RSA NETWITNESS® PLATFORM

# Guía de instalación de agentes de Endpoint Insights

para la versión 11.2

## Información de contacto

RSA Link en https://community.rsa.com contiene una base de conocimientos que responde a las preguntas comunes y brinda soluciones para problemas conocidos, documentación de productos, análisis de la comunidad y administración de casos.

## Marcas comerciales

Para obtener una lista de las marcas comerciales de RSA, visite mexico.emc.com/legal/emc-corporation-trademarks.htm#rsa (visite el sitio web de su país correspondiente).

## Acuerdo de licencia

Este software y la documentación asociada son propiedad e información confidencial de Dell, se suministran bajo licencia, y pueden utilizarse y copiarse solamente de acuerdo con los términos de dicha licencia y con el aviso de copyright mencionado a continuación. No se puede suministrar a ninguna persona, ni poner a su disposición de cualquier otra manera, este software ni la documentación, o cualquier copia de estos elementos.

Este documento no constituye ninguna transferencia de titularidad ni propiedad del software, la documentación o cualquier derecho de propiedad intelectual. Cualquier uso o reproducción sin autorización de este software y de la documentación pueden estar sujetos a responsabilidad civil o penal.

Este software está sujeto a cambios sin aviso y no debe considerarse un compromiso asumido por Dell.

## Licencias de otros fabricantes

Este producto puede incluir software que ha sido desarrollado por otros fabricantes. El texto de los acuerdos de licencia que se aplican al software de otros fabricantes en este producto puede encontrarse en la página de documentación del producto en RSA Link. Al usar este producto, el usuario acepta regirse totalmente por los términos de los acuerdos de licencia.

## Nota sobre tecnologías de cifrado

Es posible que este producto contenga tecnologías de cifrado. Muchos países prohíben o limitan el uso, la importación o la exportación de las tecnologías de cifrado, y las regulaciones actuales de uso, importación y exportación deben cumplirse cuando se use, importe o exporte este producto.

## Distribución

Dell considera que la información de esta publicación es precisa en el momento de su publicación. La información está sujeta a cambios sin previo aviso.

February 2019

# Contenido

# Introducción

**Nota:** La información de esta guía se aplica a la versión 11.1 y superior.

Los hosts pueden ser laptops, estaciones de trabajo, servidores, tabletas, enrutadores o cualquier sistema, físico o virtual, en los cuales esté instalado un sistema operativo compatible. Un agente de Endpoint Insights se puede implementar en un host con un sistema operativo Windows, Mac o Linux. El proceso de instalación implica lo siguiente:

1. Generar un empaquetador de agentes para recopilar únicamente datos de terminales o para recopilar datos de terminales y datos del registro (solo Windows)
2. Generar el instalador de agentes

Puede ejecutar el instalador de agentes específico de un sistema operativo para implementar agentes en los hosts. Los agentes recopilan datos de terminales y registros de Windows (si está habilitado) desde estos hosts. Monitorean las actividades e informan los resultados de los datos y los escaneos a Endpoint Hybrid o Endpoint Log Hybrid a través de HTTPS.

## Sistemas operativos compatibles

### Windows

El software de agente se ejecuta en los siguientes sistemas operativos Windows:

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

### Linux

El software de agente se ejecuta en la arquitectura i386 o x84_64 y en los siguientes sistemas operativos Linux:

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

### Mac

El software de agente se ejecuta en los siguientes sistemas operativos Mac:

- 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)

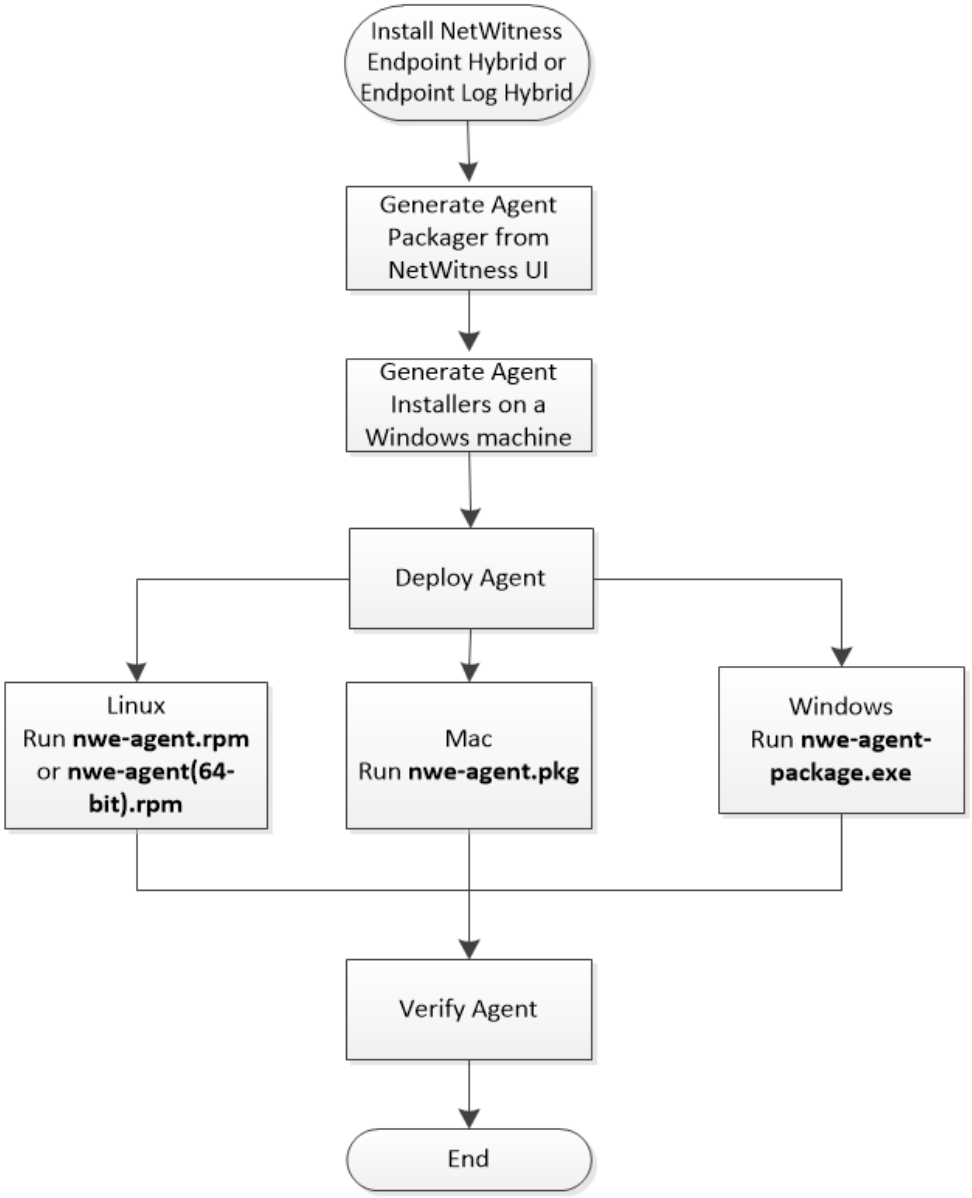
## Requisitos de hardware

Los siguientes son los requisitos mínimos de hardware para implementar un agente:

- 256 MB de RAM
- 100 MB de espacio en disco
- CPU de un core

## Diagrama de flujo de la instalación

En el siguiente diagrama de flujo se ilustra el proceso de instalación de agentes de 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

# Requisitos previos

- Instalar RSA NetWitness Platform. Para obtener más información, consulte la *Guía de instalación de hosts físicos* o la *Guía de instalación de hosts virtuales*.
- Configurar NetWitness Endpoint Hybrid o Endpoint Log Hybrid. Para obtener más información, consulte la *Guía Insights de configuración de Endpoint*.
- Configurar el reenvío de metadatos para los agentes de NetWitness Endpoint 11.1. Para obtener más información, consulte la *Guía Insights de configuración de Endpoint*.

# Generar un empaquetador de agentes de Endpoint

## Generación de un empaquetador de agentes para la recopilación de datos de Endpoint

Para generar un empaquetador de agentes con el fin de recopilar únicamente datos de terminales desde los hosts:

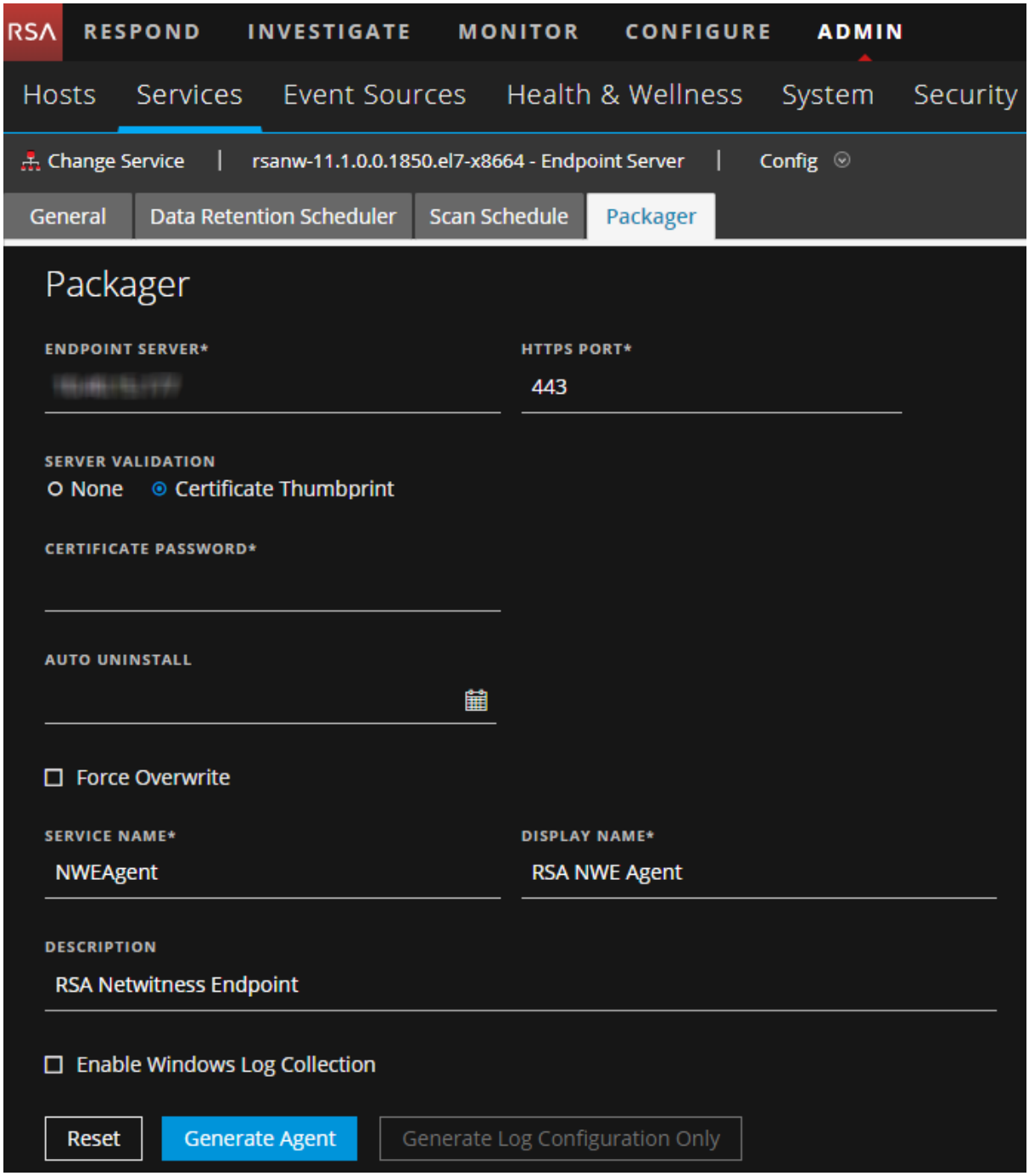
1. Inicie sesión en NetWitness Platform.

   Escriba `https://<NW-Server-IP-Address>/login` en el navegador para ir a la pantalla Inicio de sesión de NetWitness Platform.

2. Haga clic en **ADMINISTRAR > Servicios**.

3. Seleccione el servicio **Servidor de Endpoint** y haga clic en  **> Ver > Configuración >**

**pestaña Empaquetador**. Se muestra la pestaña Empaquetador.



4. Ingrese valores en los siguientes campos:

| Campo | Descripción |
|---|---|
| Servidor de Endpoint | Nombre de host o dirección IP del servidor de Endpoint. Por ejemplo, 10.10.10.3. |
| Puerto HTTPS | Número de puerto. Por ejemplo, 443. |
| Validación del servidor | Determina la manera en que el agente valida el certificado del servidor de Endpoint:<br>• Ninguno: El agente no validará el certificado del servidor.<br>• Huella digital del certificado: Selección predeterminada. El agente identifica el servidor mediante la validación de la huella digital de la CA raíz del certificado del servidor. |
| Contraseña del certificado | Contraseña que se utiliza para descargar el empaquetador. Se utiliza la misma contraseña al generar el instalador de agentes. Por ejemplo, netwitness. |
| Desinstalar automáticamente | Fecha y hora en que el agente se desinstala automáticamente. Puede dejar este campo en blanco si no es necesario. |
| Forzar sobrescritura | Sobrescribe al agente de Windows instalado independientemente de la versión. Si esta opción no se selecciona, el mismo instalador se puede ejecutar varias veces en un sistema, pero el agente se instala solo una vez.<br>Si habilita esta opción, asegúrese de proporcionar el mismo nombre de servicio que el del agente instalado anteriormente durante la creación de un agente nuevo.<br>**Nota:** Si desea forzar la sobrescritura con MSI, ejecute el siguiente comando: `msiexec /fvam <msifilename.msi>` |
| Nombre de servicio | Nombre del agente. Este campo solo se aplica a Windows. Por ejemplo, NWEAgent. |
| Nombre para mostrar | Nombre para mostrar del agente. Este campo solo se aplica a Windows. Por ejemplo, NWE. |
| Descripción | Descripción del agente. Este campo solo se aplica a Windows. Por ejemplo, RSA NetWitness Endpoint. |
| Generar agente | Genera un empaquetador de agentes. |

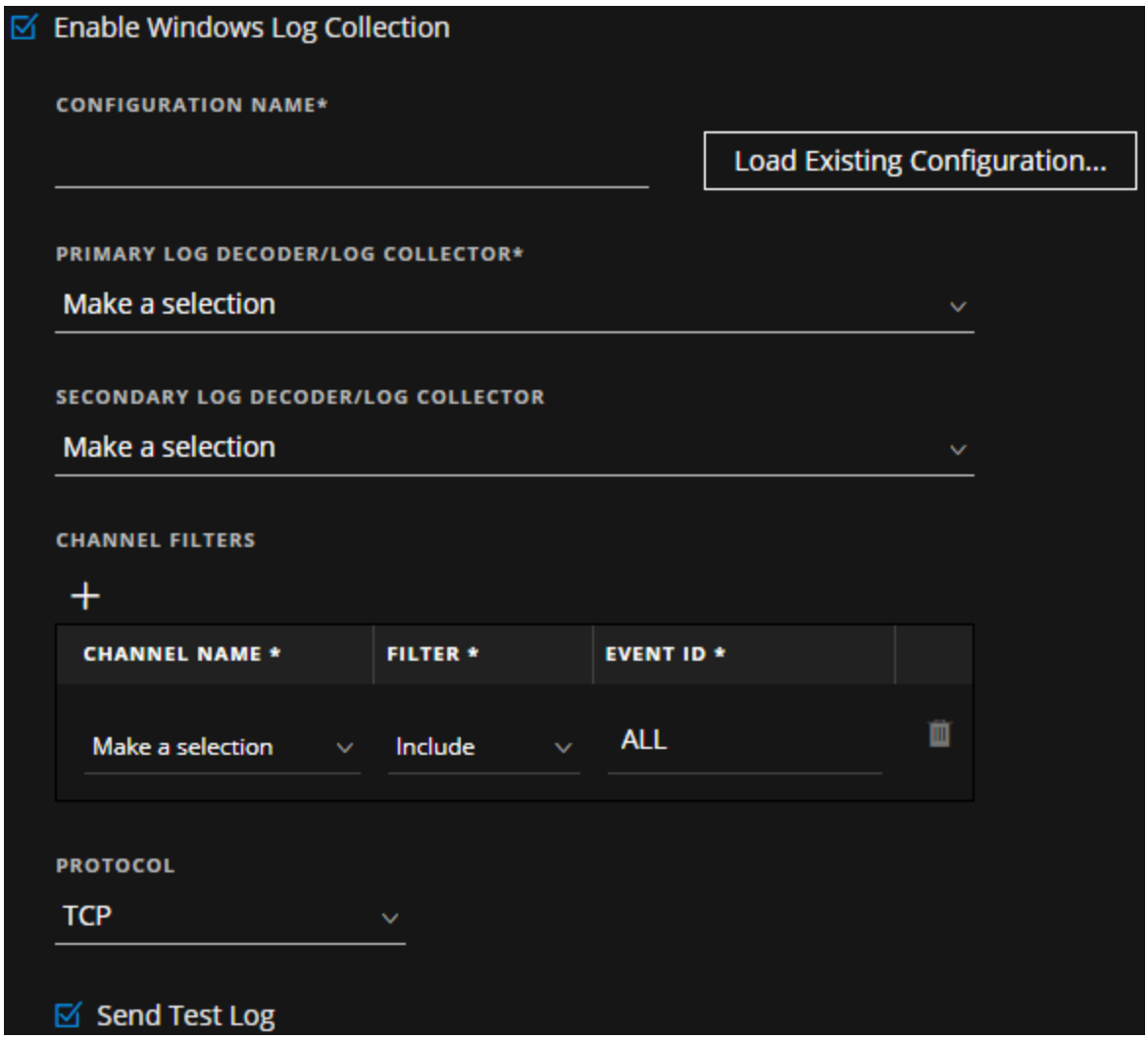
5. Haga clic en **Generar agente**.

   Esto descarga un empaquetador de agentes (**AgentPackager.zip**)en el host en el que accede a la interfaz del usuario de NetWitness Platform.

## Generación de un empaquetador de agentes con la recopilación de registros de Windows

Puede habilitar la función de recopilación de registros de Windows en el agente al generar el empaquetador de agentes. Cuando se habilita esta opción, se genera un archivo de configuración del registro y el agente puede recopilar y reenviar registros de Windows. Para habilitar la recopilación de registros de Windows:

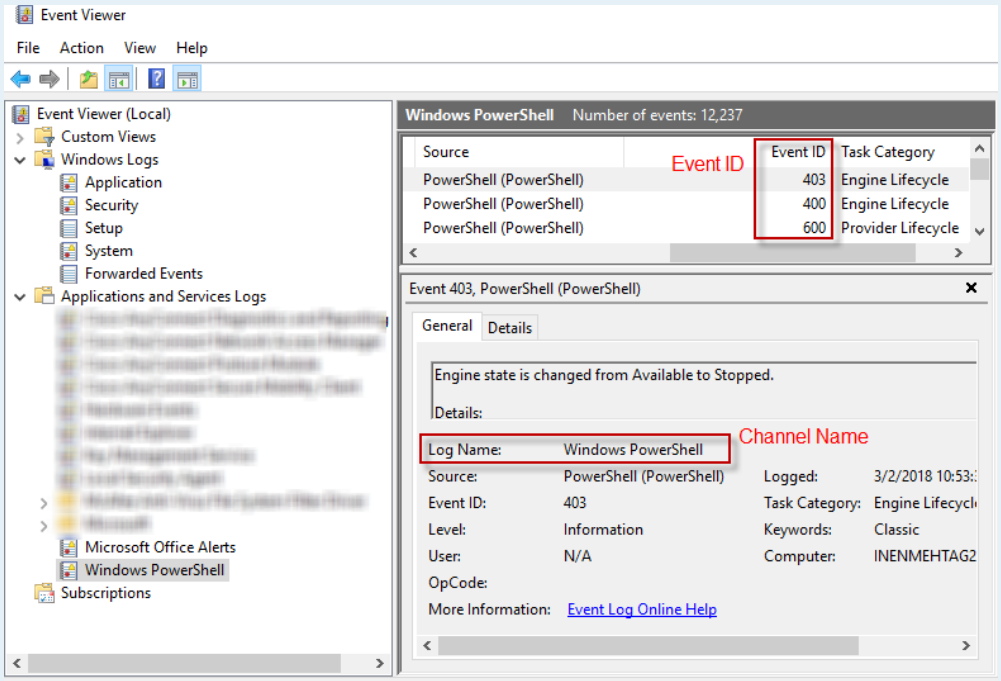
1. Realice los pasos del 1 al 4 que aparecen en Generación de un empaquetador de agentes para la recopilación de datos de Endpoint.
2. Seleccione **Habilitar la recopilación de registros de Windows**.




3. Ingrese o seleccione valores en los siguientes campos:

| Campo | Descripción |
|---|---|
| Nombre de configuración | Nombre de la configuración. El nombre de la configuración puede tener caracteres especiales, valores alfanuméricos, guiones, espacios y guiones bajos. |
| Cargar configuración existente | Carga una configuración existente desde el sistema del usuario. Los campos de recopilación de registros de Windows se completan con la información cuando la carga se realiza correctamente.<br>**Nota:** Si hay algún error o advertencia, se muestran mensajes de advertencia durante la carga. |
| Log Decoder/Log Collector primario | Log Decoder o Log Collector primario para el reenvío de registros. Esto muestra la lista de Log Decoders o Remote Log Collectors en la implementación actual. Este campo es una combinación del nombre para mostrar del servicio, el nombre de host y el tipo de servicio. |
| (Opcional) Log Decoder/Log Collector secundario | Log Decoder o Log Collector secundario para el reenvío de registros. El Log Decoder o el Log Collector secundarios reciben los eventos de Windows si el agente no puede comunicarse con el Log Decoder o el Log Collector primarios.<br>**Nota:** Cuando el agente de Endpoint está configurado para usar el protocolo UDP y el Log Decoder o el Remote Log Collector primarios no están accesibles, el Log Decoder o el Log Collector secundarios no están operativos. Los registros no se reenvían al Log Decoder ni al Log Collector secundarios cuando los primarios no están disponibles y, por lo tanto, se produce una pérdida de eventos. |
| Protocolo | Seleccione el protocolo en el menú desplegable. Las opciones disponibles son UDP, TCP y TLS. De forma predeterminada, el protocolo es TCP. |

| Campo | Descripción |
|---|---|
| Filtros del canal | Canales desde los cuales se recopilan los registros. Puede agregar o quitar un filtro de canal. Debe haber al menos un filtro de canal para recopilar los registros.<br>• **Nombre del canal**: Seleccione el canal en el menú desplegable. Las opciones disponibles son Sistema, Seguridad, Aplicación, Configuración y Eventos reenviados. También puede crear un canal personalizado mediante el ingreso de una ruta del nombre de canal personalizado. Esto se agrega a la lista de nombres de canal. Para buscar canales personalizados, vaya al **Visor de eventos de Windows** en su computadora.<br>• **Filtrar**: Haga clic en  para agregar un filtro de canal. Haga clic en el menú desplegable para incluir o excluir los ID de evento de un canal específico durante la generación del empaquetador de agentes o del archivo de configuración del registro. De forma predeterminada, para la opción Incluir, el ID de evento se configura en **TODO**. Para la opción Excluir, se configura en blanco. Haga clic en  para quitar un filtro de canal.<br>• **ID de evento**: Ingrese los ID de evento de este canal. Estos son específicos de los canales y son los ID que se deben recopilar. Los ID de evento pueden ser tanto numéricos como un rango. Por ejemplo, úselo en un rango, 15-32. Sin embargo, no se permite un rango inverso, por ejemplo, 32-15. Los ID de evento también se pueden usar como combinaciones, por ejemplo, lista de ID de evento separados por comas, como 248, 903, 16384 y así sucesivamente.<br>**Nota:** Cuando ingresa TODO, se consideran todos los ID de evento de ese canal.<br>Puede usar el Visor de eventos de Windows para identificar los ID de evento y el nombre del canal que se configurarán en la interfaz del usuario. En el siguiente ejemplo se muestra la navegación para obtener los ID de evento y el nombre del canal para Windows Powershell. Para ver la información, vaya a Ejecutar, escriba `Event Viewer` y vaya a **Registros de aplicaciones y servicios** > **Windows Powershell**. Se muestran los ID de evento y el nombre del canal en Registros de aplicaciones y servicios para Windows Powershell. |

| Campo | Descripción |
|---|---|
| |  |
| Enviar registro de prueba | Envía un mensaje de registro de prueba. De manera predeterminada, esta opción está activada. Se envía un mensaje de registro de prueba desde el agente al Log Decoder cuando se implementa un nuevo agente o cuando hay un cambio en la configuración. Contiene todos los campos configurados para el agente. Estos eventos pueden ayudar a comprender la conectividad del agente al destino. |
| Generar agente | Genera un empaquetador de agentes. El archivo de configuración del registro se crea en el archivo **AgentPackager.zip** . |
| Generar solo configuración del registro | Genera el archivo de configuración del registro según los parámetros especificados anteriormente o si se cargó mediante la opción Cargar configuración existente.<br>**Nota:** El contenido del archivo de configuración del registro generado no se debe alterar. Si se realizan cambios, el agente no lee la información del archivo. |

**Nota:** Puede habilitar la función de recopilación de registros de Windows más adelante mediante la descarga y la implementación del archivo de configuración del registro. Para obtener más información, consulte “Agregar/actualizar el archivo de recopilación de registros de Windows mediante el agente de Endpoint” en la *Guía de configuración de la recopilación de registros*.

# Generar instaladores de agentes de Endpoint

Para generar instaladores de agentes de Endpoint para implementarlos en los hosts:

**Nota:** Utilice una máquina con Windows para ejecutar el archivo del empaquetador de agentes.

1. Descomprima el archivo **AgentPackager.zip**. Esto incluye lo siguiente:
   - Carpeta **agents**: Contiene los archivos ejecutables para Linux, Mac y Windows.
   - Carpeta **config**: Contiene el archivo de configuración y los certificados necesarios para la comunicación entre el servidor de Endpoint y el agente.
   - **AgentPackager.exe** Archivo .
2. Ejecute el archivo **AgentPackager.exe**.
3. Ingrese la misma contraseña que se usa al generar el empaquetador de agentes y presione **Intro**. Esto crea los siguientes instaladores en la carpeta raíz:
   - nwe-agent-package.exe (para Windows)
   - nwe-agent.pkg (para Mac)
   - nwe-agent.rpm (para Linux de 32 bits)
   - nwe-agent(64-bit).rpm (para Linux de 64 bits)

# Implementar y verificar agentes de Endpoint

En esta sección se proporcionan instrucciones sobre cómo implementar y verificar agentes.

## Implementación de agentes (Windows)

Para implementar el agente, ejecute el archivo **nwe-agent-package.exe** en los hosts que desea monitorear.

### Verificación de agentes de Windows

Después de implementar los agentes de Windows, puede verificar si uno de ellos está en ejecución mediante cualquiera de los siguientes métodos:

- Uso de la interfaz del usuario de NetWitness

  La vista Investigar > Hosts contiene la lista de todos los hosts en los que hay un agente. Puede buscar el nombre de host en el que está instalado el agente.

  **Nota:** Haga clic en **Investigar** > **Hosts** o presione F5 para actualizar la lista y obtener los datos más recientes.

- Uso del Administrador de tareas

  Abra el Administrador de tareas y busque el nombre del servicio que configuró al generar el empaquetador de agentes.

- Uso de Services.msc

  Abra `Services.msc` en Ejecutar y busque NWEAgent.

## Implementación de agentes (Linux)

Para implementar el agente, ejecute el archivo **nwe-agent.rpm** (para 32 bits) o **nwe-agent(64-bit).rpm** (para 64 bits) en los hosts que desea monitorear. Utilice el rpm de 32 bits para máquinas i386 y el rpm de 64 bits para máquinas x84_64.

### Verificación de agentes de Linux

Después de implementar los agentes de Linux, puede verificar si uno de ellos está en ejecución mediante cualquiera de los siguientes métodos:

- Uso de la interfaz del usuario de NetWitness

  La vista Investigar > Hosts contiene la lista de todos los hosts en los que hay un agente.

  **Nota:** Haga clic en **Investigar > Hosts** o presione F5 para actualizar la lista y obtener los datos más recientes.

- Uso de la línea de comandos

  Ejecute el siguiente comando para obtener el PID:

  ```
  pgrep nwe-agent
  ```

- Para comprobar la versión de NetWitness Endpoint, ejecute el siguiente comando:

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

## Implementación de agentes (Mac)

Para implementar el agente, ejecute el archivo **nwe-agent.pkg** en los hosts que desea monitorear.

### Verificación de agentes de Mac

Después de implementar los agentes de Mac, puede verificar si uno de ellos está en ejecución mediante cualquiera de los siguientes métodos:

- Uso de la interfaz del usuario de NetWitness

  La vista Investigar > Hosts contiene la lista de todos los hosts en los que hay un agente.

  **Nota:** Haga clic en **Investigar > Hosts** o presione F5 para actualizar la lista y obtener los datos más recientes.

- Uso del Monitor de actividad

  Abra el Monitor de actividad (/Applications/Utilities/Activity Monitor.app) y busque NWEAgent.

- Uso de la línea de comandos

  Ejecute el siguiente comando para obtener el PID

  ```
  pgrep NWEAgent
  ```

- Para comprobar la versión de NetWitness Endpoint, ejecute el comando:

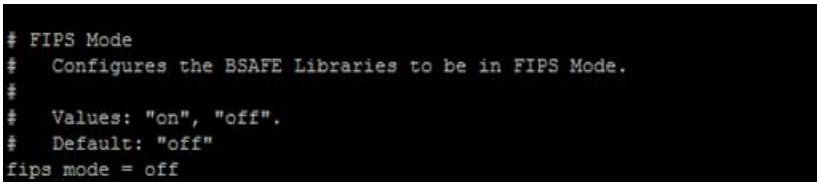
  ```
  grep a /var/log/system.log | grep NWEAgent | grep Version
  ```

### Configuración de la comunicación entre el servidor de Endpoint y agentes de Endpoint en Windows Vista, Server 2008, Mac OS X 10.9 y 10.10

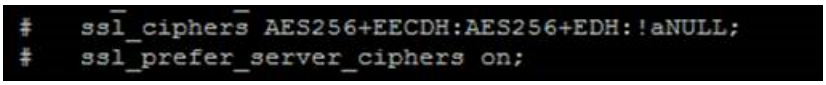
De forma predeterminada, el modo FIPS está activado en el servidor de Endpoint, lo que significa que los agentes instalados en Windows Vista, Server 2008, Mac OS X 10.9 y 10.10 no se pueden comunicar con el servidor de Endpoint.

Para resolver esto, realice los siguientes pasos en Endpoint Hybrid o Endpoint Log Hybrid para deshabilitar el modo FIPS:

1. Vaya a `/etc/pki/tls/owb.cnf` y edite el archivo para deshabilitar el modo FIPS.




2. Vaya a `/etc/nginx/conf.d/nginx.conf` y edite el archivo para dejar las siguientes líneas como comentario:




3. Reinicie el servidor de Nginx mediante el siguiente comando:

   ```
   systemctl restart nginx
   ```

# Desinstalar agentes

Esta sección proporciona los comandos para desinstalar al agente.

## Desinstalación del agente de Windows

Ejecute el siguiente comando:

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

## Desinstalación del agente de Linux

Ejecute el siguiente comando:

```
rpm –ev nwe-agent
```

## Desinstalación del agente de Mac

Ejecute los siguientes comandos:

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`