



Guía de implementación

para la versión 11.1



Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Información de contacto

RSA Link en <https://community.rsa.com> contiene una base de conocimientos que responde a las preguntas comunes y brinda soluciones para problemas conocidos, documentación de productos, análisis de la comunidad y administración de casos.

Marcas comerciales

Para obtener una lista de las marcas comerciales de RSA, visite mexico.emc.com/legal/emc-corporation-trademarks.htm#rsa (visite el sitio web de su país correspondiente).

Acuerdo de licencia

Este software y la documentación asociada son propiedad e información confidencial de Dell, se suministran bajo licencia, y pueden utilizarse y copiarse solamente de acuerdo con los términos de dicha licencia y con el aviso de copyright mencionado a continuación. No se puede suministrar a ninguna persona, ni poner a su disposición de cualquier otra manera, este software ni la documentación, o cualquier copia de estos elementos.

Este documento no constituye ninguna transferencia de titularidad ni propiedad del software, la documentación o cualquier derecho de propiedad intelectual. Cualquier uso o reproducción sin autorización de este software y de la documentación pueden estar sujetos a responsabilidad civil o penal.

Este software está sujeto a cambios sin aviso y no debe considerarse un compromiso asumido por Dell.

Licencias de otros fabricantes

Este producto puede incluir software que ha sido desarrollado por otros fabricantes. El texto de los acuerdos de licencia que se aplican al software de otros fabricantes en este producto puede encontrarse en la página de documentación del producto en RSA Link. Al usar este producto, el usuario acepta regirse totalmente por los términos de los acuerdos de licencia.

Nota sobre tecnologías de cifrado

Es posible que este producto contenga tecnologías de cifrado. Muchos países prohíben o limitan el uso, la importación o la exportación de las tecnologías de cifrado, y las regulaciones actuales de uso, importación y exportación deben cumplirse cuando se use, importe o exporte este producto.

Distribución

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

julio 2018

Contenido

| | |
|--|-----------|
| Conceptos básicos | 5 |
| Proceso básico de implementación | 7 |
| Proceso | 7 |
| Diagrama de implementación general de NetWitness Suite | 9 |
| Diagrama detallado de implementación de hosts de RSA NetWitness Suite | 10 |
| Arquitectura y puertos de red | 12 |
| Diagrama de la arquitectura de red de NetWitness Suite | 12 |
| Lista completa de puertos de hosts y servicios de NetWitness Suite | 13 |
| Host del servidor de NW | 14 |
| Host de Archiver | 16 |
| Host de Broker | 17 |
| Host de Concentrator | 18 |
| Endpoint Hybrid o Endpoint Log Hybrid | 19 |
| Host de Event Stream Analysis (ESA) | 20 |
| Host de Log Collector | 22 |
| Host de Log Decoder | 24 |
| Host de Log Hybrid | 26 |
| Host de Malware | 30 |
| Host de Packet Decoder | 32 |
| Host de Packet Hybrid | 33 |
| Arquitectura de NetWitness Endpoint Insights | 34 |
| NetWitness Endpoint Insights 11.1 | 34 |
| NetWitness Endpoint Insights 11.1 con Log Decoder | 34 |
| Integración de NetWitness Endpoint 4.4 con NetWitness Endpoint Insights 11.1 | 35 |
| Requisitos y seguridad del sitio | 36 |
| Usos previstos de la aplicación | 36 |
| Servicio | 36 |
| Información sobre seguridad | 36 |
| Selección del sitio | 36 |
| Prácticas de manejo de equipos | 37 |
| Advertencias eléctricas y de alimentación | 37 |

| | |
|--|-----------|
| Advertencias sobre el montaje en rack | 37 |
| Enfriamiento y flujo de aire | 37 |
| Colocación de la antena | 38 |
| Configurar la agregación de grupos | 39 |
| Recomendaciones para la implementación de la agregación de grupos de RSA | 39 |
| Ventajas de usar la agregación de grupos | 39 |
| Configurar la agregación de grupos | 41 |
| Requisitos previos | 41 |
| Configurar la agregación de grupos | 43 |

Conceptos básicos

En esta guía se describen los requisitos básicos de una implementación de NetWitness Suite y se presentan escenarios opcionales para abordar las necesidades de su empresa. Incluso en redes pequeñas, la planificación puede garantizar que todo funcione correctamente cuando esté listo para poner los hosts en línea.

Nota: En este documento se hace referencia a varios documentos adicionales disponibles en RSA Link. Vaya a la [Tabla maestra de contenido](#) para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.

Existen muchos factores que debe tener en cuenta antes de implementar NetWitness Suite. Los siguientes elementos son solo algunos de estos factores. Cuando considere estos factores, debe calcular los requisitos de crecimiento y almacenamiento.

- El tamaño de su empresa (es decir, la cantidad de ubicaciones y personas que utilizarán NetWitness Suite).
- El volumen de paquetes y registros que debe procesar.
- El rendimiento que necesita cada función de usuario de NetWitness Suite para desempeñar su trabajo de manera eficaz.
- La prevención del tiempo fuera (es decir, cómo evitar un punto único de falla).
- El ambiente en el cual planea ejecutar NetWitness Suite
 - Dispositivos RSA (software que se ejecuta en hardware proporcionado por RSA)
Consulte la *Guía de instalación de hosts físicos* de *RSA NetWitness® Suite* para obtener instrucciones detalladas sobre cómo implementar dispositivos RSA.
 - Software solo proporcionado por RSA:
 - Hosts virtuales en las instalaciones
Consulte la *Guía de instalación de hosts virtuales* de *RSA NetWitness® Suite* para obtener instrucciones detalladas sobre cómo implementar hosts virtuales en las instalaciones.
 - VCloud:
 - Amazon Web Services (AWS)
Consulte la *Guía de implementación de AWS* de *RSA NetWitness® Suite* para obtener instrucciones detalladas sobre cómo implementar hosts virtuales en AWS.

- Azure

Consulte la *Guía de implementación de Azure* de *RSA NetWitness® Suite* para obtener instrucciones detalladas sobre cómo implementar hosts virtuales en Azure.

Proceso básico de implementación

Antes de que pueda implementar NetWitness Suite, necesita:

- Considerar los requisitos de su empresa y comprender el proceso de implementación.
- Tener un panorama general de la complejidad y el alcance de una implementación de NetWitness Suite.

Proceso

Los componentes y la topología de una red de NetWitness Suite pueden variar en gran medida entre las instalaciones y se deben planear cuidadosamente antes del inicio del proceso. La planificación inicial incluye:

- Consideración de los requisitos del site y los requisitos de seguridad.
- Revisión de la arquitectura de red y el uso de puertos.
- Compatibilidad con la agregación de grupos en Archivers y Concentrators, y hosts virtuales.

Cuando esté listo para dar inicio a la implementación, la secuencia general es:

- Para los dispositivos RSA:
 1. Instalación de dispositivos y conexión a la red como se describe en las Guías de configuración de hardware de RSA NetWitness® Suite y la *Guía de instalación de hosts físicos de RSA NetWitness® Suite*.
 2. Configuración de la licencia de NetWitness Suite, como se describe en la *Guía de licencia de RSA NetWitness® Suite*.
 3. Configuración de los dispositivos y los servicios individuales, como se describe en la *Guía de introducción de hosts y servicios de RSA NetWitness® Suite*. Esta guía también describe los procedimientos para aplicar actualizaciones y prepararse para las actualizaciones de versión.
- Para los hosts virtuales en las instalaciones, siga las instrucciones de la *Guía de instalación de hosts virtuales de RSA NetWitness® Suite*.
- Para AWS, siga las instrucciones de la *Guía de implementación de AWS de RSA NetWitness® Suite*.
- Para Azure, siga las instrucciones de la *Guía de implementación de Azure de RSA NetWitness® Suite*.

Cuando actualice los hosts y los servicios, siga las reglas recomendadas en el tema “Ejecución en modo mixto” de la *Guía de introducción de hosts y servicios de RSA NetWitness Suite*.

También debería familiarizarse con hosts, tipos de hosts y servicios como se usan en el contexto de NetWitness Suite, lo que también se describe en la *Guía de introducción de hosts y servicios de RSA NetWitness Suite*.

Diagrama de implementación general de NetWitness Suite

El siguiente diagrama ilustra una implementación básica de NetWitness Suite de múltiples sites.

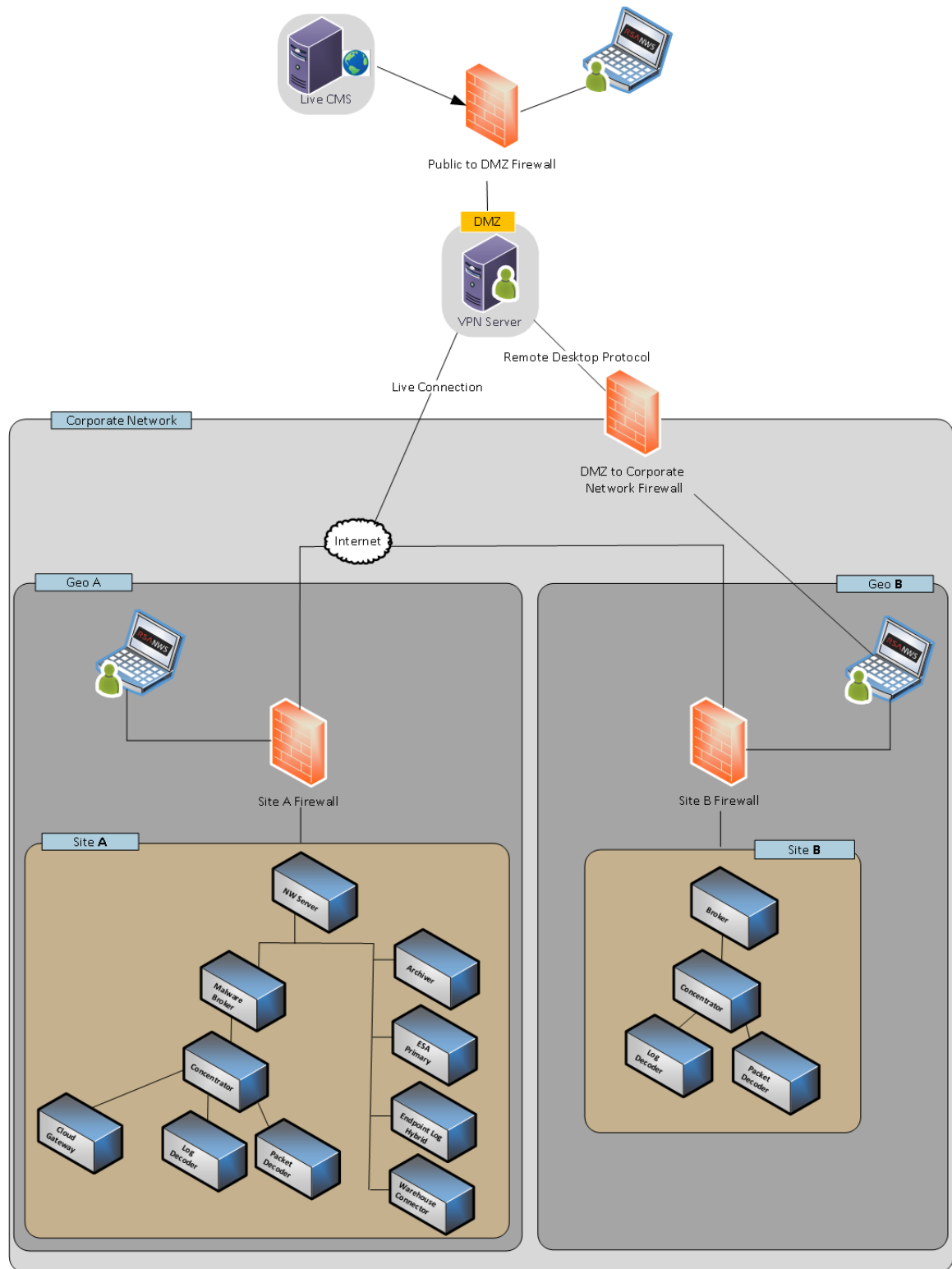
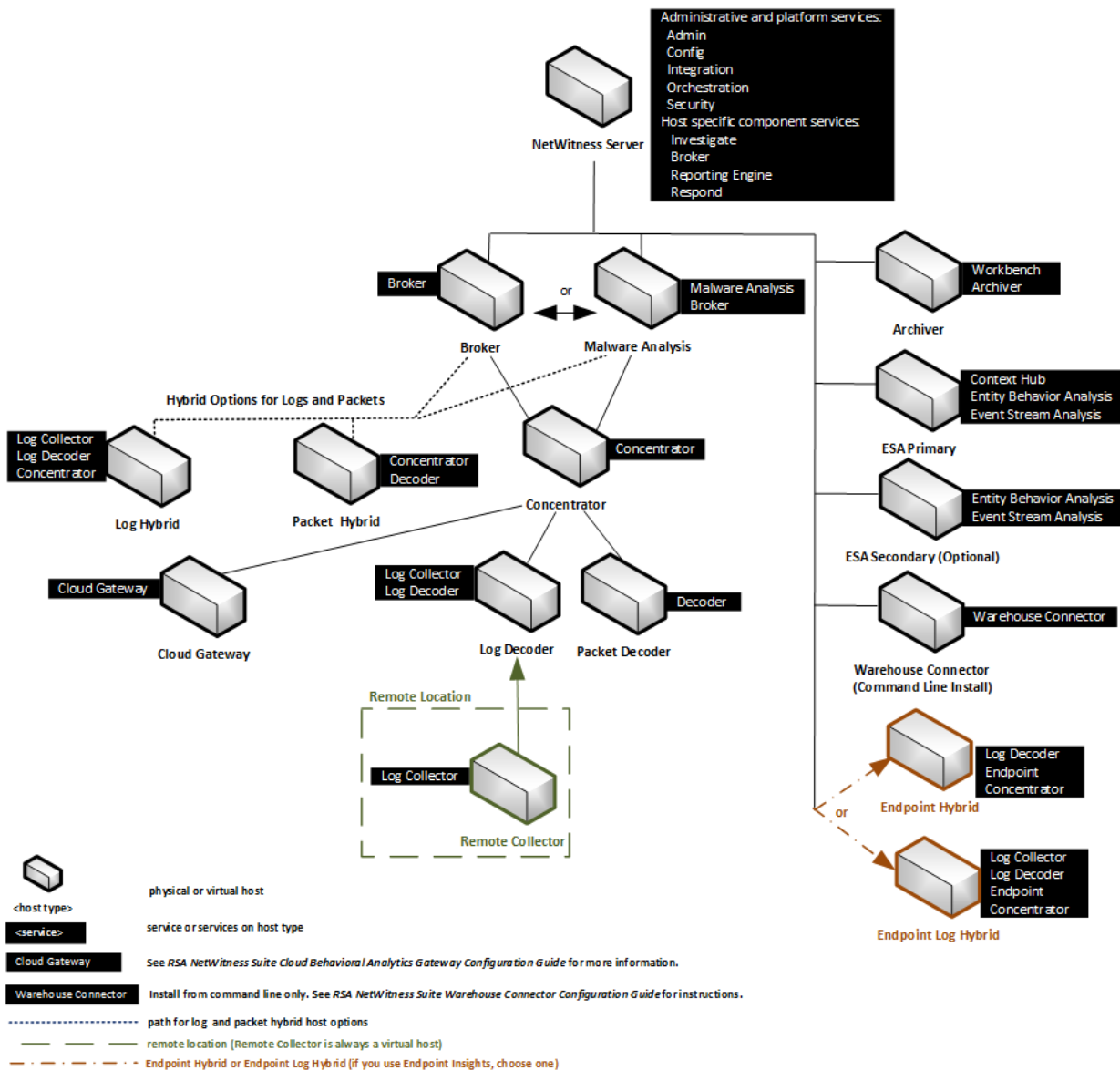


Diagrama detallado de implementación de hosts de RSA NetWitness Suite

El siguiente diagrama es un ejemplo de una implementación de NetWitness Suite alojada en máquinas físicas o virtuales. Para obtener instrucciones sobre cómo instalar NetWitness Suite, consulte la *Guía de instalación de hosts físicos*, la *Guía de instalación de hosts virtuales*, la *Guía de implementación de AWS* o la *Guía de implementación de Azure*. Vaya a la [Tabla maestra de contenido](#) para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.

RSA NetWitness® Suite Host Deployment



Arquitectura y puertos de red

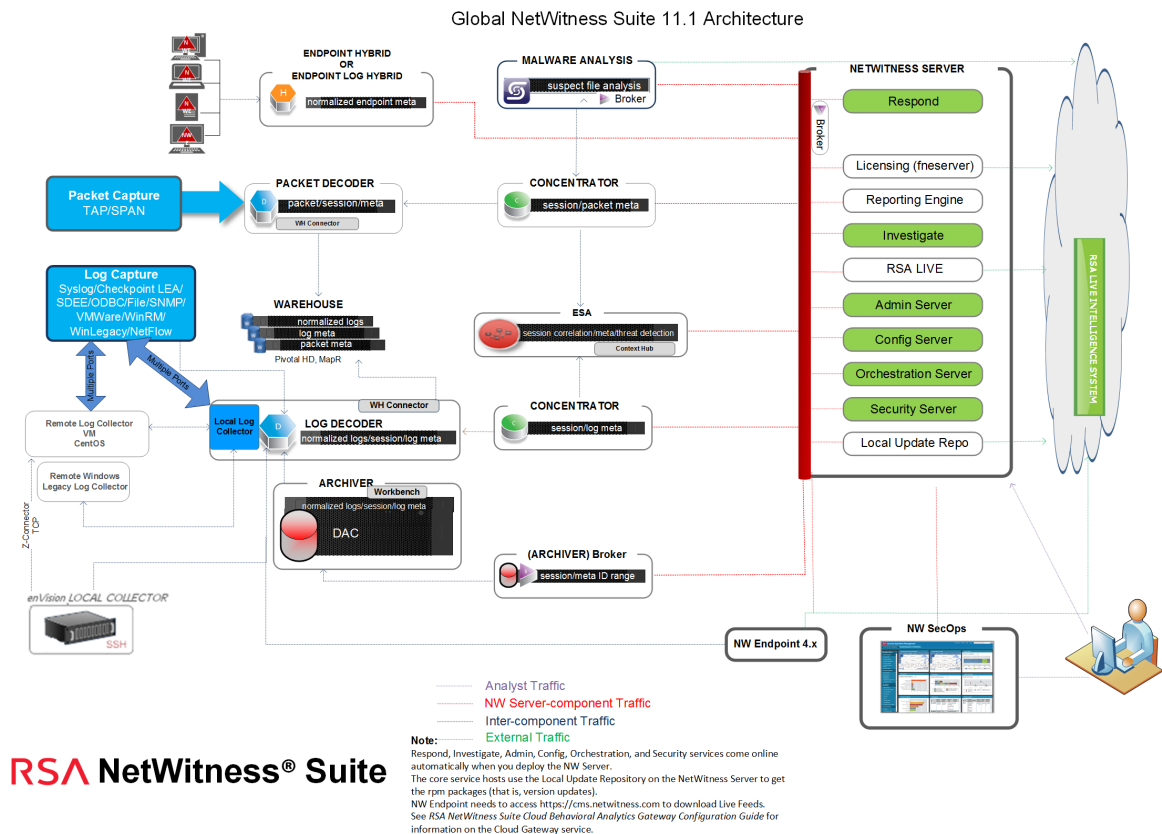
Consulte el diagrama y la tabla de puertos siguientes para asegurarse de que todos los puertos pertinentes estén abiertos para los componentes de la implementación de NetWitness Suite de modo que exista comunicación entre ellos.

Consulte [Arquitectura de NetWitness Endpoint Insights](#) al final de este tema para ver los diagramas de arquitectura de Endpoint individuales.

Diagrama de la arquitectura de red de NetWitness Suite

En el siguiente diagrama se ilustra la arquitectura de red de NetWitness Suite, incluidos todos los productos que la componen.

Nota: Los hosts de NetWitness Suite Core deben ser capaces de comunicarse con el Servidor de NetWitness (servidor primario en una implementación de múltiples servidores) a través del puerto UDP 123 para la sincronización horaria de NTP.



Lista completa de puertos de hosts y servicios de NetWitness Suite

Nota: 1.) Para los puertos que se usan en la recopilación de eventos a través del Registro de NetWitness, consulte “Aspectos básicos” en la *Guía de implementación de la recopilación de registros de RSA NetWitness Suite*. Vaya a la [Tabla maestra de contenido](#) para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.

Esta sección contiene las especificaciones de puerto para los siguientes hosts.

| | |
|---|--|
| Host del servidor de NW | Host de Log Collector |
| Host de Archiver | Host de Log Decoder |
| Host de Broker | Host de Log Hybrid |
| Host de Concentrator | Host de Malware |
| Host de Endpoint Hybrid/Endpoint Log Hybrid | Host de Packet Decoder |
| Host de Event Stream Analysis | Host de Packet Hybrid |

Host del servidor de NW

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|--------------------------------------|-----------------|-------------------------|--|
| Estación de trabajo de administrador | Servidor de NW | TCP 443, 80 | nginx: Interfaz del usuario de NetWitness |
| Estación de trabajo de administrador | Servidor de NW | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Hosts de NW | Servidor de NW | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Estación de trabajo de administrador | Servidor de NW | TCP 22 | Protocolo SSH |
| Hosts de NW | Servidor de NW | TCP 4505, 4506 | Puertos maestros de valor de sal |
| Servidor de NW | Servidor de NW | TCP 50003, 50103, 56003 | Puertos de Broker |
| Servidor de NW | Servidor de NW | TCP 5671 | RabbitMQ-amqp |
| Servidor de NW | Servidor de NW | UDP 50514 | Puertos de auditoría |

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|----------------|-----------------|-----------------------------|---------------------------------------|
| Servidor de NW | Servidor de NW | TCP 7000, 7003, 7009, 7010 | Iniciar puertos |
| Servidor de NW | Servidor de NW | TCP 50006, 50106, 56006 | Puertos de NetWitness Appliance |
| Hosts de NW | Servidor de NW | UDP 123 | NTP |
| Hosts de NW | Servidor de NW | TCP 27017 | MongoDB |
| Servidor de NW | Servidor de NW | UDP 123 | NTP |
| Servidor de NW | Servidor NFS | TCP 111 2049 UDP 111 204 | Instalaciones de iDRAC |
| Servidor de NW | NW Endpoint | TCP 443, 9443 | Para integraciones de NW Endpoint 4.x |

Host de Archiver

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|--------------------------------------|-----------------|---|---|
| Estación de trabajo de administrador | Archiver | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Archiver | Servidor de NW | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Estación de trabajo de administrador | Archiver | TCP 22 | Protocolo SSH |
| Servidor de NW | Archiver | TCP 56008 (SSL), 50008 (no SSL), 50108 (REST) | Puertos de aplicaciones de Archiver |
| Servidor de NW | Archiver | TCP 56006 (SSL), 50006 (no SSL), 50106 (REST) | Puertos de NetWitness Appliance |
| Servidor de NW | Archiver | TCP 5671 | Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW. |
| Servidor de NW | Archiver | TCP 514, 6514, 56007 (SSL), 50007 (no SSL), 50107 (REST), UDP 514 | Puertos de aplicaciones de Workbench |
| Archiver | Archiver | UDP 50514 | Datos de auditoría |
| Archiver | Archiver | UDP 123 | NTP |
| Archiver | Servidor NFS | TCP 111 2049 UDP 111 204 | Instalaciones de iDRAC |

Host de Broker

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|--------------------------------------|-----------------|---|---|
| Estación de trabajo de administrador | Broker | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Broker | Servidor de NW | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Estación de trabajo de administrador | Broker | TCP 22 | Protocolo SSH |
| Servidor de NW | Broker | TCP 56003 (SSL), 50003 (no SSL), 50103 (REST) | Puertos de aplicaciones de Broker |
| Servidor de NW | Broker | TCP 56006 (SSL), 50006 (no SSL), 50106 (REST) | Puertos de NetWitness Appliance |
| Servidor de NW | Broker | TCP 5671 | Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW. |
| Broker | Broker | UDP 50514 | Datos de auditoría |
| Broker | Broker | UDP 123 | NTP |
| Broker | Servidor de NW | TCP 111 2049 UDP 111 2049 | Instalaciones de iDRAC |

Host de Concentrator

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|--------------------------------------|-----------------|---|---|
| Estación de trabajo de administrador | Concentrator | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Concentrator | Servidor de NW | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Estación de trabajo de administrador | Concentrator | TCP 22 | Protocolo SSH |
| Servidor de NW | Concentrator | TCP 56005 (SSL), 50005 (no SSL), 50105 (REST) | Puertos de aplicaciones de Concentrator |
| Malware | Concentrator | TCP 56005 (SSL) | Malware |
| Servidor de NW | Concentrator | TCP 56006 (SSL), 50006 (no SSL), 50106 (REST) | Puertos de NetWitness Appliance |
| Servidor de NW | Concentrator | TCP 5671 | Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW. |
| Concentrator | Servidor NFS | TCP 111 2049 UDP 111 204 | Instalaciones de iDRAC |
| Concentrator | Concentrator | UDP 50514 | Datos de auditoría |
| Concentrator | Concentrator | UDP 123 | NTP |

Endpoint Hybrid o Endpoint Log Hybrid

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|---------------------------------------|---------------------------------------|--|--|
| Agente de Endpoint 11.1 | Endpoint Hybrid o Endpoint Log Hybrid | TCP 443 | HTTPS de NGINX |
| Agente de Endpoint 11.1 | Log Decoder o Virtual Log Collector | TCP 514 (Syslog) UDP 514 (Syslog) TLS 6514 | Recopilación de registros de Windows |
| Servidor de Endpoint | Log Decoder (externo) | TCP 50102, 56202, 50202 | Para reenviar metadatos a un Log Decoder externo |
| Servidor de NW | Endpoint Hybrid o Endpoint Log Hybrid | TCP 7050 | Tráfico web de la interfaz de usuario |
| Endpoint Hybrid o Endpoint Log Hybrid | Servidor de NW | TCP 5672 | Bus de mensajes |
| Servidor de Endpoint | Servidor de NW | TCP 27017 | MongoDB |

Endpoint Hybrid o Endpoint Log Hybrid con NetWitness Endpoint 4.4

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|---|-----------------|-------------------------|---|
| Servidor de la consola de NW (4.4.0.2 o superior) | Endpoint Hybrid | TCP 443 | HTTPS de NGINX |
| Servicio de metadatos | Log Decoder | TCP 50102, 56202, 50202 | HTTPS de NGINX Para reenviar metadatos a un Log Decoder Endpoint Hybrid o Endpoint Log Hybrid con NWE 4.4 |

Host de Event Stream Analysis (ESA)

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|--------------------------------------|--------------------|------------------------------|---|
| Estación de trabajo de administrador | ESA | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| ESA | Servidor de NW | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Estación de trabajo de administrador | ESA | TCP 22 | Protocolo SSH |
| Servidor de NW, ESA secundario | ESA primario | TCP 27017 | MongoDB |
| Servidor de NW | ESA primario | TCP 7005 | Puerto de lanzamiento de Context Hub: (ESA primario) |
| Servidor de NW | ESA | TCP 50030 (SSL) | Puerto de aplicaciones de ESA |
| Servidor de NW | ESA | TCP 50035 (SSL) | Puerto de aplicaciones de ESA |
| Servidor de NW | ESA | TCP 50036 (SSL) | Puerto de aplicaciones de ESA |
| Servidor de NW | ESA | TCP 5671 | Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW. |
| ESA | cms.netwitness.com | TCP 443 | Live |
| ESA | Servidor NFS | TCP 111 2049 UDP 111 2049 | NTP |
| ESA | Active Directory | 636 (SSL)/389 (no SSL) | |

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|----------------|-----------------|-------------------------------------|--------------------|
| Servidor de NW | ESA | 80 (HTTP)/ 443 (HTTPS) (REST) | |
| ESA primario | Archer | 443 (SSL)/80 (no SSL) | |
| ESA primario | ESA primario | TCP 7007 | Iniciar puerto |
| ESA primario | ESA primario | UDP 50514 | Datos de auditoría |
| ESA primario | ESA primario | UDP 123 | NTP |

Host de Log Collector

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|--------------------------------------|---------------------------------|---|--|
| Estación de trabajo de administrador | Log Collector | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Log Collector | Servidor de NW | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Estación de trabajo de administrador | Log Collector | TCP 22 | Protocolo SSH |
| Log Collector | Orígenes de eventos de registro | Consulte <i>Guía de configuración de la recopilación de registros</i> . Vaya a la Tabla maestra de contenido para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x. | |
| Orígenes de eventos de registro | Log Collector | TCP 514 (Syslog) UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow) | Puertos de recopilación de registros |
| Orígenes de eventos de registro | Log Collector | TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008,64009 | Puertos FTP/S de recopilación de registros |
| Servidor de NW | Log Collector | TCP 56001 (SSL), 50001 (Non-SSL), 50101 (REST) | Puertos de aplicaciones de Log Collector |

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|----------------|-----------------|---|---|
| Servidor de NW | Log Collector | TCP 56006 (SSL), 50006 (no SSL), 50106 (REST) | Puertos de NetWitness Appliance |
| Servidor de NW | Log Collector | TCP 5671 | Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW. |
| Log Collector | Log Collector | UDP 50514 | Datos de auditoría |
| Log Collector | Log Collector | UDP 123 | NTP |
| Log Collector | Servidor NFS | TCP 111 2049 UDP 111 2049 | Instalaciones de iDRAC |

Host de Log Decoder

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|--------------------------------------|---------------------------------|---|--|
| Estación de trabajo de administrador | Log Decoder | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Log Decoder | Servidor de NW | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Estación de trabajo de administrador | Log Decoder | TCP 22 | Protocolo SSH |
| Log Decoder | Orígenes de eventos de registro | Consulte <i>Guía de configuración de la recopilación de registros</i> . Vaya a la Tabla maestra de contenido para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x. | |
| Orígenes de eventos de registro | Log Decoder | TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow) | Puertos de recopilación de registros |
| Orígenes de eventos de registro | Log Decoder | TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009 | Puertos FTP/S de recopilación de registros |
| Servidor de NW | Log Decoder | TCP 56001 (SSL), 50001 (no SSL), 50101 (REST) | Puertos de aplicaciones de Log Collector |

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|----------------|-----------------|---|---|
| Servidor de NW | Log Decoder | TCP 56002 (SSL), 50002 (no SSL), 56202 (Endpoint), 50102 (REST) | Puertos de aplicaciones de Log Decoder |
| Servidor de NW | Log Decoder | TCP 56006 (SSL), 50006 (no SSL), 50106 (REST) | Puertos de NetWitness Appliance |
| Servidor de NW | Log Decoder | TCP 5671 | Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW. |
| Log Decoder | Log Decoder | UDP 50514 | Datos de auditoría |
| Log Decoder | Log Decoder | UDP 123 | NTP |
| Log Decoder | Log Collector | TCP 6514 | |
| Log Decoder | Servidor NFS | TCP 111 2049 UDP 111 204 | Instalaciones de iDRAC |

Host de Log Hybrid

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|--------------------------------------|-----------------|--------------------|--|
| Estación de trabajo de administrador | Log Hybrid | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Log Hybrid | Servidor de NW | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Estación de trabajo de administrador | Log Hybrid | TCP 22 | Protocolo SSH |

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|----------------|---------------------------------|---|-------------|
| Log Collector | Orígenes de eventos de registro | <p>Consulte <i>Guía de configuración de la recopilación de registros</i>. Vaya a la Tabla maestra de contenido para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.</p> | |

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|---------------------------------|-----------------|--|--|
| Orígenes de eventos de registro | Log Hybrid | TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow) | Puertos de recopilación de registros |
| Orígenes de eventos de registro | Log Hybrid | TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009 | Puertos FTP/S de recopilación de registros |
| Servidor de NW | Log Hybrid | TCP 56001 (SSL), 50001 (no SSL), 50101 (REST) | Puertos de aplicaciones de Log Collector |

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|----------------|-----------------|---|---|
| Servidor de NW | Log Hybrid | TCP 56002 (SSL), 50002 (no SSL), 56202 (Endpoint), 50102 (REST) | Puertos de aplicaciones de Log Decoder |
| Servidor de NW | Log Hybrid | TCP 56005 (SSL), 50005 (no SSL), 50105 (REST) | Puertos de aplicaciones de Concentrator |
| Servidor de NW | Log Hybrid | TCP 56006 (SSL), 50006 (no SSL), 50106 (REST) | Puertos de NetWitness Appliance |
| Servidor de NW | Log Hybrid | TCP 5671 | Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW. |
| Log Hybrid | Servidor NFS | TCP 111 2049 UDP 111 204 | Instalaciones de iDRAC |

Host de Malware

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|--------------------------------------|------------------------|---|---|
| Estación de trabajo de administrador | Malware | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Malware | Servidor de NW | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Estación de trabajo de administrador | Malware | TCP 22 | Protocolo SSH |
| Servidor de NW | Malware | TCP 60007 | Puertos de aplicaciones de Malware |
| Servidor de NW | Malware | TCP 56006 (SSL), 50006 (no SSL), 50106 (REST) | Puertos de NetWitness Appliance |
| Servidor de NW | Malware | TCP 5671 | Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW. |
| Servidor de NW | Malware | TCP 5432 | Postgresql |
| Servidor de NW | Malware | TCP 56003 (SSL), 50003 (no SSL), 50103 (REST) | Puertos de aplicaciones de Broker |
| Malware | panacea.threatgrid.com | TCP 443 | ThreatGrid |
| Malware | cloud.netwitness.com | TCP 443 | Evaluación de la comunidad/Opswat |
| Malware | Malware | UDP 50514 | Datos de auditoría |

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|----------------|-----------------|-----------------------------|------------------------|
| Malware | Malware | UDP 123 | NTP |
| Malware | Servidor NFS | TCP 111 2049 UDP 111 204 | Instalaciones de iDRAC |

Host de Packet Decoder

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|--------------------------------------|-----------------|---|---|
| Estación de trabajo de administrador | Packet Decoder | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Packet Decoder | Servidor de NW | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Estación de trabajo de administrador | Packet Decoder | TCP 22 | Protocolo SSH |
| Servidor de NW | Packet Decoder | TCP 56004 (SSL), 50004 (no SSL), 50104 (REST) | Puertos de aplicaciones de Packet Decoder |
| Servidor de NW | Packet Decoder | TCP 56006 (SSL), 50006 (no SSL), 50106 (REST) | Puertos de NetWitness Appliance |
| Servidor de NW | Packet Decoder | TCP 5671 | Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW. |
| Packet Decoder | Packet Decoder | UDP 50514 | Datos de auditoría |
| Packet Decoder | Packet Decoder | UDP 123 | NTP |
| Packet Decoder | Servidor NFS | TCP 111 2049 UDP 111 204 | Instalaciones de iDRAC |

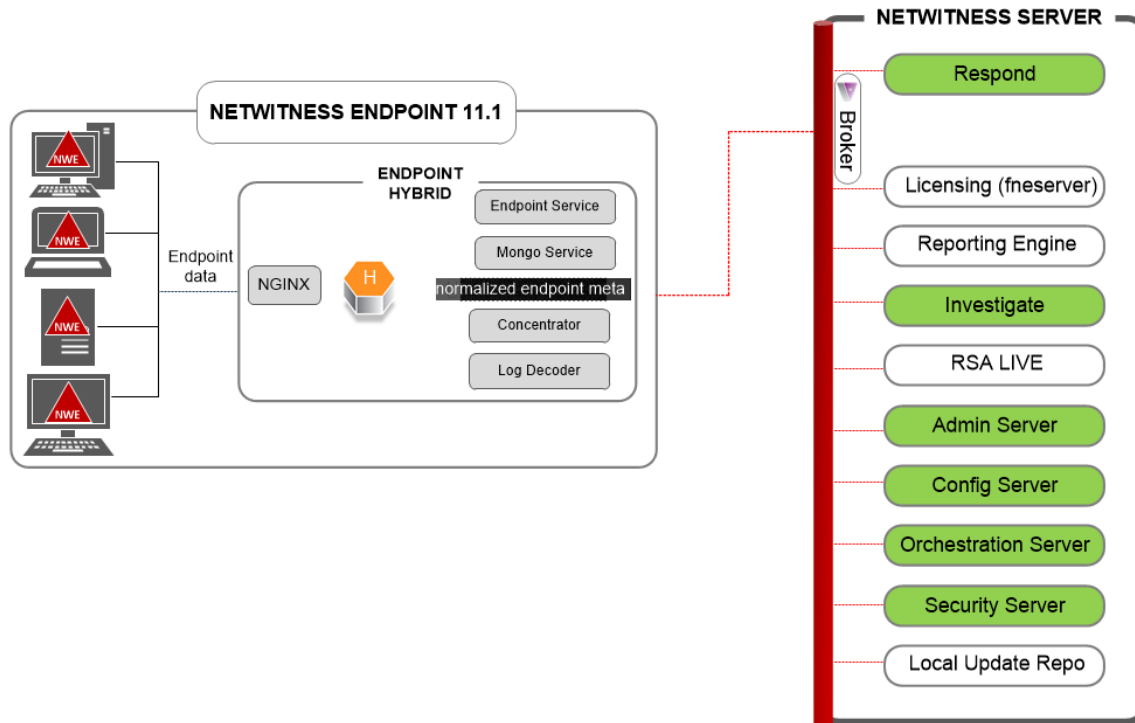
Host de Packet Hybrid

| Host de origen | Host de destino | Puertos de destino | Comentarios |
|--------------------------------------|-----------------|---|---|
| Estación de trabajo de administrador | Packet Hybrid | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Packet Hybrid | Servidor de NW | TCP 15671 | Interfaz del usuario de administración de RabbitMQ |
| Estación de trabajo de administrador | Packet Hybrid | TCP 22 | Protocolo SSH |
| Servidor de NW | Packet Hybrid | TCP 56004 (SSL), 50004 (no SSL), 50104 (REST) | Puertos de aplicaciones de Packet Decoder |
| Servidor de NW | Packet Hybrid | TCP 56005 (SSL), 50005 (no SSL), 50105 (REST) | Puertos de aplicaciones de Concentrator |
| Servidor de NW | Packet Hybrid | TCP 56006 (SSL), 50006 (no SSL), 50106 (REST) | Puertos de NetWitness Appliance |
| Servidor de NW | Packet Hybrid | TCP 5671 | Bus de mensajes de RabbitMQ (AMQPS) para todos los hosts de NW. |
| Packet Hybrid | Servidor NFS | TCP 111 2049 UDP 111 204 | Instalaciones de iDRAC |

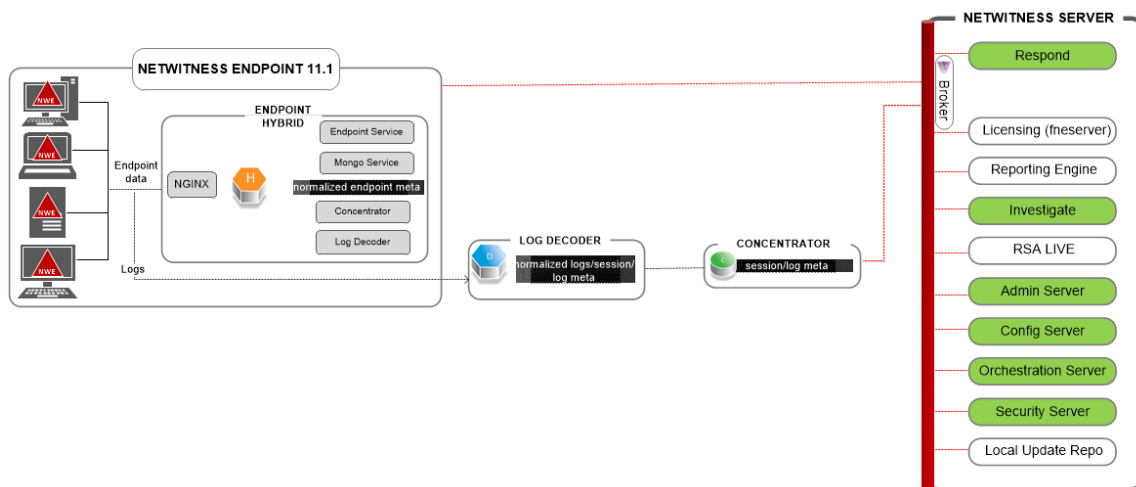
Arquitectura de NetWitness Endpoint Insights

En los siguientes diagramas se muestra la arquitectura de red de NetWitness Endpoint Insights.

NetWitness Endpoint Insights 11.1

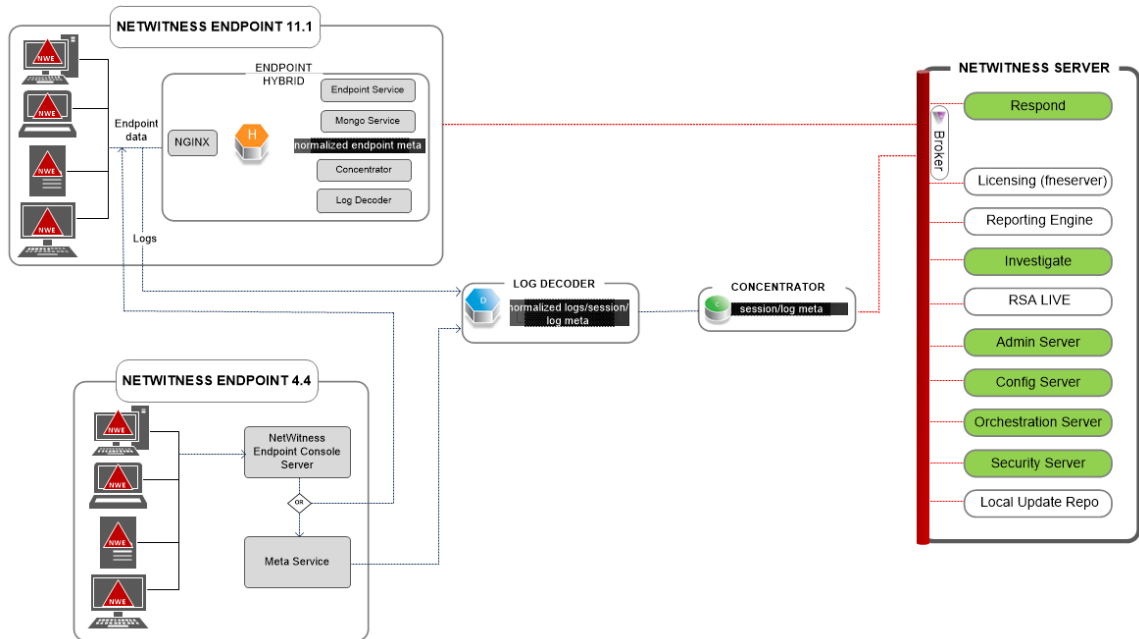


NetWitness Endpoint Insights 11.1 con Log Decoder



Integración de NetWitness Endpoint 4.4 con NetWitness Endpoint Insights

11.1



Para obtener más información sobre los servicios que se ejecutan en Endpoint Hybrid, consulte la *Guía de configuración de RSA NetWitness Endpoint Insights*. Vaya a la [Tabla maestra de contenido](#) para NetWitness Logs & Packets 11.x para buscar todos los documentos de NetWitness Suite 11.x.

Requisitos y seguridad del sitio

Asegúrese de leer este tema con detención y respete todas las advertencias y las precauciones antes de instalar o realizar el mantenimiento de los dispositivos de RSA.

Usos previstos de la aplicación

Este producto se evaluó como un equipo de tecnología de la información (ITE) que se puede instalar en oficinas, escuelas, salas de computadoras y ubicaciones interiores similares de tipo comercial. Este dispositivo no está diseñado para ningún tipo de conexión a un cable para exteriores.

Servicio

Este dispositivo no contiene componentes que el usuario pueda reparar. Si se produce un desperfecto, póngase en contacto con Atención al cliente. En una condición de falla, se pueden generar altas temperaturas dentro del sistema, las cuales pueden activar una señal de alarma. En caso de una señal de alarma, desconecte inmediatamente el dispositivo de la fuente de alimentación y póngase en contacto con Atención al cliente. El funcionamiento del dispositivo en estas condiciones será inseguro y puede causar lesiones o daños materiales.

Información sobre seguridad

Selección del sitio

El sistema está diseñado para funcionar en un ambiente de oficina típico. Elija un sitio que esté:

- Limpio, seco y libre de partículas transportadas por el aire (más allá del polvo normal de una habitación).
- Bien ventilado y lejos de fuentes de calor, entre ellas, luz solar directa y radiadores.
- Lejos de fuentes de vibración o de golpes físicos.
- Aislado de campos electromagnéticos fuertes producidos por dispositivos eléctricos.
- En regiones susceptibles a tormentas eléctricas, se recomienda conectar el sistema a un supresor de sobretensión.
- Equipado con un tomacorriente de pared correctamente conectado a tierra.
- Provisto de espacio suficiente para acceder a los cables de la fuente de alimentación, debido a que actúan como el principal medio de desconexión del producto.

Prácticas de manejo de equipos

Reduzca el riesgo de lesiones o daño en los equipos mediante:

- El cumplimiento de requisitos locales de salud y seguridad ocupacionales cuando transfiera y levante equipos.
- El uso de asistencia mecánica u otra que sea apropiada cuando transfiera y levante equipos.
- La reducción del peso para lograr un manejo más sencillo gracias a la extracción de componentes fácilmente desmontables.

Advertencias eléctricas y de alimentación

Precaución: El botón de encendido, que se señala con una marca de alimentación en espera, NO apaga totalmente la alimentación AC del sistema; la alimentación en espera de 5 V permanece activa mientras el sistema está conectado. Para cortar la alimentación del sistema, debe desconectar los cables de alimentación AC del tomacorriente de pared.

- No intente modificar ni usar un cable de alimentación AC si no es el tipo exacto que se exige. Se requiere un cable de AC por separado para cada fuente de alimentación del sistema.
- Este producto no contiene componentes que el usuario pueda reparar. No abra el sistema.
- Cuando reemplace una fuente de alimentación de conexión en caliente, desconecte el cable de alimentación de la fuente de alimentación que se va a reemplazar antes de quitarla del servidor.

Advertencias sobre el montaje en rack

- El rack del equipo se debe anclar a un soporte fijo para evitar que se incline cuando se extienda desde él un servidor o un equipo. El rack del equipo se debe instalar de acuerdo con las instrucciones de su fabricante.
- El montaje del equipo en el rack se debe realizar sin que se presente una condición de peligro debido a una carga mecánica irregular.
- Extienda solo un equipo por vez desde el rack.
- Para evitar el riesgo de una posible descarga eléctrica, debe implementarse una conexión a tierra de seguridad adecuada para el rack y cada pieza de equipo instalada en él.

Enfriamiento y flujo de aire

La instalación del equipo se debe realizar de manera tal que no sea vea afectada la cantidad de flujo de aire que se necesita para el funcionamiento seguro del equipo.

Colocación de la antena

Este equipo se debe instalar y usar con una distancia mínima de 7 cm entre el radiador y su cuerpo. Las antenas que se usan para este transmisor no deben estar en la misma ubicación ni se deben usar en conjunto con ninguna otra antena o transmisor.

Configurar la agregación de grupos

La agregación de grupos se usa para configurar varios servicios Archiver o Concentrator como un grupo y compartir las tareas de agregación entre ellos. Puede configurar varios servicios Archiver o Concentrator para que agreguen de manera eficiente desde varios servicios Log Decoder con el fin de mejorar el rendimiento de las consultas en los datos:

- Almacenados en el Archiver.
- Procesados a través del Concentrator.

Recomendaciones para la implementación de la agregación de grupos de RSA

RSA recomienda la siguiente implementación para la agregación de grupos.

- Entre uno y dos Log Decoders
- Entre tres y cinco Archivers o Concentrators

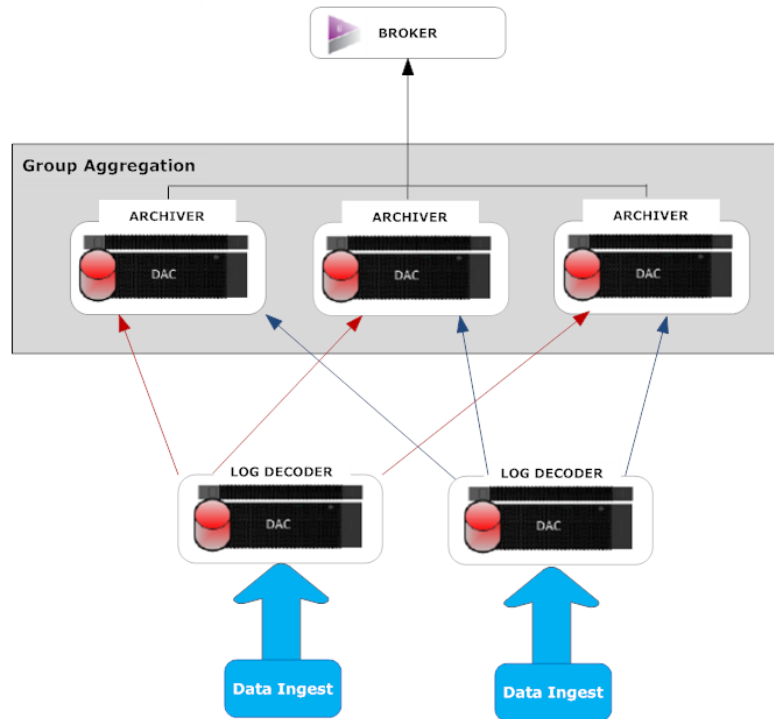
Ventajas de usar la agregación de grupos

Agregación de grupos:

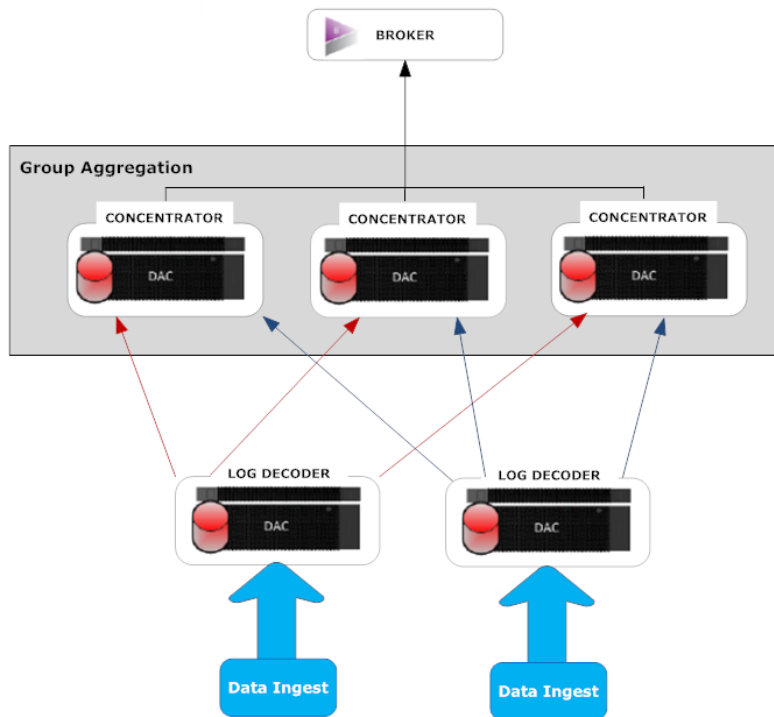
- Aumenta la velocidad de las consultas de RSA NetWitness® Suite.
- Mejora el rendimiento de las consultas agregadas (Count y Sum) en el ambiente.
- Mejora el rendimiento del servicio de investigación.
- Ofrece la opción de almacenar datos durante más tiempo con fines de investigación.

En el siguiente diagrama se ilustra la agregación de grupos.

Archivers



Concentrators



Puede haber una cantidad indefinida de Archivers o Concentrators agrupados, los cuales forman un grupo de agregación. Los servicios Archiver o Concentrator del grupo dividen toda la sesión agregada entre ellos de acuerdo con la cantidad de sesiones definidas en el parámetro Sesiones máximas de agregación.

Por ejemplo, en un grupo de agregación que contiene dos servicios Archiver o dos servicios Concentrator con el parámetro Sesiones máximas de agregación configurado en 10,000, los servicios dividirían la sesión entre ellos como se ilustra en la siguiente tabla.

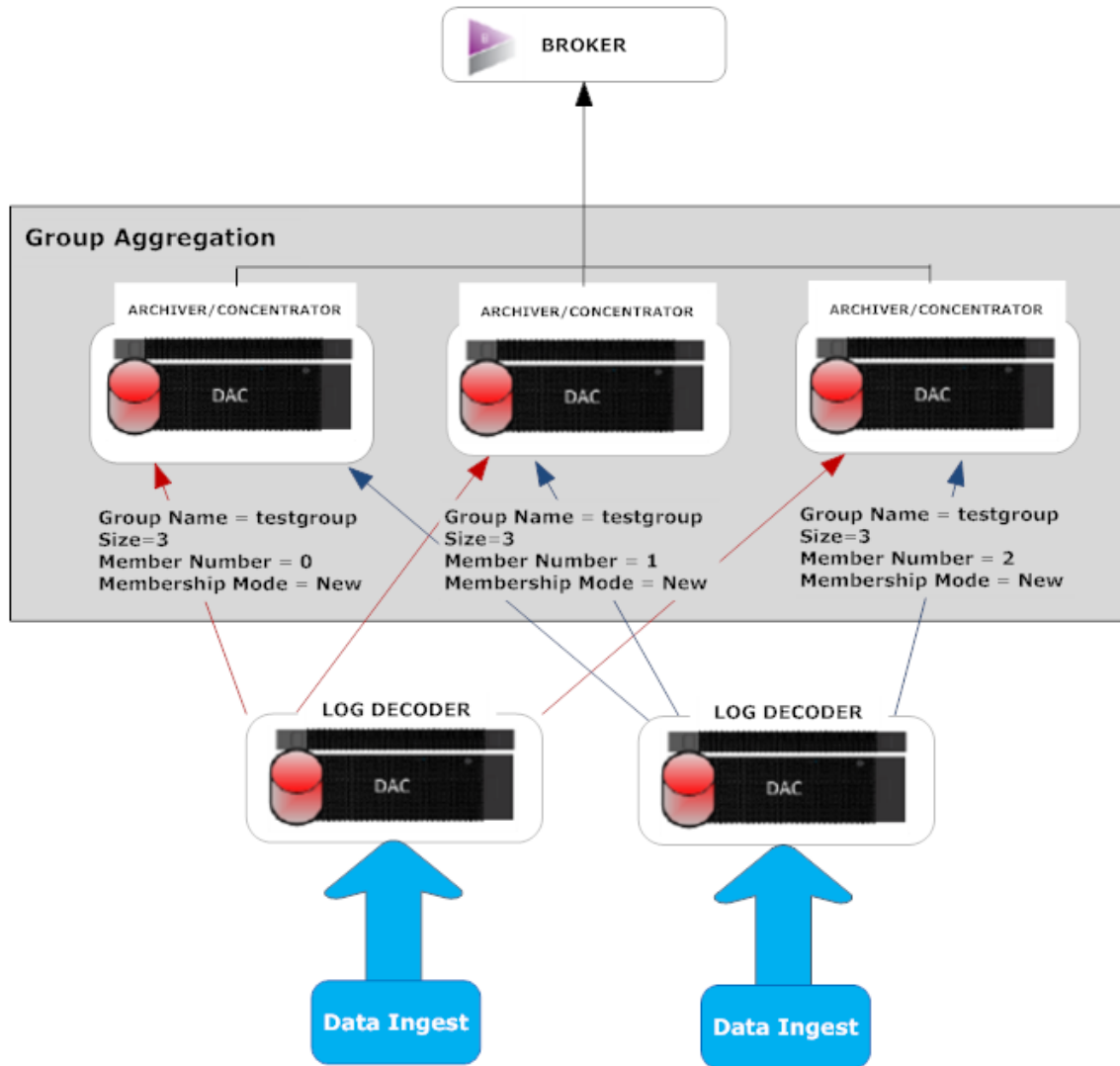
| Archiver 0 o Concentrator 0 | Archiver 1 o Concentrator 1 |
|-----------------------------|-----------------------------|
| 1 a 9,999 | 10,000 a 19,999 |
| 20,000 a 29,999 | 30,000 a 39,999 |
| 40,000 a 49,999 | 50,000 a 59,999 |

Configurar la agregación de grupos

Complete este procedimiento para configurar múltiples servicios Archiver o Concentrator como un grupo y compartir las tareas de agregación entre ellos.

Requisitos previos

Planee el diseño de la red para la agregación de grupos. La siguiente figura es un ejemplo de una configuración de agregación de grupos.

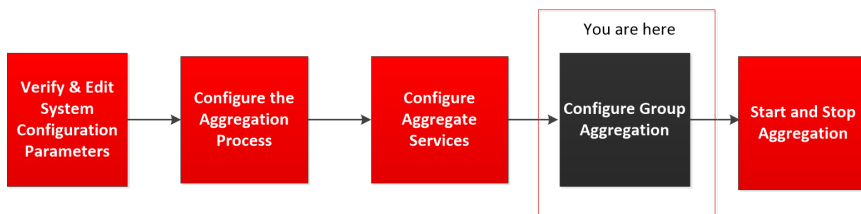


Asegúrese de comprender los parámetros de agregación de grupos de la siguiente tabla y de crear un plan de agregación de grupos.

| Parámetro | Descripción |
|------------------|--|
| Nombre del grupo | Determina el grupo al cual pertenece el Archiver o el Concentrador. Puede agregar cualquier número de datos de agregación de grupos desde un Log Decoder. Log Decoder utiliza el parámetro Nombre del grupo para identificar los servicios Archiver o Concentrador que están trabajando juntos. Todos los servicios Archiver o Concentrador en el grupo deben tener el mismo nombre de grupo. |

| | |
|-------------------|---|
| Tamaño | Determina la cantidad de servicios Archiver o Concentrator en el grupo de agregación. |
| Número de miembro | Determina la posición del Archiver o del Concentrator en el grupo de agregación. En el caso de un grupo de tamaño N, se debe configurar el número de miembro de 0 a N-1 en cada uno de los servicios Archiver o Concentrator del grupo de agregación. Por ejemplo: Si el tamaño del grupo de agregación es 2, el número de miembro de uno de los servicios Archiver o Concentrator se debe configurar en 0 y el del otro Archiver o Concentrator, en 1. |
| Modo de membresía | Hay dos modos de membresía: Nuevo y Reemplazo. Nuevo: Adición de un nuevo servicio Archiver o Concentrator como miembro del grupo de agregación existente o creación de un grupo de agregación. El servicio Archiver o Concentrator no agrega ninguna sesión existente desde el servicio, ya que otros miembros del grupo ya habrían agregado en él todas las sesiones. Este servicio Archiver o Concentrator solo agregará nuevas sesiones a medida que aparecen en el servicio. Reemplazo: Reemplazo de un miembro del grupo de agregación existente. El Archiver o el Concentrator comenzarán la agregación a partir de la sesión más antigua disponible en el servicio desde el cual realiza la agregación. |

Nota: este parámetro solo tiene efecto cuando no se han agregado sesiones desde el servicio. Después de agregar algunas sesiones este parámetro no tiene ningún efecto.



Configurar la agregación de grupos



Complete el siguiente procedimiento para configurar la agregación de grupos.

1. Configure varios servicios Archiver o Concentrator en el ambiente. Asegúrese de agregar el mismo Log Decoder como origen de datos en todos los servicios.
2. Realice lo siguiente en todos los servicios de Archiver o Concentrator que desea que formen

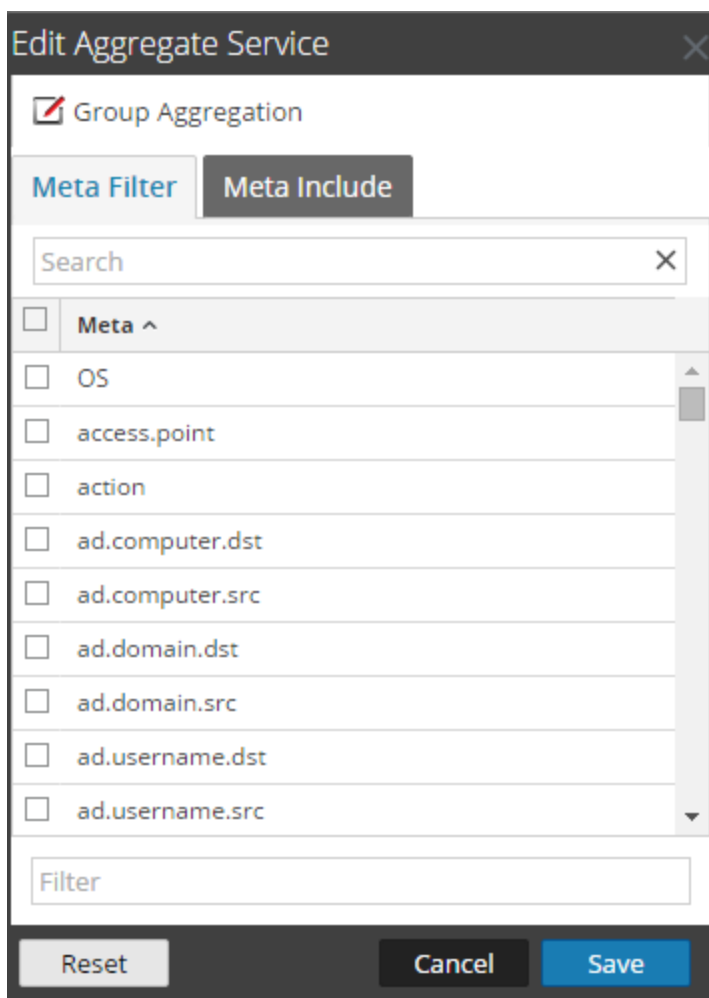
parte del grupo de agregación:

- a. En el **menú principal**, seleccione **ADMINISTRAR > Servicios**.
- b. Seleccione el servicio Archiver o Concentrator y, en la columna **Acciones**, seleccione **Ver > Configuración**.

Se muestra la vista Configuración del dispositivo de Archiver o Concentrator.

- c. En la sección **Servicios agregados**, seleccione el dispositivo de Log Decoder.
- d. Haga clic en  **Toggle Service** para cambiar el estado de Log Decoder a offline si se encuentra en línea.
- e. Haga clic en .

Se muestra el cuadro de diálogo **Editar servicio agregado**.



- f. Haga clic en  **Group Aggregation**.

Se muestra el cuadro de diálogo **Editar agregación de grupos**.

- g. Seleccione la casilla de verificación **Activado** y configure los siguientes parámetros:
 - En el campo **Nombre del grupo**, escriba el nombre del grupo.
 - En el campo **Tamaño**, seleccione la cantidad de servicios Archiver o Concentrator en el grupo de agregación.
 - En el campo **Número de miembro**, seleccione la posición de Archiver o Concentrator en el grupo de agregación.
 - En el menú desplegable **Modo de membresía**, seleccione el modo.
 - h. Haga clic en **Guardar**.
 - i. En la página Vista de configuración del dispositivo, haga clic en **Aplicar**.
 - j. Realice del **paso b** al **paso i** en todos los demás servicios Archiver o Concentrator que deben ser parte de la agregación de grupos.
3. En la sección **Configuración de agregación**, configure el parámetro **Sesiones máximas de agregación** en **10000**.

