NetWitness® Plataforma

Versión 12.4.0.0

Guía de actualización

NETWITNESS
Platform

Información de contacto

NetWitness Community en https://community.netwitness.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

RSA y otras marcas comerciales pertenecen a RSA Security LLC o sus filiales (“RSA”). Para obtener una lista de las marcas comerciales de RSA, vaya a https://www.rsa.com/en-us/company/rsa-trademarks. Las demás marcas comerciales pertenecen a sus respectivos propietarios.

Acuerdo de licencia

Este software y la documentación asociada son propiedad e información confidencial de RSA Security LLC o sus filiales, se suministran bajo licencia y pueden utilizarse y copiarse solamente de acuerdo con los términos de dicha licencia y con la inclusión del 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 RSA.

Licencias de otros fabricantes

Este producto puede incluir software desarrollado por otros fabricantes distintos de RSA. 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 NetWitness Community. 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 normativas actuales de uso, importación y exportación deben cumplirse cuando se use, importe o exporte este producto.

Distribución

El uso, la copia y la distribución de cualquier software de RSA Security LLC o sus filiales (“RSA”) descrito en esta publicación requieren la licencia de software correspondiente.

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

LA INFORMACIÓN DE ESTA PUBLICACIÓN SE PROPORCIONA “TAL CUAL”. RSA NO SE HACE RESPONSABLE NI OFRECE GARANTÍA DE NINGÚN TIPO CON RESPECTO A LA INFORMACIÓN DE ESTA PUBLICACIÓN Y ESPECÍFICAMENTE RENUNCIA A TODA GARANTÍA IMPLÍCITA DE COMERCIABILIDAD O CAPACIDAD PARA UN PROPÓSITO DETERMINADO.

Misceláneo

Este producto, este software, la documentación asociada y el contenido están sujetos a los Términos y condiciones estándar de NetWitness vigentes a la fecha de emisión de esta documentación y que se pueden encontrar en https://www.netwitness.com/standard-form-agreements/.

Marzo de 2024

Contenido

Actualizar NetWitness Platform

Este documento proporciona información sobre los beneficios y el proceso de actualización de NetWitness Platform a 12.4. Asegúrese de cumplir con los requisitos previos y las tareas previas a la actualización antes de actualizar NetWitness Platform. Puede actualizar NetWitness Platform mediante cuatro opciones diferentes según su acceso a Internet. Después de la actualización, también debería realizar ciertas tareas y comprobaciones de errores posteriores a esta que se enumeran en esta guía para completar el proceso de actualización con éxito. Las instrucciones de este documento se aplican a los hosts físicos y virtuales (que incluyen AWS, la nube pública de Azure y Google Cloud Platform), salvo que se indique lo contrario.

IMPORTANTE: Las versiones 11.7.x, 12.0 y 12.1 alcanzaron el final del ciclo de vida (EOL) el 31 de diciembre de 2023. Para obtener más información, consulte https://community.netwitness.com/t5/product-life-cycle/product-version-life-cycle-for-rsa-netwitness-platform/ta-p/569875. Si desea actualizar desde las versiones 11.7.x (paquetes de servicio) u 11.7.xx (parches) a la versión 12.4.0.0, primero debe actualizar a la versión 12.2.0.0 o 12.3.0.0 antes de actualizar a 12.4.

Nota: NetWitness Platform ahora admite la instalación de varios servidores de UEBA en su entorno. Para obtener más información, consulte el tema **Configurar varios servidores UEBA** en la *Guía de configuración de NetWitness de UEBA*.

Hay muchas funciones nuevas e increíbles que puede habilitar una vez que actualice a la versión 12.4. Para una descripción detallada de las nuevas funciones en esta versión, consulte las *Notas de la versión para NetWitness Platform 12.4*. Vaya a la página Documentos de todas las versiones de NetWitness y busque guías de NetWitness Platform para solucionar problemas. Para obtener más información sobre las nuevas funciones lanzadas en versiones anteriores, consulte https://community.netwitness.com/t5/netwitness-platform-online/what-s-new-in-previous-releases-11-x-to-12-x/ta-p/695650.

Rutas de actualización compatibles para 12.4

Las siguientes rutas de actualización son compatibles con NetWitness 12.4:

- NetWitness 12.3.1.0 a 12.4
- NetWitness 12.3.0.0 a 12.4
- NetWitness 12.2.0.1 a 12.4
- NetWitness 12.2.0.0 a 12.4

Ejecución en entorno de modo mixto

NetWitness Platform admite el modo mixto durante la actualización. El modo mixto se produce cuando se actualizan algunos de los servicios a la versión más reciente y algunos todavía están en las versiones anteriores.

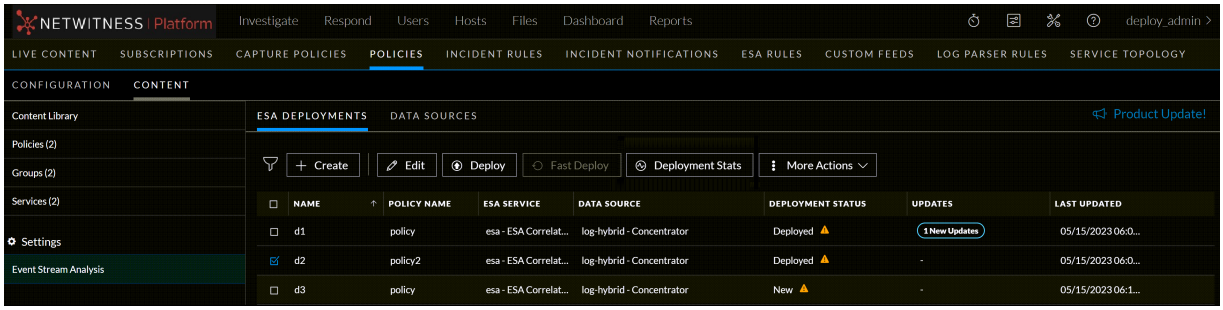
Para obtener más información, consulte **Ejecución en modo mixto** en la *Guía de introducción de hosts y servicios de NetWitness*.

Nota:
- Si lleva más tiempo actualizar todos los hosts en su entorno, comuníquese con el soporte de NetWitness para evitar cualquier tipo de problema.
- Si está ejecutando Endpoint Log Hybrid en modo mixto, asegúrese de que Endpoint Broker esté en la misma versión que uno de los servidores Endpoint.
- El modo mixto no es compatible con hosts de ESA en NetWitness Platform.

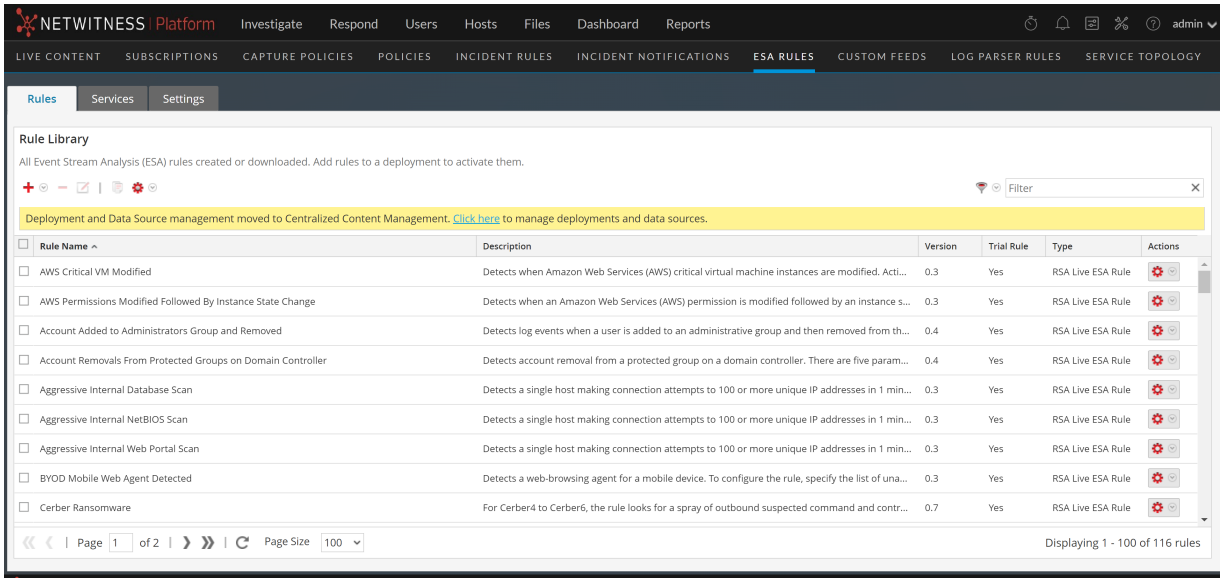
Consideraciones de actualización para hosts de ESA

IMPORTANTE: El servidor NetWitness, el host primario de ESA y el host secundario de ESA deben estar en la misma versión de NetWitness Platform.

- Solo puede administrar las implementaciones de ESA y los orígenes de datos a través de **Administración de contenido centralizada**. Vaya a la página (**CONFIGURAR**) > **Políticas** > **Contenido** > **Event Stream Analysis** para administrar las implementaciones de ESA y los orígenes de datos. Consulte la siguiente figura.



- Solo puede gestionar las reglas de ESA en la página **reglas de ESA**. Consulte la siguiente figura.



- Después de actualizar a la versión 12.4, todas las implementaciones de ESA se migrarán a la página (**CONFIGURAR**) > **Políticas**. Cada implementación se convertirá en una política y un grupo y estará disponible para administrar solo después de la actualización de los servidores de correlación a la versión 12.4. Asegúrese de planear el proceso de actualización para que los servidores de correlación se actualicen inmediatamente después del servidor Admin. No se podrá acceder a las implementaciones hasta que se actualicen los servidores de correlación correspondientes. Sin embargo, los servidores de correlación seguirán procesando las alertas y los eventos.
- Debe actualizar los hosts de ESA inmediatamente después de actualizar el servidor de administración.

  Para más información sobre la **Administración de contenidos centralizada** y cómo administrar las implementaciones, consulte la Guía de administración de contenido centralizada para NetWitness.

Actualizar o instalar la recopilación heredada de Windows

Consulte la Windows Legacy Collection Guide for NetWitness para obtener instrucciones de instalación y actualización de la colección heredada de Windows de NetWitness.

Nota: Después de actualizar o instalar la recopilación de Windows heredada, reinicie el sistema para asegurar el correcto funcionamiento de la recopilación de registros.

Terminologías

Nombre	Descripción
AVX	Extensiones vectoriales avanzadas
VMX	Extensión de máquina virtual
NFS	Network File System
BTRFS	Sistema de archivos tipo árbol B
DPDK	Kit de desarrollo del plano de datos

Ejecutar comprobaciones antes de la actualización

Debe ejecutar las comprobaciones previas a la actualización antes de actualizar a NetWitness Platform 12.4 para identificar cualquier problema que pueda provocar un error en la actualización.

Para ejecutar las comprobaciones previas a la actualización:

1. SSH a Servidor de administración.
2. Utilice la herramienta Upgrade Precheck y ejecute los siguientes comandos en secuencia:
   a. `nw-precheck-tool-standalone os-migration-checklist`: Este comando permite que la herramienta Upgrade Precheck realice comprobaciones de errores para la lista de sondeos en la Lista de verificación de migración de sistema operativo.
   b. `nw-precheck-tool-standalone upgrade-checklist`: Este comando permite que la herramienta Upgrade Precheck realice comprobaciones de errores para la lista de sondeos en la Lista de verificación de actualización.
   c. `nw-precheck-tool-standalone network-checklist`: Este comando permite que la herramienta Upgrade Precheck realice comprobaciones de errores para la lista de sondeos en la Lista de verificación de red.
   d. `nw-precheck-tool-standalone cert-checklist`: Este comando permite que la herramienta Upgrade Precheck realice comprobaciones de errores para la lista de sondeos en la Lista de verificación de certificados.

Lista de verificación de migración de sistema operativo

La herramienta Upgrade Precheck realiza las comprobaciones de errores para la siguiente lista de sondeos en la lista de verificación de migración del sistema operativo:

- **Sondeo de verificación de versión**: Comprueba si la versión de NetWitness del sistema es la versión posterior de 12.2.0.0 o no.
- **Sondeo AVX/VMX**: Comprueba si los indicadores AVX/VMX están habilitados o no para los nodos que los requieren.
- **Sondeo de montaje NFS**: Comprueba si el punto de montaje tipo NFS está activo en alguno de los nodos.
- **Sondeo de paquete kernel-devel múltiple**: Comprueba si Decoder y PacketHybrid tienen varias versiones del paquete kernel-devel o no.
- **Sondeo del dispositivo de captura de anillo PF**: Comprueba el dispositivo de captura PF_ring en los decodificadores y genera una advertencia para cambiar el dispositivo de captura PF_ring al dispositivo de captura DPDK.
- **Sondeo de montaje BTRFS**: Comprueba si la partición BTRFS está montada.

  Nota: LEAPP y Alma OS no admiten la partición BTRFS.

- **Comprobación de espacio de disco**: Comprueba que haya suficiente disco libre en la partición / de cada nodo.

- **Comprobación del modo FIPS**: Comprueba que el modo FIPS esté desactivado (configurado en falso) en todos los nodos.
- **Sondeo de comprobación de montaje**: Comprueba si todas las particiones o directorios de archivos están montados correctamente.

Lista de verificación de actualización

La herramienta Upgrade Precheck realiza las comprobaciones de errores para la siguiente lista de sondeos en la lista de verificación de actualizaciones:

- **Comprobación de archivos del cliente de seguridad**: Garantiza que el archivo `security-client-amqp.yml` no esté presente.
- **Comprobación del estado de ID de servicio del nodo 0 de NW**: Garantiza que toda la identificación del servicio esté intacta con todos los diferentes servicios en el nodo 0.
- **Comprobación de archivos de enlace simbólico de Broker Service Trustpeer**: Garantiza que el archivo de enlace simbólico de Broker Service Trustpeer `(/etc/netwitness/ng/broker/trustpeers/)` no esté dañado.
- **Comprobación del estado de servicios del nodo 0 de NW**: Comprueba el estado de todos los servicios en el nodo 0.
- **Comprobación de repositorio externo de Yum**: Garantiza que los repositorios externos no estén disponibles ni habilitados.
- **Comprobación del índice de base de datos RPM del nodo 0**: Comprueba si la base de datos RPM está dañada o no.
- **Comprobación de comunicación de Salt Master**: Comprueba la comunicación salt desde el nodo 0 a todos los nodos.
- **Comprobación de certificados del nodo 0**: Comprueba si falta algún certificado, si está caducado o si el tipo de emisor no es válido.
- **Autenticación Mongo**: Valida las credenciales `deploy_admin` obtenidas de `security-cli-client` usando el cliente Mongo.
- **Autenticación Rabbitmq**: Valida las credenciales `deploy_admin` obtenidas de `security-cli-client` usando RabbitMQ.
- **(Hosts de componentes) Comprobación del estado del servicio del nodo X NW**: Comprueba el estado de los servicios (Activo o Inactivo) en todos los nodos X.
- **(Hosts de componentes) Comprobación de certificados del nodo X**: Comprueba la caducidad del certificado, la falta, el daño y la discrepancia del emisor en todas las categorías del nodo X.
- **Proporcionar información de memoria de CPU de nodos**: Proporciona detalles de CPU y memoria de todos los nodos junto con la memoria disponible en tiempo real.

- **(Servidor de administración) Comprobación de utilización del sistema de archivos del nodo 0**: Comprueba la utilización de la partición del disco de `/var/netwitness/mongo`, `/var/netwitness` y `root` en el nodo 0.
- **(Hosts de componentes) Comprobación de utilización del sistema de archivos del nodo X**: Comprueba la utilización de la partición del disco de `/var/netwitness/mongo`, `/var/netwitness` y `root` para los servicios de ESA principal y Endpoint Log Hybrid en el nodo X.
- **Comprobación del modo de permiso del archivo Mongo (ESA primario)**: Comprueba el nodo de ESA primario en el sistema o pila y verifica el modo de permiso del archivo Mongo.
- **Comprobación del modo normal del servidor de orquestación**: Comprueba si el servicio de orquestación se está ejecutando en modo normal o seguro.
- **(Servidor de administración) Comprobación del estado de inicio del nodo 0**: Comprueba si hay algún problema que pueda fallar en el proceso de inicio.
- **Comprobación del modo FIPS**: Comprueba que el modo FIPS esté desactivado (configurado en falso) antes y después de actualizar.
- **Comprobación del índice de base de datos RPM del nodo X**: Comprueba el estado de la base de datos RPM del nodo X para asegurarse de que no esté dañado.
- **Comprobación de proxy Yum de nodo Z**: Comprueba la existencia del archivo yum.conf y la disponibilidad del proxy dentro del archivo en el nodo Z.
- **Comprobación de proxy Yum de nodo X**: Comprueba la existencia del archivo yum.conf y la disponibilidad del proxy dentro del archivo en el nodo X.
- **Sondeo de comprobación de información del host**: Comprueba si los campos obligatorios de información de todos los hosts del sistema (IP del host, nombre de host, servicios instalados y versión sin formato) están disponibles.
- **Sondeo de comprobación de cifrado de nodo Z**: Comprueba si los cifrados requeridos están disponibles en la ubicación `/etc/rabbitmq/rabbitmq.config` en el nodo 0.
- **Sondeo de comprobación de cifrado de nodo X**: Comprueba si los cifrados requeridos están disponibles en la ubicación `/etc/rabbitmq/rabbitmq.config` en todos los nodos X.
- **Sondeo de comprobación de versión de hardware de nodo X**: Comprueba la versión de hardware de todos los nodos X accesibles.
- **Sondeo de comprobación de versión de hardware de nodo Z**: Comprueba la versión de hardware del servidor de administración.
- **Sondeo de comprobación de certificados PuppetCA**: Comprueba si los certificados de Puppet CA obsoletos están presentes en la ubicación `/etc/pki/nw/trust/truststore.pem`.
- **Sondeo de comprobación de certificados de administrador**: Comprueba si los certificados de administrador en todos los nodos son los mismos que los certificados de administrador en el servidor de administración.

- **Sondeo NTP**: Comprueba todos los nodos para asegurarse de que estén sincronizados con el servidor NTP.
- **Sondeo de verificación de certificados obsoletos**: Comprueba Mongo y advierte si contiene certificados obsoletos no utilizados.
- **Sondeo de comprobación de ID de certificados de nodos**: Comprueba el campo de asunto del certificado de nodo y garantiza que sea el mismo que el ID de nodo del host.
- **Implementar sondeo de comprobación de caducidad de contraseña de administrador**: Comprueba si la contraseña de deploy_admin ha caducado en el nodo 0.
- **Comprobación de permisos de archivo/carpeta**: Este sondeo comprueba si los archivos/carpetas tienen los permisos adecuados.

Lista de verificación de red

La herramienta Upgrade Precheck realiza las comprobaciones de errores para la siguiente lista de sondeos en la lista de verificación de red:

- **(Servidor de administración) Comprobación de puertos cerrados del nodo 0**: Comprueba si los puertos de servicio necesarios para los servicios de NetWitness están abiertos y se escuchan en el nodo 0.
- **(Hosts de componentes) Comprobación de puertos cerrados del nodo X**: Comprueba si los puertos de servicio necesarios para los servicios de NetWitness están abiertos y se escuchan en el nodo X.

Lista de verificación de certificados

La herramienta Upgrade Precheck realiza las comprobaciones de errores para la siguiente lista de sondeos en la lista de verificación de certificados:

- **Comprobación de validez de los certificados de servicio del nodo 0**: Comprueba la validez de los certificados de servicio en la ubicación `/etc/pki/nw/service/` en el nodo 0.
- **Comprobación de validez de los certificados de servicio del nodo X**: Comprueba la validez de los certificados de servicio en la ubicación `/etc/pki/nw/service/` en el nodo X.
- **Comprobación de validez de los certificados en el nodo 0**: Comprueba la validez de los certificados de nodo en la ubicación `/etc/pki/nw/service` en el nodo 0.
- **Comprobación de validez de los certificados de CA raíz**: Comprueba la validez de los certificados de CA raíz en la ubicación `/etc/pki/nw/ca`.

Prepárese para actualizar NetWitness Platform

Realice las siguientes tareas para preparar la actualización a NetWitness Platform 12.4.

Tarea 1. (Importante) Prepárese para actualizar el sistema operativo AlmaLinux

Sistema de archivos no compatibles

Desmontar y eliminar BTRFS

BTRFS es un sistema de archivos de copiar al escribir (CoW) para Linux que tiene como objetivo implementar características avanzadas del sistema de archivos mientras se enfoca en la tolerancia a fallas, la reparación y la fácil administración. El sistema de archivos BTRFS está obsoleto en Red Hat Enterprise Linux 8 y el sistema operativo AlmaLinux no es compatible con el sistema de archivos BTRFS. NetWitness no utiliza BTRFS de forma predeterminada, pero en algunas categorías como decodificador de red, red híbrida, etc., el módulo BTRFS existe y está cargado. Si BTRFS está montado como un sistema de archivos, realice los pasos a continuación para desmontar la partición BTRFS manualmente (si BTRFS no está montado, omita los pasos a continuación):

a. Reubicar los datos.

b. Desmontar la partición BTRFS mediante el siguiente comando.

c. umount<ruta de partición btrfs>. Puede obtener la información de la partición btrfs desde los comandos `/etc/fstab or df -hT`.

d. Elimine la partición BTRFS de `/etc/fstab`.

e. Verifique si el módulo del kernel todavía está cargado mediante `lsmod | grep btrfs`. Si el módulo del kernel aún está cargado, use `modprobe -r btrfs` para descargar el módulo del kernel btrfs.

f. Activar/Reactivar la actualización.

Para obtener más información, consulte el artículo de la base de conocimientos "Actualizar al sistema operativo Alma cuando esté montado el sistema de archivos BTRFS".

Desmontar NFS

Los sistemas de archivos de tipo NFS activos en los nodos hacen que falle la actualización de los nodos. Debe desmontar manualmente estos puntos de montaje de la CLI de cada nodo donde se encuentre. Siga los pasos a continuación para desmontar NFS manualmente:

a. SSH a los nodos donde se detecta el punto de montaje NFS.

b. En cada nodo, ejecute `mount | grep 'type nfs'` y obtenga la ruta del directorio del punto de montaje NFS.

Nota: Antes de desmontar NFS, debe interrumpir los servicios de NetWitness que dependen de NFS.
Por ejemplo: Si el servicio Archiver y Warehouse Connector se ejecuta en NFS, debe ejecutar los siguientes comandos para detener los servicios antes de desmontar NFS.
`systemctl stop nwarchiver`
`systemctl stop nwwarehouseconnector`

c. Ejecute desmontar <dir_path> desde la terminal, donde <dir_path> es la ruta del directorio del Paso b.

d. Abra el archivo `/etc/fstab` en un editor de su elección y comente las líneas que pertenecen a los puntos de montaje NFS.

e. Ejecute la actualización de NetWitness.

f. Después de que la actualización se haya completado exitosamente, elimine el comentario de la entrada respectiva de `/etc/fstab` y ejecute `mount -a` desde la terminal para volver a agregar los puntos de montaje NFS.

Comprobación del conjunto de instrucciones de la CPU AVX/VMX

El indicador de CPU AVX/VMX debe estar habilitado para NetWitness Platform 12.4. Ejecute el comando
`salt '*' cmd.run "lscpu | grep -E 'avx|vmx'"` para verificar si el conjunto de instrucciones de CPU AVX/VMX está habilitado. Para obtener más información, consulte el artículo de la base de conocimientos "Utilizar el conjunto de instrucciones AVX para la compatibilidad con la plataforma MongoDB 5.0".

Nota: Para el dispositivo de hardware NetWitness, el conjunto de instrucciones de CPU AVX/VMX está habilitado de forma predeterminada.

Soporte de migración de PF_RING a DPDK

La configuración de captura de Decoder no será válida para clientes que utilicen la captura PF_RING (CentOS) y actualicen directamente a 12.4 (AlmaLinux). Primero, deben migrar dispositivos PF_RING a DPDK y luego actualizar.

Consulte Migrar dispositivos PF_RING a DPDK para obtener instrucciones de migración.

Tarea 2. (Opcional). Eliminar repositorios de paquetes heredados

Puede liberar espacio de disco al eliminar repositorios obsoletos de versiones anteriores.

Para eliminar los repositorios obsoletos:

1. Determine la versión del host de NetWitness Platform más antiguo de su entorno mediante la herramienta NetWitness Repo. Realice lo siguiente:

- SSH al servidor de administración como usuario `root`.
- Ejecute el siguiente comando.

  ```
  nw-repo-tool --list-obsolete
  ```

  Después de ejecutar este comando, obtendrá una lista de todos los repositorios obsoletos.

2. Ejecute el siguiente comando para eliminar todos los repositorios obsoletos.

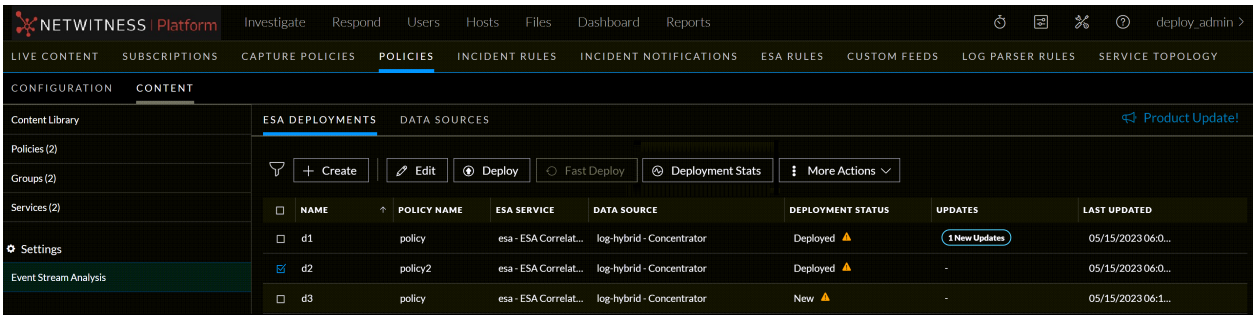
   ```
   nw-repo-tool --purge-obsolete
   ```

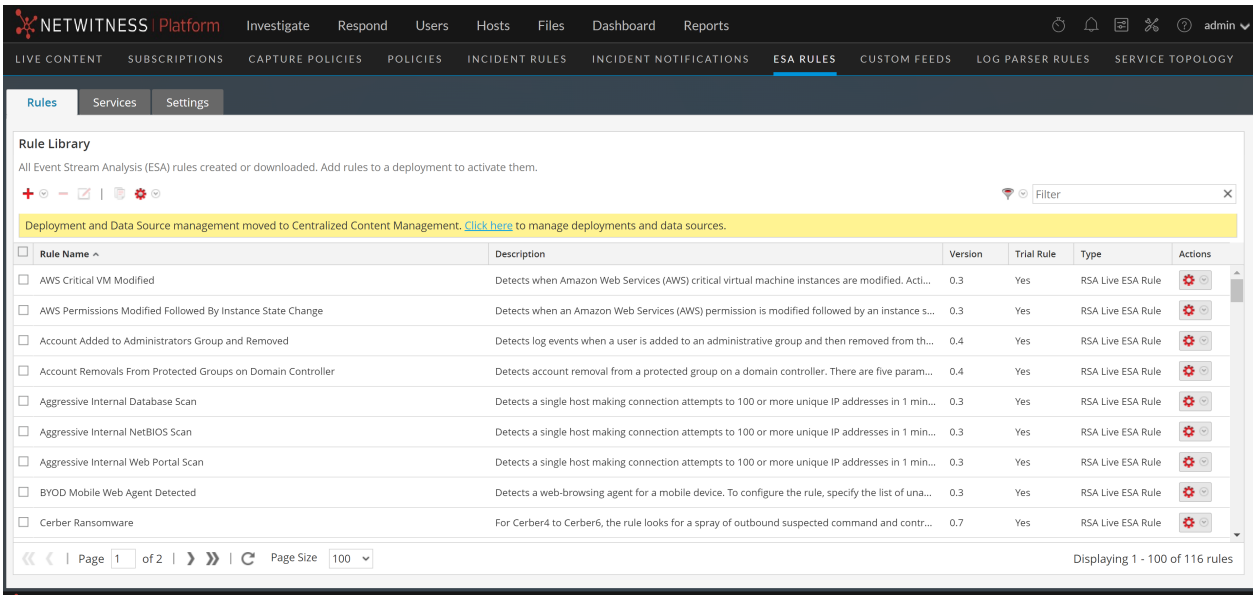
Tarea 3. Preparar las implementaciones de ESA para la migración a 12.4

Antes de actualizar a 12.4, NetWitness recomienda que todas las implementaciones de ESA mantengan un estado sin errores. Debe eliminar todas las implementaciones de ESA no utilizadas, ya que las implementaciones de ESA se migrarán a políticas y grupos después de actualizar a 12.4. Cada implementación se convertirá en una política y un grupo y estará disponible para administrar solo después de la actualización de los servidores de correlación a la versión 12.4.

Administrar implementaciones de ESA y orígenes de datos

Solo puede administrar las implementaciones de ESA y los orígenes de datos a través de **Administración de contenido centralizada**. Vaya a la página (**CONFIGURAR**) > **Políticas** > **Contenido** > **Event Stream Analysis** para administrar las implementaciones de ESA y los orígenes de datos. Solo puede gestionar las reglas de ESA en la página **reglas de ESA**. Consulte las siguientes figuras.





Asegúrese de planear el proceso de actualización para que los servidores de correlación se actualicen inmediatamente después del servidor Admin. No se podrá acceder a las implementaciones hasta que se actualicen los servidores de correlación correspondientes. Sin embargo, los servidores de correlación seguirán procesando las alertas y los eventos. Debe actualizar los hosts de ESA inmediatamente después de actualizar el servidor de administración.

Para más información sobre la **Administración de contenidos centralizada** y cómo administrar las implementaciones, consulte la Guía de administración de contenido centralizada para NetWitness.

IMPORTANTE: Si es necesario importar reglas y enriquecimientos de ESA, NetWitness recomienda importar esas reglas y enriquecimientos que faltan antes de la actualización.

Los estados de las implementaciones anteriores y posteriores a la actualización se representan en la siguiente tabla.

SINo	Estado de implementación previo a la actualización	Estado de implementación posterior a la actualización		
		Crea política	Crea grupo	La política será publicada
1	Implementación saludable	Sí	Sí	Sí
2	Implementación con errores	Sí	Sí	Sí
3	Implementación solo con reglas	Sí	No	No
4	Implementación sin reglas	No	No	No

La implementación saludable no contiene errores y se agregan los recursos necesarios, como el servidor ESA, el origen de datos y las reglas de ESA.

Nota: NetWitness recomienda que todas las implementaciones de ESA mantengan un estado sin errores. Debe eliminar cualquier implementación de ESA innecesaria o no utilizada.

Tarea 4. Single Sign-on (SSO): Habilite el registro de respuesta SAML en Microsoft Azure ADFS

La siguiente configuración solo se aplica a los casos en los que la respuesta SAML de Microsoft Azure ADFS solo se cifró sin firmar. Si su Microsoft Azure ADFS ya está configurado para firmar y cifrar respuestas SAML, puede ignorar esta configuración y continuar con el proceso de actualización.

Si no firma la respuesta SAML, NetWitness le recomienda configurar Microsoft Azure ADFS para cifrar y firmar las respuestas SAML antes de actualizar su NetWitness Platform a la versión 12.4 para un inicio de sesión Single Sign-on (SSO) exitoso. Para habilitar el registro de respuestas en el Servicio de federación de Active Directory (AD FS), ejecute el siguiente comando en ***powershell***:

```
Set-AdfsRelyingPartyTrust -TargetName <<relying-party-name>> -
SamlResponseSignature MessageAndAssertion
```

IMPORTANTE: Es obligatorio configurar Microsoft Azure ADFS para firmar respuestas SAML antes de actualizar a la versión 12.4 de NetWitness Platform. Si no cumple con estos requisitos, es posible que no pueda iniciar sesión mediante SSO.

Tarea 5. (Opcional). Deshabilitar los controles del kernel de FIPS basados en STIG

Si habilitó los controles del kernel de FIPS basados en STIG, debe deshabilitarlos antes de iniciar el proceso de actualización de NetWitness Platform para evitar errores de inicio. Para deshabilitar los controles del kernel de FIPS basados en STIG, ejecute los siguientes comandos:

```
manage-stig-controls --disable-control-groups 3 --host-all
```

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Una vez que actualice NetWitness Platform, asegúrese de habilitar los controles del kernel de FIPS basados en STIG.

Nota: Los controles de kernel de FIPS basados en STIG que requieren modificaciones a las opciones de arranque del kernel no están habilitados por NetWitness de manera inmediata.

Tarea 6. (Opcional). Comprobar la conexión al servidor de Live

Nota: Esta tarea opcional se aplica a usted solo si está actualizando NetWitness Platform mediante Live.

Vaya a `admin/system/live services` y realice una conexión de prueba para verificar si puede conectarse al servidor de Live, ya que esto es esencial para el servidor de origen desde 12.x y superior. Este es un paso opcional y solo aplica para clientes que han configurado Live.

Tarea 7. Sincronizar la hora en los hosts de componentes con el host del servidor NW

Antes de actualizar los hosts, asegúrese de que la hora de cada host esté sincronizada con la hora del servidor NetWitness.

Para sincronizar la hora, realice una de las siguientes acciones:

1. Configure el servidor NTP.

Para obtener más información, consulte **Configurar servidores NTP** en la Guía de configuración del sistema.

2. Siga los siguientes pasos:

a. Protocolo SSH al host del servidor de administrador.

b. Ejecute los siguientes comandos.

```
salt \* service.stop ntpd
salt \* cmd.run 'ntpdate nw-node-zero'
salt \* service.start ntpd
```

Realizar tareas de actualización

Primero los clientes deben descargar el RPM independiente mediante https://community.netwitness.com/t5/netwitness-platform-downloads/netwitness-platform-standalone-precheck-tool/ta-p/709096 y consultar el archivo Léame para obtener instrucciones sobre cómo instalar el RPM independiente y luego ejecutar la verificación previa. Consulte la sección "Ejecutar comprobaciones previas a la actualización" para obtener más detalles.

Actualice los sistemas de su entorno en el siguiente orden:

1. Hosts del servidor NW
2. Hosts de Analyst UI
3. Hosts primarios de ESA
4. Hosts secundario de ESA
5. Hosts independientes de Broker
6. Hosts de Concentrator
7. Hosts de Archiver
8. Hosts de Packet Decoder
9. Hosts de Log Decoder
10. Hosts de Log Collector/VLC
11. El resto de los hosts de componentes

IMPORTANTE: Todos los hosts primarios y secundarios de ESA, Analyst UI y servidor NW se deben actualizar el mismo día. El resto de los hosts de componentes pueden actualizarse el mismo día o más adelante. Asegúrese de planear el proceso de actualización para que los servidores de correlación se actualicen inmediatamente después del servidor Admin. Para obtener más información, consulte "**Tarea 3. Preparar las implementaciones de ESA para la migración a 12.4**" en el tema Prepárese para actualizar NetWitness Platform. El modo mixto no es compatible con hosts de ESA en NetWitness Platform. El servidor NetWitness, el host primario de ESA y el host secundario de ESA deben estar en la misma versión de NetWitness Platform.

Para obtener información sobre todos los tipos de host en NetWitness, consulte la *NetWitness Hosts and Services Getting Started Guide*. Vaya a la página Documentos de todas las versiones de NetWitness y busque guías de NetWitness Platform para solucionar problemas.

IMPORTANTE: Después de actualizar el servidor NW principal (incluido el servicio del servidor Respond), el servicio del servidor Respond no se vuelve a habilitar automáticamente hasta que el host primario de ESA también se actualice a la misma versión. Las tareas posteriores a la actualización de Respond solo se aplican después de que el servicio del servidor de Respond se haya actualizado y se encuentre en el estado habilitado.

Nota: Para la versión 12.4 con Log Collector de Windows heredado, debería realizar pocas tareas adicionales posteriores a la actualización. Consulte la sección Recopilación de registros de Windows heredado en Ejecución de tareas posteriores a la actualización para conocer estas tareas adicionales posteriores a la actualización.

Seleccionar Opciones de actualización

Puede seleccionar una de las siguientes opciones de actualización en función de la conexión a Internet. Se enumeran en el orden recomendado por NetWitness Platform.

- Opción 1: Actualizar NetWitness Platform mediante Live Services
- Opción 2: Actualizar NetWitness Platform sin conexión
- Opción 3: Actualizar NetWitness Platform mediante CLI (sin conexión)
- Opción 4 (opcional): Preconfigurar repositorio de actualización mediante la descarga de paquetes

Las siguientes reglas se aplican cuando actualiza hosts utilizando cualquiera de los 4 métodos de actualización:

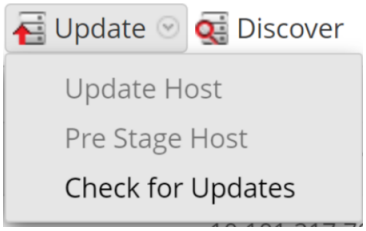
- En primer lugar, debe actualizar el servidor de NW.
- Solo puede aplicar una versión que sea compatible con la versión de host existente.
- El servidor NW, los hosts primarios y secundarios de ESA y Analyst UI deben estar en la misma versión de NetWitness Platform.

Opción 1: Actualizar NetWitness Platform mediante Live Services

Puede usar este método si el host del servidor de NW está conectado a los Servicios de Live.

Precaución: Debe revisar su política de red antes de descargar el paquete de actualización, que tiene aproximadamente 11.7 GB. Si ha configurado alguna política que no permite la descarga de archivos de más de 10 GB, la descarga del paquete de actualización fallará.

Nota: Puede preconfigurar el repositorio de actualización utilizando la función **Preconfigurar host**. Consulte la siguiente figura. Para obtener más información, consulte Opción 4 (opcional): Preconfigurar repositorio de actualización mediante la descarga de paquetes.



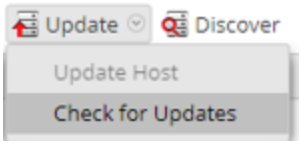
Requisitos previos

1. La opción **Descargar automáticamente información acerca de actualizaciones nuevas cada día** está seleccionada y aplicada en **(Admin) > Sistema > Actualizaciones**.

2. Hay disponibles actualizaciones. Vaya a **(Admin) > Hosts > Actualizar > Buscar actualizaciones** para buscar actualizaciones. La vista Host muestra el estado **Actualización disponible**.
3. 12.4 está disponible en la columna **Versión de actualización**.

Para actualizar de 12.2.0.0, 12.2.0.1, 12.3.0.0 y 12.3.1.0 a 12.4:

1. Vaya a **(Admin) > Hosts**.
2. Seleccione el host del servidor de NW (`nw-server`).
3. Busque las actualizaciones más recientes.



Se muestra Actualización disponible en la columna **Estado** si tiene una actualización de versión en el repositorio de actualización local para el host seleccionado.

4. Seleccione **12.4** de la columna **Actualizar versión**.

Nota:
- Si desea ver un cuadro de diálogo con las principales funciones de la actualización e información sobre las actualizaciones, haga clic en el icono ( ) a la derecha del número de versión de actualización.

- Si no puede encontrar la versión que desea, seleccione **Actualizar > Buscar actualizaciones** para buscar las actualizaciones disponibles en el repositorio. Si hay una actualización disponible, se muestra el mensaje "Están disponibles nuevas actualizaciones" y la columna **Estado** se actualiza automáticamente para mostrar Actualización disponible. De forma predeterminada, solo se muestran las actualizaciones compatibles para el host seleccionado.

5. Haga clic en **Actualizar** > **Actualizar host** en la barra de herramientas.
6. Haga clic en **Iniciar actualización**.
7. Haga clic en **Reiniciar host**.
8. Repita los pasos del 5 al 7 para otros hosts.

Nota: Puede seleccionar varios hosts para actualizar a la vez únicamente después de actualizar y reiniciar el servidor de NW. Todos los hosts de ESA, Endpoint y Malware Analysis se deben actualizar a la misma versión que la del host del servidor de NW.

Opción 2: Actualizar NetWitness Platform sin conexión

Puede actualizar NetWitness Platform manualmente realizando las siguientes tareas.

Tarea 1. Complete la carpeta de almacenamiento provisional (`/var/netwitness/common/update-stage/`) con archivos de actualización de versión. Realice lo siguiente.

1. Descargue el paquete de actualización `netwitness-12.4.0.0.zip` desde NetWitness Community (https://community.netwitness.com/) > **Descargas** > **NetWitness Platform** > **Versión 12.4** a un directorio local:
   - Si está actualizando de 12.2.0.0, 12.2.0.1, 12.3.0.0 y 12.3.1.0, descargue `netwitness-12.4.0.0.zip`.
2. Acceda mediante el protocolo SSH al host del servidor de NW.
3. Cargue `netwitness-12.4.0.0.zip` a `/var/netwitness/common/update-stage/` en el host del servidor NW.
   Por ejemplo:

   ```
   mv /var/netwitness/tmp/netwitness-12.4.0.0.zip
   /var/netwitness/common/update-stage/
   ```

Nota: NetWitness Platform descomprime el archivo automáticamente.

Tarea 2. Aplicar actualizaciones desde el área de almacenamiento provisional a cada host. Realice lo siguiente.

Precaución: Se debe actualizar el host del servidor de NW antes de actualizar cualquier host de servidor que no sea NW.

1. Inicie sesión en NetWitness.
2. Vaya a  **(Admin) > Hosts**.

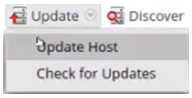
   Nota: Si ya está en la página  **(Admin) > Hosts** y la opción **Buscar actualizaciones** (**Actualización** > **Buscar actualizaciones**) está deshabilitada, actualice la página desde el navegador para buscar actualizaciones.
3. Compruebe si hay actualizaciones y espere a que se copien, validen y estén listos para iniciar los paquetes de actualización.

   Se muestra "Listo para iniciar los paquetes" si:
   - NetWitness Platform puede acceder al paquete de actualización.
   - El paquete está completo y no tiene errores.

   Consulte Solucionar problemas de instalación y actualización de versiones para obtener instrucciones sobre cómo solucionar errores (por ejemplo, "Error al implementar la versión <número-versión>" y "Faltan los siguientes paquetes de actualización", se muestran en el diálogo **Iniciar paquete de actualización para RSA NetWitness Platform**).
4. Haga clic en **Iniciar actualización**.

Demora un poco iniciar los paquetes porque los archivos son grandes y es necesario descomprimirlos. El tiempo varía según cómo esté configurado el host.
Una vez que la inicialización sea exitosa, la columna **Estado** muestra Actualización disponible.

5. Haga clic en **Actualizar** > **Actualizar hosts** en la barra de herramientas.



6. Haga clic en **Iniciar actualización** desde el cuadro de diálogo **Actualización disponible**.
Después de la actualización del host, le solicita que ejecute la acción Reiniciar host.
7. Haga clic en **Reiniciar host** en la barra de herramientas.

Opción 3: Actualizar NetWitness Platform mediante CLI (sin conexión)

Puede usar esta opción si el host del servidor de NW no está conectado a los Servicios de Live.

Antes de comenzar

Asegúrese de haber descargado el siguiente archivo de NetWitness Community (https://community.netwitness.com/) > **Productos > NetWitness Platform** > **Descargas** a un directorio local:

- Si está actualizando de 12.2.0.0, 12.2.0.1, 12.3.0.0 y 12.3.1.0 a 12.4, descargue:

  `netwitness-12.4.0.0.zip`

- Si está usando un repositorio externo, puede actualizarlo con el contenido de la actualización más reciente. Para más información, consulte Instrucciones para el repositorio externo para la actualización de CLI.

Para actualizar los hosts del servidor NW y los servidores de componentes:

Nota: Si copia y pega los comandos desde el archivo PDF al terminal del protocolo SSH de Linux, los caracteres no funcionarán. Sin embargo, puede copiar los comandos desde la página HTML https://community.netwitness.com/t5/netwitness-platform-online/upgrade-tasks-for-12-1-1/ta-p/695018#Option3 y péguelos en la terminal SSH de Linux.

1. Preconfigure los archivos 12.4.0.0 para prepararlos para la actualización. Considere los siguientes escenarios.
   - **Opción 1 (manual)** : Inicie sesión en el Servidor de NetWitness y cree el siguiente directorio:

     `/var/netwitness/tmp/upgrade/12.4.0.0/`
     Luego copie el archivo zip del paquete en el directorio `/var/netwitness/tmp/` del servidor NW y extraiga los archivos del paquete de `/var/netwitness/tmp/` al directorio apropiado mediante el siguiente comando:

`unzip netwitness-12.4.0.0.zip -d /var/netwitness/tmp/upgrade/12.4.0.0`
Asegúrese de eliminar el archivo zip de actualización del directorio de almacenamiento provisional después de extraerlo.

- **Opción 2 (automatizada)** : Inicie sesión en el Servidor de NetWitness y cree el siguiente directorio:
  `/var/netwitness/tmp/upgrade/`
  Luego copie los archivos zip del paquete NetWitness 12.4.0.0 al directorio `/var/netwitness/tmp/` en el servidor de NetWitness.
  Después de esto, ejecute el siguiente comando para extraer, validar e inicializar los archivos zip 12.4.0.0:
  `[root@SA ~]# upgrade-cli-client --init --stage-dir /var/netwitness /tmp/upgrade --download-path /var/netwitness/tmp/ --version 12.4.0.0`
  Una vez que el mensaje **(INFO) Se completó la descarga y extracción de todos los archivos zip de NetWitness necesarios** aparezca en la consola del servidor de administración, solo entonces comenzará el proceso de inicialización.

Nota: Si no recibe el mensaje **(INFO) Se completó la descarga y extracción de todos los zips de NetWitness necesarios**, ejecute el comando anterior nuevamente.

IMPORTANTE: Después del almacenamiento provisional de 12.4.0.0 (usando la opción 2), si la inicialización falla, ejecute el comando `upgrade-cli-client --init --version 12.4.0.0 --stage-dir /var/netwitness/tmp/upgrade`. Si la inicialización se realiza correctamente, ignore el paso 2: Inicializar la actualización a continuación y continúe con los pasos adicionales 3 a 6.

2. Inicialice la actualización mediante el siguiente comando:
   `upgrade-cli-client --init --version 12.4.0.0 --stage-dir /var/netwitness/tmp/upgrade`
3. Actualice el host del servidor NW mediante el siguiente comando:
   `upgrade-cli-client --upgrade --version 12.4.0.0 --host-key <ID / display name / (hostname/ IP address)>`

Nota: Una vez que se activa la actualización, NW Server se reiniciará automáticamente aproximadamente 10 minutos después del proceso de actualización. Se iniciará en el nuevo kernel (4.18 para Alma Linux 8.9).

Precaución: Se recomienda a los usuarios que esperen hasta que la interfaz de usuario esté operativa, lo que puede tardar hasta una hora en completarse. Entre 20 y 30 minutos después de la migración, puede utilizar SSH y verificar si el sistema operativo se migró. Una vez que se completa la migración del sistema operativo, la interfaz de usuario puede tardar al menos 30 minutos en aparecer mientras la actualización de NW se ejecuta en segundo plano.

Se puede realizar un seguimiento del proceso de actualización anterior a través de una consola virtual para máquinas virtuales o una consola remota para servidores con iDRAC.

Una vez que el sistema operativo se haya migrado y pueda conectarse mediante SSH al nodo de administración, ejecute el siguiente comando en el host para confirmar que la migración del sistema operativo se realizó correctamente:

- `cat /etc/redhat-release`
- `AlmaLinux release 8.9 (Midnight Oncilla)`

Precaución: Después de la migración del sistema operativo, reinstale los RPM de terceros que haya instalado anteriormente.

4. Una vez que el servidor de orquestación esté activo, activará automáticamente la actualización de NW a través de chef a la versión de NW deseada. Para comprobar el progreso, conecte SSH al servidor de administración y ejecute el siguiente comando:
   - `orchestration-cli-client --check-admin-upgrade-status`

   Nota: Ejecute el comando anterior solo para el servidor de administrador de NW.
5. Cuando la actualización del host del servidor de NW sea exitosa, reinicie el host desde la interfaz de usuario de NetWitness Platform en la vista Host.
6. (Condicional) Si se implementa el servidor en espera activa, repita los pasos del 1 al 5 en el host del servidor en espera activa.
7. Repita los pasos 3 y 5 para cada host de componentes, pero cambie la dirección IP a la del host de componentes que se actualiza.

Nota: Puede comprobar las versiones de todos los hosts mediante el comando `upgrade-cli-client --list` en el host del servidor de NW. Si desea ver el contenido de la ayuda de `upgrade-cli-client`, utilice el comando `upgrade-cli-client --help`.

Instrucciones para el repositorio externo para la actualización de CLI

Para obtener información sobre cómo configurar un repositorio externo, consulte el **Apéndice A. Configurar un repositorio externo** en la *12.4Guía de actualización para NetWitness Platform*. Las siguientes instrucciones suponen que ya tiene configurado un repositorio externo. Vaya a la página Documentos de todas las versiones de NetWitness y busque guías de NetWitness Platform para solucionar problemas.

1. Preconfigure los archivos 12.4.0.0 para prepararlos para la actualización. Considere los siguientes escenarios.
   - **Si está actualizando desde 12.2.0.0**, **12.2.0.1**, **12.3.0.0** y **12.3.1.0**, solo necesita preparar 12.4.0.0.
     - **Opción 1 (manual)** : Inicie sesión en el Servidor de NetWitness y cree el siguiente directorio:

       `/var/netwitness/tmp/upgrade/12.4.0.0/`
       Luego copie el archivo zip del paquete en el directorio `/var/netwitness/tmp/` del servidor NW y extraiga los archivos del paquete de `/var/netwitness/tmp/` al directorio apropiado mediante el siguiente comando:

       `unzip netwitness-12.4.0.0.zip -d /var/netwitness/tmp/upgrade/12.4.0.0`
       Asegúrese de eliminar el archivo zip de actualización del directorio de almacenamiento provisional después de extraerlo.

- **Opción 2 (automatizada)** : Inicie sesión en el Servidor de NetWitness y cree el siguiente directorio:
  `/var/netwitness/tmp/upgrade/`
  Luego copie los archivos zip del paquete NetWitness 12.4.0.0 al directorio `/var/netwitness/tmp/` en el servidor de NetWitness.
  Después de esto, ejecute el siguiente comando para extraer, validar e inicializar los archivos zip 12.4.0.0:
  ```
  [root@SA ~]# upgrade-cli-client --init --stage-dir /var/netwitness
  /tmp/upgrade --download-path /var/netwitness/tmp/ --version 12.4.0.0
  ```
  Una vez que el mensaje **(INFO) Se completó la descarga y extracción de todos los archivos zip de NetWitness necesarios** aparezca en la consola del servidor de administración, solo entonces comenzará el proceso de inicialización.

Nota: Si no recibe el mensaje **(INFO) Se completó la descarga y extracción de todos los zips de NetWitness necesarios**, ejecute el comando anterior nuevamente.

IMPORTANTE: Después del almacenamiento provisional de 12.4.0.0 (usando la opción 2), si la inicialización falla, ejecute el comando `upgrade-cli-client --init --version 12.4.0.0 --stage-dir /var/netwitness/tmp/upgrade`. Si la inicialización se realiza correctamente, ignore el paso 2: Inicializar la actualización a continuación y continúe con los pasos adicionales 3 a 6.

2. Inicialice la actualización mediante el siguiente comando:
   ```
   upgrade-cli-client --init --version 12.4.0.0 --stage-dir
   /var/netwitness/tmp/upgrade
   ```

3. Actualice el host del servidor NW mediante el siguiente comando:
   ```
   upgrade-cli-client --upgrade --version 12.4.0.0 --host-key <ID / display
   name / (hostname/ IP address)>
   ```

Nota: Una vez que se activa la actualización, NW Server se reiniciará automáticamente aproximadamente 10 minutos después del proceso de actualización. Se iniciará en el nuevo kernel (4.18 para Alma Linux 8.9).

Precaución: Se recomienda a los usuarios que esperen hasta que la interfaz de usuario esté operativa, lo que puede tardar hasta una hora en completarse. Entre 20 y 30 minutos después de la migración, puede utilizar SSH y verificar si el sistema operativo se migró. Una vez que se completa la migración del sistema operativo, la interfaz de usuario puede tardar al menos 30 minutos en aparecer mientras la actualización de NW se ejecuta en segundo plano.

Se puede realizar un seguimiento del proceso de actualización anterior a través de una consola virtual para máquinas virtuales o una consola remota para servidores con iDRAC.

Una vez que el sistema operativo se haya migrado y pueda conectarse mediante SSH al nodo de administración, ejecute el siguiente comando en el host para confirmar que la migración del sistema operativo se realizó correctamente:

- `cat /etc/redhat-release`
- `AlmaLinux release 8.9 (Midnight Oncilla)`

Precaución: Después de la migración del sistema operativo, reinstale los RPM de terceros que haya instalado anteriormente.

4. Una vez que el servidor de orquestación esté activo, activará automáticamente la actualización de NW a través de chef a la versión de NW deseada. Para comprobar el progreso, conecte SSH al servidor de administración y ejecute el siguiente comando:
   - `orchestration-cli-client --check-admin-upgrade-status`

   Nota: Ejecute el comando anterior solo para el servidor de administrador de NW.

5. Cuando la actualización del host del servidor de NW sea exitosa, reinicie el host desde la interfaz de usuario de NetWitness Platform en la vista Host.
6. (Condicional) Si se implementa el servidor en espera activa, repita los pasos del 1 al 5 en el host del servidor en espera activa.
7. Repita los pasos 3 y 5 para cada host de componentes, pero cambie la dirección IP a la del host de componentes que se actualiza.

Nota: Puede comprobar las versiones de todos los hosts mediante el comando `upgrade-cli-client --list` en el host del servidor de NW. Si desea ver el contenido de la ayuda de `upgrade-cli-client`, utilice el comando `upgrade-cli-client --help`.

Opción 4 (opcional): Preconfigurar repositorio de actualización mediante la descarga de paquetes

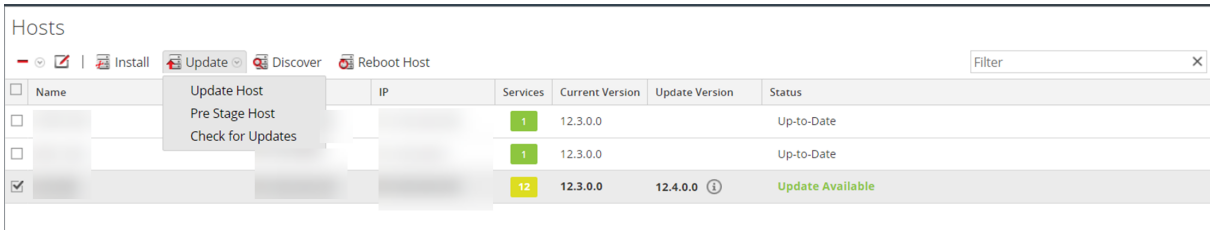
Puede preconfigurar el repositorio de actualizaciones mediante la descarga de los paquetes necesarios (.zip) sin afectar el sistema. Esto minimiza el tiempo de inactividad de la actualización y garantiza que la actualización se complete dentro del tiempo planificado.

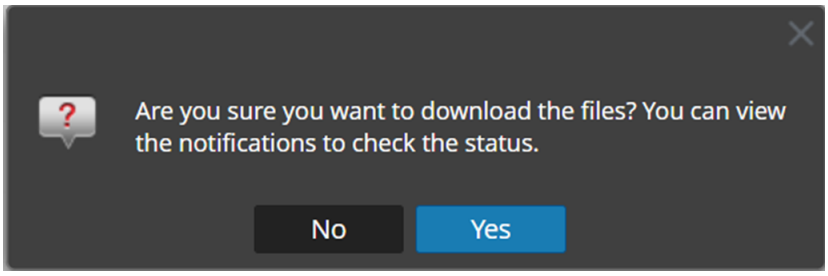
Para preconfigurar el repositorio de actualización y actualizar los hosts:

1. Vaya a  **(Admin) > Hosts**.
2. Haga clic en **Actualizar > Buscar actualizaciones** en la barra de herramientas.

   Todas las versiones de actualización posibles se mostrarán en la lista desplegable Versiones.
3. Haga clic en **Actualizar** > **Preconfigurar host** y seleccione la versión en la columna de versión de actualización.

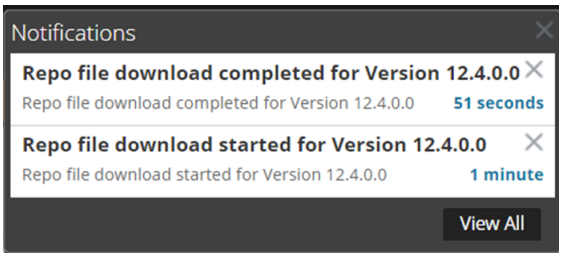
   S muestra un mensaje de confirmación para descargar los archivos.





4. Haga clic en **Sí** para descargar los paquetes de actualización al repositorio.
5. Verifique el estado de la descarga en la bandeja de notificaciones tal como se muestra a continuación.

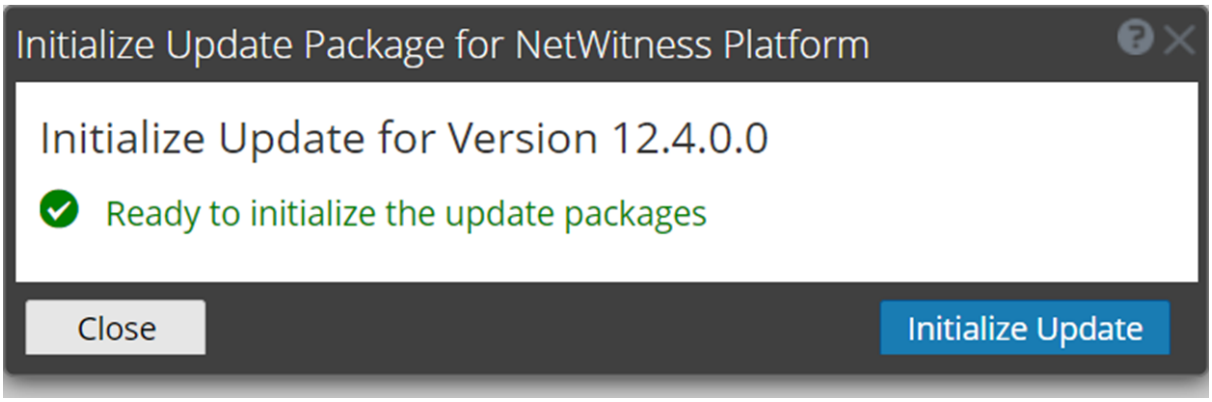
   Las opciones **Preconfigurar host** y **Actualizar host** estarán desactivadas hasta que se complete la configuración previa.



Nota: La versión actual y la versión actualizada en la interfaz de usuario serán la misma durante la configuración previa dado que no es la actualización real. Esto se debe a que solo se descargan los archivos del repositorio y no se realiza ninguna actualización real. La versión cambiará solo después de la actualización.

6. Si la descarga se realiza correctamente, seleccione **Buscar actualizaciones** nuevamente para comenzar con la inicialización.
7. Haga clic en **Iniciar actualización**.

   La inicialización del paquete llevará algún tiempo ya que los archivos son grandes y será necesario descomprimirlos.



IMPORTANTE: Se pueden realizar los pasos de preparación del 1 al 4 para preconfigurar el repositorio en cualquier momento. Sin embargo, el proceso de actualización comienza entre los pasos 5 y 8, por lo que NO debe reiniciar el host ni el servidor jetty durante este momento porque corromperá los archivos .zip.

8. Compruebe el estado de inicialización en la bandeja de notificaciones.
9. Una vez que la inicialización se complete correctamente, haga clic en **Actualizar** > **Actualizar host**.

   Una vez que actualice el host, se le pedirá que reinicie el host.
10. Configure y reinicie el host.

Ejecución de tareas posteriores a la actualización

Este tema enumera las tareas que debe realizar después de actualizar NetWitness Platform. Complete las tareas que se aplican a los hosts de su entorno.

General

Debe configurar Jetty, restaurar el contenido de los servicios principales y también iniciar la captura de red, la captura de registros y la agregación después de actualizar NetWitness Platform.

Configurar Jetty

Para la configuración de Jetty e información relacionada, consulte el tema **Administrar entradas de host personalizadas** en la Guía de mantenimiento del sistema.

Asegúrese de que los servicios se hayan reiniciado y capten y agreguen datos

Asegúrese de que los servicios se hayan reiniciado y estén capturando datos (esto depende de si tiene habilitado o no el inicio automático).

Si es necesario, reinicie la captura y agregación de datos para los siguientes servicios:

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver

Iniciar la captura de red:

1. En el menú de NetWitness Platform, vaya a  (Administrador) > **Servicios**.
   Aparecerá la vista **Servicios**.
2. Seleccione cada servicio **Decoder**.

3. En  (acciones), seleccione **Ver** > **Sistema**.
4. En la barra de herramientas, haga clic en  .

Para iniciar la captura de registros:

1. En el menú de NetWitness Platform, vaya a  (Administrador) > **Servicios**.
   Aparecerá la vista **Servicios**.
2. Seleccione cada servicio **Log Decoder**.
3. En  (acciones), seleccione **Ver** > **Sistema**.
4. En la barra de herramientas, haga clic en  .

Para iniciar la agregación:

1. En el menú de NetWitness Platform, vaya a  (Administrador) > **Servicios**.
   Se muestra la vista **Servicios**.
2. Para cada servicio **Concentrator**, **Broker** y **Archiver**:
   a. Seleccione el servicio.
   b. En  (acciones), seleccione **Ver** > **Configuración**.
   c. En la barra de herramientas, haga clic en 
3. Para Event Stream Analysis (ESA):

   Nota: El modo mixto no es compatible con hosts de ESA en NetWitness Platform versión 11.6 y posterior. El servidor NetWitness, el host primario de ESA y el host secundario de ESA deben estar en la misma versión de NetWitness Platform.

   No se requieren tareas posteriores a la actualización para ESA. Para la solución de problemas de ESA, consulte Información de solución de problemas de ESA.

   Si desea agregar compatibilidad con reglas de contenido de Endpoint, UEBA y Live, debe actualizar las claves de metadatos de los parámetros `multi-valued` y `single-valued` en el servicio de correlación de ESA para incluir todas las claves de metadatos requeridas. No es necesario realizar estos ajustes durante la actualización; podrá realizar los ajustes más tarde en un momento conveniente. Para obtener información detallada e instrucciones, consulte **Actualizar las reglas de ESA para las claves de metadatos de valor único y valor múltiple requeridas** en la Guía de configuración de ESA.

Restaurar el contenido de los servicios principales

Una vez que actualice a 12.4, el contenido de los servicios principales, como archivos de configuración (.cfg), feeds, analizadores y dispositivos de registro, se copian en la ubicación **.tar** de la versión 12.4. de los respectivos componentes como Decoder, Log Hybrid, Network Hybrid y Log Decoder.

La siguiente tabla enumera las rutas de los contenidos de los servicios principales y la ubicación **.tar** de los componentes respectivos donde se copian los contenidos de los servicios principales.

Rutas de contenido de servicios principales	Componentes	Ubicación .tar de los componentes
/etc/netwitness/ng/feeds (feeds)	Decoder	/var/netwitness/decoder/decoder_backupcontent_ccm.tar
/etc/netwitness/ng/parsers (Analizadores)	Log Hybrid	/var/netwitness/logdecoder/logdecoder_backupcontent_ccm.tar
/etc/netwitness/ng/envision/etc/devices (Dispositivos de registro)	Network Hybrid	/var/netwitness/decoder/decoder_backupcontent_ccm.tar
/etc/netwitness/ng/NwDecoder.cfg (Configuration files (.cfg))	Log Decoder	/var/netwitness/logdecoder/logdecoder_backupcontent_ccm.tar

De manera predeterminada, la opción CCM está deshabilitada. Después de actualizar a 12.4, si habilita CCM y pierde el contenido de los servicios principales, puede usar los archivos tar de respaldo para recuperar los datos perdidos. Para obtener más información, consulte https://community.netwitness.com/t5/netwitness-knowledge-base/automatic-backup-of-core-service-content-after-upgrading-core/ta-p/694527.

Event Stream Analysis (ESA)

Después de actualizar a la versión 12.4, todas las implementaciones de ESA se migrarán a la página (**CONFIGURAR**) > **Políticas**. Cada implementación se convertirá en una política y un grupo y estará disponible para administrar solo después de la actualización de los servidores de correlación a la versión 12.4. Asegúrese de planear el proceso de actualización para que los servidores de correlación se actualicen inmediatamente después del servidor Admin. No se podrá acceder a las implementaciones hasta que se actualicen los servidores de correlación correspondientes. Sin embargo, los servidores de correlación seguirán procesando las alertas y los eventos. Verifique si todas las implementaciones de ESA están en buen estado. Para obtener más información, consulte el tema **Ver una implementación** en la *Guía de administración de servicios de Live*.

Nota: Los analistas deben tener los permisos adecuados para ver las reglas de la ESA en las páginas (**CONFIGURAR**) > **Reglas de la ESA** y (**CONFIGURAR**) > **Políticas**. Para obtener más información, consulte la sección **servidor de origen** en el tema **Permisos de función** en la *Guía de administración de usuarios y de la seguridad del sistema*.

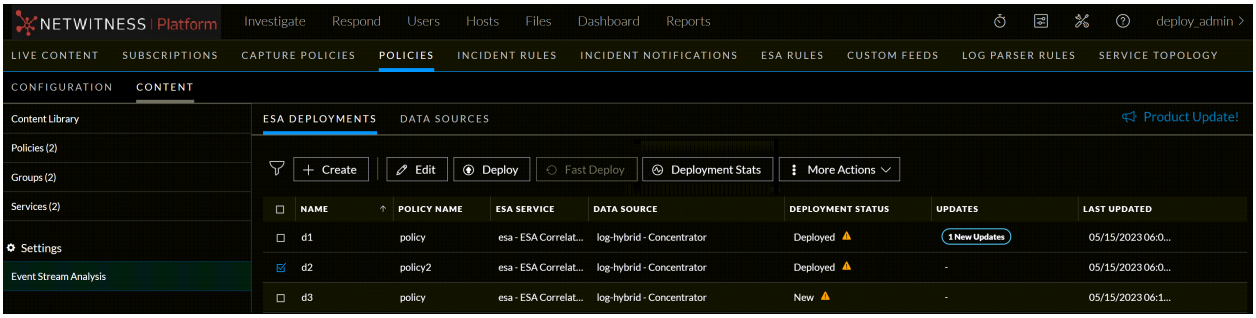
Los estados de las implementaciones anteriores y posteriores a la actualización se representan en la siguiente tabla.

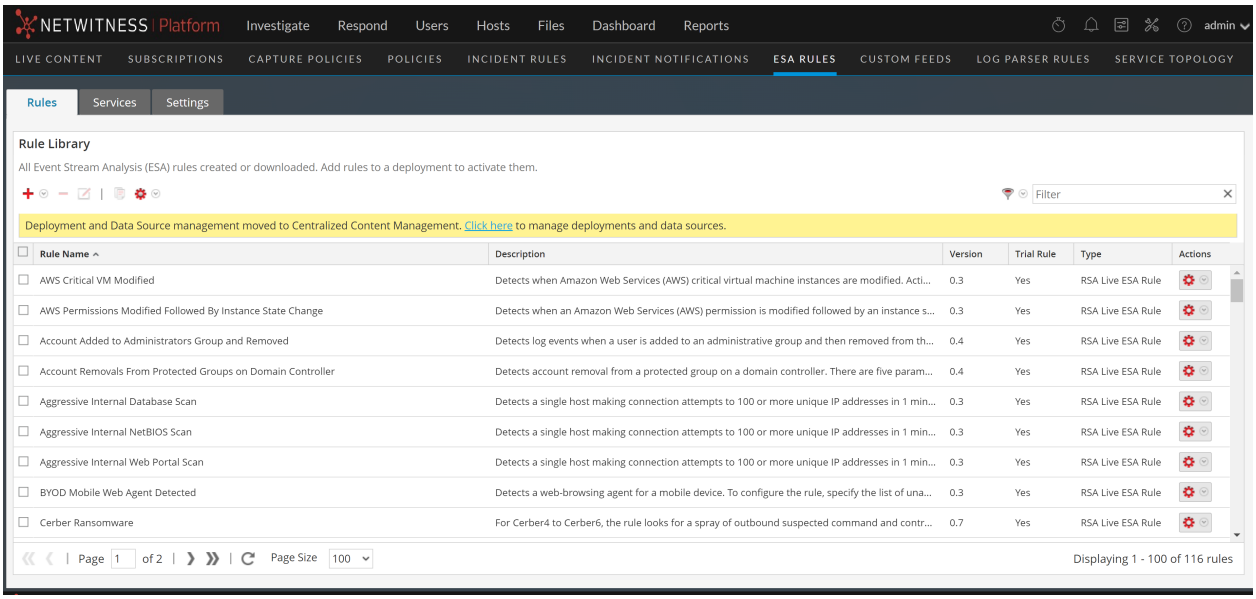
SINo	Estado de implementación previo a la actualización	Estado de implementación posterior a la actualización		
		Crea política	Crea grupo	La política será publicada
1	Implementación saludable	Sí	Sí	Sí
2	Implementación con errores	Sí	Sí	Sí
3	Implementación solo con reglas	Sí	No	No
4	Implementación sin reglas	No	No	No

(Opcional) Con el botón **Fusionar política**, puede fusionar una política que tenga contenido de ESA con una política que no tenga contenido de ESA. Para obtener más información, consulte el tema **Fusionar política con contenido de ESA** en la *Guía de administración de servicios de Live*.

Administrar implementaciones de ESA y orígenes de datos

Solo puede administrar las implementaciones de ESA y los orígenes de datos a través de **Administración de contenido centralizada**. Vaya a la página (**CONFIGURAR**) > **Políticas** > **Contenido** > **Event Stream Analysis** para administrar las implementaciones de ESA y los orígenes de datos. Solo puede gestionar las reglas de ESA en la página **reglas de ESA**. Consulte las siguientes figuras.





Debe actualizar los hosts de ESA inmediatamente después de actualizar el servidor de administración.

Para más información sobre la **Administración de contenidos centralizada** y cómo administrar las implementaciones, consulte la Guía de administración de contenido centralizada para NetWitness.

Respond

El servidor ESA primario debe actualizarse a 12.4 antes de poder completar la siguiente tarea.

Nota: Después de actualizar el servidor NW principal (incluido el servicio del servidor Respond), el servicio del servidor Respond no se vuelve a habilitar automáticamente hasta que el host primario de ESA también se actualice a 12.4. Las tareas posteriores a la actualización de Respond solo se aplican después de que el servicio del servidor de Respond se haya actualizado y se encuentre en el estado habilitado.

(Condicional) Restaure cualquier clave personalizada del servicio Respond en custom_normalize_alerts.js y admita un nuevo origen de datos

Nota: Si no personalizó manualmente custom_normalize_alerts.js, puede omitir esta tarea. Intentamos migrar automáticamente las claves personalizadas. Sin embargo, en caso de fallas, utilice este paso para verificar la integridad de los datos personalizados.

Si agregó claves personalizadas en el archivo `/var/netwitness/respond-server/scripts/custom_normalize_alerts.js` para usar en la normalización personalizada, modifique el archivo `/var/netwitness/respond-server/scripts/custom_normalize_alerts.js` y agregue las claves normalizadas personalizadas del archivo de copia de seguridad automática. El archivo de copia de seguridad se encuentra en `/var/netwitness/respond-server/scripts` y tiene el siguiente formato:

`custom_normalize_alerts.js.bak-<time of the backup>`

En caso de que falle la actualización automática del script, agregue soporte para Netwitness Core y NetWitness Insight actualizando el archivo `custom_normalize_alerts.js` manualmente para admitir estos nuevos orígenes en Respond.

User and Entity Behavior Analytics

Realice las siguientes tareas después de actualizar UEBA a 12.4.

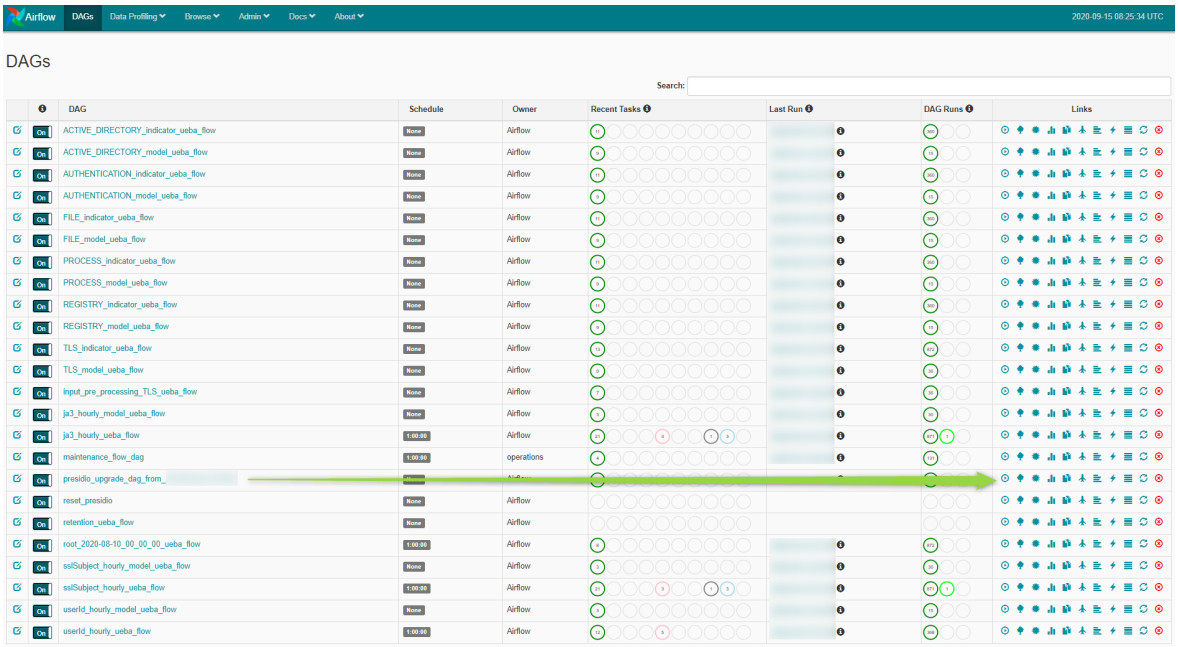
IMPORTANTE: Antes de la actualización, si encontró y resolvió los problemas de falla de la tarea, después de la actualización, debe reemplazar el archivo `authentication.json` antes de ejecutar las tareas posteriores a la actualización. Los problemas de falla de tareas en Airflow y sus soluciones se describen en el tema "Solución de problemas" de la *Guía de configuración de UEBA*.

1. Actualice la configuración de UEBA mediante el siguiente comando desde la máquina de UEBA.
   - `source /etc/sysconfig/airflow`
   - `source $AIRFLOW_VENV/bin/activate`
   - `python /var/netwitness/presidio/airflow/venv39/lib/python3.9/site-packages/presidio_workflows-1.0-py3.9.egg/presidio/resources/rerun_ueba_server_config.py`
   - `deactivate`
2. (Opcional) Actualizar el esquema de procesamiento de UEBA, de ser necesario.

   NetWitness recomienda que la fecha de inicio de UEBA se establezca 28 días antes que la fecha actual. Para los sistemas de UEBA que pretenden procesar datos TLS, debe asegurarse de que la fecha de inicio esté establecida a más tardar 14 días antes de la fecha actual.

   Para obtener más información, consulte la sección "script reset-presidio" en la *Guía de configuración de UEBA*.
3. Ejecutar la actualización de DAG en Airflow.
   - Vaya a la página principal de Airflow `https://<UEBA-host-name>/admin`
   - Escriba el nombre de usuario y la contraseña del administrador.

- Haga clic en **Reproducir** en `presidio_upgrade_dag_from_<previous_version> to_ 12.4`.

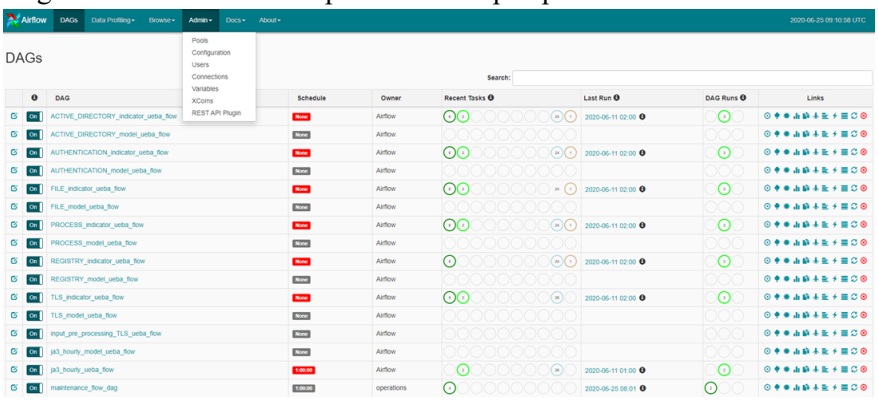


Nota: Aparecerá un círculo verde claro junto a la fila de actualización de DAG durante la actualización. Si el proceso de actualización se completa con éxito, el círculo verde claro cambia a verde. Si se produce un error durante el proceso de actualización, el círculo verde claro cambia a rojo.

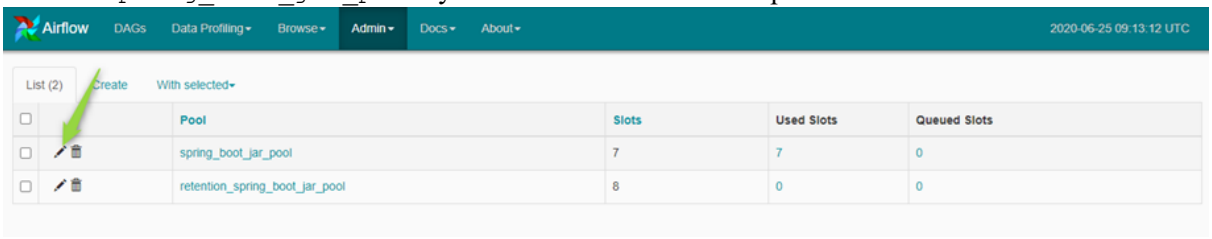
4. Configure las ranuras "Iniciar grupos de archivos JAR" correctas.
   - **Dispositivo físico**: Actualice el valor de la ranura `spring_boot_jar_pool` a 18.
   - **Dispositivo virtual**: Actualice el valor de ranura `spring_boot_jar_pool` a 22.
     Para actualizar las ranuras **Grupos de archivos JAR en Spring Boot**, vaya a la página principal de Airflow, pulse la pestaña **Administrador** en la barra superior y luego pulse **Grupos**.

   a. Para acceder a la interfaz de usuario de Airflow, vaya a `https://<UEBA_host>/admin` e ingrese las credenciales.
      Usuario: admin
      Contraseña: La implementación del entorno y la contraseña del administrador.

b. Haga clic en la marca de lápiz de los Grupos para actualizar los valores de las ranuras.



5. Edite el `spring_boot_jar_pool` y actualice la cantidad de espacios a 22.



Log Collector de Windows heredado

Actualice los certificados heredados Log Collector de Windows con certificados SA actualizados

Pasos posteriores a la actualización:

1. Ejecute el siguiente comando en SA:

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

      Introduzca la siguiente información:

      i. **Nombre de usuario y contraseña de REST de Log Collector de Windows heredado**: Ingrese las credenciales del administrador para el Log Collector de Windows heredado.

      ii. **Nombre de usuario y contraseña del servidor de seguridad**: Ingrese las credenciales del administrador para NetWitness.

2. Reinicie el sistema.

Realice comprobaciones de errores después de la actualización

Debe realizar las siguientes comprobaciones de errores después de actualizar a NetWitness 12.4.

1. Vaya a la vista (Administrador) > **Servicios** para verificar que todos los servicios estén activos (aparecen en verde) después de la actualización.
2. Verifique que los servicios estén actualizados para que coincidan con la versión del host. La versión del servicio en la vista (Administrador) > **Servicios** debe coincidir con la versión del host en la vista (Administrador) > **Hosts** después de la actualización.
3. En la vista (Administrador) > **Servicios**, realice una de las siguientes acciones:
   - Seleccione un servicio de Log Collector y vaya a la vista (acciones) > **Ver** > **Sistema** para verificar si se inició la recopilación de registros requerida. Debe hacer clic en la opción desplegable Collection e ir al protocolo de recopilación correcto para verificar si se inició la recopilación de registros. Si no se inicia la recopilación requerida, seleccione Start junto al protocolo de recopilación requerido de la lista para iniciar la recopilación.
   - Seleccione un servicio de Log Decoder y vaya a la vista (acciones) > **Ver** > **Sistema** para verificar si Log Decoder está capturando los registros correctamente.
   - Seleccione un servicio de decodificador de paquetes y vaya a la vista (acciones) > **Ver** > **Configuración** para comprobar si la interfaz de captura está configurada en la sección **Configuración de Decoder**. Si la interfaz de captura no está configurada, debe seleccionar la interfaz de captura requerida de la lista desplegable para configurarla. Si la interfaz de captura ya está configurada, vaya a la vista (acciones) > **Ver** > **Sistema** del Packet Decoder y compruebe si se ha iniciado la captura. Si la captura no se inicia, haga clic en Start Capture para iniciar la captura de paquetes.
4. Vaya a la vista (Administrador) > **Servicios** > Seleccionar un servicio de Log Decoder o Packet Decoder > (acciones) > **Ver** > **Estadísticas** > **Vista general** para analizar la velocidad de captura actual.
5. Verifique que los Concentrator, Archiver y Broker estén agregando los datos. Asegúrese de poder investigar desde cada Concentrator, Archiver y Broker para validar que esté operativo.
6. Vaya a la vista **Responder** > **Alertas** para verificar si las alertas se activan desde diferentes fuentes.
7. Vaya a la vista (Administrador) > **Salud y bienestar** > **Alarmas** y verifique si el servidor de SMS está en funcionamiento.
8. Vaya a la vista (Administrador) > **Orígenes de eventos** > **Políticas de monitoreo** y verifique si aparecen las políticas configuradas antes de la actualización.

9. Vaya a la vista  (Administrador) > **Salud y bienestar** > **Nueva salud y bienestar** > **Cambiar a Dashboard** > **Elastic** > **Dashboard** y asegúrese de que realiza lo siguiente.
   - Las visualizaciones que creó antes de la actualización aún existen.
   - El servidor de métricas esté en funcionamiento.
   - Las alertas se generan correctamente para los monitores que configuró antes de la actualización.

Instale el servidor de retransmisión 12.4

IMPORTANTE: Después de actualizar EPLH de las versiones 12.2.xx y 12.3.xx a 12.4, debe reinstalar el servidor de retransmisión en la caja EL 8 (Alma Linux), ya que el servidor de retransmisión es un servidor independiente.

Antes de comenzar

- Asegúrese de tener la caja EL 8.
- Realice las siguientes tareas antes de instalar el servidor de retransmisión 12.4:
  1. Actualice NetWitness Platform XDR.
  2. Una vez actualizado el EPLH, descargue el paquete de retransmisión.
  3. Copie el empaquetador a la caja EL 8.
  4. Apague el servidor de retransmisión existente.
  5. Configure la dirección IP de EL 8 reutilizando la dirección IP del servidor de retransmisión existente.

     Una vez que configure la dirección IP de EL 8, instale el servidor de retransmisión. Para obtener más información, consulte la sección **(Opcional) Cómo instalar y configurar el servidor de retransmisión** en la Guía de configuración de Endpoint. Vaya a la página Documentos de todas las versiones de NetWitness y busque guías de NetWitness Platform para solucionar problemas.

Nota: Debe mantener actualizados los parches de seguridad en el servidor de retransmisión.

Actualizar los agentes de Endpoint

Consulte **Actualizar agentes** en la Guía de instalación del agente de Endpoint para NetWitness Platform para obtener instrucciones sobre cómo actualizar los agentes.

Problemas de actualización de solución de problemas

En esta sección se describen los mensajes de error que se muestran en la vista Hosts cuando se producen problemas durante la actualización de versiones de hosts y la instalación de servicios en hosts en la vista Hosts. Si no puede resolver un problema de actualización o instalación con los siguientes consejos de solución de problemas, póngase en contacto con el Servicio al cliente.

En esta sección se describen las instrucciones de solución de problemas para los siguientes errores que pueden ocurrir durante la actualización.

- Información de solución de problemas del sistema operativo AlmaLinux
- Error de contraseña de deploy_admin vencida
- Error de descarga
- Error al implementar la versión <número-versión> Falta actualizar paquetes
- Error de actualización fallida
- Error al actualizar el repositorio externo
- Error actualización del host falló
- Error de falta de paquetes de actualización
- Parche de actualización de servidor que no es de NW
- Error de la línea de comandos al reiniciar host después de actualización
- Reporting Engine reinicia después de la actualización

También se proporcionan instrucciones de solución de problemas para los siguientes hosts y servicios que pueden ocurrir durante o después de una actualización.

- Servicio Log Collector
- Servidor de NW
- Orchestration
- Reporting Engine
- Event Stream Analysis
- Log Collector de Windows heredado

Problema	No se puede iniciar el dispositivo después de la actualización
Solución alternativa	1. Modifique manualmente la línea de inicio de GRUB a `FIPS=0` para que arranque. 2. Desde aquí, deshabilite FIPS con el siguiente comando: `manage-stig-controls --disable-control-groups 3 --host-all` 3. Verifique que se elimine la línea `FIPS=1` de `/boot/grub2/grub.cfg`

- De lo contrario, ejecute el siguiente comando:

  ```
  grub2-mkconfig -o /boot/grub2/grub.cfg
  ```

4. Reinicie.
5. Ejecute el siguiente comando para habilitar el FIPS:

   ```
   manage-stig-controls --enable-control-groups 3 --host-all
   ```

6. Reinicie nuevamente.

Información de solución de problemas del sistema operativo AlmaLinux

Para una mejor comprensión, la actualización del sistema operativo AlmaLinux se puede dividir en 4 partes:

1. Ejecutar la utilidad de comprobación previa para garantizar el estado del sistema y detectar cualquier problema de actualización. Esto se puede hacer en cualquier momento antes de la actualización utilizando la herramienta de comprobación previa independiente de RPM. (es necesario solo en el servidor de NW)

   Los registros se registran aquí: `/var/log/netwitness/precheck-tool/checklist.log`

2. Inicialización o fase inicial (sucede sólo en el servidor de NW)

   En caso de que ocurra cualquier problema durante la fase inicial, consulte estos registros.

   - Registros de salt minion: `/var/log/salt/minion`
   - registros de Implementación y actualización: `/var/log/netwitness/deployment-upgrade/chef-solo.log`

   Nota: Realice el inicio solo cuando planee realizar la actualización real. No se recomienda realizar un inicio sin actualizar el sistema en la misma ventana de cambios.

3. Actualización del sistema operativo de CentOS a AlmaLinux

   Como primer paso de la actualización del sistema operativo, se actualiza salt. Puede ejecutar el siguiente comando para ver que salt se actualiza a la versión 3006:

   ```
   cat /var/log/yum.log | grep salt
   ```

   Puede ver una actualización similar a la siguiente, donde xxx representa el registro de fecha y hora actual:

   ```
   xxx Updated: salt-master-3006.2-0.x86_64
   xxx Updated: salt-api-3006.2-0.x86_64
   xxx Updated: salt-minion-3006.2-0.x86_64
   ```

   Si tiene algún problema con la actualización de salt, verifique:

- /var/log/netwitness/node-infra-server/node-infra-server.log
- /var/log/salt/master
- /var/log/salt/minion

Una vez que se haya actualizado salt, comenzará el proceso de Leapp.

Los registros se pueden ver en `/var/log/salt/minion`:

```
xxx [salt.loaded.ext.module.nw_platform:445 ][INFO ][139407] [1/5]
Searching for leapp config for version: 12.4.0.0

xxx [salt.loaded.ext.module.nw_platform:453 ][INFO ][139407] [2/5]
Retrieving leapp config for version: 12.4.0.0

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'config/12.4.0.0-pre-upgrade.repo'

xxx [salt.loaded.ext.module.nw_platform:467 ][INFO ][139407] [3/5] Running
pre-requisites required to perform leapp upgrade

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/netwitnessmigrate/actor.py'

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/netwitnessmigrate/libraries/netwitnessmigrate.py'

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/netwitnessmigrate.py'

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/addupgradebootentry.py'

xxx [salt.loaded.ext.module.nw_platform:500 ][INFO ][139407] [4/5] Running
leapp pre-upgrade

xxx [salt.loaded.ext.module.nw_platform:503 ][INFO ][139407] [5/5] Running
leapp upgrade
```

En caso de que se encuentre con cualquier problema durante la actualización del sistema operativo, los registros a continuación le resultarán útiles para solucionarlo.

- `/var/log/salt/minion`
- Si la actualización previa falla: `/var/log/leapp/leapp-preupgrade.log`
- Si la actualización de Leapp falla: `/var/log/leapp/leapp-upgrade.log`

Si Leapp falla, `/var/log/leapp/leapp-report.txt` le proporcionará detalles sobre los inhibidores.

Unos minutos después de este registro "Ejecutar actualización de leapp" en /var/log/salt/minion, el sistema se reiniciará y puede tardar entre 20 y 30 minutos en regresar.

Una vez que esté activo, puede confirmar el sistema operativo con el comando cat `/etc/almalinux-release`. Si no muestra la versión de Alma Linux, llame a Servicio al cliente antes de realizar cualquier acción.

Además, si activó la actualización a través de la interfaz de usuario y ve el estado "`Performing OS Migration`" en cualquier NodeX durante más de una hora, verifique los registros de Leapp y comuníquese con Atención al cliente.

4. Actualización del software de NW a 12.4

   Una vez que se haya completado la migración del sistema operativo, comenzará la actualización del software de NW y tardará hasta 30 minutos antes de que la interfaz de usuario esté funcional.

   Puede ver estos registros en `/var/log/salt/minion` cuando se inicia la actualización del software de NW:

   ```
   xxx [salt.loaded.ext.module.nw_platform:276 ][INFO ][14035] Preparing node for upgrade to 12.4.0.0
   ```

   ```
   xxx [salt.loaded.ext.module.nw_platform:280 ][INFO ][14035] [1/2] Searching for yum config for version: 12.4.0.0
   ```

   ```
   xxx [salt.loaded.ext.module.nw_platform:287 ][INFO ][14035] [2/2] Retrieving yum config for version: 12.4.0.0
   ```

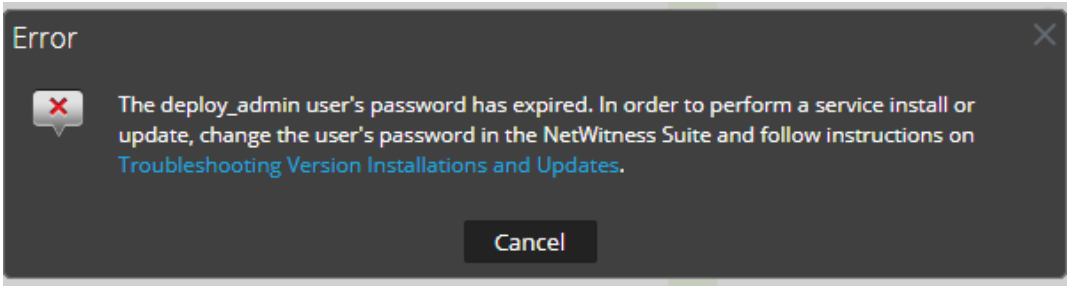
   ```
   xxx [salt.fileclient :1333][INFO ][14035] Fetching file from saltenv 'base', ** done ** 'config/12.4.0.0-pre-upgrade.repo'
   ```

   ```
   xxx [salt.loaded.ext.module.nw_platform:300][INFO ][14035] Upgrading chef package
   ```

   ```
   xxx [salt.loaded.ext.module.nw_platform:300][INFO ][14035] Upgrading rsa-nw-config-management package
   ```

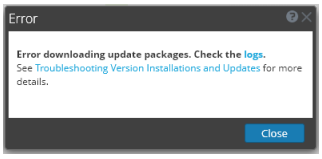
   También puede consultar los registros de administración de configuración en `/var/log/netwitness/config-management/chef-solo.log` o los registros de UI `/var/netwitness/uax/logs/sa.log`

Error de contraseña de usuario de deploy_admin vencida

Mensaje de error	
Causa	La contraseña del usuario `deploy_admin` venció.

Solución	Restablezca la contraseña de `deploy_admin`. Realice lo siguiente.
	1. Solo en el host del servidor de NW, ejecute el siguiente comando.
	`nw-manage --update-deploy-admin-pw`
	`Please enter the new deploy_admin account password: <new-deploy-admin-password>`
	`Please confirm the new deploy_admin account password: <new-deploy-admin-password>`
	2. Revise el resultado del comando `nw-manage --update-deploy-admin-pw` para verificar que la contraseña `deploy_admin` se haya actualizado correctamente en todos los hosts. Si un host de NW está inactivo o falla por cualquier motivo, como se muestra en el resultado del comando `nw-manage --update-deploy-admin-pw`, ejecute `nw-manage --sync-deploy-admin-pw --host-key <host-identifier>` para sincronizar la contraseña entre el servidor de NW y el host que falló una vez que el fallo de comunicación se resuelva.
	3. En el host cuya instalación u orquestación falló, ejecute el comando `nwsetup-tui` y use la nueva contraseña de **deploy_admin** en respuesta a la solicitud de **contraseña de implementación**.

Error de descarga

Mensaje de error	
Problema	Cuando selecciona una versión de actualización y hace clic en **Actualizar** >**Actualizar host**, la descarga comienza, pero no se completa.
Causa	Los archivos de descarga de versiones pueden ser grandes y su descarga puede tardar mucho tiempo. Si se producen problemas de comunicación durante la descarga, esta fallará.
Solución	1. Intente actualizar nuevamente. 2. Si vuelve a fallar con el mismo error, intente actualizar usando los métodos sin conexión como se describe en "Método sin conexión desde la vista de hosts" o "Método sin conexión usando la interfaz de línea de comandos" en la *Guía de actualización para NetWitness Platform*. Vaya a la página Documentos de todas las versiones de NetWitness y busque guías de NetWitness Platform para solucionar problemas. 3. Si aún no puede actualizar, comuníquese con Atención al cliente.

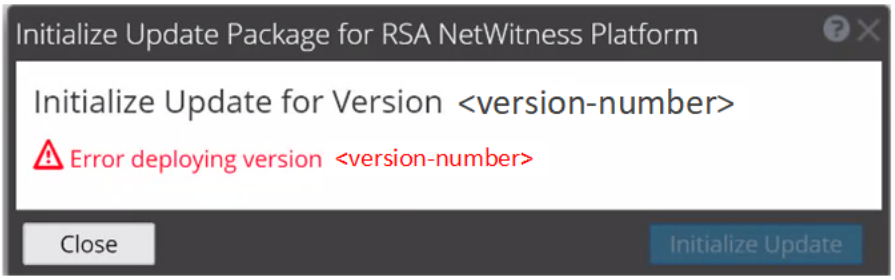
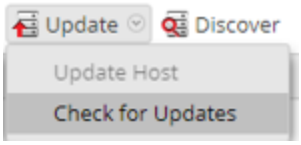
Mensaje de error	Si está actualizando de NetWitness Platform 11.x.x.x a 11.6.x.x o posterior, la actualización de la interfaz de usuario sin conexión falla y muestra el mensaje Error de descarga.

Solución	1. En la interfaz de línea de comandos (CLI), haga lo siguiente:
	a. SSH a servidor de NW.
	b. Ejecute el siguiente comando:
	`upgrade-cli-client --upgrade --host-key <ID, IP address, hostname or display name of host> --version <version number>`
	`For example:`
	`upgrade-cli-client --upgrade --host-key <ID, IP address, hostname or display name of host> --version 11.6.0.0`
	2. Una vez que el servidor de NW se haya actualizado correctamente, inicie sesión en la interfaz de usuario del servidor de NW y vaya a **(Administrador) > Hosts**, donde se le solicitará que reinicie el host.
	3. Haga clic en **Reiniciar host** en la barra de herramientas.
	Para actualizar todos los demás hosts directamente desde la interfaz de usuario:
	1. Haga clic en **Iniciar actualización** desde el cuadro de diálogo **Actualización disponible**.
	Después de la actualización del host, le solicita que ejecute la acción Reiniciar

host.

2. Haga clic en **Reiniciar host** en la barra de herramientas.

Error al implementar la versión <número-versión> Falta actualizar paquetes

Mensaje de error	
Problema	Error al implementar la versión <número-versión> se muestra en el cuadro de diálogo **Inicializar paquete de actualización para NetWitness Platform** una vez que hace clic en **Inicializar actualización** si el paquete de actualización está dañado.
Solución	1. Haga clic en **Cerrar** para cerrar el cuadro de diálogo. 2. Elimine la carpeta de versión de la carpeta de almacenamiento provisional. 3. Asegúrese de que el servicio salt-master esté en ejecución. 4. Vuelva a copiar el archivo zip del paquete de actualización a la carpeta de almacenamiento provisional. 5. En la barra de herramientas de la vista **Hosts**, seleccione **Buscar actualizaciones** nuevamente.  6. Haga clic en **Iniciar actualización**. 7. Haga clic en **Actualizar** > **Actualizar hosts** en la barra de herramientas. 8. Haga clic en **Comenzar actualización** en el cuadro de diálogo **Actualización disponible**. Después de actualizar el host, le solicita que reinicie el host. 9. Haga clic en **Reiniciar** desde la barra de herramientas.

Error de actualización fallida

Mensaje de error	Recibirá un error en el registro de errores similar al siguiente al intentar actualizar a la versión 11.6 o posterior:

	`FATAL: Chef::Exceptions::Package: yum_package[rsa-protobufs-rt] (rsa-audit::packages line 11) had an error: Chef::Exceptions::Package: No version specified, and no candidate version available for rsa-protobufs-rt`
Causa	Compilaciones/rpms personalizadas instaladas para determinados componentes instalados en los hosts, como en el caso de la instalación de Hotfixes.

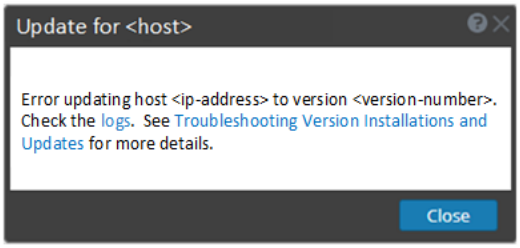
Solución	**Para resolver el problema:**
	1. SSH a Servidor de administración.
	2. Localice el archivo descriptor del componente ejecutando el siguiente comando.
	`cd /etc/netwitness/component-descriptor/`
	3. Abra el archivo descriptor del componente ejecutando el siguiente comando.
	`vi nw-component-descriptor. json`
	4. Busque la sección "paquetes" para el componente que tiene de compilación/rpm personalizado. Por ejemplo, a continuación se muestran los detalles del paquete para el host de Concentrator que tiene una compilación/rpm personalizada.
	`"concentrator": {`
	`"cookbook_name": "rsa-concentrator",`
	`"service_names": ["rsa-nw-concentrator"],`
	`"family": "launch",`
	`"default_port": xxxx, "description": "Concentrator",`
	`"packages":[{ "name": "rsa-nw-concentrator",`
	`"version" : "11.6.0.0-2003001075220.5.cecf24b.e.17.centos"`
	`},`
	5. Borre los detalles completos de la versión incluidos el caracter (,) en la sección paquetes. Por ejemplo, debe verse como se muestra a continuación una vez que borre los detalles de la versión.
	`"packages": [{`
	`"name": "rsa-nw-concentrator"`
	`},`
	Nota: Debe eliminar los detalles de la versión de todos los hosts que tengan compilaciones/rpms personalizados en el descriptor de componentes del servidor de administración.
	6. Ejecute el proceso de actualización otra vez.

Error al actualizar el repositorio externo

Mensaje de error	Recibirá un error similar al siguiente al intentar actualizar a una nueva versión de: `.Repository 'nw-rsa-base': Error parsing config: Error parsing "baseurl = 'https://nw-node-zero/nwrpmrepo /<version-number>/RSA'": URL must be http, ftp, file or https not ""`
Causa	Ruta especificada incorrecta.

Solución	Asegúrese de: • que la URL exista en el host del servidor de NW. • que usó la ruta correcta y eliminó los espacios.

Error actualización del host falló

Mensaje de error	
Problema	Cuando selecciona una versión de actualización y hace clic en **Actualizar** > **Actualizar host**, el proceso de descarga se realiza correctamente, pero el proceso de actualización falla.

Solución	1. Intente aplicar la actualización de la versión al host nuevamente.
	A menudo, esto es todo lo que necesita hacer.
	2. Si aún no puede aplicar la actualización de la nueva versión:
	Supervise los siguientes registros en el servidor de NW a medida que avanza (por ejemplo, ejecute el comando `tail -f` desde la línea de comando):
	`/var/netwitness/uax/logs/sa.log`
	`/var/log/netwitness/orchestration-server/orchestration-server.log`
	`/var/log/netwitness/deployment-upgrade/chef-solo.log`
	`/var/log/netwitness/config-management/chef-solo.log`
	`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`
	El error aparece en uno o más de estos registros.
	3. Si aún no puede aplicar la actualización, recopile los registros del **paso 2** que figura arriba y comuníquese con Atención al cliente.

Mensaje de error	
Problema	Cuando selecciona una versión de actualización y hace clic en **Actualizar** > **Buscar actualizaciones**, se muestra el mensaje de error **no autorizado**. Como resultado, falla la conexión al servicio en vivo.
Solución	1. Asegúrese de que pase la conexión de prueba en Live. 2. Actualizar https://update.netwitness.com/RSA-netwitness en **(Administrador)** >

	Sistema > **Actualizaciones**.
	3. SSH al servidor de administración y copia de seguridad `/etc/default/jetty`.
	4. Actualice la siguiente entrada al final de JAVA_OPTIONS en `/etc/default/jetty`.
	`JAVA_OPTIONS="${JAVA_OPTIONS} -Drsa.nw.legacy.web.server.system.update.repo.url=https://update.netwitness.com/RSA-netwitness/ -Drsa.nw.legacy.system.update.auth.url=https://update.netwitness.com/authenticate "`
	5. Reinicie el servicio jetty. Ejecute el siguiente comando.
	`service jetty restart`

Error de falta de paquetes de actualización

Mensaje de error	**Inicializar actualización para la versión xx.x.x.x** Faltan los siguientes paquetes de actualización Descargar paquetes de NetWitness Link
Problema	Faltan los siguientes paquetes de actualización se muestra en el cuadro de diálogo **Inicializar paquete de actualización para NetWitness Platform** cuando actualiza un host desde **Hosts** se ven sin conexión y faltan paquetes en la carpeta provisional.
Solución	1. Haga clic en Descargar paquetes de NetWitness Community en el cuadro de diálogo **Inicializar paquete de actualización para NetWitness Platform** . Se muestra la página de la comunidad NetWitness que contiene los archivos de actualización para la versión seleccionada. 2. Seleccione los paquetes que faltan desde la carpeta de almacenamiento provisional. Se muestra el cuadro de diálogo **Inicializar paquete de actualización para NetWitness Platform** indicándole que está listo para inicializar los paquetes de actualización.

Parche de actualización de servidor que no es de NW

Mensaje de error	El `/var/log/netwitness/orchestration-server/orchestration-server.log` tiene un error similar al siguiente: **`API|Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgumentException::Version '11.x.x.n' is not supported`**
Problema	Después de actualizar el host del servidor de NW a una versión, debe actualizar todos los hosts de servidores que no son de NW a la misma versión. Por ejemplo, si actualiza el servidor de NW de 11.4.0.0 a 11.6.0.0 o posterior, la única ruta de actualización para los hosts que no son del servidor de NW es la misma versión (es decir, 11.6.0.0). Si intenta actualizar cualquier host de servidor que no es de NW a una versión diferente (por ejemplo, de 11.4.0.0 a 11.4.x.x), se mostrará este mensaje de error.
Solución	Realice cualquiera de las siguientes acciones:

	• Actualice el host de servidor que no es de NW a 11.6.0.0 o posterior. • No actualice el host de servidor que no es de NW (mantenga su versión actual).

Error de la línea de comandos al reiniciar host después de actualización

Mensaje de error	Recibirá un mensaje en la interfaz del usuario que le solicita reiniciar el host después de actualizar y reiniciar el host offline. 
Causa	El error anterior ocurre cuando usa CLI para reiniciar el host. Debe utilizar la interfaz de usuario para reiniciar el host.
Solución	Reinicie el host en la vista **Host** de la interfaz del usuario.

Reporting Engine reinicia después de la actualización

Problema	En algunos casos, después de actualizar a versiones 11.6 o posterior de versiones de 11.x, como 11.4, el servicio de Reporting Engine intenta reiniciar continuamente sin éxito.
Causa	Los archivos de base de datos para gráficos en vivo, estado de alerta o estado de informe no pueden cargarse correctamente porque es posible que los archivos estén dañados.
Solución	**Para resolver el problema:** 1. Compruebe qué archivos de base de datos están dañados. Navegue hasta el archivo ubicado en `/var/netwitness/reserver/rsa/soc/reporting-engine/logs/reporting-engine.log` y verifique los siguientes bloques: • Si el archivo de base de datos de gráficos de Live está dañado, se muestran los siguientes registros: Attempt Failed!!! Clearing pending acquires. While trying to acquire a needed new resource, we failed to succeed more than the maximum number of allowed acquisition attempts (30). Last acquisition attempt exception: org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196] at org.h2.message.DbException.getJdbcSQLException(DbException.java:345) at org.h2.message.DbException.get(DbException.java:168) org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'chartSummaryDAOImpl': Invocation of init method failed; nested exception is com.rsa.soc.re.exception.ReportingException: java.sql.SQLException: Connections could not be acquired from the underlying database! • Si el archivo de base de datos de estado de alerta está dañado, se muestran los siguientes registros:

	Attempt Failed!!! Clearing pending acquires. While trying to acquire a needed new resource, we failed to succeed more than the maximum number of allowed acquisition attempts (30). Last acquisition attempt exception: org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196] at org.h2.message.DbException.getJdbcSQLException(DbException.java:345) at org.h2.message.DbException.get(DbException.java:168) org.springframework.beans.factory.UnsatisfiedDependencyException: Error creating bean with name 'alertStatusHandler': Unsatisfied dependency expressed through field 'alertExecutionStatsDAO'; nested exception is org.springframework.beans.factory.UnsatisfiedDependencyException: Error creating bean with name 'alertExecutionStatsDAOImpl': Unsatisfied dependency expressed through field 'persistedAlertExecutionStatsDAO'; nested exception is org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'persistedAlertExecutionStatsDAOImpl' • Si el archivo de base de datos de estado de informe está dañado, se muestran los siguientes registros: `org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196]` 2. Para resolver el daño del archivo de la base de datos de gráficos en vivo, haga lo siguiente: a. Detenga el servicio Reporting Engine. b. Mueva el archivo `livechart.mv.db` de la carpeta `/var/netwitness/reserver/rsa/soc/reporting-engine/livecharts` a una ubicación temporal. c. Reinicie el servicio Reporting Engine. **Nota:** Algunos datos de gráficos en vivo pueden perderse al realizar los pasos anteriores. 3. Para resolver el daño del archivo de la base de datos de estado de alerta o estado de informe, realice los siguientes pasos: a. Detenga el servicio Reporting Engine. b. Reemplace el archivo de base de datos dañado con el archivo más reciente `alertstatusmanager.mv.db` o `reportstatusmanager.mv.db` de la carpeta `/var/netwitness/reserver/rsa/soc/reporting-engine/archives`. c. Reinicie el servicio Reporting Engine. Para obtener más información, consulte el artículo de la base de conocimientos Reporting Engine se reinicia después de la actualización a NetWitness Platform 11.4.

Problema	Cuando actualice a la versión 11.6 o posterior, el servicio Reporting Engine no reiniciará.
Causa	Es posible que el servicio Reporting Engine no se inicie debido a cualquiera de los siguientes motivos. - workspace.xml no actualizado. - La hora no se convierte correctamente en la base de datos Livechart H2.

Solución	- JCR (repositorio de Jackrabbit) está dañado por violación de la clave principal.
	Para resolver el problema, ejecute la herramienta de recuperación de migración de Reporting Engine (`rsa-nw-re-migration-recovery.sh`) en el servidor de administración donde está instalado el servicio Reporting Engine.
	Nota: Puede encontrar la herramienta de recuperación de migración de Reporting Engine en la siguiente ubicación.
	`/opt/rsa/soc/reporting-engine-<version number>-<Tag>/nwtools`
	Por ejemplo:
	`/opt/rsa/soc/reporting-engine-11.6.0.0-<Tag>/nwtools`
	1. SSH a Servidor de administración.
	2. Descomprima la herramienta RE (Reporting Engine), ejecute el siguiente comando.
	`tar -xvf rsa-nw-re-recovery-tool-bundle.tar`
	3. (Opcional) Si desea descomprimir el archivo de la herramienta RE en algún otro directorio, puede crear un directorio y hacerlo. Ejecute los siguientes comandos.
	`mkdir <NAME OF THE DIRECTORY>`
	`tar -xvf rsa-nw-re-recovery-tool-bundle.tar --directory <PATH OF THE DIRECTORY>`
	4. Ejecute el script, ejecute el siguiente comando.
	`./<PATH OF THE DIRECTORY>/rsa-nw-re-recovery-tool.sh`
	Para obtener más información, consulte el artículo de la base de conocimientos **Herramienta de recuperación de migración de Reporting Engine**.

Servicio Log Collector (`nwlogcollector`)

Los registros de instalación de Log Collector se publican en `/var/log/install/nwlogcollector_install.log` en el host que ejecuta el servicio `nwlogcollector`.

Mensaje de error	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Causa	El Lockbox de Log Collector no se pudo abrir después de la actualización.
Solución	Inicie sesión en NetWitness y restablezca la huella digital del sistema mediante el restablecimiento de la contraseña de valor de sistema estable para el Lockbox como se describe en el tema **Restablecer el valor de sistema estable** bajo el tema **Configurar ajustes de seguridad de Lockbox** en la *Guía de configuración de la recopilación de registros*.

Mensaje de error	`<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found`
Causa	El Lockbox de Log Collector no se configuró después de la actualización.
Solución	Si utiliza un Lockbox de Log Collector, inicie sesión en NetWitness y configure el Lockbox como se describe en el tema **Configurar ajustes de seguridad de Lockbox** de

	la *Guía de configuración de la recopilación de registros*.

Mensaje de error	`<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
Causa	Debe restablecer el campo de umbral de valor estable para el Lockbox de Log Collector.
Solución	Inicie sesión en NetWitness y restablezca la contraseña de valor de sistema estable para el Lockbox como se describe en el tema **Restablecer el valor de sistema estable** bajo el tema **Configurar ajustes de seguridad de Lockbox** en la *Guía de configuración de la recopilación de registros*.

Mensaje de error	Decoder intenta iniciar la captura de eventos pero falla. `Aug 27 01:44:41 nwdecoder NwDecoder[8052]: [Decoder] [failure] The PF_RING driver is not installed.`
Causa	La configuración de captura de Decoder no será válida para clientes que utilicen la captura PF_RING (CentOS) y actualicen directamente a 12.4 (AlmaLinux). Primero, deben migrar dispositivos PF_RING a DPDK y luego actualizar.
Solución	**Para resolver el problema:** Consulte Migrar dispositivos PF_RING a DPDK para obtener instrucciones de migración.

Servidor de NW

Estos registros se publican en `/var/netwitness/uax/logs/sa.log` en el host del servidor de NW.

Problema	Después de la actualización, notará uno de los siguientes: • Los registros de auditoría no se reenvían a la configuración de auditoría global configurada. • El siguiente mensaje se muestra en `sa.log`. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Causa	La migración de la configuración de auditoría global del servidor de NW no pudo migrar de 11.4.x.x u 11.5.x.x. a 11.6.0.0 o posterior.
Solución	1. Acceda mediante el protocolo SSH al servidor de NW. 2. Ejecute el siguiente comando. `orchestration-cli-client --update-admin-node`

Orchestration

Los registros del servidor de Orchestration se publican en `/var/log/netwitness/orchestration-server/orchestration-server.log` en el host del servidor de NW.

Problema	1. Se intentó sin éxito actualizar un host que no es de servidor de NW. 2. La actualización de este host se reintentó y volvió a fallar. Verá el siguiente mensaje en `orchestration-server.log`. `"'file' _virtual_ returned False: cannot import name HASHES""`
Causa	Salt minion se puede haber actualizado y nunca se reinició en el host fallido que no es de servidor de NW

Solución	1. Acceda mediante el protocolo SSH al host que no es de servidor de NW que no se pudo actualizar.
	2. Ejecute los siguientes comandos.
	`systemctl unmask salt-minion`
	`systemctl restart salt-minion`
	3. Reintente la actualización del host que no es de servidor de NW.

Problema	Cuando instala y organiza un Node-X central 12.4 nuevo en el servidor de administración (Node-0) actualizado de 12.0 o versiones anteriores a 12.4, los servicios principales como Concentrator, Log Decoder, Log Collector, Archiver, Decoder, Appliance, Workbench, Warehouse Connector y Broker aparecen inactivos en la columna **Servicios** en la vista **Admin** > **Hosts**. Como resultado, no puede acceder a los servicios principales en la interfaz de usuario. Esto no se aplica si está organizando un Nodo-X central 12.4 nuevo en el servidor de administración 12.4 recién instalado (no actualizado desde 12.0 o versiones anteriores a 12.4).
Causa	El nodo X central 12.4 utiliza un certificado de servidor SA dedicado en lugar del certificado de nodo 0 común bajo sus pares de confianza si se organiza directamente en un host del servidor de administración 12.4 actualizado.

Solución	Antes de iniciar y organizar el host de nodo X central 12.4, ejecute los siguientes comandos.
	1. `mkdir -p /etc/netwitness/platform`
	`touch /etc/netwitness/platform/nw-upgrade-mode`
	Realice esta solución alternativa si solo saltea la solución alternativa anterior (Solución alternativa 1). Ejecute los siguientes comandos antes de arrancar el host de nodo X central 12.4.
	2. `touch /etc/netwitness/platform/nw-upgrade-mode`
	`nw-manage --refresh-host --host-key <core-node-x-salt-minion-`

	uuid> systemctl restart <core-service-name> **Nota:** - Consulte el archivo /etc/salt/minion para buscar <core-node-x-salt-minion-uuid>. - Debe ingresar el nombre del servicio principal, como **nwarchiver** (Archiver), **nwdecoder** (Decoder), **nwlogcollector** (Log Collector), **nwappliance** (Appliance), **nwconcentrator** (Concentrator), **nwlogdecoder** (Log Decoder), **nwbroker** (Broker), **nwworkbench** (Workbench) y **nwwarehouseconnector** (Warehouse Connector) en <core-service-name>.

Servicio Reporting Engine

Los registros de actualización de Reporting Engine se publican en el archivo /var/log/re_install.log en el host que ejecuta el servicio Reporting Engine.

Mensaje de error	<timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [><existing-GB] is less than the required space [<required-GB>]
Causa	La actualización de Reporting Engine falló debido a que no hay espacio en disco suficiente.
Solución	Libere el espacio en disco requerido según se muestra en el mensaje de registro. Consulte el tema **Agregar espacio adicional para informes grandes** de la *Guía de configuración de Reporting Engine* para obtener instrucciones sobre cómo liberar espacio en disco.

Event Stream Analysis

Problema	Después de actualizar a la versión 12.4 o posterior, el servidor de correlación de ESA no agrega eventos de los orígenes de datos configurados.
Mensaje de error	Invalid username or password at com.rsa.netwitness.streams.base.RecordSourceSubscription.run (RecordSourceSubscription.java:173)
Solución	**Para resolver el problema:** En la interfaz de usuario NetWitness, 1. Vaya a (**CONFIGURAR**) > **Políticas** > **Contenido** > **Event Stream Analysis** > **Orígenes de datos**. Se muestra el panel **Orígenes de datos**. 2. Seleccione el origen de datos y haga clic en **Editar origen de datos** en la barra de herramientas. Se muestra el cuadro de diálogo **Editar origen de datos**.

	3. En el cuadro de diálogo **Editar origen de datos**, realice una de las siguientes acciones: • Seleccione **Autenticación de confianza**. • Seleccione **Usar credenciales** e ingrese el nombre de usuario y la contraseña. 4. Haga clic en **Probar conexión** para asegurarse de que pueda comunicarse con el servicio ESA y luego haga clic en **Aceptar**. **Nota:** Realice el procedimiento anterior para todos los orígenes de datos configurados. 5. Realice todas las implementaciones asociadas con los orígenes de datos editados en el panel **Orígenes de datos** luego de terminar de realizar cambios en los orígenes de datos.

Log Collector de Windows heredado

Problema	• Log Collector de Windows heredado aparece como inactivo después de la actualización de SA a la versión 12.4 y Log Collector de Windows heredado a las versiones 11.6.x u 11.7.x. • Log Collector de Windows heredado aparece como inactivo cuando la pila se actualiza a 12.4.
Causa	Actualización del certificado en el nodo SA.
Solución	Consulte la sección Log Collector de Windows heredado en Ejecución de tareas posteriores a la actualización.

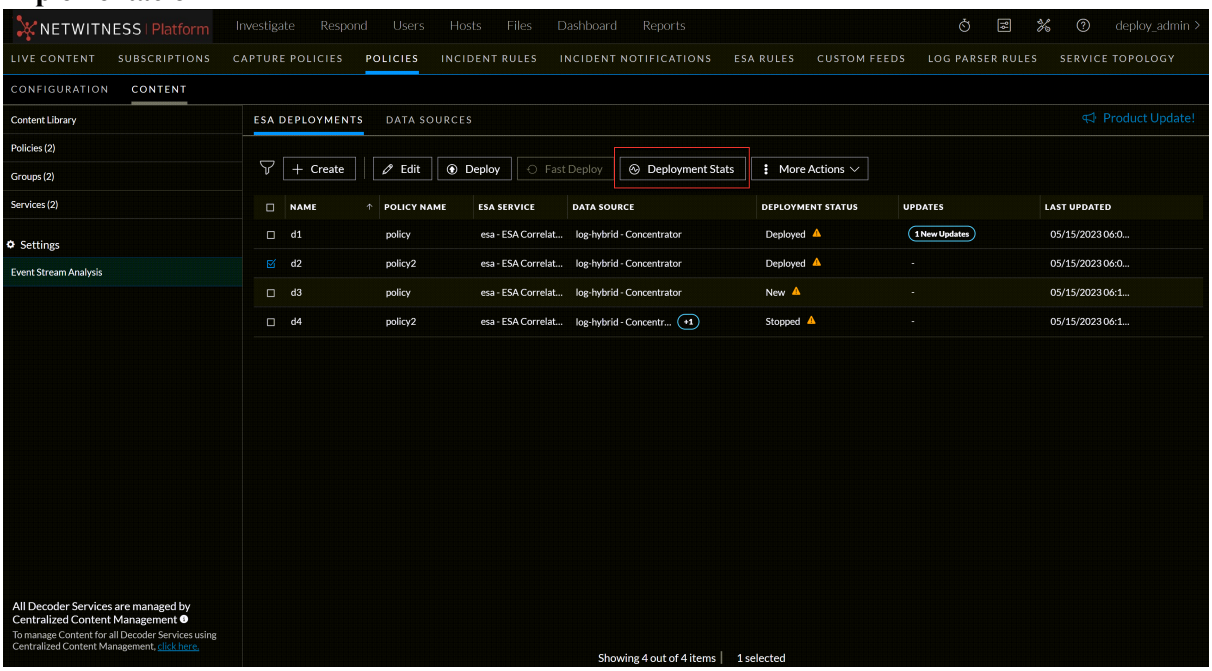
Información de solución de problemas de ESA

Las reglas de la ESA no crean alertas

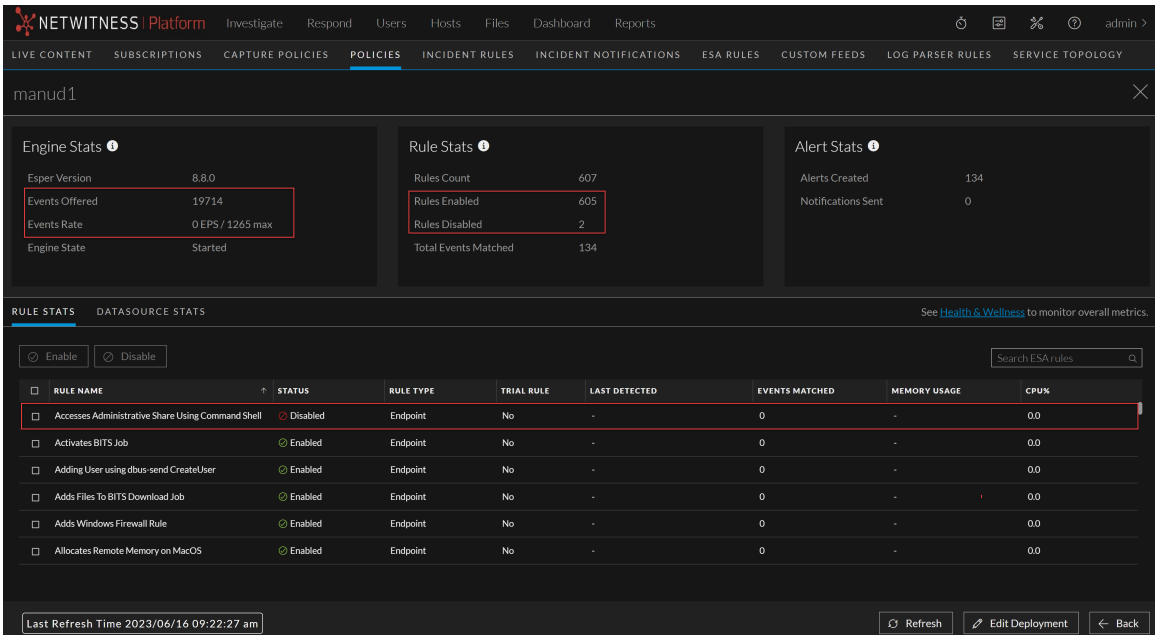
Si no ve ninguna alerta, verifique el estado de las implementaciones de reglas de ESA.

1. Vaya a (**CONFIGURAR**) > **Políticas** > **Contenido** > **Event Stream Analysis** > **Implementaciones de ESA**.
   Aparecerá el panel **Implementación de ESA**.

2. Seleccione la implementación requerida de la lista y haga clic en la pestaña **Estadísticas de implementación**.



3. Se muestra la página Estadísticas de implementación, que muestra el estado de sus servicios e implementaciones de ESA.
4. Para cada regla de implementación de ESA:
   a. En la sección **Estadísticas del motor**, consulte los **Eventos ofrecidos** y la **Tarifa ofrecida**. Estos confirman que los datos se están agregando y analizando correctamente. Si ve 0 en Eventos ofrecidos, no ingresará nada para la implementación.
   b. En la sección **Estadísticas de reglas**, mire las **Reglas habilitadas** y **Reglas deshabilitadas**. Si hay reglas deshabilitadas, consulte la sección **Estadísticas de reglas implementadas** a continuación para ver los detalles de las reglas deshabilitadas. Las reglas deshabilitadas se muestran con un círculo blanco. Las reglas habilitadas se muestran con un círculo verde.



5. Si observa cualquier regla deshabilitada que debería habilitarse:

   a. Vaya a la pestaña  **(Configurar) > Reglas de ESA > Reglas** y vuelva a implementar las implementaciones de reglas de ESA que contienen reglas deshabilitadas.

   b. Vuelva a la pestaña **Servicios** y verifique si las reglas aún están deshabilitadas. Si las reglas aún están deshabilitadas, verifique los archivos de registro del servicio de correlación de ESA, que se encuentran en `/var/log/netwitness/correlation-server/correlation-server.log`.

Nota: Para evitar la sobrecarga de procesamiento innecesario, se eliminó la opción Omitir mayúsculas y minúsculas del cuadro de diálogo Desarrollador de reglas de ESA - Crear una declaración para claves de metadatos que no contienen valores de datos de texto. Durante la actualización a 11.4 o posterior, NetWitness Platform no modifica las reglas existentes para la opción Omitir mayúsculas y minúsculas. Si una regla existente del Desarrollador de reglas tiene la opción Omitir mayúsculas y minúsculas seleccionada para una clave de metadatos que ya no está disponible, ocurrirá un error si intenta editar la declaración e intenta guardarla nuevamente sin borrar la casilla de verificación.

Ejemplo de mensaje de advertencia del servidor de correlación de ESA por claves de metadatos faltantes

Si ve un mensaje de advertencia en los registros de errores del servidor de correlación de ESA, eso significa que hay una diferencia entre el parámetro `default-multi-valued` y los valores de claves de metadatos `multi-valued parameter`, las reglas de contenido nuevas de Endpoint, UEBA y Live no funcionarán. Completar el procedimiento **Actualizar las claves de metadatos de parámetros de valor múltiple y de valor único para las últimas reglas de contenido de Endpoint, UEBA y RSA Live** en la *Guía de configuración de ESA* debería solucionar el problema.

Ejemplo de mensaje de advertencia de valor múltiple

```
2019-08-23 08:55:07,602 [ deployment-0] WARN Stream|[alert, alert_id,
browserprint, cert_thumbprint, checksum, checksum_all, checksum_dst, checksum_
src, client_all, content, context, context_all, context_dst, context_src, dir_
path, dir_path_dst, dir_path_src, directory, directory_all, directory_dst,
directory_src, email_dst, email_src, feed_category, feed_desc, feed_name,
file_cat, file_cat_dst, file_cat_src, filename_dst, filename_src, filter,
function, host_all, host_dst, host_orig, host_src, host_state, ip_orig, ipv6_
orig, OS, param, param_dst, param_src, registry_key, registry_value, risk,
risk_info, risk_suspicious, risk_warning, threat_category, threat_desc,
threat_source, user_agent] are still MISSING from multi-valued
```

Ejemplo de mensaje de advertencia de valor único

```
2019-08-23 08:55:07,602 [ deployment-0] WARN Stream|[accesses, context_target,
file_attributes, logon_type_desc, packets] are still MISSING from single-
valued
```

Utilice el portal de NetWitness Community para obtener ayuda

Puede utilizar el portal de NetWitness Community para buscar documentos específicos, encontrar información relacionada con el fin del ciclo de vida de los dispositivos y leer blogs.

Recursos de autoayuda

Hay varias opciones que le brindan ayuda según la necesite para instalar y usar NetWitness:

- Consulte la documentación para conocer todos los aspectos de NetWitness aquí: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation
- Utilice los campos **Buscar** y **Crear una publicación** en el portal de NetWitness Community para buscar información específica aquí: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
- Ver la NetWitness base de conocimientos: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base
- consulte la sección Solución de problemas en las guías.
- Consulte también Publicaciones del blog de NetWitness® Platform.
- Si necesita más ayuda, póngase en contacto con el servicio de soporte de NetWitness.

Comuníquese con Soporte de NetWitness

Si se comunica con el soporte de NetWitness, debe encontrarse en su computadora. Prepárese para proporcionar la siguiente información:

- Número de versión de la aplicación o el producto NetWitness Platform que está usando.
- El tipo de hardware que está usando.

Use la siguiente información de contacto si tiene preguntas o necesita ayuda.

Portal de NetWitness Community	https://community.netwitness.com En el menú principal, haga clic en **Soporte > Portal de casos > Ver mis casos**.
Contactos internacionales (cómo comunicarse con soporte de NetWitness)	https://community.netwitness.com/t5/support/ct-p/support
Comunidad	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
Actualización de NW	https://update.netwitness.com

UI de Live	https://live.netwitness.com

Comentarios sobre la documentación del producto

Puede enviar un correo electrónico a nwdocsfeedback@netwitness.com para proporcionar comentarios sobre la documentación de NetWitness Platform.