Cisco Secure Network Analytics

Guía de instalación del appliance de hardware serie x2xx 7.4.2

Índice

Introducción **5**

Descripción general 5

Público 6

Instalación de dispositivos y configuración del sistema 6

Información relacionada 6

Terminología 7

Abreviaturas frecuentes 7

Acerca de los appliances de Secure Network Analytics **8**

Administrador 2210 8

Almacén de datos 6200 8

Recopilador de flujo 4210 y 5210 9

UDP Director 2210 9

Sensor de flujo 1210, 3210 y 4240 10

Secure Network Analytics sin almacén de datos **11**

Secure Network Analytics con del almacén de datos **12**

Consultas 13

Almacenamiento del almacén de datos y tolerancia a errores 13

Ejemplo de almacenamiento de telemetría 14

Requisitos generales de la implementación **15**

Matriz de las versiones de hardware y software 15

Especificaciones 15

Cisco Integrated Management Controller (CIMC) 15

Requisitos estándar del appliance (sin almacén de datos) 16

Requisitos de implementación del administrador y recopilador de flujo 16

Requisitos para la implementación del almacén de datos **17**

Requisitos del appliance (con almacén de datos) 17

Requisitos de implementación del administrador y recopilador de flujo 17

Requisitos para la implementación del nodo de datos 18

Implementación de varios nodos de datos 18
Implementación de un único nodo de datos 19
Requisitos para configurar un nodo de datos 19
Consideraciones de red y switching 20
Ejemplo de conmutador de hardware 22
Consideraciones sobre la ubicación del almacén de datos 23
Requisitos del despliegue de análisis 24
1. Configuración del firewall para las comunicaciones 25
Puertos abiertos (todos los appliances) 25
Puertos abiertos adicionales para nodos de datos 25
Puertos de comunicación y protocolos 26
Puertos abiertos adicionales para el almacén de datos 28
Puertos de comunicación opcionales 30
Secure Network Analytics Ejemplo de implementación 31
Secure Network Analytics Ejemplo de implementación con almacén de datos 32
2. Advertencias y pautas de instalación 33
Advertencias de instalación 33
Instrucciones de instalación 40
Recomendaciones de seguridad 41
Mantener la seguridad con electricidad 41
Evitar daños por ESD 42
Entorno del sitio 42
Consideraciones de la fuente de alimentación 43
Consideraciones sobre la configuración en rack 43
3. Montaje de los appliances 44
Hardware incluido en el appliance 44
Hardware adicional necesario 44
4. Conectar sus appliances a la red 45
1. Revisar las especificaciones 45
2. Conectar su appliance a la red 46

5. Conectarse a su appliance **47**
Conexión con un teclado y un monitor 47
Conexión con un cable de serie o una consola de serie 48
Conexión con CIMC (obligatorio para el acceso remoto) 49
6. Configuración del sistema Secure Network Analytics **50**
Requisitos para configurar el sistema 50
Ponerse en contacto con el servicio de asistencia **54**
Historial de cambios **56**

Introducción

Descripción general

En esta guía se explica cómo instalar appliances de hardware de la serie x2xx de Cisco Secure Network Analytics (antes Stealthwatch). En esta guía, también se describe el montaje y la instalación del hardware de Secure Network Analytics.

> ⚠ Lea el documento Información de seguridad normativa y de cumplimiento antes de instalar los appliances de la serie Secure Network Analytics x2xx.

El hardware de la serie x2xx incluye:

Appliance	**Número de pieza**
Administrador 2210 (anteriormente Consola de gestión de Stealthwatch)	ST-SMC2210-K9
Almacén de datos 6200 (tres nodos de datos)	ST-DS6200-K9 (tres ST-DNODE-G1)
Recopilador de flujo 4210	ST-FC4210-K9
Motor del recopilador de flujo 5210	ST-FC5210-E
Base de datos del recopilador de flujo 5210	ST-FC5210-D
UDP Director 2210	ST-UDP2210-K9
Sensor de flujo 1210	ST-FS1210-K9
Sensor de flujo 3210	ST-FS3210-K9
Sensor de flujo 4240	ST-FS4240-K9

Público

Esta guía está diseñada para la persona responsable de la instalación del hardware de Secure Network Analytics. Damos por sentado que ya dispone de ciertos conocimientos generales sobre la instalación de equipos de red.

Si prefiere trabajar con un profesional para la instalación, póngase en contacto con su partner local de Cisco o con el soporte de Cisco.

Instalación de dispositivos y configuración del sistema

Tenga en cuenta el flujo de trabajo general para la instalación y configuración de Secure Network Analytics.

1. **Instalar appliances:** instale los dispositivos (físicos) de hardware de la serie Secure Network Analytics x2xx con esta guía de instalación. Para instalar dispositivos de la edición virtual, siga las instrucciones de la Guía de instalación de dispositivos de la edición virtual.
2. **Configuración de Secure Network Analytics:** después de instalar el hardware y los dispositivos virtuales, estará listo para configurar Secure Network Analytics en un sistema administrado. Siga las instrucciones de la Secure Network Analytics Guía de configuración del sistema v7.4.2.x.

Información relacionada

Para obtener más información sobre Secure Network Analytics, consulte los siguientes recursos en línea:

- **Información de seguridad normativa y de cumplimiento:** lea el documento Información de seguridad normativa y de cumplimiento antes de instalar los appliances de la serie Secure Network Analytics x2xx.
- **Descripción general:** https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
- **Guía para el diseño del almacén de datos:** https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-data-store-guide.pdf
- **Matriz de compatibilidad de versiones de hardware y software:** https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html
- **Especificaciones del appliance:** https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html

Terminología

Esta guía utiliza el término "**appliance**" para cualquier producto de Secure Network Analytics.

Un "**clúster**" es el grupo de dispositivos Secure Network Analytics administrados por el Administrador.

Abreviaturas frecuentes

En esta guía, se incluyen las siguientes abreviaturas:

Abreviatura	**Descripción**
DMZ	Zona desmilitarizada (una red perimetral)
HTTPS	Protocolo (seguro) de transferencia de hipertexto
ISE	Identity Services Engine
NIC	Tarjeta de interfaz de red
NTP	Protocolo de tiempo de red
PCIe	Interconexión rápida de componentes periféricos
SNMP	Protocolo simple de administración de red
SPAN	Analizador de puerto de switch
TAP	Puerto de acceso de prueba
UPS	Fuente de alimentación ininterrumpida
VLAN	Red de área local virtual

Acerca de los appliances de Secure Network Analytics

Secure Network Analytics consta de varios appliances de hardware que recopilan, analizan y presentan información sobre su red para mejorar su rendimiento y seguridad. Esta sección describe cada appliance de la serie Secure Network Analytics x2xx.

Administrador 2210

El Administrador gestiona, coordina, configura y organiza los distintos componentes del sistema. El software Secure Network Analytics le permite acceder a la web de la consola desde cualquier ordenador con acceso a un navegador. Puede acceder con facilidad a la información de red y seguridad en tiempo real sobre partes fundamentales de su empresa. Gracias a la independencia de la plataforma basada en Java, el Administrador permite:

- La configuración, la información y la administración centralizada de hasta 25 recopiladores de flujo de Secure Network Analytics
- Gráficos para visualizar el tráfico
- Análisis de detalles para la resolución de problemas
- Informes consolidados y personalizables
- Análisis de tendencias
- Supervisión del rendimiento
- Notificación inmediata de las brechas de seguridad

Si está implementando un almacén de datos, puede configurar un Administrador 2210 con una interfaz SFP+ DAC de 10 Gbps como eth0 para aumentar el rendimiento. Si no está implementando un almacén de datos, solo puede configurar la interfaz de 1 Gbps/10 Gbps como eth0.

Almacén de datos 6200

El almacén de datos proporciona un repositorio central para almacenar la telemetría de su red, recogida por los recopiladores de flujo. El almacén de datos se compone de un clúster de nodos de datos, cada uno con una parte de sus datos, y una copia de seguridad de los datos de un nodo de datos independiente. Dado que todos sus datos se encuentran en una base de datos centralizada en lugar de extenderse a través de varios recopiladores de flujo, su Administrador puede recuperar los resultados de las consultas del almacén de datos más rápidamente que si consultara a todos los recopiladores de flujo por separado. El clúster del almacén de datos proporciona una tolerancia a errores

mejorada, una respuesta de consulta mejorada y una población de gráficos y gráficos más rápida.

Consulte **Secure Network Analytics con del almacén de datos** para obtener más información.

Recopilador de flujo 4210 y 5210

El recopilador de flujo incluye datos NetFlow, cFlow, J-Flow, Packeteer2, NetStream e IPFIX para ofrecer protección de red basada en el comportamiento.

El recopilador de flujo agrega datos de comportamiento de la red de alta velocidad procedentes de varias redes o segmentos de red para posibilitar una protección integral y mejorar el rendimiento en redes situadas en diversas ubicaciones.

Si está implementando un almacén de datos, puede configurar un recopilador de flujo 4210 con una interfaz SFP+ DAC de 10 Gbps como eth0 para aumentar el rendimiento. Si no está implementando un almacén de datos, solo puede configurar la interfaz de cobre de 100 Mbps/1 Gbps/10 Gbps como eth0.

> A medida que el recopilador de flujo recibe datos, identifica ataques conocidos o desconocidos, el uso indebido interno y dispositivos de red mal configurados independientemente de si hay fragmentación o cifrado de paquetes. Una vez que Secure Network Analytics identifica el comportamiento, el sistema puede llevar a cabo cualquier medida que haya configurado, si es que la hay, para dicho tipo de comportamiento.

UDP Director 2210

El UDP Director es un replicador del paquete de UDP de gran velocidad y alto rendimiento. El UDP Director es de gran utilidad para la redistribución de las trampas de NetFlow, sFlow, syslog o del Protocolo simple de administración de red (SNMP) en varios recopiladores. Puede recibir datos de cualquier aplicación UDP sin conexión y, a continuación, los retransmite a varios destinos y los duplica si así se requiere.

Si utiliza la configuración de alta disponibilidad (HA) del UDP Director, compruebe que ha conectado dos appliances de UDP Director con cables cruzados. Para ver las instrucciones, consulte **2. Conectar su appliance a la red**.

Sensor de flujo 1210, 3210 y 4240

El sensor de flujo es un appliance de red que funciona de forma similar a la de los habituales appliances de captura de paquetes o IDS que se conecta en un analizador de puerto de switch (SPAN), un puerto de reflejo o un puerto de acceso de prueba (TAP) de Ethernet. El sensor de flujo aumenta la visibilidad en las siguientes áreas de red:

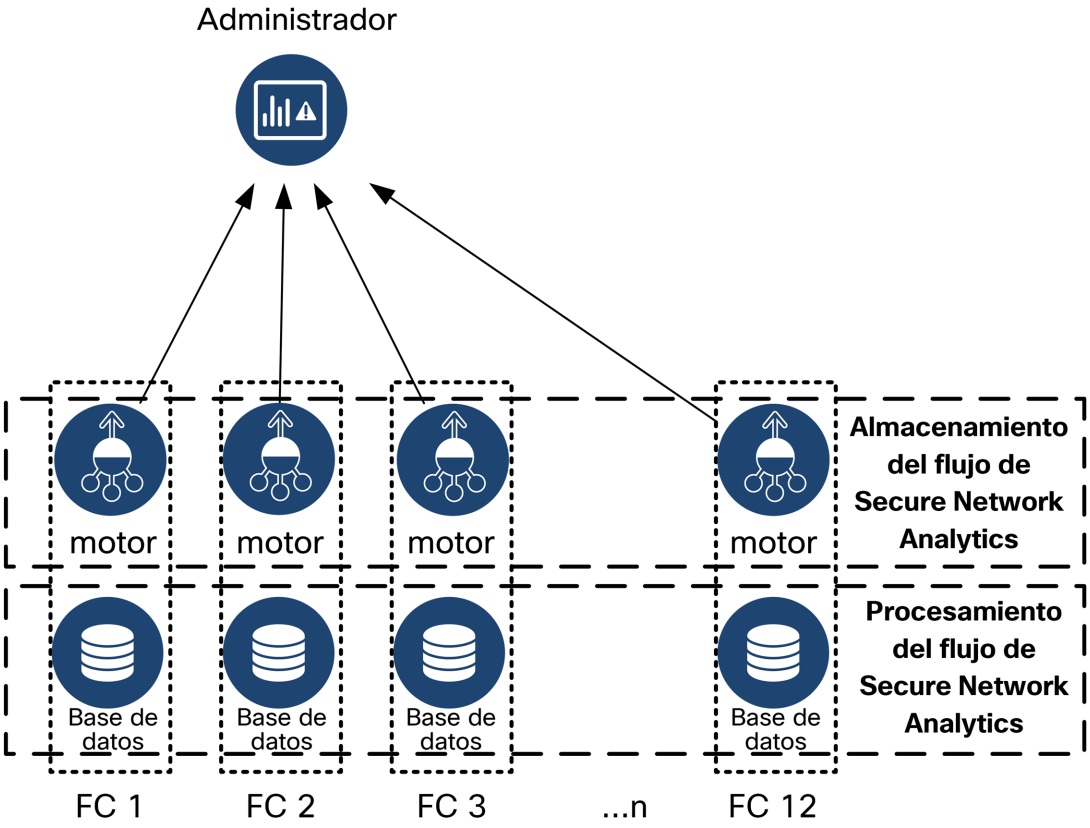
- Donde NetFlow no está disponible.
- Donde NetFlow está disponible pero desea obtener una mayor visibilidad de los indicadores de rendimiento y datos del paquete.

Al dirigir el sensor de flujo hacia cualquier recopilador de flujo compatible con NetFlow v9, obtendrá útiles estadísticas del tráfico detalladas de NetFlow. Cuando se combina con el recopilador de flujo de Secure Network Analytics, el sensor de flujo también ofrece una visión detallada de los indicadores de rendimiento y de comportamiento. Estos indicadores de rendimiento del flujo ofrecen una visión de latencia de recorrido de ida y vuelta introducida por la red o por la aplicación del lado servidor.

Ya que el sensor de flujo consta de visibilidad a nivel del paquete, puede calcular el tiempo de ida y vuelta (RTT), el tiempo de respuesta del servidor (SRT) y la pérdida de paquetes para sesiones TCP. Incluye todos estos campos adicionales en los registros de NetFlow que envía al recopilador de flujo.

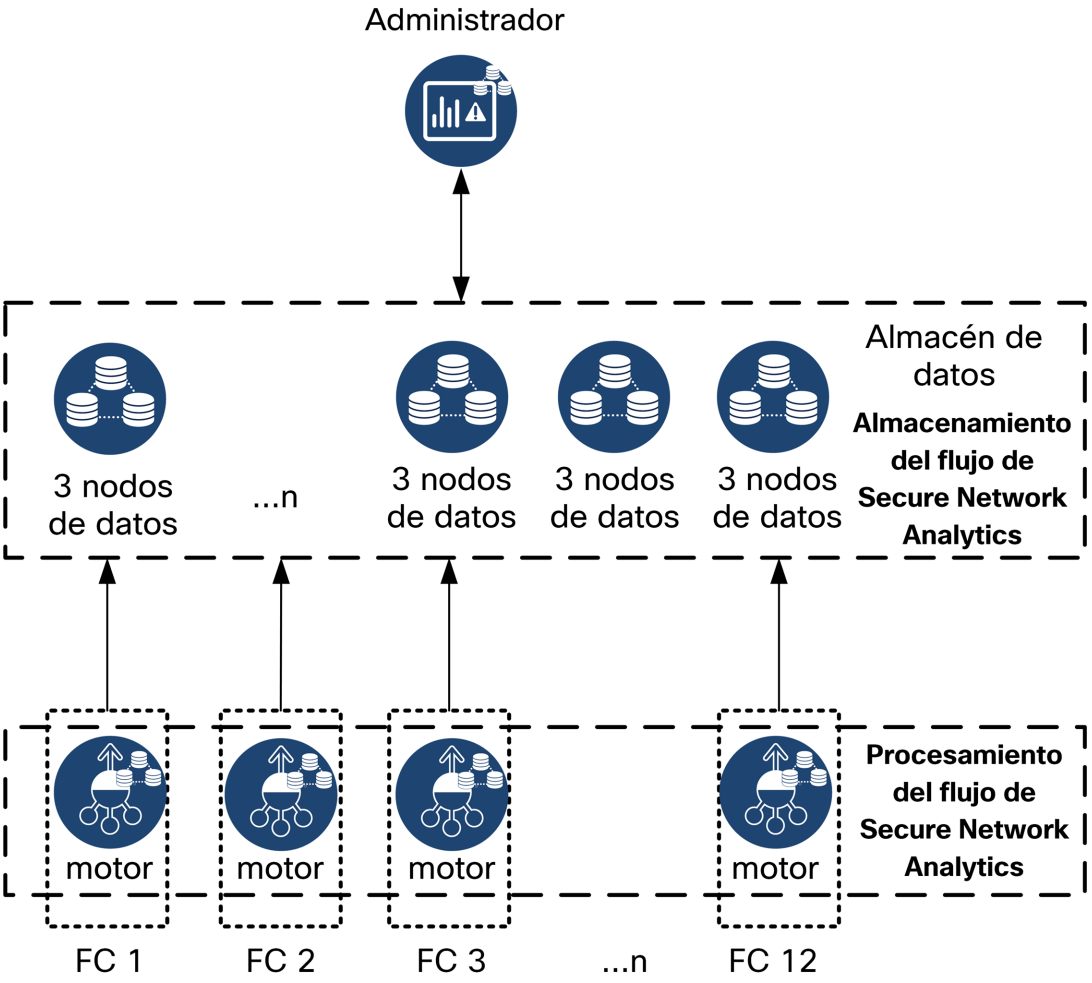
Secure Network Analytics sin almacén de datos

En una implementación de Secure Network Analytics sin un almacén de datos, uno o más recopiladores de flujo ingieren y deduplican datos, realizan análisis y notifican datos y resultados directamente al Administrador. Para resolver las consultas enviadas por el usuario, incluidos los gráficos y las tablas, el Administrador consulta todos los recopiladores de flujos gestionados. Cada Flow Collector devuelve resultados coincidentes al Administrador. El Administrador recopila la información de los diferentes conjuntos de resultados y, a continuación, genera un gráfico o un gráfico que muestra los resultados. En esta implementación, cada Flow Collector almacena datos en una base de datos local. Consulte el siguiente diagrama para ver un ejemplo.



Secure Network Analytics con del almacén de datos

En una implementación de Secure Network Analytics con un almacén de datos, el clúster del almacén de datos se sitúa entre el Administrador y los recopiladores de flujo. Uno o más recopiladores de flujo ingieren y deduplican los flujos, realizan análisis e informan de los datos y resultados directamente al almacén de datos, distribuyéndolos aproximadamente por igual a todos los nodos de datos. El almacén de datos facilita el almacenamiento de datos, mantiene todo su tráfico en dicha ubicación centralizada en lugar de repartirlo entre varios recopiladores de flujo y ofrece una mayor capacidad de almacenamiento que varios recopiladores de flujo. Vea el siguiente diagrama de ejemplo.



El almacén de datos proporciona un repositorio central para almacenar la telemetría de su red, recogida por los recopiladores de flujo. El almacén de datos se compone de un clúster de nodos de datos, cada uno con una parte de sus datos, y una copia de

seguridad de los datos de un nodo de datos independiente. Dado que todos sus datos se encuentran en una base de datos centralizada en lugar de extenderse a través de varios recopiladores de flujo, su Administrador puede recuperar los resultados de las consultas del almacén de datos más rápidamente que si consultara a todos los recopiladores de flujo por separado. El clúster del almacén de datos proporciona una tolerancia a errores mejorada, una respuesta de consulta mejorada y una población de gráficos y gráficos más rápida.

Consultas

Para resolver consultas enviadas por el usuario, incluidos gráficos y tablas, el Administrador consulta el almacén de datos. El almacén de datos encuentra resultados coincidentes en las columnas relevantes para la consulta, luego recupera las filas coincidentes y devuelve los resultados de la consulta al Administrador. El Administrador genera el gráfico o la tabla sin necesidad de recopilar varios conjuntos de resultados de varios recopiladores de flujo. Esto reduce el coste de las consultas, en comparación con las consultas de varios recopiladores de flujo, y mejora el rendimiento de las consultas.

Almacenamiento del almacén de datos y tolerancia a errores

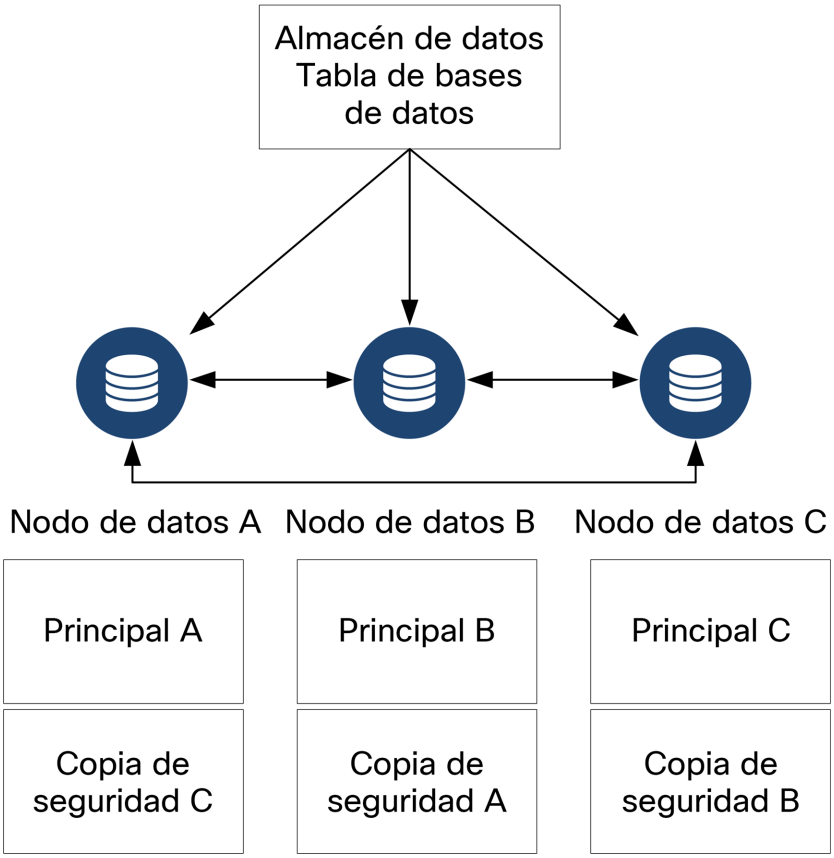
El almacén de datos recopila datos de los recopiladores de flujo y los distribuye de manera equitativa entre los nodos de datos en el clúster. Cada nodo de datos, además de almacenar una parte de su telemetría general, también almacena una copia de seguridad de la telemetría de otro nodo de datos. Almacenar datos de esta manera:

- ayuda con el equilibrio de carga
- distribuye el procesamiento entre cada nodo
- garantiza que todos los datos introducidos en el almacén de datos tienen una copia de seguridad de tolerancia a errores
- permite aumentar el número de nodos de datos para mejorar el almacenamiento general y el rendimiento de las consultas

Si su almacén de datos tiene 3 o más nodos de datos y un nodo se cae, el almacén de datos en conjunto permanece activo siempre y cuando el nodo de datos que contiene su copia de seguridad todavía esté disponible y al menos la mitad del número total de nodos de datos todavía esté activo. Esto le deja tiempo para reparar la conexión caída o el hardware defectuoso. Después de sustituir el nodo de datos defectuoso, el almacén de datos restaura los datos de ese nodo de la copia de seguridad existente almacenada en el nodo de datos adyacente y crea una copia de seguridad de los datos en ese nodo de datos.

Ejemplo de almacenamiento de telemetría

Consulte el siguiente diagrama para ver un ejemplo de cómo 3 nodos de datos almacenan la telemetría:



Requisitos generales de la implementación

Antes de comenzar, revise esta guía para comprender el proceso, la preparación, el tiempo y los recursos que necesitará planificar para la instalación.

Matriz de las versiones de hardware y software

Revise la Matriz de las versiones de hardware y software para obtener detalles sobre la compatibilidad. La matriz está disponible en https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html.

Especificaciones

Descargue la hoja de especificaciones de cada appliance que quiera instalar. Las especificaciones están disponibles en https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html.

Cisco Integrated Management Controller (CIMC)

Después de instalar sus appliances, configure Cisco Integrated Management Controller (CIMC) para habilitar el acceso a la configuración del servidor y a una consola del servidor virtual. También puede utilizar el CIMC para supervisar el estado del hardware.

- **Instrucciones:** consulte **Conexión con CIMC (obligatorio para el acceso remoto)** y siga las instrucciones de la Guía de configuración de la GUI del controlador de administración integrado CIMC de Cisco UCS de la serie C.
- **Contraseña predeterminada:** como parte de la configuración inicial, iniciará sesión en el CIMC como administrador y escribirá **password** en el campo Contraseña.
- **Requisitos de la contraseña:** cuando inicie sesión, cambie la contraseña predeterminada para proteger la seguridad de su red.

Requisitos estándar del appliance (sin almacén de datos)

Si está instalando Secure Network Analytics sin un almacén de datos, instale los siguientes dispositivos:

Appliance	Requisito
Administrador	• Mínimo 1 Administrador
Recopilador de flujo	• Mínimo de 1 recopilador de flujo
Sensor de flujo	Opcional
UDP Director	Opcional

Para revisar los requisitos de instalación de Secure Network Analytics con un almacén de datos, consulte **Requisitos para la implementación del almacén de datos**.

Requisitos de implementación del administrador y recopilador de flujo

Por cada Administrador y recopilador de flujo que implemente, asignará una dirección IP enrutable al puerto de gestión `eth0`.

Requisitos para la implementación del almacén de datos

Para implementar Secure Network Analytics con un almacén de datos, revise los siguientes requisitos y recomendaciones.

Requisitos del appliance (con almacén de datos)

La siguiente tabla proporciona una descripción general de los appliances necesarios para implementar Secure Network Analytics con un almacén de datos.

Appliance	Requisito
Administrador	• Mínimo 1 Administrador
Almacén de datos	• Mínimo 1 o 3 nodos de datos • Conjuntos adicionales de 3 nodos de datos para ampliar el almacén de datos, máximo de 36 nodos de datos • Implementar solo 2 nodos de datos en un clúster no es compatible.
Recopilador de flujo	• Mínimo de 1 recopilador de flujo
UDP Director	Opcional
Sensor de flujo	Opcional

⚠ No actualice la BIOS del appliance, ya que puede provocar problemas con la funcionalidad del appliance.

Requisitos de implementación del administrador y recopilador de flujo

Por cada Administrador y recopilador de flujo que implemente, asignará una dirección IP enrutable al puerto de gestión `eth0`.

- **Configuración del puerto eth0:** puede configurar el uso de un puerto de 1 G/10 G de cobre **BASE-T** o un puerto de 10 G de cable twinaxial SFP+ para el puerto de

gestión `eth0` del Administrador y el recopilador de flujo.

- **Rendimiento:** se requiere un rendimiento de 10 G en el puerto de cobre BASE-T para el uso del almacén de datos. Si no está implementando un almacén de datos, solo puede configurar la interfaz de cobre de 100 Mbps/1 Gbps/10 Gbps como `eth0`.

Requisitos para la implementación del nodo de datos

Los almacenes de datos constan de nodos de datos.

- **Hardware:** cada nodo de datos de hardware es su propio chasis. Cuando compra un almacén de datos de hardware, recibe varios chasis de hardware de nodos de datos, correspondientes a la cantidad de nodos indicados por ese modelo de almacén de datos. Por ejemplo, un almacén de datos DS 6200 proporciona 3 chasis de hardware de nodos de datos.
- **Edición virtual:** cuando descarga un almacén de datos virtual, puede implementar 1, 3 o más nodos de datos de la edición virtual (en grupos de 3).

> Compruebe que sus nodos de datos sean todos de hardware o de edición virtual. No se admite la combinación de nodos de datos virtuales y hardware y el hardware debe ser de la misma generación de hardware (todos DS 6200 o todos DN 6300).

Implementación de varios nodos de datos

Una implementación de varios nodos de datos proporciona los máximos resultados de rendimiento. Por ejemplo, un almacén de datos 6200 con 3 nodos de datos puede gestionar aproximadamente 1 000 000 de flujos por segundo y conservar esos datos durante unos 90 días.

Tenga en cuenta lo siguiente:

- **Grupos de tres:** los nodos de datos se pueden agrupar como parte de su almacén de datos de 3 en 3, desde un mínimo de 3 hasta un máximo de 36. Implementar solo 2 nodos de datos en un clúster no es compatible.
- **Todo hardware o todo virtual:** sus nodos de datos deben ser todos de hardware o de edición virtual. No se admite la combinación de nodos de datos virtuales y de hardware ni la combinación de nodos de datos de almacenes de datos 6200 y 6300.

Implementación de un único nodo de datos

Si elige implementar un único (1) nodo de datos:

- **Recopiladores de flujo:** se admite un máximo de 4 Recopilador de flujo.
- **Agregar nodos de datos:** si implementa solo un nodo de datos, puede agregar nodos de datos a su implementación en el futuro. Consulte **Implementación de varios nodos de datos** para obtener más información.

> Estas recomendaciones solo tienen en cuenta la telemetría. Su rendimiento puede variar en función de otros factores, como el recuento de hosts, el uso del sensor de flujo, los perfiles de tráfico y otras características de la red. Póngase en contacto con el soporte de Cisco para obtener ayuda con el tamaño.

> Actualmente, el almacén de datos no admite la implementación de nodos de datos de repuesto como reemplazos automáticos si un nodo de datos principal deja de funcionar. Póngase en contacto con el soporte de Cisco para obtener asesoramiento.

Requisitos para configurar un nodo de datos

Para implementar un almacén de datos, asigne lo siguiente a cada nodo de datos. La información que prepare se aplicará en la configuración inicial mediante la Guía de configuración del sistema.

- **Dirección IP enrutable (eth0):** para la administración, ingesta y comunicación de consultas con sus dispositivos Secure Network Analytics.
- **Configuración del puerto eth0:** puede configurar el uso de un puerto de 1 G/10 G de cobre **BASE-T** o un puerto de 10 G de cable twinaxial SFP+ para el puerto de gestión `eth0`.
- **Rendimiento:** se requiere un rendimiento de 10 G en el puerto de cobre BASE-T para el uso del almacén de datos.
- **Comunicaciones entre nodos de datos:** configure una dirección IP no enrutable desde el bloque CIDR `169.254.42.0/24` dentro de una LAN o VLAN privada que se utilizará para la comunicación entre nodos de datos.

  Para un mejor rendimiento, conecte el puerto `eth2` del nodo de datos (o el canal de puerto que contenga `eth2` y `eth3`) a los conmutadores para la comunicación entre nodos de datos. Como parte del almacén de datos, sus nodos de datos se comunican entre sí.

- **Conexiones de red:** necesita dos conexiones de red 10 G, una para las comunicaciones de gestión, ingesta y consulta, y otra para las comunicaciones entre nodos de datos
- **Conexión y conmutador adicional:** opcionalmente, solo en los nodos de datos de hardware, para la redundancia de red y la importancia de las comunicaciones entre nodos de datos, instale una conexión 10 G adicional y un switch adicional para establecer un canal de puerto en el nodo de datos.

> Configure sus nodos de datos para que los nodos de datos de números adyacentes se alimenten con fuentes de alimentación redundantes e independientes. Esta configuración mejora la redundancia de datos y el tiempo de actividad general del almacén de datos.

Consideraciones de red y switching

La tabla siguiente proporciona una descripción general de las consideraciones de red y switching al implementar Secure Network Analytics con un almacén de datos.

Consideraciones sobre la red	Descripción
Comunicaciones entre nodos de datos	• Establezca una latencia de tiempo de ida y vuelta (RTT) recomendada inferior a 200 microsegundos entre los nodos de datos • Mantenga una diferencia del reloj de 1 segundo o menos entre sus nodos de datos. • Establezca un rendimiento recomendado de 6,4 Gbps o mayor (conexión conmutada de dúplex completo de 10 Gbps) entre sus nodos de datos. • En los nodos de datos de hardware, configurar un puerto `eth2` para un rendimiento de 10 G es suficiente para una comunicación normal entre nodos de datos. La creación de un canal de puerto `eth2/eth3` LACP vinculado para un rendimiento de hasta 20 G permite una comunicación más rápida entre los nodos de datos y una adición o sustitución más rápida de los nodos de datos en el almacén de datos, ya que cada nuevo nodo de datos recibe tráfico de los nodos de datos adyacentes para rellenar sus datos. Tenga en cuenta que la vinculación de puertos LACP es la única

	opción de vinculación disponible para los nodos de datos de hardware.
Alimentación del hardware de los nodos de datos	• Si un nodo de datos de hardware pierde la alimentación inesperadamente, los datos pueden dañarse. Utilice ambas fuentes de alimentación en circuitos separados de fuentes de alimentación ininterrumpidas. • Cuando inicie el clúster del almacén de datos, alterne la configuración de los nodos de datos según las fuentes de alimentación que utiliza cada nodo de datos. Esto puede optimizar la tolerancia a fallos minimizando el número de nodos de datos que se caen si se pierde la alimentación.
Conmutación de nodos de datos	• Los nodos de datos necesitan sus propias VLAN de capa 2 para permitir la comunicación entre nodos de datos. Los nodos de datos de hardware se pueden conectar a un switch 10G compartido o específico. • Recomendamos que los nodos de datos de hardware se conecten a 2 switches para garantizar una conectividad constante durante las interrupciones de alimentación y actualizaciones del switch. Debido a la baja latencia necesaria para la comunicación entre nodos de datos, Cisco recomienda un par de switches redundantes, en el que los 2 switches estén interconectados y transporten la VLAN de capa 2 a través de ambos switches.
Secure Network Analytics Comunicaciones de appliances	• Administrador y los recopiladores de flujo deben poder alcanzar todos los nodos de datos • Los nodos de datos deben poder alcanzar el Administrador, todos los recopiladores de flujo y cada nodo de datos

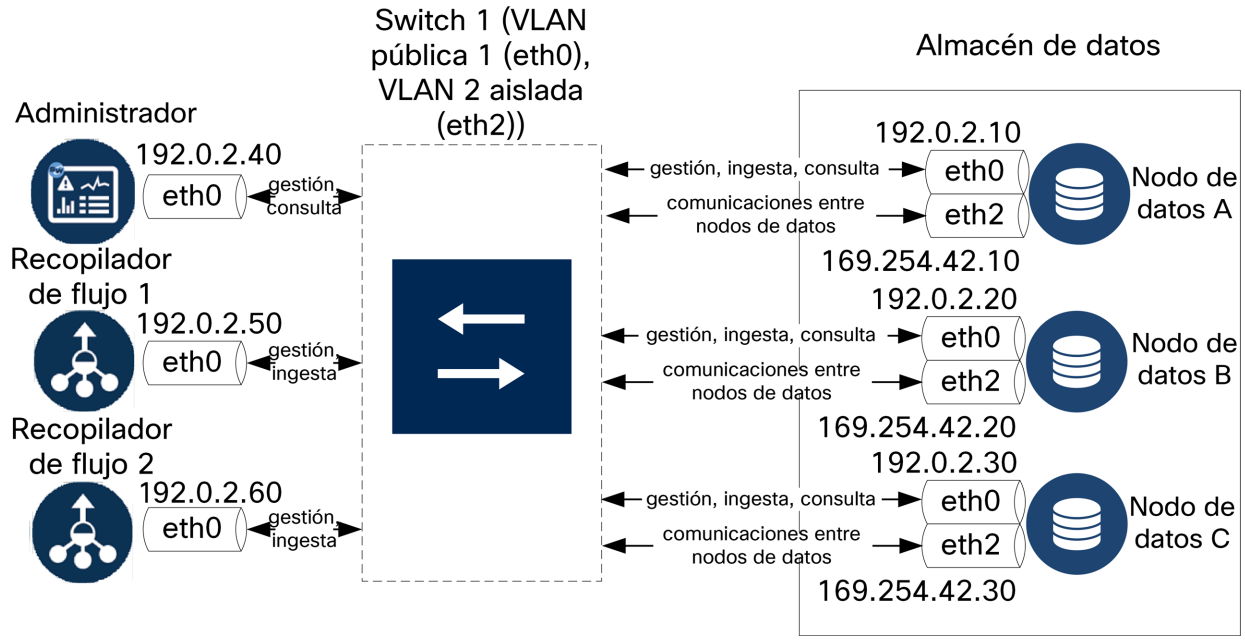
Actualmente, el almacén de datos no admite la implementación de nodos de datos de repuesto como reemplazos automáticos si un nodo de datos principal deja de funcionar. Póngase en contacto con el soporte de Cisco para obtener asesoramiento.

Ejemplo de conmutador de hardware

Para activar las comunicaciones entre nodos de datos a través de `eth2` o el canal de puerto `eth2/eth3`, implemente 1 switch que admita velocidades de 10G.

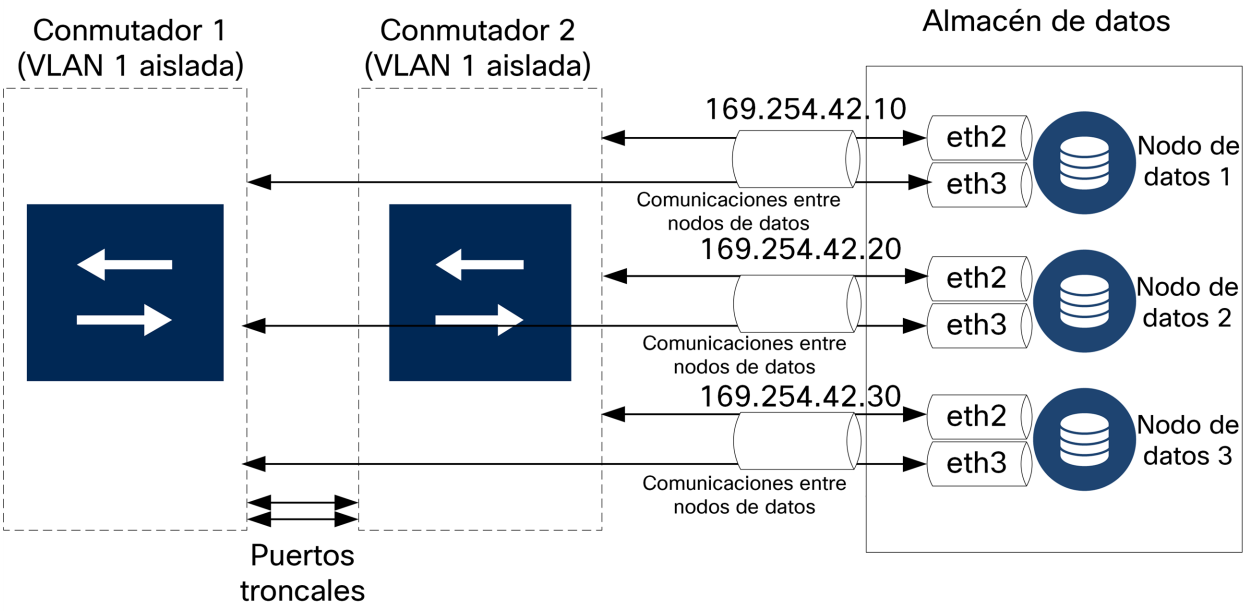
Configure una LAN o VLAN para las comunicaciones `eth0` de nodos de datos con el Administrador y los recopiladores de flujo, así como una LAN o VLAN aislada para las comunicaciones entre nodos de datos.

Puede compartir estos switches con otros appliances, pero cree LAN o VLAN independientes para el tráfico adicional del appliance. Vea el siguiente diagrama de ejemplo:



El clúster del almacén de datos requiere un latido continuo entre los nodos dentro de la VLAN aislada. Sin este latido, los nodos de datos podrían desconectarse, lo que aumenta el riesgo de que el almacén de datos se desconecte.

Si desea redundancia de red adicional, para planificar las actualizaciones del switch y la interrupción de alimentación planificada, configure sus nodos de datos con canales de puerto para una comunicación específica entre nodos de datos. Conecte cada nodo de datos a 2 switches, con cada puerto físico conectado a un switch diferente. Vea el siguiente diagrama de ejemplo:



Póngase en contacto con los servicios profesionales de Cisco para obtener ayuda con la planificación de su implementación.

Consideraciones sobre la ubicación del almacén de datos

Coloque cada nodo de datos de manera que se pueda comunicar con todos sus recopiladores de flujo, su Administrador y el resto de los nodos de datos. Para obtener el mejor rendimiento, coloque sus nodos de datos y sus recopiladores de flujo para minimizar la latencia de comunicación, y coloque sus nodos de datos y Administrador para un rendimiento óptimo de las consultas.

- **Firewall:** recomendamos encarecidamente colocar los nodos de datos en el firewall, como en un NOC.
- **Alimentación:** si el almacén de datos deja de funcionar debido a una pérdida de alimentación o a un fallo de hardware, corre un mayor riesgo de daño y pérdida de los datos. Instale los nodos de datos teniendo en cuenta el tiempo de actividad constante.

Si un nodo de datos pierde energía inesperadamente y reinicia el appliance, la instancia de base de datos de ese nodo de datos no se reiniciará automáticamente. Consulte la Guía de configuración del sistema para solucionar problemas y reiniciar manualmente la base de datos.

- **Política:** compruebe que haya una política de restauración de energía del nodo de datos de hardware establecida en **Restaurar último estado**, que reinicia el nodo de datos automáticamente tras la pérdida de energía e intenta restaurar los procesos en ejecución. Consulte la Guía de configuración de la GUI del UCS Serie C para obtener más información sobre la configuración de la política de restauración de energía en CIMC.

Requisitos del despliegue de análisis

Secure Network Analytics utiliza el modelado dinámico de entidades para rastrear el estado de su red. En el contexto de Secure Network Analytics, una entidad es algo que se puede rastrear en el tiempo, como un host o terminal en su red. El modelado dinámico de entidades recopila información sobre las entidades en función del tráfico que transmiten y las actividades que realizan en su red. Para obtener más información, consulte la Guía de análisis: detecciones, alertas y observaciones.

Para habilitar los análisis, su despliegue debe configurarse

- en un despliegue de almacén de datos virtual o de hardware con cualquier número de recopiladores de flujo.
- con solo 1 dominio de almacén de datos Secure Network Analytics.

1. Configuración del firewall para las comunicaciones

Para que los appliances se puedan comunicar de forma correcta, debe configurar la red de forma que los firewall o las listas de control de acceso no bloqueen las conexiones requeridas. Utilice la información que se proporciona en esta sección para configurar su red de forma que los appliances puedan comunicarse a través de la red.

Puertos abiertos (todos los appliances)

Póngase en contacto con el administrador de su red para garantizar que los siguientes puertos están abiertos y no tienen acceso restringido en sus appliances (Administrador, recopiladores de flujos, nodos de datos, sensores de flujo y UDP Directors):

- TCP 22
- TCP 25
- TCP 389
- TCP 443
- TCP 2393
- TCP 8910
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 389
- UDP 514
- UDP 2055
- UDP 6343

Puertos abiertos adicionales para nodos de datos

Además, si implementa nodos de datos en su red, asegúrese de que los siguientes puertos están abiertos y cuentan con acceso sin restricciones:

- TCP 5433
- TCP 5444
- TCP 9450

Puertos de comunicación y protocolos

La siguiente tabla muestra cómo se utilizan los puertos en Secure Network Analytics:

De (cliente)	A (servidor)	Puerto	Protocolo
PC del usuario administrador	Todos los appliances	TCP/443	HTTPS
Todos los appliances	Fuente de tiempo de red	UDP/123	NTP
Active Directory	Administrador	TCP/389, UDP/389	LDAP
Cisco ISE	Administrador	TCP/443	HTTPS
Cisco ISE	Administrador	TCP/8910	XMPP
Fuentes de registro externo	Administrador	UDP/514	SYSLOG
Recopilador de flujo	Administrador	TCP/443	HTTPS
UDP Director	Administrador	TCP/443	HTTPS
UDP Director	Recopilador de flujo (sFlow)	UDP/6343*	sFlow
UDP Director	Recopilador de flujo (NetFlow)	UDP/2055*	NetFlow
UDP Director	Sistemas de gestión de eventos de terceros	UDP/514	SYSLOG
Sensor de flujo	Administrador	TCP/443	HTTPS
Sensor de flujo	Recopilador de flujo (NetFlow)	UDP/2055	NetFlow
Exportadores de NetFlow	Recopilador de flujo (NetFlow)	UDP/2055*	NetFlow
Exportadores de sFlow	Recopilador de flujo (sFlow)	UDP/6343*	sFlow

De (cliente)	A (servidor)	Puerto	Protocolo
Administrador	UDP Director	TCP/443	HTTPS
Administrador	Cisco ISE	TCP/443	HTTPS
Administrador	Cisco ISE	TCP/8910	XMPP
Administrador	DNS	UDP/53	DNS
Administrador	Recopilador de flujo	TCP/443	HTTPS
Administrador	Sensor de flujo	TCP/443	HTTPS
Administrador	Exportadores de flujo	UDP/161	SNMP
Administrador	LDAP	TCP/636	TLS
Administrador	Puntos de distribución de CRL	TCP/80	HTTP
Administrador	Respondedores OCSP	TCP/80	OCSP
PC del usuario	Administrador	TCP/443	HTTPS

*Este es el puerto predeterminado pero cualquier puerto UDP se puede configurar en el exportador.

Puertos abiertos adicionales para el almacén de datos

A continuación se enumeran los puertos de comunicación que deben abrirse en el firewall para implementar el almacén de datos.

N.º	**De (cliente)**	**A (servidor)**	**Puerto**	**Protocolo o propósito**
1	Administrador	Recopiladores de flujo y nodos de datos	22/TCP	Se necesita SSH para inicializar la base de datos del almacén de datos
1	Nodos de datos	Todos los demás nodos de datos	22/TCP	Se necesita SSH para inicializar la base de datos del almacén de datos y para las tareas de administración de la base de datos
2	Administrador Recopiladores de flujo y nodos de datos	Servidor NTP	123/UDP	Se necesita NTP para la sincronización horaria
2	Servidor NTP	Administrador Recopiladores de flujo y nodos de datos	123/UDP	Se necesita NTP para la sincronización horaria
3	Administrador	Recopiladores de flujo y nodos de datos	443/TCP	Se necesita HTTPS para una comunicación segura entre los dispositivos
3	Recopiladores de flujo	Administrador	443/TCP	Se necesita HTTPS para una comunicación segura entre los dispositivos
3	Nodos de datos	Administrador	443/TCP	Se necesita HTTPS para una comunicación segura entre los dispositivos

4	Exportadores de NetFlow	Recopiladores de flujo: NetFlow	2055/UDP	Ingestión de NetFlow
5	Nodos de datos	Todos los demás nodos de datos	4803/TCP	Servicio de mensajería entre nodos de datos
6	Nodo de datos	Todos los demás nodos de datos	4803/UDP	Servicio de mensajería entre nodos de datos
7	Nodos de datos	Todos los demás nodos de datos	4804/UDP	Servicio de mensajería entre nodos de datos
8	Administrador Recopiladores de flujo y nodos de datos	Nodos de datos	5433/TCP	Conexiones de cliente de Vertica
9	Nodo de datos	Todos los demás nodos de datos	5433/UDP	Supervisión del servicio de mensajería de Vertica
10	Exportadores de sFlow	Recopilador de flujo (sFlow)	6343/UDP	Ingestión de sFlow
11	Nodos de datos	Todos los demás nodos de datos	6543/UDP	Servicio de mensajería entre nodos de datos

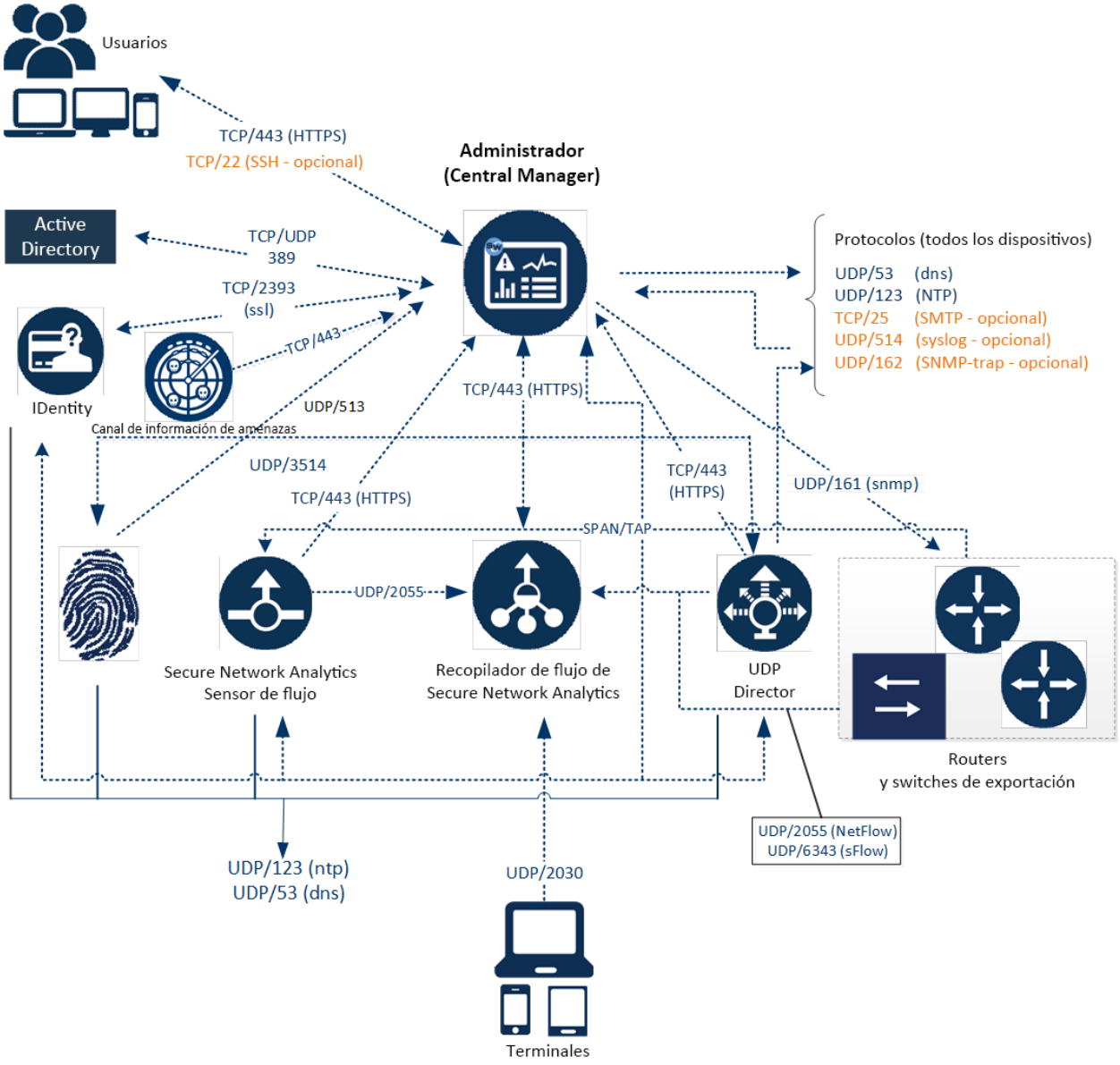
Puertos de comunicación opcionales

La siguiente tabla es para configuraciones opcionales determinadas por sus necesidades de red:

De (cliente)	A (servidor)	Puerto	Protocolo
Todos los dispositivos	PC del usuario	TCP/22	SSH
Administrador	Sistemas de gestión de eventos de terceros	UDP/162	SNMP-trap
Administrador	Sistemas de gestión de eventos de terceros	UDP/514	SYSLOG
Administrador	Gateway de correo electrónico	TCP/25	SMTP
Administrador	Canal de información de amenazas	TCP/443	SSL
PC del usuario	Todos los dispositivos	TCP/22	SSH

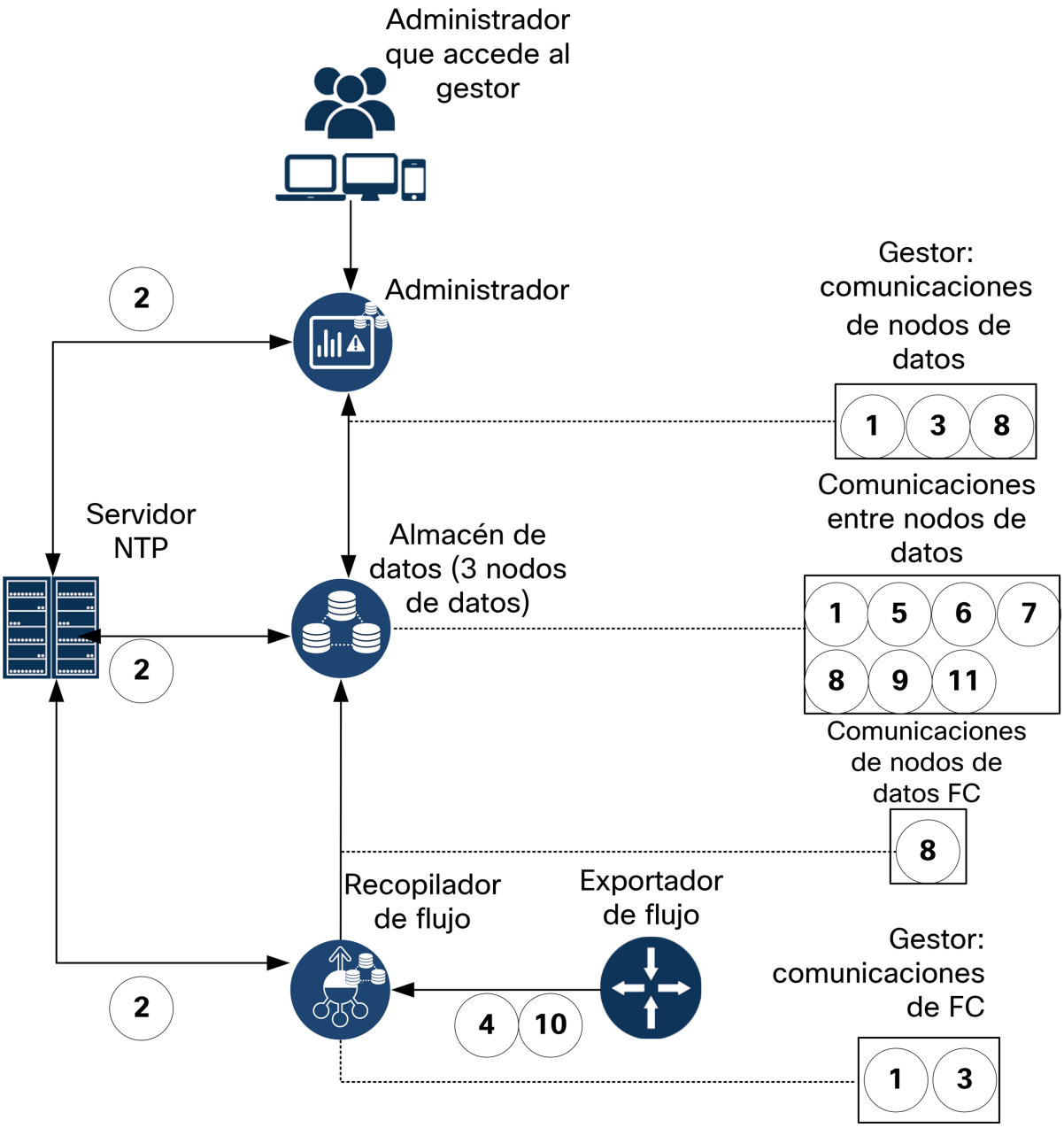
Secure Network Analytics Ejemplo de implementación

El siguiente diagrama muestra las distintas conexiones que Secure Network Analytics utiliza. Algunos de estos puertos son opcionales.



Secure Network Analytics Ejemplo de implementación con almacén de datos

Tal y como se muestra en la siguiente figura, puede implementar de forma estratégica los appliances de Secure Network Analytics para ofrecer una cobertura óptima de los segmentos de la red claves en la red, ya sea en la red interna, en el perímetro o en el DMZ.



2. Advertencias y pautas de instalación

Advertencias de instalación

Lea el documento Información de seguridad normativa y de cumplimiento antes de instalar los appliances de la serie Secure Network Analytics x2xx.

Tome nota de las siguientes advertencias:

Advertencia 1071: definición de advertencia

INSTRUCCIONES DE SEGURIDAD IMPORTANTES

Este símbolo de advertencia indica peligro. Se encuentra en una situación que podría causar lesiones corporales. Antes de manipular cualquier equipo, debe ser consciente de los peligros que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. Utilice el número de advertencia que aparece al final de cada una para localizar su traducción en las advertencias de seguridad que acompañan a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Advertencia 1004: instrucciones de instalación

Lea las instrucciones de instalación antes de usar, instalar o conectar el sistema a la fuente de alimentación.

Advertencia 1005: disyuntor del circuito

Este producto utiliza el sistema de protección contra cortocircuitos (sobretensión) instalado en el edificio.

Advertencia 1006: advertencia del chasis para montaje en rack y reparación

Para evitar daños físicos al montar o reparar esta unidad en un rack, debe prestar especial atención a que el sistema se mantenga estable. Le ofrecemos las siguientes directrices para garantizar su seguridad:
- Esta unidad debe montarse en la parte inferior del rack si es la única unidad del rack.
- Al montar esta unidad en un rack parcialmente completo, cargue el rack de

abajo a arriba con el componente más pesado en la parte inferior.
• Al montar esta unidad en un rack parcialmente completo, cargue el rack de abajo a arriba con el componente más pesado en la parte inferior.

Advertencia 1015: manejo de la batería

Para reducir el riesgo de incendio, explosión o fugas de líquidos o gases inflamables:
• Sustituya la batería únicamente por otra del mismo tipo o por una equivalente recomendada por el fabricante
• No desmonte, aplaste, perfore ni utilice herramientas afiladas para retirar o poner en corto los contactos externos, ni arroje la batería al fuego.
• No utilice la batería si está combada o hinchada.
• No almacene ni utilice la batería con una temperatura > 60 °C/140 °F.
• No almacene ni utilice la batería en un entorno de baja presión de aire < 69,7 kPa.

Advertencia 1017: área restringida

Esta unidad ha sido diseñada para ser instalada en áreas de acceso restringido. Solo el personal cualificado, capacitado o instruido puede acceder a un área de acceso restringido.

Advertencia 191: advertencia de clase A del Consejo de Control Voluntario de Interferencias (VCCI) para Japón

Este es un producto de Clase A basado en la norma del Consejo VCCI. Si este equipo se utiliza en un entorno doméstico, pueden producirse interferencias de radio, en cuyo caso es posible que deba tomar medidas correctivas.

Advertencia 164: requisito de izado

Se necesitan dos personas para levantar las piezas pesadas del producto. Para evitar lesiones, mantenga la espalda recta y levántelo con las piernas, no con la espalda.

Advertencia 256: advertencia de clase A para Hungría

Este equipo es un producto de clase A y debe utilizarse e instalarse correctamente de acuerdo con los requisitos de EMC de clase A de Hungría (MSZEN55022). Los equipos de clase A están diseñados para establecimientos comerciales típicos para los que se utilizan condiciones especiales de instalación y distancia de protección.

Advertencia 294: advertencia de clase A para Corea

Este es un dispositivo de clase A y está registrado según los requisitos de compatibilidad electromagnética (EMC) para uso industrial. El vendedor o comprador debe tenerlo en cuenta. Si se vendió o adquirió por error este tipo, debería sustituirse por un tipo de uso residencial.

Advertencia 340: advertencia de clase A para CISPR22/EN55022/CISPR32/EN55032

Este es un producto de clase A. En un entorno doméstico, este producto puede provocar interferencias de radio, en cuyo caso se requiere tomar las medidas adecuadas.

Advertencia 1021: circuito SELV

Con el fin de evitar descargas eléctricas, no conecte circuitos de voltaje muy bajo de seguridad (SELV) a los circuitos de voltaje de la red telefónica (TNV). Los puertos LAN contienen circuitos SELV, mientras que los puertos WAN tienen circuitos TNV. Algunos puertos, tanto LAN como WAN, utilizan conectores RJ-45. Tenga cuidado al conectar los cables.

Advertencia 1024: conductor de puesta a tierra

Este equipo debe conectarse a tierra. No desactive nunca el conductor de puesta a tierra ni utilice el equipo sin un conductor de puesta a tierra correctamente instalado. Póngase en contacto con la autoridad de inspección eléctrica pertinente o con un electricista si no está seguro de contar con una conexión a tierra apropiada.

Advertencia 1028: más de una fuente de energía

Esta unidad puede tener más de una conexión de fuente de energía. Para reducir el riesgo de descarga eléctrica, desconecte todas las conexiones para descargar la unidad.

Advertencia 1029: placas y paneles de cubierta ciegos

Las placas frontales y los paneles de cubierta ciegos desempeñan tres importantes funciones: reducen el riesgo de descarga eléctrica o incendio, contienen la interferencia electromagnética (EMI) que puede interrumpir el funcionamiento de otros equipos y dirigen el flujo de aire de refrigeración por el chasis. No ponga el sistema en funcionamiento a menos que todas las tarjetas, placas frontales, cubiertas delanteras y cubiertas traseras estén en su sitio.

Advertencia 1030: instalación del equipo

Solo se debe permitir a personal formado y cualificado que instale, sustituya o repare este equipo.

Advertencia 1032: elevación del chasis

Para evitar lesiones personales o daños en el chasis, nunca intente levantar o inclinar el chasis utilizando las asas de los módulos, como las fuentes de alimentación, los ventiladores o las tarjetas. Este tipo de tiradores no están diseñados para soportar el peso de la unidad.

Advertencia 9001: eliminación del producto

Al desechar este producto deben tenerse en cuenta todas las leyes y normativas nacionales.

Advertencia 1051: radiación láser

Los conectores o fibras desconectados pueden emitir radiación láser invisible. No mire fijamente los haces ni mire directamente con instrumentos ópticos.

Advertencia 1055: láser de clase 1/1M

La radiación por láser invisible está presente. No exponga a los usuarios de telescopios ópticos. Esto se aplica a los productos láser de clase 1 y 1M.

Advertencia 1008: producto láser de clase 1

Este producto es un producto láser de clase 1.

Advertencia 1056: cable de fibra sin terminal

Puede que se emita radiación láser invisible desde el final del cable de fibra o conector sin terminal. No lo mire directamente con instrumentos ópticos. Mirar la salida láser con determinados instrumentos ópticos (por ejemplo, lupas binoculares o de aumento y microscopios) a una distancia de 100 mm puede ser peligroso para los ojos.

Tipo de fibra y diámetro del núcleo (µm)	**Longitud de onda (nm)**	**Alimentación máxima (mW)**	**Beam Divergence (rad)**
SM 11	1200–1400	39–50	0,1–0,11
MM 62,5	1200–1400	150	0,18 NA
MM 50	1200–1400	135	0,17 NA
SM 11	1400–1600	112–145	0,11–0,13

Advertencia 1089: definiciones de persona instruida y capacitada

Una persona instruida es aquella persona que ha sido instruida y formada por una persona capacitada y que toma las precauciones necesarias a la hora de trabajar con el equipo.

Una persona capacitada o cualificada es aquella persona que posee formación o experiencia en la tecnología del equipo y que entiende los posibles riesgos a la hora de trabajar con el equipo.

Advertencia 1090: instalación por parte de una persona capacitada

Solo se debe permitir a una persona capacitada que instale, sustituya o repare este equipo. Consulte la advertencia 1089 para obtener la definición de persona capacitada.

Advertencia 1091: instalación por parte de una persona instruida

Solo se debe permitir a una persona instruida o capacitada que instale, sustituya o repare este equipo. Consulte la declaración 1089 para obtener la definición de persona capacitada o instruida.

Advertencia 1074: cumplimiento de los códigos eléctricos locales y nacionales

La instalación del equipo debe cumplir con los códigos eléctricos locales y nacionales.

Advertencia 2017: aviso sobre clase A de FCC

La modificación del equipo sin la autorización de Cisco puede derivar en que los equipos no cumplan los requisitos de la FCC para dispositivos digitales de clase A. En tal caso, su derecho a utilizar el equipo puede verse limitado por la normativa de la FCC y se podrá solicitar al usuario que corrija las posibles interferencias con las comunicaciones de radio o televisión a su cargo.
Este equipo ha superado satisfactoriamente las pruebas de cumplimiento de las especificaciones para dispositivos digitales de Clase A de acuerdo con la parte 15 de la normativa FCC. Estos límites están diseñados para proporcionar una protección razonable frente a cualquier interferencia perjudicial al utilizar el equipo en un entorno comercial. Este equipo genera, utiliza y puede emitir

energía de radiofrecuencia y, si no se instala y utiliza de acuerdo con el manual de instrucciones, puede provocar interferencias en las comunicaciones de radio. El funcionamiento de este equipo en una zona residencial puede provocar interferencias perjudiciales; en tal caso, se exigirá a los usuarios que corran con los gastos de la reparación de dichos daños.

Advertencia 2021: aviso sobre clase A para Canadá

Este aparato digital de clase A cumple con el estándar canadiense ICES-003/NMB-003.

Advertencia 7001: mitigación de ESD

Este equipo puede ser sensible a ESD. Utilice siempre una pulsera o tobillera antiestática antes de manipular el equipo. Conecte el extremo del equipo de la correa antiestática a una superficie inacabada del chasis del equipo o a la clavija ESD del equipo, si se proporciona.

Advertencia 7003: requisitos de cables protegidos contra sobretensión por rayos dentro de un edificio

Los puertos internos del equipo o subequipo deben utilizar un cableado interno protegido o cableado que esté conectado a tierra por ambos extremos.
Los siguientes puertos se consideran puertos internos en este equipo:

Advertencia 7005: fallo de alimentación de CA y sobretensión por rayos dentro del edificio

Los puertos internos del equipo o subequipo son aptos únicamente para la conexión a cableado interno o que no esté expuesto. Los puertos internos del equipo o subconjunto NO DEBEN estar conectados metálicamente a las interfaces que conectan con el OSP o su cableado a lo largo de más de 6 metros (aproximadamente 20 pies). Estas interfaces están diseñadas para usarse solo como interfaces internas (puertos tipo 2, 4 o 4a como se describe en GR-1089) y necesitan aislarse del cableado OSP expuesto. La incorporación de protectores principales no es protección suficiente para conectar metálicamente estas interfaces a un sistema de cableado OSP.
Los siguientes puertos se consideran puertos internos en el equipo:

Instrucciones de instalación

Tome nota de las siguientes advertencias:

> Advertencia 1047: prevención contra sobrecalentamiento
>
> Para evitar que el sistema se sobrecaliente, no lo utilice en una zona que supere la temperatura ambiente máxima recomendada de: 5 a 35 °C (41 a 95 °F).

> Advertencia 1019: dispositivo de desconexión principal
>
> La combinación de la caja de enchufe debe estar siempre accesible porque sirve como dispositivo principal de desconexión.

> Advertencia 1075: cable de alimentación y adaptador de CA
>
> Utilice los cables de conexión/cables de alimentación/adaptadores de corriente alterna/baterías proporcionados o designados cuando instale el producto. Usar cualquier otro cable o adaptador podría provocar un error o un incendio. La ley de seguridad de aparatos y materiales eléctricos prohíbe el uso de cables con la certificación UL (aquellos que lleven las marcas “UL” o “CSA” en el cable), que no estén sujetos a dicha ley y por la cual debe figurar “PSE” en el cable, en ningún dispositivo eléctrico que no sean los productos designados por CISCO.

> Advertencia 1073: ninguna pieza que el usuario pueda reparar
>
> Ninguna pieza interior del dispositivo puede ser reparada por el usuario. No abrir.

Cuando instale un chasis, utilice las siguientes directrices:

- Asegúrese de que haya un espacio adecuado alrededor del chasis para permitir el mantenimiento y un flujo de aire adecuado. El flujo de aire en el chasis va desde la parte frontal a la trasera.

> Para asegurar el flujo de aire adecuado es necesario asegurar su chasis con un kit de raíles. La colocación física de las unidades una encima de otra o el apilamiento sin el uso de los kits de raíles bloquea las ranuras de ventilación encima del chasis, lo que podría dar como resultado sobrecalentamiento, velocidades del ventilador más altas y un mayor consumo energético. Le recomendamos que monte su chasis en los kits de raíles cuando los instale en el

rack, ya que estos raíles ofrecen el espaciado mínimo necesario entre los chasis. No se necesita un espaciado adicional entre el chasis cuando los monte utilizando kits de raíles.

- Asegúrese de que el aire acondicionado pueda mantener el chasis a una temperatura de 5 a 35 °C (41 a 95 °F).
- Asegúrese de que el armario o rack cumpla con los requisitos del rack.
- Asegúrese de que la alimentación del sitio cumpla con los requisitos de alimentación que aparecen en la hoja de especificaciones de su appliance. Si está disponible, puede utilizar una UPS para protegerse frente a fallos de alimentación.

Evite las UPS que utilizan la tecnología ferrorresonante. Este tipo de UPS pueden volverse inestables con estos sistemas, que pueden tener importantes fluctuaciones de toma de corriente de patrones de trafico de datos fluctuantes.

Recomendaciones de seguridad

La siguiente información le ayuda a garantizar su seguridad y a proteger el chasis. Puede que esta información no sea aplicable a todas las situaciones potencialmente peligrosas de su entorno de trabajo, así que esté atento y siga siempre un buen criterio.

Tenga en cuenta estas directrices de seguridad:

- Mantenga el área limpia y sin polvo antes, durante y después de la instalación.
- Mantenga las herramientas fuera de las zonas de paso donde usted u otras personas podrían tropezarse.
- No lleve ropa holgada ni joyas como pendientes, pulseras o cadenas que puedan engancharse en el chasis.
- Utilice gafas de seguridad si trabaja en cualquier condición que pueda ser peligrosa para sus ojos.
- No realice ninguna acción que pueda resultar potencialmente peligrosa para las personas o que haga que el equipo no sea seguro.
- Nunca intente levantar un objeto demasiado pesado para una sola persona.

Mantener la seguridad con electricidad

Antes de trabajar en un chasis, asegúrese de que el cable de alimentación esté desconectado.

Siga estas directrices cuando trabaje con equipo eléctrico:

- No trabaje solo si hay condiciones potencialmente peligrosas en su espacio de trabajo.
- Nunca dé por hecho que la alimentación está desconectada; compruébelo siempre.
- Busque cuidadosamente posibles riesgos en su zona de trabajo como suelos húmedos, cables de alimentación de prolongación sin conexión a tierra, cables de alimentación desgastados y la falta de conexiones a tierra de seguridad.
- Si se produce un accidente eléctrico:
    - Tenga precaución, no se perjudique a usted mismo.
    - Desconecte la alimentación del sistema.
    - Si es posible, envíe a otra persona para conseguir asistencia médica. Si no, evalúe el estado de la víctima y, a continuación, pida ayuda.
    - Determine si el accidentado necesita respiración boca a boca o masaje cardíaco y, a continuación, realice la acción apropiada.
- Utilice el chasis según las especificaciones eléctricas y las instrucciones de uso del producto.

Evitar daños por ESD

La ESD se produce cuando se manejan de manera incorrecta los componentes electrónicos y puede dañar el equipo y afectar al circuito eléctrico, lo que puede dar lugar a un fallo intermitente o completo de su equipo.

Siga siempre los procedimientos de prevención de ESD cuando retire y sustituya componentes. Asegúrese de que el chasis esté eléctricamente conectado a tierra. Utilice una correa para la muñeca antiestática y asegúrese de que esté en contacto con su piel. Conecte la pinza de toma a tierra a una zona sin pintura del marco del chasis para conectar a tierra de forma segura los voltajes de ESD. Para protegerse de manera adecuada frente a daños y descargas causadas por ESD, tanto la correa para la muñeca como el cable deben funcionar correctamente. Si no hay una correa de muñeca disponible, establezca una conexión a tierra usted mismo tocando una parte metálica del chasis.

Por su seguridad, compruebe periódicamente el valor de resistencia de la correa antiestática, que debe estar entre 1 y 10 megaohmios.

Entorno del sitio

Para evitar fallos en el equipo y reducir la posibilidad de que se apague por el entorno, planifique el diseño del sitio y la ubicación del equipo con cuidado. Si su equipo actual se apaga o experimenta tasas de error inusualmente altas, estas consideraciones pueden ayudarle a aislar la causa de los fallos y evitar futuros problemas.

Consideraciones de la fuente de alimentación

Al instalar el chasis, tenga en cuenta lo siguiente:

- Compruebe la alimentación en el sitio antes de instalar el chasis para garantizar que no tenga picos ni ruido. Instale un acondicionador de potencia si es necesario para asegurarse de utilizar niveles de tensión y potencia adecuados en la tensión de entrada del appliance.
- Instale una conexión a tierra adecuada para el sitio para evitar daños por rayos y subidas de potencia.
- El chasis no cuenta con un rango de funcionamiento seleccionable por el usuario. Consulte la etiqueta del chasis para conocer los requisitos de potencia de entrada correctos del appliance.
- Hay disponibles varios tipos de cables de alimentación de entrada de CA para el appliance; asegúrese de utilizar el adecuado para su sitio.
- Si utiliza fuentes de alimentación redundantes (1+1) dobles, le recomendamos que use circuitos eléctricos independientes para cada fuente de alimentación.
- Instale una fuente de alimentación continua para su sitio si es posible.

Consideraciones sobre la configuración en rack

Tenga en cuenta lo siguiente durante la planificación de la configuración en rack:

- Si monta un chasis en un rack abierto, asegúrese de que el marco del rack no bloquee los puertos de entrada o salida.
- Asegúrese de que los racks encerrados dispongan de una ventilación adecuada. Asegúrese de que el rack no se congestione excesivamente, puesto que cada chasis genera calor. Un rack encerrado debe tener laterales de ventilación y un ventilador que proporcione aire de refrigeración.
- En un rack encerrado con un ventilador en la parte superior, el calor generado por el equipo que está cerca de la parte inferior del rack puede dirigirse hacia arriba y por los puertos de entrada del equipo de encima en el rack. Asegúrese de que se proporcione una ventilación adecuada al equipo de la parte inferior del rack.
- Los deflectores pueden ayudar a aislar el aire de salida del aire de entrada, lo cual también ayuda a guiar el aire de refrigeración en su paso por el chasis. La mejor ubicación de los deflectores depende de los patrones del flujo de aire en el rack. Pruebe diferentes disposiciones para colocar los deflectores de forma eficaz.

3. Montaje de los appliances

Puede montar appliances de Secure Network Analytics directamente en un rack o armario estándar de 19", cualquier otro armario adecuado o en una superficie plana. Al montar un appliance en un rack o en un armario, siga las instrucciones que se incluyen en los kits de montaje en raíles. Al determinar dónde colocar un appliance, asegúrese de que la separación en los paneles frontales y traseros sea la siguiente:

- Los indicadores del panel frontal se pueden leer con facilidad
- El acceso a los puertos en el panel trasero es suficiente para conectar el cableado sin restricciones
- La entrada de alimentación del panel trasero está al alcance de una fuente de alimentación de CA acondicionada.
- El flujo de aire en torno al appliance y a través de los orificios de ventilación no se encuentra obstaculizado.

Hardware incluido en el appliance

El siguiente hardware se incluye en appliances de Secure Network Analytics:

- Cable de alimentación de CA
- Llaves de acceso (para la placa frontal)
- Kit de raíles para el montaje en rack o agarraderas de montaje para appliances más pequeños
- Un cable SFP de 10 GB para el recopilador de flujo 5210

Hardware adicional necesario

Debe proporcionar el siguiente hardware adicional necesario:

- Tornillo de montaje para un rack estándar de 19"
- Fuente de alimentación ininterrumpida (UPS) para cada appliance que instale
- Para configurar de forma local (opcional), utilice uno de los siguientes métodos:
    - Un ordenador portátil con un cable de vídeo y un cable USB (para el teclado)
    - Un monitor de vídeo con un cable de vídeo y un teclado con un cable USB

4. Conectar sus appliances a la red

Utilice el mismo procedimiento para conectar cada appliance a la red. La única diferencia para la conexión es el tipo de appliance que tiene.

1. Revisar las especificaciones

Utilice el mismo procedimiento para conectar cada appliance a la red. La única diferencia para la conexión es el tipo de appliance que tiene.

- **Hojas de especificaciones:** para obtener información detallada sobre las especificaciones de cada appliance, consulte las Secure Network Analytics Hojas de especificaciones.
- **Plataforma de UCS:** todo el hardware de Cisco x2xx utiliza la misma plataforma de UCS, UCSC-C220-M5SX, excepto en el caso del recopilador de flujo de 5120 DB, que utiliza UCSC-C240-M5SX. Las variaciones en los appliances se encuentran en las tarjetas NIC, el procesador, la memoria, el almacenamiento y RAID.
- **Administrador 2210:** si está implementando un almacén de datos, puede configurar un Administrador 2210 con una interfaz SFP+ DAC de 10 Gbps como eth0 para aumentar el rendimiento. Si no está implementando un almacén de datos, solo puede configurar la interfaz de cobre de 100 Mbps/1 Gbps/10 Gbps como eth0.
- **Recopilador de flujo 4210:** si está implementando un almacén de datos, puede configurar un colector de flujo 4210 con una interfaz SFP+ DAC de 10 Gbps como eth0 para aumentar el rendimiento. Si no está implementando un almacén de datos, solo puede configurar la interfaz de cobre de 100 Mbps/1 Gbps/10 Gbps como eth0.
- **Recopilador de flujo 5210:** el recopilador de flujo 5210 consta de dos servidores conectados (base de datos y motor) para que funcionen como un solo appliance. Por este motivo, la instalación cambia ligeramente respecto a otros appliances. En primer lugar, conéctelos directamente mediante un cable cruzado de 10 G SFP+ de conexión directa. A continuación, conéctese a la red.

  Cuando configure su sistema, asegúrese de configurar la base de datos y el motor en el orden especificado en la Guía de configuración del sistema.

> ⚠ No actualice la BIOS del appliance, ya que puede provocar problemas con la funcionalidad del appliance.

2. Conectar su appliance a la red

Para conectar su appliance a su red:

1. Conecte un cable de Ethernet al puerto de gestión, en la parte trasera del appliance.
2. Conecte al menos un puerto de supervisión para el sensor de flujo y los UDP Director.

    - **Alta disponibilidad de UDP Director:** conecte los dos UDP Director mediante cables cruzados. Conecte el puerto eth2 de un UDP Director al puerto eth2 del segundo UDP Director. De manera similar, conecte el puerto de eth3 de cada UDP Director con un segundo cable cruzado. Puede ser el cable de fibra o de cobre.
    - **Etiqueta de Ethernet:** compruebe que tiene la etiqueta de Ethernet (eth2, eth3, etc.) para cada puerto. Estas etiquetas corresponden a las interfaces de red (eth2, eth3, etc.) que se utilizan en la configuración del sistema.

3. Conecte el otro extremo de los cables Ethernet a su switch de red.
4. Conecte los cables de alimentación a la fuente de alimentación. Algunos appliances tienen dos conexiones de alimentación: fuente de alimentación 1 y fuente de alimentación 2.

5. Conectarse a su appliance

En esta sección se describe cómo conectarse a su dispositivo para la configuración del sistema.

Elija su procedimiento de conexión:

- **Conexión con un teclado y un monitor**
- **Conexión con un cable de serie o una consola de serie**
- **Conexión con CIMC (obligatorio para el acceso remoto)** Para conectarse al appliance con acceso remoto, utilice este procedimiento.

Conexión con un teclado y un monitor

Para configurar la dirección IP de forma local, siga estos pasos:

1. Conecte el cable de alimentación al appliance.
2. Pulse el botón de alimentación para encender el appliance. Espere a que haya terminado de arrancar por completo. No interrumpa el proceso de arranque.

> Puede que tenga que quitar el panel frontal para que llegue la alimentación.
>
> Los ventiladores de la fuente de alimentación se conectan en algunos modelos cuando el sistema no está encendido. Compruebe que el LED en el panel frontal está encendido.
>
> Asegúrese de conectar el appliance a una fuente de alimentación ininterrumpida (UPS). La fuente de alimentación precisa alimentación o de lo contrario el sistema mostrará un error.

3. Conecte el teclado:
    - Si dispone de un teclado estándar, conéctelo al conector estándar de teclado.
    - Si dispone de un teclado USB, conéctelo a un conector USB.
4. Conecte el cable de vídeo al conector de vídeo. Aparecerá la indicación de inicio de sesión.
5. Vaya a **6. Configuración del sistema Cisco Secure Network Analytics**.

Conexión con un cable de serie o una consola de serie

También puede conectarse al appliance con cable o una consola de serie, como un ordenador portátil que tenga un emulador del terminal. Usamos un ordenador portátil como ejemplo en las instrucciones.

1. Conecte su ordenador portátil al appliance utilizando uno de los siguientes métodos:

    - Conecte un cable RS232 del conector de puertos en serie (DB8) en su ordenador portátil al puerto de consola en el appliance.
    - Conecte un cable cruzado del puerto Ethernet en su ordenador portátil al puerto de gestión en el appliance.

2. Conecte el cable de alimentación al appliance.
3. Pulse el botón de alimentación para encender el appliance. Espere a que haya terminado de arrancar por completo. No interrumpa el proceso de arranque.

    > Puede que tenga que quitar el panel frontal para que llegue la alimentación.
    >
    > Los ventiladores de la fuente de alimentación se conectan en algunos modelos cuando el sistema no está encendido. Compruebe que el LED en el panel frontal está encendido. Asegúrese de conectar el appliance a una fuente de alimentación ininterrumpida (UPS). La fuente de alimentación precisa alimentación o de lo contrario el sistema mostrará un error.

4. En el ordenador portátil, establezca una conexión con el appliance.

    Puede utilizar cualquier emulador del terminal para comunicarse con el appliance.

5. Aplique los siguientes ajustes:

    - BPS: 115200
    - Bits de datos: 8
    - Bit de parada: 1
    - Paridad: ninguna
    - Control de flujo: ninguno

Se muestran la pantalla y la indicación de inicio de sesión.

6. Vaya a **6. Configuración del sistema Cisco Secure Network Analytics**.

Conexión con CIMC (obligatorio para el acceso remoto)

El Cisco Integrated Management Controller (CIMC) habilita el acceso a la configuración del servidor y a una consola del servidor virtual; además, supervisa el estado del hardware. También utilizará el CIMC en la configuración del sistema Secure Network Analytics.

1. Siga las instrucciones de la Guía de configuración de la GUI del controlador de administración integrado CIMC de Cisco UCS de la serie C.
2. Inicie sesión en el CIMC como administrador y escriba la **password** en el campo Contraseña.
3. Cambie la contraseña predeterminada para proteger la seguridad de su red.
4. Vaya a **6. Configuración del sistema Cisco Secure Network Analytics**.

6. Configuración del sistema Secure Network Analytics

Si ha terminado de instalar sus appliances de edición virtual o de hardware, está listo para configurar Secure Network Analytics en un sistema administrado.

> ⚠ Para configurar Secure Network Analytics, siga las instrucciones de la Guía de configuración del sistema v7.4.2.x. Este paso es fundamental para la correcta configuración y comunicación de su sistema.
>
> Asegúrese de configurar sus appliances en el orden especificado en la Guía de configuración del sistema.

Requisitos para configurar el sistema

Debe tener acceso a la consola del dispositivo a través del CIMC.

Utilice la siguiente tabla para preparar la información necesaria para cada dispositivo.

Requisitos de configuración	Detalles	Appliance
Dirección IP	Asigne una dirección IP enrutable al puerto de administración `eth0`.	
Máscara de red		
Gateway		
Nombre de host	Se necesita un nombre de host único para cada appliance. No podemos configurar un appliance con el mismo nombre de host que otro. Todos los nombres de host del appliance deben cumplir los requisitos estándar de Internet para los hosts de Internet.	

Nombre de dominio	Se necesita un nombre de dominio completo para cada appliance. No podemos instalar un appliance con un dominio vacío.	
Servidores DNS	Servidor DNS interno para resolución de nombres	
Servidores NTP	Servidor de hora interno para la sincronización entre servidores. Se requiere al menos 1 servidor NTP para cada appliance. Elimine el servidor NTP 130.126.24.53 si está en su lista de servidores. Sabemos que este servidor es problemático y ya no es compatible con nuestra lista predeterminada de servidores NTP.	
Servidor de retransmisión de correo	Servidor de correo SMTP para enviar alertas y notificaciones	
Recopilador de flujo Puerto de exportación	Obligatorio solo para los recopiladores de flujo. Valor predeterminado de NetFlow: 2055	

Dirección IP no enrutable dentro de una LAN o VLAN privada (para comunicaciones entre nodos de datos)	Obligatorio solo para los nodos de datos. • Hardware eth2 o enlace de eth2 y eth3. La creación de un canal de puerto `eth2/eth3` LACP vinculado para un rendimiento de hasta 20 G permite una comunicación más rápida entre los nodos de datos y una adición o sustitución más rápida de los nodos de datos en el almacén de datos. Tenga en cuenta que la vinculación de puertos LACP es la única opción de vinculación disponible para los nodos de datos de hardware. • Eth1 virtual **Dirección IP:** puede utilizar la dirección IP proporcionada o introducir un valor que cumpla los siguientes requisitos para las comunicaciones entre nodos de datos. • **Dirección IP no enrutable** del **bloque CIDR 169.254.42.0/24**, entre 169.254.42.2 y 169.254.42.254. • **Primeros tres octetos:** 169.254.42 • **Subred**: / 24 • **Consecutivas:** para facilitar el mantenimiento, seleccione direcciones IP consecutivas (como 169.254.42.10, 169.254.42.11 y 169.254.42.12). **Máscara de red:** La máscara de red está codificada en 255.255.255.0 y no se puede modificar.	

Puerto de conexión de hardware eth0	Obligatorio solo para con appliances de Secure Network Analytics de hardware con almacén de datos: • Administrador 2210 • Recopilador de flujo 4210 • Nodos de datos Opciones de puerto de conexión de hardware eth0: • **SFP+**: SFP+: puerto de fibra 10G SFP+/DAC para eth0. • **BASE-T**: 100 Mbs/1 GbE/10 GbE Puerto de cobre BASE-T para eth0. BASE-T es el predeterminado.	

Ponerse en contacto con el servicio de asistencia

Si necesita soporte técnico, realice una de las siguientes acciones:

- Póngase en contacto con su partner de Cisco local
- Póngase en contacto con el soporte de Cisco
- Para abrir un caso en la página web: http://www.cisco.com/c/en/us/support/index.html
- Para abrir un caso por correo electrónico: tac@cisco.com
- Para obtener asistencia telefónica: 1-800-553-2447 (EE. UU.)
- Para consultar los números de soporte en todo el mundo: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Información de copyright

Historial de cambios

Versión del documento	Fecha de publicación	Descripción
1_0	27 de febrero de 2023	Versión inicial.
1_1	16 de marzo de 2023	Se ha corregido un problema en el capítulo Requisitos generales de la implementación.
1_2	27 de marzo de 2023	Se ha actualizado la tabla de puertos y protocolos de comunicación.
1_3	27 de marzo de 2023	Se ha corregido un error tipográfico.
1_4	29 de marzo de 2023	Se ha añadido información sobre la vinculación de puertos LACP.
1_5	7 de junio de 2023	Se ha actualizado la sección de instrucciones y advertencias de instalación.