centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1210

Procedimiento de empleo seguro
RSA NetWitness Platform 11

Septiembre 2021

MINISTERIO DE DEFENSA

cpage.mpr.gob.es

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.07.18 14:22:12 +02'00'

© Centro Criptológico Nacional, 2021
NIPO: 083-21-178-2.

Fecha de Edición: julio de 2022

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL

1. **RSA NetWitness® Platform** es una suite de detección de amenazas que facilita que los centros de operaciones de seguridad (SOC) realicen tareas de **localización, asignación de prioridades y triaje de amenazas**. Además, permite aislar y corregir amenazas conocidas y desconocidas, así como proporcionar información detallada de paquetes, registros y terminales de la organización.
2. NetWitness Platform facilita el uso para los analistas de nivel 1, ya que automatiza el proceso de identificar y dar prioridad a las amenazas sospechosas. Los analistas de nivel 2 y nivel 3 pueden buscar y localizar amenazas mediante la búsqueda y el filtrado de eventos y, a continuación, su estudio mediante herramientas de reconstrucción y análisis.
3. Este producto ha sido cualificado y, por tanto, incluido en el CPSTIC en la familia de '*Sistemas de gestión de eventos de seguridad*'.

1.2 ARQUITECTURA

4. RSA NetWitness Platform es un sistema distribuido y modular que permite arquitecturas de implementación que escalan según las necesidades de la organización. Con NetWitness Platform, los administradores pueden recopilar tres (3) tipos de datos desde la infraestructura de red: datos de paquetes, datos del registro y datos de terminales. Los aspectos clave de la arquitectura son:

    a) **Recopilación de datos distribuidos**. El ***Decoder*** recopila datos de paquetes y el ***Log D*ecoder**, datos del registro. Los *Decoders* analizan y reconstruyen todo el tráfico de red recopilado desde las capas 2 a la 7 del modelo OSI, o los datos de registros y eventos de cientos de dispositivos y orígenes de eventos, incluidos los datos de ***NetWitness Endpoint*** (si está instalado y configurado). ***Concentrator*** indexa metadatos extraídos de los datos de red o de registros y los pone a disposición para realizar un análisis en tiempo real y crear consultas de toda la organización, a la vez que facilita la creación de informes y alertas. ***Broker*** agrega datos que capturan otros dispositivos y orígenes de eventos. Los *Brokers* agregan datos de *Concentrators* configurados; los *Concentrators* agregan datos de *Decoders*. Por lo tanto, un *Broker* conecta las distintas áreas de almacenamiento de datos en tiempo real ubicadas en varios pares de *Decoder/Concentrator* a lo largo de la infraestructura.

    b) **Alertas en tiempo real**. El servicio ***NetWitness Platform Event Stream Analysis*** (ESA) proporciona análisis de flujo avanzado, como correlación y procesamiento de eventos complejos, a alto rendimiento y baja latencia. Puede procesar grandes volúmenes de datos de eventos dispares que provienen de *Concentrators*. ESA utiliza un lenguaje de procesamiento de eventos (EPL) avanzado que permite a los analistas expresar filtrado,

agregación, combinaciones, reconocimiento de patrones y correlación en múltiples flujos de eventos dispares. ***Event Stream Analysis*** ayuda a realizar detección de incidentes y alertas eficaces.

c) **Análisis en tiempo real** (análisis automático de eventos). La funcionalidad Detección de amenazas automatizadas de RSA incluye módulos **ESA *Analytics*** preconfigurados para detectar el tráfico de comando y control.

d) **Servidor de NetWitnkess**. En el Servidor de NetWitness se proporcionan las funcionalidades de creación de informes, investigación, administración y otros aspectos de la interfaz del usuario.

e) **Capacidad**. *NetWitness Platform* cuenta con una arquitectura de capacidad modular, habilitada con capacidad de conexión directa (DAC) o redes de almacenamiento SAN, que se adapta a las necesidades de investigación a corto plazo y de retención de datos y analítica a más largo plazo.

5. NetWitness Platform ofrece gran flexibilidad de implementación. En el diseño de la arquitectura, es posible usar varias docenas de hosts físicos o un único host físico en función de los detalles específicos de los requisitos de rendimiento y seguridad de la organización. Además, todo el sistema NetWitness Platform permite ejecución en una infraestructura virtualizada.

6. La arquitectura del sistema incluye los siguientes componentes principales: *Decoders, Brokers, Concentrators, Archivers, ESA* y *Warehouse Connectors*. Los componentes de NetWitness Platform se pueden utilizar en conjunto como un sistema o de manera individual.

7. **En una implementación de información de seguridad y administración de eventos (SIEM),** la configuración básica requiere los siguientes componentes: Log Decoder, Concentrator, Broker, Event Stream Analysis (ESA) y el Servidor de NetWitness.

8. En una implementación de análisis forense, la configuración básica requiere los siguientes componentes: *Decoder, Concentrator, Broker, ESA, Malware Analysis y Endpoint Log Hybrid*. El servicio *Respond Server* también se requiere y se utiliza para dar prioridad a las alertas.

9. La siguiente tabla proporciona una descripción de cada componente principal:

Componente del sistema	Descripción
Decoder/Log Decoder	NetWitness Platform recopila datos de paquetes de red, logs y equipos finales o de usuario (*endpoints*). Los datos de paquetes de red se recopilan mediante *Decoder* a través del puerto TAP o SPAN de la red, el cual normalmente se determina que es un punto de salida en la red de una organización. Un *Log Decoder* puede recopilar cuatro tipos de logs diferentes: Syslog, ODBC, eventos de Windows y archivos de log en formato texto. Eventos de Windows se refiere a la metodología de recopilación de Windows 2008 y los archivos de log en formato texto pueden obtenerse a través de SFTP. Ambos tipos de *Decoders* recopilan datos transaccionales en crudo (*raw*) que se enriquecen, cierran y agregan a otros componentes de NetWitness Platform. Los procesos de recopilación y análisis de datos transaccionales en Netwitness se basan en una plataforma dinámica y abierta.
(Virtual) Log Collector	El servicio *Log Collector* es el que se encarga de recopilar los registros o logs de las fuentes de eventos. Este servicio se encuentra instalado en los hosts *Log Decoders*, pero también se puede instalar individualmente en sistemas virtuales separados que sólo contienen el servicio Log *Collector* y no el *Log Decoder*. Estos sistemas virtuales se llaman *Virtual Log Collector (VLC).* Los Virtual Log *Collectors* no enriquecen los datos ni crean metadatos, éstas funciones sólo las hace el Log *Decoder*, por lo que siempre hay que configurar los Virtual Log *Collectors* para que envíen los logs recopilados a los Log *Decoders*.
Endpoint Log Hybrid	Recopila y administra datos de equipos de usuario Windows, Mac o Linux. Registra datos sobre cada acción crítica, como procesos, archivos, la modificación del registro, las conexiones de red y las interacciones de la consola del usuario. Soporta la recopilación de logs de hosts de Windows si se habilita esta opción en la configuración. Genera metadatos para correlacionar los datos de los sistemas de usuario con las sesiones de otros orígenes de eventos, como los logs de otros sistemas y los paquetes de red. Realiza un análisis activo de la memoria, analiza el tráfico de red y detecta comportamientos de usuario sospechosos.

Componente del sistema	Descripción
Concentrator	Proporciona la funcionalidad de índice y consulta para las recopilaciones de NetWitness. Opcionalmente, también puede enviar datos a los sistemas ESA, explicados un poco más abajo en esta tabla.
Broker	Unifica y distribuye las consultas de los datos recopilados a múltiples *Concentrators* o Arckhivers, lo que hace que todos los datos recopilados por *NetWitness Platform* aparezcan como una única recopilación y no sea necesario enviar una consulta independiente a cada uno de los Concentradores o *Archivers*.
Archiver	El servicio *Archiver* permite el almacenamiento de logs a largo plazo mediante la indexación y la compresión de los logs y su envío a sistemas de almacenamiento destinados a archivado de larga retención. Los sistemas de almacenamiento están optimizados para la retención de datos a largo plazo y los informes de cumplimiento de normas. El *Archiver* almacena los logs en crudo (raw) y metadatos recopilados y generados por los Log *Decoders*, para su retención a largo plazo. Utiliza unidades de capacidad de conexión directa (DAC) para el almacenamiento. Los paquetes de red en crudo y sus metadatos no se almacenan en el Archiver, éste sólo almacena datos de tipo log y sus metadatos.
Event Stream Analysis (ESA)	El servicio *Event Stream Analysis* proporciona analítica de flujo de eventos, como correlación y procesamiento de eventos complejos, a alto rendimiento y baja latencia. Puede procesar grandes volúmenes de datos de eventos dispares que provienen de los *Concentrators*. ESA utiliza un lenguaje de procesamiento de eventos avanzado que permite a los usuarios expresar filtrado, agregación, combinaciones, reconocimiento de patrones y correlación en múltiples flujos de eventos dispares. ESA ayuda a la detección de incidentes y alertas eficaces. La funcionalidad Detección de amenazas automatizadas de RSA incluye módulos ESA *Analytics* preconfigurados para detectar el tráfico de comando y control.

Componente del sistema	Descripción
Malware Analysis	Malware *Analysis* es un servicio de análisis automático de malware diseñado para analizar cierto tipo de archivos (por ejemplo Windows portable ejecutable (PE), PDF y documentos *MS Office*) y evaluar la probabilidad de que un archivo sea malicioso.
Servidor de NetWitness	En el Servidor de *NetWitness* se proporcionan las funcionalidades de creación de informes (*Reporting*), investigación (*Investigate*), administración y otros aspectos de la interfaz del usuario.

1.3 COMPONENTES PRINCIPALES FRENTE A DESCENDENTES

10. En NetWitness Platform, los servicios principales recopilan y analizan datos, generan metadatos y agregan los metadatos generados con los datos crudos. Entre los servicios principales se incluyen Decoder, Log Decoder, Concentrator y Broker. Los sistemas descendentes usan los datos almacenados en los servicios principales para el análisis. Por lo tanto, las operaciones de los servicios descendentes dependen de los servicios principales. Los sistemas descendentes son Archiver, ESA, Malware Analysis, Investigate y Reporting.

11. Aunque los servicios principales pueden funcionar y proporcionar una buena solución de análisis sin los sistemas descendentes, los componentes descendentes ofrecen funciones de análisis adicionales. ESA proporciona correlación en tiempo real entre sesiones y eventos, y también entre distintos tipos de eventos, como datos de registros, paquetes y terminales. *Investigate* brinda la capacidad de desglosar a datos, examinar eventos y archivos, y reconstruir eventos en un ambiente seguro. El servicio de *Malware Analysis* ofrece inspección automatizada en tiempo real de actividad maliciosa en sesiones de red y archivos asociados.

12. La plataforma NetWitness proporciona funciones para la gestión de la privacidad de datos. Las funciones proporcionan a los usuarios con el rol de Oficial de privacidad de datos o Administrador la capacidad de administrar y proteger los datos sensibles a la privacidad, sin reducir significativamente la capacidad analítica. NetWitness Platform se puede configurar para limitar la exposición de metadatos y contenido sin procesar (paquetes y registros) mediante una combinación de técnicas. Los métodos disponibles para proteger los datos en NetWitness Platform incluyen la ofuscación de datos, la aplicación de la retención de datos y el registro de auditoría. La característica de Registro de auditoría genera entradas de registro de auditoría que son relevantes para la privacidad de los datos.

13. Las funciones de administración de seguridad se realizan a través de la interfaz de usuario (UI) de la plataforma NetWitness, que es una GUI basada en web. Esta interfaz permite a los administradores autorizados administrar las cuentas de

usuario, los valores de bloqueo de sesión y otros datos, y ver los datos y alertas de IDS. La navegación en la interfaz de usuario se basa en roles y se divide en áreas funcionales principales, como Responder, Investigar y Administrador.

14. La vista Responder consolida todas las alertas, como las reglas de correlación de ESA, la detección automatizada de amenazas de ESA, el análisis de malware y las alertas de informes en una ubicación y se utiliza para el seguimiento de incidentes y el triaje.
15. La vista Investigar presenta siete (7) vistas diferentes en un conjunto de datos, lo que permite a los usuarios autorizados ver metadatos, eventos e indicadores potenciales de compromiso.
16. En la vista Administrador, los administradores pueden administrar hosts y servicios de red; gestionar la seguridad a nivel del sistema; y administrar métodos de recopilación/fuentes de eventos.

2. OBJETO Y ALCANCE

18. El objeto del presente documento es servir como guía para realizar una instalación y configuración segura de la solución **RSA NetWitness Platform, versión 11.6.**

19. Un ejemplo del entorno operativo del producto es el siguiente:

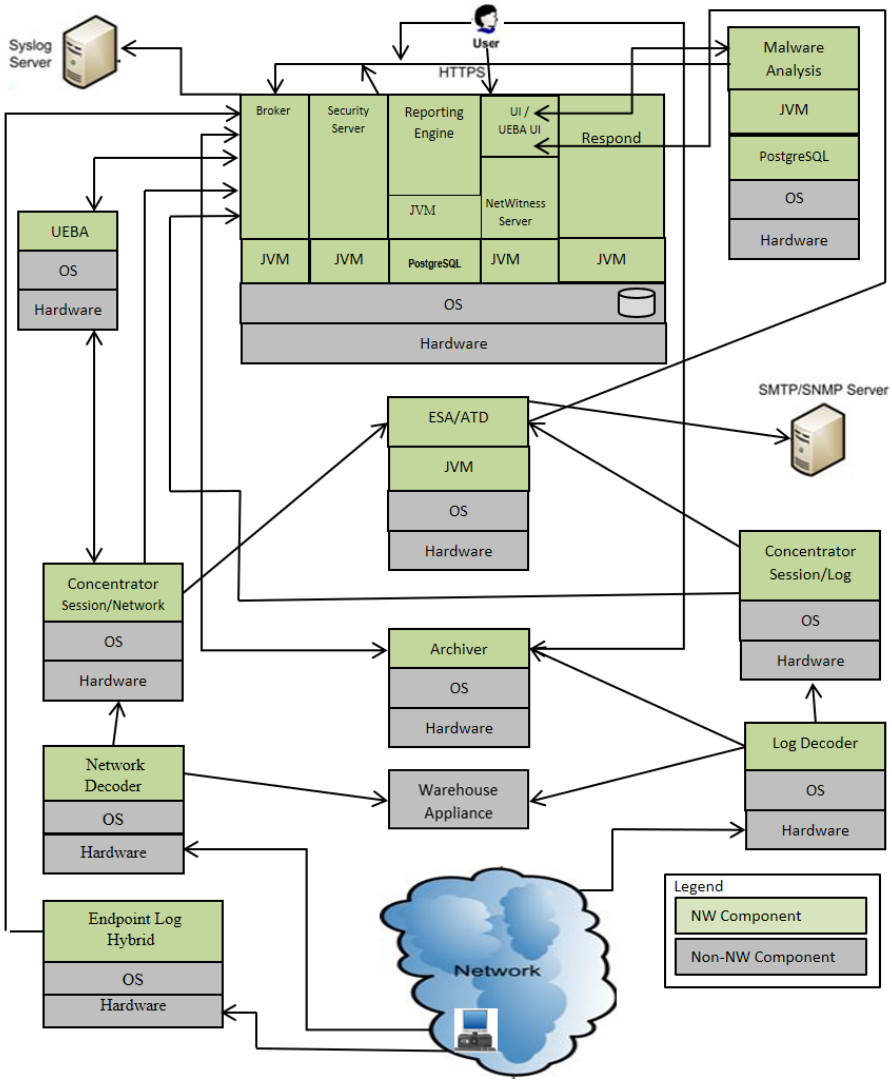

Ilustración 1. Ejemplo entorno operativo.

20. El presente documento aplica únicamente al siguiente entorno operativo:

    a) Sistema Operativo CentOS versión 7.9 ejecutado sobre *Dell R630,Dell R730xd (Series 5), Dell R640 o Dell R740xd (Series 6)*: proporciona un entorno de ejecución para los componentes de NetWitness.

    b) Servidor Windows para ejecutar el recolector de eventos de Windows que cumpla, al menos, con los siguientes requisitos:

        i. Sistema operativo: *Windows 2008 R2 SP1* de 64 bits, *Windows 2012* de 64 bits o Windows 2016 de 64 bits.

        ii. Procesador: *CPU Intel Xeon 2.0Ghz* o más rápido.

iii. Memoria: 8 GB o más rápido.

iv. Espacio en disco disponible: 320 GB.

c) *Hipervisor ESXi* versión 5.5, 6.0, 6.5, 6.7 o 7.0: proporciona virtualización para los *appliances* virtuales de NetWitness.

d) Estación de trabajo / Navegador de administrador: proporciona a los usuarios acceso a la interfaz de usuario de *NetWitness Server*. Los navegadores compatibles que admiten las funciones necesarias para NetWitness 11.6 incluyen versiones actuales de *Google Chrome, Mozilla Firefox, Microsoft Edge* y *Apple Safari*.

3. ORGANIZACIÓN DEL DOCUMENTO

21. La estructura de capítulos del documento es la siguiente:

a) **Apartado 4.** En este apartado se recogen recomendaciones para tener en cuenta durante la fase de despliegue e instalación del producto.

b) **Apartado 5.** En este apartado se recogen las recomendaciones para tener en cuenta durante la fase de configuración segura del producto, para lograr una configuración segura.

c) **Apartado 6.** En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

d) **Apartado 7.** En este apartado se incluye una lista de comprobación para verificar que se han seguido todas las recomendaciones de seguridad.

e) **Apartado 8.** En este apartado se incluyen las referencias utilizadas a lo largo del documento.

f) **Apartado 9.** En este apartado se incluyen las abreviaturas usadas a lo largo del documento.

g) **ANEXO A .** En este anexo se detallan las variables de los eventos de auditoría.

h) **ANEXO B .** En este anexo se detallan los distintos tipos de mensajes de auditoría.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

22. Durante el proceso de entrega deberán llevarse a cabo una serie tareas de comprobación, de cara a garantizar que el producto recibido no se ha manipulado indebidamente.

23. En el caso de que el producto sea hardware, se verificará:

    a) Etiqueta de envío. Deberá comprobarse que la etiqueta de envío identifica correctamente el nombre del usuario, su dirección y el dispositivo.

    b) Embalaje externo. Deberá inspeccionarse la caja de envío externa y la cinta adhesiva. Se comprobará que la cinta adhesiva no esté cortada ni se haya deteriorado en ningún punto. Así mismo, la caja no deberá presentar cortes ni daños que permitan acceder al dispositivo.

    c) Embalaje interno. Deberá inspeccionarse la bolsa de plástico y el sistema de sellado. La bolsa no deberá presentar cortes ni haber sido extraída. El sistema de sellado deberá estar intacto.

    d) Sello de garantía del hardware. Deberá comprobarse que el hardware dispone del correspondiente sello intacto.

    e) Número de serie. Deberá coincidir el número de serie de la caja y del *appliance*, así como el de la orden enviada por correo electrónico al contacto principal.

24. En el caso de que el producto sea software se deberán seguir los siguientes pasos:

    a) Realizar la descarga solo desde la web de descargas de RSA: https://my.rsa.com. Se verificará la validez del certificado de la página desde el navegador de la siguiente forma:

        i. Por ejemplo, en *Google Chrome*:

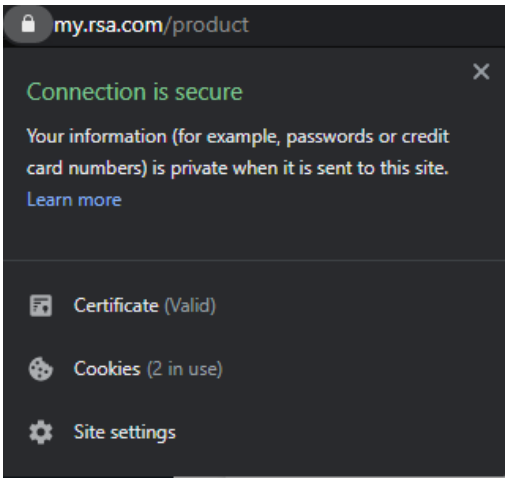

Ilustración 2. Verificación del certificado de la página de descargas.

    b) Utilizar las credenciales del contacto principal.

c) Verificar que el número de serie del componente que se va a descargar corresponde con el indicado en la orden de compra recibida por su contacto principal del equipo de Ventas de NetWitness.

d) Para verificar la integridad, realizar el hash *sha256* del fichero descargado y comprobar que coincide con el fichero hash que acompaña a la descarga.

e) Repetir el paso anterior durante la cadena de custodia del fichero antes de desplegarlo para verificar que no se ha alterado una vez descargado.

25. En caso de identificarse algún problema durante la inspección, el usuario deberá ponerse en contacto inmediatamente con el proveedor, al que se le indicará el número de pedido, el número de seguimiento y una descripción del problema.

4.2 ENTORNO DE INSTALACIÓN SEGURO

26. Si es hardware, el producto deberá instalarse en un Centro de Proceso de Datos (CPD), cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa.

4.3 REGISTRO Y LICENCIAS

27. El proceso para registrar el producto se puede consultar en el apartado Licencia: Paso 1. Registrar el servidor de NetWitness, de la *Guía de administración de licencia – REF1.*

4.4 CONSIDERACIONES PREVIAS

28. A lo largo de este apartado se mencionan varios documentos adicionales disponibles en NetWitness. En la tabla maestra de contenido – REF2 se pueden encontrar todos los documentos de *RSA NetWitness Platform 11.x.*

29. Hay muchos factores que se deben tener en cuenta antes de instalar NetWitness Platform. Por ejemplo, será necesario estimar algunos requisitos de crecimiento y almacenamiento, como los que se indican a continuación:

a) El tamaño de la organización (es decir, el número de ubicaciones y personas que utilizarán *NetWitness Platform*).

b) El volumen de datos de red y registros que se necesita procesar.

c) El rendimiento que cada rol de usuario de *NetWitness Platform* necesita para realizar su trabajo de forma eficaz.

d) El requerimiento o política de prevención del tiempo fuera de servicio de los sistemas (es decir, cómo diseñar la implementación para evitar un único punto de error).

e) El entorno en el que se planea ejecutar *NetWitness Platform*:

i. Hosts físicos NetWitness (*software* que se ejecuta en hardware suministrado por NetWitness). Consultar la *Guía de instalación de host físico de RSA NetWitness Platform* para obtener instrucciones detalladas sobre cómo implementar hosts físicos NetWitness.

ii. Software proporcionado por NetWitness:

- Hosts virtuales locales (locales). Consultar la *Guía de instalación de host virtual de RSA NetWitness Platform* para obtener instrucciones detalladas sobre cómo implementar hosts virtuales locales.

iii. VCloud:

- *Amazon Web Services (AWS).* Consultar la *Guía de instalación de AWS de RSA NetWitness Platform* para obtener instrucciones detalladas sobre cómo implementar hosts virtuales en AWS.
- *Azure*. Consultar la *Guía de instalación de Azure de RSA NetWitness Platform* para obtener instrucciones detalladas sobre cómo implementar hosts virtuales en Azure.
- *Google Cloud Platform (GCP)*. Consultar la *Guía de instalación de GCP de RSA NetWitness Platform* para obtener instrucciones detalladas sobre cómo implementar hosts virtuales en GCP.

4.4.1 DESPLIEGUE BÁSICO

30. Antes de poder implementar *NetWitness Platform*, se debe:

a) Tener en cuenta los requisitos de la organización y comprender el proceso de implementación.

b) Tener una imagen de alto nivel de la complejidad y el alcance de una implementación de *NetWitness Platform*.

4.4.2 PROCESO DE DESPLIEGUE

31. Los componentes y la topología de una red de *NetWitness Platform* pueden variar mucho entre instalaciones y deben planificarse cuidadosamente antes de comenzar el proceso de despliegue. La planificación inicial incluye:

a) Consideración de los requisitos del centro de procesamiento de datos y los requisitos de seguridad.

b) Revisión de la arquitectura de red y el uso de puertos.

c) Consideración de crear grupos de agregación de archivadores, concentradores y hosts virtuales para distribuir la carga ente ellos.

32. Una vez realizada la planificación inicial, los pasos a seguir son:

a) Para *hosts* físicos RSA:

   i. Instalar los hosts físicos y conectar a la red como se describe en la Guía de configuración de *hardware* de *RSA NetWitness Platform* y la *Guía de instalación* de host físico de *RSA NetWitness Platform.*

   ii. Configurar las licencias para NetWitness Platform como se describe en la *Guía de licencias de RSA NetWitness Platform*.

   iii. Configurar hosts y servicios físicos individuales como se describe en la *Guía de introducción de hosts y servicios para RSA NetWitness Platform*. Esta guía también describe los procedimientos para aplicar actualizaciones y prepararse para las actualizaciones de versiones.

b) Para hosts virtuales *on-Prem*, seguir las instrucciones de la Guía de configuración del host virtual de RSA *NetWitness Platform.*

c) Para AWS, seguir las instrucciones de la Guía de instalación de AWS de RSA *NetWitness Platform*.

d) Para Azure, seguir las instrucciones de la Guía de instalación de RSA *NetWitness Platform Azure*.

e) Para GCP, seguir las instrucciones de la Guía de instalación de GCP de RSA NetWitness Platform.

33. Al actualizar hosts y servicios, seguir las directrices recomendadas en el tema Ejecutar en modo mixto de la *Guía de introducción a servicios y host de la plataforma RSA NetWitness.*

34. Se recomienda familiarizarse con los hosts, tipos de host y servicios, ya que se utilizan en el contexto de la plataforma NetWitness, descritos en la Guía de introducción a servicios y host de la plataforma RSA NetWitness.

35. A continuación, se muestra un diagrama de implementación de alto nivel de la plataforma *NetWitness*.

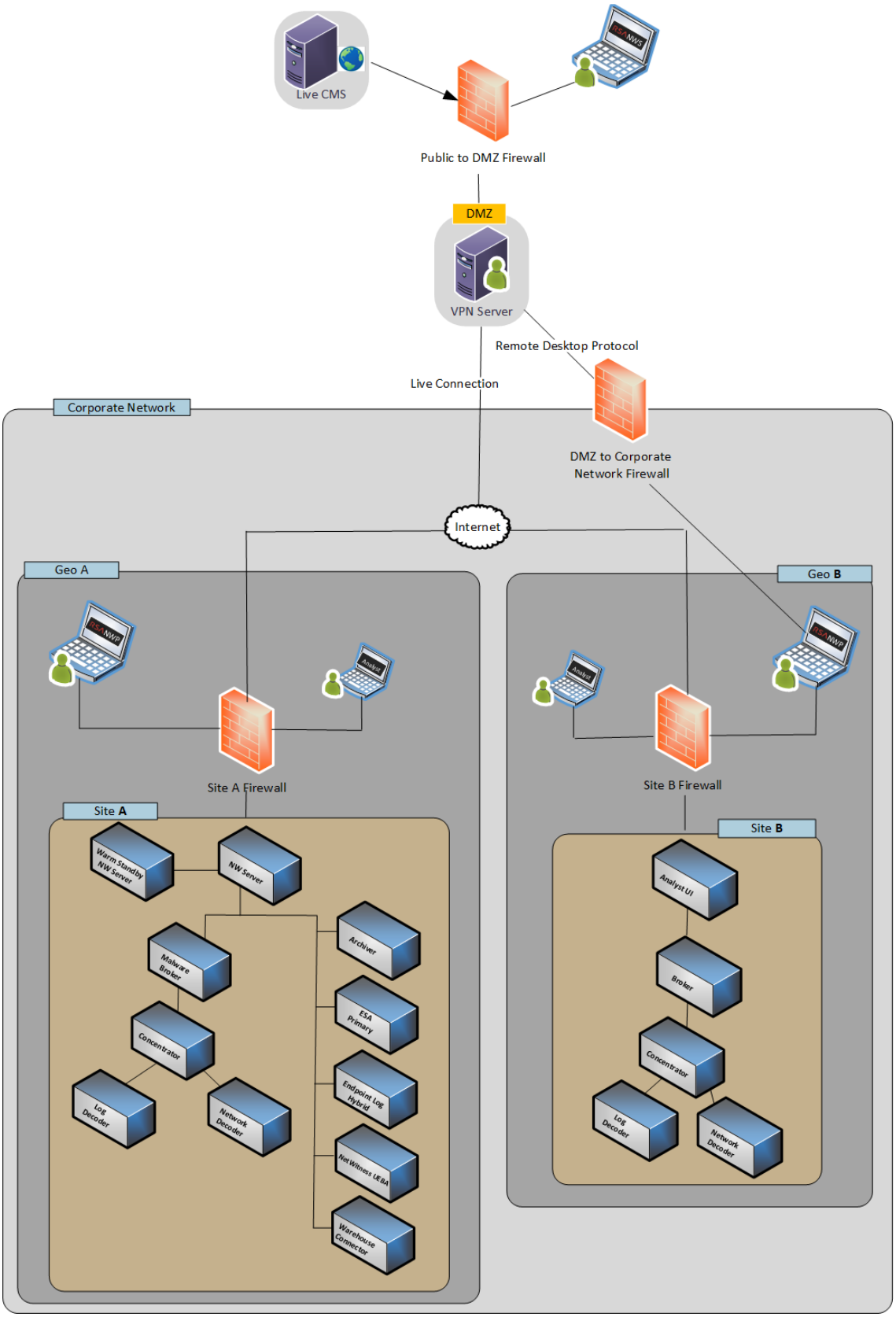

Ilustración 3 . Diagrama de implementación de alto nivel

36. A continuación, se muestra un diagrama detallado de implementación de host de la plataforma *RSA NetWitness*. El siguiente diagrama es un ejemplo de una implementación de *NetWitness Platform* hospedada en máquinas físicas o virtuales.

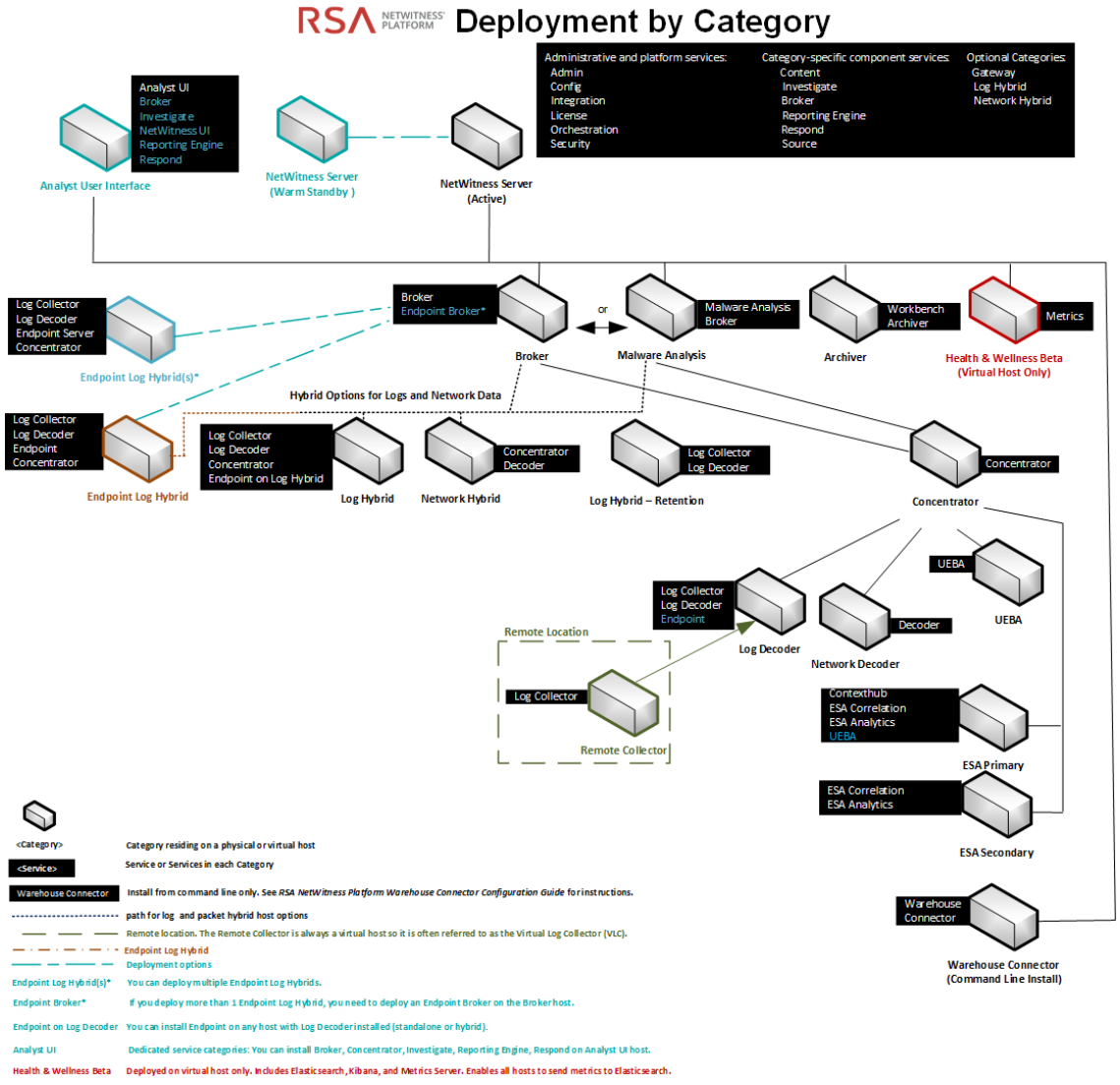

Ilustración 4. Diagrama de implementación.

4.5 INSTALACIÓN

37. Para la instalación se deben seguir las guías correspondientes de despliegue del producto mencionadas en el apartado anterior que incluyen tanto las consideraciones previas para cada tipo de despliegue como los pasos precisos y exactos a realizar.

38. Dado que los procedimientos de instalación detallados de cada componente de la plataforma Netwitness son muy extensos, se aconseja visitar los enlaces a cada uno de ellos descritos en el Apartado 8. REFERENCIAS. A continuación, se indican los más relevantes para la instalación inicial:

    a) Guía de implementación para *RSA NetWitness Platform:*

https://community.netwitness.com//t5/netwitness-platform-online/deployment-guide-for-11-6/ta-p/611035

b) Guía de instalación de hosts físicos de *RSA NetWitness Platform*:

https://community.netwitness.com//t5/netwitness-platform-online/physical-host-installation-guide-for-11-6/ta-p/611056

c) Guía de instalación de hosts virtuales de *RSA NetWitness Platform*:

https://community.netwitness.com//t5/netwitness-platform-online/virtual-host-installation-guide-for-11-6/ta-p/611069

d) Guía de introducción de hosts y servicios para RSA NetWitness Platform:

https://community.netwitness.com//t5/netwitness-platform-online/hosts-and-services-getting-started-guide-for-11-6/ta-p/611048

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

39. *NetWitness Platform 11.x* hace uso de módulos criptográficos seguros que gestionan todas las operaciones criptográficas. *NetWitness Platform* aprovecha dos módulos que cumplen con los requisitos de diseño de seguridad de nivel 3 del estándar FIPS 140-2:

    a) *RSA BSAFE Crypto-J.*

    b) *OpenSSL with BSAFE (OWB).*

40. De forma predeterminada, los módulos criptográficos aplican el uso de conjuntos de cifrado seguros siempre que sea posible. Por defecto, los grupos de cifrado configurados son los siguientes:

    a) **Servicio *Web nginx*:** *AESGCM:-aNULL:-DH:-kRSA:@STRENGTH*

    b) **Servicios *Core*** *(Log Collector, Log Decoder, Decoder, Concentrator, Broker, Archiver):* *-ALL:!aNULL:!DES:!3DES:HIGH*

41. Para obtener más información sobre cada uno de estos grupos, consultar la página: *https://www.openssl.org/docs/man1.0.2/man1/ciphers.html*.

42. El grupo de cifrado por defecto para el servicio Nginx (*AESGCM:-aNULL:-DH:-kRSA:@STRENGTH*) soporta las siguientes *cipher suites*, correspondientes al protocolo TLSv1.2 y con el nivel de seguridad mínimo requerido en la CCN-STIC-807:

```
[root@EndpointLogHybrid ~]# /usr/bin/openssl ciphers -v cipherlist AESGCM:-aNULL:-DH:-kRSA:@STRENGTH
ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AESGCM(256) Mac=AEAD
ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AESGCM(256) Mac=AEAD
ECDH-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH/RSA Au=ECDH Enc=AESGCM(256) Mac=AEAD
ECDH-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH/ECDSA Au=ECDH Enc=AESGCM(256) Mac=AEAD
ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AESGCM(128) Mac=AEAD
ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AESGCM(128) Mac=AEAD
ECDH-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH/RSA Au=ECDH Enc=AESGCM(128) Mac=AEAD
ECDH-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH/ECDSA Au=ECDH Enc=AESGCM(128) Mac=AEAD
```

Ilustración 5. Cipher suites del servicio Nginx.

    a. Se hace uso únicamente de TLSv1.2.

    b. Se utilizan únicamente *cipher suites* con autenticación.

    c. Se utilizan únicamente *cipher suites* con cifrado.

    d. No se utilizan *cipher suites* con DES o triple DES.

    e. Se utilizan longitudes de clave de 128 bits o superiores.

43. Sin embargo, podrán cambiarse las *cipher s*uites utilizadas por el servicio Web Nginx si así se requiere, cumpliendo con la fortaleza exigida en la CCN-STIC-807. Es importante tener en cuenta que estos cambios deberán revisarse y repetirse en caso necesario, siempre que se haga una actualización del sistema. Para ello se seguirán los siguientes pasos:

    a) Conectar por SSH al Servidor de *Netwitness*.

b) Abrir el archivo */var/netwitness/config-management/cookbooks/nw-nginx/templates/default/nw-ui.conf.erb* y editar la siguiente línea con los cifrados que se requieran:

ssl_ciphers "AESGCM:-aNULL:-DH:-kRSA:@STRENGTH";

c) Por ejemplo, se puede restringir la seguridad mínima AES a 256 bits para excluir el uso de longitudes de 128 bits. Para ello, se puede realizar la siguiente configuración:

ssl_ciphers "AESGCM:-aNULL:-DH:-kRSA:!AES128:@STRENGTH"";

d) Reiniciar el servicio nginx:

systemctl restart nginx

44. Deberán cambiarse los protocolos criptográficos utilizados por el servicio Core para poder cumplir con la fortaleza exigida en la CCN-STIC-807. Para ello se seguirán los siguientes pasos:

a) Conectar a la interfaz gráfica del Servidor de *Netwitness*.

b) Ir a *Admin > Services* y seleccionar el servicio que se desea cambiar. Después ir a *Explore.*

c) En el menú *Explore*, seleccionar los siguientes nodos en el árbol mostrado a la izquierda:

/sys > config

d) Aparecerá a la derecha una lista de opciones de configuración.

e) Editar la opción *ssl.cipher.list* con los cifrados requeridos. Se recomienda realizar la siguiente configuración para el uso de algoritmos seguros:

ssl_ciphers "-TLSv1.2:!SSLv3:!aNULL:!eNULL:!DES:!3DES:HIGH";

i. Se hace uso de *TLSv1.2*, para asegurar el uso de la versión 1.2 de TLS únicamente.

ii. Se hace uso de !SSLv3, para evitar las cipher suites que utilicen SSLv3.

iii. Se hace uso de *!aNULL,* para evitar las *cipher suites* sin autenticación.

iv. Se hace uso de *!eNULL,* para evitar las *cipher suites* sin cifrado.

v. Se hace uso de *!DES y !3DES,* para evitar las *cipher suites* que utilicen DES y triple DES.

vi. Se hace uso de *HIGH*¸ para forzar el uso de *cipher suites* que utilicen longitudes de clave de 128 bits o superiores.

f) Reiniciar el servicio (*<nwservicio>* puede tomar los valores: *nwlogcollector, nwlogdecoder, nwdecoder, nwconcentrator, nwbroker, nwarchiver*):

systemctl restart <nwservicio>

45. El modo de operación seguro está habilitado por defecto en todos los servicios excepto en el *Log Collector*. El modo de operación seguro no se puede deshabilitar en ningún servicio excepto para *Log Collector, Log Decoder* y *Decoder*. **No se recomienda deshabilitar el modo de operación seguro en ningún servicio.**

46. Los pasos necesarios para habilitar el modo de empleo seguro en los Log Collector, pueden consultarse en el apartado 5.1.1 MODO DE OPERACIÓN SEGURA PARA *LOG COLLECTORS*. De igual forma, en el apartado 5.1.2 MODO DE OPERACIÓN SEGURA PARA *DECODERS* Y *LOG DECODERS*, se pueden consultar los pasos necesarios para dichos servicios.

47. Para las actualizaciones a las versiones 11.x de NetWitness desde versiones anteriores, se aplican las siguientes condiciones para los servicios del *Log Collector, Log Decoder* y *Decoder:*

a) *Log Collector* no tendrá habilitado el modo de operación seguro después de actualizar a 11.x, incluso si se había habilitado en una versión anterior. Se debe habilitar la compatibilidad con FIPS después de actualizar a 11.x siguiendo los pasos indicados en el apartado 5.1.1.

b) Si el modo de operación seguro se había habilitado para los *servicios Log Decoder* y *Network Decoder* en una versión anterior, también se habilitará en 11.x. En caso contrario, se puede habilitar el modo de operación seguro manualmente para estos servicios si es necesario, siguiendo los pasos indicados en el apartado 5.1.2.

5.1.1 MODO DE OPERACIÓN SEGURA PARA *LOG COLLECTORS*

48. Para habilitar el modo de operación segura para los *Log Collector*:

a) Detener el servicio *Log Collector*.

b) Abrir el archivo:

/etc/systemd/system/nwlogcollector.service.d/nwlogcollector-opts-managed.conf

c) Cambiar el valor de la variable *Environment*:

Environment="OWB_ALLOW_NON_FIPS=on"

a desactivado:

Environment="OWB_ALLOW_NON_FIPS=off"

d) Volver a cargar el daemon del sistema ejecutando el siguiente comando:

systemctl daemon-reload

e) Reiniciar el servicio *Log Collector*.

f) Establecer el modo de operación segura para el servicio *Log Collector* en la interfaz de usuario:

i. Ir a *Admin > Services*.

ii. Seleccionar el servicio del *Log Collector*. Ir a *View > Config*.

iii. En el **modo SSL FIPS**, seleccionar la casilla de verificación en Valor de configuración y hacer clic en *Apply*.

5.1.2 MODO DE OPERACIÓN SEGURA PARA *DECODERS* Y *LOG DECODERS*

49. Para habilitar el modo de operación segura para *Decoders* y *Log Decoders*:

a) Ir a *Admin > Services* y seleccionar un servicio *de Decoder o Log Decoder.*

b) Seleccionar *View > Config* y, en *System Configuration*, habilitar SSL FIPS Mode seleccionando la casilla de verificación en la columna *Config Value.*

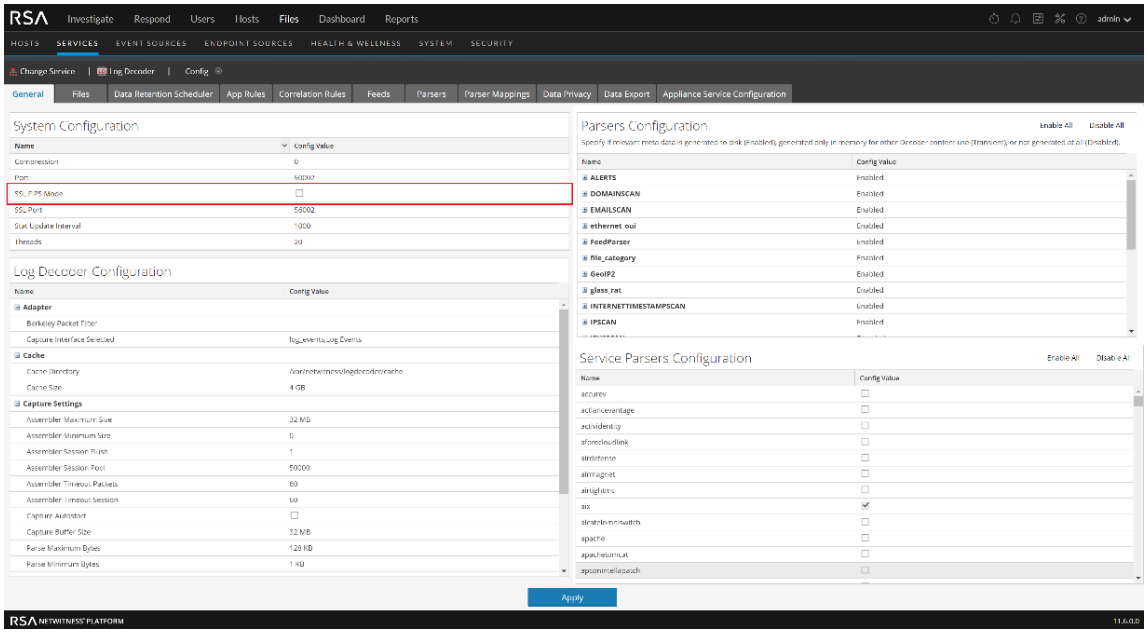

Ilustración 6. Configuración del modo seguro en Log *Decoders* y *Decoders*

c) Reiniciar el servicio.

d) Hacer clic en *Apply*.

5.2 AUTENTICACIÓN

5.2.1 AUTENTICACIÓN DE USUARIOS

50. En la guía *Administración de los usuarios y seguridad del sistema – REF3*, se encuentran detallados los distintos mecanismos de administración de usuarios y seguridad del sistema.

51. *RSA NetWitness Platform* dispone de los siguientes mecanismos de autenticación de usuarios:

    a) Credenciales Locales. El producto puede crear y gestionar cuentas de usuario localmente. La configuración de la creación y gestión de cuentas de usuarios locales se describe en el apartado 5.3.2 Configuración de las cuentas de usuario.

    b) Servidores Externos de Autenticación. La configuración de servidores externos de autenticación se encuentra detallada en el apartado Configurar la autenticación externa de la guía *Administración de los usuarios y seguridad del sistema – REF3.*

    c) *Active Directory*. La configuración de *Active Directory* se describe a continuación.

5.2.1.1 CONFIGURACIÓN DE ACTIVE DIRECTORY

52. Para configurar el uso de *Active Directory*, deberán seguirse los siguientes pasos desde la interfaz de administración:

    a) Ir a Administrar > Seguridad.

    b) Hacer clic en la pestaña Ajustes de configuración.

    c) Agregar, editar o eliminar dominios en caso necesario.

    d) En Configuraciones de *Active Directory*, hacer clic en el icono de añadir ("+").

    e) Seleccionar la casilla de verificación Activado.

    f) Ingresar la información de Dominio, Host y Puerto para el servicio de *Active Directory*.

    g) Para elegir SSL para esta configuración, seleccionar la casilla de verificación Usar SSL. A continuación, ingresar un archivo de certificado del servidor de *Active Directory*. Para ello, hacer clic en Navegar y seleccionar el archivo.

    h) En el campo Mapeo de nombres de usuario, seleccionar el campo de búsqueda de *Active Directory* que se usará para el mapeo de nombre de usuario. Es posible seleccionar *userPrincipalName (UPN)* o *sAMAccountName.*

    i) Para sitios que tengan múltiples servidores de autenticación, hacer clic en Seguir referencias para activar o desactivar el seguimiento de referencias de LDAP para búsquedas de grupos de AD.

    j) Para proporcionar credenciales para vincular al servicio *Active Directory* mientras busca un grupo de *Active Directory*, ingresar las credenciales en los campos *Nombre de usuario* y *Contraseña*.

    k) Hacer clic en *Guardar*.

53. Es posible consultar el detalle en el apartado "*Configurar Active Directory*" de la guía Administración de los usuarios y seguridad del sistema – REF3.

54. Autenticación por certificados (PKI). Es posible encontrar el detalle en la guía *Set Up Public Key Infrastructure (PKI) Authentication – REF4.* A continuación, se indican los pasos necesarios para realizar la configuración de la autenticación por certificados en *Active Directory* desde la interfaz de administración:

    a) Configurar *Active Directory* siguiendo los pasos indicados anteriormente.

    b) Mapear, al menos, un grupo de usuarios de *Active Directory* al rol de *Administrators* de Netwitness:

        i. Ir a Administrar > Seguridad > pestaña Usuarios.

        ii. Hacer clic en la pestaña *Mapeo de grupo externo*.

        iii. En la barra de herramientas, hacer clic en el icono de añadir ("*+*").

        iv. Hacer clic en *Buscar*, buscar el nombre del grupo de *Active Directory* en el cuadro de diálogo *Buscar* y seleccionar el nombre del grupo encontrado.

        v. Para agregar el rol de Administradores al grupo de *Active Directory*, hacer clic en el icono de añadir ("+") debajo de la sección Funciones mapeadas.

        vi. Seleccionar la casilla de verificación que hay al lado del rol Administradores.

        vii. Hacer clic en *Agregar*.

        viii. Hacer clic en *Guardar*.

    c) Importar el certificado de la Autoridad de Certificación (CA) desde el menú *Administrar > Seguridad > pestaña de Configuración PKI > Autoridades de Certificación confiables (Trusted CAs).*

    d) En el menú de importación del CA, se dará también la opción de importar los certificados de usuario. Copiar y pegar los certificados en formato PEM (Base64).

    e) Deberán generarse los certificados de usuario **con claves de 3072 bits o superior.** El procedimiento para generar los certificados de usuario es externo a *Netwitness*, por favor consulte con su Autoridad de Certificación (CA).

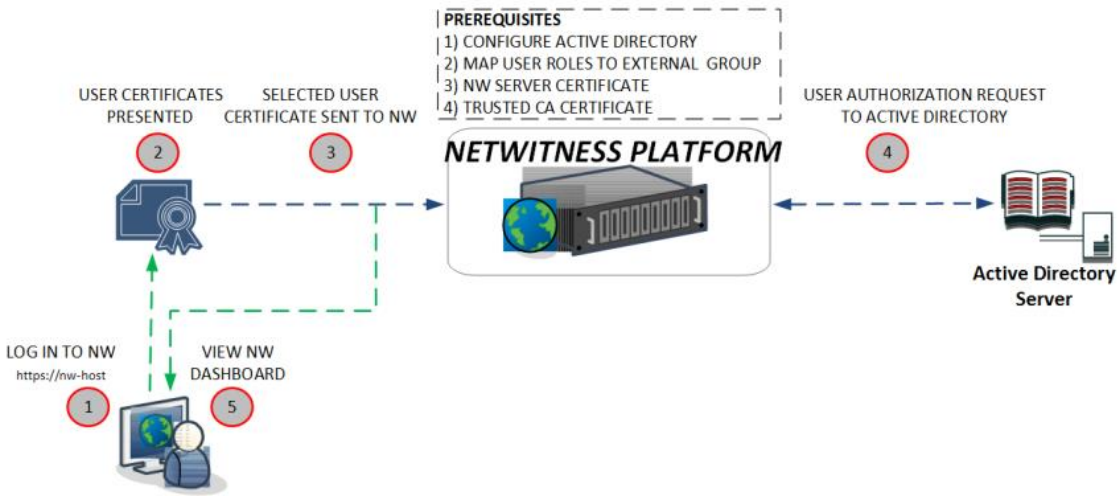

Ilustración 7. Esquema autenticación *NetWitness*

5.2.2 AUTENTICACIÓN ENTRE COMPONENTES

55. Los *endpoints* se comunican de forma segura con el servidor *Endpoint Log Hybrid* a través de HTTPS mediante TLS.

56. *RSA NetWitness* realiza operaciones criptográficas TLS en un modo de operación seguro. Estas operaciones TLS se utilizan para la comunicación entre los usuarios y la consola gráfica de administración (servicio web en el Servidor de Netwitness) y para la comunicación interna entre los servicios Core de *Netwitness*, que consisten en el *Log Collector*, *Log Decoder*, *Concentrator*, Broker y *Archiver*.

57. La comunicación interna se produce entre los distintos componentes que forman la solución *RSA Netwitness*. Cada instancia del sistema garantiza que dicha comunicación se produce solo a través de TLS en la vía de comunicación protegida en modo de operación seguro.

58. La comunicación a través de TLS se usa por defecto al instalar cada componente, pero se puede verificar su uso siguiendo los siguientes pasos:

    a) Ir a *Administrar > Servicios*.

    b) Seleccionar el servicio Core que se desee verificar (por ejemplo, un *Concentrator*) y hacer clic en el icono de Editar servicio.

    c) En el cuadro de diálogo que aparece, verificar que la casilla SSL está habilitada.

    d) Verificar que no hay ningún usuario ni contraseña especificados en los campos de *Usuario* y *Password*, respectivamente. Los campos de *usuario* y *password* se usan si se quiere configurar el servicio con protocolo estándar no encriptado (no-TLS).

    e) Hacer clic en el botón *Comprobar conexión* para verificar que la conexión TLS con el servicio funciona correctamente.

59. El producto utiliza la biblioteca criptográfica R*SA BSAFE Crypto-J: BSAFE SSL-J 6.2.1.1* para la comunicación interna entre los servicios basados en Java, que incorpora *BSAFE Crypto-J 6.2*. Los servicios basados en Java son:

    a) Servicios internos instalados en el *Servidor de Netwitness*:

        i. *nw-admin-server*: administra los demás servicios *Netwitness*.

        ii. *nw-config-server*: administra la configuración de todos los servicios.

        iii. *nw-orchestration-server*: administra la orquestación de los servicios.

        iv. *nw-security-server*: administra la seguridad de los servicios.

    b) Servicios instalados fuera del Servidor de Netwitness:

        i. *rsa-nw-correlation-server*: servicio de correlación de alertas (instalado en *Event Stream Analysis* (ESA)).

        v. *nw-malware-analytics*: servicio que realiza el análisis de malware (instalado en *Malware Analysis*).

60. El sistema *Lockbox* instalado en los *Log Collectors*, se utiliza para proteger las credenciales que se configuran para recolectar los logs de las fuentes de eventos. Utiliza *Common Security Toolkit*, versión 3.3.0.12. *Crypto-C ME 4.1.4*. Utiliza las Cipher Suites:

    a) *TLS_ECDHE_RSA_AES_128_GCM_SHA256*

    b) *TLS_ECDHE_RSA_AES_128_CBC_SHA256*

    c) *TLS_DHE_RSA_AES_128_GCM_SHA256*

61. El sistema utiliza *Crypto-C ME 4.1.4* para las conexiones mediante SSH y TLS en el modo de operación seguro.

62. Cualquier comunicación interna entre los servicios de NetWitness utilizará las *Cipher Suites* mencionadas anteriormente, mientras que los clientes externos que no admiten dichos conjuntos de cifrado e interactúen con estos servicios podrán seguir admitiendo el protocolo de enlace SSH/TLS y la conexión.

63. El sistema utiliza TLS versión 1.2 para las comunicaciones internas usando los siguientes *ciphersuites*:

    a) *TLS_ECDHE_RSA_AES_256_GCM_SHA384*

    b) *TLS_ECDHE_ECDSA_AES_128_GCM_SHA256*

    c) *TLS_DHE_RSA_AES_128_GCM_SHA256*

    d) *TLS_ECDHE_RSA_AES_128_CBC_SHA256*

    e) *TLS_RSA_AES_128_CBC_SHA256*

    f) *TLS_ECDHE_ECDSA_AES_256_GCM_SHA384*

g) *TLS_ECDH_RSA_AES_256_GCM_SHA384*

h) *TLS_ECDH_ECDSA_AES_256_GCM_SHA384*

i) *TLS_ECDH_RSA_AES_128_GCM_SHA256*

j) *TLS_ECDH_ECDSA_AES_128_GCM_SHA256*

k) *TLS_ECDHE_RSA_AES_128_GCM_SHA256*

2. Se puede configurar el conjunto de cifrados aceptados por cada servicio siguiendo los pasos indicados en el apartado 5.1 MODO DE OPERACIÓN SEGURO.

5.2.3 AUTENTICACIÓN DE SESIONES

64. Una sesión de administración remota se inicia mediante un inicio de sesión y se produce solo a través de HTTPS mediante TLS versión 1.2.

65. El producto implementa el protocolo SSH para el acceso CLI y utiliza la autenticación basada en clave pública. El producto utiliza los siguientes algoritmos de cifrado para el transporte SSH: *AES-CTR-128, AES-CTR-192* y *AES-CTR-256*. La implementación del transporte SSH utiliza los algoritmos de clave pública ecdsa-sha2-nistp256; y algoritmos de integridad de datos *hmac-sha1*, *hmac-sha2-256* y *hmac-sha2-512* para la conexión de transporte SSH. Los métodos de intercambio de claves utilizados para el protocolo SSH incluyen: *ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512* y *diffie-hellman-group14-sha256*.

66. Se deberá modificar la configuración por defecto editando las siguientes opciones del archivo */etc/ssh/sshd_config*:

a) Algoritmos de cifrado. Modificar el siguiente valor:

***Ciphers**: aes256-ctr*

b) Algoritmos de intercambio de clave. Modificar el siguiente valor:

***KexAlgorithms:** ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512*

c) Algoritmos de integridad de datos. Modificar el siguiente valor:

***MACs**: hmac-sha2-256, hmac-sha2-512*

5.2.4 AUTENTICACIÓN EN REENVÍO DE LOGS A SISTEMAS EXTERNOS

67. El *Log Decoder* puede reenviar logs a dispositivos externos a *Netwitness* a través de *Syslog TLS*. Para el detalle de la configuración del reenvío de logs a sistemas externos, se deberá consultar el siguiente enlace:

https://community.netwitness.com/t5/netwitness-platform-online/configure-syslog-forwarding-to-destination/ta-p/669178

68. A continuación, se muestran los pasos principales para el uso de Syslog TLS en dichas comunicaciones:

a) Durante la definición del destino de *Syslog*, indicar el uso del protocolo TLS y del puerto 6514, que es el normalmente utilizado para *Syslog TLS*, en el parámetro */decoder/config/logs.forwarding.destination*:

name=tls:<nombrehostdestino>:6514

b) Para ello, acceder con usuario administrador a la siguiente ruta: *Services > Log Decoder > Explore > Decoder > Config*, a través de la Interfaz de usuario.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

69. En caso de realizar la administración del producto de manera remota, se utilizará la GUI web a través de HTTPS.

70. En caso de llevar a cabo las tareas de administración de forma local, se utilizará SSH.

5.3.2 CONFIGURACIÓN DE LAS CUENTAS DE USUARIO

71. El producto mantiene cuentas de usuario para los usuarios autorizados del sistema y una lista de atributos de seguridad para cada usuario que incluye el nombre de usuario, el rol asignado y la contraseña cifrada (en caso de hacer uso de la autenticación local). El sistema proporciona los siguientes roles o perfiles predefinidos:

    a) ***Administrators***: Tienen acceso completo al sistema. El perfil Administradores del sistema cuenta con todos los permisos de forma predeterminada.

    b) ***Respond Administrators***: Pueden acceder a todos los permisos del módulo Respond, que es el módulo para ver y analizar alertas e incidentes. El perfil Administrador de *Respond* se centra en la configuración del sistema de *Respond*.

    c) ***Operators***: Tienen acceso a configuraciones, pero no a metadatos ni a contenido de sesiones. El perfil Operadores del sistema se centra en la configuración del sistema, pero no en I*nvestigation, ESA, Alerting, Reporting ni Respond.*

    d) ***Analysts***: Tienen acceso a metadatos y al contenido de los logs y de los paquetes de red (sesiones), pero no tienen acceso a ninguna configuración. Este perfil se centra en los módulos de *Investigation, ESA, Alerting, Reporting* y *Respond*, pero no tienen acceso a la configuración del sistema.

    e) ***SOC Managers***: Tienen el mismo acceso que poseen los *Analysts*, además del permiso adicional para administrar y configurar incidentes y notificaciones.

f) ***Malware Analysts***: Tienen acceso a investigaciones y eventos de malware. El único acceso que se otorga al perfil Analistas de malware es al módulo *Malware Analysis*.

g) ***UEBA_Analyst***: Tienen acceso al servicio *RSA NetWitness UEBA en Investigate* > vista Usuarios. *NetWitness UEBA* es una solución de analítica avanzada para descubrir, investigar y monitorear comportamientos sospechosos en los usuarios del entorno de red.

h) ***Data Privacy Officer (DPO):*** Este perfil es similar al de los Administradores, pero está centrado en opciones de configuración que administran la ofuscación y la visualización de datos confidenciales dentro del sistema. Los usuarios a los cuales se asigna la función DPO pueden ver qué claves de metadatos están configuradas como ofuscadas y también pueden ver sus valores.

i) ***Reporting Engine Content Administrators:*** Este perfil da acceso a gestionar el contenido de Live Content. Los usuarios con este perfil podrán desplegar contenido de Reporting Engine (reglas, reportes, gráficos, listas) desde Live Content, ver y gestionar los permisos para el contenido desplegado en Reporting Engine.

72. Como norma general, a la hora de configurar usuarios deberá seguirse una política de mínima funcionalidad y mínimo privilegio. Es decir, el menor número de usuarios privilegiados a los que se asignará un rol con los mínimos privilegios requeridos para hacer su trabajo. Además, se recomienda no compartir cuentas de usuario y darlas de baja cuando ya no sean necesarias.

73. El detalle sobre la configuración de usuarios y roles se puede consultar en la guía Administración de usuarios y de la seguridad del sistema *Guía para la versión 11.x – REF3.*

74. Para agregar Roles y asignar permisos, seguir los siguientes pasos:

    a) Ir a *Administrar > Seguridad > pestaña Usuarios.*

    b) Hacer clic en la pestaña *Roles*.

    c) Hacer clic en el icono de añadir ("+") en la barra de herramientas.

    d) En el cuadro de diálogo Agregar Rol, escribir la siguiente información para definir el rol: Nombre y Descripción.

    e) En la sección Permisos:

        i. Seleccionar un módulo al que se quiera dar permisos de acceso para el rol, por ejemplo: *Administration, Alerting, Dashboard*, etc.

        ii. Seleccionar cada permiso dentro del módulo al que podrá acceder el rol.

        iii. Repetir los pasos anteriores hasta seleccionar todos los permisos deseados.

f) Hacer clic en *Guardar*.

75. Para crear Usuarios, seguir los siguientes pasos:

a) Ir a *Administrar > Seguridad > pestaña Usuarios.*

b) Hacer clic en el icono de añadir ("+") en la barra de herramientas.

c) En el cuadro de diálogo Agregar usuario, escribir la siguiente información para definir el nuevo usuario:

i. Tipo de autenticación: *NetWitness* (local) / *Active Directory* / PAM.

ii. Nombre de usuario.

iii. Dirección de Correo electrónico.

iv. Contraseña.

v. Nombre completo del nuevo usuario.

vi. Descripción de la cuenta de usuario.

vii. Forzar cambio de contraseña en el próximo *login*: seleccionar esta opción para forzar al usuario a cambiar la contraseña la primera vez que inicie sesión.

d) Asignar un *Rol* al usuario:

i. Hacer clic en el icono de añadir ("+") en la pestaña Roles.

ii. El cuadro de diálogo de selección *Agregar Role* se muestra la lista de Roles disponibles.

iii. Seleccionar el Rol deseado y hacer clic en *Agregar*.

e) Haga clic en *Guardar*.

76. Para configurar los parámetros de complejidad de contraseña de los usuarios, seguir los siguientes pasos:

a) Ir a *Administrar > Seguridad*.

b) Hacer clic en la pestaña Ajustes de configuración.

c) En la sección *Configuración de contraseña*, seleccionar los requisitos de complejidad de contraseña.

d) Hacer clic en *Aplicar*.

77. Los requisitos de complejidad de las contraseñas deberán ser, como mínimo:

a) Longitud de la contraseña: valor recomendado **12 caracteres**.

b) Deben estar compuestas por una combinación de caracteres pertenecientes, al menos, a 3 o 4 de los siguientes grupos de caracteres:

i. Caracteres en minúscula.

ii. Caracteres en mayúscula.

iii. Números.

iv. Caracteres especiales.

b) Cuando se cambia la contraseña, esta tendrá que:

i. Diferir de la anterior en, al menos, 4 caracteres.

ii. Diferir, al menos, de las 5 contraseñas anteriores.

c) El cambio de contraseña debe realizarse cada cierto tiempo, máximo de 60 días para los administradores.

d) Desde el cambio de contraseña, esta no puede ser cambiada en un mínimo de 4 días.

e) Algunas buenas prácticas en la selección de la contraseña, son: evitar palabras de diccionario, secuencias numéricas, secuencias de caracteres seguidos en el teclado, evitar añadir números al final de la palabra o números al final de la contraseña anterior, caracteres repetidos, información personal, etc.

78. Deberán cambiarse las contraseñas predeterminadas de las cuentas de administrador tras acceder por primera vez al sistema con estas. Los pasos para cambiar la contraseña del usuario *Admin* de *NetWitness Platform* son los siguientes:

a) Acceder a la interfaz de *Netwitness* con el usuario *Admin*.

b) Hacer clic en el icono de usuario situado en la parte superior derecha de la pantalla y seleccionar *Perfil*.

c) En la sección *Cambiar mi contraseña*, ingresar los datos:

i. Contraseña anterior.

ii. Nueva contraseña.

iii. Confirmar contraseña.

d) Hacer clic en Restablecer contraseña.

e) Se cerrará la sesión de *NetWitness Platform* para aplicar los cambios.

79. Seguir los siguientes pasos para cambiar la contraseña del usuario administrador de los servicios:

a) En la interfaz de *Netwitness*, ir a *Administar > Servicios*.

b) Seleccionar un servicio, hacer clic en el icono de la rueda *> Ver > Seguridad*.

c) En la pestaña *Usuarios*, seleccionar el usuario *Admin*.

d) En el campo *Contraseña*, ingresar una nueva contraseña de administrador para el servicio seleccionado.

e) En el campo *Confirmar contraseña*, volver a escribir la nueva contraseña.

f) Hacer clic en *Aplicar*.

g) Repetir los pasos *a)-f)* para todos los servicios.

h) Después de cambiar la contraseña en los servicios, es necesario eliminar y volver a agregar un origen de datos en *Reporting Engine*, siguiendo los siguientes pasos:

i. En la interfaz de *Netwitness*, ir a *Administrar > Servicios*.

ii. En la vista *Servicios*, seleccionar *Reporting Engine*, hacer clic en el icono de la rueda *> Ver > Configurar*.

iii. Hacer clic en la pestaña *Orígenes*.

iv. Seleccionar el servicio que se desee quitar y hacer clic en el icono de borrado ("-").

v. Hacer clic en el icono de añadir ("*+*") y seleccionar *Servicios disponibles*.

vi. Seleccionar el servicio eliminado en el paso *iv)* y hacer clic en *Aceptar*.

vii. Cuando se solicite, ingresar el nombre de usuario *admin* y la nueva contraseña para el servicio.

5.3.3 CONFIGURACIÓN DE LOS PARÁMETROS DE SEGURIDAD

80. Deberán configurarse los parámetros de seguridad descritos en el paso 3 'Configurar ajustes de seguridad en el nivel del sistema' de la guía Administración de usuarios y de la seguridad del sistema Guía para la versión 11.x – REF3. A continuación se indican las recomendaciones principales:

a) En la interfaz de *NetWitness*, ir a *Administrar > Seguridad*.

b) Se mostrará la vista *Seguridad* con la pestaña *Usuarios* abierta.

c) Hacer clic en la pestaña Ajustes de configuración.

d) En la sección Configuración de seguridad, especificar los valores de la siguiente lista:

i. **Periodo de bloqueo.** Cantidad de minutos para bloquear a un usuario de *NetWitness Platform* después de que se haya excedido la cantidad configurada de inicios de sesión fallidos. El valor predeterminado es 20 minutos.

ii. **Número máximo de errores al iniciar sesión.** Cantidad máxima de intentos de inicio de sesión fallidos antes de que un usuario se bloquee. El valor predeterminado es 5 y no se recomienda utilizar un número mayor.

iii. **Tiempo de espera de sesión agotado.** Duración máxima en minutos de una sesión de usuario, una vez alcanzado el valor definido se cierra

la sesión y es necesaria una reautenticación. El valor predeterminado es 480 y el valor máximo permitido es 30,000.

iv. **Periodo de inactividad.** Cantidad de minutos de inactividad antes de que se cierre la sesión y sea necesaria una reautenticación. El valor predeterminado es 10, que es el recomendado. El valor máximo permitido es 30,000.

v. **Los nombres de usuario distinguen mayúsculas de minúsculas.** Esta opción permite que el campo Nombre de usuario de la pantalla de inicio de sesión de *NetWitness Platform* distinga mayúsculas de minúsculas. Por ejemplo, si los nombres de usuario distinguen mayúsculas de minúsculas, podría usar *admin* para iniciar sesión en *NetWitness Platform*, pero no podría usar *admin*).

81. Se recomienda configurar un mensaje de aviso en inicio de sesión. El detalle de configuración del banner de acceso se puede consultar en el apartado Pestaña Banner de inicio de sesión de la guía Administración de usuarios y de la seguridad del sistema *Guía para la versión 11.x – REF3.* A continuación se indican los principales pasos a seguir:

    a) En la interfaz de *Netwitness*, ir a *Administrar > Seguridad*.

    b) Se mostrará la vista *Seguridad* con la pestaña *Usuarios* abierta.

    c) Hacer clic en la pestaña *Banner de inicio de sesión*.

    d) Escribir los datos del banner en los siguientes campos:

        i. **Prefijo de título del servidor:** Muestra el prefijo del servidor *NetWitness* en la barra de título.

        ii. **Habilitar:** Casilla de verificación para indicar la activación del banner de inicio de sesión (por defecto está desactivado).

        iii. **Título del anuncio de inicio de sesión:** Muestra el título del banner de inicio de sesión.

        iv. **Mensaje del anuncio de inicio de sesión:** Muestra el mensaje que le aparecerá al usuario que inicie sesión en *Netwitness*.

    e) Hacer clic en *Aplicar* para guardar los cambios.

82. Para evitar modificaciones no autorizadas del menú de arranque, se recomienda modificar la contraseña por defecto del *boot loader*. Para ello, se seguirán los siguientes pasos:

    a) Como usuario *root*, ejecutar el comando *grub2-setpassword.*

    b) Introducir la contraseña deseada.

83. Para prevenir el inicio interactivo del sistema, se recomienda desactivar el parámetro PROMPT en el fichero */etc/sysconfig/init*:

    PROMPT= no

84. El producto permite la configuración de distintos parámetros de seguridad de la información:

    a) *Data Obfuscation*: definición de la información considerada sensible para la organización, la cual será ofuscada. Se deberá hacer uso de *sha-256* como algoritmo de hash.

    b) *Data Retention Enforcement*: definición de los periodos de retención de la información necesarios.

85. El detalle de la configuración de la seguridad de la información se puede consular en la guía *Data Privacy Management Guide for RSA NetWitness – REF23.*

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

86. Deberán desactivarse todos aquellos puertos considerados no seguros, para lo cual se recomienda consultar el apartado FIPS *Compliance*, *Disabling Unencrypted Ports* de la guía *Security Configuration Guide for NetWitness 11.x* – REF6. Los principales pasos a seguir son los siguientes:

    a) En la interfaz de Netwitness, ir a *Administrar > Servicios.*

    b) Seleccionar un servicio Core (*Log Collector, Log Decoder, Concentrator, Broker, Archiver*).

    c) Hacer clic en el icono de la rueda *> Ver > Config.*

    d) Seleccionar la pestaña *General.*

    e) En la sección de *Configuración del Sistema*, cambiar el campo *Puerto* al valor “0”.

    f) En la pestaña de *Configuración del servicio Appliance*, cambiar el campo *Puerto* al valor “0”.

    g) Hacer clic en Aplicar para guardar los cambios y en reiniciar el servicio si lo solicita la interfaz.

5.5 GESTIÓN DE CERTIFICADOS

87. El procedimiento para el cambio de certificado del servidor web que utiliza la interfaz de NetWitness se encuentra en el apartado *Security Configuration: Customer Provided Certificates de la guía Security Configuration Guide for NetWitness 11.x – REF6*. Los principales pasos a seguir son los siguientes:

    a) Renombrar los archivos de certificado que se desea utilizar de la siguiente forma:

        i. Renombrar *cert.pem* a *web-server-cert.pem.*

        ii. Renombrar *key.pem* a *web-server-key.pem*.

        iii. Renombrar *cert.chain* a *web-server-cert.chain*.

        iv. Renombrar *cert.p7b* a *web-server-cert.p7b.*

b) Copiar los archivos del paso *a)* en el Servidor de Netwitness, por ejemplo, en la carpeta */root/*. Para copiar los archivos puede usar el comando *scp* desde un sistema Linux/UNIX o el programa *WinSCP* desde Windows.

c) Conectar por SSH al Servidor de Netwitness.

d) Hacer una copia de seguridad de los archivos de certificado actual:

cp /etc/pki/nw/web/web-server-cert.pem Directorio_Destino

cp /etc/pki/nw/web/web-server-key.pem Directorio_Destino

cp /etc/pki/nw/web/web-server-cert.chain Directorio_Destino

cp /etc/pki/nw/web/web-server-cert.p7b Directorio_Destino

e) Si los archivos del paso *a)* se copiaron a la carpeta */root*, utilizar el siguiente comando para copiarlos a la carpeta de certificados del servidor web:

cp web-server- /etc/pki/nw/*

f) Reiniciar el servicio con el siguiente comando:

systemctl restart nginx

88. Para refirmar los certificados que usa internamente NetWitness para la intercomunicación de sus servicios, debe utilizarse la herramienta *CA Security Reissue Tool*. Consultar el apartado *Security Configuration: Reissue Certificates* de REF6. Los certificados CA Root tienen una validez de 10 años mientras que los certificados de servicios tienen una validez de 1000 días.

89. Se recomienda consultar el apartado indicado de la guía REF6 para el detalle del proceso de refirmado de los certificados, ya que éste puede cambiar y tener un impacto elevado en la plataforma si no se siguen las indicaciones actualizadas.

90. Antes de comenzar el proceso, es importante saber que los servicios se reinician durante el proceso de refirmado y pueden causar interrupciones en la captura de paquetes de red o de logs.

91. Se debe completar el proceso de refirmado de los distintos sistemas del entorno NetWitness en la misma ventana de mantenimiento.

92. En caso de contar con sistemas WLC (*Windows Legacy Collector*) instalados en el entorno, se debe seguir un procedimiento distinto que para el resto de *hosts*. Se debe completar el refirmado de los sistemas WLC también en la misma ventana de tiempo que el resto.

93. A continuación, se detalla el proceso de refirmado del certificado CA Root para todos los hosts exceptuando los sistemas WLC (REF5):

a) Descargar el archivo *root-ca-update.zip* desde la siguiente dirección:

https://community.netwitness.com//t5/netwitness-platform-downloads/certificate-re-issue-tool-for-rsa-netwitness-11-x/ta-p/564444

y el archivo *ca-expire-test.sh* desde la siguiente dirección:

https://community.netwitness.com/t5/netwitness-knowledge-base/reissue-root-ca-security-certificates-on-rsa-netwitness-platform/ta-p/677405

b) Descomprimir y copiar los archivos a una carpeta del servidor de Netwitness, por ejemplo */root/reissue-certs/*.

c) Conectar por SSH al Servidor de Netwitness.

d) Ir a la carpeta donde se hayan copiado los archivos, por ejemplo:

cd /root/reissue-certs/

e) Ejecutar el test de expiración de certificados con el comando:

sh ca-expire-test.sh --version 11.x

Si se ejecuta correctamente, el resultado muestra si el certificado está expirado o no, y los días que le faltan para que expire. Por ejemplo:

You must re-issue certificate within 297 days

f) Ejecutar el siguiente comando para guardar información sobre el certificado actual en un archivo:

keytool -printcert -file /etc/rabbitmq/ssl/truststore.pem | grep -Ei "owner|valid" >> /var/log/netwitness/cert-renew-precheck.out

g) Ejecutar el siguiente comando para quitar el certificado de la antigua versión de Netwitness del trustore:

nw-root-ca-update --clean-imports

h) Ejecutar el siguiente comando para renovar el certificado raíz de Netwitness:

nw-root-ca-update --renew-ca

i) Introducir la contraseña del usuario deploy_admin cuando se pida. Este paso durará varios minutos, espere a que termine.

j) Si termina de forma correcta, se mostrará el siguiente mensaje:

root CA update successful, run --synch-host to update component hosts

k) Para sincronizar el nuevo certificado raíz con el resto de sistemas, ejecutar el siguiente comando:

nw-root-ca-update --synch-host --host-all

l) Tardará varios minutos por cada uno de los sistemas configurados. Durante el proceso, los servicios pueden aparecer offline en la interfaz gráfica. Estimar el tiempo necesario basándose en el número de sistemas Netwitness configurados en el entorno y esperar a que termine completamente el proceso.

m) En vez de ejecutar el comando anterior para sincronizar todos los sistemas en un mismo comando, es posible lanzar los siguientes comandos para sincronizar los sistemas en grupos de varios sistemas especificados como parámetros:

Opción 1: Ejecutar el siguiente comando para sincronizar los sistemas de forma secuencial:

nw-root-ca-update --synch-host --host-id <node-id1> --host-id <node-id2>

Opción 2: Ejecutar el siguiente comando para sincronizar los sistemas de forma paralela:

nw-root-ca-update --use-parallel --synch-host --host-id <node-id1> --host-id <node-id2>

a) Es posible consultar el node-id de los sistemas dentro del archivo /etc/salt/minion en cada sistema, o lanzando el comando *upgrade-cli-client --list* en el Servidor de Netwitness para listarlos todos.

b) Cuando termine el proceso, lanzar de nuevo el test de expiración del certificado para confirmar que se ha renovado correctamente. Verificar que la validez es la establecida en la política de seguridad del organismo:

sh ca-expire-test.sh --version 11.x

c) Confirmar que todos los servicios de Netwitness se están ejecutando correctamente desde la interfaz de *Netwitness > Admin > Services*.

94. A continuación, se indican los pasos necesarios para la renovación del certificado CA Root en sistemas WLC (REF5):

a) Confirmar que el certificado se ha renovado en todos los demás sistemas antes de seguir con los siguientes pasos.

b) Conectar al Servidor de Netwitness por SSH.

c) Cambiar a la siguiente carpeta:

cd /var/netwitness/root-ca-update/wlc

d) Hacer un listado de archivos y comprobar que los siguientes dos archivos existen:

 # ls

wlc-cert-renew-11.x.sh

update-WLC-truststore.bat

e) Crear un archivo llamado "*wlc-systems*":

vi wlc-systems

Este archivo deberá contener los datos de cada sistema WLC en cada línea, en el formato:

<dirección_ip_wlc1>,<usuario_admin_wlc1>,<password_admin_wlc1>

<dirección_ip_wlc2>,<usuario_admin_wlc2>,<password_admin_wlc2>

...

f) Comprobar los datos de los certificados actuales con el comando:

#./wlc-cert-renew-11.x.sh wlc-systems

g) Renovar los certificados con el comando:

 # ./wlc-cert-renew-11.x.sh --renew wlc-systems

Si el proceso termina correctamente mostrará un mensaje con el texto "*completed success*fuly".

h) Conectar al WLC usando las credenciales de administrador de Windows.

i) Copiar el archivo *update-WLC-truststore.bat*, mencionado en el paso *d)* a una carpeta del WLC.

j) Ejecutar una línea de comandos de Windows y cambar a la carpeta donde está el archivo *update-WLC-truststore.bat*. Ejecutar el archivo con el comando:

 # update-WLC-truststore.bat

k) Cuando termine, reiniciar los servicios de RabbitMQ, NwLogCollector y *nwStatCollector*, desde el Panel de Control de Windows > Servicios.

l) Confirmar que todos los servicios de WLC se están ejecutando correctamente desde la interfaz de *Netwitness > Admin > Services*.

95. El proceso de renovación de los certificados de servicio se puede encontrar en el apartado *Security Configuration: Reissue Certificates* de REF6. Los certificados de servicio se pueden renovar de dos maneras: todos a la vez, si el cliente tiene numerosos hosts, o uno por uno.

96. Renovar los certificados de todos los hosts a la vez (excepto el host WLC). Para ello:

a) Se debe asegurar primero que todos los hosts se encuentran online y los servicios de tiempo de ejecución del servidor de NetWitness se están ejecutando.

b) Conectar por SSH al Servidor de Netwitness

c) Ejecutar el siguiente comando:

cert-reissue –host-all

d) Una vez el comando se haya completado, reiniciar el Servidor NetWitness.

97. Renovar los certificados de cada host uno a uno (excepto el host WLC). Para ello:

    a) Se debe asegurar primero que el host que se va a renovar se encuentra online y los servicios de tiempo de ejecución del servidor de NetWitness se están ejecutando. Además, se debe haber renovado el certificado del servidor NetWitness y haber reiniciado el servidor NetWitness antes de proceder con la renovación del resto de hosts.

    b) Conectar por SSH al Servidor de Netwitness

    c) Ejecutar el siguiente comando:

    cert-reissue –host-key <ID, IP, hostname or display name of host>

98. Renovar los certificados del WLC.

    a) Conectar por SSH al Servidor de Netwitness

    b) Ejecutar el siguiente comando:

    wlc-cli-client --cert-renew --host 10.129.43.13 --port 50101 --use-ssl false --username <nwadmin service account> --password <'nwadmin service account password'> --ss-username <deploy_admin> --ss-password <'deploy_admin password'>

    Siendo nwadmin service account el usuario REST UI del WLC.

5.6 SINCRONIZACIÓN HORARIA

99. De forma predeterminada, el Servidor de Netwitness sincroniza su fecha y hora a través del reloj interno del sistema. Para una sincronización más precisa, se recomienda configurar al menos un servidor externo NTP en el Servidor de Netwitness. Todos los demás sistemas de Netwitness se sincronizan con el Servidor principal a través también del protocolo NTP (para ellos en servidor NTP será en propio Servidor de Netwitness).

100. A continuación, se indican los principales pasos para llevar a cabo la configuración de un servidor externo NTP:

    a) Ir a *Admin > Sistema*.

    b) En el panel de opciones, seleccionar *Configuración de NTP*.

    c) Introducir el nombre o la dirección IP del servidor NTP.

    d) Hacer clic en el botón *Añadir*.

    e) Repetir los mismos pasos si se desea añadir servidores NTP adicionales.

    f) Hacer clic en el botón *Aplicar*.

    g) Se mostrará un cuadro de diálogo solicitando si se quiere aplicar la configuración, hacer clic en *Sí*.

5.7 ACTUALIZACIONES

5.7.1 IMPLEMENTACIÓN DE CONTENIDOS

101. La biblioteca del sistema de administración de contenido (*CMS*), conocida como RSA Live, es una fuente de los últimos recursos de seguridad de Internet para los clientes de la plataforma NetWitness. Los diferentes tipos de contenidos que se pueden implementar con *RSA Live* son:

    a) Reglas de Aplicación para los *Decoders/Log Decoders*.

    b) Reglas de Correlación para los *Event Stream Analysis (ESA).*

    c) Reglas de detección de *malware*.

    d) Reglas de Informes.

    e) Listas (*Feeds*).

    f) Módulos de recolección de logs.

    g) Parseadores de logs.

    h) Parseadores LUA.

    i) Definiciones de informes.

102. El detalle sobre la actualización de contenidos utilizando RSA Live, se puede consultar en la *Guía de administración de servicios de Live para la versión 11.x – REF7.*

103. El producto utiliza RSA Live para la actualización de los componentes y contenidos: indicadores, alertas, informes, reputación, etc. Así mismo, están disponibles modos de actualización offline para los casos en los que es necesario.

104. Para llevar a cabo la búsqueda e implementación de contenidos de forma online, deberán seguirse los siguientes pasos:

    a) Ir a *Configure* > *Live Content*.

    b) En el panel de Criterios de Búsqueda, especificar los criterios de búsqueda. Los criterios pueden ser: palabra, categoría, tipo de contenido, medio, claves de metadatos, valores de metadatos, fecha en que el contenido fue creado y fecha en que fue modificado.

    c) Hacer clic en *Buscar*.

    d) El panel de Resultados Encontrados muestra los resultados de la búsqueda. En dicho panel, hacer clic en el contenido que se desee implementar. Hacer clic en el botón *Deploy*.

    e) Hacer clic en Siguiente. Se mostrará una lista de servicios de *Netwitness*.

    f) Seleccionar los servicios en los que se quiera implementar el contenido seleccionado. Hacer clic en Siguiente.

g) Hacer clic en *Deploy*. Se mostrará una barra de progreso que indicará el estado de la instalación de los contenidos.

h) Una vez terminado, hacer clic en Cerrar.

105. El procedimiento de actualización offline se utiliza para entornos seguros aislados en los que el Servidor de Netwitness no tiene acceso a Internet y por tanto no puede conectar con el servidor RSA Live de contenidos. En estos casos se requiere configurar un Servidor de Netwitness secundario (normalmente se configura uno virtual si el entorno no dispone de otros Servidores de Netwitness secundarios físicos ya configurados) para conectar con RSA Live, descargar los contenidos requeridos y crear paquetes (*packages*) que más tarde se pueden implementar en el Servidor de Netwitness que se encuentra en el entorno aislado.

106. A continuación, se indican los principales pasos a seguir para llevar a cabo la implementación de contenidos offline:

a) Conectar a la interfaz del Servidor de Netwitness Secundario que tiene acceso a Internet.

b) Ir a *Configure > Live Content.*

c) En el panel de *Criterios de Búsqueda*, especificar los criterios de búsqueda. Los criterios pueden ser: palabra, categoría, tipo de contenido, medio, claves de metadatos, valores de metadatos, fecha en que el contenido fue creado y fecha en que fue modificado.

d) Hacer clic en *Buscar*.

e) El panel de *Resultados Encontrados* se muestran los resultados de la búsqueda. En dicho panel, hacer clic en *Package > Create*.

f) Este paso creará un archivo .zip que contiene los contenidos seleccionados con la configuración necesaria para implementarlos en el Servidor de Netwitness principal.

g) Para instalar el paquete, conectar a la interfaz del Servidor de *Netwitness* principal que se encuentra aislado de Internet.

h) Ir a *Configure > Live Content*.

i) El panel de Resultados de la derecha, hacer clic en *Package > Deploy.*

j) Hacer clic en el botón *Explorar (Browse)* y seleccionar el paquete .zip que se ha creado en el paso *e)*.

k) Hacer clic en *Siguiente*. Se mostrará una lista de servicios de Netwitness.

l) Seleccionar los servicios en los que se desee implementar el contenido seleccionado. Hacer clic en *Siguiente*.

m) Hacer clic en *Deploy*. Se mostrará una barra de progreso que indicará el estado de la instalación de los contenidos.

n) Una vez terminado, hacer clic en *Cerrar*.

5.7.2 ACTUALIZACIÓN DE LOS COMPONENTES

107. El detalle sobre la actualización de los componentes o sistemas de NetWitness se puede consular en la guía *Upgrade Guide for NetWitness Plaform – REF8.*

108. A continuación, se indican los principales pasos necesarios para la actualización de los componentes de NetWitness:

Fase de preparación:

a) En el capítulo *Overview,* de la *REF8,* revisar si es posible actualizar desde la versión actual a la versión a la que se quiere actualizar.

b) Revisar el documento correspondiente de *Release Notes* que acompaña a cada nueva versión de Netwitness.

c) Revisar los puertos necesarios en el cortafuegos.

d) Revisar y ejecutar cada una de las pre-tareas de actualización para cada tipo de componente (estas se indican en cada documento de actualización y son diferentes para cada versión y cada tipo de componente).

Fase de *backup*:

a) Configurar un sistema externo para ejecutar el *backup* de los sistemas *Netwitness* antes de empezar con cada actualización. El sistema requiere actualmente un sistema operativo CentOS 6 para poder ejecutar el script de *backup*, aunque este requisito puede cambiar en versiones posteriores.

b) Descargar el script *NetWitness Recovery Tool* (NTR) para realizar el *backup* y copiarlo en el sistema externo que se ha preparado en el paso anterior. Para más información sobre el script NTR, consultar el apartado 5.12 BACKUP.

c) Ejecutar el script NTR para crear la lista de sistemas *Netwitness* a actualizar.

d) Ejecutar el script NTR para configurar la autentificación por claves de SSH entre el sistema externo de *backup* y todos los componentes *Netwitness*.

Fase de actualización:

a) Revisar y ejecutar cualquier pre-tarea de *backup* para cada tipo de componente (éstas se indican en cada documento de actualización y son diferentes para cada versión y cada tipo de componente).

b) Ejecutar el *script* de *backup* para realizar una copia de seguridad del Servidor de Netwitness.

Actualización Online:

a) Actualizar el Servidor de *Netwitness*:

b) Desde *Admin > Hosts >* seleccionar la versión a la que quiere actualizar en la columna de *Version > Update > Update Host*.

c) La actualización del servidor puede tardar debido a que tiene que descargar la totalidad de los paquetes, que pueden ocupar varios gigabytes.

d) Una vez termine la actualización aparecerá un mensaje para Reiniciar el sistema. Hacer clic en *Reiniciar*.

e) Para actualizar el resto de sistemas Netwitness, seguir los pasos descritos en las fases de *Backup* y *Actualización* para cada uno de los sistemas.

Actualización Offline:

a) Descargar el archivo de actualización desde el sitio oficial:

b) *https://community.netwitness.com/*El archivo está comprimido y su nombre sigue el siguiente formato: *netwitness-11.6.0.0.zip*

c) Copiar el archivo al Servidor de Netwitness, a la carpeta /root.

d) Conectar por SSH al Servidor de Netwitness y crear la siguiente carpeta:

mkdir /tmp/upgrade/11.6.0.0

e) Descomprimir el archivo con el siguiente comando:

unzip netwitness-11.6.0.0.zip -d /tmp/upgrade/11.6.0.0

f) Inicializar los paquetes con el siguiente comando:

upgrade-cli-client --init --version 11.6.0.0 --stage-dir /tmp/upgrade

g) Actualizar el Servidor con el siguiente comando:

upgrade-cli-client –-upgrade --host-addr <IP_Servidor_Netwitness> --version 11.6.0.0

h) Cuando termine, reiniciar el equipo desde la interfaz gráfica *Admin > Hosts > seleccione el servidor > Reboot.*

i) Para actualizar el resto de sistemas Netwitness, seguir estos pasos para cada sistema.

j) Realizar un *backup* del sistema.

109. Tras finalizar el proceso de actualización, revisar todas las tareas Post-actualización para cada uno de los sistemas (éstas se indican en cada documento de actualización y son diferentes para cada versión y cada tipo de componente).

5.8 AUTO-CHEQUEOS

110. El sistema realiza múltiples auto-chequeos relacionados con políticas de salud y seguridad del sistema. Si alguno falla, mostrará dicha información en la consola de *Health & Wellness* junto con información útil para resolverlo. Para más información consultar la *guía Mantenimiento del sistema: Monitorear el estado y la condición de Security Analytics – REF9.*

111. El módulo *Health & Wellness de NetWitness* proporciona la capacidad de ver y monitorizar el estado de todos los hosts y servicios de Netwitness y la posibilidad de enviar alertas y notificaciones en caso de que se detecte algún problema. Las políticas que definen los valores más importantes a monitorizar en los hosts y servicios (como el uso de procesador, uso de memoria, espacio libre en disco, servicio caído, etc) ya vienen configuradas de forma predeterminada en el producto para hacer saltar las alertas, pero se recomienda configurar notificaciones para que las alertas se envíen a las personas o departamentos correspondientes encargados de mantener el producto.

112. Para agregar una notificación a una política de Health & Wellness seguir los siguientes pasos:

    a) Ir a *Admin > Health & Wellness > Políticas.*

    b) Seleccionar la política que se quiera modificar.

    c) En la sección *Notificación*, hacer clic en el icono *Añadir* ("+") y seleccionar el tipo de notificación. Las opciones disponibles son *Email, SNMP* y *Syslog*.

    d) Configurar las siguientes opciones:

        i. Destinatario.

        ii. Servidor de notificación.

        iii. Plantilla de notificación.

5.9 SNMP

113. Existe la posibilidad de configurar un agente SNMP en los sistemas de Netwitness para recibir peticiones de un servidor SNMP, pero no está habilitado por defecto. No se recomienda habilitarlo en una configuración segura del sistema.

114. Sin embargo, sí que se pueden configurar notificaciones y alertas de estado del sistema a través del protocolo SNMP, tal como se ha descrito en el apartado anterior, configurando las políticas de *Health & Wellness*.

5.10 ALTA DISPONIBILIDAD

115. RSA NetWitness es un sistema distribuido, por tanto, permite añadir tantos componentes duplicados como sea necesario, formará parte de la fase de diseño y

arquitectura inicial del producto el decidir la redundancia óptima para cada despliegue.

5.10.1 ALTA DISPONIBILIDAD DEL SERVIDOR NETWITNESS

116. Se puede desplegar un servidor Netwitness secundario para acceso de emergencia a los logs y paquetes cuando el servidor Netwitness primario se encuentre fuera de servicio. Cabe recalcar que el fallo en el servidor Netwitness no afecta a la disponibilidad de recolección de logs. Para conseguir alta disponibilidad en la recolección de logs, ver apartado 5.10.2 ALTA DISPONIBILIDAD EN LA RECOLECCIÓN DE LOGS.

117. Para configurar un servidor NetWitness secundario, también llamado servidor *Warm Standby NetWitness*, se deberán seguir los siguientes pasos:

    a) Acceder por SSH al dispositivo con las credenciales del usuario *root*. Ejecutar el comando *nwsetup-tui* para iniciar la configuración.

    b) Cuando se pregunte si pertenece a un *NW Server*, hacer clic en *Sí*.

    c) En el tipo de instalación, seleccionar la opción "*3. Install (Warm/Standby)*" y hacer clic en *OK*.

    d) Indicar la dirección IP del servidor NetWitness principal, es decir, con el rol activo.

    e) Utilizar las mismas credenciales del usuario *Deploy Admin* que las existentes en el servidor principal.

118. El detalle sobre la instalación del servidor Netwitness secundario se puede consultar en la *Guía de Despliegue de Netwitness* – REF16, en el apartado *"Warm Standby NW Server Host"*.

5.10.2 ALTA DISPONIBILIDAD EN LA RECOLECCIÓN DE LOGS

119. En la recolección de logs, se puede conseguir redundancia con el uso de varios *Log Collectors*. En caso de que el *Log Collector* principal deje de operar por cualquier razón, el colector configurado recogerá los logs asegurando que todos los logs han sido recogidos.

120. Los pasos necesarios para configurar un *Virtual Log Collector* para alta disponibilidad son los siguientes:

    a) Acceder a la interfaz de usuario de Netwitness con el rol de administrador. Acceder a *Admin > Services* y seleccionar el servicio de *Virtual Log Collector* correspondiente.

    b) Acceder a la vista de *Configuración*. Seleccionar la pestaña *Local Collectors*.

    c) Seleccionar Sources en el menú Select Configuration.

    d) Hacer clic en "+" para añadir una nueva fuente.

e) Definir el Virtual Log Collector de respaldo y pulsar *OK*.

121. Para más información sobre la configuración de los Log Collector, revisar la Guía de configuración de los Colectores de Logs en la plataforma NetWitness – REF15.

5.10.3 CONFIGURACIÓN RAID

122. La configuración RAID (Matriz Redundante de Discos Independientes), evita la pérdida de datos en caso de un fallo de hardware.

123. La configuración RAID en la plataforma NetWitness es:

a) Los hosts son RAID 1 (espejo).

b) Los estantes de disco de capacidad de conexión directa (DAC) son RAID 5 (distribuidos con paridad).

124. La plataforma Netwitness incluye los comandos necesarios para obtener información de la configuración RAID. Tras añadir estantes de disco de capacidad de conexión directa, se pueden seguir los siguientes pasos para la configuración RAID:

a) Ejecutar el comando *raidList* para identificar los controladores y compartimentos que están conectados al host.

b) Seleccionar el esquema de diseño para el compartimento. Para más información sobre estos esquemas, consultar la *Guía de almacenamiento de NetWitnes – REF14*, el apartado *Tareas de configuración de almacenamiento, Tarea 2. Configuración RAID para DAS.*

c) Ejecutar el comando *raidNew* para crear nuevos volúmenes RAID. Por ejemplo:

Send /appliance raidNew controller=1 enclosure=82 scheme=decoder preferSecure=false

d) Ejecutar el comando *raidList* de nuevo para revisar la configuración.

5.11 AUDITORÍA

5.11.1 REGISTRO DE EVENTOS

125. RSA NetWitness incluye funcionalidades de registro de auditoría global. Cuando se configura el registro de auditoría global, los registros de auditoría de todos los componentes de NetWitness se recopilan en un sistema centralizado, que los convierte al formato requerido y los reenvía a un servidor de *syslog* externo o a un *Log Decoder*.

126. Para configurar el registro de auditoría global, seguir los siguientes pasos:

a) Ir a *Admin > Sistema*.

b) En el panel de opciones, seleccionar *Auditoría global*.

c) Hacer clic en el icono de agregar ("+").

d) Especificar las siguientes opciones:

i. Nombre de la configuración.

ii. Notificaciones, seleccionar el Servidor de notificación de Syslog que se usará para esta configuración.

iii. Plantilla de notificación, seleccionar la plantilla de notificación que se usará para esta configuración.

e) Hacer clic en *Guardar*.

127. Para configurar servidores de *syslog* externos, seguir los siguientes pasos:

a) Ir a *Admin > Sistema*.

b) En el panel de opciones, seleccionar *Notificaciones globales*.

c) Hacer clic en la pestaña *Servidores*.

d) En el menú desplegable, seleccionar *Syslog*.

e) Especificar las siguientes opciones:

i. Nombre.

ii. Descripción.

iii. Dirección IP o nombre de host del servidor *Syslog*.

iv. Puerto del servidor.

v. Protocolo.

vi. *Facility*.

128. El producto proporciona plantillas predefinidas del registro de auditoría global que se pueden usar para las configuraciones del registro de auditoría global. Para servidores de *syslog* de otros fabricantes, se puede definir un formato de plantilla (CEF o no CEF) propio mediante el uso de variables de claves de metadatos compatibles. Se puede encontrar una lista de variables soportadas en el *Anexo A - Variables de eventos de Auditoría.*

129. Los tipos de mensajes que registran los diversos componentes de NetWitness Suite se pueden encontrar en el *Anexo B - Tipos de mensajes de Auditoría*.

130. Para ver más opciones de configuración de auditoria global se recomienda consultar la guía *Configuración de Netwitness: Configurar el registro de auditoría global* – REF11.

5.11.2 ALMACENAMIENTO LOCAL

131. El producto realiza un almacenamiento local de los registros de cada componente. Se pueden ver los registros de auditoría de cada servicio a través de las distintas

rutas indicadas en la guía *Configuración de Netwitness: Ubicaciones de los registros de auditoría locales* – REF10.

132. Se puede configurar el almacenamiento local de los registros de cada componente accediendo a la configuración de dicho componente a través de la interfaz de administración (UI web a través de HTTPS). Para ello, acceder a la siguiente ruta: *Admin > Services > Componente > Explore > logs > config*. La configuración se hace a través de los siguientes parámetros, entre otros:

    a) *log.dir*: establece el directorio donde se ubica la base de datos de logs así como el tamaño máximo asignado (en MBs).

    b) *log.levels*: controla el tipo de mensajes de auditoría registrados (Ver ANEXO B para obtener más información de los tipos de mensajes de auditoría)

    c) *syslog.size.max*: controla el tamaño máximo de los logs que son enviados a syslog. Se puede configurar un tamaño indefinido fijando este parámetro a cero.

133. Para obtener más detalle de la configuración de auditoría local, consultar la Guía de introducción de hosts y servicios para RSA NetWitness Platform – REF22.

134. Cuando se alcancen los límites de almacenamiento configurados (parámetro log.dir) se activarán las correspondientes alarmas en el módulo de *Health & Wellness* y se producirá la rotación de logs. Mediante la rotación de logs, se eliminan los registros de auditoría más antiguos. Se recomienda la configuración de un servidor *syslog* externo, para evitar la pérdida de información en caso de alcanzar el límite de almacenamiento.

5.11.3 ALMACENAMIENTO REMOTO

135. El almacenamiento remoto de los registros de auditoría se hace a través de la funcionalidad de registro de auditoria global. Para su configuración debe seguirse la guía *Configuración de Netwitness: Configurar el registro de auditoría global – REF11.* Adicionalmente, se han incluido los pasos necesarios para su configuración en el apartado 5.11.1 REGISTRO DE EVENTOS.

5.12 BACKUP

136. RSA NetWitness incluye los comandos necesarios para realizar el *backup* y restauración de estos de manera segura y centralizada mediante *NetWitness Recovery Tool* (NRT). Es un script que se ejecuta desde la línea de comandos y que permite realizar *backup* y restaurar de manera centralizada y segura. Para mayor detalle consultar la Guía del usuario de la herramienta de recuperación – REF12.

137. Los pasos principales para realizar el backup del dispositivo Netwitness Server son:

    a) Accediendo mediante SSH como *root*, ejecutar el siguiente comando:

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

b) Reemplazar */var/netwitness/backup* con la ruta donde se deba exportar los datos. Verificar que existe suficiente espacio.

c) Introducir la contraseña (del usuario *deploy_admin* utilizado en la instalación) cuando se solicite o incluir el siguiente argumento tras en el comando nw-recovery-tool:

–deploy-password <password>

d) Mover los datos de *backup* a un servidor externo o un USB.

138. Los pasos principales para restaurar una copia de seguridad de *Netwitness Server* son:

a) Restablecer la imagen de *Netwitness Server* utilizando la misma configuración de red del servidor original.

b) Ejecutar el comando *nwsetup-tui*, que iniciará el programa de *Setup*. Solicitará que se introduzca la configuración de red, asegurar que la configuración introducida es igual a la utilizada durante la instalación original.

c) Seleccionar como tipo de instalación: *Recover (Reinstall)* y pulsar *OK*. Seleccionar la ruta donde se encuentran los datos de *backup*.

d) Cuando se complete la instalación, asegurar que el dispositivo está en la misma versión y parche que los datos recuperados. En caso necesario, actualizar el host (ver apartado 5.7 ACTUALIZACIONES).

e) Ejecutar el siguiente comando para restaurar los datos:

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

f) Reiniciar el dispositivo *Netwitness Server*.

139. Los pasos principales para realizar el back up de otros dispositivos distintos de Netwitness Server son:

a) Accediendo como root, ejecutar el siguiente comando:

nw-recovery-tool –export –dump-dir /var/netwitness/backup –category <category name>

b) El *<category name>* identificará el dispositivo del que se quiere hacer el *backup*. Ejemplo: *Broker, Concentrator, LogDecoder, LogCollector*…

c) Reemplazar */var/netwitness/backup* con la ruta donde se debe exportar los datos.

d) Mover los datos de *backup* a un servidor externo o un USB.

140. Los pasos para restaurar los datos de otros dispositivos distintos de Netwitness Server son:

a) Restablecer la imagen del dispositivo utilizando la misma configuración de red del servidor original.

b) Ejecutar el comando *nwsetup-tui*, que iniciará el programa de *Setup*. Solicitará que introduzcamos la configuración de red, asegurar que la configuración introducida es igual a la utilizada durante la instalación original.

c) Seleccionar como tipo de instalación: *Recover (Reinstall*) y pulsar *OK*. Seleccionar la ruta donde se encuentran los datos de backup.

d) Acceder a la Interfaz de Usuario de Netwitness para reinstalar los servicios necesarios en el dispositivo.

e) Cuando se complete la instalación, asegurar que el dispositivo está en la misma versión y parche que los datos recuperados. En caso necesario, actualizar el dispositivo (ver apartado 5.7 ACTUALIZACIONES).

f) Ejecutar el siguiente comando para restaurar los datos:

nw-recovery-tool –import –dump-dir /var/netwitness/backup –category <category name>

g) Reiniciar el dispositivo.

5.13 SERVICIOS DE SEGURIDAD

141. Se describen a continuación los servicios de seguridad presentes en RSA *NetWitness Platform*.

5.13.1 MONITORIZACIÓN DE LOGS

142. RSA NetWitness Logs es una solución de monitorización de seguridad y análisis forense que recoge, analiza, reporta y almacena los datos de logs recibidos de una gran variedad de fuentes de eventos. Las fuentes de eventos son activos de la red, tales como servidores, *switches*, *routers*, matrices de almacenamiento, sistemas operativos o firewalls.

143. Soporta la recolección de un amplio rango de protocolos, incluyendo: Syslog, *ODBC, SFTP, SCP, FTPS, SNMP, Check Point LEA, WinRM*, etc.

144. Normalmente, se configura la fuente de eventos para que envíe los logs al *Log Collector* y el administrador de Netwitness configura el servicio *Log Collector* para recoger los logs. Cada fuente de eventos soportada por *RSA Netwitness* tiene un documento de configuración disponible públicamente en RSA Link. Para más detalle consultar la guía *Catálogo de integraciones Netwitness Platform – REF17.*

145. La configuración del servicio Log Collector se hace desde la interfaz de administración de RSA Netwitness. Los pasos principales necesarios para configurar la recolección de logs son los siguientes:

a) Acceder a los parámetros de configuración del servicio Log Collector, desde *Admin > Services*, seleccionar el servicio *Log Collection*. Hacer clic en *Actions > View > Config*.

b) Seleccionar en la pestaña *Event Sources* el protocolo de recolección de eventos que se quiera utilizar.

c) Completar los datos de la fuente que se va a configurar. Hacer clic en *OK* una vez completados.

d) Habilitar los parsers necesarios. Para ello acceder a *Admin > Services*, pulsar en *Actions > View > Config*.

e) En la ventana de *Configuración de Parsers*, seleccionar *Enabled* en la columna *Config Value* para aquellos parsers que se desee utilizar.

146. Para iniciar la recolección para el protocolo deseado acceder a *Admin > Services,* seleccionar el servicio *Log Collector*. Hacer clic en *Actions > View > System*. Hacer clic en *Collection*, seleccionar el protocolo y hacer clic en *Start*.

147. El detalle sobre la configuración de la recolección de logs se puede consultar en la *Guía de configuración de Colectores de Logs – REF15.*

148. Para configurar la captura de tráfico de red, se debe configurar el adaptador de red necesario. La configuración del adaptador de red se lleva a cabo desde la interfaz de administración de RSA Netwitness:

a) Acceder a los parámetros de configuración del servicio *Decoder*, para ello acceder a *Admin > Services*, seleccionar el servicio *Decoder*. Hacer clic en *Actions > View > Config*.

b) En el campo *Capture Interface Selected*, seleccionar el adaptador de red correspondiente.

c) Habilitar los parseadores necesarios. Para ello acceder a *Admin > Services*, hacer clic en *Actions > View > Config*. En la ventana de *Configuración de Parseadores*, seleccionar *Enabled* en la columna *Config Value* para aquellos parseadores que se desee utilizar.

d) Para que los cambios sean efectivos se debe reiniciar el servicio Decoder. Para ello acceder a *Admin > Services*, seleccionar el servicio Decoder y hacer clic en *Actions > Restart*.

e) Para comenzar a capturar datos de tráfico de red, acceder a *Admin > Services*, seleccionar el servicio *Decoder* y pulsar en Actions > View > System. Hacer clic en *Start Capture*.

149. Para más información sobre la configuración de la recolección de datos de red, consultar la *Guía de configuración de Decoders – REF18.*

5.13.2 ENDPOINT DETECTION & RESPONSE

150. *RSA NetWitness Endpoint* es una herramienta de detección y respuesta en Endpoint que continuamente monitoriza el comportamiento de todos los dispositivos en la red para proporcionar una visibilidad profunda y el análisis de ejecutables y procesos. Ayuda a detectar ataques nuevos, desconocidos y dirigidos, destaca actividades sospechosas para su investigación, detecta comportamientos

anómalos, y determina el alcance de un compromiso para ayudar a los analistas a responder a amenazas avanzadas de forma más rápida.

151. La configuración de la monitorización de Endpoint, se lleva a cabo accediendo a la interfaz de RSA NetWitness. Para ello, se seguirán los siguientes pasos:

a) Revisar las reglas de aplicación y de correlación correspondientes al módulo de Endpoint accediendo a *Admin > Services > Endpoint Log Hybrid-Log Decoder > Config > App Rules*.

b) Configurar el reenvío de metadatos al Log Decoder. Para ello acceder a *Admin > Services > Endpoint Server > Config*. En la pestaña *General*, añadir el servicio de Log Decoder correspondiente. Una vez configurado, iniciar el reenvío de datos seleccionando *Start*.

c) Generar el *Agent Installer*. Para ello, acceder a *Admin > Services > Config > Endpoint Server*. Descargar el *Packager*, un archivo zip que contiene los ejecutables y ficheros de configuración para el agente de Linux, Mac y Windows.

d) Instalar el agente en los Endpoints correspondientes con el *Agent Installer* obtenido en el paso anterior. Para más información, consultar la *Guía de instalación del Endpoint Agent para la versión 11.x – REF20*.

e) Definir los grupos y políticas de *Endpoint*, es decir, las características de los Endpoints a monitorizar (p.e. Sistema operativo, IPs, etc). Así como la información a monitorizar (recolección de logs, uso máximo de CPU, periodicidad de los escáneres, etc). Para ello, acceder a *Admin > Endpoint Sources*. Seleccionar *Groups* y/o *Policies*.

152. Para información más detallada, se recomienda consultar la Guía de configuración de Endpoint para la versión 11.x – REF19.

5.13.3 *UEBA (USER & ENTITY BEHAVIOR ANALYTICS)*

153. *RSA NetWitness UEBA* proporciona capacidades de análisis avanzado para descubrir, investigar y monitorizar comportamientos sospechosos en usuarios y entidades de la red. Para su configuración acceder al servidor UEBA e iniciar sesión con el usuario *root*. Ejecutar el script *ueba-server-config.*

154. El detalle de la configuración de la funcionalidad UEBA se puede consultar en la *Guía de configuración de UEBA para la versión 11.x – REF21.*

6. FASE DE OPERACIÓN

155. Para la operación segura del producto, se recomienda consultar la *Guía de mantenimiento del sistema para la versión 11.x – REF13.*

156. Las mejores prácticas incluyen:

a) Protección de recursos con políticas que suministra RSA. El objetivo de las políticas principales de RSA que se incluyen con *NetWitness Suite* es ayudar a proteger de inmediato los recursos del dominio de *NetWitness Suite* (antes de configurar reglas específicas del ambiente y la política de seguridad). Netwitness tiene políticas creadas por defecto que pueden ser copiadas para su modificación (las reglas estándar no son editables) o se pueden crear políticas nuevas.

b) Se recomienda configurar notificaciones por correo electrónico a los propietarios de recursos correspondientes para estas políticas lo antes posible. Esto permitirá recibir notificaciones cuando se traspasen los umbrales de rendimiento y capacidad, de modo que puedan tomar medidas de inmediato.

c) Se recomienda evaluar las políticas principales e inhabilitar una política o cambiar sus asignaciones de servicios/grupos de acuerdo con requisitos de monitoreo específicos. Para ello se debe acceder a la interfaz de administración (UI web a través de HTTPS), al apartado *Health and Wellness > Policies*. Acceder a la política que se desee inhabilitar o modificar y realizar los cambios necesarios, hacer clic en *Guardar* una vez finalizado.

d) Protección de recursos con políticas en función del ambiente. Las políticas principales de RSA son genéricas y es posible que no proporcionen cobertura de monitoreo suficiente para un ambiente. Se recomienda reunir problemas durante un periodo, que las políticas principales de RSA no identifican, y configurar reglas para ayudarlo a impedir que se produzcan. Para ello se debe acceder a la interfaz de administración, al apartado *Health and Wellness > Policies*. Pulsar en el botón "+" y crear la política en función de las necesidades (reglas, servicios a los que aplica dicha regla, notificaciones, etc).

e) Se recomienda implementar únicamente las reglas y políticas necesarias, así como revisar la validez de las políticas implementadas de manera habitual. Las alarmas y las notificaciones por correo electrónico no válidas pueden afectar adversamente el centro de atención de los propietarios de los recursos.

f) Solución de problemas. Se recomienda consultar Solución de problemas de *Health and Wellness* y Solucionar problemas de *NetWitness Suite* cuando se reciban mensajes de error en la interfaz del usuario y los archivos de registro de los hosts y los servicios.

g) Comprobaciones periódicas del *hardware* y *software* para asegurar que no se ha introducido *hardware* o *software* no autorizado.

h) Escaneo de virus. Se recomienda:

   i. Implementar *software* de cliente antivirus en los servidores implementados de acuerdo con los requisitos de la organización.

   ii. Ejecutar herramientas antivirus y *antimalware* con los archivos de definición más recientes en los servidores implementados.

   iii. Escanear todos los archivos / controladores antes de cargarlos en el servidor implementado.

   iv. Seguir buenas prácticas para la administración de parches y revisar periódicamente los parches disponibles para todos los programas antivirus y *antimalware*.

i) Gestión de parches de seguridad. Todos los parches de seguridad para la plataforma RSA NetWitness se originan en RSA y están disponibles a través de la interfaz de usuario de la plataforma NetWitness. Se recomienda mantener el producto actualizado a la última versión y llevar a cabo los parches de seguridad tan pronto como sea posible. Para obtener más información, consultar el apartado *Administrar actualizaciones de la plataforma NetWitness* de la *Guía de mantenimiento del sistema – REF9*.

j) Monitoreo continuo y auditoría. Se recomienda supervisar constantemente el sistema y realizar auditorías periódicas y aleatorias (por ejemplo, configuración, permisos y registros de seguridad). Debe asegurarse que las configuraciones coincidan con las políticas de seguridad y necesidades de la organización. Para obtener más información, consultar el apartado *Panel de configuraciones de registro de auditoría global* de la *Guía de configuración del sistema – REF11*.

k) Auditar, al menos, los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

l) Reemplazo de hardware. Si el hardware de la plataforma RSA NetWitness falla o es defectuoso, solicitar un reemplazo poniéndose en contacto con el servicio de atención al cliente de RSA. Mientras se espera el reemplazo, la configuración de matriz redundante de discos independientes (RAID) está diseñada para garantizar que no haya pérdida de datos debido a un fallo de hardware gracias a este sistema de almacenamiento que utiliza múltiples unidades de almacenamiento.

m) La configuración RAID en la plataforma NetWitness es:

   i. Los *hosts* son RAID 1.

   ii. Los estantes de disco de capacidad de conexión directa (DAC) son RAID 5.

7. CHECKLIST

157. Este *checklist* contiene todas las recomendaciones de configuración segura especificadas a lo largo de esta guía:

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Registro de los equipos	☐	☐	
Registro de las licencias	☐	☐	
Consideraciones Previas	☐	☐	
Instalación	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Soporte FIPS Colectores de Logs	☐	☐	
Soporte FIPS Decodificadores	☐	☐	
AUTENTICACIÓN			
Usuarios	☐	☐	
Componentes	☐	☐	
Sesiones	☐	☐	
ADMINISTRACIÓN			
Local	☐	☐	
Remota	☐	☐	
Configuración Administradores	☐	☐	
CONFIGURACIÓN			
Interfaces, puertos y servicios	☐	☐	
Protocolos Seguros	☐	☐	
Certificados	☐	☐	
Servidores de Autenticación	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Sincronización Horaria	☐	☐	
Actualizaciones	☐	☐	
Auto-chequeos	☐	☐	
SNMP	☐	☐	
Alta Disponibilidad	☐	☐	
AUDITORÍA			
Registro de Eventos	☐	☐	
Almacenamiento Local	☐	☐	
Almacenamiento Remoto	☐	☐	
OTROS			
Backup	☐	☐	
Servicios de Seguridad	☐	☐	
FASE DE OPERACIÓN			
Mantenimiento	☐	☐	

8. REFERENCIAS

REF1 Guía de Administración de Licencias: https://community.netwitness.com//t5/netwitness-platform-online/licensing-management-guide-for-11-6/ta-p/611049

REF2 Tabla maestra de contenido para encontrar todos los documentos de RSA NetWitness Platform 11.x: https://community.netwitness.com/t5/netwitness-platform-online/netwitness-platform-all-documents/ta-p/676246

REF3 Administración de usuarios y de la seguridad del sistema Guía para la versión 11.x: https://community.netwitness.com//t5/netwitness-platform-online/system-security-and-user-management-for-11-6/ta-p/611063

REF4 Set Up Public Key Infrastructure (PKI) Authentication: https://community.netwitness.com/t5/netwitness-platform-online/configure-pki-authentication/ta-p/669671

REF5 Certificate Re-issue Tool for RSA NetWitness 11.x: https://community.netwitness.com/t5/netwitness-knowledge-base/reissue-root-ca-security-certificates-on-rsa-netwitness-platform/ta-p/677405

REF6 Security Configuration Guide for NetWitness 11.x: https://community.netwitness.com//t5/netwitness-platform-online/security-configuration-guide-for-11-6/ta-p/611370

REF7 Guía de administración de servicios de Live para la versión 11.x: https://community.netwitness.com//t5/netwitness-platform-online/live-services-management-guide-for-11-6/ta-p/611050

REF8 Upgrade Guide for RSA NetWitness Platform https://community.netwitness.com//t5/netwitness-platform-online/upgrade-guide-for-11-6/ta-p/611068

REF9 Guía de mantenimiento del sistema para la versión 11.x: https://community.netwitness.com//t5/netwitness-platform-online/system-maintenance-guide-for-11-6/ta-p/611065

REF10 Configuración de Netwitness: Ubicaciones de los registros de auditoría locales: https://community.netwitness.com/t5/netwitness-platform-online/local-audit-log-locations/ta-p/669737

REF11 Configuración de Netwitness: Configurar el registro de auditoría global: https://community.netwitness.com/t5/netwitness-platform-online/configure-global-audit-logging/ta-p/669719

REF12 Guía del usuario de la herramienta de recuperación: https://community.netwitness.com//t5/netwitness-platform-online/recovery-tool-user-guide-for-11-6/ta-p/611057

REF13 Guía de mantenimiento del sistema para la versión 11.x: https://community.netwitness.com//t5/netwitness-platform-online/system-maintenance-guide-for-11-6/ta-p/611065

REF 14 Guía de almacenamiento de Netwitness para la versión 11.x: https://community.netwitness.com//t5/netwitness-platform-online/storage-guide-for-11-6/ta-p/611062

REF.15 Guía de configuración de Colectores de Logs para la versión 11.x: https://community.netwitness.com//t5/netwitness-platform-online/log-collection-configuration-guide-for-11-6/ta-p/611051

REF.16 Guía de despliegue de Netwitness para la versión 11.x https://community.netwitness.com//t5/netwitness-platform-online/deployment-guide-for-11-6/ta-p/611035

REF.17 Catálogo de integraciones Netwitness Platform https://community.netwitness.com/t5/netwitness-platform-integrations/tkb-p/netwitness-integrations

REF.18 Guía de configuración de decoders en Netwitness para la versión 11.x https://community.netwitness.com//t5/netwitness-platform-online/decoder-configuration-guide-for-11-6/ta-p/611349

REF 19 Guía de configuración de Endpoint para la versión 11.x https://community.netwitness.com//t5/netwitness-platform-online/endpoint-configuration-guide-for-11-6/ta-p/611038

REF 20 Guía de instalación del Endpoint Agent para la versión 11.x https://community.netwitness.com//t5/netwitness-platform-online/endpoint-agent-installation-guide-for-11-6/ta-p/611036

REF.21 Guía de configuración de UEBA para la versión 11.x https://community.netwitness.com//t5/netwitness-platform-online/ueba-configuration-guide-for-11-6/ta-p/611066

REF.22 Guía de introducción de hosts y servicios para RSA NetWitness® Platform https://community.netwitness.com//t5/netwitness-platform-online/hosts-and-services-getting-started-guide-for-11-6/ta-p/611048

REF23 Data Privacy Management Guide for RSA NetWitness https://community.netwitness.com//t5/netwitness-platform-online/data-privacy-management-guide-for-11-6/ta-p/611315

9. ABREVIATURAS

AD	*Active Directory*
AWS	*Amazon Web Services*
CA	*Certification Authority*
CCN	Centro Criptológico Nacional
CLI	*Command Line Interface*
CPD	Centro de Proceso de Datos
CPU	*Central Processing Unit*
ENS	Esquema Nacional de Seguridad
GCP	Google Cloud Platform
GUI	*Graphical User Interface*
HTTPS	*Hyper Text Transfer Protocol Secure*
LDAP	*Lightweight Directory Access Protocol*
PKI	*Public Key Infrastructure*
SAN	*Storage Area Network*
SOC	*Security Operations Center*
SPAN	*Switched Port Analyzer*
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
TLS	*Transport Layer Security*
UI	*User Interface*
WLC	*Windows Legacy Collector*

ANEXO A - VARIABLES DE EVENTOS DE AUDITORÍA

158. En la siguiente tabla se describen las variables de claves de metadatos compatibles con el registro de auditoría global de NetWitness Suite. Utilizar estos valores para crear una plantilla personalizada del registro de auditoría para un servidor de syslog de otros fabricantes.

Variable	Descripción
${category}	Identificador del evento de auditoría. Especifica la categoría del evento de auditoría.
${destinationAddress}	Dirección IP de destino
${destinationPort}	Puerto de destino
${deviceExternalId}	ID único del servicio que genera el evento de auditoría
${deviceFacility}	Funcionalidad de *syslog* que se usa cuando el evento se escribe en el *daemon* de syslog. Por ejemplo, *authpriv*.
${deviceProcessId}	ID del proceso que genera el evento, que es el ID de proceso del servicio de NetWitness Suite
${deviceProcessName}	Nombre del archivo ejecutable que corresponde a *dvcpid*
${deviceProduct}	La familia de productos. Es siempre auditoría de NetWitness Suite.
${deviceService}	Servicio responsable de generar el evento
${deviceVendor}	El proveedor del producto, RSA
${deviceVersion}	Versión del host/servicio
${identity}	Identidad del usuario que inició sesión y que es responsable de generar el evento de auditoría
${key}	Clave de elemento de configuración. Es el parámetro de configuración para el cual se captura el evento de auditoría.
${operation}	Descripción del evento
${outcome}	Resultado de la operación realizada correspondiente al evento de auditoría
${parameters}	Parámetros de la API y de operación que capturan parámetros específicos sobre una consulta
${referrerUrl}	URL principal que hace referencia a la URL actual
${sessionId}	Identificador de la sesión o la conexión
${severity}	Severidad del evento de auditoría

Variable	Descripción
${sourceAddress}	Dirección IP de origen
${sourcePort}	Puerto de origen
${sourceService}	Servicio que es responsable de generar este evento
${text}	Texto libre, información adicional o descripción real del evento
${timestamp}	Hora en que se informa el evento
${transportProtocol}	Protocolo de red utilizado
${userAgent}	Detalle del navegador del usuario que accede a la página
${userGroup}	Asignación de funciones
${userRole}	Asignación de permisos de función del usuario
${value}	Valor de configuración. Es el valor capturado durante la actualización

ANEXO B - TIPOS DE MENSAJES DE AUDITORÍA

159. Los tipos de mensajes que registran los diversos componentes de NetWitness Suite se muestran en las siguientes tablas.

CARLOS (servicio interno de intercomunicación entre servicios)

Nº de serie	Nombre de la operación	Significado
1	*SetProviderConfiguration*	Se agregó o se actualizó un nuevo servidor de notificación (por ejemplo, servidor de SMTP)
2	*SetInstanceConfiguration*	Se agregó o se actualizó un nuevo tipo de notificación (por ejemplo, destino de correo electrónico)
3	*SetTemplateDefinition*	Se agregó o se actualizó una nueva plantilla
4	*RemoveProviderConfiguration*	Se eliminó un servidor de notificación
5	*RemoveInstanceConfiguration*	Se eliminó un tipo de notificación
6	*RemoveTemplateDefinition*	Se eliminó una definición de plantilla
7	*Confirmar*	Se confirmó un cambio en un bean de configuración
8	*Establecer*	Se estableció un valor de propiedad JMX a través de la vista Explorar de NetWitness Suite

ESA

Nº de serie	Nombre de la operación	Significado
9	*SetSourceRequest*	Se agregó o se actualizó un Concentrator a ESA como origen
10	*RemoveSourceRequest*	Se eliminó un Concentrator de ESA como origen
11	*SetEplModule*	Se implementó o se actualizó un módulo de EPL en ESA
12	*RemoveEplModule*	Se eliminó un módulo de EPL de ESA
13	*SetEnrichmentSourceRequest*	Se agregó/actualizó un origen de enriquecimiento de ESA
14	*RemoveEnrichmentSourceRequest*	Se eliminó un origen de enriquecimiento de ESA

Nº de serie	Nombre de la operación	Significado
15	*SetDatabaseReference*	Se hizo una referencia a la base de datos de enriquecimiento a ESA
16	*UpdateEnrichmentData*	Se agregaron filas de datos a un origen de enriquecimiento de ESA
17	*SetEnrichmentConnection*	Se hizo una conexión entre un módulo de EPL y un origen de enriquecimiento
18	*RemoveEnrichmentConnection*	Se eliminó una conexión entre un módulo de EPL y un origen de enriquecimiento
19	*DisableTrialModule*	Se inhabilitaron reglas de prueba de ESA

Investigation

Nº de serie	Nombre de la operación	Significado
1	*VisualizePreferences*	Operaciones relacionadas con una solicitud de visualización de Informer.
2	*ParallelCoordinates*	Operaciones relacionadas con la carga de la navegación en la vista Coordinar.
3	*TimeLine*	Operaciones relacionadas con la carga de la navegación en la vista Cronograma.
4	*ExteralQuery*	Operación cuando se activa una consulta directa a través de la dirección URL.
5	*PrintView*	Operaciones para abrir Investigation en la vista Imprimir.
6	*submitExtractFiles*	Operación para enviar una solicitud de extracción de archivos desde sesiones.
7	*submitExtractLogs*	Operación para enviar una solicitud de extracción de registros desde sesiones.
8	*submitExtractPcap*	Operación para enviar una solicitud de extracción de sesiones desde sesiones.
9	*DataScienceDrill*	Operación para investigar desde el informe de Data Science.
10	*breadCrumbs*	Operación para acceder a las rutas de navegación de consulta.

Nº de serie	Nombre de la operación	Significado
11	*Crear*	Operación cuando se guarda una nueva consulta de Investigation como un predicado que se usará para la integración de URL.
12	*userPredicates*	Operación para acceder a las consultas recientes de un usuario.
13	*chartDefaultMetas*	Operación para acceder a los últimos metadatos usados para generar el gráfico de coordenadas.
14	*defaultDevice*	Operación para acceder al dispositivo de Investigation predeterminado.
15	*deleteDefaultDevice*	Operación para eliminar el dispositivo de Investigation predeterminado.
16	*chartPreferences*	Operación para editar los parámetros del gráfico de navegación de Investigation, como la Altura.
17	*devicePreferences*	Operación para guardar las preferencias del dispositivo de Investigation, como Rango de tiempo, Perfil, Grupos de metadatos, etc.
18	*topValues*	Operación para obtener los valores principales para los metadatos. Normalmente se llama desde el dashlet Valores principales.
19	*MetaLanguages*	Operación para leer los idiomas de metadatos desde un dispositivo.
20	*MetaGroups*	Operaciones relacionadas con grupos de metadatos de Investigation.
21	*DefaultMetaKeys*	Operaciones relacionadas con claves de metadatos predeterminadas de Investigation.
22	*UpdateDefaultMetaKeys*	Operaciones para actualizar claves de metadatos predeterminadas de Investigation.
23	*UpdateMetaGroup*	Operaciones para actualizar grupos de metadatos de Investigation.
24	*ApplyMetaGroup*	Operaciones para usar grupos de metadatos de Investigation.
25	*DeactivateMetaGroup*	Operaciones para restablecer grupos de metadatos de Investigation en la interfaz del usuario.
26	*DeleteMetaGroup*	Operaciones para quitar el grupo de metadatos de Investigation.

Nº de serie	Nombre de la operación	Significado
27	*DeleteMetaGroups*	Operaciones para quitar varios grupos de metadatos de Investigation.
28	*ImportMetaGroups*	Operaciones para importar grupos de metadatos de Investigation.
29	*ExportMetaGroup*	Operaciones para exportar varios grupos de metadatos de Investigation.
30	*GeoMap*	Operación para acceder a la vista Geomap de Investigation.
31	*deleteEndpointCache*	Operación para borrar la caché de reconstrucción de un dispositivo.
32	*eliminación*	Operación para eliminar plantillas de alerta.
33	*CustomColumnGroup*	Operación para aplicar o leer un grupo de columnas personalizado.
34	*Importar*	Operaciones relacionadas con la importación de un grupo de columnas o perfiles.
35	*Exportar*	Operaciones relacionadas con la exportación de un grupo de columnas o perfiles.
36	*SaveProfile*	Operación para guardar un perfil de Investigation.
37	*ApplyProfile*	Operación para aplicar un perfil de Investigation.
38	*DeactivateProfile*	Operación para desactivar un perfil de Investigation.
39	*DeleteProfile*	Operación para eliminar un perfil de Investigation.
40	*DeleteProfiles*	Operación para eliminar varios perfiles de Investigation.

Reporting Engine

Nº de serie	Nombre de la operación	Significado
1	*TEMPLATE*	Para todas las operaciones relacionadas con plantillas
2	*CHART*	Para todas las operaciones relacionadas con gráficos

Nº de serie	Nombre de la operación	Significado
3	*REPORT*	Para todas las operaciones relacionadas con informes
4	*RULE*	Para todas las operaciones relacionadas con reglas
5	*IMAGEN*	Para todas las operaciones relacionadas con imágenes de logotipo que se usan en los informes.
6	*LISTA*	Para todas las operaciones relacionadas con listas
7	*ALERTA*	Para todas las operaciones relacionadas con alertas
8	*CONFIG*	Para todas las operaciones relacionadas con cambios en la configuración
9	*SCHEDULE*	Para todas las operaciones relacionadas con calendarios
10	*FUNCIÓN*	Para todas las operaciones relacionadas con funciones/autorizaciones
11	*BATCH_JOB*	Para todas las operaciones relacionadas con trabajos por lotes
12	*SCHEDULER*	Para todas las operaciones relacionadas con el programador
13	*QUERYPROCESSOR*	Para todas las operaciones relacionadas con procesadores de consultas
14	*FORMATTER*	Para todas las operaciones relacionadas con formateadores
15	*OUTPUTACTION*	Para todas las operaciones relacionadas con acciones de salida
16	*STATUSMANAGER*	Para todas las operaciones relacionadas con administrador de estado
17	*BATCH_RUNDEF*	Para todas las operaciones relacionadas con valores predeterminados de ejecución de lote
18	*CHARTGROUP*	Para todas las operaciones relacionadas con grupos de gráficos
19	*REPORTGROUP*	Para todas las operaciones relacionadas con grupos de informes

Nº de serie	Nombre de la operación	Significado
20	*RULEGROUP*	Para todas las operaciones relacionadas con grupos de reglas
21	*LISTGROUP*	Para todas las operaciones relacionadas con grupos de listas
22	*DISKSPACE*	Para todas las operaciones relacionadas con espacio de disco

Warehouse Connector

Nº de serie	Nombre de la operación	Significado
1	Creación de contraseña de Lockbox	Operación para crear la contraseña de Lockbox.
2	Actualización de contraseña de Lockbox	Operación para actualizar la contraseña de Lockbox.
3	Actualización de contraseña de Lockbox	Operación para actualizar la contraseña de Lockbox.
4	Adición de flujo	Operación para agregar un flujo.
5	Adición de origen	Operación para agregar un origen.
6	Adición de destino	Operación para agregar un destino.
7	Eliminación	Operación para quitar un origen, un flujo o un destino.
8	Cambio de contraseña	Operación para cambiar la contraseña.
9	Actualización de origen	Operación para actualizar un origen.
10	Adición de origen a flujo	Operación para agregar un origen a un flujo.
11	Eliminación de origen de flujo	Operación para eliminar un origen de un flujo.
12	Configuración de destino en flujo	Operación para configurar un destino en un flujo.
13	Finalización de flujo	Operación para finalizar un flujo e iniciar la agregación.
14	Detención de flujo	Operación para detener un flujo.
15	Inicio de flujo	Operación para iniciar un flujo.
16	Recarga de flujo	Operación para volver a cargar un flujo.

Estado y condición (*Health & Wellness*)

Nº de serie	Nombre de la operación	Significado
1	SavePolicyRequest	Operación mientras se agrega o se modifica una política.
2	RemovePolicyRequest	Operación mientras se quita una política.

Servicios principales

Nº de serie	Nombre de la operación	Significado
1	*FILE-Command*	Operación para enumerar, recuperar y eliminar archivos de directorios aprobados en este dispositivo.
2	*SERVICE-Start*	Servicio iniciado
3	*SERVICE-Stop*	Servicio detenido
4	*REDIRECT-Syslog*	Operación para reenvío de syslog.
5	*ADD-Monitor*	Emisión de una operación de monitoreo del sistema de archivos
6	*DELETE-Monitor*	Emisión de una operación de eliminación del sistema de archivos
7	*SHUTDOWN-Service/shutdown.service*	Apagado del servicio del dispositivo
8	*REBOOT-Service*	Reinicio del servicio del dispositivo
9	*CONFIGURE-Network*	Emisión de un cambio en la configuración de la red
10	*SET-NTP*	Emisión de una operación de configuración de NTP
11	*STOP-NTP*	Emisión de una operación de detención de NTP
12	*NTP-Timesync*	Emisión de una operación de sincronización de hora de NTP
13	*SET-SNMP*	Emisión de una configuración de SNMP
14	*UPGRADE/upgrade*	Emisión de una operación de actualización
15	*create.collection*	Operación para crear una recopilación vacía.

Nº de serie	Nombre de la operación	Significado
16	*restauración*	Emisión de una restauración
17	*session.aggregation*	Emisión de un inicio/detención de agregación
18	*add.device*	Adición de un dispositivo para agregación
19	*edit.device*	Edición de un dispositivo que se usa para agregación
20	*delete.device*	Eliminación de un dispositivo que se usa para agregación
21	*capture.start*	Inicio de la operación de captura
22	*capture.stop*	Detención de la operación de captura
23	*select.interface*	Selección de una interfaz de captura
24	*export*	Operación para exportar paquetes o sesiones.
25	*reload*	Emisión de una recarga de analizador
26	*schema*	Emisión de una solicitud de esquema para los analizadores cargados
27	*upload/file.upload*	Emisión de una carga de archivo
28	*notify*	Emisión de una notificación de feed
29	*eliminación*	Emisión de una eliminación de archivo
30	*edit.config*	Operación de cambio en la configuración
31	*parsers.transforms*	Realización de una transformación de clave de idioma
32	*data.reset*	Operación de restablecimiento de datos
33	*timeout*	Tiempo de espera agotado de solicitud REST
34	*cancelar*	Cancelación de una consulta en ejecución
35	*timeroll*	Operación para eliminar los archivos de base de datos que superan un determinado límite.
36	*volcado*	Operación para volcar información fuera de la base de datos en archivos con formato nwd.
37	*session.wipe*	Emisión de una operación de borrado de sesión
38	*REPLACE-Rule*	Emisión de una operación de reemplazo de regla

Nº de serie	Nombre de la operación	Significado
39	*MERGE-Rule*	Emisión de una operación de combinación de regla
40	*ERASE-Rule*	Emisión de la eliminación de un conjunto de todas las reglas
41	*ADD-Rule*	Emisión de una operación de adición de regla
42	*DELETE-Rule*	Emisión de la eliminación de un conjunto de reglas
43	*sdk.info*	Emisión de información de resumen de SDK
44	*sdk.session*	Emisión de información de sesión de SDK
45	*sdk.language*	Emisión del lenguaje de SDK
46	*sdk.aliases*	Emisión de una solicitud de alias de SDK
47	*sdk.transform*	Emisión de una solicitud de transformación de SDK
48	*sdk.search*	Emisión de una solicitud de búsqueda de contenido de sesión
49	*sdk.cache*	Operación relacionada con la caché de contenido de sesión
50	*sdk.content*	Emisión de una solicitud de contenido de sesión
51	*check.authorization*	Operación para comprobar las funciones de usuario relacionadas con permisos de ejecución de una operación.
52	*close.connection*	Emisión de una operación de cierre de conexión
53	*handshake*	Emisión de handshake de SSL
54	*logon/login*	Operación para iniciar sesión desde Netwitness a los demás servicios, principalmente para los usuarios con privilegios.
55	*STOREDPROCOP*	Emisión de una cancelación/inicio de carga de archivo
56	*ADD-Task*	Adición de una tarea calendarizada
57	*DELETE-Task*	Eliminación de una tarea calendarizada
58	*logoff*	Emisión de una operación de cierre de sesión

Nº de serie	Nombre de la operación	Significado
59	*list.cacerts*	Emisión de una operación de enumeración de certificados de CA de confianza
60	*delete.cacerts*	Emisión de una operación de eliminación de certificados de CA de confianza
61	*add.cacerts*	Emisión de una operación de adición de certificados de CA de confianza
62	*restart.command*	Emisión de la opción de reinicio de la línea de comandos
63	*delete.file/file.delete*	Operación para eliminar los archivos de configuración del sistema.
64	*update.file/file.update*	Operación para actualizar el archivo de configuración del sistema.
65	*create.file*	Emisión de una operación de creación de archivo
66	*query*	Emisión de una consulta de base de datos
67	*desbloquear*	Emisión de una operación de desbloqueo de cuenta de usuario
68	*user.add*	Operación para crear cuentas de usuario en dispositivos individuales.
69	*user.delete*	Operación para eliminar un usuario en dispositivos individuales.
70	*group.create*	Operación para agregar un nuevo grupo al sistema.
71	*user.remove*	Eliminar una cuenta de usuario de un grupo
72	*group.delete*	Eliminar un grupo del árbol de usuarios/grupos
73	*add.user*	Emisión de un comando de adición de usuario a recopilación
74	*delete.user*	Emisión de un comando de eliminación de usuario de recopilación
75	*remove.user*	Eliminación de un usuario de una recopilación
76	*collection.open*	Emisión de un comando de apertura para una recopilación
77	*collection.close*	Emisión de un comando de cierre para una recopilación

Nº de serie	Nombre de la operación	Significado
78	*collection.delete*	Emisión de un comando de eliminación de una recopilación
79	*reingest.start*	Operación para iniciar nuevamente la recopilación de datos de paquetes en la recopilación.
80	*feed.notify*	Emisión de un comando de notificación de feed
81	*collect*	Emisión de un comando de recopilación
82	*collect.start*	Emisión de un inicio de recopilación de datos
83	*collection.global*	Emisión de un comando de importación de analizador
84	*parser.reload*	Emisión de un comando de recarga de analizador
85	*reingest*	Operación para volver a recopilar datos de paquetes en la recopilación.
86	*collection.create*	Emisión de un comando de creación de recopilación
87	*collection.restore*	Emisión de un comando de restauración de recopilación
88	*collection.clone*	Emisión de un comando de clonación de recopilación
89	*parser.reload*	Emisión de un comando de recarga de analizador
90	*sdk.query*	Ejecuta una consulta contra la base de datos de metadatos
91	*sdk.msearch*	Busca coincidencias de patrones en muchas sesiones o paquetes
92	*sdk.values*	Ejecuta una consulta de conteo de valores y devuelve los valores coincidentes para un informe
93	*sdk.timeline*	Devuelve el conteo de sesiones/tamaño/paquetes en intervalos de tiempo discretos

Malware Analysis

Nº de serie	Nombre de la operación	Significado
1	*GetDashBoardSummaryRequest*	Obtener estadísticas de análisis de tableros
2	*GetFileScoreSummaryRequest*	Obtener puntajes de archivos agregados por tipo de puntaje y nivel de riesgo
3	*CountEventsAndFilesRequest*	Obtener el conteo de eventos y archivos en un intervalo de tiempo
4	*GetAvVendorDetectionRequest*	Obtener resultados de análisis del proveedor de antivirus
5	*GetAVVendorsRequest*	Obtener la lista de proveedores de antivirus compatibles
6	*SetInstalledAVVendors*	Solicitar la actualización de la lista de proveedores de antivirus instalados en la configuración
7	*CountEventByCriteriaRequest*	Contar eventos por criterios
8	*FindEventByIdRequest*	Obtener evento por ID
9	*FindEventByCriteriaRequest*	Obtener evento por criterios
10	*DeleteEventRequest*	Eliminar evento
11	*CommentOnEventRequest*	Agregar un comentario a un evento
12	*ReSubmitEventRequest*	Reenviar un evento para análisis
13	*FindEventScoreByIdRequest*	Obtener el puntaje del evento por ID de evento
14	*FindEventScoreByCriteriaRequest*	Obtener el puntaje del evento por criterios
15	*FindMetaByIdRequest*	Obtener metadatos por ID
16	*FindMetaByCriteriaRequest*	Obtener metadatos por criterios
17	*FindMetaValueByCriteriaRequest*	Obtener el valor de metadatos por criterios
18	*CountByDistinctMetaValueRequest*	Contar valores de metadatos distintos
19	*CountByMetaNameAndValueWithDateRangeIntervalRequest*	Contar metadatos y valores con intervalo para la creación de gráficos

Nº de serie	Nombre de la operación	Significado
20	*CountByValueAndAverageOverallScore Request*	Contar metadatos y mapear a puntajes generales para eventos
21	*CountByValueAndAverageGroupScore Request*	Contar metadatos y mapear a puntajes de grupo para eventos
22	*CountFileEntryByCriteriaRequest*	Contar archivos por criterios
23	*FindFileEntryByIdRequest*	Obtener archivo por ID
24	*FindFileEntryByCriteriaRequest*	Obtener archivo por criterios
25	*ReSubmitFileEntryRequest*	Reenviar un archivo para análisis
26	*FileDownloadRequest*	Descargar archivo del repositorio
27	*FileUploadRequest*	Cargar un archivo para análisis
28	*FindFileScoreByIdRequest*	Obtener puntaje de archivo por ID
29	*FindFileScoreByCriteriaRequest*	Obtener puntaje de archivo por criterios
30	*FindHashValueByIdRequest*	Obtener valor de hash de lista blanca/lista negra por ID
31	*FindHashValueByCriteriaRequest*	Obtener valor de hash de lista blanca/lista negra por criterios
32	*AddHashValueRequest*	Agregar valor de hash de lista blanca/lista negra
33	*UpdateHashValueRequest*	Actualizar valor de hash de lista blanca/lista negra
34	*DeleteHashValueRequest*	Eliminar valor de hash de lista blanca/lista negra
35	*FindHashValueByMd5Request*	Buscar valor de hash de lista blanca/lista negra por md5
36	*AddHashValueInFileRequest*	Agregar el archivo al repositorio y también el valor de hash
37	*GetDefaultRulesRequest*	Obtener la configuración predeterminada de reglas de IOC

Nº de serie	Nombre de la operación	Significado
38	*ResetToDefaultRulesRequest*	Restablecer la configuración de reglas de IOC al valor predeterminado
39	*GetAllOverrideRulesRequest*	Obtener la configuración de reemplazo creada por el usuario de reglas de IOC
40	*FindOverrideRuleByIdRequest*	Buscar regla de reemplazo de IOC por ID
41	*AddOverrideRuleRequest*	Agregar regla de reemplazo de IOC
42	*UpdateOverrideRuleRequest*	Actualizar regla de reemplazo de IOC
43	*DeleteOverrideRuleRequest*	Eliminar regla de reemplazo de IOC
44	*SubmitOnDemandNextGenRequest*	Enviar nuevo escaneo de NextGen según demanda
45	*FindOnDemandJobEntryByIdRequest*	Obtener entidad de trabajo según demanda por ID
46	*FindOnDemandJobEntryByCriteria Request*	Obtener entidad de trabajo según demanda por criterios
47	*GetOnDemandJobInfoRequest*	Obtener entidad de referencia de trabajo según demanda por ID
48	*GetOnDemandDefaultConfiguration*	Solicitud para obtener configuración predeterminada según demanda
49	*CancelOnDemandJobRequest*	Cancelar trabajo según demanda en curso
50	*DeleteOnDemandJobRequest*	Eliminar un trabajo según demanda
51	*ReSubmitOnDemandJobRequest*	Reenviar un trabajo según demanda
52	*SubscriptionRequest*	Suscribirse a la comunicación con la nube de MA
53	*UnSubscribeRequest*	Cancelar la suscripción a la comunicación con la nube de MA
54	*GetTopEventInfluencesRequest*	Obtener las N influencias de evento principales

Nº de serie	Nombre de la operación	Significado
55	*GetServerInfoRequest*	Obtener información del servidor, como la hora del servidor
56	*DataResetRequest*	Restablecer la base de datos
57	*OnDemandJobStatusNotification*	Informar el progreso del trabajo según demanda a los suscriptores
58	*LicenseStatusNotification*	Informar el estado de la licencia, cantidad de muestras analizadas
59	*DataResetNotification*	Informar que se restablecieron los datos
60	*GetIocSummaryRequest*	Obtener reglas de IOC agregadas por puntajes de evento/archivo
61	*FindAlertTemplatesByCriteriaRequest*	Obtener plantillas de alerta de rabbitmq por criterios
62	*SaveAlertTemplateRequest*	Actualizar una plantilla de alerta
63	*DeleteAlertTemplateRequest*	Eliminar una plantilla de alerta
64	*GetJobStatusRequest*	Obtener el estado del hilo de ejecución de análisis del trabajo en curso
65	*GetEventTypeCountSummaryRequest*	Obtener conteos de análisis de evento por gráfico de fecha
66	*Inicio de sesión*	Iniciar sesión en el servicio de MA
67	*Modificada*	Modificación de cambios en la configuración
68	*GetNextGenSummaryRequest*	Obtener estadísticas de resumen del tablero de NextGen

Interfaz del usuario

Nº de serie	Nombre de la operación	Significado
1	*uploadTrialLicense*	Cargar licencia de prueba

Nº de serie	Nombre de la operación	Significado
2	*LicenseEntitle*	Autorizar licencia
3	*LicenseDeactivation*	Inhabilitar licencia
4	*ExpiredLicense*	Venció la licencia
5	*LicenseOutOfComplianceAcknowledgement*	Confirmación de EULA
6	*resetLicense*	Restablecer licencia
7	*usageDateExport*	Uso de datos de licencia: csv/pdf
8	*refreshLicense*	Actualizar licencia de LLS
9	*LicenseOutOfCompliance*	Incumplimiento de normas
10	*OOTBEntitlementOutOfCompliance*	Incumplimiento de normas de licencia de prueba OOTB
11	*OOTBEntitlementFirstLoginTimeModified*	Se modificó la hora de OOTB
12	*OOTBEntitlementFileDeleted*	Se eliminó el archivo de OOTB
13	*OOTBEntitlementDataTampering*	Manipulación de datos de OOTB
14	*uploadOfflineResponse*	Cargar respuesta offline
15	*offlineDownloadCapRequest*	Descargar solicitud offline
16	*movePerpetualToMetered*	Cambiar licencia basada en servicios a medida
17	*moveMeteredToPerpetual*	Cambiar licencia medida a basada en servicios
18	*mapServiceLicense*	Mapear servicio a licencia real
19	*eliminación*	Operación para eliminar plantillas de alerta.
20	*HttpRequest*	Operación para el registro de auditoría de la dirección URL a la cual se accedió.
21	*Página a la cual se accedió*	Operación para el registro de auditoría de la página a la cual se accedió.
22	*Navegar*	Operación para navegar a la página a la cual se accedió.
23	*Eventos*	Operación para ver la página de evento a la cual se accedió.

Nº de serie	Nombre de la operación	Significado
24	*Recon*	Operación para la reconstrucción de evento solicitada.
25	*Servicios*	Operación al leer la lista de dispositivos disponibles para la investigación.
26	*Servicio*	Operación para una lista de dispositivos cuya investigación se solicitó.
27	*Recopilaciones*	Operación para ver la lista de recopilaciones que se solicitó.
28	*Perfiles.*	Operación para aplicar un perfil.
29	*ColumnGroups*	Operación para aplicar o leer un grupo de columnas.
30	*ParallelCoordinates*	Operaciones relacionadas con la carga de la navegación en la vista Coordinar.
31	*Cronograma*	Operaciones relacionadas con la carga de la navegación en la vista Cronograma.
32	*PrintView*	Operaciones para abrir Investigation en la vista Imprimir.
33	*Preferencias*	Operaciones relacionadas con una solicitud de Informer.
34	*import*	Operaciones relacionadas con la importación de un grupo de columnas o perfiles.
35	*export*	Operaciones relacionadas con la exportación de un grupo de columnas o perfiles.
36	*Predicado*	Operaciones relacionadas con consultas (predicados) que se usan para Investigation.
37	*Idiomas*	Operación para el idioma que se solicitó desde un dispositivo.
38	*CancelLanguageLoad*	Operación para la carga de idioma que se canceló desde la página Navegar.
39	*resumen*	Operación para un resumen que se solicitó desde un dispositivo.
40	*languages*	Operación para un idioma que se solicitó desde un dispositivo.
41	*aliases*	Operación para alias de metadatos que se solicitaron desde un dispositivo.

Nº de serie	Nombre de la operación	Significado
42	*query*	Operación para consulta de SDK que se solicitó desde un dispositivo.
43	*msearch*	Operación para una búsqueda de metadatos que se solicitó desde un dispositivo.
44	*nodeListing*	Enumeración de nodos correspondiente a un nodo que se solicitó desde un dispositivo.
45	*contenido*	Llamada SDK Content que se solicitó desde un dispositivo para la descarga de una PCAP o un registro.
46	*Export Files*	Enumeración de archivos que se solicitó para una sesión en la vista Archivo o en trabajos de extracción.
47	*packets*	Paquetes que se solicitaron para sesiones en la vista Paquete o en trabajos de extracción.
48	*deleteEndpointCache*	Operación para borrar la caché de reconstrucción de un dispositivo.
49	*Inicio de sesión*	Operación para que el usuario inicie sesión en la interfaz del usuario de NetWitness Suite.
50	*Logoff*	Operación para que el usuario cierre sesión en la interfaz del usuario de NetWitness Suite.
51	*defaultDevice*	Operación para acceder al dispositivo Interfaz del usuario de SA predeterminado.
52	*deleteDefaultDevice*	Operación para eliminar el dispositivo de Investigation predeterminado.
53	*submitExtractFiles*	Operación para enviar una solicitud de extracción de archivos desde sesiones.
54	*submitExtractLogs*	Operación para enviar una solicitud de extracción de registros desde sesiones.
55	*submitExtractPcap*	Operación para enviar una solicitud de extracción de sesiones desde sesiones.
56	*MetaGroup*	Operaciones relacionadas con grupos de metadatos de la interfaz del usuario de SA.
57	*ExternalQuery*	Operación cuando se activa una consulta directa a través de la dirección URL.

Nº de serie	Nombre de la operación	Significado
58	*GeoMap*	Operación para acceder a la vista Geomap de Investigation.
59	*SaveProfile*	Operación para guardar un perfil de Investigation.
60	*ApplyProfile*	Operación para aplicar un perfil de Investigation.
61	*DeleteProfile*	Operación para aplicar un perfil de Investigation.
62	*DeactivateProfile*	Operación para aplicar un perfil de Investigation.
63	*VisualizePreferences*	Operaciones relacionadas con una solicitud de visualización de Informer.
64	*ExportMetaGroup*	Operaciones para exportar varios grupos de metadatos de la interfaz del usuario de SA.
65	*userPredicates*	Operaciones para exportar varios grupos de metadatos de la interfaz del usuario de SA.
66	*FileView*	Operación para la solicitud de reconstrucción para la vista Archivo.
67	*resource.update*	Operación cuando cambia el estado de suscripción de Live.

Respond

Nº de serie	Nombre de la operación	Significado
1	*update*	Actualizar la configuración de la notificación
2	*update*	Actualizar la configuración de los ajustes de integración
3	*eliminate*	Eliminar alertas
4	*create*	Crear incidente nuevo
5	*update*	Actualizar los detalles de incidentes
6	*read*	Leer los detalles de incidentes
7	*eliminate*	Eliminar incidentes
8	*read*	Leer las tareas de corrección
9	*eliminate*	Eliminar las tareas de corrección
10	*update*	Actualizar las tareas de corrección

Nº de serie	Nombre de la operación	Significado
11	*create*	Crear nueva regla
12	*update*	Actualizar regla de alerta existente
13	*reorder*	Cambiar el orden de prioridad de las reglas de alertas

Investigate Server

Nº de serie	*Nombre de la operación*	Significado
1	*Aliases*	Fetch aliases
2	*BackgroundJob*	Category for all background job
3	*ColumnGroup*	Category for all column group operation
4	*Count-query*	Default Investigate
5	*Countdistict-query*	Default Investigate
6	*Content*	Default Session Content
7	*Create*	User entity
8	*Create*	User preferences
9	*Create*	Predicate
10	*Delete*	User preferences
11	*Delete*	Predicate
12	*Extract-content*	Extract Content from Session
13	*Folders*	Category for all folder operation
14	*Files*	SDK content request
15	*InvestigateExport*	Category for extraction invocation
16	*Key-refs*	Fetch meta keys
17	*Languages*	SDK language call
18	*MetaGroup*	Category for all meta group operation
19	*Metakey*	Category for all metakey operation
20	*MailReconstruction*	Category for all mail reconstruction operation
21	*ParsingRequest*	Category for all request parsing operation

Nº de serie	*Nombre de la operación*	Significado
22	*PacketReconstruction*	Category for all packet reconstruction operation
23	*Predicate InvestigateIncidents*	Category for all predicate operation
24	*Query*	SDK query
25	*Reconstruction*	Category for common shared reconstruction operation
26	*ReconstructionCache*	Category for reconstruction caching operation
27	*ReconstructionStreaming*	Category for reconstruction streaming operation
28	*ReconstructDataSecurity*	Category for reconstruction security operations (data-scrubbing)
29	*Session-Meta*	SDK query to get session meta
30	*Summary*	SDK summary
33	*Timeline*	Timeline request
34	*UserPreferences*	Category for all user preferences operation
35	*Update*	User entity
36	*Update*	User preferences
37	*Update*	Profile group
38	*Update*	Predicate
39	*Values*	SDK values

Security Server

Log Category	Significado
Create	Add record for a role with new ID.
Create	Add user record with new ID.
Update	Update the user account with a new ID.
Authentication	Logs events pertaining to user logins and logouts.
Authorization	Logs events pertaining to user access checks and RBAC management.
UserAccount	Logs events pertaining to NetWitness domain account management.

Log Category	Significado
ExternalProvider	Tracks events pertaining with external account providers (for example, Active Directory).

Admin Server

Log Category	Significado
Restore	System operation to restore a data springboard.

Config Server

Log Category	Significado
newregistration	Record the registration to config server that manages the collection storage.

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL