NetWitness® Plataforma

Versión 12.4.0.0

Notas de la versión

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

Novedades de la versión 12.4.0.0

Las notas de la versión de NetWitness 12.4.0.0 describen nuevas funciones, mejoras, reparaciones de seguridad, rutas de actualización, problemas resueltos, problemas conocidos, funcionalidad al final del ciclo de vida, números de compilación y recursos de autoayuda.

Mejoras

Las siguientes secciones son una lista completa y una descripción de las mejoras a capacidades específicas:

- Actualización
- Funcionalidad SASE
- Investigate
- Respond
- Acciones de respuesta
- Insight
- User and Entity Behavior Analytics
- Terminal
- Administración de contenido centralizada (CCM) basada en políticas
- Servicios de Concentrator, Decoder, Log Collector y Archiver
- Integraciones de registros
- Seguridad

Para localizar los documentos a los que se hace referencia en esta sección, consulte https://community.netwitness.com/t5/netwitness-platform-online/netwitness-platform-all-documents/ta-p/676246.

La sección Documentación del producto tiene enlaces a la documentación de esta versión.

Actualización

La siguiente sección describe la nueva mejora para Actualización:

Migración del sistema operativo Alma

RedHat anunció que CentOS Linux 7 llegará al final del ciclo de vida (EOL) el 30 de junio de 2024. Para abordar este cambio, NetWitness Platform ahora está integrada con la nueva versión, AlmaLinux. Cuando actualice a la versión NetWitness 12.4, se migrará automáticamente de CentOS 7.9 a AlmaLinux 8.9. El proceso de actualización de NetWitness Platform 12.4 es sencillo y regular, como cualquier otra actualización anterior. No es necesario seguir ningún procedimiento específico para actualizar al sistema operativo AlmaLinux.
AlmaLinux proporciona varios beneficios clave y nuevas características:

- La actualización a AlmaLinux es un proceso inherentemente automatizado sin intervención manual.
- Viene con una herramienta previa a la actualización que ayuda a los administradores a descubrir y mitigar problemas antes de ejecutar el proceso de actualización real.
- Ahorra tiempo y esfuerzos administrativos.
- Mantiene el control sobre las aplicaciones instaladas.
- Conserva la mayor parte de la información de configuración.

NetWitness Platform agiliza el proceso de actualización, ahorra tiempo y recursos y mantiene el control sobre las aplicaciones y configuraciones instaladas al migrar de CentOS 7.9 a AlmaLinux 8.9.

Funcionalidad SASE

La siguiente sección describe la nueva mejora para SASE:

Integraciones de NetWitness SASE

- **Integración de NetWitness SASE con Palo Alto Networks:** presenta la integración de NetWitness con Palo Alto Prisma SASE para proporcionar visibilidad completa de la red y los registros. Con esta integración técnica personalizada, los usuarios de NetWitness obtienen información sobre el comportamiento y la comunicación entre dispositivos y servicios en redes remotas y distribuidas en implementaciones en las instalaciones, híbridas y en la nube. La integración NetWitness-Palo Alto SASE permite a los clientes aprovechar la flexibilidad de SASE y sus ventajas de seguridad inherentes, manteniendo al mismo tiempo una visibilidad completa para la detección y respuesta a amenazas.
- **Integración de NetWitness SASE con Symantec de Broadcom (modo de vista previa privada):** presenta la integración de NetWitness con Symantec de Broadcom SASE para proporcionar visibilidad completa de la red y los registros. Con esta integración técnica personalizada, los usuarios de NetWitness obtienen información sobre el comportamiento y la comunicación entre dispositivos y servicios en redes remotas y distribuidas en implementaciones en las instalaciones, híbridas y en la nube. La integración NetWitness-Broadcom SASE permite a los clientes aprovechar la flexibilidad de SASE y sus ventajas de seguridad inherentes, manteniendo al mismo tiempo una visibilidad completa para la detección y respuesta a amenazas.

  Nota: En la versión 12.4, la integración de NetWitness SASE con Symantec de Broadcom está en modo de vista previa privada.

Para obtener más información, consulte la *Guía de configuración de Broadcom SASE para 12.4* y la *Guía de configuración de Palo Alto Prisma SASE para 12.4*.

Configuración de nube híbrida NetWitness SASE

Los administradores ahora pueden optar por un modelo de nube híbrida para SASE. La configuración de la nube híbrida de SASE es un diseño basado en datos. La nube híbrida SASE proporciona comunicaciones más eficientes y seguras entre los componentes de NetWitness Platform. El servidor de administración de NetWitness contiene un script nw-create-cloud-hybrid, que implementará la red de superposición de NetWitness y los nodos de NetWitness definidos en sus respectivas regiones en Google Cloud Platform (GCP). La red entre iguales de NetWitness (nw-ppn) proporciona una comunicación segura, autenticada mutuamente y basada en PKI entre los componentes de NetWitness.

Para más información, consulte la *Guía de instalación para 12.4*.

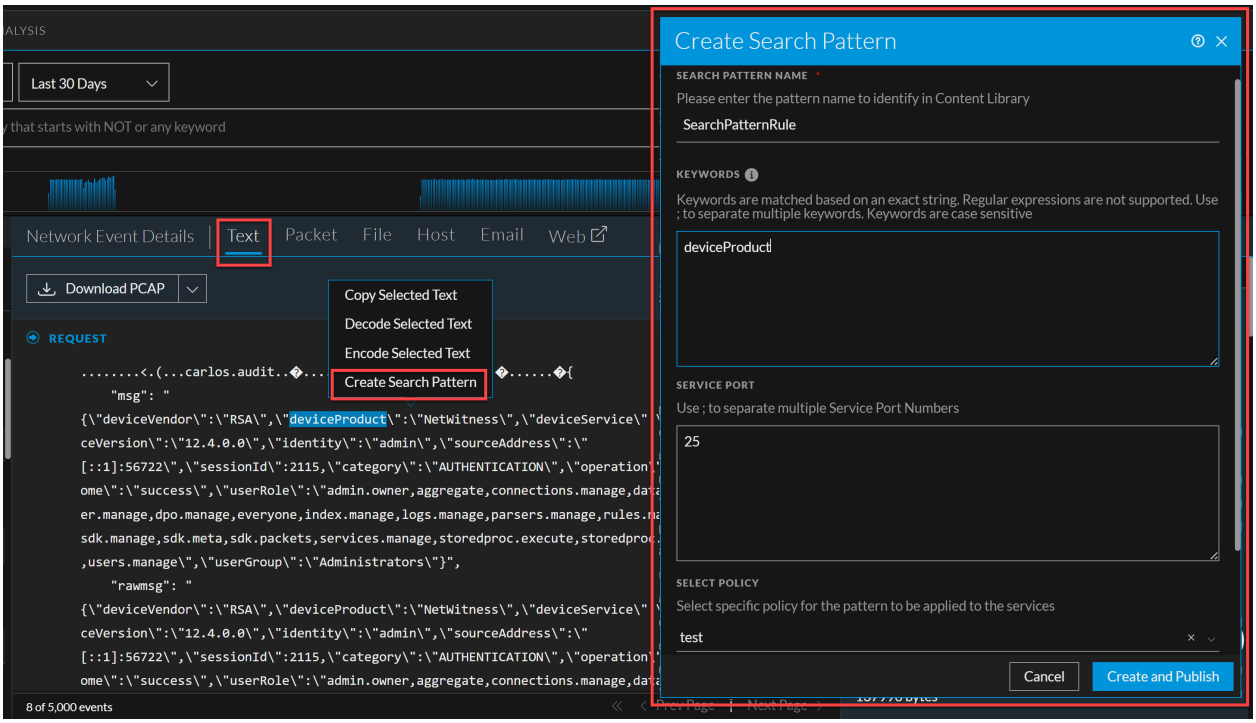
Investigate

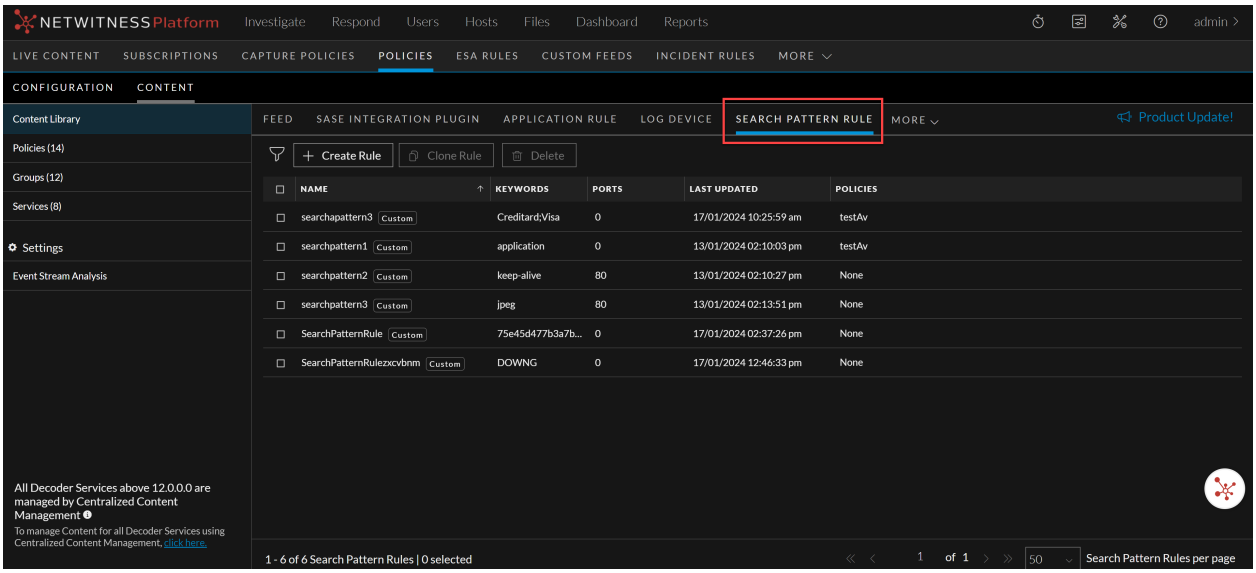
La siguiente sección describe las nuevas mejoras para el componente Investigate:

Creación de un Parser de red interactivo

En la vista **Investigar** > **Eventos**, los usuarios pueden convertir los patrones exactos seleccionados o las palabras clave encontradas en el tráfico de red que revisan en la reconstrucción de la sesión de texto en un analizador de red. Este proceso simplificado permite al usuario generar meta datos para desencadenar un incidente (por ejemplo, una detección futura) sin comprender cómo crear el analizador.

Los usuarios también pueden crear un analizador de red utilizando palabras clave de la vista **(Configurar)** > **Políticas** > **Biblioteca de contenido** > **Más** > **Regla de patrón de búsqueda**.

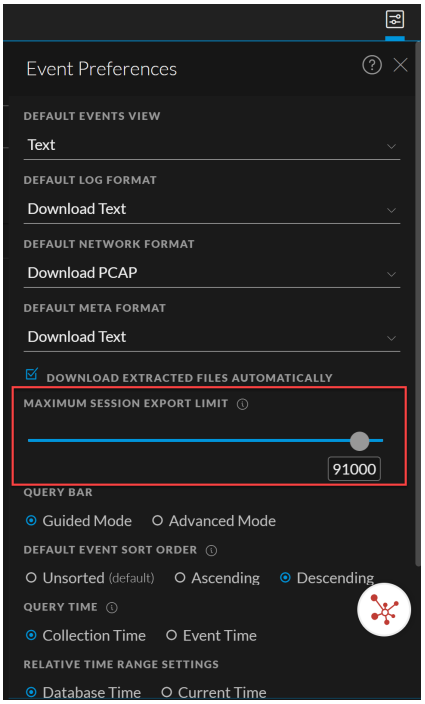




Para más información, consulte el tema **Crear un patrón de búsqueda en la pestaña Texto** en la *Guía del usuario de NetWitness Investigate* y el tema **Administrar regla de patrón de búsqueda** en la *Guía de gestión de contenido centralizada basada en políticas*.

Descargar más sesiones de las que se muestran en la tabla de eventos

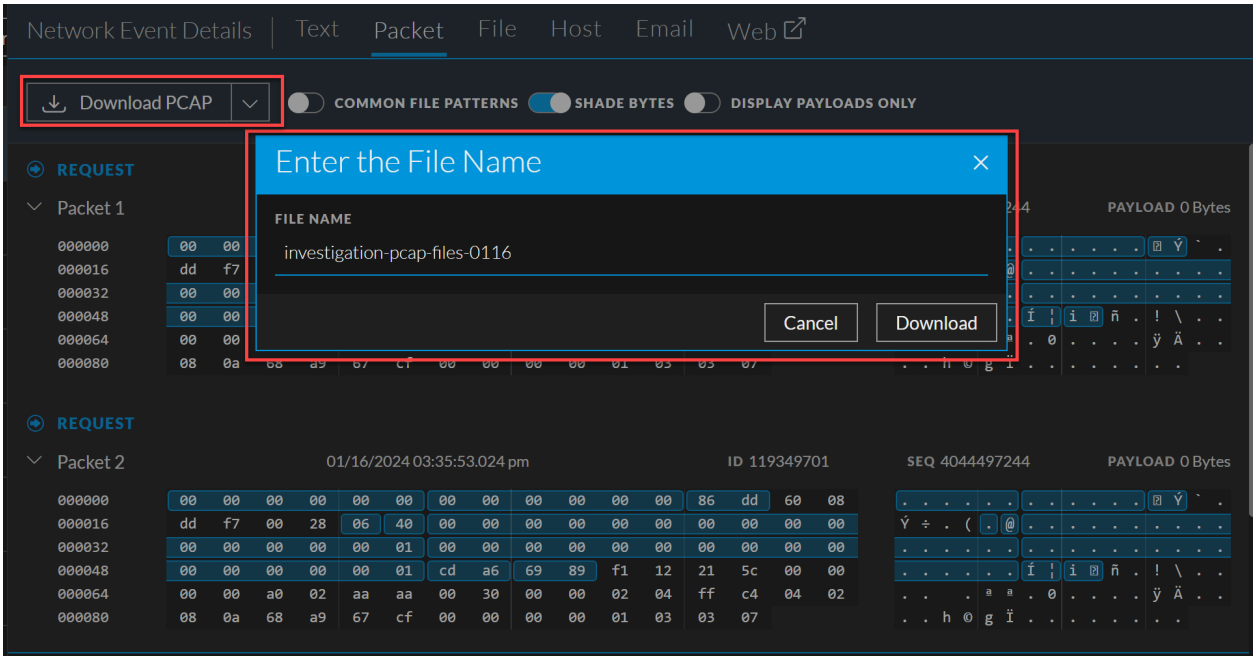
Se ha agregado una nueva preferencia de usuario, **Límite máximo de exportación de sesiones**, al panel **Preferencias de eventos** en la vista **Investigar** > **Eventos**. Los analistas pueden usar esta configuración para ajustar la cantidad de sesiones disponibles para exportar usando las opciones del menú **Descargar todo**. Esta mejora hace que la cantidad de sesiones exportadas sea independiente de la cantidad de sesiones que se muestran en la tabla Eventos.



Para obtener más información, consulte el tema **Establecer preferencias de usuario para la vista de eventos** en la *Guía del usuario de NetWitness Investigate*.

Opción para descargar archivos con nombres personalizados

Los analistas ahora pueden usar nombres personalizados al descargar archivos de eventos desde la vista del panel **Eventos**. Los nombres personalizados facilitan la organización y gestión de archivos de eventos descargados, lo que ahorra tiempo y esfuerzo a los analistas.



Para obtener más información, consulte **Descargar datos en la vista Eventos** en la *Guía del usuario de NetWitness Investigate*.

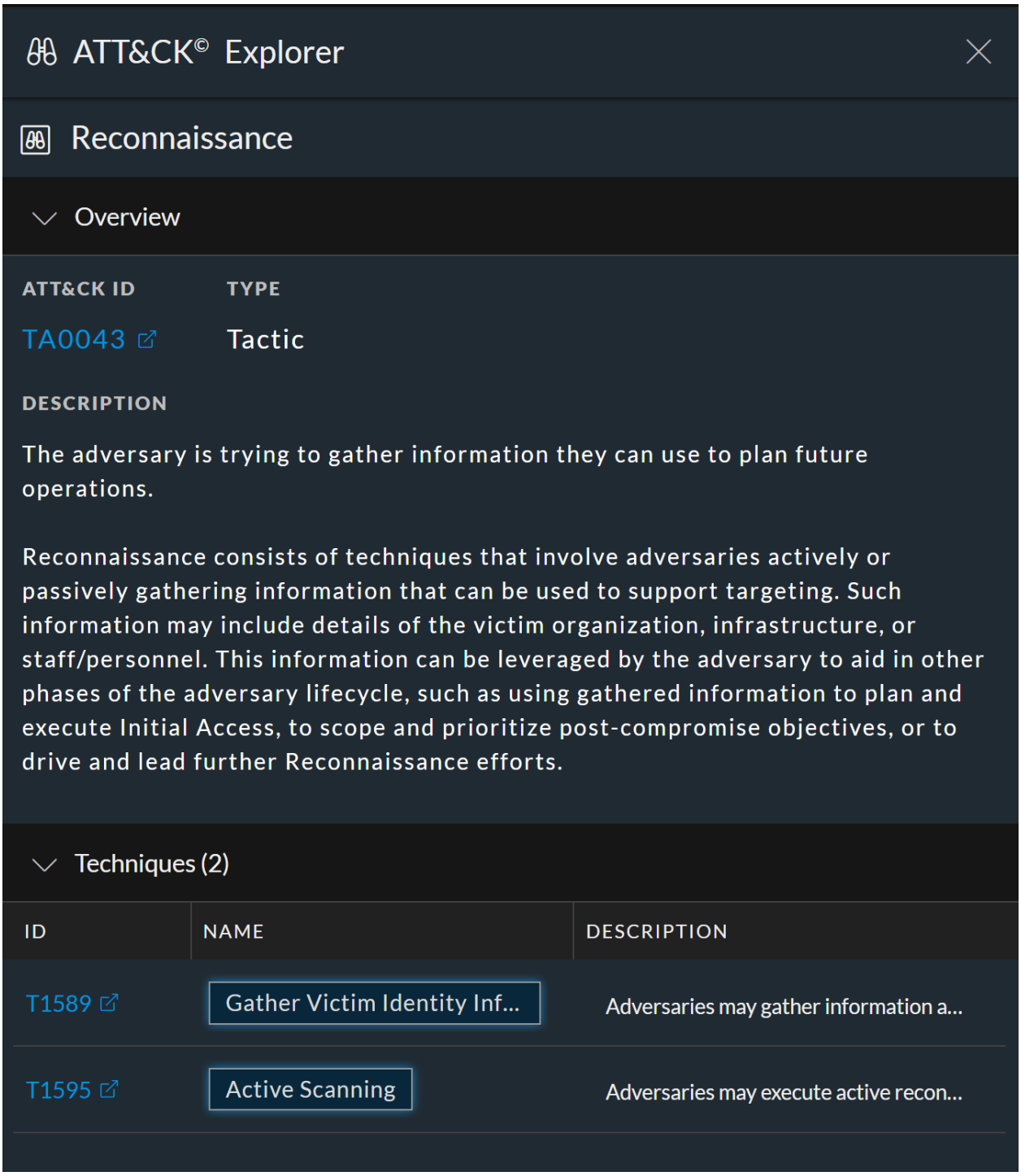
Respond

Las siguientes secciones describen las nuevas mejoras para el componente Respond:

Integración de MITRE ATT&CK® con NetWitness

MITRE ATT&CK® es una base de conocimientos seleccionada sobre técnicas y tácticas del adversario. Proporciona un nivel apropiado de categorización para la acción del adversario y formas específicas de defenderse contra ella. Los analistas pueden ver la lista de alto nivel de tácticas, técnicas y subtécnicas específicas junto con sus detalles y aprender cómo las amenazas y vulnerabilidades potenciales en su entorno están asociadas con el marco MITRE ATT&CK.

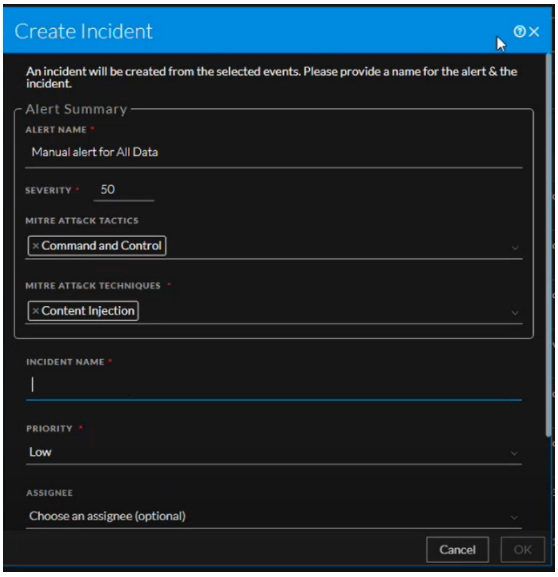
El nuevo panel **ATT&CK© Explorer** proporciona información sobre las tácticas y técnicas del adversario asociadas con los incidentes en la vista **Respond**.



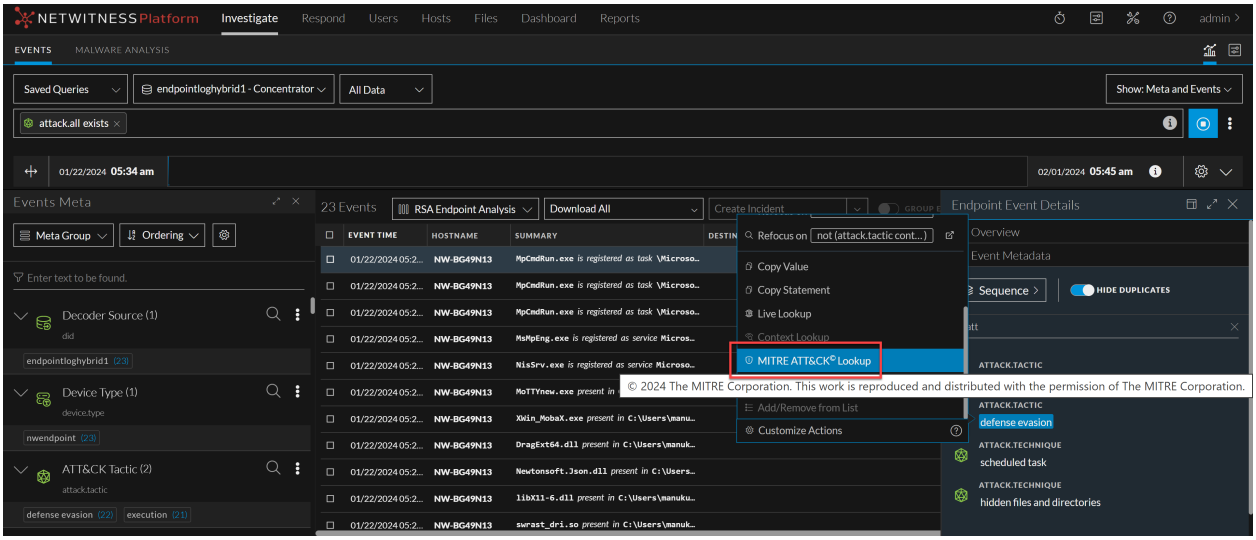
NetWitness Live está integrado con el marco MITRE ATT&CK para ayudar a los analistas a ver las tácticas y técnicas de MITRE ATT&CK asociadas con las **Reglas de aplicación** y **Reglas de Event Stream Analysis**. El panel derecho de Detalles del servicio (**(Configurar)** > **Políticas** > **Contenido** > **Biblioteca de contenido** > **Regla de aplicación** o **Regla de Event Stream Analysis** > haga clic en una fila > Detalles del servicio (panel derecho) mejoró para proporcionar información sobre las tácticas y técnicas de MITRE ATT&CK.

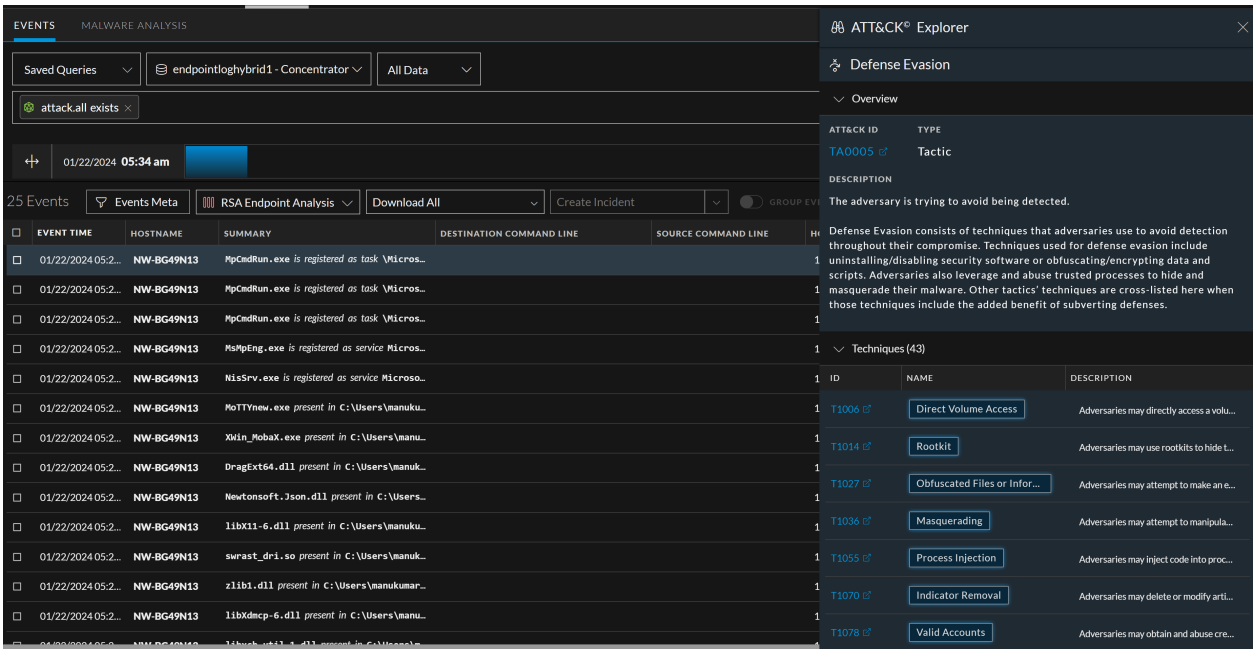
Puede etiquetar tácticas y técnicas de MITRE ATT&CK mientras crea una **Regla de aplicación** o **Regla de Event Stream Analysis**.

También puede seleccionar las tácticas y técnicas de MITRE ATT&CK mientras crea un incidente desde la vista **Investigate** > **Eventos**.



Con esto, las claves de metadatos **ATTACK.TACTIC** y **ATTACK.TECHNIQUE** en el panel **Metadatos de eventos** ha mejorado con la integración de **MITRE ATT&CK© Lookup** para ayudarle a obtener más información sobre la táctica y técnica específicas asociadas con el evento.





Aparece el nuevo panel **ATT&CK© Explorer** al hacer clic en **MITRE ATT&CK© Lookup**.

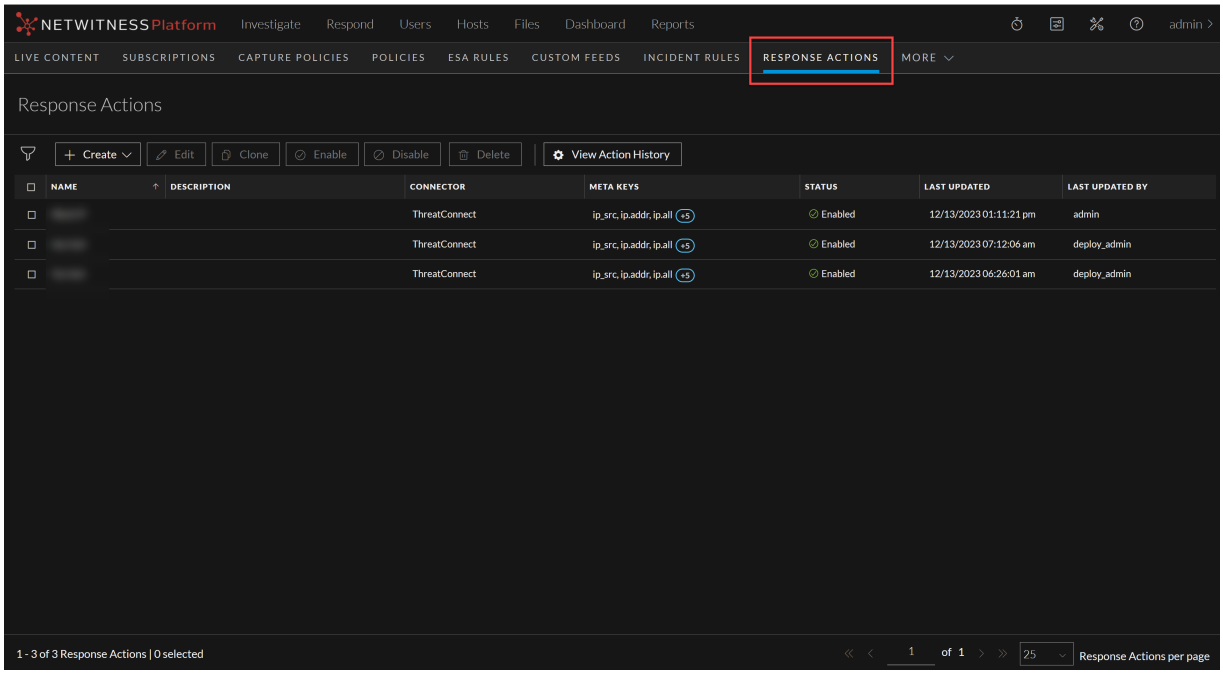
Para obtener más información, consulte Guía del usuario de NetWitness Respond para 12.4, *Guía del usuario de NetWitness Investigate* y *Guía de gestión de contenido centralizada basada en políticas*.

Acciones de respuesta

Las acciones de respuesta son operaciones reactivas realizadas en metadatos configurados utilizando una herramienta o conector de terceros, como ThreatConnect, después de clasificar un evento. **Acciones de respuesta**, la nueva función agregada en **(CONFIGURAR)** > **Más** le permite realizar las siguientes acciones:

- Cree y administre acciones de respuesta para los metadatos admitidos disponibles en la vista **Respond**, **Investigate**, **Hosts** y **Usuarios**.
- Realice acciones rápidas en el metadato configurado y publique el metadato con parámetros

adicionales en el conector para realizar más acciones.



Para obtener más información, consulte la *Guía de configuración de NetWitness Respond para 12.4*.

Insight

Las siguientes secciones describen las nuevas mejoras para el componente Insight:

Incluir alertas de Insight en la lista blanca en la vista Respond

Los administradores y analistas ahora pueden incluir en la lista blanca las alertas de Insight recurrentes y no deseadas generadas en la vista **Respond** > **Alertas**. Esta mejora brinda la capacidad de seleccionar valores específicos, como dirección IP y tipo de activo, así como también definir una condición de lista blanca para evitar que se generen alertas no deseadas para estos valores. Con esta mejora, los analistas pueden optimizar el proceso de gestión de alertas al excluir direcciones IP específicas o tipos de activos que se sabe que son confiables y seguros. Esta optimización minimiza las alertas innecesarias generadas en la vista **Respond** > **Alertas**, lo que reduce el tiempo y el esfuerzo necesarios para revisar y analizar alertas.

Para obtener más información, consulte la sección **NetWitness Insight** en el *Portal de documentación de NetWitness*.

User and Entity Behavior Analytics

La siguiente sección describe las nuevas mejoras para el componente UEBA:

Soporte para dispositivos Cisco Adaptive Security Appliance (ASA) y Fortinet VPN

NetWitness UEBA ha agregado soporte para los dispositivos Cisco ASA y Fortinet VPN. Con esta mejora, UEBA ahora puede procesar registros de Cisco ASA y Fortinet VPN, lo que ayuda a recopilar y analizar información de la actividad del usuario.

Para obtener más información, consulte la sección **Fuentes compatibles con UEBA por esquema** en la *Guía de configuración UEBA*.

Mejoras del rendimiento de UEBA

Se realizan las siguientes mejoras de rendimiento para UEBA en la versión 12.4.0.0:

- Optimización de los modelos de agregación y acumulación para generar y almacenar modelos en paralelo.
- Optimización de la tarea de agregación de puntajes por hora para agregar y calificar en paralelo.

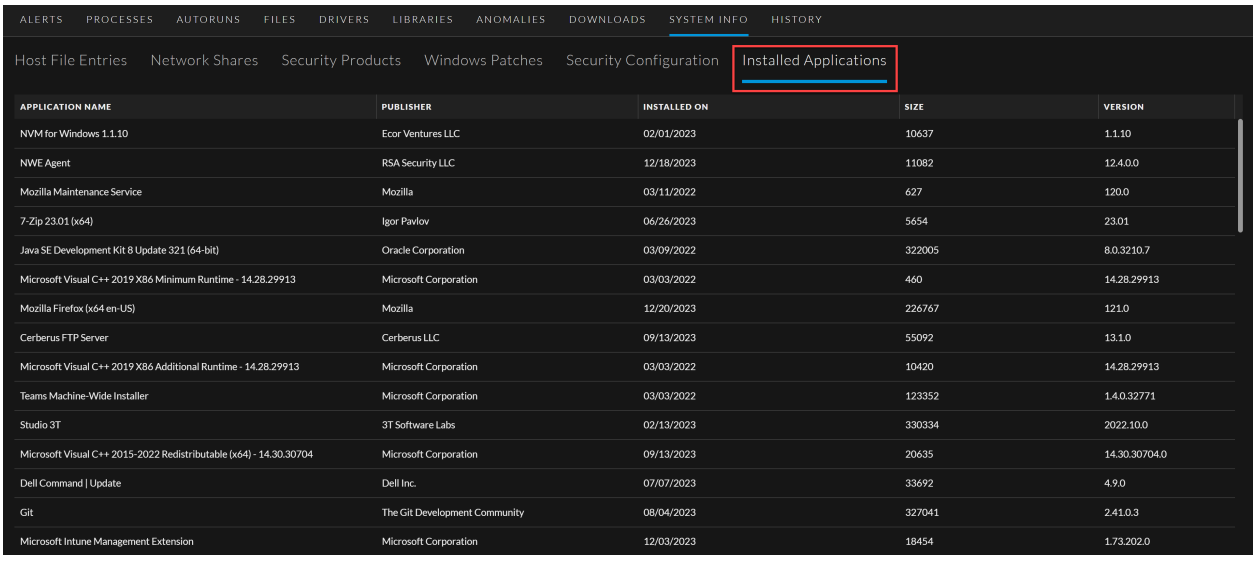
Para obtener más información sobre la escala compatible, consulte el tema **Período de aprendizaje por escala para 12.4** en la *Guía de configuración UEBA*.

Terminal

La siguiente sección describe las nuevas mejoras para el componente de Endpoint:

Ver aplicaciones instaladas

La vista detalles de **Hosts** > **Información del sistema** ha mejorado para permitir a los analistas ver la información sobre las distintas aplicaciones instaladas en una máquina con Windows.

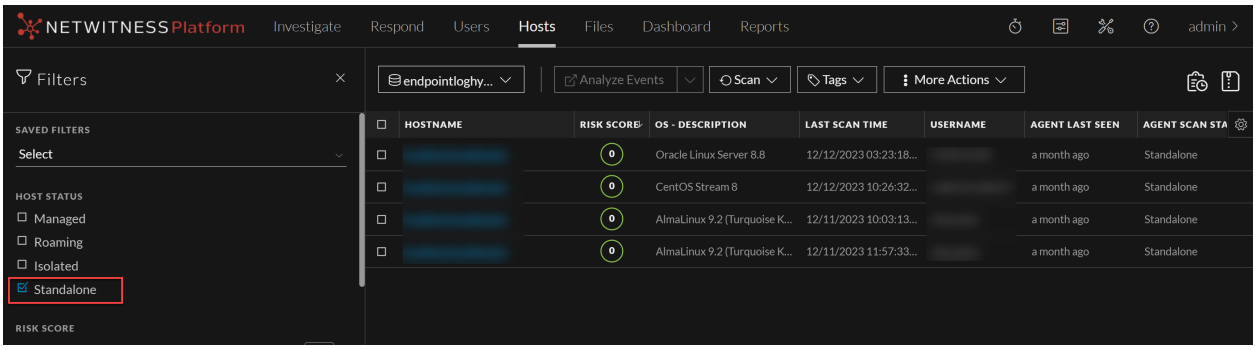


APPLICATION NAME	PUBLISHER	INSTALLED ON	SIZE	VERSION
NVM for Windows 1.1.10	Ecor Ventures LLC	02/01/2023	10637	1.1.10
NWE Agent	RSA Security LLC	12/18/2023	11082	12.4.0.0
Mozilla Maintenance Service	Mozilla	03/11/2022	627	120.0
7-Zip 23.01 (x64)	Igor Pavlov	06/26/2023	5654	23.01
Java SE Development Kit 8 Update 321 (64-bit)	Oracle Corporation	03/09/2022	322005	8.0.3210.7
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29913	Microsoft Corporation	03/03/2022	460	14.28.29913
Mozilla Firefox (x64 en-US)	Mozilla	12/20/2023	226767	121.0
Cerberus FTP Server	Cerberus LLC	09/13/2023	55092	13.1.0
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29913	Microsoft Corporation	03/03/2022	10420	14.28.29913
Teams Machine-Wide Installer	Microsoft Corporation	03/03/2022	123352	1.4.0.32771
Studio 3T	3T Software Labs	02/13/2023	330334	2022.10.0
Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.30.30704	Microsoft Corporation	09/13/2023	20635	14.30.30704.0
Dell Command | Update	Dell Inc.	07/07/2023	33692	4.9.0
Git	The Git Development Community	08/04/2023	327041	2.41.0.3
Microsoft Intune Management Extension	Microsoft Corporation	12/03/2023	18454	1.73.202.0

Para obtener más información, consulte la *Guía de configuración de NetWitness Endpoint*.

Análisis independiente para agentes de Linux

Los administradores pueden ejecutar escaneos independientes o sin conexión en hosts Linux para realizar análisis de amenazas en las máquinas aisladas Linux.



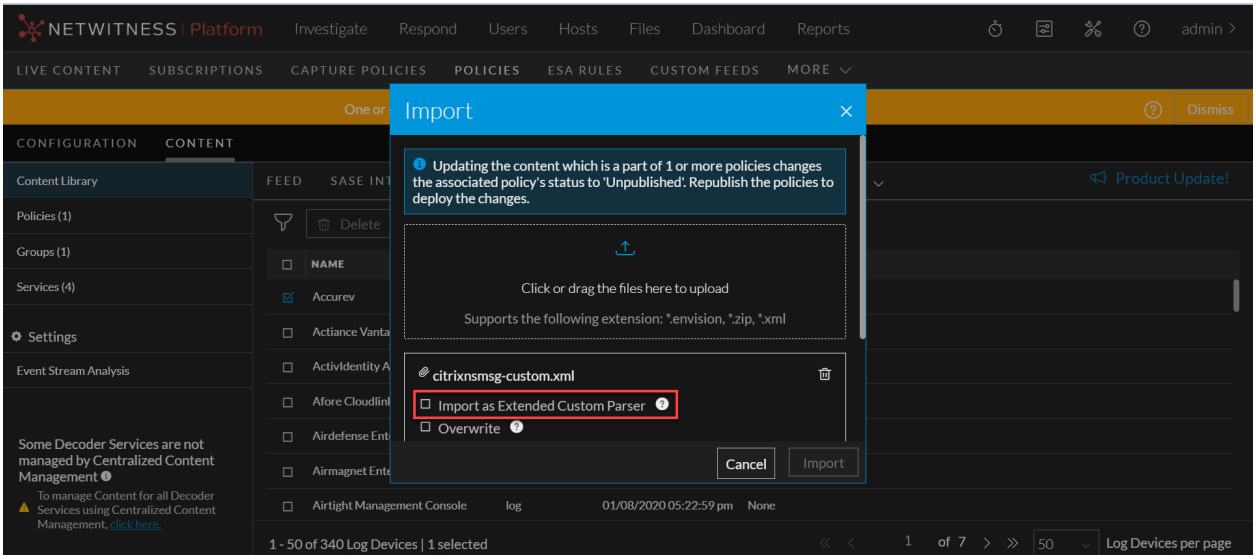
Para obtener más información, consulte la *Guía de configuración de NetWitness Endpoint*.

Administración de contenido centralizada (CCM) basada en políticas

Se realizan las siguientes mejoras para CCM en la versión 12.4.0.0:

Mejoras para el funcionamiento adecuado y la implementación de analizadores personalizados en servicios a través de CCM

Se introdujo la funcionalidad para importar XML individual (tipo de contenido del dispositivo de registro) a la biblioteca de contenido. Puede cargar los analizadores base o los analizadores extendidos como un archivo XML independiente. Al importar archivos XML, puede asociarlos de manera opcional con su analizador base correspondiente, tratándolo efectivamente como un analizador de extensión. Para importar un XML independiente como un analizador extendido, seleccione **Importar como analizador personalizado extendido** en la pantalla **Importar**.



La biblioteca de contenido ahora muestra los analizadores base y los analizadores de extensión como elementos distintos, lo que proporciona una vista clara y organizada para los usuarios. Esta separación garantiza que los usuarios puedan identificar y gestionar fácilmente ambos tipos de analizadores dentro de la biblioteca. Además, cuando se agrega un analizador de extensión a una política, el analizador base correspondiente también se incluye automáticamente en la política. Esta integración optimizada simplifica el proceso para los usuarios, lo que elimina la necesidad de vincular manualmente los analizadores base y de extensión al crear o editar políticas.

Para obtener más información, consulte la sección **Importar contenido a la biblioteca de contenido** en la *Guía de administración de contenido centralizada basada en políticas*.

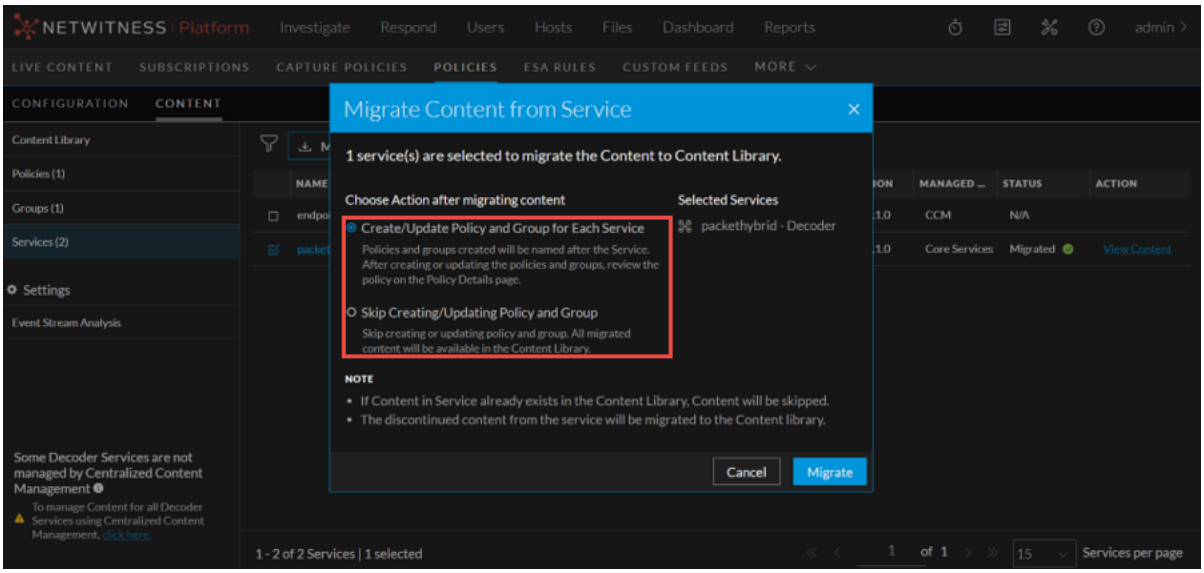
Mejoras durante la eliminación de un servicio del grupo

Al eliminar un servicio del grupo, puede optar por eliminar el contenido del servicio y luego eliminar el servicio del grupo o eliminar el servicio del grupo sin eliminar el contenido.

Para obtener más información, consulte las secciones **Editar un grupo**, **Editar una política** y **Eliminar una política** en la *Guía de administración de contenido centralizada basada en políticas*.

Funcionalidad para volver a migrar contenido del servicio

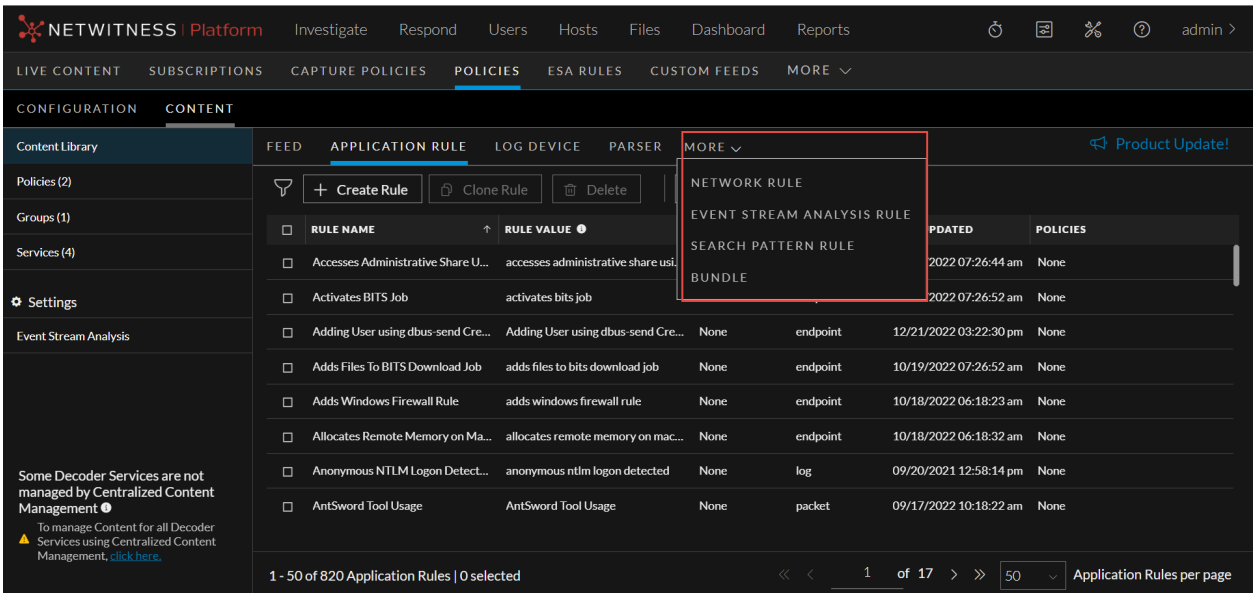
CCM cuenta con la mejora para volver a migrar contenido de un servicio incluso si ya está migrado y/o asignado a Grupos y Políticas. Al migrar contenido de un servicio ya asociado a una política, opcionalmente puede actualizar la política asociada con contenido migrado. Para actualizar la política y el grupo existentes para el servicio después de volver a migrarlo, las opciones disponibles en la página **Migrar contenido del servicio** se actualizan a **Crear/Actualizar la política y el grupo para cada servicio** y **Omitir la creación/actualización de una política y un grupo**.



Para obtener más información, consulte la sección **Migrar contenido del servicio** en la *Guía de administración de contenido centralizada basada en políticas*.

Mejoras de la interfaz del usuario

El menú de navegación **MÁS** se agrega a la interfaz de usuario de CCM para ver paquetes, patrones de búsqueda e integraciones de forma predeterminada. Al seleccionar el tipo de contenido en el menú **MÁS**, ese tipo de contenido aparece a la izquierda del menú **MÁS**.

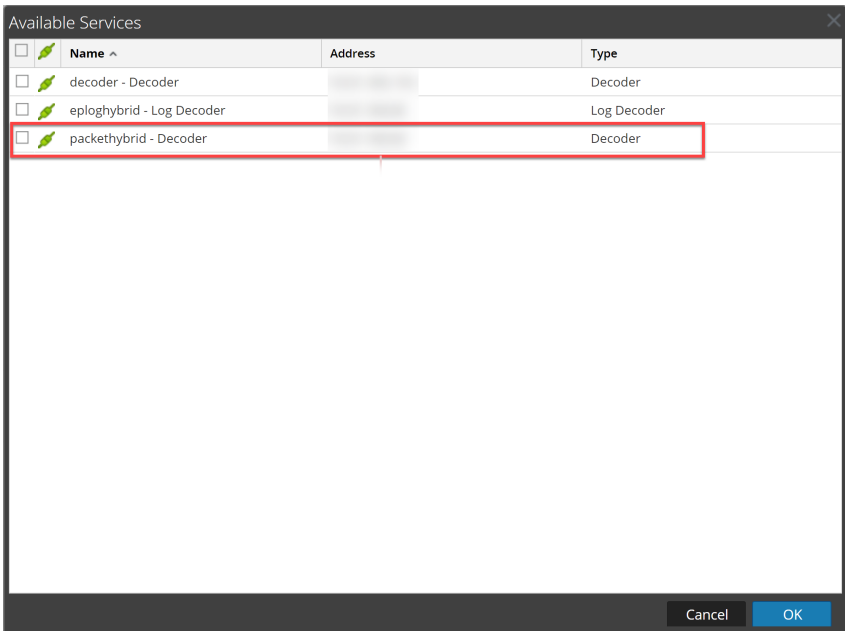


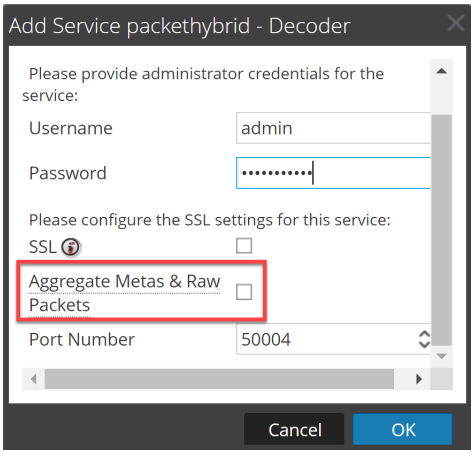
Servicios de Concentrator, Decoder, Log Collector y Archiver

Se realizan las siguientes mejoras para los servicios de Concentrator, Decoder, Log Collector y Archiver en la versión 12.4.0.0:

Retención selectiva para Packet Decoder

Esta versión proporciona una opción de retención selectiva para los clientes de NDR, lo que les permite disminuir agresivamente los requisitos de retención requeridos y al mismo tiempo mantener evidencia importante para continuar liderando las capacidades forenses y de búsqueda de amenazas. Esto se logra dado que los administradores ahora pueden configurar el host Packet Decoder para Archiver como origen de datos sin problemas desde  **(Admin)** > **Servicios** > vista **Configuración** > pestaña **General**. Además, los administradores ahora pueden seleccionar el tipo de agregación deseado mediante la nueva opción **Agregar metadatos y paquetes crudos**. De esta manera, los administradores pueden elegir si agregar el servicio Decoder en función de los valores de metadatos o de los valores de metadatos y de los paquetes sin procesar.





Para obtener más información, consulte el tema **Agregar el Packet Decoder como origen de datos a Archiver** en la *Guía de configuración de Archiver*.

Funcionalidad para desaprobar el uso de la dirección IP para la autenticación básica

Netwitness ha desaprobado el uso de la dirección IP para la autenticación básica de la colección de Windows. Ahora, debe usar el FQDN en la dirección de origen de eventos y agregar una entrada del mismo FQDN en '/etc/hosts' mientras configura la autenticación básica.

Nueva utilidad para transmitir metadatos desde decodificadores a herramientas de terceros

Se introdujo una utilidad beta para transmitir metadatos desde decodificadores de red a otras herramientas de terceros, lo que facilita la integración de NetWitness Platform con otros productos. Se pueden transmitir todos o un subconjunto de metadatos para limitar la cantidad enviada a la herramienta de terceros según el caso de uso.

Para obtener más información, consulte la *Guía de instalación y configuración de exportación de metadatos*.

Integraciones de registros

NetWitness Platform admite la integración de los siguientes orígenes de eventos para recopilar y analizar registros. A menos que se especifique lo contrario, estos servicios son compatibles con NetWitness Platform 12.2.0.0 o posterior.

- Acceso a Palo Alto Prisma
- VMware vSphere
- DeepInspect
- Registros de VM de Windows de GCP (a través del complemento de GCP)

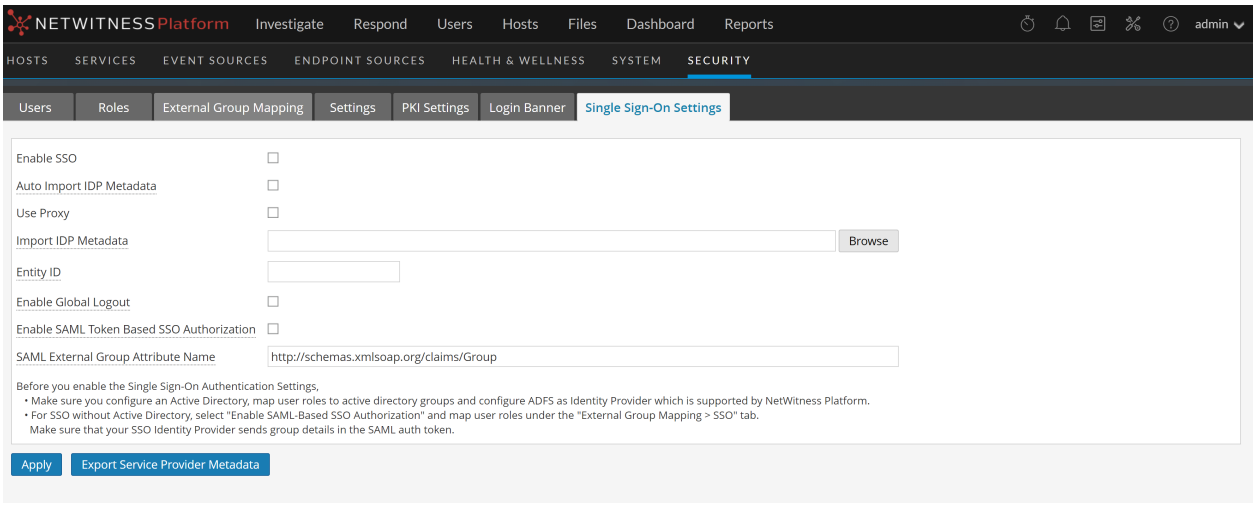
Nota: A partir de la versión 12.4, el complemento VMWare también está disponible para la recopilación de eventos y tareas de VMWare.

Para obtener más información sobre la integración de los servicios del analizador, consulte la Guía de integraciones de NetWitness Platform.

Seguridad

Autenticación de Single Sign On (SSO) independiente de la configuración de Active Directory (AD) en NetWitness

A partir de la versión 12.4 de NetWitness Platform, NetWitness ofrece SSO que es independiente de la configuración de AD en NetWitness. Permite la autorización de usuarios mediante la lista de grupos de usuarios integrada en el token de autenticación SAML proveniente de ADFS y se verifica con grupos de usuarios ya configurados en NetWitness. Esto elimina la necesidad de que los usuarios configuren o dependan de la configuración de Active Directory dentro de NetWitness para la autenticación de usuarios. NetWitness ahora es compatible con Azure ADFS y Microsoft ADFS.



Para más información, consulte el tema **Configurar la autenticación de Single Sign-On** en la *Guía de seguridad del sistema y gestión de usuarios*.

Reparaciones relacionadas con la seguridad

Para obtener más información sobre correcciones de seguridad, consulte https://community.netwitness.com/t5/netwitness-platform-advisories/ct-p/netwitness-advisories#security.

Rutas de actualización

Las siguientes rutas de actualización son compatibles con NetWitness Platform 12.4.0.0

- NetWitness 12.3.1.0 a 12.4.0.0
- NetWitness 12.3.0.0 a 12.4.0.0
- NetWitness 12.2.0.1 a 12.4.0.0
- NetWitness 12.2.0.0 a 12.4.0.0

Para obtener más información sobre la actualización a 12.4.0.0, consulte la Guía de actualización para NetWitness 12.4.0.0

IMPORTANTE: Si desea actualizar desde las versiones 11.7.x u 11.7.xx 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.

Ciclo de vida del producto de NetWitness Platform

Consulte el Ciclo de vida de la versión del producto para NetWitness Platform para conocer una lista de versiones que alcanzan el fin del soporte primario (EOPS).

Novedades de versiones anteriores (11.7 a 12.3.1.0)

La sección proporciona nuevas funciones y mejoras para todas las versiones anteriores compatibles.

Para obtener más información, consulte https://community.netwitness.com/t5/netwitness-platform-online/what-s-new-in-previous-releases-11-7-to-12-1-1/ta-p/695650.

Problemas resueltos en la versión 12.4.0.0

Esta sección enumera los problemas resueltos en la versión 12.4.0.0.

Para obtener información adicional sobre problemas resueltos, consulte la columna Versión reparada en la lista de problemas conocidos de NetWitness® Platform (https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872) en el portal de NetWitness Community.

Reparaciones de administración de contenido centralizada (CCM) basada en políticas

Número de rastreo	Descripción
ASOC-142018	El contenido del dispositivo de registro publicado desde CCM no se desactiva cuando se elimina el contenido de un servicio.
ASOC-141524	Las reglas de ESA no se pudieron guardar al editar o actualizar la regla de ESA. Los registros de UI y SA de NetWitness mostraron una excepción de tiempo de ejecución al guardar la regla. Además, en la solución de problemas, la **RSA OSINT Non-IP Threat Intel Feed** no tenía un ID único asociado con la política y aparecía en varios documentos en las recopilaciones de políticas de contenido.

Problemas conocidos en la versión 12.4.0.0

Los problemas que siguen sin resolverse en esta versión están documentados en la lista de problemas conocidos de NetWitness® Platform en el portal de la comunidad de NetWitness: https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872

Números de compilación para componentes 12.4.0.0

En la siguiente tabla se muestran los números de compilación de los diversos componentes de NetWitness 12.4.0.0.

Componente	Número de versión
NetWitness Servidor de administración	rsa-nw-admin-server-12.4.0.0-240117024246.5.165a1f70.el8.alma.noarch.rpm
NetWitness Contenido de análisis avanzado	rsa-nw-advanced-analytics-content-12.4.0.0-231212110357.5.9b3b362.el8.alma.noarch.rpm
NetWitness Servidor de análisis avanzado	rsa-nw-advanced-analytics-server-12.4.0.0-231212110325.5.9b3b362.el8.alma.noarch.rpm
NetWitness Appliance	rsa-nw-appliance-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Archiver	rsa-nw-archiver-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Complemento de auditoría	rsa-audit-plugins-12.4.0.0-4892.5.9d0750b41.el8.noarch.rpm
NetWitness RT de auditoría	rsa-audit-rt-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Bootstrap	rsa-nw-bootstrap-12.4.0.0-2401240926.5.a3d68ef.el8.noarch.rpm
NetWitness Broker	rsa-nw-broker-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Carlos RT	rsa-carlos-rt-12.4.0.0-2787.5.721a8daa7.el7.x86_64.rpm
NetWitness Nube	rsa-nw-cloud-12.4.0.0-12867.5.957818c84.el8.x86_64.rpm
NetWitness Servidor de Cloud Connector	rsa-nw-cloud-connector-server-12.4.0.0-240116135943.5.4220688.el8.alma.noarch.rpm
NetWitness Servidor de enlace de la nube	rsa-nw-cloud-link-server-12.4.0.0-240117032857.5.d4a8422.el8.alma.noarch.rpm
NetWitness Collectd	rsa-collectd-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Collectd SMS	rsa-collectd-sms-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Descripción del componente	rsa-nw-component-descriptor-12.4.0.0-2402080831.5.a403c19.el8.noarch.rpm
NetWitness Concentrator	rsa-nw-concentrator-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm

NetWitness Gestión de configuración	rsa-nw-config-management-12.4.0.0-2402050947.5.b7e9f64.el8.noarch.rpm
NetWitness Servidor de Config	rsa-nw-config-server-12.4.0.0-240109020724.5.dc657b7.el8.alma.noarch.rpm
Consola de NetWitness	rsa-nw-console-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Servidor de contenido	rsa-nw-content-server-12.4.0.0-240109040529.5.314fc043.el8.alma.noarch.rpm
NetWitness Servidor de Context Hub	rsa-nw-contexthub-server-12.4.0.0-240122010054.5.d98d0ac61.el8.alma.noarch.rpm
NetWitness Servidor de correlación (ESA)	rsa-nw-correlación-server-12.4.0.0-240117103632.5.61d080a9.el8.alma.noarch.rpm
NetWitness Contenido de Dashboard	rsa-nw-dashboard-content-20231220155210-5.noarch.rpm
NetWitness Decoder	rsa-nw-decoder-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Contenido analítico de Decoder	rsa-nw-decoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Contenido de Decoder	rsa-nw-decodercontent-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Actualización de implementación	rsa-nw-deployment-upgrade-12.4.0.0-2402050945.5.1903a3b.el8.noarch.rpm
NetWitness Agentes de Endpoint	rsa-nw-endpoint-agents-12.4.0.0-2402061657.5.db93b9a.el8.x86_64.rpm
NetWitness Servidor de Endpoint Broker	rsa-nw-endpoint-broker-server-12.4.0.0-240103053136.5.8430874.el8.alma.noarch.rpm
NetWitness Contenido analítico de Endpoint Decoder	rsa-nw-endpointdecoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Servidor de terminal	rsa-nw-endpoint-server-12.4.0.0-240125030031.5.12c246114.el8.alma.noarch.rpm
NetWitness Empresa Esper	rsa-nw-esper-enterprise-12.4.0.0-2311071130.5.04c15de.el8.alma.noarch.rpm
NetWitness Servidor de integración	rsa-nw-integration-server-12.4.0.0-240117101347.5.0ed5cc33.el8.alma.noarch.rpm
NetWitness Servidor de Investigate	rsa-nw-investigate-server-12.4.0.0-240109023320.5.2a0d2764.el8.alma.noarch.rpm
NetWitness Servidor web heredado	rsa-nw-legacy-web-server-12.4.0.0-240122162503.5.40628dd.el8.almalinux.noarch.rpm
NetWitnessServidor de licencias	rsa-nw-license-server-12.4.0.0-240111044400.5.a6108af.el8.alma.noarch.rpm

NetWitness Log Collector	rsa-nw-logcollector-12.4.0.0-15127.5.527ec7727.el8.x86_64.rpm
NetWitness Contenido de Log Collector	rsa-nw-logcollectorcontent-20240105141144-5.x86_64.rpm
NetWitness Perl de Log Collector	rsa-nw-logcollector-perl-12.4.0.0-15127.5.527ec7727.el8.x86_64.rpm
NetWitness Herramientas de Log Collector	rsa-nw-logcollector-tools-12.4.0.0-15127.5.527ec7727.el8.x86_64.rpm
NetWitness Log Decoder	rsa-nw-logdecoder-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Contenido analítico de Log Decoder	rsa-nw-logdecoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Contenido base de Log Decoder	rsa-nw-logdecoder-base-content-20240124060008-5.x86_64.rpm
NetWitness Log Player	rsa-nw-logplayer-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Servidor de Malware Analytics	rsa-nw-malware-analytics-server-12.4.0.0-240207115909.5.1511622.el8.almalinux.x86_64.rpm
NetWitness Utilidad de exportación de metadatos	rsa-nw-metaexport-utility-12.4.0.0-110124.5.el8.x86_64.rpm
NetWitness Servidor de métricas	rsa-nw-metrics-server-12.4.0.0-240109050254.5.c078db1.el8.alma.noarch.rpm
NetWitness Servidor de infraestructura de nodo	rsa-nw-node-infra-server-12.4.0.0-240116091133.5.70861f6.el8.alma.noarch.rpm
NetWitness Interfaz de línea de comandos (CLI) de organización	rsa-nw-orchestration-cli-12.4.0.0-2401091103.5.7317baa.el8.noarch.rpm
NetWitness Servidor de Orchestration	rsa-nw-orchestration-server-12.4.0.0-240119064852.5.a87bb81f.el8.alma.noarch.rpm
NetWitness Marcador de posición	rsa-nw-placeholder-12.4.0.0-2310040926.5.cebd204.el8.noarch.rpm
NetWitness Flujo de aire Presidio	rsa-nw-presidio-airflow-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Servidor de configuración de Presidio	rsa-nw-presidio-configserver-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Núcleo del Presidio	rsa-nw-presidio-core-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Inicio de búsqueda elástica de Presidio	rsa-nw-presidio-elasticsearch-init-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Ext NetWitness	rsa-nw-presidio-ext-netwitness-12.4.0.0-2401151152.5.18bd06b.el8.noarch.rpm

NetWitness Gerente de Presidio	rsa-nw-presidio-manager-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Salida de Presidio	rsa-nw-presidio-output-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness UI de Presidio	rsa-nw-presidio-ui-12.4.0.0-2402270745.5.0844250.el8.noarch.rpm
NetWitness Protobufs	rsa-protobufs-rt-12.4.0.0-928.5.6254aabd8.el8.x86_64.rpm
NetWitness Herramientas de recuperación	rsa-nw-recovery-tool-12.4.0.0-2401230435.5.f34a9fd.el8.noarch.rpm
NetWitness Servidor de retransmisión	rsa-nw-relay-server-12.4.0.0-240112083607.5.6d41796.el8.alma.noarch.rpm
NetWitness Servidor de Reporting Engine	rsa-nw-re-server-12.4.0.0-5996.5.b76234be4.el8.x86_64.rpm
NetWitness Servidor de Respond	rsa-nw-respond-server-12.4.0.0-240110052505.5.1eda6132f.el8.alma.noarch.rpm
NetWitness Servidor de acciones de respuesta	rsa-nw-respuesta-acciones-serv-12.4.0.0-240116034125.5.0af5d71.el8.alma.noarch.rpm
NetWitness Actualización de CA raíz	rsa-nw-root-ca-update-12.4.0.0-2401221231.5.96cd15b.el8.noarch.rpm
NetWitness Herramientas SA	rsa-sa-tools-12.4.0.0-2401251338.5.89600eb.el8.noarch.rpm
NetWitness CLI de seguridad	rsa-nw-security-cli-12.4.0.0-2401091103.5.18ab320.el8.noarch.rpm
NetWitness Servidor de seguridad	rsa-nw-security-server-12.4.0.0-240123034132.5.11d93f41.el8.alma.noarch.rpm
NetWitness Shell	rsa-nw-shell-12.4.0.0-240108140410.5.0b0d73f5.el8.alma.noarch.rpm
NetWitness Complementos de informes SOS	rsa-nw-sosreport-plugins-12.4.0.0-2401162235.5.af21a76.el8.noarch.rpm
NetWitness Tiempo de ejecución (RT) de SMS	rsa-sms-runtime-rt-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Servidor de SMS	rsa-sms-server-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Servidor de origen	rsa-nw-source-server-12.4.0.0-240207074107.5.4b84868b1.el8.alma.noarch.rpm
NetWitness Contenido del servidor de origen	rsa-nw-sourceserver-content-20240105141144-5.x86_64.rpm
Interfaz del usuario de NetWitness	rsa-nw-ui-12.4.0.0-240131063757.5.d1b137ecbc.el8.alma.noarch.rpm

NetWitness Workbench	rsa-nw-workbench-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm

Cómo obtener ayuda con NetWitness Platform

Documentación del producto

Con esta versión se proporciona la siguiente documentación.

Documentación	Dirección URL de ubicación
Tabla de contenidos principal de NetWitness Platform	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
Documentación de producto de NetWitness Platform 12.4.0.0	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
Guía de actualización de NetWitness Platform 12.4.0.0	https://community.netwitness.com/t5/rsa-netwitness-platform-staged/upgrade-guide-for-12-4/ta-p/709308
Análisis de NetWitness en la nube	Para obtener más información sobre las nuevas funciones y mejoras en las versiones de NetWitness Analytics on Cloud, consulte la siguiente sección Novedades: Para UEBA Cloud, consulte https://docs.netwitness.com/netwitnessueba/release_information/whats_new/. Para obtener información, consulte https://docs.netwitness.com/netwitnessinsight/release-information/insight_whatsnew/.

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

Servicios educativos de NetWitness

Regístrese para acceder a los cursos de NetWitness y a recursos adicionales en los servicios educativos y de capacitación de NetWitness.

Portal educativo de NetWitness	https://netwitness.sabacloud.com/Saba/Web_spf/NA10P2PRD088/guestapp/home;spf-url=guest%2Fguestlearningcatalog
Catálogo de cursos de servicios educativos de NetWitness	https://community.netwitness.com/t5/netwitness-education-courses/tkb-p/netwitness-training
Programa de capacitación de servicios educativos de NetWitness	https://community.netwitness.com/t5/netwitness-education-blog/netwitness-instructor-led-training-schedule/ba-p/655826
Contacto de soporte de servicios educativos de NetWitness	education.support@netwitness.com

Comentarios sobre la documentación del producto

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