RSA NETWITNESS® PLATFORM

Endpoint Insightsエージェント インストール ガイド

バージョン 11.2

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、Dell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、民事および刑事上の責任が課せられる可能性があります。

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、これらの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

この資料に記載される情報は、発行日時点で正確であるとみなされます。この情報は予告なく変更されることがあります。

2月 2019

目次

概要

注 : このガイドに記載されている情報はバージョン11.1以降に適用されます。

ホストは、サポート対象のオペレーティング システムがインストールされているラップトップ、ワークステーション、サーバ、タブレット、ルータ等の任意のシステムです。物理ホストか仮想ホストかは問いません。Endpoint Insights エージェントは、Windows、Mac、Linuxのいずれかのオペレーティング システムが搭載されたホストに導入できます。インストール処理には、次のタスクが含まれます。

1. エンドポイント データのみを収集するか、またはエンドポイント データとログ データ(Windowsのみ) の両方を収集するエージェント パッケージを生成する
2. エージェント インストーラーを生成する

オペレーティング システムに固有のエージェント インストーラーを実行して、ホストにエージェントを導入できます。エージェントは、それらのホストからエンドポイント データおよびWindowsログ(有効な場合) を収集します。エージェントは、ホスト上のアクティビティを監視し、データとスキャン結果を、Endpoint HybridまたはEndpoint Log HybridにHTTP経由で報告します。

サポート対象のオペレーティング システム

Windows

エージェント ソフトウェアは、次のWindowsオペレーティング システムで実行されます。

- Windows Vista(32ビットおよび64ビット)
- Windows 7(32ビットおよび64ビット)
- Windows 8(32ビットおよび64ビット)
- Windows 8.1(32ビットおよび64ビット)
- Windows 10(32ビットおよび64ビット)
- Windows 2008 Server(32ビットおよび64ビット)
- Windows 2008 R2(32ビットおよび64ビット)
- Windows 2012 Server
- Windows 2012 Server R2
- Windows 2016 Server

Linux

エージェント ソフトウェアは、i386またはx84_64のどちらのアーキテクチャでも実行できます。次のLinuxオペレーティング システムで実行されます。

- CentOS 6.xおよび7.x
- Red Hat Linux 6.xおよび7.x

Mac

エージェント ソフトウェアは、次のMacオペレーティング システムで実行されます。

- MacOS X 10.9(Mavericks)
- MacOS X 10.10(Yosemite)
- MacOS X 10.11(El Capitan)
- MacOS X 10.12(Sierra)

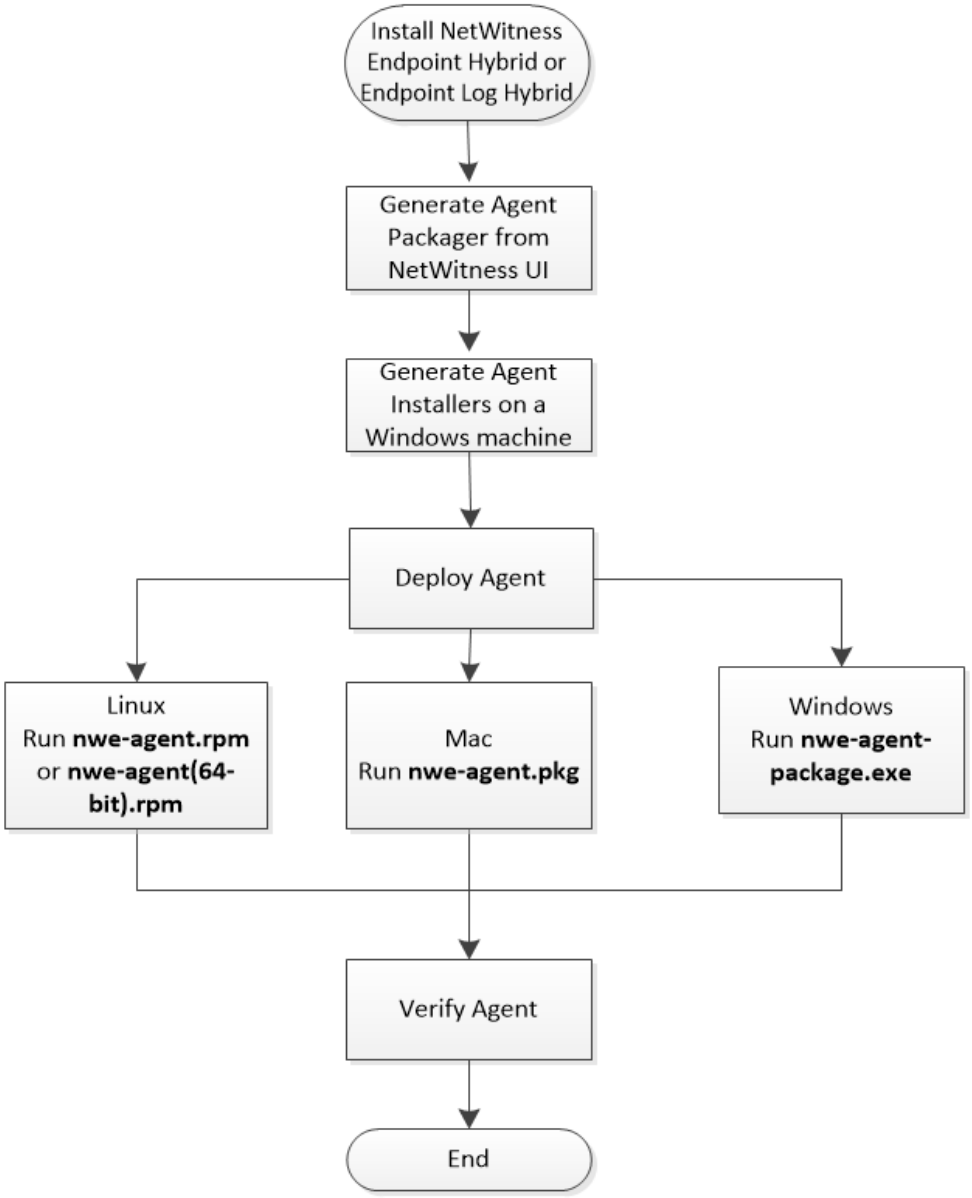
ハードウェア要件

エージェントを導入するための最小ハードウェア要件は次のとおりです。

- 256 MBのRAM
- 100 MBのディスク領域
- シングルコアCPU

インストールのフローチャート

次のフローチャートは、エンドポイント エージェントのインストール処理を示しています。


Install NetWitness Endpoint Hybrid or Endpoint Log Hybrid
Generate Agent Packager from NetWitness UI
Generate Agent Installers on a Windows machine
Deploy Agent
Linux
Run **nwe-agent.rpm** or **nwe-agent(64-bit).rpm**
Mac
Run **nwe-agent.pkg**
Windows
Run **nwe-agent-package.exe**
Verify Agent
End

前提条件

- RSA NetWitness Platformをインストールします。詳細については、「*物理ホスト インストール ガイド*」または「*仮想ホスト インストール ガイド*」を参照してください。
- NetWitness Endpoint HybridまたはEndpoint Log Hybridを構成します。詳細については、『*EndpointInsights 構成ガイド*』を参照してください。
- NetWitness Endpoint 11.1エージェントのメタデータ転送を構成します。詳細については、『*EndpointInsights 構成ガイド*』を参照してください。

Endpointエージェント パッケージの生成

エンドポイント データ収集用のエージェント パッケージの生成

ホストからエンドポイント データのみを収集するエージェント パッケージを生成するには、次の手順を実行します。

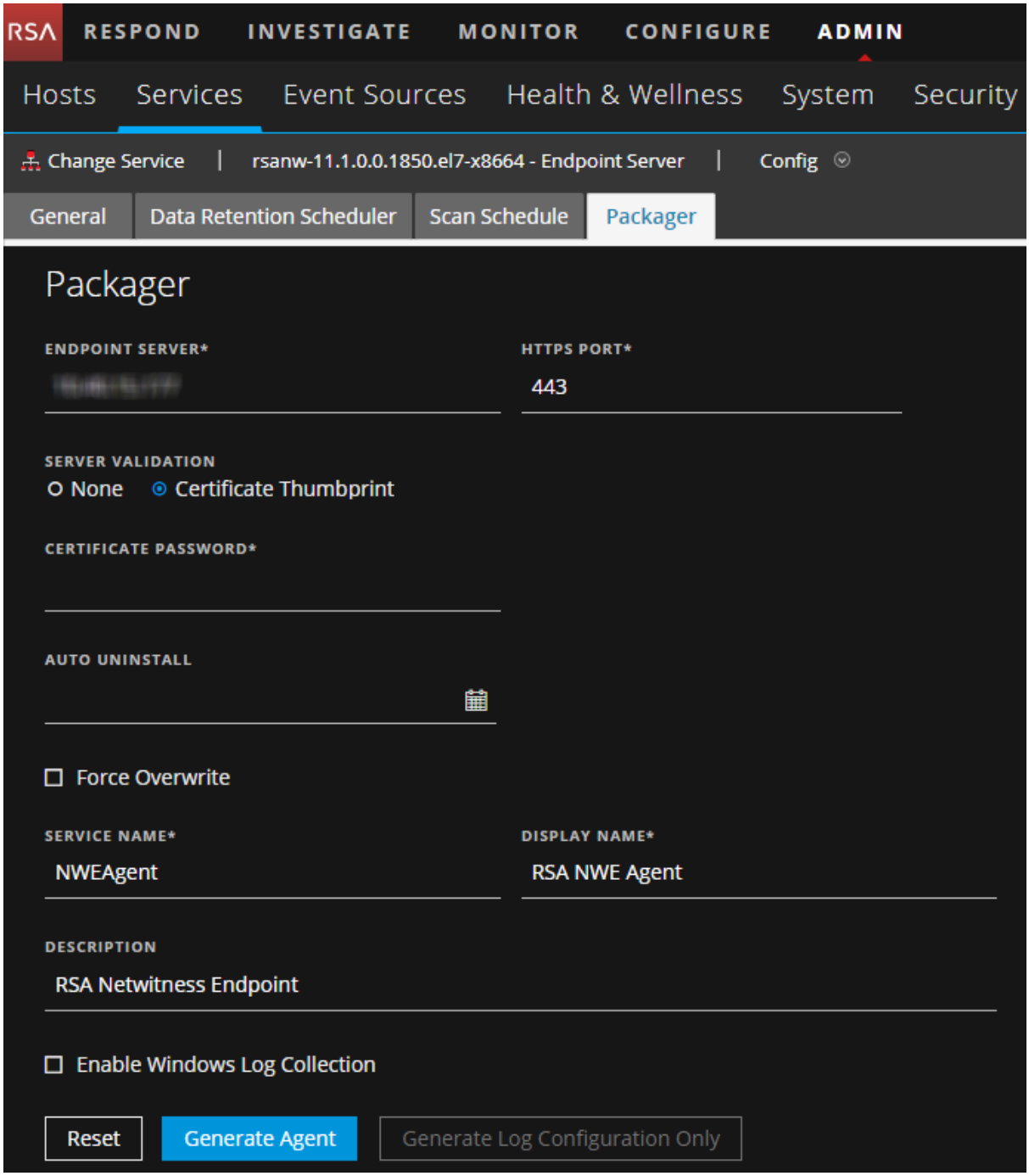
1. NetWitness Platformにログインします。

   ブラウザに、`https://<NW-Server-IP-Address>/login`と入力し、NetWitness Platformログイン画面を表示します。

2. **[管理]＞[サービス]**をクリックします。

3. [**Endpoint Server**]サービスを選択し、  **＞[表示]＞[構成]＞[Packager]**タブをクリックしま

す。[Packager]タブが表 示されます。



4. 次のフィールドに値を入力します。

フィールド	説明
Endpoint Server	Endpoint Serverのホスト名またはIPアドレス。例 : 10.10.10.3
HTTPSポート	ポート番号。たとえば、443です。
サーバの検証	エージェントがEndpoint Serverの証明書を検証する方法を指定します。 • [なし] : エージェントはサーバ証明書を検証しません。 • [証明書の拇印] : デフォルトの選択です。エージェントは、サーバ証明書のルートCAの拇印を検証することにより、サーバを識別します。
証明書のパスワード	パッケージのダウンロードに使用するパスワード。同じパスワードが、エージェント インストーラーの生成時に使用されます。たとえば、netwitnessです。
自動アンインストール	エージェントが自動的にアンインストールされる日付と時刻。不要な場合は、空白のままにします。
強制的に上書き	バージョンに関係なく、インストールされているWindowsエージェントを上書きします。このオプションを選択しない場合、1つのシステムで同じインストーラーを複数回実行できますが、エージェントがインストールされるのは1回のみです。 このオプションを有効にする場合は、新しいエージェントを作成する際に、必ず、以前にインストールしたエージェントと同じサービス名を指定してください。 **注 :** MSIで強制的に上書きする場合は、次のコマンドを実行します。 `msiexec /fvam <msifilename.msi>`
サービス名	エージェントの名前。このフィールドは、Windowsにのみ適用されます。たとえば、NWEAgentです。
表示名	エージェントの表示名。このフィールドは、Windowsにのみ適用されます。たとえば、NWEです。
説明	エージェントの説明。このフィールドは、Windowsにのみ適用されます。たとえば、RSA NetWitness Endpointです。
エージェントの生成	エージェント パッケージを生成します。

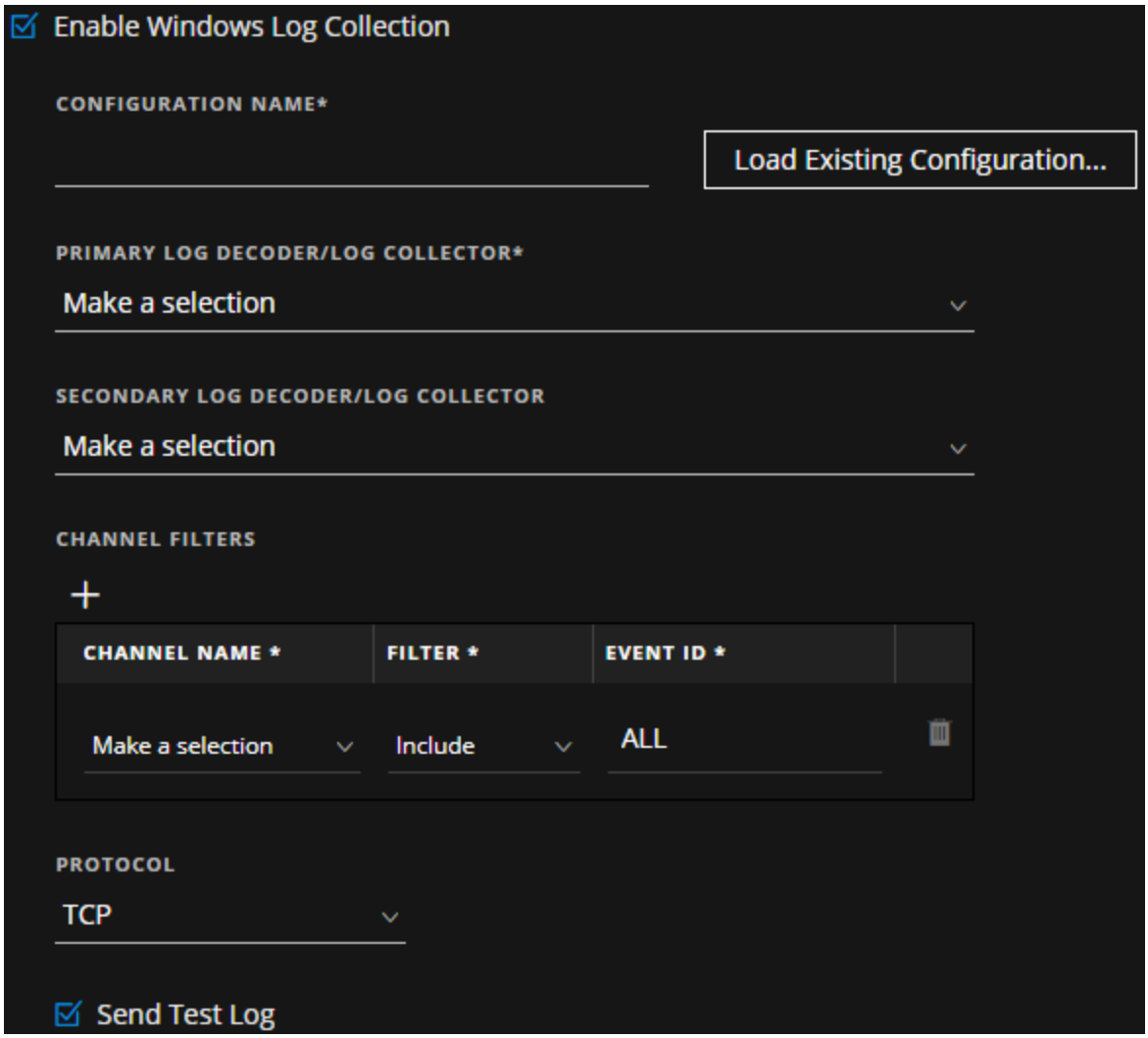
5. [**エージェントの生成**]をクリックします。

エージェント パッケージ (**AgentPackager.zip**)が、NetWitness Platformユーザ インタフェースにアクセスしているホスト上にダウンロードされます。

Windowsログ収集付きのエージェント パッケージの生成

エージェント パッケージの生成時に、エージェントのWindowsログ収集機能を有効にすることができます。このオプションを有効にすると、ログ構成ファイルが生成され、エージェントがWindowsログを収集して転送できるようになります。Windowsログ収集を有効化するには、次の手順を実行します。

1. 「エンドポイント データ収集用のエージェント パッケージの生成」の手順1～4を実行します。
2. [**Windowsログ収集を有効化する**]を選択します。

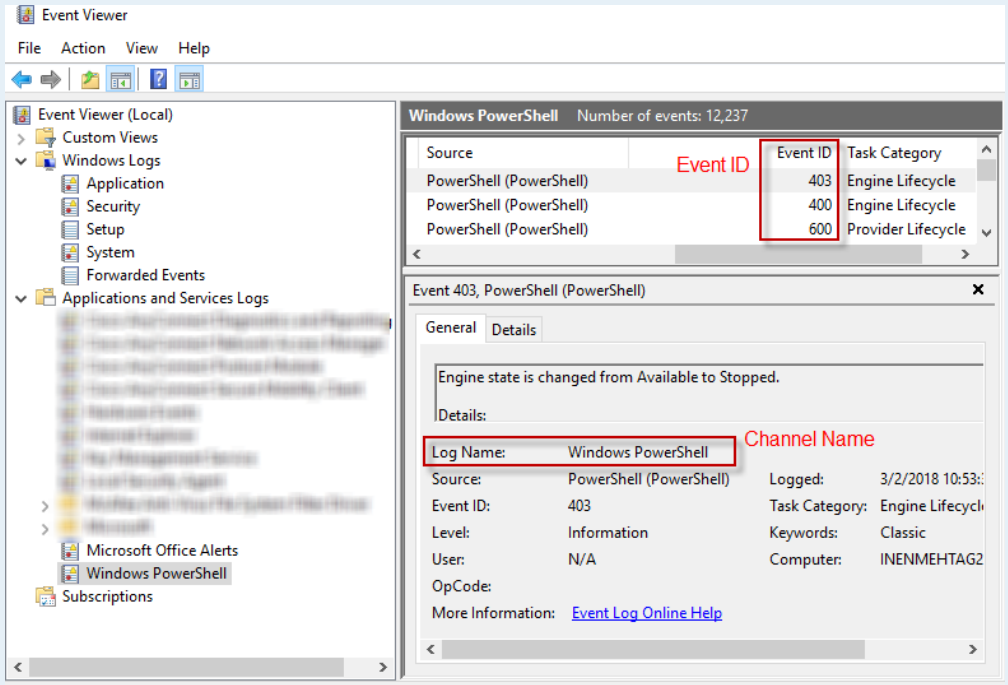


3. 次のフィールドに値を入力するか、選択します。

フィールド	説明
構成名	構成の名前。構成名には、特殊文字、英数字、ハイフン、スペース、アンダースコアを使用できます。
既存の構成をロード	ユーザのシステムから既存の構成をロードします。アップロードが正常に完了すると、Windowsログ収集のフィールドに情報が入力されます。 **注**：エラーまたは警告がある場合、アップロード中に警告メッセージが表示されます。

フィールド	説明
プライマリ Log Decoder/Log Collector	ログ転送先のプライマリLog DecoderまたはLog Collector。ここには、現在の導入環境にあるLog DecoderまたはリモートLog Collectorのリストが表示されるので、その中から選択します。このフィールドには、サービスの表示名、ホスト名、サービスタイプの組み合わせが表示されます。
(オプション) セカンダリ Log Decoder/Log Collector	ログ転送先のセカンダリLog DecoderまたはLog Collector。エージェントがプライマリLog DecoderまたはLog Collectorに到達できない場合には、セカンダリLog DecoderまたはLog CollectorがWindowsイベントを受信します。 **注：**Endpointエージェントが UDPプロトコルを使用するよう構成され、プライマリLog Decoder/リモートLog Collectorにアクセスできない場合、セカンダリLog DecoderまたはLog Collectorは機能しません。プライマリがダウンしても、ログはセカンダリLog DecoderまたはLog Collectorに転送されないため、イベントは失われます。
プロトコル	ドロップダウン メニューからプロトコルを選択します。利用可能なオプションは、[UDP]、[TCP]、[TLS]です。デフォルトのプロトコルはTCPです。

フィールド	説明
チャネル フィルタ	ログを収集するチャネル。チャネル フィルタは追加または削除できます。ログを収集するには、少なくとも1つのチャネル フィルタが必要です。 • **チャネル名**：ドロップダウン メニューからチャネルを選択します。選択可能なオプションは、[System]、[Security]、[Application]、[Setup]、[Forwarded Events]です。カスタム チャネル名のパスを入力して、カスタム チャネルを作成することもできます。カスタム チャネルは、チャネル名のリストに追加されます。カスタム チャネルを検索するには、コンピュータの[**Windowsイベント ビューアー**]にアクセスしてください。 • **フィルタ**：  をクリックして、チャネル フィルタを追加します。ドロップダウン メニューをクリックして、[Include]または[Exclude]を選択し、特定のチャネルから収集するイベントIDを指定したり、除外するイベントIDを指定します。エージェント パッケージまたはログ構成ファイルの生成時に反映されます。[Include]オプションの場合、デフォルトで、[イベントID]は[**ALL**]に設定されます。[Exclude]オプションの場合、[イベントID]は空白に設定されます。チャネル フィルタを削除するには、  をクリックします。 • **イベントID**：このチャネルのイベントIDを入力します。これらはチャネルに固有のIDであり、収集する必要があるIDです。イベントIDには、数値または範囲を指定できます。たとえば、15-32のように範囲を指定できます。ただし、32-15のような逆の指定方法は許可されません。イベントIDの組み合わせを指定することもできます。たとえば、248, 903, 16384のように、イベントIDをコンマで区切って指定できます。 **注**：[ALL]と入力した場合、そのチャネルのすべてのイベントIDを意味します。 Windowsイベント ビューアーを使用して、UIに設定するイベントIDおよびチャネル名を確認できます。次の例は、Windows PowershellのイベントIDとチャネル名を取得するための操作を示しています。情報を表示するには、[ファイル名を指定して実行]を選択し、「`Event Viewer`」と入力して、[**アプリケーションとサービス ログ**]＞[**Windows Powershell**]を選択します。[アプリケーションとサービス ログ]にWindows PowershellのイベントIDおよびチャネル名が表示されます。

フィールド	説明
	
テスト ログを送信	テスト ログ メッセージを送信します。このオプションは、デフォルトで有効です。テスト ログ メッセージが、エージェントの新規導入時または構成変更時にエージェントからLog Decoderに送信されます。テスト ログ メッセージには、エージェントに構成されたすべてのフィールドが含まれます。テスト ログ メッセージは、エージェントから宛先への接続を調べるために役立ちます。
エージェントの生成	エージェント パッケージを生成します。ログ構成ファイルは **AgentPackager.zip** ファイルに含まれます。
ログ構成のみ生成	指定したパラメータ、または[既存の構成をロード]オプションを使用してアップロードしたパラメータに従って、ログ構成ファイルを生成します。 **注**：生成されたログ構成ファイルの内容は変更しないでください。編集した場合は、エージェントがそのファイルから情報を読み取れなくなります。

注：ログ構成ファイルをダウンロードして導入することにより、Windowsログ収集機能を後から有効化することができます。詳細については、『*ログ収集の構成ガイド*』の「Endpointエージェントを使用したWindowsログ収集ファイルの追加/更新」を参照してください。

Endpointエージェント インストーラーの生成

ホストに導入するEndpointエージェント インストーラーを生成するには、次の手順を実行します。

注：エージェント パッケージ ファイルはWindowsマシンで実行します。

1. エージェント パッケージ ファイル、**AgentPackager.zip**を解凍します。次のファイルが含まれています。
   - **agents**フォルダ：Linux、Mac、Windows用の実行プログラムが含まれます。
   - **config**フォルダ：Endpoint Serverとエージェントの通信に必要な構成ファイルと証明書が含まれます。
   - **AgentPackager.exe**ファイル
2. 実行ファイル、**AgentPackager.exe**を実行します。
3. エージェント パッケージの生成時に使用したのと同じパスワードを入力して、**Enter**キーを押します。これにより、ルート フォルダに次のインストーラーが作成されます。
   - nwe-agent-package.exe(Windows用)
   - nwe-agent.pkg(Mac用)
   - nwe-agent.rpm(Linux 32ビット用)
   - nwe-agent(64-bit).rpm(Linux 64ビット用)

Endpointエージェントの導入および検証

このセクションでは、エージェントを導入して検証する手順について説明します。

エージェントの導入(Windows)

エージェントを導入するには、監視するホスト上で**nwe-agent-package.exe**ファイルを実行します。

Windowsエージェントの検証

Windowsエージェントの導入後、次のいずれかの方法を使用して、Windowsエージェントが実行されているかどうかを検証できます。

- NetWitnessのUIの使用

  [調査]>[ホスト]ビューには、エージェントが導入されているすべてのホストのリストが表示されます。エージェントがインストールされているホスト名で検索することができます。

  注:リストを更新して最新データを表示するには、[**調査**]>[**ホスト**]をクリックするか、F5を押します。

- タスク マネージャの使用

  タスク マネージャを開き、エージェント パッケージの生成時に構成したサービス名を探します。

- Services.mscの使用

  [ファイル名を指定して実行]で`Services.msc`を開き、NWEAgentを探します。

エージェントの導入(Linux)

エージェントを導入するには、監視するホスト上で**nwe-agent.rpm**(32ビットの場合)または**nwe-agent (64-bit).rpm**(64ビットの場合)を実行します。i386マシンには32-bit rpmを使用し、x84_64マシンには64-bit rpmを使用します。

Linuxエージェントの検証

Linuxエージェントの導入後、次のいずれかの方法を使用して、Linuxエージェントが実行されているかどうかを検証できます。

- NetWitnessのUIの使用

  [調査]>[ホスト]ビューには、エージェントが導入されているすべてのホストのリストが表示されます。

  注:リストを更新して最新データを表示するには、[**調査**]>[**ホスト**]をクリックするか、F5を押します。

- コマンド ラインの使用

次のコマンドを実行して、PIDを取得します。

```
pgrep nwe-agent
```

- NetWitness Endpointのバージョンを確認するには、次のコマンドを実行します。

```
cat /opt/rsa/nwe-agent/config/nwe-agent.config | grep version
```

エージェントの導入(Mac)

エージェントを導入するには、監視するホスト上で**nwe-agent.pkg**ファイルを実行します。

Macエージェントの検証

Macエージェントの導入後、次のいずれかの方法を使用して、Macエージェントが実行されているかどうかを検証できます。

- NetWitnessのUIの使用

  [調査]>[ホスト]ビューには、エージェントが導入されているすべてのホストのリストが表示されます。

  注:リストを更新して最新データを表示するには、**[調査]>[ホスト]**をクリックするか、F5を押します。

- アクティビティ モニタの使用

  アクティビティ モニタ(/Applications/Utilities/Activity Monitor.app) を開き、NWEAgentを探します。

- コマンド ラインの使用

  次のコマンドを実行して、PIDを取得します。

```
pgrep NWEAgent
```

- NetWitness Endpointのバージョンを確認するには、次のコマンドを実行します。

```
grep a /var/log/system.log | grep NWEAgent | grep Version
```

Endpoint ServerとWindows Vista、2008 Server、MacOS X 10.9および10.10にインストールされたEndpointエージェントの間の通信の構成

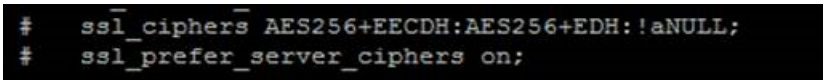
デフォルトでは、Endpoint ServerではFIPSモードが有効になっています。このため、Windows Vista、2008 Server、MacOS X 10.9および10.10にインストールされているエージェントは、Endpoint Serverと通信できません。

これを解決するには、Endpoint HybridまたはEndpoint Log Hybridで次の手順を実行して、FIPSモードを無効にします。

1. `/etc/pki/tls/owb.cnf`ファイルを編集してFIPSモードを無効にします。

```
# FIPS Mode
#   Configures the BSAFE Libraries to be in FIPS Mode.
#
#   Values: "on", "off".
#   Default: "off"
fips mode = off
```

2. /etc/nginx/conf.d/nginx.confファイルを編集して次の行をコメント アウトします。



3. 次のコマンドを使用して、Nginx Serverを再起動します。

```
systemctl restart nginx
```

エージェントのアンインストール

このセクションでは、エージェントをアンインストールするためのコマンドを示します。

Windowsエージェントのアンインストール

次のコマンドを実行します。

```
msiexec /x{63AC4523-5F19-42F0-BC43-97C8B5373589}
```

Linuxエージェントのアンインストール

次のコマンドを実行します。

```
rpm -ev nwe-agent
```

Macエージェントのアンインストール

次のコマンドを実行します。

1. `sudo launchctl unload /Library/LaunchDaemons/com.rsa.nwe.agent.daemon.plist`
2. `sudo rm -Rf /usr/local/nwe`
3. `sudo rm -Rf '/Library/Application Support/NWE'`
4. `sudo rm -Rf /Library/LaunchDaemons/com.rsa.nwe.agent.daemon.plist`
5. `sudo pkgutil --forget com.rsa.pkg.nwe`