現され、NetWitness Endpointイベントと他のLog Decoderデータとの関連付け、NetWitness Endpointイベントに関するNetWitness Suiteレポート作成、NetWitness Endpointイベントに関するNetWitness Suiteアラートの発行などが可能になります。

前提条件

この統合の要件を次に示します。

- バージョン4.3.0.4、4.3.0.5、または4.4のNetWitness Endpoint UIであること。
- NetWitnessサーババージョン11.0がインストールされていること。
- バージョン10.4以降のRSA Log DecoderおよびConcentratorがネットワーク内のNetWitnessサーバに接続されていること。
- NetWitness EndpointサーバからLog Decoderに対してポートUDP 514またはTCP 1514でアクセスできるようファイアウォールが構成されていること。

手順

1. 必要なParser(CEFまたはrsaecat)をLog Decoderに導入します(「Live サービス管理」の「Liveリソースの管理」トピックを参照してください)。Parserを導入した後、Parserが有効になっていることを確認します。詳細については、「サービスの[構成]ビュー:[全般]タブ」を参照してください。

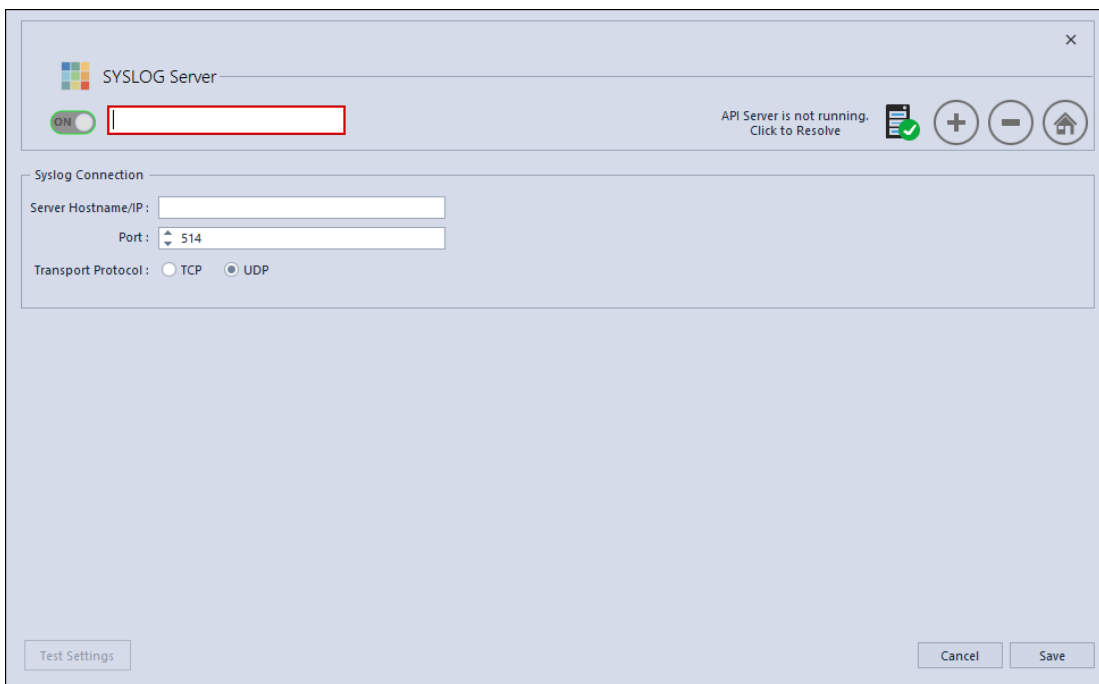
注: Parserは1種類のみ使用します。CEF Parserが導入されている場合は、それがNetWitness Endpoint Parserより優先され、NetWitness Suiteに送られるすべてのCEFメッセージがCEF Parserによって処理されます。両方のParserを有効にすると、パフォーマンスに不要な負荷がかかります。

2. NetWitness Endpointを構成して、Syslog出力をNetWitness Suiteに送信し、Log Decoderに対するNetWitness Endpointアラートを生成するよう設定します。
3. (オプション) table-map-custom.xmlとindex-concentrator-custom.xmlでテーブルマッピングを編集し、NetWitness Suiteに割り当てるメタデータを必要に応じて追加します。

NetWitness SuiteへのSyslog出力を送信するNetWitness Endpointの構成

Log DecoderをSyslog外部コンポーネントとして追加し、NetWitness Endpointアラートを生成してLog Decoderに送信するには、次の手順を実行します。

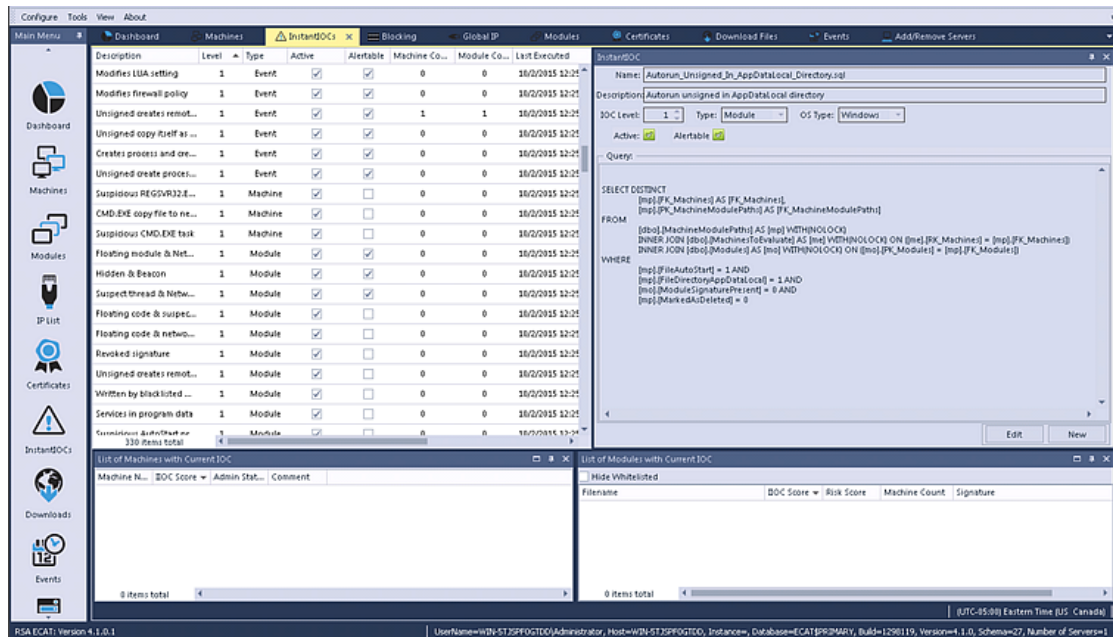
1. NetWitness Endpointのユーザ インタフェースを開き、適切な認証情報を使用してログオンします。
2. メニュー バーから[構成]>[監視と外部コンポーネント]を選択します。
[外部コンポーネントの構成]ダイアログが表示されます。
3. [SYSLOG Server]で、**+**をクリックします。
[SYSLOG Serve]ダイアログが表示されます。



4. NetWitness Suiteパネルの[オン]で、Log Decoderの分かりやすい名前を入力します。
5. [Syslog接続]パネルで、次を実行してSyslogメッセージを有効にします。

[サーバホスト名/IP] = RSA Log Decoderのホスト名 DNSまたはIPアドレス
 [ポート] = 514
 [トランスポート プロトコル] = Syslogサーバのトランスポート プロトコルとして
 [UDP]または[TCP]を選択します。

- [保存]をクリックします。
- NetWitness Endpoint UIで[InstantIOCs]ウィンドウを開き、[アラート対象]列で、Log Decoderにアラートを送信する各IIOCをクリックして有効にします。



インスタントIOCがトリガーされると、NetWitness EndpointサーバからのSyslogアラートがLog Decoderに送信されます。その後で、Log DecoderアラートがConcentratorで集計されます。これらのイベントはConcentratorにメタデータとして挿入されます。

table-map-custom.xmlでのテーブル マッピングの編集

RSAが提供するデフォルトのtable-map.xmlファイルでは、メタキーはTransientに設定されています。メタキーをInvestigationで表示するには、キーがNoneに設定されている必要があります。マッピングを変更するには、エントリをLog Decoderのtable-map-custom.xmlに追加する必要があります。

以下は、table-map.xml内のメタキーのリストです。

NetWitness Endpointの フィールド	NetWitness Suiteの マッピング	NetWitness Suiteの Transient設定
agentid	client	なし

NetWitness Endpointのフィールド	NetWitness Suiteのマッピング	NetWitness SuiteのTransient設定
CEF Header Hostname Field	alias.host	なし
CEF Header Product Version	version	あり
CEF Header Product Name	product	あり
CEF Header Severity	Severity	あり
CEF Header Signature ID	event.type	なし
CEF Header Signature Name	event.desc	なし
destinationDnsDomain	ddomain	あり
deviceDnsDomain	DOMAIN	あり
dhost	host.dst	なし
dst	ip.dst	なし
end	endtime	あり
fileHash	checksum	あり
fname	filename	なし
fsize	filename.size	あり
gatewayip	gateway	あり
instantIOCLLevel	threat.desc	なし
instantIOCName	threat.category	なし
machineOU	dn	あり
machineScore	risk.num	なし
md5sum	checksum	あり

NetWitness Endpointのフィールド	NetWitness Suiteのマッピング	NetWitness SuiteのTransient設定
os	OS	あり
port	ip.dstport	なし
protocol	protocol	あり
Raw Message	msg	あり
remoteip	stransaddr	あり
rt	alias.host	なし
sha256sum	checksum	あり
shost	host.src	なし
smac	eth.src	あり
src	ip.src	なし
start	starttime	あり
suser	user.dst	なし
timezone	timezone	あり
totalreceived	rbytes	あり
totalsent	bytes.src	なし
useragent	user.agent	なし
userOU	org	あり

以下の7個のキーはtable-map.xmlに含まれていません。これらのキーをNetWitness Suiteで使用するには、キーをtable-map-custom.xmlに追加して、フラグをNoneに設定する必要があります。

NetWitness Endpointのフィールド	NetWitness Suiteのマッピング	NetWitness SuiteのTransient設定
moduleScore	cs.modulescore	あり
moduleSignature	cs.modulesign	あり
Target module	cs.targetmodule	あり
YARA result	cs.yarareult	あり
Source module	cs.sourcemodule	あり
OPSWATResult	cs.opswatresult	あり
ReputationResult	cs.represult	あり

必要な場合は、以下のエントリをtable-map-custom.xmlに追加します。

```
<mapping envisionName="cs_represult" nwName="cs.represult" flags="None"
envisionDisplayName="ReputationResult"/>
<mapping envisionName="cs_modulescore" nwName="cs.modulescore" format="Int32"
flags="None" envisionDisplayName="ModuleScore"/>
<mapping envisionName="cs_modulesign" nwName="cs.modulesign" flags="None"
envisionDisplayName="ModuleSignature"/>
<mapping envisionName="cs_opswatresult" nwName="cs.opswatresult" flags="None"
envisionDisplayName="OpswatResult"/>
<mapping envisionName="cs_sourcemodule" nwName="cs.sourcemodule" flags="None"
envisionDisplayName="SourceModule"/>
<mapping envisionName="cs_targetmodule" nwName="cs.targetmodule" flags="None"
envisionDisplayName="TargetModule"/>
<mapping envisionName="cs_yarareult" nwName="cs.yarareult" flags="None"
envisionDisplayName="YaraResult"/>
```

注: Log Decoderを再起動するか、ログParserを再ロードすることによって、変更を有効にします。

NetWitness Suite Concentratorサービスの構成

1. NetWitness Suiteにログオンし、[管理]>[サービス]に移動します。
 1. リストからConcentratorを選択して、[表示]>[構成]を選択します。
2. [ファイル]タブを選択し、[編集するファイル]ドロップダウン リストから、index-concentrator-custom.xmlを選択します。

3. NetWitness Endpointメタ キーをファイルに追加して、[適用]をクリックします。このファイルにはXMLセクションがすでに含まれることに注意してください。
4. Concentratorを再起動します。
5. Reporting Engineのデータ ソースとしてConcentratorを追加するには、[管理]>[サービス]ビューでReporting Engineを選択し、[表示]>[構成]>[ソース]を選択します。
NetWitness EndpointメタはReporting Engineに取り込まれ、適切なメタ キーを選択してレポートを実行できます。

例

注:以下の行は例です。使用環境やFeed定義に含める列名に合わせて値を調整してください。各項目の意味は以下のとおりです。

descriptionは、NetWitness Suite Investigationで表示されるメタ キー名になります。

levelは「IndexValues」です。

nameは以下の表のNetWitness Endpointメタ キー名です。

```
<language>
<key description="Product" format="Text" level="IndexValues" name="product"
valueMax="250000" defaultAction="Open"/>
  <key description="Severity" format="Text" level="IndexValues" name="severity"
valueMax="250000" defaultAction="Open"/>
  <key description="Destination Dns Domain" format="Text" level="IndexValues"
name="ddomain" valueMax="250000" defaultAction="Open"/>
  <key description="Domain" format="Text" level="IndexValues" name="domain"
valueMax="250000" defaultAction="Open"/>
  <key description="Destination Host" format="Text" level="IndexValues"
name="host.dst" valueMax="250000" defaultAction="Open"/>
  <key description="End Time" format="TimeT" level="IndexValues" name="endtime"
valueMax="250000" defaultAction="Open"/>
  <key description="Checksum" format="Text" level="IndexValues" name="checksum"
valueMax="250000" defaultAction="Open"/>
  <key description="Filename Size" format="Int64" level="IndexValues"
name="filename.size" valueMax="250000" defaultAction="Open"/>
  <key description="Gateway" format="Text" level="IndexValues" name="gateway"
valueMax="250000" defaultAction="Open"/>
  <key description="Distinguished Name" format="Text" level="IndexValues" name="dn"
valueMax="250000" defaultAction="Open"/>
  <key description="Risk Number" format="Float64" level="IndexValues"
name="risk.num" valueMax="250000" defaultAction="Open"/>
  <key description="ReputationResult" format="Text" level="IndexValues"
name="cs.represult" valueMax="250000" defaultAction="Open"/>
  <key description="Module Score" format="Text" level="IndexValues"
name="cs.modulescore" valueMax="250000" defaultAction="Open"/>
  <key description="Module Sign" format="Text" level="IndexValues"
name="cs.modulesign" valueMax="250000" defaultAction="Open"/>
  <key description="opswat result" format="Text" level="IndexValues"
name="cs.opswatresult" valueMax="250000" defaultAction="Open"/>
  <key description="source module" format="Text" level="IndexValues"
```

```
name="cs.sourcemodule" valueMax="250000" defaultAction="Open"/>
  <key description="Target Module" format="Text" level="IndexValues"
name="cs.targetmodule" valueMax="250000" defaultAction="Open"/>
  <key description="yara result" format="Text" level="IndexValues"
name="cs.yarareresult" valueMax="250000" defaultAction="Open"/>
  <key description="Protocol" format="Text" level="IndexValues" name="protocol"
valueMax="250000" defaultAction="Open"/>
  <key description="Event Time" format="TimeT" level="IndexValues"
name="event.time" valueMax="250000" defaultAction="Open"/>
  <key description="Source Host" format="Text" level="IndexValues" name="host.src"
valueMax="250000" defaultAction="Open"/>
  <key description="Start Time" format="TimeT" level="IndexValues" name="starttime"
valueMax="250000" defaultAction="Open"/>
  <key description="Timezone" format="Text" level="IndexValues" name="timezone"
valueMax="250000" defaultAction="Open"/>
  <key description="Received Bytes" format="UInt64" level="IndexValues"
name="rbytes" valueMax="250000" defaultAction="Open"/>
  <key description="Agent User" format="Text" level="IndexValues" name="user.agent"
valueMax="250000" defaultAction="Open"/>
  <key description="Source Bytes" format="UInt64" level="IndexValues"
name="bytes.src" valueMax="250000" defaultAction="Open"/>
  <key description="Strans Address" format="Text" level="IndexValues"
name="stransaddr" valueMax="250000" defaultAction="Open"/>
</language>
```

結果

アナリストは次の操作を実行できます。

- NetWitness Endpointイベントをエンリッチメント ソースとして構成することにより、NetWitness Endpointイベントに基づいてNetWitness Suiteアラートを作成する。
- NetWitness Endpointメタを使用してESAルールを作成する(「*ESAを使用したアラート ガイド*」の「ルールライブラリへのルールの追加」トピックを参照)。
- NetWitness Endpointメタを使用してNetWitness Endpointイベントに関するレポートを作成する(「*レポート ガイド*」の「ルールの構成」トピックを参照)。
- NetWitness RespondにNetWitness Endpointアラートを表示する(「*NetWitness インシデント対応ユーザガイド*」の「アラートの表示」トピックを参照)。
- 標準のNetWitness Suiteコア キーとともにNetWitness Endpointメタ キーをInvestigationで表示する(「*調査およびマルウェア解析ユーザガイド*」の「調査の実施」トピックを参照)。