Remediar el aviso de seguridad de Catalyst SD-WAN - Mayo de 2026

Contenido

Introducción

Este documento describe los pasos para identificar y solucionar vulnerabilidades de seguridad críticas en SD-WAN basándose en los avisos PSIRT del 14 de mayo de 2026.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Arquitectura Cisco Catalyst SD-WAN y componentes de control (vManage, vSmart, vBond)
- Procedimiento de actualización de Cisco Catalyst SD-WAN
- Administración de casos del TAC de Cisco y procedimientos de recopilación de tecnología de administración

Componentes Utilizados

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

Para obtener información general detallada y las últimas actualizaciones, consulte la página oficial de asesoramiento sobre PSIRT.

Estos consejos están disponibles en los siguientes enlaces:

- Vulnerabilidad de omisión de autenticación del controlador Cisco Catalyst SD-WAN
- Vulnerabilidades de la SD-WAN de Cisco Catalyst

Estos defectos se abordan en las siguientes recomendaciones PSIRT:

- ID de bug de Cisco CSCwt50498
- ID de bug de Cisco CSCwt38739
- ID de bug de Cisco CSCwt38767
- ID de bug de Cisco CSCwt55544

Flujo de trabajo de remediación

Nota: Todos los controladores y administradores de SD-WAN son vulnerables y requieren una actualización inmediata para todos los componentes de control. Sin embargo, no todos los controladores muestran evidencia de compromiso.

Acción requerida: Recopile técnicos administrativos, actualice a una versión fija y abra un caso del TAC de Cisco para que el TAC pueda analizar a sus técnicos administrativos en busca de indicadores de compromiso.

TAC está disponible para:

- Analice los técnicos de administración que proporcione para ver los indicadores de compromiso
- Proporcionar soporte de actualización si experimenta problemas durante la actualización
- Guiarle a través de soluciones adicionales si se identifican indicadores de compromiso.

1. Recopile Admin-Techs - Ejecute admin-tech en todos los componentes de control (vSmart, vManage, vBond) antes de la actualización para asegurarse de que no se pierdan datos de diagnóstico. Seleccione Log and Tech options (Opciones de registro y tecnología). El

núcleo no es necesario.

Precaución: vSmart admin-techs no se debe ejecutar simultáneamente: ejecútelos de uno en uno. Todas las demás se pueden recopilar en cualquier orden

2. Actualizar a una versión fija: actualice todos los componentes de control de SD-WAN (vManage, vSmart, vBond) a una versión de software fija enumerada en la tabla Versiones de software fijas.

Nota: No espere los resultados del análisis del TAC antes de actualizar. La actualización a una versión fija es la prioridad más alta y cierra la vulnerabilidad. El análisis del TAC del paso 3 determina si se necesita alguna acción adicional después de la actualización.

3. Abra un caso del TAC y cargue los técnicos de administración para buscar indicadores de compromiso - Abra un caso del TAC de Cisco y cargue todos los paquetes de registro de la tecnología de administración recopilados en el paso 1. El TAC escanea los técnicos de administración en busca de indicadores de compromiso.
4. Si se identifica un riesgo, siga las directrices del TAC: si el TAC identifica indicadores de riesgo en su entorno, complete todas las directrices de remediación proporcionadas por el TAC. Si no se encuentran indicadores de compromiso, no se requiere ninguna acción adicional más allá de la actualización.

Paso 1: Recopilar archivos técnicos de administración de todos los componentes de control

required (obligatorio): Recopile los archivos admin-tech de todos los componentes de control antes de actualizar para asegurarse de que no se pierdan datos de diagnóstico. El TAC utiliza estos archivos en el paso 3 para analizar su entorno en busca de indicadores de compromiso.

Colección:

Nota: Para admin-tech generation, seleccione Log and Tech options (Opciones de registro y tecnología). El núcleo no es necesario.

1. Ejecute admin-tech en TODOS los controladores (vsmarts) - no ejecute estos simultáneamente; recolectar uno a la vez
2. Ejecute admin-tech en ALL Managers (vManagers)
3. Ejecute admin-tech en ALL Validators (vBonds)

Nota: Los vSmart admin-techs no se deben ejecutar simultáneamente: recójelos de uno en uno. Los técnicos de administración para gerentes y validadores se pueden recopilar en cualquier orden.

Recopile una Admin-Tech en un entorno SD-WAN y cárguela en un caso TAC

Nota: TAC analiza estos archivos para evaluar su entorno en busca de indicadores de compromiso y guiar la ruta de remediación adecuada.

Alternativa: Verificación manual (solo si Admin-Tech no puede ser recolectada)

Para aquellos que no pueden compartir archivos de administración y tecnología, hay disponibles pasos de verificación manual. Estos pasos proporcionan indicadores preliminares que deben documentarse y compartirse con el TAC.

Consulte la sección "Pasos de verificación manual" al final de este documento para ver los procedimientos detallados. Documente todas las conclusiones y proporciónelas al TAC en su caso de soporte.

Paso 2: Actualización a una versión de software fija

Después de recopilar los técnicos de administración en el paso 1, actualice todos los componentes de control de SD-WAN (vManage, vSmart y vBond) a una versión de software fija.

Importante: No espere los resultados del análisis del TAC antes de actualizar. La actualización a una versión fija es la prioridad más alta y cierra la vulnerabilidad. El análisis del TAC del paso 3 determina si se necesita alguna acción adicional después de la actualización.

Seleccione la versión adecuada de la tabla Versiones fijas de software de este documento.

Advertencia: La actualización debe permanecer dentro de su versión principal actual. No actualice a una versión principal superior sin una guía explícita del TAC.

Actualización de controladores SD-WAN con el uso de vManage GUI o CLI

Nota: Si encuentra algún problema durante la actualización, abra un caso del TAC para obtener soporte para la actualización.

Paso 3: Abra un caso TAC y cargue archivos técnicos de administración para escanear

Después de actualizar en el paso 2, abra un caso de soporte del TAC de Cisco y cargue los archivos admin-tech recopilados en el paso 1. El TAC explora los admin-tech en busca de indicadores de compromiso.

Acciones necesarias:

1. Abra un caso TAC de Gravedad 3 con "CVE-2026-20182" y la ID de PSIRT relevante en el título para iniciar el proceso de escaneo.
2. Cargue TODOS los paquetes de registro de tecnología de administración recopilados en el paso 1 (Controladores, administradores y validadores)
3. Espere a que el TAC complete el análisis y comunique los resultados

Nota: El TAC analiza los archivos técnicos de administración y comunica los resultados del análisis. Si no se encuentran indicadores de compromiso, no se requiere ninguna acción adicional más allá de la actualización.

Paso 4: Si se identifica algún riesgo, siga las directrices del TAC

Si el TAC identifica indicadores de compromiso en su entorno, el TAC se pone en contacto con usted para ofrecerle una guía de remediación específica. Complete todas las instrucciones proporcionadas por el TAC.

Si no se identifican indicadores de compromiso, la actualización realizada en el paso 2 es suficiente y no se requiere ninguna otra solución.

Versiones de software fijas

Estas versiones de software contienen correcciones para las vulnerabilidades identificadas:

Se aplica a las versiones actuales	Versión fija	Software disponible
20.3, 20.6, 20.9	20.9.9.1	20.9.9.1 imágenes de actualización para vManage, vSmart y vBond
20.10, 20.11, 20.12.5 y anteriores en 20.12	20.12.5.4	20.12.5.4 imágenes de actualización para vManage, vSmart y vBond

Se aplica a las versiones actuales	Versión fija	Software disponible
20.12.6.x	20.12.6.2	20.12.6.2 imágenes de actualización para vManage, vSmart y vBond
20.12.7	20.12.7.1	20.12.7.1 imágenes de actualización para vManage, vSmart y vBond
20.13, 20.14, 20.15.4.3 y anteriores en 20.15	20.15.4.4	20.15.4.4 imágenes de actualización para vManage, vSmart y vBond
20.15.5.x	20.15.5.2	20.15.5.2 imágenes de actualización para vManage, vSmart y vBond
20.16, 20.17 y 20.18.x	20.18.2.2	20.18.2.2 imágenes de actualización para vManage, vSmart y vBond

Nota: Para los clientes de SD-WAN Cloud (anteriormente conocido como Cloud Delivered Cisco Catalyst SD-WAN [CDCS]), el 20.15.506 también es una versión fija. Esto se aplica específicamente a la implementación de clústeres alojados por Cisco y se gestiona por separado de la ruta de actualización estándar. Todos estos clientes ya han actualizado a la versión fija 20.15.506.

Referencias importantes:

- Matriz de actualización
- Matriz de compatibilidad del controlador

Apéndice: Pasos de verificación manual (solo si no es posible la recopilación de tecnología de administrador)

Nota: La colección Admin-tech es el método preferido y recomendado. Utilice la verificación manual únicamente si no puede recopilar y compartir archivos de tecnología administrativa. Si no puede recopilar archivos de administración-tecnología, utilice estos pasos manuales para recopilar indicadores preliminares para TAC.

Nota:

- Estos pasos proporcionan solo datos preliminares
- La recopilación de tecnología de administración es muy preferible para realizar una evaluación precisa
- Documentar sus conclusiones y compartirlas con el TAC en su caso de soporte
- TAC realiza la determinación de evaluación oficial

Requerimientos: Estos pasos se deben realizar en todos los componentes del control.

Verificación 1: Verifique si hay Logins SSH No Autorizados en los Logs de Autenticación

Paso 1: Identificar direcciones IP del sistema vManage válidas

Acceda a cada controlador vSmart y ejecute:

```
west-vsmart# show control connections | inc "vmanage|PEER|IP"
```

Ejemplo de salida:

```
                                          PEER
      PEER  PEER  PEER            SITE       DOMAIN  PRIV    PEER                          PUB
INDEX TYPE  PROT  SYSTEM IP       ID         ID      PRIVATE IP                      PORT    PUBLIC I
-------------------------------------------------------------------------------------------------
0     vmanage dtls 10.1.0.18     101018     0       10.1.10.18                      12346   10.1.10.1
```

Paso 2: Generar cadena de expresión regular (sólo vBond y vSmart)

Combine todas las IP del sistema del paso 1 en un patrón de regex OR:

```
system-ip1|system-ip2|...|system-ipn
```

Paso 2b: Paso adicional para sistemas vManage

Si ejecuta estos comandos en el propio vManage, añada la IP de host local (127.0.0.1), la IP del sistema local, todas las IP de clúster y la IP de la interfaz de transporte VPN 0 al regex:

```
system-ip1|system-ip2|...|system-ipn|127.0.0.1|
```

Para buscar la dirección IP del sistema vManage local, utilice:

```
show control local-properties
```

Para buscar la IP de la interfaz de transporte VPN 0 y la IP del clúster, utilice:

```
show interface | tab
```

Paso 3: Ejecutar comando de verificación

Ejecute este comando, reemplazando REGEX con su cadena regex del Paso 2:

```
west-vsmart# vs
west-vsmart:~$ zgrep "Accepted publickey for vmanage-admin from " /var/log/auth.log* | grep -vE "\s(REG
```

Nota: Este comando filtra los registros de autenticación para mostrar solamente los inicios de sesión de vmanage-admin de orígenes inesperados. Los inicios de sesión legítimos solo deben originarse en direcciones IP relacionadas con vManage.

Paso 4: Interpretar resultados y documentos para TAC

Si se muestra NO output:

- No se detectaron indicadores de compromiso en este dispositivo
- Documente este resultado para su caso TAC
- Continuar la evaluación de los controladores restantes

Si se imprimen líneas de registro:

- Examine cuidadosamente cada dirección IP mostrada
- Verifique que la IP no esté relacionada con la infraestructura de vManage (IP del clúster, IP del sistema antiguo o similar)
- Si no puede identificar la IP de origen como legítima, esto puede indicar posibles indicadores de compromiso
- La entrada del registro muestra una marca de tiempo y una dirección IP de origen

- Documentar todas las conclusiones y abrir un caso TAC inmediatamente
- Incluya las entradas de registro, las marcas de tiempo y las IP de origen en su caso
- TAC realiza la determinación de evaluación oficial

Verificación 2: Comprobar conexiones de pares no autorizadas en registros del sistema del controlador

Este comando extrae todos los pares peer-type e peer-system-ip de los archivos syslog del controlador y los genera como una lista para que la revise. No marca automáticamente entradas sospechosas: debe inspeccionar la salida y determinar si cada IP del sistema de peer es una parte conocida y legítima de su infraestructura SD-WAN. Ejecute esto en todos los componentes del control (controladores, administradores y validadores).

Paso 1: Ejecute el comando en cada componente del control:

Primero, acceda a vshell y navegue hasta el directorio de registro:

```
vs
cd /var/log
```

A continuación, ejecute este comando para buscar el glob del archivo vsyslog*:

```
awk '{
  match($0, /peer-type:([a-zA-Z0-9]+)[^ ]* peer-system-ip:([0-9.:]+)/, arr);
  if(arr[1] && arr[2]) print "(" arr[1] ", " arr[2] ")";
}' vsyslog* | sort | uniq
```

Repita esto para messages* file glob así como para vdebug* file glob.

Paso 2: Interpretar resultados y documentos para TAC

Si el resultado solo muestra direcciones IP del sistema vManage/vSmart/vBond conocidas:

- No se detectaron indicadores de compromiso en esta comprobación
- Documente este resultado para su caso TAC
- Continuar la evaluación de los componentes de control restantes

Si el resultado contiene IPs del sistema de peer no reconocidas:

- Examine cuidadosamente cada dirección IP y el tipo de par que se muestra
- Verifique que la IP no esté relacionada con su infraestructura de plano de control SD-WAN conocida
- Si no puede identificar la IP de origen como legítima, esto puede indicar posibles indicadores de compromiso

- Documentar todas las conclusiones y abrir un caso TAC inmediatamente
- Incluya el resultado completo del comando con pares peer-type y peer-system-ip en su caso
- TAC realiza la determinación de evaluación oficial

Verificación 3: Comprobar si falta desafío-ack en las conexiones de control activo

Esta verificación inspecciona la salida de detalle de las conexiones de control para las sesiones de peer que se informan como activas (o recientemente desactivadas) pero que no tienen el intercambio `challenge-ack` esperado. Una sesión que intercambia paquetes de `saludo` en ambas direcciones mientras muestra `challenge-ack 0` en las estadísticas de Tx o Rx indica que el par nunca completó el saludo de desafío esperado, una anomalía que justifica una investigación. Ejecute esto en todos los componentes del control (controladores, administradores y validadores).

Paso 1: Recopile el resultado detallado de las conexiones de control

En la CLI del dispositivo, ejecute:

```
show control connections detail
show control connections-history detail
```

Guarde el resultado en un archivo (por ejemplo, `vdaemon.txt`) para su inspección.

Paso 2: Qué buscar

Para cada registro par (delimitado por los encabezados `REMOTE-COLOR-` / `SYSTEM-IP-`), marque el registro si todas estas condiciones son verdaderas:

- El estado de sesión es UP o TEAR_DOWN
- Tanto el contador de saludo de Estadísticas Tx como el contador de saludo de Estadísticas Rx no son cero (los saludo fluyen en ambas direcciones)
- challenge-ack es 0 en el bloque Estadísticas de Tx o Estadísticas de Rx (o en ambos)

Ejemplo de registro coincidente (observe las flechas `<<<<<` que resaltan el `challenge-ack` que falta)

```
----------------------------------------------------------------------------------------------
 REMOTE-COLOR- default SYSTEM-IP- 10.2.2.2   PEER-PERSONALITY- vmanage
----------------------------------------------------------------------------------------------
site-id             432567
domain-id           0
protocol            dtls
private-ip          10.0.0.1
private-port        12346
public-ip           192.168.1.1
public-port         50825
state               up [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime              0:00:16:58
hello interval      1000
hello tolerance     12000
```

```
  Tx Statistics-
  --------------
    hello                   3423293
    challenge               1
    challenge-response      0
    challenge-ack           0           <<<< MISSING challenge-ack (Tx)
    ...

  Rx Statistics-
  --------------
    hello                   3423291
    challenge               0
    challenge-response      1
    challenge-ack           0           <<<< MISSING challenge-ack (Rx)
    ...
```

En el ejemplo anterior, los contadores de `saludo` Tx y Rx no son cero (conexión activa), pero `challenge-ack` es `0` en ambas direcciones.

Paso 3: Comando de búsqueda manual

Para encontrar rápidamente registros candidatos de un archivo `vdaemon.txt` guardado (o cualquier archivo que contenga el resultado `show control connections detail`), ejecute:

```
grep -A20 'SYSTEM-IP' vdaemon.txt | grep -B5 'challenge-ack  0'
```

Cada bloque devuelto representa una sesión de peer donde challenge-ack se informa como 0. Revise cada bloque en su totalidad para confirmar que el estado es `up` o `drop_down` y que los contadores hello en Tx y Rx no son cero antes de tratarlo como un hit.

Paso 4: Interpretar resultados y documentos para TAC

Si ningún registro cumple las tres condiciones:

- No se detectaron indicadores de compromiso en esta comprobación
- Documente este resultado para su caso TAC
- Continuar la evaluación de los componentes de control restantes

Si uno o más registros cumplen las tres condiciones:

- Examine cuidadosamente los valores `SYSTEM-IP-`, `private-ip` y `public-ip` para cada registro marcado
- Compruebe que el par no es una parte conocida y legítima del plano de control de la SD-WAN (miembro del clúster, sitio de DR, dirección IP asignada previamente a un componente)
- Si no puede identificar al par como legítimo, esto puede indicar posibles indicadores de compromiso

- Documentar todas las conclusiones y abrir un caso TAC inmediatamente
- Incluya el registro o registros pares coincidentes completos y el resultado del comando source en su caso
- TAC realiza la determinación de evaluación oficial

Preguntas Frecuentes

A: ¿Cuál es el primer paso para abordar este aviso de seguridad?

R: Recopile los archivos admin-tech de todos los componentes de control y, a continuación, actualice todos los componentes de control a una versión de software fija. Después de actualizar, abra un caso TAC y cargue los técnicos administrativos para que TAC pueda analizar su entorno en busca de indicadores de compromiso.

P. ¿A qué versión necesito actualizar?

R. Actualice a la versión fija más cercana lo antes posible.

A: ¿Necesito recopilar técnicos de administración de todos los componentes de control?

R: Sí, TAC requiere archivos de tecnología de administración de todos los controladores (vSmart, recopilados de uno en uno), todos los administradores (vManage) y todos los validadores (vBond) para evaluar correctamente su entorno.

A: ¿Cómo determina el TAC si mi sistema se ha visto comprometido?

R: El TAC analiza los archivos técnicos de administración mediante herramientas especializadas para evaluar su entorno en busca de indicadores de compromiso.

A: ¿Hay alguna manera de que pueda realizar mi propio escaneo automatizado usando las herramientas del TAC?

R: Los clientes también pueden utilizar la herramienta de autoservicio "Comprobar aplicabilidad del error", que está integrada en la página de la herramienta de búsqueda de errores para el ID de error de Cisco CSCwt50498 para volver a analizar los técnicos de administración desde los componentes de control.

A: ¿Qué ocurre si se identifican indicadores de compromiso?

R: El TAC se pone en contacto con usted para hablar sobre los siguientes pasos y la orientación específica para su entorno. Cisco no lleva a cabo la remediación en su nombre. TAC proporciona la orientación necesaria para que pueda continuar.

A: ¿Cómo sé qué versión de software fija debo utilizar?

R: Consulte la tabla Versiones fijas de software en este documento. TAC confirma la versión adecuada para su entorno específico.

A: ¿Puedo iniciar la actualización antes de que el TAC analice mis técnicos administrativos?

R: Yes. Recopile técnicos de administración, actualice a una versión fija y luego abra un caso TAC para que TAC pueda escanear los técnicos de administración en busca de indicadores de compromiso.

A: ¿Se espera tiempo de inactividad durante la remediación?

R: El impacto depende de la arquitectura de implementación y de la ruta de remediación. El TAC proporciona orientación sobre cómo minimizar el impacto del servicio durante el proceso.

A: ¿Es necesario actualizar todos los controladores en caso de que no se encuentren indicadores de compromiso?

R: Sí, todos los componentes de control de SD-WAN (vManage, vSmart y vBond) deben actualizarse a una versión de software fija. No es suficiente actualizar sólo un subconjunto de controladores.

A: Tengo una superposición de SD-WAN alojada en la nube. ¿Cuáles son mis opciones de actualización?

R: Para las superposiciones alojadas en la nube, los clientes tienen dos opciones:

1. Compruebe si su entorno está programado para una actualización automatizada. Para ello, vaya a SSP > Detalles de superposición > Cambiar ventanas.
2. Si no desea esperar a la actualización programada, tiene dos opciones:
    - Realice la actualización por sí mismo utilizando las guías de actualización disponibles en este documento.
    - Abra un caso de TAC en espera para su ventana de mantenimiento preferida. El TAC está disponible para ayudarle en caso de que tenga dificultades con la actualización.

A: ¿También necesitamos actualizar los routers de extremo?

R: No, los dispositivos Cisco IOS XE no se ven afectados por este aviso.

P.: Somos una solución de superposición alojada de Cisco. ¿Tenemos que corregir alguna ACL o realizar alguna acción en el SSP?

R: Se recomienda a todos los clientes alojados en Cisco que revisen sus propias reglas de entrada permitidas en SSP y que se aseguren de que sólo se permiten los prefijos necesarios de su parte. Estas reglas son solo para el acceso a la administración y no se aplican a los routers de borde. Revíselas en SSP > Detalles de superposición > Permitir reglas de entrada. Tenga en cuenta que el puerto 22, 830 siempre estaba bloqueado de forma predeterminada el día 0 de aprovisionamiento por parte de Cisco desde el exterior a los controladores alojados en la nube.

A: Estamos en la nube de SD-WAN (anteriormente conocida como nube ofrecida por Cisco Catalyst SD-WAN [CDCS]). ¿A qué versión se va a actualizar?

R: Según la versión actual, los clústeres de nube de SD-WAN se están actualizando según lo previsto o bien ya se han actualizado a las versiones fijas. Estas son las versiones fijas de SD-

WAN Cloud (anteriormente CDCS):

1. Clústeres de Early Adopter = 20.18.2.2 (en realidad es lo mismo que la versión estándar)

2. Clústeres de versión recomendados = 20.15.506 (versión específica de CDCS con correcciones de PSIRT)

Los clientes de la nube de SD-WAN no necesitan realizar ninguna acción de forma eficaz para abordar este PSIRT.

A: Estamos en un arrendatario compartido. ¿A qué versión se va a actualizar?

R: De acuerdo con la versión actual, los arrendatarios compartidos están actualmente programados para actualizarse O ya se han actualizado a las versiones fijas. Estas son las versiones fijas de arrendatario compartido:

1. Clústeres de liberación recomendados = 20.15.5.2

A: ¿Proporciona Cisco TAC servicios de análisis o investigación de diagnóstico para estas vulnerabilidades?

R: El Cisco TAC puede ayudar a los clientes buscando indicadores de compromiso (IoC) relacionados con estas vulnerabilidades. Sin embargo, el TAC no realiza análisis forenses exhaustivos ni investigaciones de incidentes. Para llevar a cabo un trabajo de diagnóstico completo o investigaciones de seguridad detalladas, recomendamos que los clientes contraten a su empresa de respuesta ante incidentes (IR) de terceros preferida.

A: ¿Cuáles son las prácticas recomendadas generales o las formas de reducir las vulnerabilidades de mi superposición de SD-WAN?

R: Consulte la Guía de endurecimiento de SD-WAN de Cisco Catalyst para conocer las mejores prácticas y recomendaciones para reducir las vulnerabilidades en su superposición de SD-WAN.

A: Vemos los registros de un usuario "root" en nuestro sistema. ¿Es esto preocupante?

R: Compruebe qué más está sucediendo en el sistema en ese momento. Estos registros son totalmente esperables. Por ejemplo, los registros de cambio de inicio de sesión del sistema de un usuario "root" se ven cuando se generan admin-techs. Los registros también se pueden ver desde un usuario "root" durante un reinicio.

```
Feb 28 23:03:44 Manager01 SYSMGR[863]: %Viptela-Manager01-sysmgrd-6-INFO-1400002: Notification: system-

       user-name:"root" user-id:245  generated-at:2-28-2026T23:3:44

Feb 28 23:03:47 Manager01 SYSMGR[863]: %Viptela-Manager01-sysmgrd-6-INFO-1400002: Notification: system-
```

```
user-name:"root" user-id:248  generated-at:2-28-2026T23:3:47
```

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).