RSA NETWITNESS® SUITE

Config. recopilación Windows existente

para la versión 11.0

RSA

Marcas comerciales

Acuerdo de licencia

Licencias de otros fabricantes

Nota sobre tecnologías de cifrado

Distribución

Contenido

Instrucciones de actualización e instalación de la recopilación de Windows existente de NetWitness

La recopilación de Windows existente de RSA NetWitness® Suite recopila datos de eventos de múltiples dominios de orígenes de eventos de Windows.

Es compatible con la recopilación desde:

- Orígenes de eventos de Windows 2003 y versiones anteriores
- Archivos evt del host ONTAP de NetApp

El documento incluye las siguientes secciones:

Requisitos de configuración

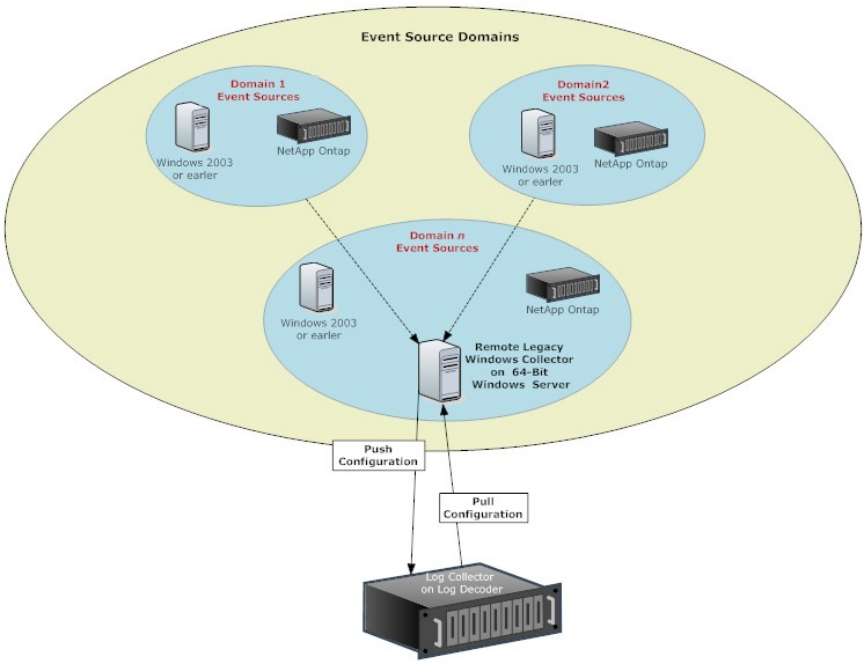
En esta sección se proporcionan los requisitos de configuración del recopilador de Windows existente de RSA NetWitness® Suite.

Precaución: Si va a instalar o actualizar a la versión 11.0, para utilizar el recopilador de Windows existente de Security Analytics con NetWitness, primero debe instalar la actualización KB2999226 de Windows. Si esa actualización no está instalada, recibirá un mensaje de error y el recopilador de Windows existente no se instalará.

Para configurar el recopilador de Windows existente de RSA NetWitness® Suite, necesita:

- Cualquier servidor físico o virtual Windows 2008 R2 SP1 de 64 bits que pueda comunicarse con los dominios del origen de eventos de Windows 2003.
- 20 % como mínimo de espacio libre en disco. Por ejemplo, necesita por lo menos 20 GB de espacio libre si la unidad del sistema tiene un tamaño de 100 GB.

Nota: La instalación del colector de Windows heredado en una controladora de dominio puede afectar el rendimiento del sistema.



Actualizar el recopilador de Windows existente de RSA NetWitness® Suite de 10.6.x a 11.0

En esta sección se indica cómo actualizar el recopilador de Windows existente de Suite RSA NetWitness 10.6.x a 11.

Para actualizar el recopilador de Windows existente de RSA NetWitness® Suite 10.6.x a 11 en un servidor Windows 2008 R2 SP1 de 64 bits:

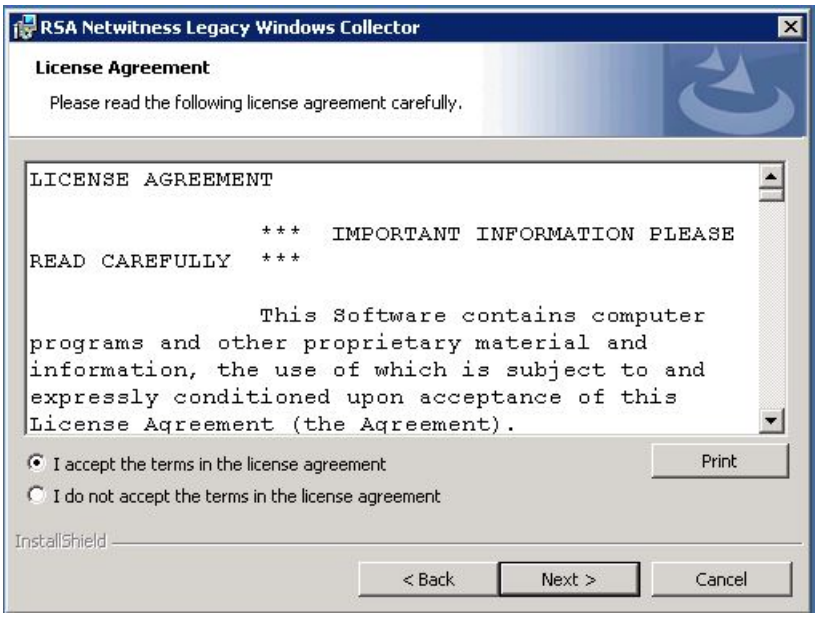
1. Navegue a https://community.rsa.com/docs/DOC-44986 en RSA Link. Haga clic para descargar **SA-11.0.0.0-LegacyWindowsCollector.zip** y descomprima el archivo.
2. Inicie sesión en una máquina Windows 2008.
3. Copie el archivo **WindowsCollector-version-number.exe** al servidor de Windows 2008.
4. Haga clic con el botón secundario en **WindowsCollector-version-number.exe** y seleccione **Ejecutar como administrador**.

   Se muestra la página Preparando la instalación… del Asistente para instalación de actualizaciones.

   Una vez que el programa de instalación de la actualización extrae los archivos de instalación del recopilador de Windows existente de RSA NetWitness® Suite, se muestra la página **Bienvenido**.

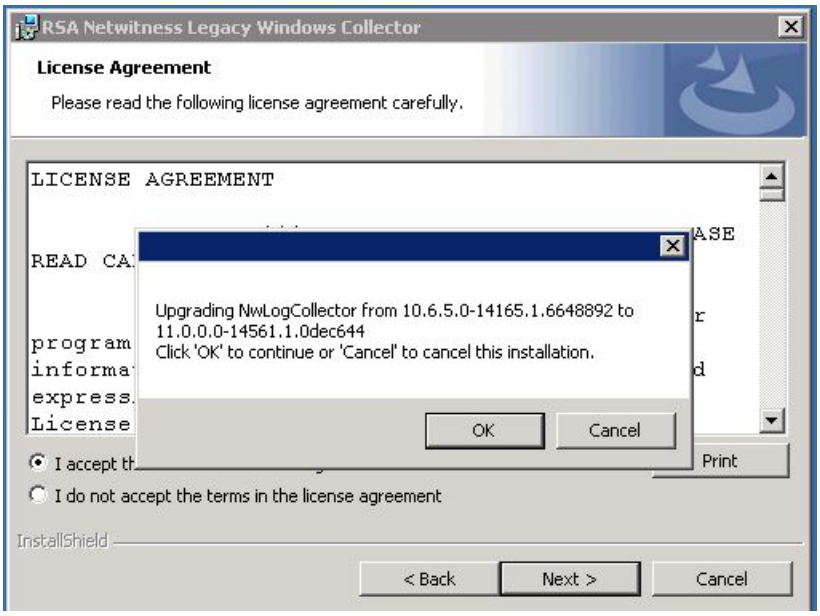
5. Haga clic en **Siguiente**.

   Se muestra la página Acuerdo de licencia.



6. Lea detenidamente el acuerdo de licencia, seleccione el botón de opción **Acepto los términos del acuerdo de licencia** y haga clic en **Siguiente**.

   Antes de comenzar con la actualización, el asistente pregunta si desea continuar con la instalación de la actualización o cancelarla.



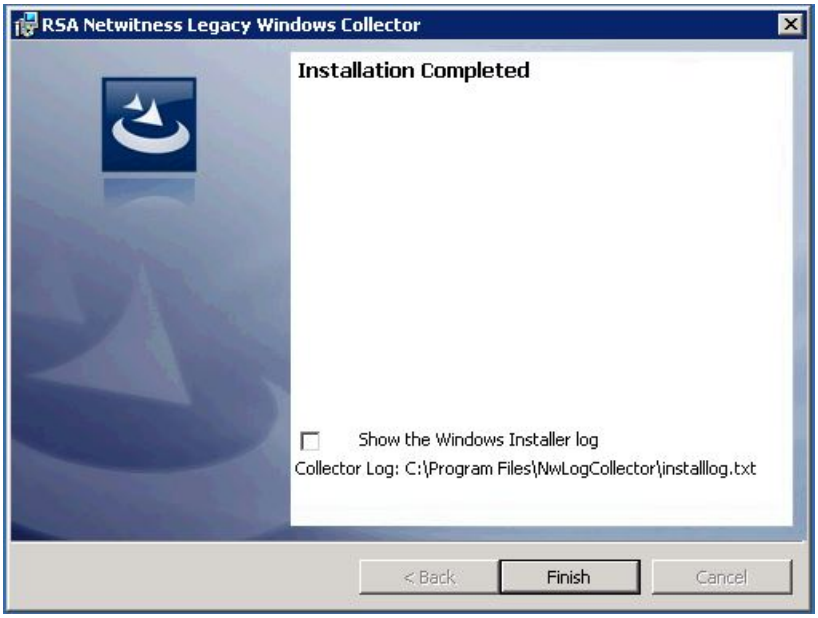
7. Haga clic en **Aceptar** para continuar instalando la actualización.
8. Haga clic en Instalar.

   Se muestran las pantallas de instalación de la página del recopilador de Windows existente.

Cuando se completa la instalación de la actualización, se habilita el botón **Siguiente**.

9. Haga clic en **Siguiente**.

   Se muestra la página Instalación completada.



11. (Opcional) Si desea revisar un registro de la instalación de la actualización, seleccione la casilla de verificación **Mostrar el registro del instalador de Windows**.
12. Haga clic en **Finalizar**.
13. Reinicie la máquina.

Esto pone fin a la actualización del recopilador de Windows existente a Suite RSA NetWitness 11.0.

Instalación nueva del recopilador de Windows existente de la versión 11.0

En esta sección se describe cómo instalar el recopilador de Windows existente 11.0 en un servidor Windows 2008 R2 SP1 de 64 bits.

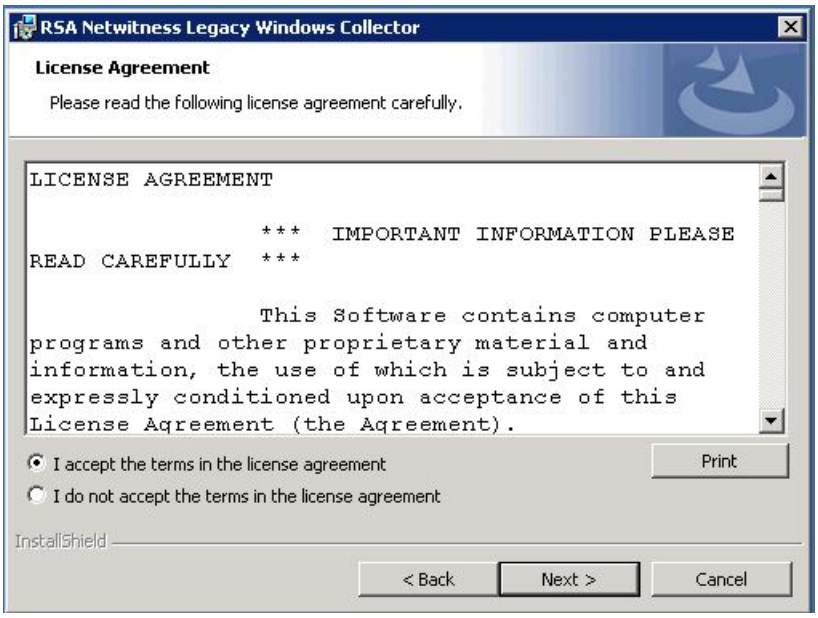
Para instalar el recopilador de Windows existente de Suite RSA NetWitness en un servidor Windows 2008 R2 SP1 de 64 bits:

1. Navegue a https://community.rsa.com/docs/DOC-44986 en RSA Link. Haga clic para descargar **SA-11.0.0.0-LegacyWindowsCollector.zip** y descomprima el archivo.
2. Copie el archivo **SALegacyWindowsCollector-version-number.exe** al servidor de Windows 2008.
3. Haga clic con el botón secundario en **SALegacyWindowsCollector-version-number.exe** y seleccione **Ejecutar como administrador**.

   Se muestra la página **Bienvenido** del asistente para la instalación.

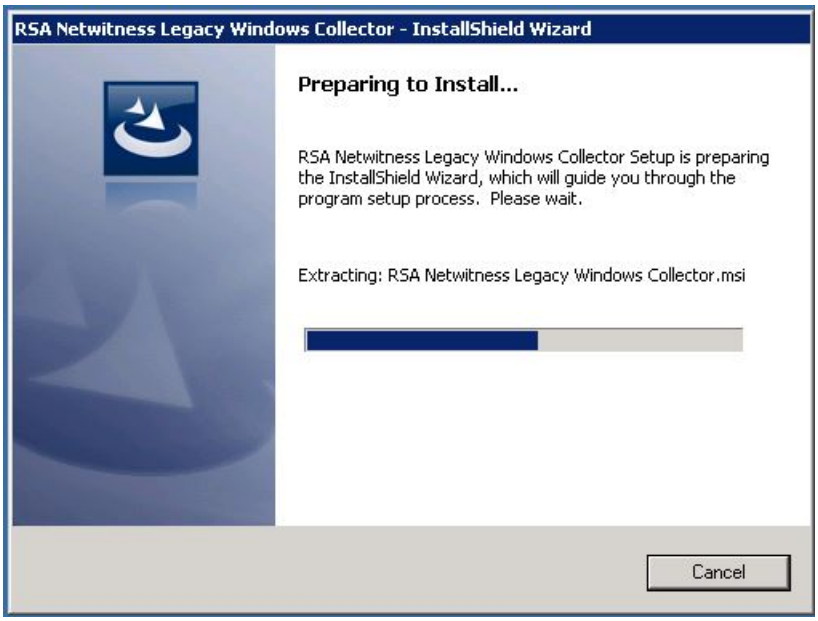
4. Haga clic en **Siguiente**.

   Se muestra la página Acuerdo de licencia.



5. Lea detenidamente el acuerdo de licencia, seleccione el botón de opción **Acepto los términos del acuerdo de licencia** y haga clic en **Siguiente**.

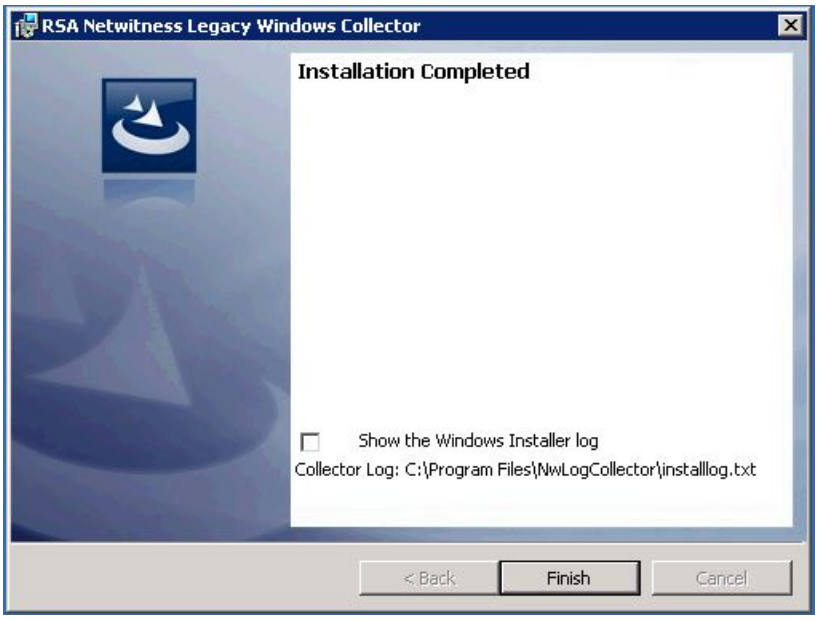
   Se muestra la página Preparado para instalar el programa.



6. Haga clic en **Instalar**.

   Se muestran las pantallas de instalación de la página del recopilador de Windows existente.

Se muestra la página Instalación completada.



7. (Opcional) Si desea revisar un registro de la instalación, seleccione la casilla de verificación **Mostrar el registro del instalador de Windows**.
8. Haga clic en **Finalizar**.
9. Reinicie la máquina.

Esto pone fin a la instalación del recopilador de Windows existente de 11.0. Consulte la **Guía de configuración de la recopilación de Windows existente y NetApp** en RSA Link para obtener instrucciones sobre cómo configurar la recopilación de Windows existente en Suite RSA NetWitness.

Solución de problemas de la instalación nueva o la actualización

Consulte los siguientes archivos de registro si necesita solucionar problemas:

- `%systemDrive%\Netwitness\ng\logcollector\MessageBroker.log`
- `%systemDrive%\Program Files\NwLogCollector\installlog.txt`

Ejecute `C:\Program Files\NwLogCollector\ziplogfiles.vbs` para generar el archivo ***hostname***`_WLCversion_timestamp.zip` que contiene todos los archivos de registro y otra información necesaria para la solución de problemas.

(Opcional) Respaldar y restaurar el recopilador de Windows existente

En esta sección se indica cómo respaldar y restaurar el recopilador de Windows existente.

Nota: Solo debe hacer esto si va a cambiar la VM de Windows donde ejecuta el recopilador de Windows existente.

Para la versión 10.6.4

Para la versión 10.6.4 del recopilador de Windows existente de Suite RSA NetWitness, se proporcionan scripts manuales para realizar el respaldo y la instalación:

- WLC-Backup.bat
- WLC-Restore.bat

Estos archivos están disponibles para su descarga en la siguiente ubicación de RSA Link: https://community.rsa.com/docs/DOC-71397.

Respaldo

Para respaldar el recopilador de Windows existente:

1. Descargue los scripts de respaldo y restauración desde RSA Link al recopilador de Windows existente.
2. En el recopilador de Windows existente, abra una ventana del símbolo del sistema y navegue a la carpeta donde guardó los scripts.
3. Ejecute el comando para crear un respaldo:
   - Archivos de configuración de respaldo: `WLC-Backup.bat config`
   - Archivos de hora de ejecución de respaldo: `WLC-Backup.bat runtime`

   Nota: Respalde únicamente los archivos de hora de ejecución si ya inició la recopilación.

   Las carpetas de respaldo se crean en **C:\Archivos de programa\NwLogCollector**.

   Los nombres de archivo son los siguientes:

   - Config-bkup_***timestamp***.zip
   - Runtime-bkup_***timestamp***.zip

Restauración

Para restaurar un respaldo creado anteriormente para el recopilador de Windows existente:

1. En el recopilador de Windows existente, abra una ventana del símbolo del sistema y navegue a la carpeta donde guardó los scripts.
2. Ejecute el siguiente comando para restaurar un respaldo:
   - Archivos de configuración de respaldo: `WLC-Restore.bat "Config-bkup_`***`timestamp`***`.zip"`
   - Archivos de hora de ejecución de respaldo: `WLC-Restore.bat "Runtime-bkup_`***`timestamp`***`.zip"`
3. Una vez que finalice la restauración, configure la SSV de Lockbox para usar la contraseña que creó durante la configuración de 10.6.4.
   a. En el menú de **Security Analytics**, seleccione **Servicios**, seleccione el recopilador de Windows existente y elija **Explorar**.
   b. En el panel de navegación izquierdo, expanda **logcollection > properties > crypto**.
   c. Ejecute el siguiente comando: `op=setssv pw=`***`password_for_10.6.x_lockbox`*** y presione **Enviar**.

Para actualizar de 10.6.4 a NetWitness 11

Durante la actualización a Suite RSA NetWitness 11, el script de respaldo del recopilador de Windows existente se invoca automáticamente y crea los respaldos de configuración y hora de ejecución de 10.6.4. Una vez que finalice la instalación de 11.0, ejecute el script de restauración para restaurar los archivos de configuración y hora de ejecución para la recopilación de Windows existente actualizada.

Restaurar el respaldo de la recopilación de Windows existente después de la actualización

Para restaurar la configuración de la recopilación de Windows existente en una plataforma Suite RSA NetWitness 11 recién actualizada:

1. En el recopilador de Windows existente, abra una ventana del símbolo del sistema.
2. Navegue a **C:\Archivos de programa\NwLogCollector**, donde se almacenan los scripts.
3. Ejecute los siguientes comandos para restaurar un respaldo:

- Archivos de configuración de respaldo: `WLC-Restore.bat "Config-bkup_timestamp.zip"`
- Archivos de hora de ejecución de respaldo: `WLC-Restore.bat "Runtime-bkup_timestamp.zip"`

4. Una vez que finalice la restauración, configure la SSV de Lockbox para usar la contraseña que creó durante la configuración de 10.6.4.
   a. En el menú de **Security Analytics**, seleccione **Servicios**, seleccione el recopilador de Windows existente y elija **Explorar**.
   b. En el panel de navegación izquierdo, expanda **logcollection > properties > crypto**.
   c. Ejecute el siguiente comando: `op=setssv pw=password_for_10.6.x_lockbox` y presione **Enviar**.

Revertir la recopilación de Windows existente de 11.0 a 10.6.4

Para revertir la configuración de la recopilación de Windows existente de 11.0 a 10.6.4:

1. Desinstale la configuración de 11.0. Tome nota de la ubicación de la carpeta de respaldo que creó el sistema durante el procedimiento de desinstalación.
2. Instale la versión 10.6.4 del recopilador de Windows existente.
3. Navegue a **C:\Archivos de programa\NwLogCollector**, donde se almacenan los scripts.
4. Ejecute el script de restauración desde la carpeta de respaldo presente en **C:\Archivos de programa\NwLogCollector** para restaurar los archivos de configuración y hora de ejecución en el recopilador de Windows existente 10.6.4.
   - Archivos de configuración de respaldo: `WLC-Restore.bat "Config-bkup_timestamp.zip"`
   - Archivos de hora de ejecución de respaldo: `WLC-Restore.bat "Runtime-bkup_timestamp.zip"`
5. Una vez que finalice la restauración, configure la SSV de Lockbox para usar la contraseña que creó durante la configuración de 10.6.4.
   a. En el menú de **Security Analytics**, seleccione **Servicios**, seleccione el recopilador de Windows existente y elija **Explorar**.
   b. En el panel de navegación izquierdo, expanda **logcollection > properties > crypto**.
   c. Ejecute el siguiente comando: `op=setssv pw=password_for_10.6.x_lockbox` y presione **Enviar**.

Agregar un host y un servicio del recopilador de Windows existente en RSA NetWitness® Suite

Para esta versión del recopilador de Windows existente, RSA proporcionó un script que reemplaza los pasos manuales de adición de un host y un servicio del recopilador de Windows existente en la interfaz del usuario de NetWitness.

Para crear un host y un servicio del recopilador de Windows existente en NetWitness:

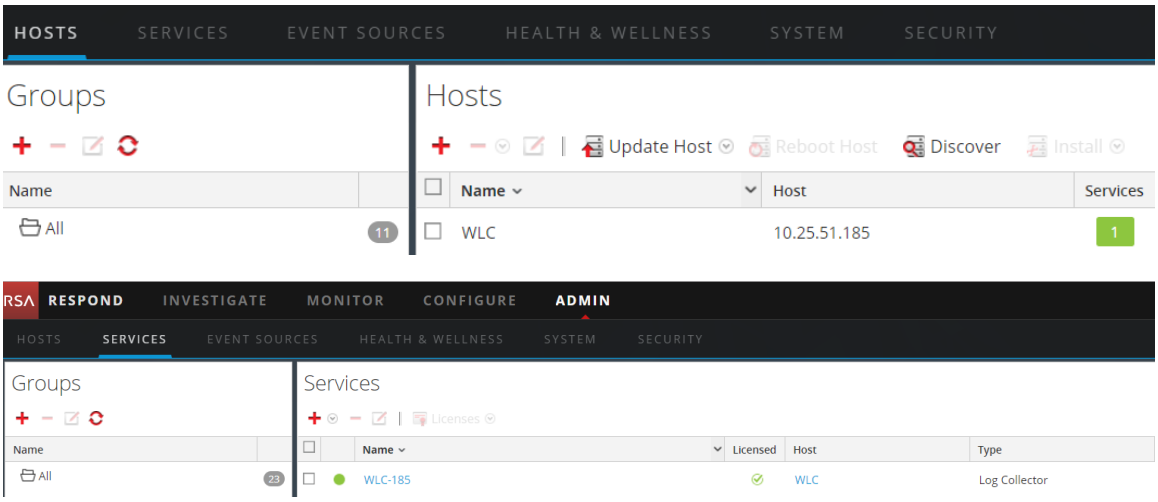
1. Acceda mediante el protocolo SSH al servidor de NetWitness.
2. Ejecute el siguiente comando:

   ```
   wlc-cli-client --host-display-name hostDisplayName --service-display-name serviceDisplayName --host WLChostIPAddress --port 50101 --use-ssl false
   ```

   Los parámetros se explican a continuación:

   - **--host-display-name**: El nombre del host como se muestra en la página Hosts de NetWitness.
   - ***--service-display-name***: El nombre del host como se muestra en la página Servicios de NetWitness.
   - **--host**: La dirección IP del recopilador de Windows existente.
   - **--port**: El puerto que usa NetWitness para comunicarse con el recopilador de Windows existente. El valor recomendado es 50101.
3. Se le solicitará que proporcione la siguiente información:
   - **Nombre de usuario de REST de Log Collector de Windows** y **Contraseña de REST de Log Collector de Windows**: Debe proporcionar credenciales de administrador para el recopilador de Windows existente.
   - **Nombre de usuario del servidor de seguridad** y **Contraseña del servidor de seguridad**: Debe proporcionar credenciales de administrador para RSA NetWitness Suite.

Cuando complete este procedimiento, debería ver el host y el servicio del recopilador de Windows existente, como se muestra en las siguientes capturas de pantalla.


HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Groups
Name
All
11
Hosts
Update Host
Reboot Host
Discover
Install
Name
Host
Services
WLC
10.25.51.185
1
RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Groups
Name
All
23
Services
Licenses
Name
Licensed
Host
Type
WLC-185
WLC
Log Collector