Cisco Telemetry Broker

Guía de instalación y configuración del appliance de hardware 2.0.1

Índice

Introducción **5**

Descripción general 5

Matriz de compatibilidad con versiones de hardware y software 5

Público 5

Instalación de nodos de agente virtual 6

Terminología 6

Abreviaturas frecuentes 6

Conceptos y arquitectura **8**

Requisitos del despliegue **10**

Matriz de las versiones de hardware y software 10

Especificaciones 10

Cisco Integrated Management Controller (CIMC) 10

Migrar configuración a un nuevo sistema **11**

Copia de seguridad de las reglas de configuración de CTB 11

Restaurar las reglas de configuración de CTB 11

1. Configurar su firewall para las comunicaciones **13**

Puertos de comunicación abiertos 13

2. Advertencias y pautas de instalación **15**

Advertencias de instalación 15

Instrucciones de instalación 17

Recomendaciones de seguridad 19

Mantener la seguridad con electricidad 19

Evitar daños por ESD 20

Entorno del sitio 20

Consideraciones de la fuente de alimentación 21

Consideraciones sobre la configuración en rack 21

3. Montaje de sus appliances **22**

Hardware incluido en el appliance 22

Hardware adicional necesario 22
4. Conectar sus appliances a la red 23
1. Revise las especificaciones 23
2. Conecte su appliance a la red 23
Determine la configuración de red 24
Interfaces que pertenecen a la misma subred 26
Interfaces que pertenecen a diferentes subredes 26
5. Conectarse a su appliance 27
Conexión con un teclado y un monitor 27
Conexión con un cable de serie o una consola de serie 28
Conexión con CIMC (obligatorio para el acceso remoto) 29
6. Configuración de su sistema de Cisco Telemetry Broker 30
Requisitos del navegador 30
Requisitos para configurar el sistema 30
Instalar el nodo de agente 31
1. Iniciar sesión como usuario de instalación 31
2. Ejecute el comando sudo ctb-install --init 31
(Opcional) Cambiar un parámetro individual 32
Tabla Número de puerto - Asignación del nombre de la interfaz 34
3. Ejecute el comando sudo ctb-manage 35
4. Cerrar sesión 35
5. Configurar la interfaz de telemetría 35
Administrar clústeres de alta disponibilidad 37
VIP y enrutamiento 38
Administrar clústeres 38
Ver el estado actual del clúster 38
Ver la configuración actual del clúster 40
Habilitar y deshabilitar el modo de espera del nodo 40
Mover un VIP a un nodo específico 41
Finalizar la configuración de su sistema 42

Póngase en contacto con el servicio de asistencia 43
Historial de cambios 44

Introducción

Descripción general

Esta guía explica cómo instalar el Cisco Telemetry Broker TB2300. En esta guía, también se describe el montaje y la instalación del hardware de Cisco Telemetry Broker. Tenga en cuenta que Cisco Telemetry Broker a veces se referencia como CTB en este documento.

> ⚠ Antes de instalar el nodo de agente TB2300, lea el documento Información de seguridad reglamentaria y de conformidad.

Matriz de compatibilidad con versiones de hardware y software

Appliance	Plataforma	Gen.	v.2.0
Nodo de agente TB2300	UCSC-C220	M6	●

Utilice esta leyenda cuando lea la Matriz de compatibilidad con versiones de hardware y software.

Símbolo	Descripción
●	Funciona a plena capacidad en el hardware
o	Compatible, pero el rendimiento no es óptimo
x	No compatible

Público

Esta guía está diseñada para la persona responsable de la instalación del hardware de Cisco Telemetry Broker. 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 nodos de agente virtual

Si desea instalar nodos de agente virtual, siga las instrucciones de la Guía de despliegue y configuración del appliance virtual de Cisco Telemetry Broker.

Terminología

Esta guía a veces utiliza el término "**appliance**" para hacer referencia al nodo de agente TB2300.

Un "**clúster de alta disponibilidad**" es un grupo de nodos de agente administrados por un nodo de administrador.

Abreviaturas frecuentes

En esta guía, se incluyen las siguientes abreviaturas:

Abreviatura	Descripción
CIMC	Cisco Integrated Management Controller
DNS	Servicio/Servidor de nombres de dominio
FTP	Protocolo de transferencia de archivos
Gbps	Gigabits por segundo
GB	Gigabyte
HTTPS	Protocolo (seguro) de transferencia de hipertexto
Mbps	Megabits por segundo
NAT	Traducción de direcciones de red
NIC	Tarjeta de interfaz de red
NTP	Protocolo de tiempo de red
SNMP	Protocolo simple de administración de red
SPAN	Analizador de puerto de switch

Abreviatura	Descripción
SSH	Secure Shell
TAP	Puerto de acceso de prueba
UDPD	UDP Director
UPS	Fuente de alimentación ininterrumpida
URL	Localizador de recursos universal
VLAN	Red de área local virtual
VM	Máquina virtual

Conceptos y arquitectura

Cisco Telemetry Broker le permite introducir telemetría de red desde varias entradas, transformar el formato de la telemetría y reenviarla a uno o varios destinos. Consulte la siguiente tabla para ver algunos ejemplos.

> Actualmente, el único appliance de hardware que existe para Cisco Telemetry Broker es un nodo de agente (TB2300). Se debe emparejar con un nodo de VM Manager para su despliegue.
>
> Puede desplegar una combinación de nodos de agente virtuales y físicos, o bien puede desplegar solamente todos los nodos de agente virtuales o únicamente todos los nodos de agente físicos.
>
> No es necesario un orden de instalación para los nodos de agente, incluso si está desplegando una combinación de nodos de agente virtuales y físicos.

Puede introducir cualquiera de los siguientes tipos de telemetrías:	**Y reenviar esa telemetría a cualquiera de los siguientes destinos o a todos ellos:**
• Telemetría de red local, incluidos NetFlow, syslog e IPFIX • Entradas de telemetría basadas en la nube, como los registros de flujo de la nube privada virtual (VPC) de Amazon Web Services (AWS)	• Plataformas de análisis, como Secure Network Analytics o Secure Cloud Analytics • Plataformas de administración y automatización de redes, como Cisco DNA Center • Plataformas de gestión de información y eventos de seguridad (SIEM)

Para ello, se despliegan uno o varios nodos de Cisco Telemetry Broker, que introducen la telemetría y la envían a los destinos configurados.

De serie, Cisco Telemetry Broker admite las siguientes transformaciones:

Formato de datos introducidos	**Formato de datos reenviados**
Registros de flujo de VPC	IPFIX
Registros de flujo de Microsoft Network Security Group (NSG)	IPFIX
IPFIX, NetFlow v5, NetFlow v9	JSON (solo para destinos SCA)

Todos sus nodos de agente son administrados por un administrador de Cisco Telemetry Broker. Puede iniciar sesión en la interfaz web de este administrador y realizar varias tareas de configuración, incluida la administración de los nodos de agente, la configuración de las reglas de reenvío, la creación de usuarios y la revisión del panel de control para su uso.

Requisitos del despliegue

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 compatibilidad de versiones de hardware y software para obtener detalles sobre la compatibilidad. La matriz se documenta en el capítulo **Introducción** de esta guía.

Especificaciones

Descargue la hoja de especificaciones del nodo de agente TB2300 que quiere instalar.

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** 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.

Migrar configuración a un nuevo sistema

Complete los siguientes procesos para realizar una copia de seguridad y restaurar las reglas de configuración de CTB que estableció en el administrador de Cisco Telemetry Broker.

- Los clientes de UDPD pueden migrar su configuración actual de UDPD a Cisco Telemetry Broker. Para obtener más detalles, consulte la sección "Importar y exportar la configuración de UDP Director" en la Guía de usuario de Cisco Telemetry Broker.

Copia de seguridad de las reglas de configuración de CTB

Ejecute el siguiente comando en el nodo de administrador de CTB:

```
$ sudo ctb-backup-config -v -f ctb_config.json
```

Una vez finalizado este proceso, se realizará una copia de seguridad de las reglas de configuración en el archivo ~/.ctb_config.json, después de lo cual podrá copiar las reglas de configuración en otra ubicación.

- No se realiza una copia de seguridad de las reglas de registro de flujo de VPC/NSG, por lo que deberá volver a crear sus reglas de registro de flujo de VPC/NSG al migrar a un nuevo sistema.
- Puede realizar copias de seguridad y restaurar las reglas de configuración de CTB solo dentro de la misma versión. Si intenta hacerlo entre distintas versiones, el proceso puede fallar.

Restaurar las reglas de configuración de CTB

> ⚠ Debe ejecutar `ctb-restore-config` después de completar `ctb-install --init` en el nodo de administrador. Si crea manualmente una cuenta de inicio de sesión de GUI, se sobrescribirá con la información de cuenta de `ctb-restore-config`.

Siga estos pasos:

1. Cierre la sesión como un usuario de *instalación*.
2. Copie el archivo **ctb-config.json** de un sistema existente.
3. Inicie sesión en el nuevo sistema como *administrador*.

4. Ejecute el siguiente comando en el nodo de administrador de CTB:

   ```
   $ sudo ctb-restore-config -v -f ctb_config.json
   ```

   Las entradas que se añadan a Cisco Telemetry Broker debido a la restauración no se asignarán a ningún nodo o clúster. Deberá asignarlas según sea necesario.

1. Configurar su 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 de comunicación abiertos

La siguiente tabla proporciona detalles de todas las conexiones de red realizadas hacia y desde sus appliances de Cisco Telemetry Broker. Para asegurarse de que su red permite estas conexiones, necesita modificar los controles de acceso aplicables que tiene actualmente (por ejemplo, su firewall).

Cliente	Servidor	Puerto	Descripción
usuarios	nodos de agente y nodo de administrador	22/TCP	Acceso SSH a la consola
Administrador	internet externo	443/TCP	HTTPS para comunicaciones externas seguras, como Smart Licensing y Software Update
Administrador	servidor syslog del cliente	puerto definido por el cliente	Telemetría de Syslog para notificaciones de Cisco Telemetry Broker
Administrador	servidor SMTP del cliente	puerto definido por el cliente	Telemetría SMTP para notificaciones de Cisco Telemetry Broker
cada nodo de agente	Administrador	443/TCP	HTTPS para conexiones de administración seguras

cada nodo de agente	internet externo	443/TCP	HTTPS para recuperar los registros de flujo de VPC/NSG de los buckets de almacenamiento de AWS S3/Azure SAS, respectivamente. HTTPS para que el nodo de agente acceda de forma segura al servidor SCA y cargue archivos en el bucket S3 de SCA.
usuarios	Administrador	443/TCP	HTTPS para un acceso seguro a la interfaz web
nodos de agente y nodo de administrador	servidores DNS del cliente	53/UDP	Telemetría de DNS
cada nodo de agente de *hardware*	servidor NTP del cliente	123	Datos de NTP para la sincronización horaria

Además, debe abrir puertos basados tanto en el tipo de telemetría que se envía a un nodo de agente como en el tipo de telemetría que un nodo de agente envía a un destino. La siguiente tabla proporciona detalles sobre los puertos comunes para varios tipos de telemetría:

Puerto	**Descripción**
514/UDP	syslog
2055/UDP	NetFlow v5, NetFlow v9
4739/UDP	IPFIX
6343/UDP	sFlow

2. Advertencias y pautas de instalación

Advertencias de instalación

Lea el documento Información de seguridad normativa y de cumplimiento antes de instalar cualquier appliance de Cisco Telemetry Broker.

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 12: advertencia de desconexión de la fuente de alimentación

⚠ Antes de trabajar en un chasis o cerca de fuentes de alimentación, desconecte el cable de alimentación de las unidades de CA; desconecte la alimentación de las unidades de CC en el disyuntor de circuitos.

Advertencia 43: advertencia de retirada de joyas

⚠ Antes de comenzar a trabajar con el equipo conectado a las líneas de alimentación, quítese las joyas (incluidos anillos, collares y relojes). Los objetos metálicos se calientan cuando están conectados a una fuente de alimentación y a tierra, y pueden provocar quemaduras graves o que el objeto metálico se suelde a los terminales.

Advertencia 94: advertencia sobre la correa para la muñeca

Durante este procedimiento, utilice correas para la muñeca para evitar daños por descarga electrostática en la tarjeta. No toque directamente la placa base con la mano o cualquier herramienta metálica o podría electrocutarse.

Advertencia 1045: protección contra cortocircuitos

Este producto requiere protección contra cortocircuitos (sobretensión), que se suministra como parte de la instalación del edificio. Instale solo conforme a las normativas de cableado locales y nacionales.

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 1040: eliminación del producto

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

Advertencia 19: advertencia sobre alimentación de TN

El dispositivo ha sido diseñado para trabajar con sistemas de alimentación TN.

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 1005: disyuntor del circuito

Este producto utiliza el sistema de protección contra cortocircuitos (sobretensión) instalado en el edificio. Asegúrese de que el dispositivo de protección no sea superior a: EU: 250 V, 16 A (EE. UU.: 120, 15 A).

Advertencia 1074: cumplimiento de los códigos eléctricos locales y nacionales

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

Advertencia 371: 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 sus appliances

Puede montar appliances de Cisco Telemetry Broker 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 Cisco Telemetry Broker:

- 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

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 el nodo de agente TB2300 que está instalando
- 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

1. Revise las especificaciones

Utilice el mismo procedimiento para conectar cada nodo de agente TB2300 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, consulte las Hojas de especificaciones de Cisco Telemetry Broker.
- **Plataforma UCS:** el TB2300 de Cisco Telemetry Broker utiliza la plataforma UCS, UCSC-C225-M6SX.

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

2. Conecte su appliance a la red

Para conectar su appliance a su red:

1. Conecte un cable Ethernet al puerto de administración como se define en la hoja de especificaciones.
2. Conecte un cable Ethernet al puerto de telemetría como se define en la hoja de especificaciones.
    - Asegúrese de que el puerto de administración está conectado a la red de administración y de que el puerto de telemetría está conectado a la red de telemetría. Para obtener más información, consulte la siguiente sección, Determinar la configuración de red.
3. Conecte el otro extremo de los cables Ethernet a sus switches 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.

Determine la configuración de red

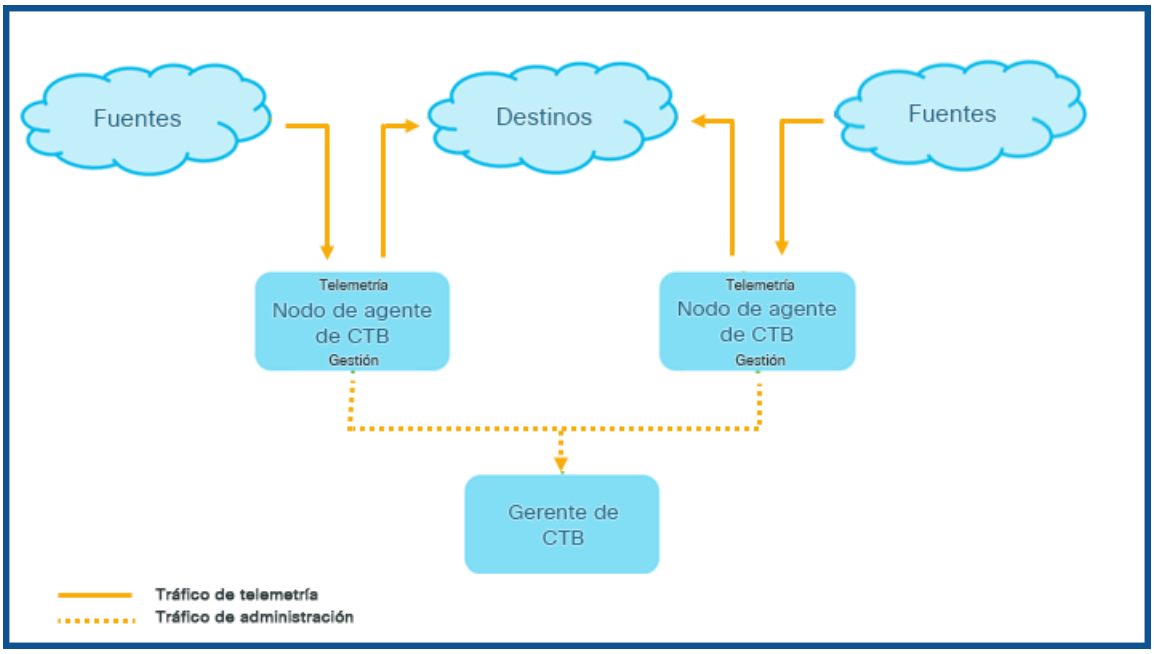
Cisco Telemetry Broker es compatible con configuraciones de varios nodos, en las que un único administrador de Cisco Telemetry Broker puede administrar varios nodos de agente. Dado que Cisco Telemetry Broker actualiza cada nodo de agente con todos los destinos y reglas, debe planificar cuidadosamente su configuración para evitar algunos problemas comunes, que se enumeran a continuación.

- Puede desplegar nodos de agente en diferentes segmentos de telemetría, donde las interfaces de telemetría de cada nodo de agente pueden no ser accesibles a través de la red. Es necesario elaborar reglas cuidadosamente para que los paquetes de un exportador que llegan a un nodo específico no se reenvíen a destinos que no son accesibles desde ese nodo. Para lograrlo, debe crear reglas que excluyan a los exportadores que puedan causar este problema de enrutamiento. Un ejemplo sería no utilizar ninguna regla predeterminada, ya que estas coincidirían con todas las entradas.
- Es posible que no todos los destinos sean relevantes para cada nodo de agente. Sin embargo, con la función Comprobar accesibilidad del destino, dado que cada nodo de agente intenta determinar la accesibilidad de cada destino, los nodos de agente podrían enviar información contradictoria al administrador. Si existe la posibilidad de que algunos nodos de agente no se puedan conectar con algunos destinos, desactive Comprobar accesibilidad del destino para esos destinos.

Si está migrando desde UDP Director a Cisco Telemetry Broker, antes de desplegar el nodo de administrador y los nodos de agente, debe planificar cómo conectará el nodo de administrador y los nodos de agente a la red, ya que existen diferencias entre cómo se configuran tanto Cisco Telemetry Broker, como UDP Director.

Cisco Telemetry Broker diferencia el tráfico de telemetría del tráfico de administración. El nodo de agente tiene dos interfaces: la interfaz de red de telemetría y la interfaz de red de administración. El nodo de administrador solo tiene la interfaz de red de administración. El siguiente diagrama muestra cómo desplegar lógicamente el nodo de administrador y los nodos de agente.

> Tenga en cuenta que los ejemplos de este tema representan situaciones de despliegue típicas. Para obtener información sobre cómo configurar un despliegue más avanzado (por ejemplo, uno que utilice VLAN), póngase en contacto con un administrador de red.



Cisco Telemetry Broker recibe el tráfico de administración *solo* en la interfaz de la red de administración; utiliza esta interfaz para todas las comunicaciones entre el nodo de agente y el nodo de administrador. El tráfico de telemetría se administra principalmente en la interfaz de red de telemetría del nodo de agente. La única excepción a esto es cuando Cisco Telemetry Broker recupera los registros de flujo de AWS VPC o los registros de flujo de Azure NSG, o cuando Cisco Telemetry Broker envía telemetría a SCA; las cuales se producen a través de la interfaz de red de administración del nodo de agente.

Puede colocar el nodo de administrador en cualquier lugar de la red en cualquier subred, pero debe tener conectividad TCP a través del puerto 443 con los nodos de agente.

Puede utilizar uno de los siguientes modos de despliegue con el nodo de agente:

1. Las subredes de telemetría y las subredes de administración son las mismas. En este modo, la interfaz de red de telemetría y la interfaz de red de administración del nodo de agente pertenecen a la misma subred. Para obtener más información, consulte la siguiente sección, Interfaces que pertenecen a la misma subred.
2. Las subredes de telemetría y las subredes de administración son diferentes, por lo que el nodo de agente conserva su interfaz de red de telemetría y su interfaz de red de administración en dos subredes separadas. Para obtener más información, consulte dos secciones más abajo, Interfaces que pertenecen a diferentes subredes.

Proporcionar rutas separadas tanto para el tráfico de telemetría como para el de administración ofrece las siguientes ventajas:

- Las rutas separadas aumentan el rendimiento, especialmente cuando se aproxima al rendimiento de la velocidad de línea de la interfaz, ya que el tráfico no necesita compartir recursos.
- Separar el tráfico de administración del tráfico de telemetría simplemente tiene sentido para una configuración de red.

Interfaces que pertenecen a la misma subred

Este modo de despliegue es muy similar al de UDP Director, donde la interfaz de la red de administración y la interfaz de la red de telemetría son la misma. La única diferencia en este primer modo de despliegue es que se necesitan direcciones IP independientes para las interfaces del nodo de agente.

Para ello, conecte la interfaz de red de telemetría y la interfaz de red de administración del nodo de agente a la misma subred.

Interfaces que pertenecen a diferentes subredes

En este modo de despliegue, la interfaz de red de telemetría y la interfaz de red de administración están en subredes diferentes.

5. Conectarse a su appliance

En esta sección se describe cómo conectarse a su appliance 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 al siguiente capítulo, **6. Configuración de su sistema de Cisco Telemetry Broker**.

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 la siguiente configuración:

    - 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 al siguiente capítulo, **6. Configuración de su sistema de Cisco Telemetry Broker**.

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.

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 **password** en el campo Contraseña.
3. Cambie la contraseña predeterminada para proteger la seguridad de su red.
4. Vaya al siguiente capítulo, **6. Configuración de su sistema de Cisco Telemetry Broker**.

6. Configuración de su sistema de Cisco Telemetry Broker

Si ha terminado de instalar sus appliances de hardware, está listo para configurar Cisco Telemetry Broker en un sistema administrado.

Requisitos del navegador

Cisco Telemetry Broker es compatible con los siguientes navegadores (probados con la última versión rápida y con una resolución de 1024 x 768 px):

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

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 nodo de agente TB2300.

Requisitos de configuración	Detalles
Dirección IP	Asigne una dirección IP enrutable al puerto de administración.
Máscara de red	Establezca la subred para la dirección IP que ha elegido.
Gateway	Indique la dirección IP de la puerta de enlace de su subred.
Nombre de host	Se necesita un nombre de host único para cada nodo de agente TB2300. No podemos configurar un appliance con el mismo nombre de host que otro nodo de agente. Todos los nombres de host del nodo de agente deben cumplir los requisitos estándar de Internet para los hosts de Internet.

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 nodo de agente TB2300.

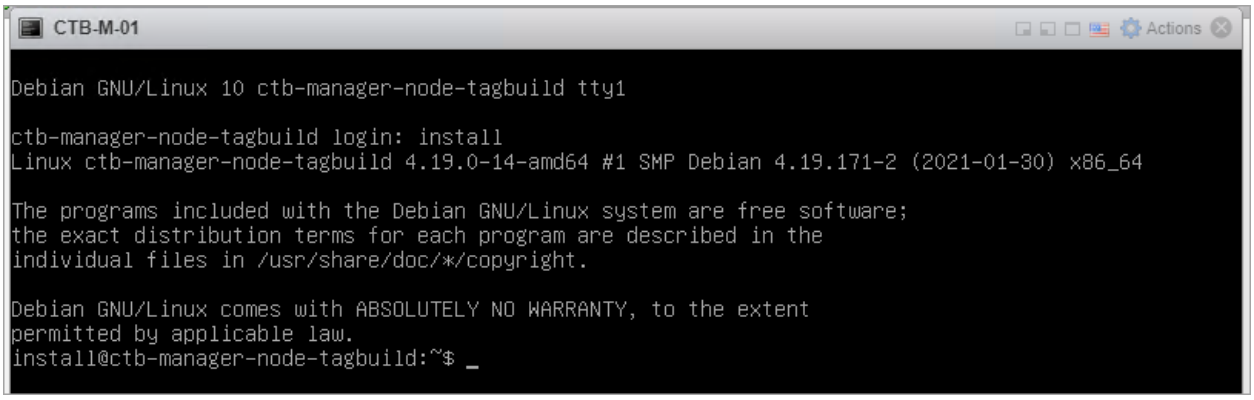
Instalar el nodo de agente

Complete los siguientes pasos en orden.

> Actualmente, el único appliance de hardware que existe para Cisco Telemetry Broker es un nodo de agente (TB2300). Se debe emparejar con un nodo de VM Manager para su despliegue.

1. Iniciar sesión como usuario de instalación

En la consola de CIMC, haga clic en **Launch vKVM**.



2. Ejecute el comando sudo ctb-install --init

1. Ejecute el comando `sudo ctb-install --init`.
2. Especifique la siguiente información:
    - Contraseña para el usuario **administrador**

      La contraseña debe cumplir los siguientes requisitos:
        - Debe contener al menos 8 caracteres
        - Debe contener al menos 1 letra minúscula
        - Debe contener al menos 1 letra mayúscula
        - Debe contener al menos 1 dígito

- Debe contener al menos 1 de estos caracteres especiales: @ # $ % ^ & * ! + ?
- No puede ser una frase o secuencia de uso frecuente
- No puede ser similar a ningún atributo de identificación del usuario (como el nombre de usuario)

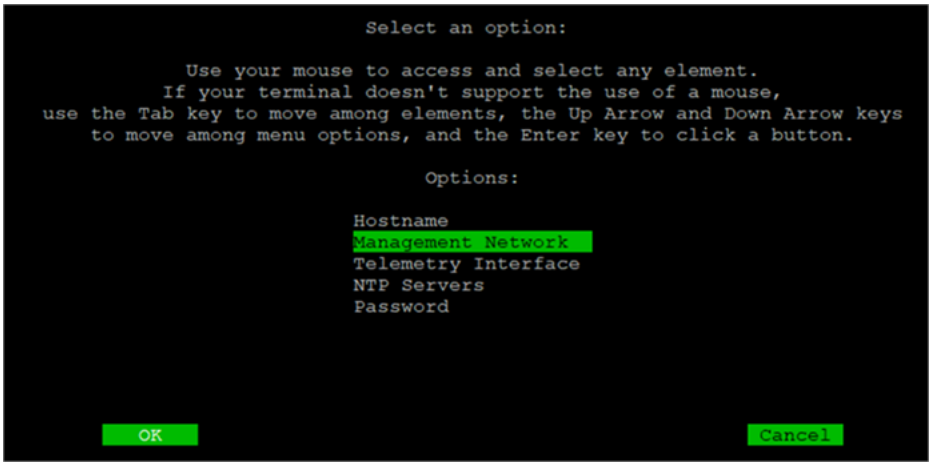
- Nombre de host (máximo 255 caracteres, solo letras y números)
- Puede introducir uno o ambos de los siguientes parámetros de dirección IP:
  - Dirección IPv4, máscara de subred y dirección de gateway predeterminada para la interfaz de la red de administración
  - Dirección IPv6, máscara de subred y dirección de gateway predeterminada para la interfaz de la red de administración
- Dirección IP válida del servidor de nombres DNS accesible desde el nodo de agente (puede introducir una o dos)
- Dirección IP NTP válida accesible desde el nodo de agente.

(Opcional) Cambiar un parámetro individual

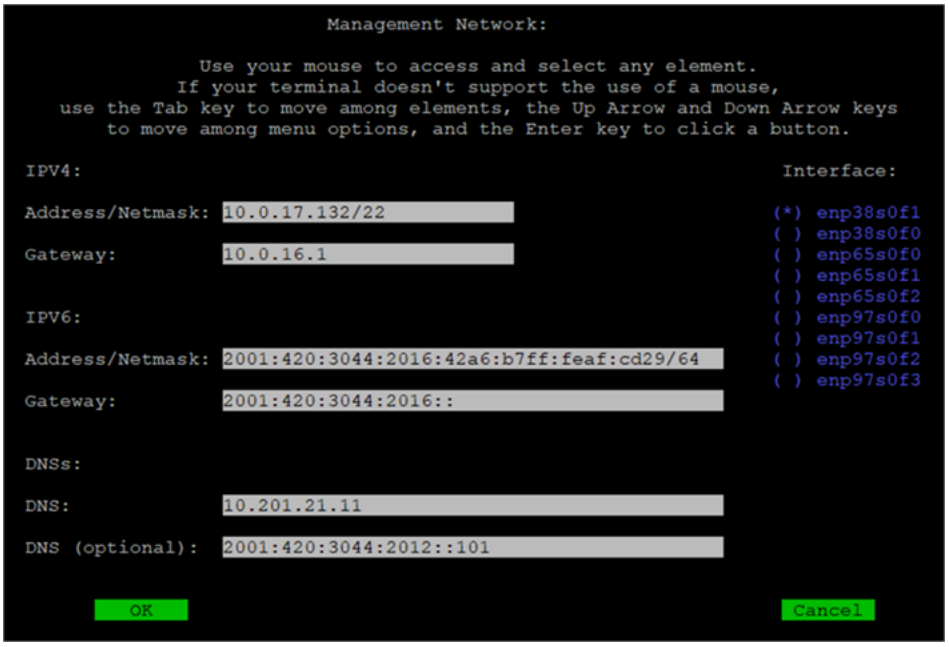
Para cambiar cualquier parámetro individual, ejecute el comando `sudo ctb-install --config`.

Cambiar la interfaz de administración de redes

1. Para cambiar la interfaz de la red de administración, seleccione **Red de administración** en la pantalla principal, como se muestra a continuación:

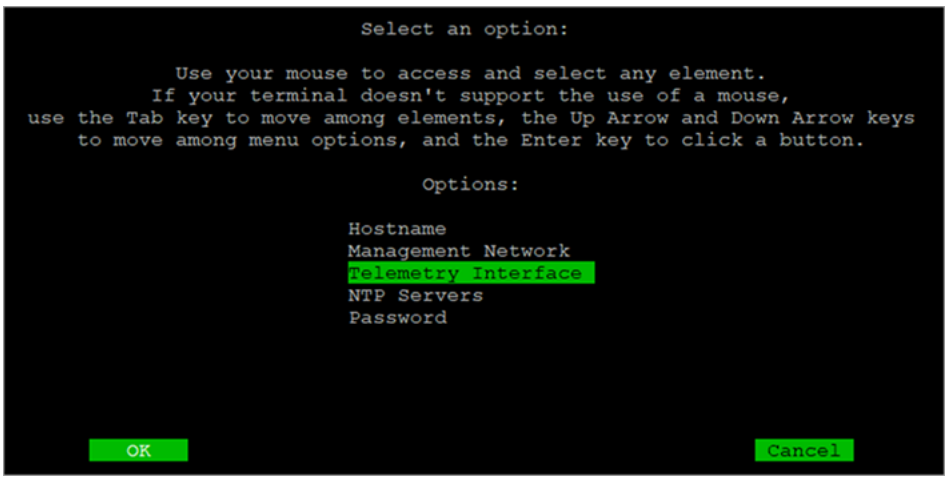


2. En la pantalla Red de administración que se abre, realice los cambios pertinentes en la configuración de la red de administración, incluida la selección de una nueva interfaz de red de administración. Consulte la tabla Número de puerto - Asignación del nombre de la interfaz que se muestra al final de esta sección para saber qué nombre de interfaz elegir para un número de puerto concreto.



Cambiar la interfaz de red de telemetría

1. Para cambiar la interfaz de la red de telemetría, seleccione **Interfaz de telemetría** en la pantalla principal, como se muestra a continuación:



2. En la pantalla que se abre, seleccione la interfaz de red de telemetría correspondiente. Consulte la tabla Número de puerto - Asignación del nombre de la interfaz que se muestra al final de esta sección para saber qué nombre de interfaz elegir para un número de puerto concreto.

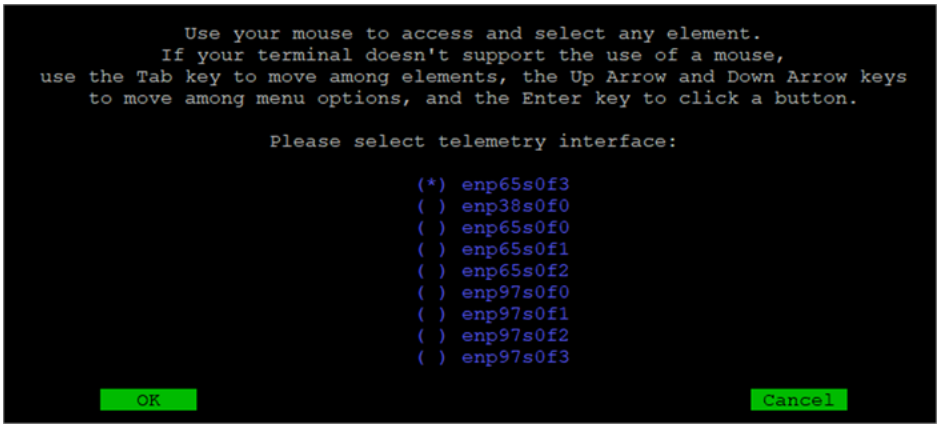
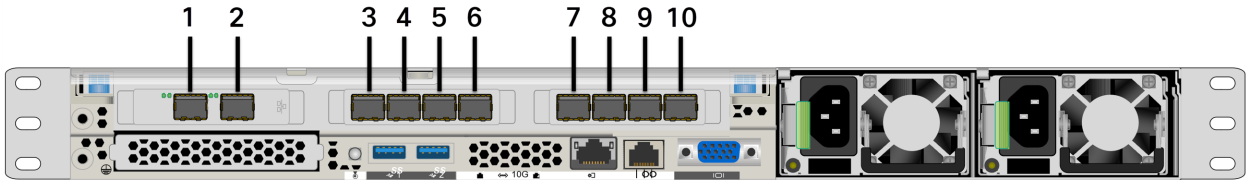


Tabla Número de puerto - Asignación del nombre de la interfaz



Número de puerto	Nombre de la interfaz
1	enp38s0f1
2	enp38s0f0
3	enp65s0f3
4	enp65s0f2
5	enp65s0f1
6	enp65s0f0
7	enp97s0f0

Número de puerto	Nombre de la interfaz
8	enp97s0f1
9	enp97s0f2
10	enp97s0f3

> También se hace referencia a estos números de puerto en las páginas 2 y 3 de la hoja de especificaciones del nodo de agente TB2300.

3. Ejecute el comando sudo ctb-manage

1. Ejecute el comando `sudo ctb-manage`.
2. Especifique la siguiente información:
    - Dirección IP del nodo de administrador
    - Nombre de usuario de la cuenta de superusuario que crea en el nodo de administrador
    - Contraseña de la cuenta de superusuario que crea en el nodo de administrador

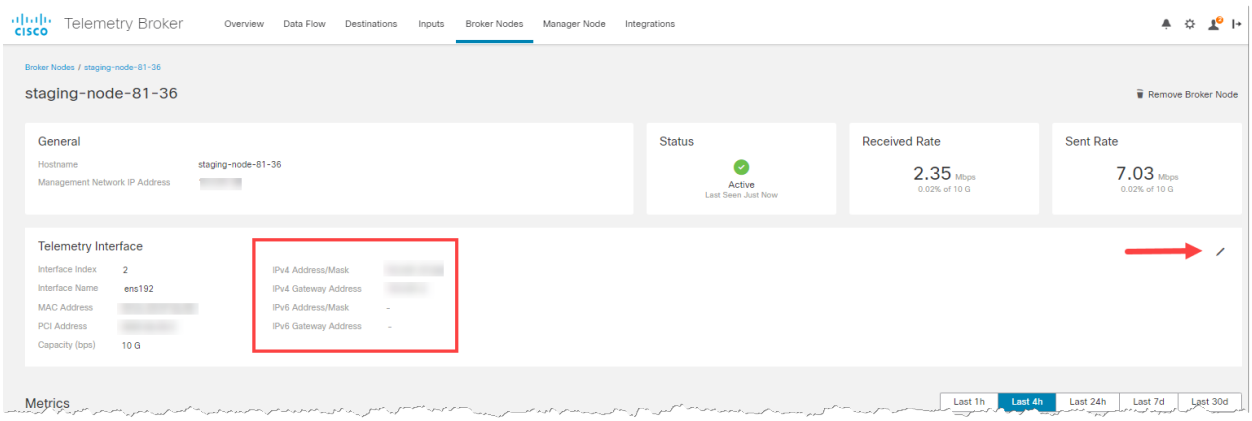
4. Cerrar sesión

Para cerrar la sesión, escriba `exit`.

5. Configurar la interfaz de telemetría

> Cisco Telemetry Broker está configurada para funcionar en modo de sondeo en un appliance de hardware.

1. Inicie sesión en Cisco Telemetry Broker. En un navegador web, introduzca la dirección IP de la interfaz de administración del administrador y pulse **Intro** para acceder al inicio de sesión de la interfaz web del administrador.
2. En el menú principal, seleccione **nodos de agente**.
3. En la tabla de nodos de agente, haga clic en el nodo de agente correspondiente.
4. En la sección Interfaz de telemetría, haga clic en el icono **(Editar)** (indicado por la flecha en la siguiente imagen).



5. Configure las direcciones IP y de puerta de enlace (delimitadas en un borde rojo).

Administrar clústeres de alta disponibilidad

Cisco Telemetry Broker la alta disponibilidad proporciona direcciones IP virtuales IPv4 e IPv6 de alta disponibilidad para que sean objetivos de sus entradas, lo que garantiza una prestación fiable de la telemetría desde las entradas hasta los destinos.

Para establecer una alta disponibilidad del nodo de agente, puede crear clústeres de alta disponibilidad y asignar varios nodos de agente a cada uno de ellos. En cada cluster, un nodo de agente se designa como *Activo*, lo que significa que pasa telemetría y sirve métricas a Cisco Telemetry Broker, y el resto se designan como *Pasivos*, lo que significa que no pasan telemetría ni sirven métricas actualmente. Si un nodo de agente activo deja de transmitir telemetría o pierde la conectividad con el agente de telemetría, uno de los nodos de agente pasivo se convierte en nodo de agente activo y comienza a transmitir telemetría.

Ten en cuenta lo siguiente sobre los clústeres:

- Cada nodo de agente solamente puede pertenecer a un clúster a la vez.
- Para crear un clúster, es necesario asignar como mínimo un nodo de agente a ese clúster.
- Tenga en cuenta que si crea un clúster con un solo nodo de agente y este nodo de agente falla, no habrá ningún otro nodo de agente disponible para ser promovido a nodo de agente activo. Del mismo modo, si todos los nodos de agente de un clúster fallan, ningún nodo de agente puede promocionarse a nodo de agente activo. Si falla un nodo de agente, vuelva a ponerlo en línea lo antes posible.
- No se puede elegir qué nodo de agente está activo en un clúster determinado.
- Si falla un nodo de agente activo para una dirección IP virtual, uno de los nodos de agente pasivo del mismo clúster se convierte en el nodo de agente activo para la dirección IP virtual. Cuando el nodo de agente que ha fallado vuelve a funcionar, sigue siendo un nodo de agente pasivo. Si desea volver a activar ese nodo, deberá hacerlo manualmente utilizando los comandos proporcionados en la sección Mover un VIP a un nodo específico de este capítulo.
- Puede asignar una dirección IPv4 virtual o IPv6 virtual, o ambas, a un clúster. El agente de telemetría utiliza esta dirección IP virtual para comunicarse con el clúster y promover los nodos de agente pasivos a nodos de agente activos cuando un nodo de agente activo pierde la conectividad con el agente de telemetría.

Para obtener información sobre cómo se actualizan los clústeres de alta disponibilidad durante el proceso de actualización del software de Cisco Telemetry Broker, consulte el capítulo "Actualización del software" de la Guía del usuario de Cisco Telemetry Broker.

VIP y enrutamiento

La alta disponibilidad configura la interfaz de red de telemetría del nodo de agente de direcciones VIP. Tenga en cuenta que la interfaz de red de telemetría de cada nodo de agente del clúster *ya debe estar configurada* con una dirección IP primaria IPv4 o IPv6, así como con una máscara de subred y una puerta de enlace. Puede configurarlas en la interfaz de red de telemetría.

Debe configurar las direcciones IP IPv4 o IPv6 del VIP para que estén en la misma subred que las direcciones IP primarias de las **interfaces de red de telemetría** del clúster, ya que el VIP también debe estar en la misma subred. Esto garantiza un enrutamiento correcto a través de la puerta de enlace preconfigurada y una conmutación por falla rápida.

Si las direcciones VIP no están en la misma subred que las direcciones IP primarias de las interfaces de red de telemetría, o si las interfaces de red de telemetría dentro de un clúster están configuradas con subredes diferentes, es muy probable que la alta disponibilidad no funcione.

Administrar clústeres

La implementación de Cisco Telemetry Broker se basa en dos paquetes Linux de uso común para proporcionar la infraestructura de alta disponibilidad subyacente:

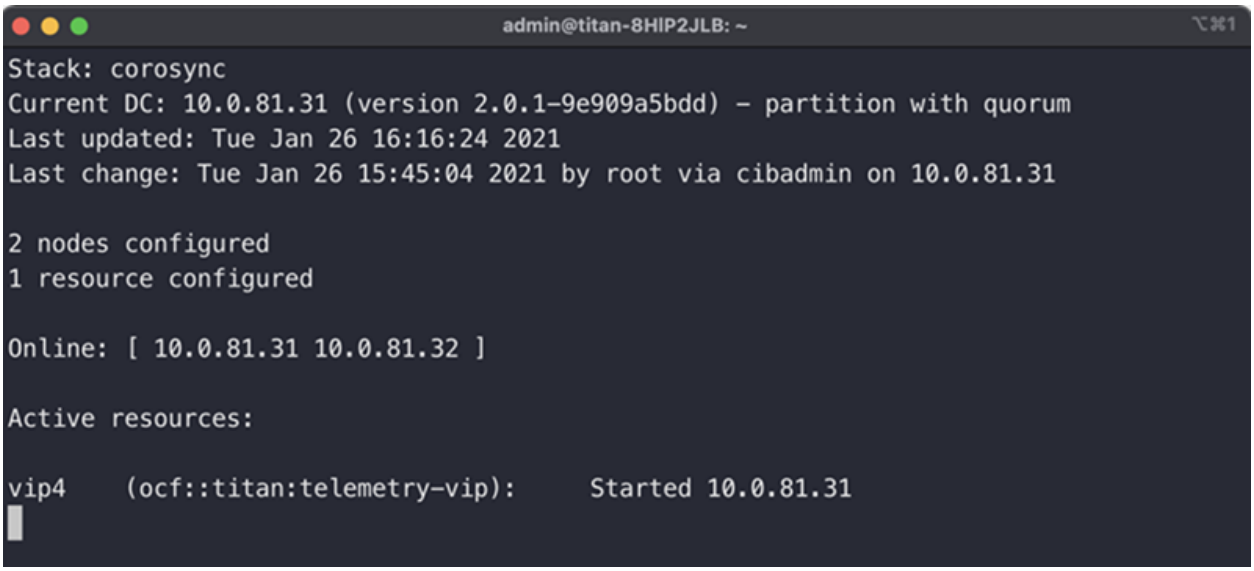
Corosync: este es el motor de clúster de bajo nivel que proporciona la comunicación subyacente entre los nodos del clúster. También proporciona la capacidad de cuórum para tomar la decisión sobre el papel de cada nodo (Activo o En espera).

Pacemaker: es el administrador de recursos de clúster que administra todas las relaciones entre las máquinas y las aplicaciones. Utiliza Corosync para comunicarse.

Ver el estado actual del clúster

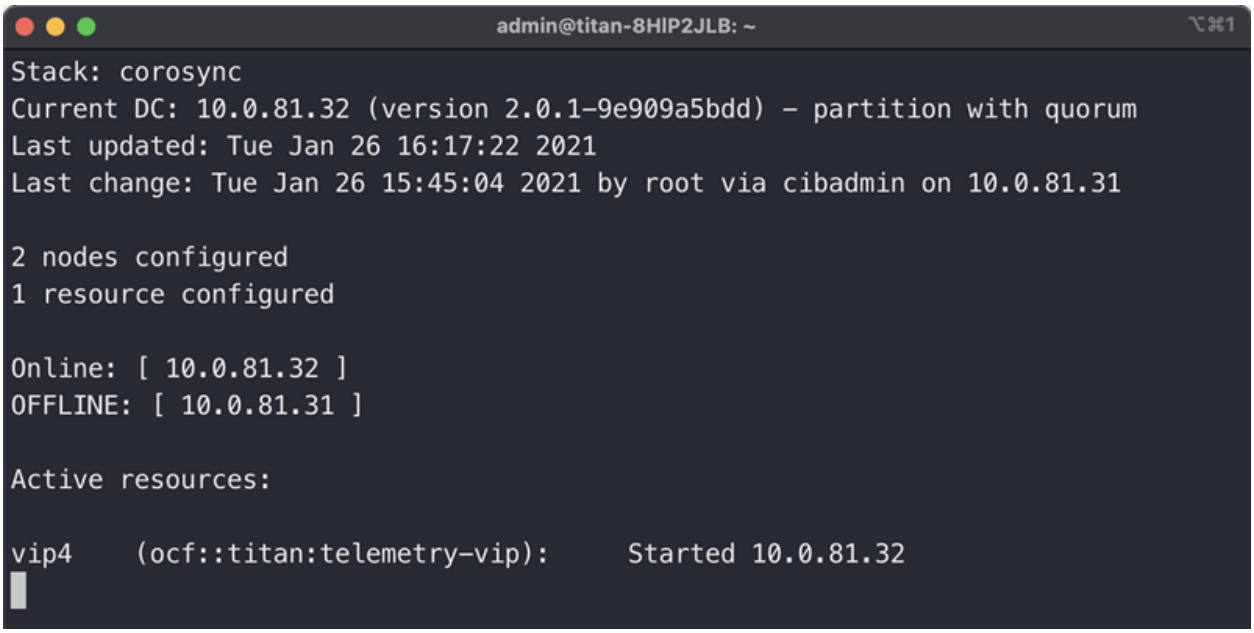
Para ver el estado actual del clúster, incluido el estado (Offline u Online) de cada nodo y la ubicación de la dirección IP IPv4 VIP (vip4) y la dirección IP IPv6 VIP (vip6), complete los siguientes pasos:

1. Inicie sesión como **administrador** en cualquiera de los nodos de agente del clúster mediante SSH. Utilice la contraseña proporcionada durante la instalación del nodo.
2. Ejecute el comando `sudo crm_mon`. Presenta una vista de los atributos configurados actualmente en el clúster. Puede ver más detalles sobre este comando aquí.
3. Salga de la herramienta presionando **Ctrl+C**.



La imagen anterior describe un clúster de dos nodos, 10.0.81.31 y 10.0.81.32, ambos con el estado *Online*. El VIP IPv4 (vip4) se ejecuta actualmente en 10.0.81.31. El VIP IPv6 (vip6) no es visible porque no se ha configurado.

Si 10.0.81.31 fallara, su estado sería el siguiente:



Observe cómo 10.0.81.31 aparece ahora como *OFFLINE* y el vip4 se ha movido a 10.0.81.32.

Ver la configuración actual del clúster

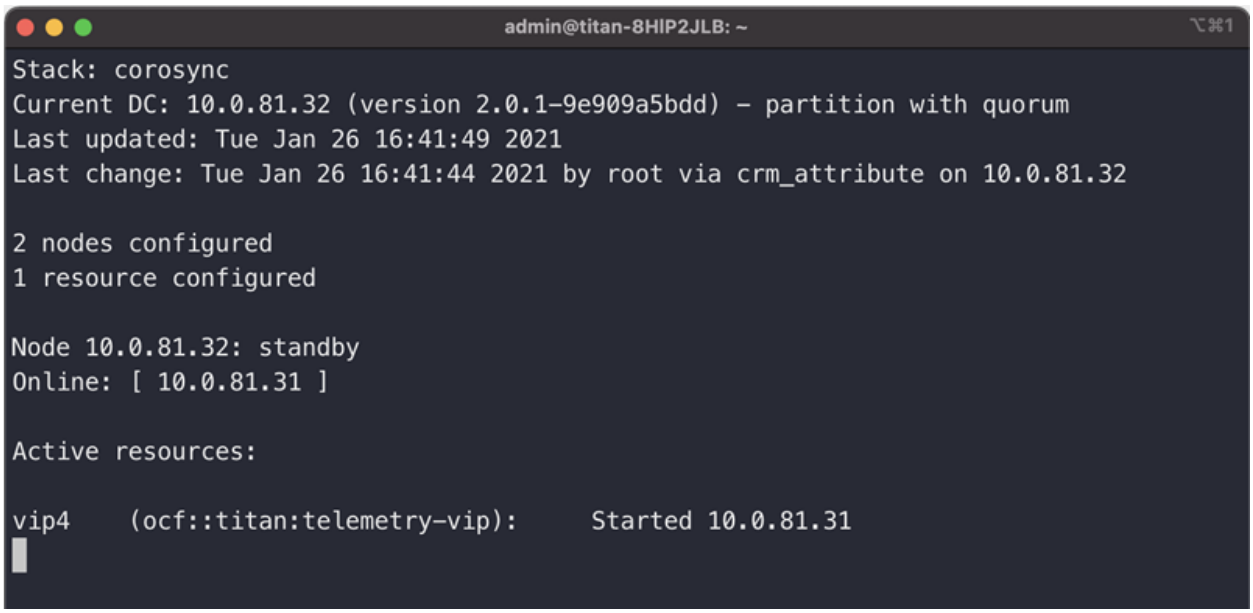
Para ver la configuración actual del clúster y comprobar que las configuraciones de Corosync y Pacemaker son correctas, siga los pasos que se indican a continuación:

1. Inicie sesión como **administrador** en cualquiera de los nodos de agente del clúster mediante SSH. Utilice la contraseña proporcionada durante la instalación del nodo.
2. Ejecute el comando `sudo crm configure show`. Presenta una vista del atributo configurado actualmente en el clúster. Puede ver más detalles sobre este comando aquí.

Habilitar y deshabilitar el modo de espera del nodo

En el modo En espera, el nodo no puede alojar las direcciones IP virtuales IPv4 o IPv6.

1. Inicie sesión como **administrador** en cualquiera de los nodos de agente del clúster mediante SSH. Utilice la contraseña proporcionada durante la instalación del nodo.
2. Ejecute el comando `sudo crm node standby 10.0.81.32`. Puede omitir el nombre del nodo si está ejecutando este comando en ese nodo. Puede ver más detalles sobre este comando aquí.
3. Ejecute el comando `sudo crm node online 10.0.81.32` para sacar el nodo del estado *En espera*. Puede ver más detalles sobre el comando aquí.



Como puede ver, *crm_mon* muestra el estado de espera del nodo 10.0.81.32.

Mover un VIP a un nodo específico

Es posible que se encuentre con circunstancias en las que desee especificar qué nodo está ejecutando la dirección IP virtual IPv4 o IPv6. Si es así, siga estos pasos:

1. Inicie sesión como **administrador** en cualquiera de los nodos de agente del clúster mediante SSH. Utilice la contraseña proporcionada durante la instalación del nodo.
2. Ejecute el comando `sudo crm resource move vip4 10.0.81.32`. Puede ver más detalles sobre este comando aquí.
3. Ejecute el comando `sudo crm resource unmove vip4` para asegurarse de que el VIP permanece en el nodo de destino, de lo contrario el VIP volverá al nodo en el que estaba anteriormente (antes del traslado) en el siguiente momento.

Finalizar la configuración de su sistema

Para finalizar la configuración de su sistema, consulte las siguientes secciones de la Guía del usuario de Cisco Telemetry Broker:

- Destinos
- Entradas
- Nodos de agente

Póngase en contacto con el servicio de asistencia

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

- Póngase en contacto con su partner local de Cisco Telemetry Broker
- Póngase en contacto con la asistencia de Cisco Telemetry Broker
- 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

Historial de cambios

Versión del documento	Fecha de publicación	Descripción
1_0	Abril de 2023	Versión inicial.
1_1	Mayo de 2023	Se agregó el capítulo "Migrar configuración a un nuevo sistema".

Información de copyright

LAS ESPECIFICACIONES E INFORMACIÓN RELATIVAS A LOS PRODUCTOS DE ESTE MANUAL ESTÁN SUJETAS A CAMBIOS SIN PREVIO AVISO. TODAS LAS INDICACIONES, INFORMACIÓN Y RECOMENDACIONES CONTENIDAS EN ESTE MANUAL SE CONSIDERAN EXACTAS, PERO SE PRESENTAN SIN GARANTÍA DE NINGUNA CLASE, NI EXPRESA NI IMPLÍCITA. LOS USUARIOS DEBEN ASUMIR LA PLENA RESPONSABILIDAD SOBRE LA UTILIZACIÓN QUE HAGAN DE LOS PRODUCTOS.

LA LICENCIA DE SOFTWARE Y LA GARANTÍA LIMITADA DEL PRODUCTO QUE LA ACOMPAÑA SE EXPONEN EN EL PAQUETE DE INFORMACIÓN QUE SE ENVÍA CON EL PRODUCTO Y SE INCORPORAN AL PRESENTE DOCUMENTO MEDIANTE ESTA REFERENCIA. SI NO ENCUENTRA LA LICENCIA DEL SOFTWARE O LA GARANTÍA LIMITADA, PÓNGASE EN CONTACTO CON SU REPRESENTANTE DE CISCO PARA OBTENER UNA COPIA.

La implementación por parte de Cisco de la compresión del encabezado de TCP es una adaptación de un programa desarrollado por la Universidad de California, Berkeley (UCB) como parte de la versión de dominio público del sistema operativo UNIX de la UCB. Todos los derechos reservados. Copyright © 1981, Regentes de la Universidad de California.

INDEPENDIENTEMENTE DE CUALQUIER OTRA GARANTÍA DISPUESTA EN EL PRESENTE DOCUMENTO, TODOS LOS ARCHIVOS DEL DOCUMENTO Y EL SOFTWARE DE ESTOS PROVEEDORES SE ENTREGAN "TAL CUAL" CON TODOS LOS ERRORES. CISCO Y LOS PROVEEDORES ANTERIORMENTE MENCIONADOS NIEGAN CUALQUIER GARANTÍA, EXPRESA O IMPLÍCITA, INCLUIDAS, SIN LIMITACIÓN, AQUELLAS DE COMERCIABILIDAD, ADECUACIÓN A UN FIN DETERMINADO E INCUMPLIMIENTO O QUE PUEDAN SURGIR DE UN PROCESO DE NEGOCIACIÓN, USO O PRÁCTICA COMERCIAL.

NI CISCO NI SUS PROVEEDORES SE HARÁN RESPONSABLES EN NINGÚN CASO DE NINGÚN DAÑO INDIRECTO, ESPECIAL, CONSECUENTE O INCIDENTAL, INCLUIDAS, SIN LIMITACIÓN, LAS GANANCIAS PERDIDAS, PÉRDIDAS O DAÑOS EN LOS DATOS COMO CONSECUENCIA DEL USO O DE LA INCAPACIDAD DE USAR ESTE MANUAL, INCLUSO CUANDO SE HAYA AVISADO A CISCO O A SUS PROVEEDORES DE QUE TALES DAÑOS ERAN POSIBLES.

Las direcciones de protocolo Internet (IP) y los números de teléfono utilizados en este documento no pretenden indicar direcciones y números de teléfono reales. Los ejemplos, los resultados en pantalla de los comandos, los diagramas topológicos de la red y otras figuras incluidas en el documento sólo tienen fines ilustrativos. El uso de direcciones IP o números de teléfono reales en el material ilustrativo no es intencionado, sino mera coincidencia.

Se carece de control sobre todas las copias impresas y duplicados en formato electrónico de este documento. Consulte la versión en línea actual para obtener la versión más reciente.

Cisco tiene más de 200 oficinas en todo el mundo. Direcciones y números de teléfono se enumeran en el sitio web de Cisco en https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.