RSA NETWITNESS® PLATFORM

Guide d'installation de l'agent Endpoint Insights

pour la version 11.2

Informations de contact

RSA Link à l'adresse https://community.rsa.com contient une base de connaissances qui répond aux questions courantes et fournit des solutions aux problèmes connus, de la documentation produit, des discussions communautaires et la gestion de dossiers.

Marques commerciales

Pour obtenir la liste des marques commerciales de RSA, rendez-vous à l'adresse suivante : france.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Contrat de licence

Ce logiciel et la documentation qui l'accompagne sont la propriété de Dell et considérés comme confidentiels. Délivrés sous licence, ils ne peuvent être utilisés et copiés que conformément aux modalités de ladite licence et moyennant l'inclusion de la note de copyright ci-dessous. Ce logiciel et sa documentation, y compris toute copie éventuelle, ne peuvent pas être remis ou mis de quelque façon que ce soit à la disposition d'un tiers.

Aucun droit ou titre de propriété sur le logiciel ou sa documentation ni aucun droit de propriété intellectuelle ne vous est cédé par la présente. Toute utilisation ou reproduction non autorisée de ce logiciel et de sa documentation peut faire l'objet de poursuites civiles et/ou pénales.

Ce logiciel est modifiable sans préavis et ne doit nullement être interprété comme un engagement de la part de Dell.

Licences tierces

Ce produit peut inclure des logiciels développés par d'autres entreprises que RSA. Le texte des contrats de licence applicables aux logiciels tiers présents dans ce produit peut être consulté sur la page de la documentation produit du site RSA Link. En faisant usage de ce produit, l'utilisateur convient qu'il est pleinement lié par les conditions des contrats de licence.

Remarque sur les technologies de chiffrement

Ce produit peut intégrer une technologie de chiffrement. Étant donné que de nombreux pays interdisent ou limitent l'utilisation, l'importation ou l'exportation des technologies de chiffrement, il convient de respecter les réglementations en vigueur lors de l'utilisation, de l'importation ou de l'exportation de ce produit.

Distribution

Dell estime que les informations figurant dans ce document sont exactes à la date de publication. Ces informations sont modifiables sans préavis.

March 2019

Sommaire

Introduction

Remarque : Les informations de ce guide s'appliquent à la version 11.1 ou ultérieure.

Les hôtes peuvent être des ordinateurs portables, stations de travail, serveurs, tablettes, routeurs ou n'importe quel système, physique ou virtuel, où un système d'exploitation pris en charge est installé. Un agent Endpoint Insights peut être déployé sur un hôte avec un système d'exploitation Windows, Mac ou Linux. Le processus d'installation implique les éléments suivants :

1. La génération d'un packager d'agent pour collecter les données du point de terminaison uniquement ou pour collecter les données à la fois du point de terminaison et des logs (Windows uniquement)
2. La génération d'un programme d'installation d'agent

Vous pouvez exécuter le programme d'installation de l'agent spécifique à votre système d'exploitation pour déployer des agents sur les hôtes. Les agents collectent les données de point de terminaison et les logs Windows (si l'option est activée) à partir de ces hôtes. Ils surveillent les activités, créent des rapports de données et analysent les résultats dans Endpoint Hybrid ou Endpoint Log Hybrid via HTTPS.

Systèmes d'exploitation pris en charge

Windows

Le logiciel de l'agent s'exécute sur les systèmes d'exploitation Windows suivants :

- Windows Vista (32 et 64 bits)
- Windows 7 (32 et 64 bits)
- Windows 8 (32 et 64 bits)
- Windows 8.1 (32 et 64 bits)
- Windows 10 (32 et 64 bits)
- Windows Server 2008 (32 et 64 bits)
- Windows 2008 R2 (32 et 64 bits)
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Linux

Le logiciel de l'agent s'exécute sur une architecture i386 ou x84_64 et sur les systèmes d'exploitation Linux suivants :

- CentOS 6.x et 7.x
- Red Hat Linux 6.x et 7.x

Mac

Le logiciel de l'agent s'exécute sur les systèmes d'exploitation Mac suivants :

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

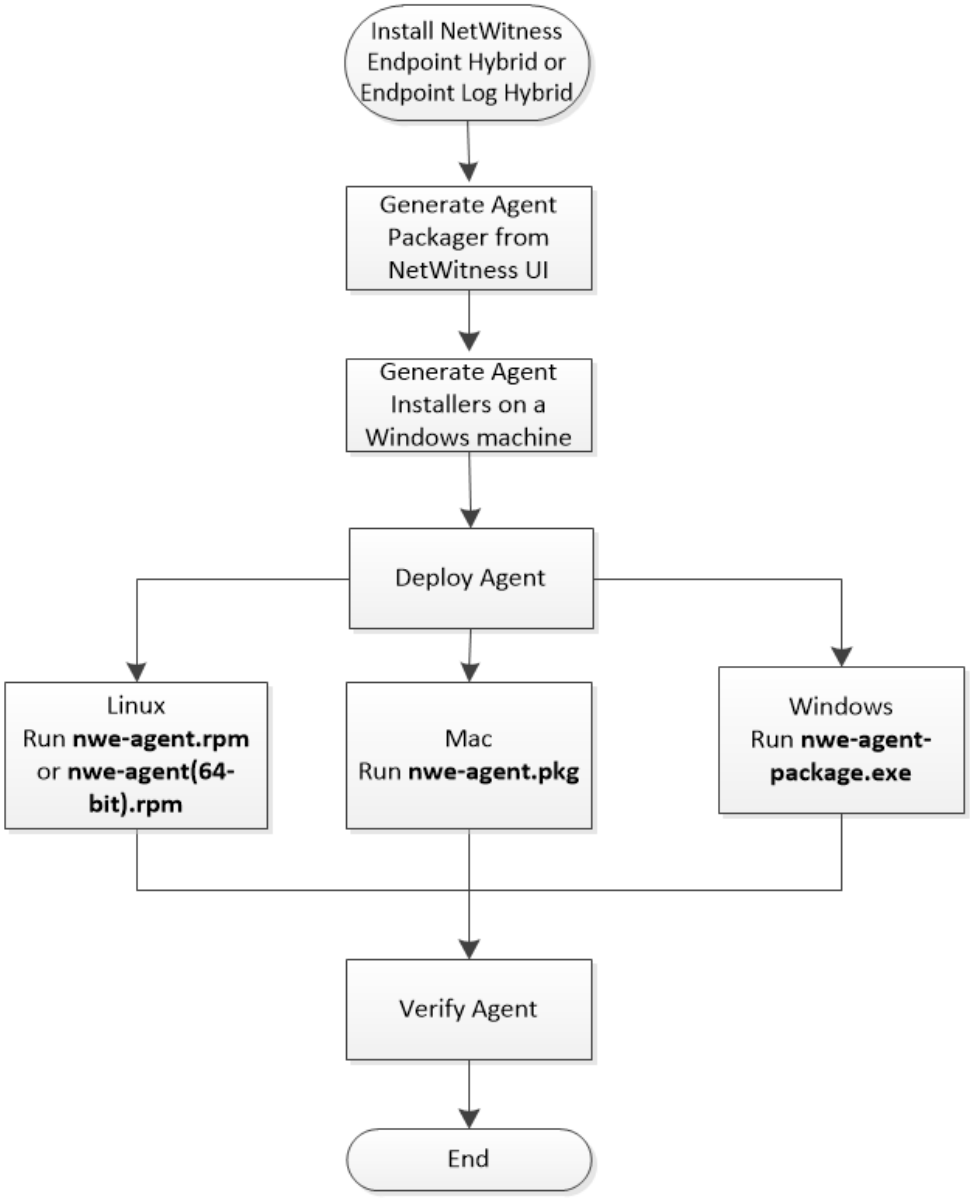
Configuration matérielle requise

Voici la configuration matérielle minimale requise pour déployer un agent :

- 256 Mo de RAM
- 100 Mo d’espace disque
- Un CPU simple cœur

Organigramme de l'installation

Le diagramme suivant illustre le processus d'installation de l'agent Endpoint :


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

Conditions préalables

- Installez RSA NetWitness Platform. Pour plus d'informations, reportez-vous au *Guide d'installation des hôtes physiques* ou au *Guide d'installation des hôtes virtuels*.
- Configurer NetWitness Endpoint Hybrid ou Endpoint Log Hybrid. Pour plus d'informations, reportez-vous au *Guide Insights Guide de configuration*.
- Configurer le transfert de métadonnées pour les agents NetWitness Endpoint 11.1 Pour plus d'informations, reportez-vous au *Guide Insights Guide de configuration*.

Générer un packager d'agent Endpoint

Génération d'un packager d'agent pour Endpoint Data Collection

Pour générer un packager d'agent afin de collecter uniquement des données Endpoint à partir d'hôtes :

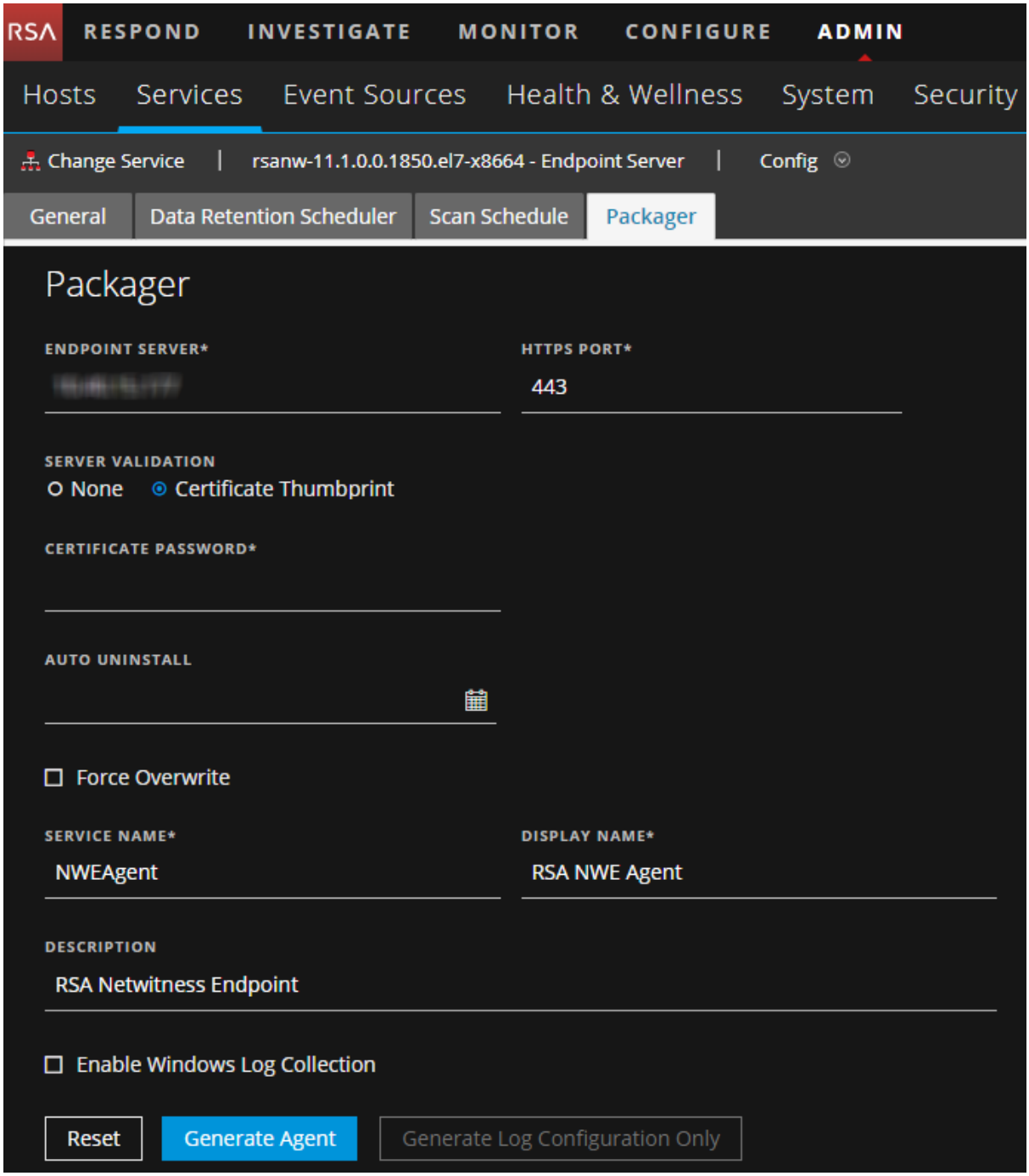
1. Connectez-vous à NetWitness Platform.

   Saisissez `https://<NW-Server-IP-Address>/login` dans votre navigateur pour accéder à l'écran de connexion NetWitness Platform.

2. Cliquez sur **ADMIN > Services**.

3. Sélectionnez le service **Serveur Endpoint**, puis cliquez sur  **> Vue > Config > onglet**

Packager. L'onglet Packager s'affiche.



4. Saisissez les valeurs dans les champs suivants :

Champ	Description
Serveur Endpoint	Nom d'hôte ou adresse IP du serveur Endpoint Par exemple, 10.10.10.3.
Port HTTPS	Numéro de port. Par exemple, 443.
Validation du serveur	Détermine la façon dont l'agent valide le certificat du serveur Endpoint : • Aucune : l'agent ne validera pas le certificat du serveur. • Empreinte du certificat : sélection par défaut. L'agent identifie le serveur en validant l'empreinte de l'autorité de certification racine du certificat du serveur.
Mot de passe du certificat	Mot de passe utilisé pour télécharger le packager. Le même mot de passe est utilisé lors de la génération du programme d'installation de l'agent. Par exemple, netwitness.
Désinstallation automatique	Date et heure de désinstallation automatique de l'agent. Vous pouvez la laisser vide si elle n'est pas requise.
Forcer le remplacement	Remplace l'agent Windows installé, quelle que soit la version. Si cette option n'est pas sélectionnée, le même programme d'installation peut être exécuté plusieurs fois sur un système, mais il installe l'agent une seule fois. Si vous activez cette option, veillez à indiquer le même nom de service que l'agent précédemment installé, lors de la création d'un nouvel agent. **Remarque :** Si vous souhaitez forcer le remplacement avec MSI, exécutez la commande suivante : `msiexec /fvam <msifilename.msi>`
Nom du service	Nom de l'agent. Ce champ s'applique uniquement à Windows. Par exemple, NWEAgent.
Nom d'affichage	Nom d'affichage de l'agent. Ce champ s'applique uniquement à Windows. Par exemple, NWE.
Description	Description de l'agent. Ce champ s'applique uniquement à Windows. Par exemple, RSA NetWitness Endpoint.
Générer l'agent	Génère un packager d'agent.

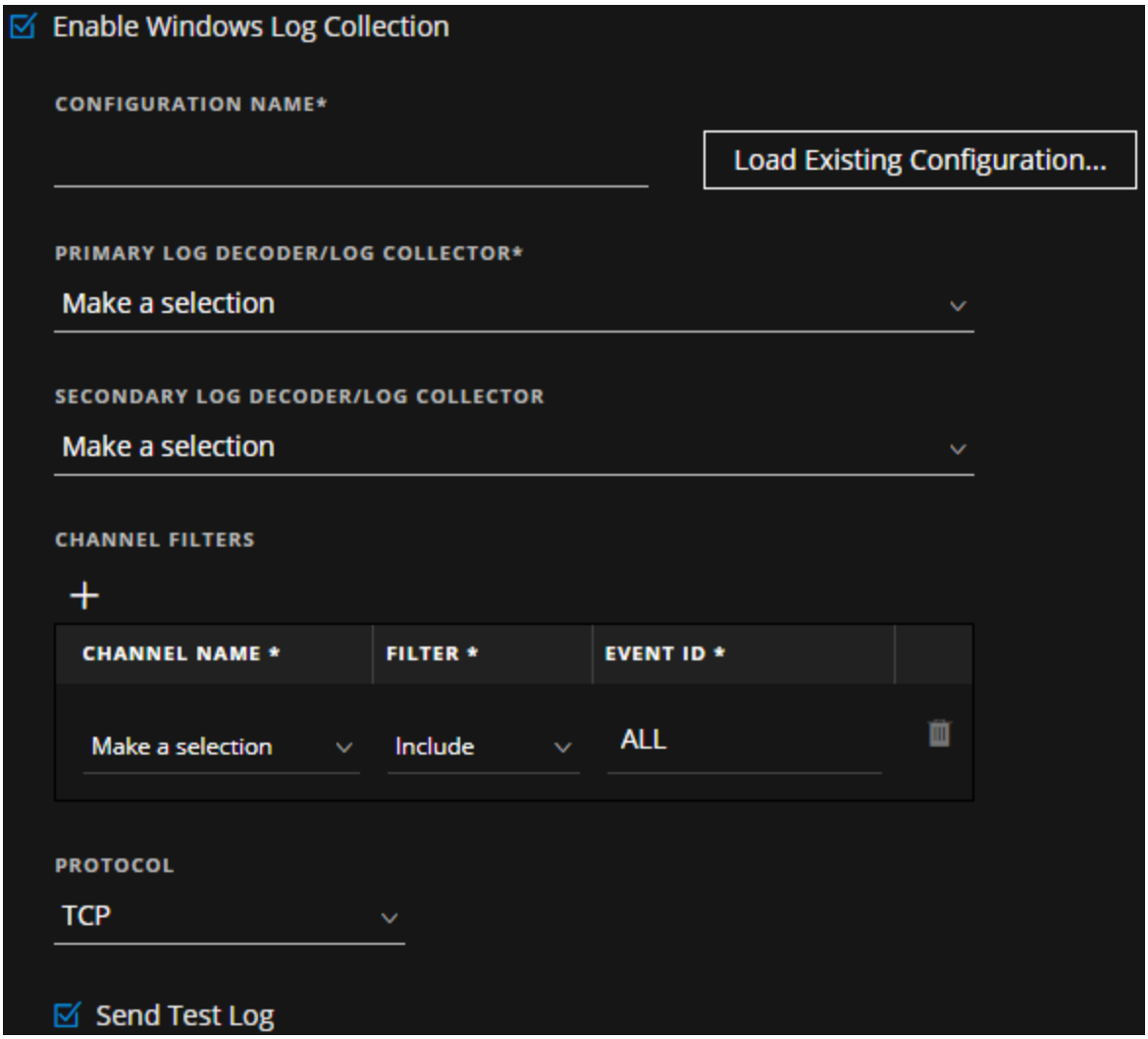
5. Cliquez sur **Générer l'agent.**.

   Cela télécharge un packager d'agent (**AgentPackager.zip**)sur l'hôte où vous accédez à l'interface utilisateur NetWitness Platform.

Génération d'un packager d'agent avec Windows Log Collection

Vous pouvez activer la fonction Windows Log Collection dans l'agent lors de la génération du packager d'agent. Grâce à cette option, un fichier de configuration de log est généré, et l'agent peut collecter et transférer des logs Windows. Pour activer Windows Log Collection :

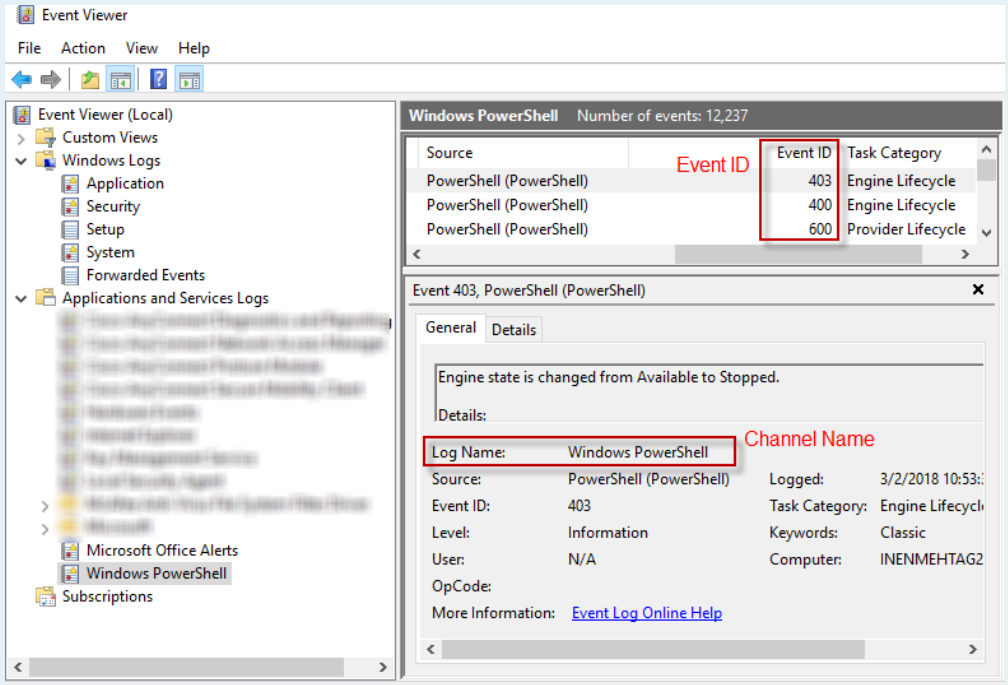
1. Exécutez les étapes 1 à 4 de la rubrique Génération d'un packager d'agent pour Endpoint Data Collection.
2. Sélectionnez **Activer Windows Log Collection**.



3. Saisissez ou sélectionnez les valeurs dans les champs suivants :

Champ	Description
Nom de configuration	Nom de la configuration. Le nom de la configuration peut comporter des caractères spéciaux, des valeurs alphanumériques, des traits d'union, des espaces et des traits de soulignement.
Charger la configuration existante	Charge une configuration existante à partir du système utilisateur. Les champs Windows Log Collection sont renseignés avec les informations sur la réussite du téléchargement. **Remarque :** Les messages d'avertissement s'affichent pendant le téléchargement s'il existe des erreurs ou avertissements.
Log Decoder/Log Collector principal	Log Decoder/Log Collector principal pour le transfert de logs. Affiche la liste des Log Decoders ou Remote Log Collectors dans le déploiement actuel. Ce champ est une combinaison du nom d'affichage du service, du nom d'hôte et du type de service.
(Facultatif) Log Decoder/Log Collector secondaire	Log Decoder/Log Collector secondaire pour le transfert de logs. Le Log Decoder ou Log Collector secondaire reçoit les événements de Windows, si l'agent ne peut pas atteindre le Log Decoder ou Log Collector principal. **Remarque :** Lorsque le Log Decoder/Remote Log Collector primaire n'est pas accessible et que l'agent Endpoint est configuré pour utiliser le protocole UDP, le Log Decoder ou Log Collector secondaire n'est pas utilisable. Les logs ne sont pas transférés au Log Decoder ou Log Collector secondaire lorsque le principal est défaillant, ce qui engendre la perte de l'événement.
Protocole	Dans le menu déroulant, sélectionnez le protocole. Les options disponibles sont UDP, TCP et TLS. Par défaut, le protocole est TCP.

Champ	Description
Filtres de canal	Canaux à partir desquels les logs sont collectés. Vous pouvez ajouter ou supprimer un filtre de canal. Il devrait y avoir au moins un filtre de canal pour collecter les logs. • **Nom du canal** : Dans le menu déroulant, sélectionnez le canal. Les options disponibles sont Système, Sécurité, Application, Configuration et Événements transmis. Vous pouvez également créer un canal personnalisé en saisissant un chemin d'accès de nom de canal personnalisé. Il est ajouté à la liste Nom du canal. Pour rechercher des canaux personnalisés, rendez-vous dans **l'Observateur d'événements Windows** sur votre ordinateur. • **Filtrer** : Cliquez sur  pour ajouter un filtre de canal. Cliquez sur le menu déroulant pour inclure ou exclure les ID d'événements à partir d'un canal spécifique lors de la génération du packager d'agent ou du fichier de configuration du log. Par défaut, pour l'option Inclure, l'ID d'événement est défini sur **TOUS**. Pour l'option Exclure, l'ID d'événement est vide. Cliquez sur  pour supprimer un filtre de canal. • **ID d'événement** Saisissez les ID d'événement de ce canal. Ceux-ci sont spécifiques aux canaux et ce sont les ID qui doivent être collectés. Les ID d'événement peuvent être une valeur numérique ou une plage de valeurs. Par exemple, utilisez-le dans une plage comme 15-32. Mais, une plage inversée n'est pas autorisée, par exemple 32-15. Les ID d'événement peuvent également servir de combinaisons, par exemple, liste des événements d'ID séparés par des virgules, par exemple 248, 903, 16384 et ainsi de suite. **Remarque :** Lorsque vous indiquez TOUS, cela implique tous les ID d'événement pour ce canal. Vous pouvez utiliser l'Observateur d'événements Windows afin d'identifier les ID d'événement et le nom du canal à configurer dans l'interface utilisateur. L'exemple suivant indique comment obtenir un ID d'événement et nom de canal avec Windows Powershell. Pour afficher les informations, accédez à Exécuter et saisissez `Event Viewer`, accédez à **Journaux des applications et des services** > **Windows Powershell**. Les ID d'événement et le nom du canal s'affichent dans Journaux des applications et des services de Windows Powershell.

Champ	Description
	
Envoyer un log de test	Envoie un message de log de test. Cette option est activée par défaut. Un message de log de test est envoyé lors d'un nouveau déploiement d'agent ou modification de configuration depuis l'agent vers le Log Decoder. Il contient tous les champs configurés pour l'agent. Ces événements peuvent aider à comprendre la connectivité des agents vers la destination.
Générer l'agent	Génère un packager d'agent. Le fichier de configuration de log est créé dans le fichier **AgentPackager.zip** .
Générer uniquement la configuration de log	Génère le fichier de configuration de log selon les paramètres indiqués ci-dessus ou, s'il est téléchargé, à l'aide de l'option Charger la configuration existante. **Remarque :** Le contenu du fichier de configuration de log généré ne doit pas être falsifié. Si des modifications sont apportées, l'agent ne lit pas les informations à partir du fichier.

Remarque : Vous pouvez activer la fonction Windows Log Collection ultérieurement en téléchargeant et déployant le fichier de configuration de log. Pour plus d'informations, reportez-vous au fichier « Ajouter/Mettre à jour le fichier Windows Log Collection à l'aide de l'agent Endpoint » du *Guide de configuration de Log Collection.*

Générer les programmes d'installation de l'agent Endpoint

Pour générer les programmes d'installation de l'agent Endpoint à déployer sur des hôtes :

Remarque : Utilisez une machine Windows pour exécuter le fichier du packager d'agent.

1. Décompressez le fichier **AgentPackager.zip**. Il inclut les éléments suivants :
   - Dossier **agents** – Contient des exécutables pour Linux, Mac et Windows.
   - Dossier **config** – Contient les certificats et le fichier de configuration requis pour communiquer entre Endpoint Server et l'agent.
   - **AgentPackager.exe**.
2. Exécutez le fichier **AgentPackager.exe**
3. Saisissez le mot de passe utilisé lors de la génération du packager d'agent, puis appuyez sur la touche **Entrée**.
   Cette opération crée les programmes d'installation suivants dans le dossier racine :
   - nwe-agent-package.exe (pour Windows)
   - nwe-agent.pkg (pour Mac)
   - nwe-agent.rpm (pour Linux 32 bits)
   - nwe-agent(64 bits).rpm (pour Linux 64 bits)

Déployer et vérifier des agents Endpoint

Cette section fournit des instructions sur la façon de déployer et de vérifier des agents.

Déploiement d'agent (Windows)

Pour déployer un agent, exécutez le fichier **nwe-agent-package.exe** sur les hôtes que vous souhaitez surveiller.

Vérification des agents Windows

Après avoir déployé les agents Windows, vous pouvez vérifier si un agent Windows est en cours d'exécution en utilisant l'une des méthodes suivantes :

- Utilisation de l'interface utilisateur NetWitness

  La vue Enquêter > Hôtes contient la liste de tous les hôtes dotés d'un agent. Vous pouvez rechercher le nom d'hôte sur lequel l'agent est installé.

  Remarque : Cliquez sur **Enquêter** > **Hôtes** ou appuyez sur F5 pour actualiser la liste et obtenir les données les plus récentes.

- À l'aide du Gestionnaire de tâches

  Ouvrez le Gestionnaire de tâches et recherchez le nom du service que vous avez configuré lors de la génération du packager d'agent.

- À l'aide de Services.msc

  Ouvrez `Services.msc` dans l'exécution et recherchez NWEAgent.

Déploiement d'agent (Linux)

Pour déployer l'agent, exécutez le fichier **nwe-agent.rpm** (pour 32 bits) ou **nwe-agent(64-bit).rpm** (pour 64 bits) sur les hôtes que vous souhaitez surveiller. Utilisez le RPM 32 bits pour i386 et le RPM 64 bits pour les machines x84_64.

Vérification des agents Linux

Après avoir déployé les agents Linux, vous pouvez vérifier si un agent Linux est en cours d'exécution en utilisant l'une des méthodes suivantes :

- Utilisation de l'interface utilisateur NetWitness

  La vue Enquêter > Hôtes contient la liste de tous les hôtes dotés d'un agent.

  Remarque : Cliquez sur **Enquêter > Hôtes** ou appuyez sur F5 pour actualiser la liste et obtenir les données les plus récentes.

- À l'aide de la ligne de commande

  Exécutez la commande suivante pour obtenir le PID :

  ```
  pgrep nwe-agent
  ```

- Pour vérifier la version NetWitness Endpoint, exécutez la commande :

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

Déploiement d'agent (Mac)

Pour déployer un agent, exécutez le fichier **nwe-agent.pkg** sur les hôtes que vous souhaitez surveiller.

Vérification des agents Mac

Après avoir déployé les agents Mac, vous pouvez vérifier si un agent Mac est en cours d'exécution en utilisant l'une des méthodes suivantes :

- Utilisation de l'interface utilisateur NetWitness

  La vue Enquêter > Hôtes contient la liste de tous les hôtes dotés d'un agent.

  Remarque : Cliquez sur **Enquêter > Hôtes** ou appuyez sur F5 pour actualiser la liste et obtenir les données les plus récentes.

- À l'aide de la surveillance de l'activité

  Ouvrez le Moniteur d'activité (/Applications/Utilitaires/Activity Monitor.app) et recherchez NWEAgent.

- À l'aide de la ligne de commande

  Exécutez la commande suivante pour obtenir le PID

  ```
  pgrep NWEAgent
  ```

- Pour vérifier la version de NetWitness Endpoint, exécutez la commande :

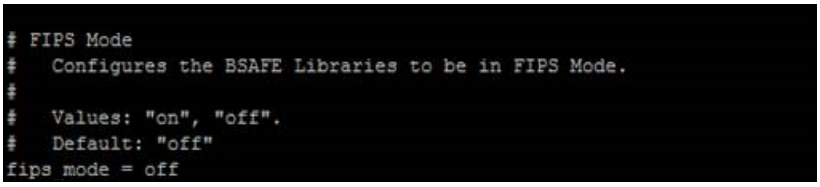
  ```
  grep a /var/log/system.log | grep NWEAgent | grep Version
  ```

Configuration de la communication entre le serveur Endpoint et les agents Endpoint sur Windows Vista, Server 2008, Mac OS X 10.9 et 10.10

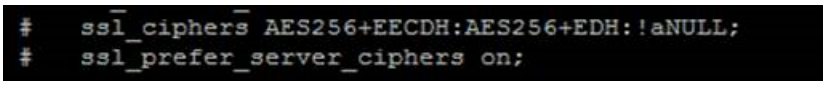
Par défaut, le mode FIPS est activé sur le serveur Endpoint, ce qui signifie que les agents installés sur Windows Vista, Server 2008, Mac OS X 10.9 et 10.10 ne peuvent pas communiquer avec le serveur Endpoint.

Pour résoudre ce problème, effectuez les opérations suivantes sur Endpoint Hybrid ou Endpoint Log Hybrid pour désactiver le mode FIPS :

1. Accédez à `/etc/pki/tls/owb.cnf` et modifiez le fichier pour désactiver le mode FIPS.



2. Accédez à `/etc/nginx/conf.d/nginx.conf` et modifiez le fichier pour commenter les lignes suivantes :



3. Redémarrez le serveur Nginx grâce à la commande suivante :

```
systemctl restart nginx
```

Désinstaller des agents

Cette section fournit les commandes suivantes pour désinstaller l'agent.

Désinstallation d'un agent Windows

Exécutez la commande suivante :

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

Désinstallation d'un agent Linux

Exécutez la commande suivante :

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

Désinstallation d'un agent Mac

Exécutez les commandes suivantes :

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`