RSA NETWITNESS® PLATFORM

Guía del usuario de la herramienta de recuperación

para la versión 11.2

Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

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.

febrero 2019

Contenido

Recuperación ante desastres (instrucciones de respaldo y restauración) 4

Uso básico de la herramienta de recuperación de NetWitness 5

Condiciones requeridas 6

Flujo de trabajo de recuperación ante desastres 7

Respaldar y restaurar datos para hosts 11.x 7

Respaldar y restaurar datos en NetWitness Server 11.x 8

Respaldar datos en un host de NetWitness Server 8

Restaurar datos en un host de NetWitness Server 9

Respaldar y restaurar datos en otros hosts de componentes 11

Respaldar datos en un host de componentes 11

Restaurar datos en un host de componentes 12

Solamente actualización de hardware: Usar espacio adicional en nuevos hosts de hardware 14

Recuperación ante desastres en una implementación de Azure 15

Tarea 1: Respaldar y exportar datos 15

Tarea 2: Restaurar e importar datos 15

Recuperación ante desastres en una implementación de AWS 17

Tarea 1: Respaldar y exportar datos 17

Tarea 2: Restaurar e importar datos 17

Recuperación ante desastres (instrucciones de respaldo y restauración)

Puede utilizar la herramienta de recuperación de NetWitness (NRT) para respaldar y restaurar datos desde los sistemas host de NetWitness Server y de componentes. La NRT es un script que se ejecuta desde la línea de comandos para respaldar y restaurar datos en hosts con fines de RMA, actualizaciones de hardware y requisitos generales de respaldo y restauración. Consulte Recuperación ante desastres en una implementación de Azure para conocer los pasos específicos de la realización de una recuperación ante desastres para los hosts implementados en VM de Azure.

Nota: Debe ejecutar la NRT en cada sistema host localmente. No puede ejecutarla desde hosts remotos ni desde un host externo.

Los siguientes tipos de hosts se pueden respaldar y restaurar.

Nota: En el script de la NRT, los siguientes términos en negrita se mencionan como categorías.

- **Servidor de NetWitness Admin** (puede incluir Respond, Estado y condición, y Reporting Engine)
- **Malware** Malware Analysis (independiente)
- **Archiver** Log Archiver
- **Broker** Broker independiente
- **Concentrator** Red o registro
- **Decoder** Network Decoder
- **Endpoint Hybrid**
- **Endpoint Log Hybrid**
- **Event Stream Analysis (ESA) primario** Incluida la base de datos de Context Hub e Incident Management
- **ESA secundario**
- **Gateway** Cloud Gateway
- **Log Collector** Incluido Virtual Log Collector, si está instalado
- **Log Decoder** Incluidos Local Log Collector y Warehouse Connector, si están instalados
- **Log Hybrid**
- **Network Hybrid**
- **UEBA** User and Entity Behavior Analytics
- **Warehouse**

Uso básico de la herramienta de recuperación de NetWitness

Puede utilizar la NRT para respaldar datos mediante la opción `export`. Para restaurar datos, utilice la opción `import`. El uso básico de la herramienta es la ejecución del siguiente comando desde el nivel de directorio raíz:

```
nw-recovery-tool [command] [option]
```

Los comandos y las opciones que puede utilizar con esta herramienta se describen en las siguientes tablas.

Comandos y opciones	Descripción
`-h, --help`	Mostrar ayuda sobre los comandos y las opciones. Por ejemplo, especifique: `nw-recovery-tool --help-categories` para obtener una lista de todos los nombres de categoría válidos.
`-e, --export`	Exportar datos o configuración.
`-i, --import`	Importar datos o configuración.
`-d, --dump-dir <path>`	Ruta donde se exportarán o se importarán los datos (por ejemplo, `/var/netwitness/backup`).
`-C, --category <name>`	Seleccione componentes por categoría. Los nombres de categoría válidos son `AdminServer`, `Archiver`, `Broker`, `Concentrator`, `Decoder`, `EndpointHybrid`, `EndpointLogHybrid`, `ESAPrimary`, `ESASecondary`, `Gateway`, `LogCollector`, `LogDecoder`, `LogHybrid`, `Malware`, `NetworkHybrid`, `UEBA` y `Warehouse`. Puede especificar una o varias categorías. Por ejemplo: `--category AdminServer` exclusivamente para el servidor de Admin. `--category AdminServer --category Gateway` para el servidor de Admin y Cloud Gateway.
`-p, --deploy-password <pwd>`	Especifique la contraseña de la implementación. Esto es necesario únicamente si la categoría o el componente seleccionados incluyen Mongo (para hosts como AdminServer, Endpoint o ESA primario).

Condiciones requeridas

Asegúrese de que se cumplan las siguientes condiciones:

- Lea todo el documento antes de respaldar datos. El documento explica todos los escenarios de implementación, razón por la cual es útil asegurarse de contar con toda la información necesaria para respaldar y restaurar la implementación de NetWitness Platform antes de realizar este proceso.
- Ejecute la NRT para realizar tareas de respaldo y recuperación localmente en cada sistema que se respalda o se restaura. No puede ejecutar la NRT en un host externo ni respaldar o restaurar varios hosts simultáneamente. Sin embargo, puede respaldar varios componentes en el mismo sistema host de manera simultánea.
- Exporte e importe los datos en el mismo host. Si un host falla y se necesita crear un nuevo sistema, este debe tener los mismos parámetros de identidad (es decir, la misma dirección IP) y estar en la misma versión de NetWitness Suite.
- Asegúrese que haya espacio en disco suficiente en la ubicación de respaldo (`/var/netwitness/backup` es el directorio recomendado) antes de que se ejecute el comando de exportación en la herramienta nw-recovery. No utilice un directorio `tmp` porque se llena rápidamente y puede causar una falla general en el sistema.
- Compruebe el dimensionamiento de los discos de Malware y ajústelos antes de respaldarlos. En la siguiente tabla se muestra el tamaño máximo de las bases de datos de Malware que puede respaldar por tipo de hardware con las acciones que puede realizar para reducirlos al tamaño máximo.

Host	Hardware de origen	Hardware de destino	Base de datos	Tamaño máximo para respaldo	Acciones para reducir el tamaño al máximo de respaldo
Malware	Hybrid serie 4S	Core serie 6	`/var/netwitness`	2.5 TB	Configurar una transferencia. Depurar los datos que no necesita de la base de datos.

- Restaure a la imagen ISO exacta que tenía cada host en el momento del respaldo.
- Si tiene varios servicios colocalizados en un único host, incluya todos ellos en una sola cadena de comandos para los comandos `import` y `export` en la herramienta nw-recovery.

Nota: 1.) Cuando ejecuta la NRT, los servicios Malware, Reporting Engine y Postgresql se detienen y se reinician durante los procesos de respaldo (exportación) y restauración (importación). La recopilación de registros y paquetes no se detiene.

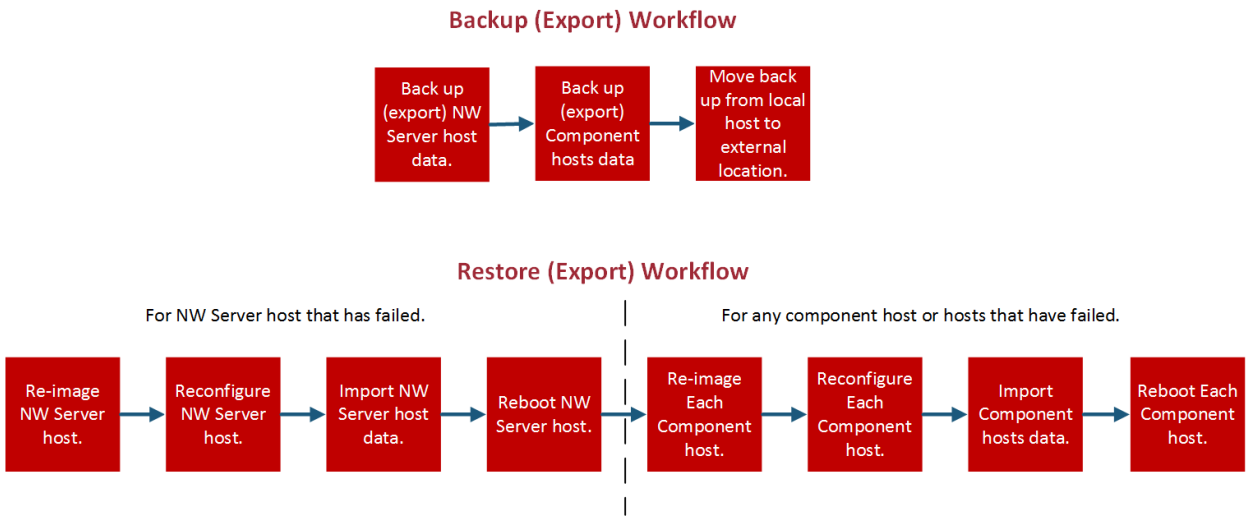
Flujo de trabajo de recuperación ante desastres

En el siguiente diagrama se muestran las tareas generales de recuperación ante desastres.

Nota: Solamente debe recuperar un host si falló. Esto significa que puede recuperar un único host o cualquier combinación de ellos en función del host o de los hosts que fallaron.

En el siguiente diagrama se muestran las tareas para lo siguiente:

- Respaldo (realícelo lo antes posible y con la mayor frecuencia posible).
- Restauración (se requiere únicamente si necesita restaurar sus datos).



Respaldar y restaurar datos para hosts 11.x

Los procedimientos para respaldar y restaurar datos son diferentes para los sistemas host de NetWitness Server y para los sistemas de componentes.

Precaución: 1.) No quite hosts de componentes (es decir, cualquier host que no sea el host del servidor de NW) en la vista Hosts (Administrar > Hosts) de la interfaz del usuario cuando realice el siguiente procedimiento de recuperación ante desastres. 2.) Debe conservar (restaurar) el “nombre de host” que existía antes de realizar el procedimiento de recuperación ante desastres. 3.) Asegúrese de registrar la contraseña maestra y guardarla en una ubicación segura de modo que pueda acceder al sistema en caso de una recuperación ante desastres.

Respaldar y restaurar datos en NetWitness Server 11.x

Nota: Si utiliza almacenamiento compartido para exportar datos de varios hosts (por ejemplo, una unidad o un montaje compartidos), utilice subcarpetas específicas de los hosts como ruta a la ubicación de los archivos exportados de cada host, con el fin de evitar sobrescribir los datos exportados de un host con los de otro. Por ejemplo, podría utilizar una ruta similar a `--dump-dir /mnt/storage/<host-specific-name>` como ruta a la ubicación de los archivos exportados.

Respaldar datos en un host de NetWitness Server

Realice este procedimiento en un sistema host de NetWitness Server 11.x funcional existente.

1. En el nivel raíz, escriba el siguiente comando:

   ```
   nw-recovery-tool --export --dump-dir /var/netwitness/backup --category
   AdminServer
   ```

   Nota: Si un servicio (por ejemplo, Cloud Gateway) está colocalizado en el servidor de NW con el servidor de Admin en lugar de estar en su propio host exclusivo, debe incluirlo en la cadena de comandos. Por ejemplo, `nw-recovery-tool--export --dump-dir /var/netwitness/backup --category AdminServer --category Gateway.`

2. Reemplace `/var/netwitness/backup` por la ruta a la ubicación donde se deben exportar los datos.

   a. Asegúrese de que esta ubicación tenga espacio suficiente para almacenar los datos de respaldo.

   b. La ruta del directorio de respaldo debe estar en el host local. Sin embargo, los archivos de respaldo podrían estar en un montaje de red o en un dispositivo externo.

3. Cuando se le solicite la contraseña de administración de la implementación, escriba la contraseña o incluya el siguiente argumento adicional para el comando `nw-recovery-tool`:

   `--deploy-password <password>`

   Nota: Utilice la contraseña de `deploy_admin` existente que se utilizó en la instalación inicial del host.

   Los datos se respaldan en el host de NetWitness Server en la ubicación que configuró en el paso 2.

4. Transfiera los datos respaldados del host local a un servidor externo o a una memoria USB.

Restaurar datos en un host de NetWitness Server

1. Vuelva a crear la imagen del host de NetWitness Server utilizando los mismos ajustes de configuración de red que los del host original. Para obtener información sobre la creación de una nueva imagen del host de NetWitness Server, consulte "Tarea 1: Instalar 11.2 en el host de NetWitness Server" en la *Guía de instalación de hosts físicos para la versión 11.2*.

   a. **Opcional** Si necesita establecer conectividad de red antes de poder obtener datos de respaldo, por ejemplo, si están en un host remoto, ejecute el siguiente script utilizando los mismos ajustes de dirección IP, subred, puerta de enlace, DNS e información de domino que los del host original:

   ```
   netconfig --static --interface <name> --ip <address> --netmask <netmask>
   --gateway <gateway>
   ```

   Por ejemplo:

   ```
   netconfig --static --interface eth0 --ip 192.168.1.100 --netmask
   255.255.255.0 --gateway 192.168.1.1
   ```

   Opcional: Para especificar servidores DNS, incluya el siguiente parámetro adicional:

   ```
   --dns <address>
   ```

   Opcional: Para establecer el nombre de dominio local, incluya el siguiente parámetro adicional:

   ```
   --domain <name>
   ```

   b. (**Opcional**) Si utiliza DHCP, ejecute el siguiente script:

   ```
   netconfig --dhcp --interface <name>
   ```

   Por ejemplo:

   ```
   netconfig --dhcp --interface eth0
   ```

   c. Agregue los datos de respaldo a la ruta del directorio de respaldo en el host local; por ejemplo:

   ```
   /var/netwitness/backup
   ```

2. Ejecute el comando `nwsetup-tui`. Esto inicia el programa de instalación.

   > **Nota:** Durante el programa de instalación, cuando se le solicite la configuración de red del host, asegúrese de especificar la misma configuración de red que se utilizó para la instalación original de 11.x en este host.

3. Cuando se le solicite, seleccione la opción de tipo de instalación **3: Recuperar (reinstalar)**, haga clic en **Aceptar** y, a continuación, ingrese la ruta al directorio de respaldo que contiene los datos de respaldo.

4. Cuando la instalación se complete correctamente, asegúrese de que la versión y el parche que se ejecutan en el host sean exactamente los mismos que los de los datos que se respaldaron:

   - Si los datos estaban en un sistema 11.x que se actualizó a una versión de parche superior, actualice el host de acuerdo con las instrucciones para actualizar sistemas offline que aparecen en la guía de actualización para la misma versión de parche que estaba en ejecución en el host (la versión y el parche exactos para los que se respaldaron los datos).
   - Si los datos estaban en una versión principal (por ejemplo, 11.x) que no se había actualizado a una versión de parche superior, no es necesario actualizar el sistema host.

5. Cuando el host se esté ejecutando en la versión correcta, ejecute el siguiente comando en

NetWitness Server para restaurar los datos:

```
nw-recovery-tool --import --dump-dir /var/netwitness/backup --category
AdminServer
```

Nota: Si un servicio está colocalizado en el servidor de NW con el servidor de Admin en lugar de estar en su propio host exclusivo, debe incluirlo en la cadena de comandos. Por ejemplo, `nw-recovery-tool--import--dump-dir /var/netwitness/backup --category AdminServer --category Gateway.`

6. (Condicional) Los clientes que utilizan reglas de firewall personalizadas (es decir, que respondieron "Sí" al indicador "Deshabilitar el firewall" de nwsetup-tui durante la instalación) deben restaurar el archivo `/etc/sysconfig/iptables` desde la copia de respaldo ubicada en el archivo `<dump-dir>/unmanaged/etc/sysconfig/iptables`.
7. Reinicie el host de NetWitness Server.

Respaldar y restaurar datos en otros hosts de componentes

Realice estos procedimientos en cada sistema host de componentes de 11.x funcional existente.

Respaldar datos en un host de componentes

1. En el nivel raíz, escriba el siguiente comando:
   `nw-recovery-tool --export --dump-dir /var/netwitness/backup --category <category name>`
   donde el nombre de categoría es uno de los siguientes:
   `Archiver, Broker, Concentrator, Decoder, EndpointHybrid, EndpointLogHybrid, ESAPrimary, ESASecondary, LogCollector, LogDecoder, LogHybrid, Malware, NetworkHybrid, UEBA`

   Nota: 1.) Utilice la categoría que coincida con el tipo de host. 2.) Si los servicios están colocalizados en un host de componentes en lugar de estar en su propio host exclusivo, debe incluirlos en la cadena de comandos. Por ejemplo, un Warehouse Connector reside en un host de Log Decoder. El siguiente es un ejemplo de esta cadena de comandos.
   `nw-recovery-tool--export --dump-dir /var/netwitness/backup --category LogDecoder --category Warehouse`

2. **(Opcional)** Reemplace `/var/netwitness/backup` por la ruta a la ubicación donde se deben exportar los datos.
   a. Asegúrese de que esta ubicación tenga espacio suficiente para almacenar los datos de respaldo.
   b. La ruta del directorio de respaldo debe estar en el host local. Sin embargo, los archivos de respaldo podrían estar en un montaje de red o en un dispositivo externo.

3. Para los sistemas **EndpointHybrid**, **EndpointLogHybrid** y **ESAPrimary**, puede exportar los datos de las aplicaciones que se almacenan en la base de datos ejecutando el siguiente comando:
   `nw-recovery-tool --export --dump-dir /var/netwitness/backup --component mongo`
   Puede reemplazar `/var/netwitness/backup` por la ruta a la ubicación donde se deben exportar los datos.

   Nota: 1.) Asegúrese de que haya suficiente espacio en la ubicación de exportación para los archivos de la base de datos de Mongo. 2.) Puede respaldar los datos de los hosts de **EndpointHybrid**, **EndpointLogHybrid** o **ESAPrimary** y de la base de datos de Mongo en una sola cadena de comandos. Por ejemplo, `nw-recovery-tool --export --dump-dir /var/netwitness/backup --category EndpointHybrid --component mongo`

   Cuando se le solicite la contraseña de administración de la implementación, escriba la contraseña o incluya el siguiente argumento adicional para el comando `nw-recovery-tool`:
   `--deploy-password <password>`

4. Para **Malware**, puede exportar los datos de las aplicaciones desde la base de datos de aplicaciones de Malware ejecutando el siguiente comando:
   `nw-recovery-tool --export --dump-dir /var/netwitness/backup --component postgresql`

Puede reemplazar `/var/netwitness/backup` por la ruta a la ubicación donde se deben exportar los datos.

> **Nota:** Asegúrese de que haya suficiente espacio en la ubicación de exportación para los archivos de la base de datos de Malware.

5. Transfiera los datos respaldados del host local a un servidor externo o a una memoria USB.

Restaurar datos en un host de componentes

1. Vuelva a crear la imagen del host de componentes utilizando los mismos ajustes de configuración de red que los del host original. Para obtener información sobre la creación de una nueva imagen del host de componentes, consulte "Tarea 2: Instalar 11.x en otros hosts de componentes" en la *Guía de instalación de hosts físicos para la versión 11.x*.
2. **Opcional** Si necesita establecer conectividad de red antes de poder obtener datos de respaldo, por ejemplo, si están en un host remoto, ejecute el siguiente script utilizando los mismos ajustes de dirección IP, subred, puerta de enlace, DNS e información de domino que los del host original:
   `netconfig --static --interface <name> --ip <address> --netmask <netmask> --gateway <gateway>`
   Por ejemplo:
   `netconfig --static --interface eth0 --ip 192.168.1.100 --netmask 255.255.255.0 --gateway 192.168.1.1`
   Opcional: Para especificar servidores DNS, incluya el siguiente parámetro adicional:
   `--dns <address>`
   Opcional: Para establecer el nombre de dominio local, incluya el siguiente parámetro adicional:
   `--domain <name>`
   a. (**Opcional**) Si utiliza DHCP, ejecute el siguiente script:
      `netconfig --dhcp --interface <name>`
      Por ejemplo:
      `netconfig --dhcp --interface eth0`
   b. Agregue los datos de respaldo a la ruta del directorio de respaldo en el host local; por ejemplo, `/var/netwitness/backup`.
3. Ejecute el comando `nwsetup-tui`. Esto inicia el programa de instalación.

> **Nota:** Durante el programa de instalación, cuando se le solicite la configuración de red del host, asegúrese de especificar la misma configuración de red que se utilizó para la instalación original de 11.x en este host.

4. Cuando se le solicite, seleccione la opción de tipo de instalación **3: Recuperar (reinstalar)**, haga clic en **Aceptar** y, a continuación, ingrese la ruta al directorio que contiene los datos de respaldo.

5. Después de completar la instalación del comando `nwsetup-tui`, debe reinstalar los servicios apropiados (excepto EndpointHybrid y EndpointLogHybrid) en el host mediante el comando Instalar en la vista Hosts de la interfaz del usuario de NetWitness Platform.
   Para EndpointHybrid y EndpointLogHybrid, debe usar orchestration-cli-client en el servidor de Admin para instalar los servicios de Endpoint. Ejecute el siguiente comando:

   ```
   orchestration-cli-client --hostaddr-as-id -i -o <host IP Address> --
   category <EndpointHybrid or EndpointLogHybrid> --version <version>
   ```

   Por ejemplo:

   ```
   orchestration-cli-client --hostaddr-as-id -i -o 192.168.200.83 --category
   EndpointLogHybrid --version 11.2.0.0
   ```

   Nota: El número de versión debe coincidir con la versión de los medios que se utilizó para volver a crear la imagen del host.

6. Cuando la instalación de los servicios se complete, asegúrese de que la versión y el parche que se ejecutan en el host sean exactamente los mismos que los de los datos que se respaldaron:
   - Si los datos estaban en un sistema 11.x que se actualizó a una versión de parche superior, actualice el host de acuerdo con las instrucciones para actualizar sistemas offline correspondientes a la misma versión de parche que estaba en ejecución en el host (la versión y el parche exactos para los que se respaldaron los datos).
   - Si los datos estaban en una versión principal (por ejemplo, 11.x) que no se había actualizado a una versión de parche superior, no es necesario actualizar el sistema host.

7. Cuando el host se esté ejecutando en la versión correcta, regrese al nivel raíz del host de componentes y ejecute el siguiente comando para restaurar los datos:
   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --category
   <category name>
   ```

   Nota: Si los servicios están colocalizados en un host de componentes en lugar de estar en su propio host exclusivo, debe incluirlos en la cadena de comandos. Por ejemplo, un Warehouse Connector reside en un host de Log Decoder. El siguiente es un ejemplo de esta cadena de comandos.
   ```
   nw-recovery-tool--import --dump-dir /var/netwitness/backup --category
   LogDecoder --category Warehouse
   ```

8. Para los sistemas **EndpointHybrid**, **EnpointLogHybrid** y **ESAPrimary**, puede importar los datos de las aplicaciones que se restaurarán ejecutando el siguiente comando:
   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --component
   mongo
   ```

   Cuando se le solicite la contraseña de administración de la implementación, escriba la contraseña o incluya el siguiente argumento adicional para el comando `nw-recovery-tool`:
   `--deploy-password <password>`

9. Para **Malware**, puede importar los datos de las aplicaciones desde la base de datos de aplicaciones de Malware que se restaurará ejecutando el siguiente comando:
   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --component
   postgresql
   ```

10. Para un Decoder, un Log Decoder, un Concentrator, un Archiver, un Network Hybrid o un Log Hybrid configurados con almacenamiento externo (JBOD, SAN, Unity o PowerVault):
    a. Examine el archivo `<dump-dir>/unmanaged/etc/fstab` en busca de dispositivos con puntos de montaje que no existan en el archivo `/etc/fstab` del sistema.

    IMPORTANTE: Si va a migrar al nuevo hardware del host (es decir, un nuevo host de Decoder, Log Decoder, Concentrator, Archiver, Network Hybrid o Log Hybrid), debe realizar este procedimiento antes de continuar con el paso siguiente:
    1. Apague el host de hardware antiguo y el dispositivo de almacenamiento externo conectado a él.
    2. Conecte el dispositivo de almacenamiento externo al nuevo hardware del host.
    3. Encienda tanto el nuevo hardware del host como el dispositivo de almacenamiento externo conectado a él.

    b. Realice los siguientes pasos para cada dispositivo en la copia de respaldo de `<dump-dir>/unmanaged/etc/fstab`.
        i. Verifique que el dispositivo correspondiente esté presente y que esté conectado. Si no está conectado, conéctelo. Si el dispositivo ya no corresponde, omita este paso y vaya al dispositivo siguiente.
        ii. Verifique que el directorio del punto de montaje exista en el sistema de archivos. Si no existe, cree el directorio con el comando `mkdir <path>` .
        iii. Agregue la entrada `fstab` desde la copia de respaldo al archivo `/etc/fstab` del sistema.
    c. Ejecute el siguiente comando en cada host.
    `mount -a`
11. (De ASOC-59466) (Condicional) Los clientes que utilizan reglas de firewall personalizadas (es decir, que respondieron “Sí” al indicador “Deshabilitar el firewall” de nwsetup-tui durante la instalación) deben restaurar el archivo `/etc/sysconfig/iptables` desde la copia de respaldo ubicada en el archivo `<dump-dir>/unmanaged/etc/sysconfig/iptables`.
12. Reinicie el host de componentes.

Solamente actualización de hardware: Usar espacio adicional en nuevos hosts de hardware

Consulte la *Guía de ajuste de RSA NetWitness Platform Core* (https://community.rsa.com/docs/DOC-95938

) para obtener instrucciones sobre cómo utilizar todo el espacio disponible en el nuevo hardware.

Recuperación ante desastres en una implementación de Azure

En esta sección se indica cómo respaldar y restaurar NetWitness Platform 11.x implementado en hosts virtuales de Azure (también denominados VM en esta sección). Las dos tareas principales para respaldar y restaurar datos de la versión 11.x en una implementación de Azure son las siguientes:

- Tarea 1: Respaldar y exportar datos
- Tarea 2: Restaurar e importar datos

Tarea 1: Respaldar y exportar datos

1. Exporte los datos ejecutando los comandos `nw-recovery-tool --export`, como se describe en Recuperación ante desastres (instrucciones de respaldo y restauración).

Tarea 2: Restaurar e importar datos

Para completar esta tarea, debe consultar la *Guía de actualización de Azure 10.6.5 a 11.2*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

1. Elimine la VM.

   Precaución: No elimine los recursos (por ejemplo, no elimine los discos, la interfaz de red, etc.).

2. Realice los siguientes pasos para el host de AdminServer, el host de Broker, el host de ESA, el host de Endpoint y el host de Log Collector (donde host = `--category`).

   a. Elimine todos los recursos, excepto la tarjeta de interfaz de red de la VM 11.2 más antigua.

   b. Implemente la VM de 11.2 nueva con el mismo disco y los mismos recursos, y apáguela.
   Para obtener instrucciones detalladas sobre cómo implementar un host virtual en Azure, consulte la *Guía de implementación de Azure 11.2*.

   c. Ejecute `azure-mac-retention.ps1` desde la máquina local.
   Consulte la *Guía de actualización de Azure 10.6.5 a 11.2* para obtener instrucciones sobre cómo ejecutar este script.

   d. Siga el procedimiento para la restauración de la NRT del host respectivo, como se describe en Restaurar datos en un host de componentes.

   e. Después de la restauración de la NRT del host de componentes, restaure los siguientes archivos.

      - `/etc/fstab`
      - `/etc/hosts` (si no se cambia el nombre de host)
      - `/etc/waagent.conf`

- `/etc/logrotate.d/waagent.logrotate`
- `/etc/krb5.conf` desde la carpeta `<dump-dir>/unmanaged`

3. Realice los siguientes pasos para el host de Log Decoder, el host de Concentrator y el host de Archiver (donde host = `--category`).

   a. Elimine todos los recursos, excepto los discos nombrados como **externos** y la tarjeta de interfaz de red de la VM 11.2 más antigua.

   b. Implemente la VM de 11.2 nueva con el mismo disco y los mismos recursos que se señalan en la *Guía de implementación de Azure 11.2* y apáguela.

   > **Nota:** No cree el disco **externo**. Cree únicamente los discos **nwhome**.

   c. Ejecute `azure-mac-retention.ps1` desde la máquina local.
   Consulte la *Guía de actualización de Azure 10.6.5 a 11.2* para obtener instrucciones sobre cómo ejecutar este script.

   d. Siga el procedimiento para la restauración de la NRT de los hosts respectivos, como se describe en Restaurar datos en un host de componentes.

   e. Después de la restauración de la NRT del host de componentes, restaure los siguientes archivos.

   - `etc/fstab`
   - `/etc/hosts` (si no se cambia el nombre de host)
   - `/etc/waagent.conf`
   - `etc/logrotate.d/waagent.logrotate`
   - `/etc/krb5.conf`

Recuperación ante desastres en una implementación de AWS

En esta sección se indica cómo respaldar y restaurar NetWitness Platform 11.x implementado en hosts virtuales de AWS (también denominados VM en esta sección). Las dos tareas principales para respaldar y restaurar datos de la versión 11.x en una implementación de AWS son las siguientes:

- Tarea 1: Respaldar y exportar datos
- Tarea 2: Restaurar e importar datos

Tarea 1: Respaldar y exportar datos

1. Exporte los datos ejecutando los comandos `nw-recovery-tool --export`, como se describe en Recuperación ante desastres (instrucciones de respaldo y restauración).
2. Registre las direcciones IP. Debe consultarlas más adelante en el proceso de recuperación ante desastres.
   Consulte la *Guía de actualización de AWS 10.6.5 a 11.2* para obtener instrucciones sobre cómo conservar las direcciones IP. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Tarea 2: Restaurar e importar datos

Para completar esta tarea, debe consultar la *Guía de actualización de AWS 10.6.5 a 11.2*.

1. Elimine la VM.

   Precaución: No elimine los recursos (por ejemplo, no elimine los discos).

2. Realice los siguientes pasos para el host de AdminServer, el host de Broker, el host de ESA (primario y secundario), el host de Endpoint Hybrid, el host de Endpoint Log Hybrid y el host de Log Collector (donde host = `--category`).

   a. Elimine todos los recursos de la VM de 11.2 más antigua.

   b. Implemente la VM de 11.2 nueva con la misma dirección IP, el mismo disco y los mismos recursos, y apáguela.
      Para obtener instrucciones detalladas sobre cómo implementar un host virtual en AWS, consulte la *Guía de implementación de AWS 11.2*.

   c. Siga el procedimiento para la restauración de la NRT del host respectivo, como se describe en Restaurar datos en un host de componentes.

   d. Después de la restauración de la NRT del host de componentes, restaure los siguientes archivos.

      - `/etc/fstab`
      - `/etc/hosts` (si no se cambia el nombre de host)

3. Realice los siguientes pasos para el host de Log Decoder, el host de Decoder (Network Decoder), el host Concentrator y el host de Archiver (donde host = `--category`).
   a. Elimine todos los recursos, excepto los **discos externos**, de la VM de 11.2 más antigua.
   b. Implemente la VM de 11.2 nueva con la misma dirección IP, el mismo disco y los mismos recursos que se señalan en la *Guía de implementación de AWS 11.2* y apáguela.

      Nota: No cree el disco **externo**. Cree únicamente los discos **nwhome**.

   c. Siga el procedimiento para la restauración de la NRT de los hosts respectivos, como se describe en Restaurar datos en un host de componentes.
   d. Después de la restauración de la NRT del host de componentes, restaure los siguientes archivos.
      - `etc/fstab`
      - `/etc/hosts` (si no se cambia el nombre de host)
      - `/etc/krb5.conf`