Configuración de NetFlow/IPFIX para la Ingesta de Telemetría en SNA

Contenido

Introducción

Este documento describe las prácticas recomendadas y la configuración básica de Netflow/IPFIX que Secure Network Analytics (SNA) necesita para la ingesta de telemetría.

Prerequisites

- Conocimiento de Cisco SNA
- Conocimiento de NetFlow/IPFIX

Requirements

- Secure Network Analytics en 7.2.1 o posterior
- Flow Collector en 7.2.1 o posterior
- Acceso CLI como raíz al Flow Collector

Componentes Utilizados

- Esto depende completamente del diseño de la red y de los dispositivos que haya seleccionado para enviar NetFlow/IPFIX a Secure Network Analytics. La configuración de NetFlow/IPFIX es diferente en cada exportador. Para obtener información detallada sobre la configuración, póngase en contacto con el equipo de asistencia de cada exportador.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo,

asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

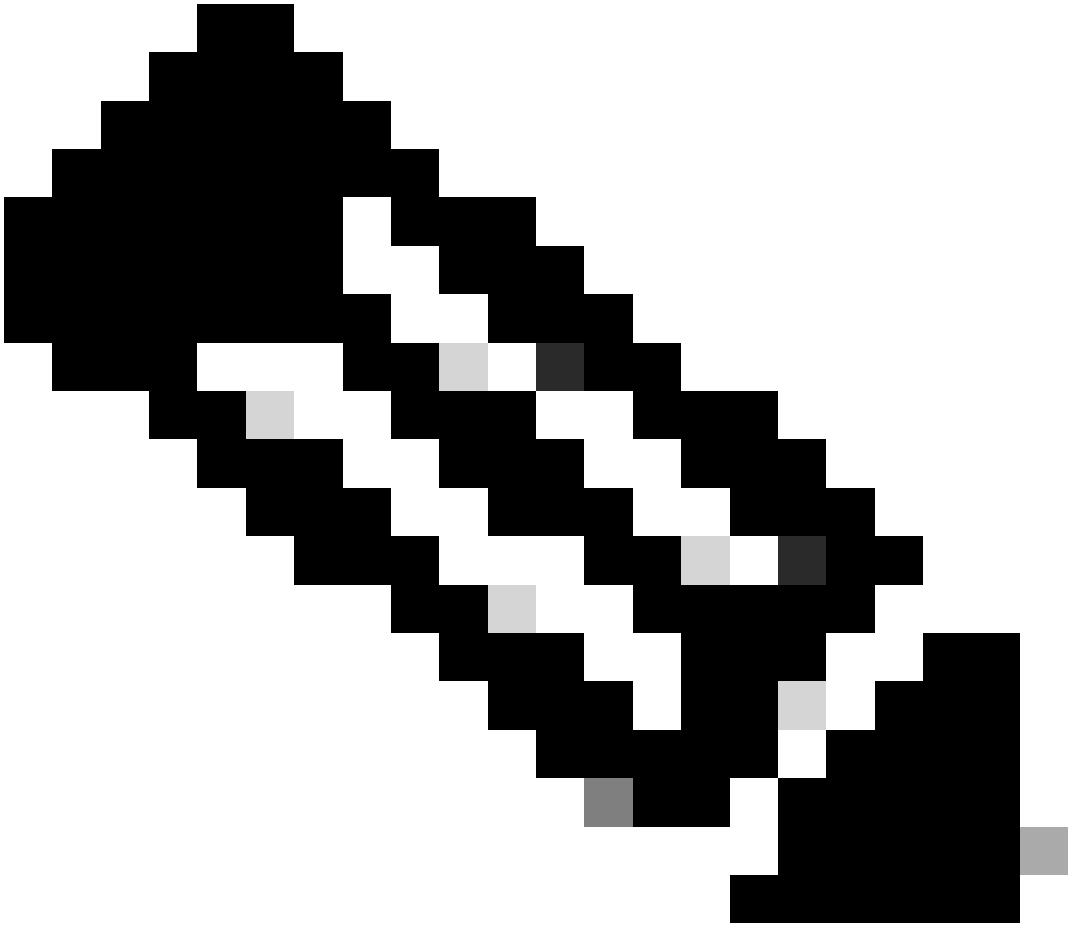
Flow Collector es un dispositivo SNA encargado de recopilar, procesar y almacenar los flujos que se envían a Secure Network Analytics. Para NetFlow versión 9 o IPFIX, se podrían incluir varios campos en la plantilla NetFlow/IPFIX para agregar más información relacionada con el tráfico de red; sin embargo, hay 9 campos específicos que se deben incluir en la plantilla NetFlow/IPFIX para que Flow Collector procese esos flujos. Flow Collector no procesa los flujos entrantes que incluyen una plantilla no válida, por lo que SNA no muestra la información de flujo de esos exportadores en la interfaz de usuario web o el cliente de escritorio.

Configurar

Campos obligatorios

Los siguientes campos deben incluirse en la plantilla NetFlow/IPFIX para la ingesta de telemetría. Asegúrese de que estos 9 campos estén incluidos en la plantilla NetFlow/IPFIX para que Secure Network Analytics procese los flujos entrantes.

- Dirección IP de origen
- Dirección IP de destino
- Puerto de Origen
- Puerto de Destino
- Protocolo de capa 3
- Recuento de bytes
- Recuento de paquetes
- Tiempo de inicio de flujo
- Tiempo de finalización de flujo



Nota: se podrían incluir más campos en la configuración de NetFlow/IPFIX; sin embargo, los campos anteriores son los requisitos mínimos de Secure Network Analytics for Telemetry Ingest.

Campos recomendados

Se recomienda incluir los siguientes campos en la plantilla NetFlow/IPFIX para recopilar información sobre la información de la interfaz; esta configuración es necesaria para mostrar la información de la interfaz, como el nombre y la velocidad:

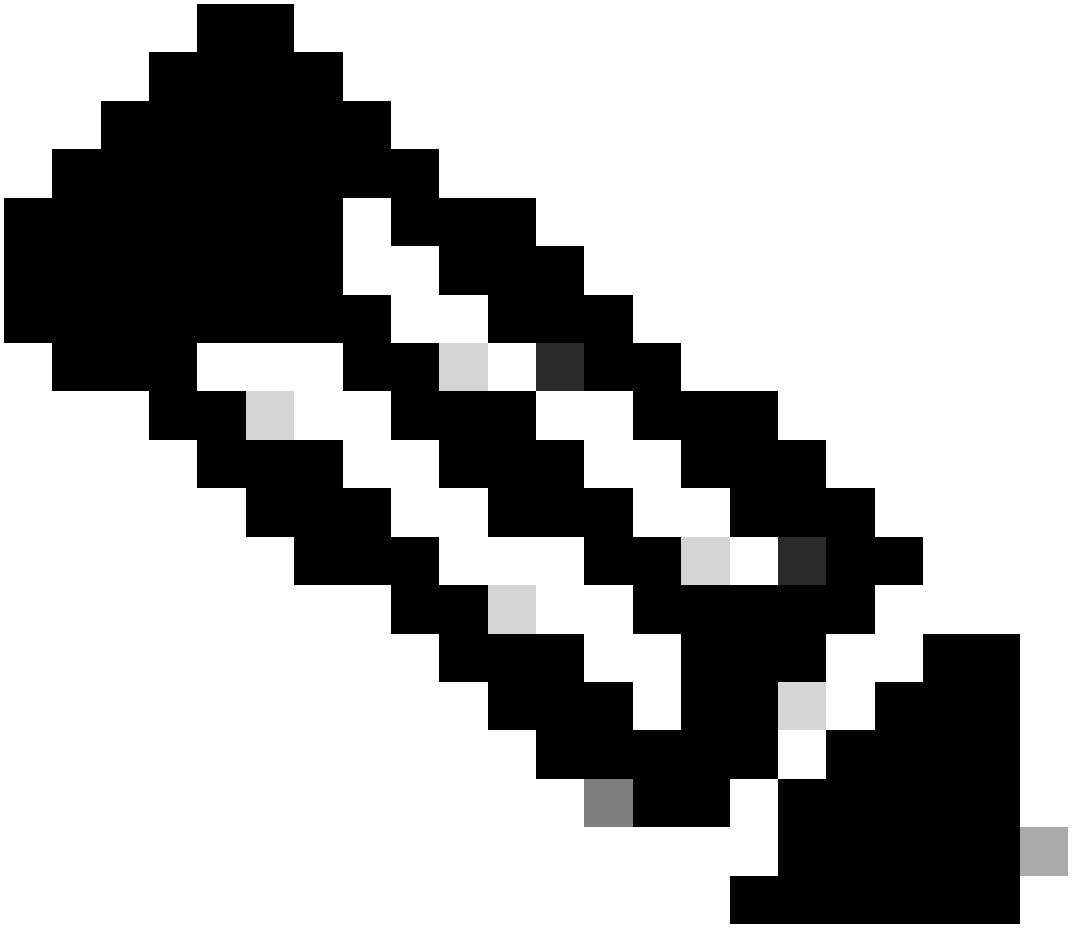
- Entrada de la Interfaz
- Salida de la Interfaz

Prácticas recomendadas

Además, se recomienda la siguiente configuración como prácticas recomendadas para garantizar un rendimiento adecuado de Secure Network Analytics.

- Establecer el tiempo de espera activo en 60 segundos
- Establecer el tiempo de espera inactivo en 15 segundos
- Establecer el tiempo de espera de la plantilla en 30 segundos

---



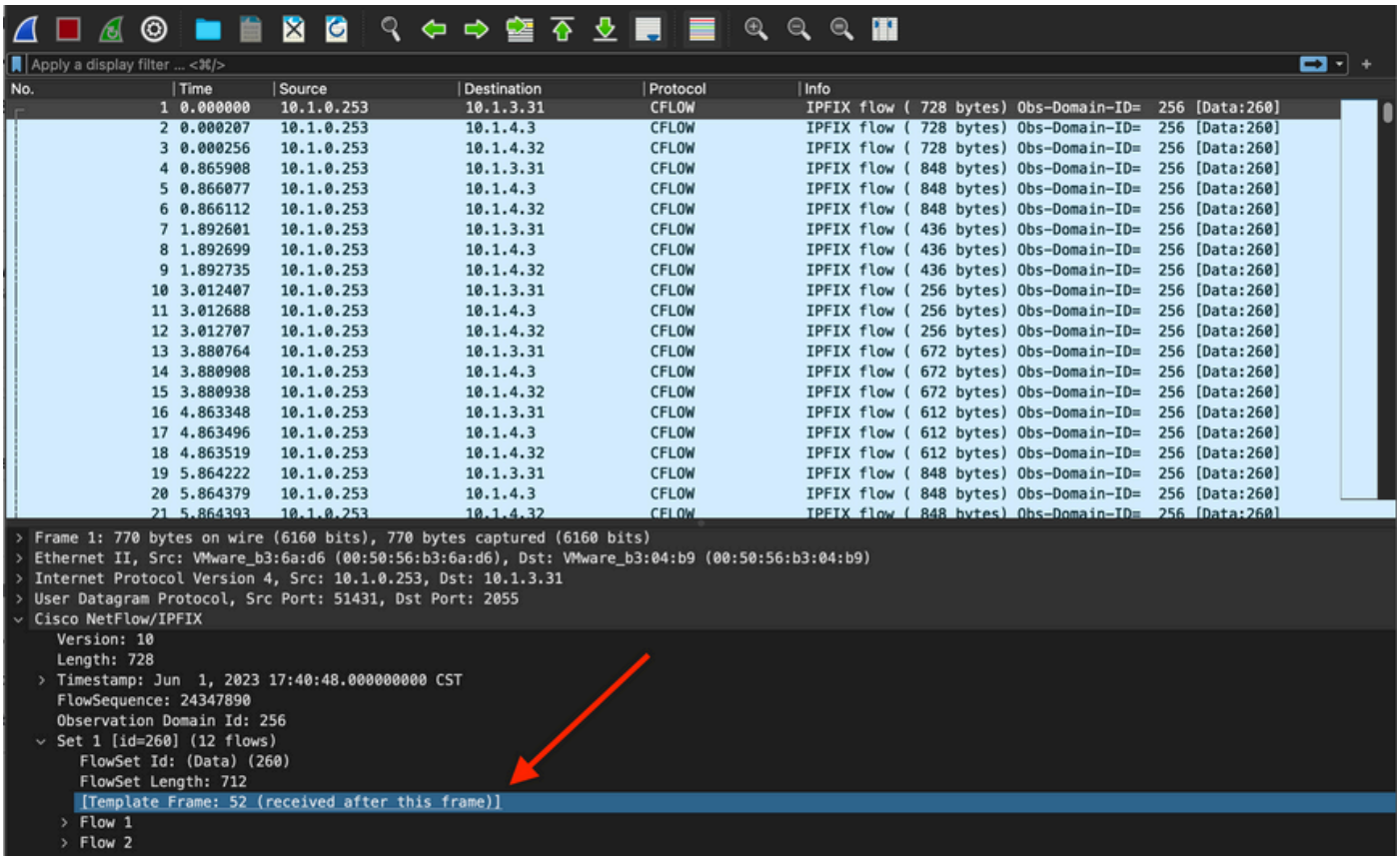
> Nota: El puerto predeterminado para NetFlow es 2055; sin embargo, puede seleccionar otro puerto; asegúrese de utilizar el mismo puerto durante el proceso lc-ast en los Flow Collector(s).

Verificación

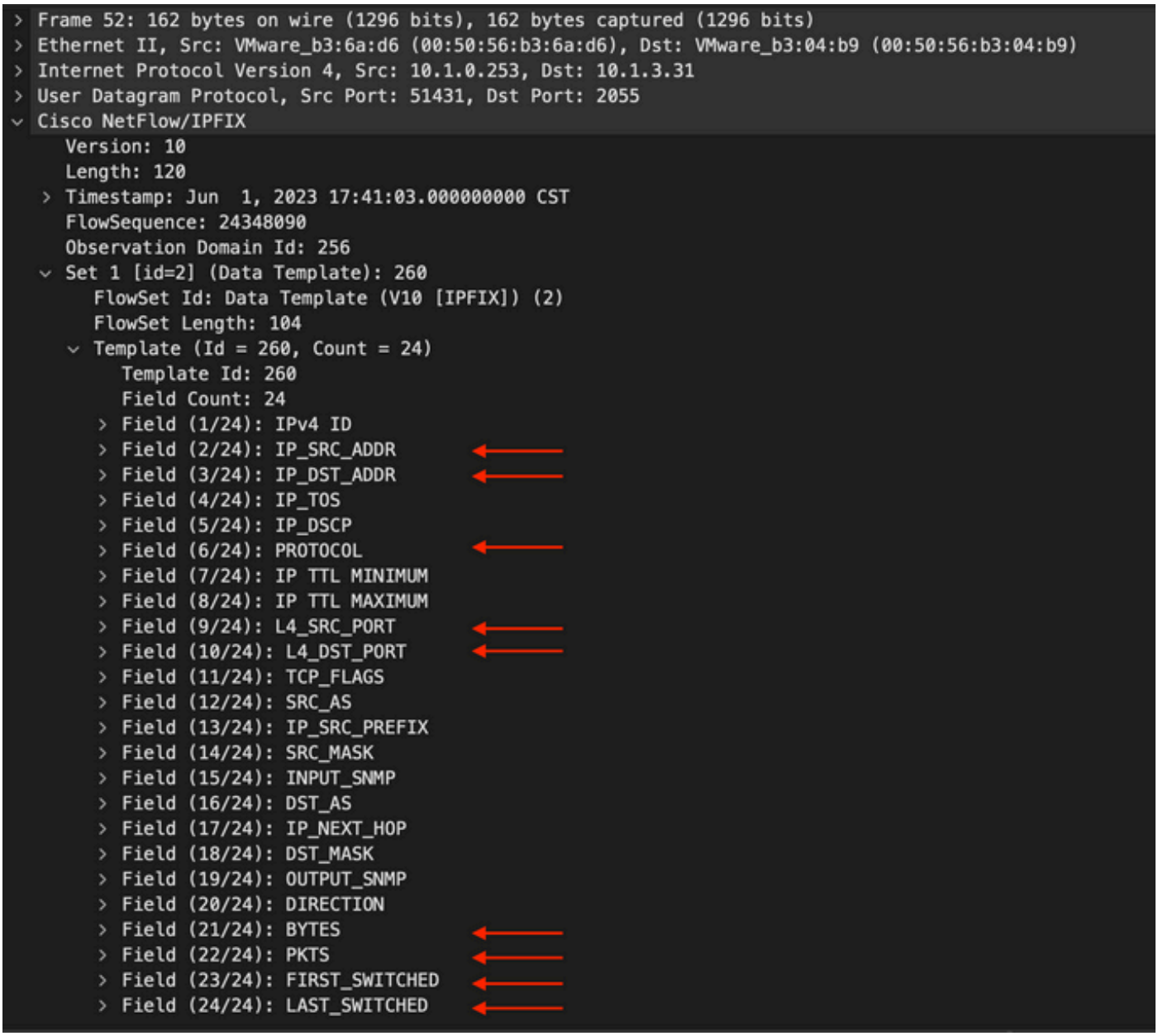
Para validar la configuración de la plantilla NetFlow/IPFIX, puede ejecutar una captura de paquetes entre el exportador y Flow Collector. Inicie sesión en el Flow Collector con el usuario root a través de SSH y ejecute el comando:

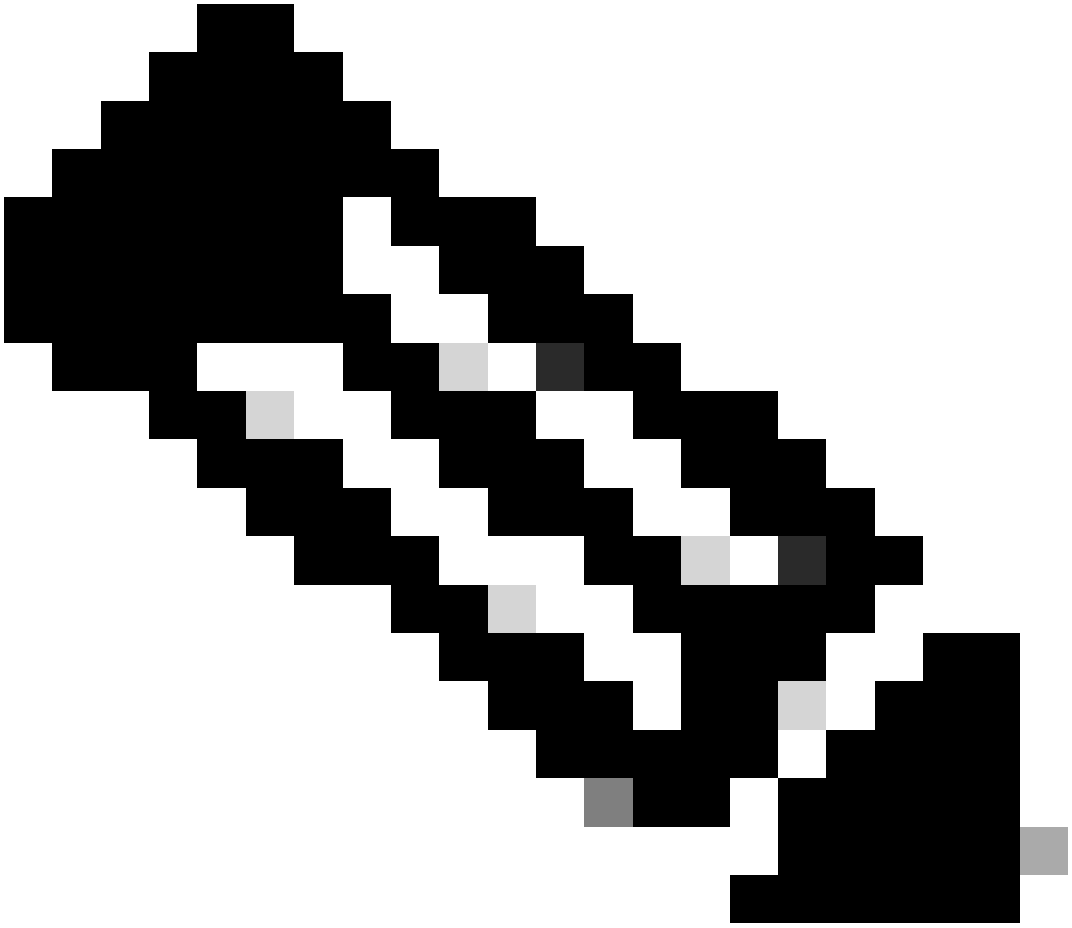
```
tcpdump -nli [Collecting_Interface] host [Exporter_IP_Address] and port [NetFlow_Port] -w /lancope/var/
```

- Utilice una herramienta SCP para exportar la captura de paquetes desde el Flow Collector (ubicado en /lancope/var/tcpdump) a su máquina local y luego ábrala en Wireshark



- Identifique la trama en la que se recibió la plantilla NetFlow/IPFIX y ábrala para validar los campos que incluye la plantilla


Frame 52: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
Ethernet II, Src: VMware_b3:6a:d6 (00:50:56:b3:6a:d6), Dst: VMware_b3:04:b9 (00:50:56:b3:04:b9)
Internet Protocol Version 4, Src: 10.1.0.253, Dst: 10.1.3.31
User Datagram Protocol, Src Port: 51431, Dst Port: 2055
Cisco NetFlow/IPFIX
Version: 10
Length: 120
Timestamp: Jun 1, 2023 17:41:03.000000000 CST
FlowSequence: 24348090
Observation Domain Id: 256
Set 1 [id=2] (Data Template): 260
FlowSet Id: Data Template (V10 [IPFIX]) (2)
FlowSet Length: 104
Template (Id = 260, Count = 24)
Template Id: 260
Field Count: 24
Field (1/24): IPv4 ID
Field (2/24): IP_SRC_ADDR
Field (3/24): IP_DST_ADDR
Field (4/24): IP_TOS
Field (5/24): IP_DSCP
Field (6/24): PROTOCOL
Field (7/24): IP TTL MINIMUM
Field (8/24): IP TTL MAXIMUM
Field (9/24): L4_SRC_PORT
Field (10/24): L4_DST_PORT
Field (11/24): TCP_FLAGS
Field (12/24): SRC_AS
Field (13/24): IP_SRC_PREFIX
Field (14/24): SRC_MASK
Field (15/24): INPUT_SNMP
Field (16/24): DST_AS
Field (17/24): IP_NEXT_HOP
Field (18/24): DST_MASK
Field (19/24): OUTPUT_SNMP
Field (20/24): DIRECTION
Field (21/24): BYTES
Field (22/24): PKTS
Field (23/24): FIRST_SWITCHED
Field (24/24): LAST_SWITCHED



Nota: Los nombres de campo mostrados pueden tener un aspecto diferente en cada exportador, esto es solo una referencia de cómo se pueden validar esos campos.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).