Guía de inicio rápido: recopilación de datos para diversos problemas de SD-WAN

Contenido

Introducción

Este documento describe varios problemas de SD-WAN junto con los datos relevantes que deben recopilarse de antemano antes de abrir un caso de TAC para mejorar la velocidad de resolución de problemas y/o resolución de problemas. Este documento se divide en dos secciones técnicas principales: Routers vManage y Edge. Los resultados relevantes y la sintaxis de los comandos se proporcionan según el dispositivo en cuestión.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Arquitectura SDWAN de Cisco
- Comprensión general de la solución, incluido el controlador vManage, así como los dispositivos cEdge (routers SD-WAN IOS-XE) y vEdge (routers ViptelaOS)

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Información básica solicitada

- Describa el problema y su impacto en su red y usuarios: Describa un comportamiento esperado.Describa en detalle el comportamiento observado.Prepare un diagrama de topología con direccionamiento si es posible, incluso si se dibuja a mano.
- ¿Cuándo comenzó el problema? Observe el día y la hora en que se observó/notó el problema por primera vez.
- ¿Cuál podría ser el detonador potencial del problema? Documentar cualquier cambio reciente realizado antes de que se iniciara el problema.Tenga en cuenta las acciones o eventos específicos que se hayan producido y que puedan haber provocado el inicio del problema.¿Este problema corresponde a cualquier otro evento o acción de red?
- ¿Cuál es la frecuencia del problema? ¿Ocurrió esto una sola vez?Si no es así, ¿con qué frecuencia ocurre el problema?
- Proporcione información sobre los dispositivos en cuestión: Si se ven afectados dispositivos específicos (no aleatorios), ¿qué tienen en común?System-IP y Site-ID para cada dispositivo.Si el problema se encuentra en un clúster de vManage, proporcione los detalles del nodo (si no los mismos en todos los nodos del clúster).Para los problemas generales dentro de la GUI de vManage, capture todas las capturas de pantalla de un archivo que muestre mensajes de error u otras anomalías/disecciones que deban investigarse.
- Proporcione información sobre los resultados deseados del TAC y sus prioridades: ¿Desea recuperarse de la falla lo antes posible o descubrir la causa raíz de la falla?

vManage

Los problemas aquí descritos son condiciones de problemas comunes notificadas para vManage junto con salidas útiles para cada problema que se deben recopilar además de un archivo **admin-tech**. Para los controladores alojados en la nube, el ingeniero del Technical Assistance Center (TAC) puede tener acceso para recopilar las salidas **admin-tech necesarias** para los dispositivos en función de los comentarios de la sección Información básica solicitada si proporciona un consentimiento explícito para esto. Sin embargo, se recomienda capturar resultados **admin-tech** si los pasos descritos aquí para asegurarse de que los datos contenidos dentro son relevantes para el momento del problema. Esto es específicamente cierto si el problema no es persistente, lo que significa que el problema puede desaparecer para el momento en que se contrate el TAC. Para los controladores in situ**,** se debe incluir **admin-tech** con cada conjunto de datos aquí**.** Para un clúster vManage, asegúrese de capturar un **administrador-tech** para cada nodo del clúster o sólo los nodos afectados.

Lentitud/Lentitud

Informe de problemas: Lentitud al acceder a la GUI de vManage, latencia al realizar operaciones dentro de la GUI, lentitud general o lentitud observada en vManage

Paso 1. Capture 2-3 instancias de una impresión de subproceso, cambie el nombre de cada archivo **de impresión de subproceso** con una designación numérica después de cada uno (observe el uso del nombre de usuario con el que inicia sesión en vManage en la ruta de acceso del archivo), por ejemplo:

```
vManage# request nms application-server jcmd thread-print | save /home/<username>/thread-print.1
```

Paso 2. Inicie sesión en **vshell** y ejecute **vmstat** como se indica a continuación:

```
vManage# vshell
vManage:~$ vmstat 1 10
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
r b swpd free buff cache si so bi bo in cs us sy id wa st
1 0 0 316172 1242608 5867144 0 0 1 22 3 5 6 1 93 0 0
0 0 0 316692 1242608 5867336 0 0 0 8 2365 4136 6 1 93 0 0
0 0 0 316204 1242608 5867344 0 0 0 396 2273 4009 6 1 93 0 0
0 0 0 316780 1242608 5867344 0 0 0 0 2322 4108 5 2 93 0 0
0 0 0 318136 1242608 5867344 0 0 0 0 2209 3957 9 1 90 0 0
0 0 0 318300 1242608 5867344 0 0 0 0 2523 4649 5 1 94 0 0
1 0 0 318632 1242608 5867344 0 0 0 44 2174 3983 5 2 93 0 0
0 0 0 318144 1242608 5867344 0 0 0 64 2182 3951 5 2 94 0 0
0 0 0 317812 1242608 5867344 0 0 0 0 2516 4289 6 1 93 0 0
0 0 0 318036 1242608 5867344 0 0 0 0 2600 4421 8 1 91 0 0
vManage:~$
```

Paso 3. Recopile detalles adicionales de la **vshell**:

```
vManage:~$ top (press '1' to get CPU counts)
vManage:~$ free -h
vManage:~$ df -kh
```

Paso 4. Capture todos los diagnósticos de servicios NMS:

```
vManage# request nms application-server diagnostics
vManage# request nms configuration-db diagnostics
vManage# request nms messaging-server diagnostics
vManage# request nms coordination-server diagnostics
vManage# request nms statistics-db diagnostics
```

Problemas/fallas de API

Informe de problemas: Las llamadas de la API no devuelven ningún dato o los datos correctos, problemas generales al ejecutar consultas

Paso 1. Compruebe la memoria disponible:

```
vManage:~$ free -h
total used free shared buff/cache available
Mem: 31Gi 24Gi 280Mi 60Mi 6.8Gi 6.9Gi
Swap: 0B 0B 0B
vManage:~$
```

Paso 2. Capture de 2 a 3 instancias de una impresión de subproceso con un intervalo de 5 segundos entre ambas, cambie el nombre de cada archivo **de impresión de subproceso** con una designación numérica después de cada ejecución del comando (observe el uso del nombre de usuario con el que inicia sesión en vManage en la ruta de acceso del archivo):

```
vManage# request nms application-server jcmd thread-print | save /home/<username>/thread-print.1
<WAIT 5 SECONDS>
vManage# request nms application-server jcmd thread-print | save /home/<username>/thread-print.2
```

Paso 3. Recopilar detalles de cualquier sesión HTTP activa:

```
vManage# request nms application-server jcmd gc-class-histo | i
io.undertow.server.protocol.http.HttpServerConnection
```

Paso 4. Proporcione estos detalles:

1. Llamadas API ejecutadas

2. Frecuencia de invocación

3. Método de inicio de sesión (es decir, el uso de un único token para ejecutar las llamadas API subsiguientes o el uso de la autenticación básica para ejecutar la llamada y, a continuación, cerrar la sesión)

4. ¿Se está reutilizando el JSESSIONID?

> **Nota** A partir del software vManage 19.2, sólo se admite la autenticación basada en token para las llamadas API. Para obtener más detalles sobre la generación de token, el tiempo de espera y el vencimiento, vea este enlace.

Estadísticas/lentitud de la inspección profunda de paquetes (DPI)

Informe de problemas: Con DPI activado, el procesamiento de estadísticas puede ser lento o introducir lentitud dentro de la GUI de vManage.

Paso 1. Verifique el tamaño de disco asignado para DPI dentro de vManage navegando hasta **Administration > Settings > Statistics Database > Configuration**.

Paso 2. Verifique el estado del índice ejecutando el siguiente comando CLI de vManage:

```
vManage# request nms statistics-db diagnostics
```

Paso 3. Confirme si las llamadas de API relacionadas con las estadísticas de DPI se ejecutan externamente.

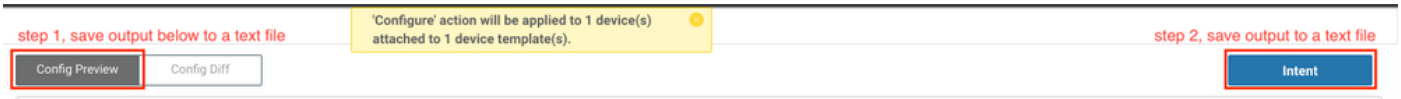
Paso 4. Verifique las estadísticas de E/S del disco con la ayuda de este comando CLI de vManage:

```
vManage# request nms application-server diagnostics
```

Errores de inserción de plantilla

Informe de problemas: La inserción de plantillas o la actualización de plantillas de dispositivos fallan o se agota el tiempo de espera.

Paso 1. Capture **Config Preview** y **Intent** config de vManage antes de hacer clic en el botón **Configurar dispositivos** (ejemplo de navegación que se proporciona aquí):



Paso 2. Habilite **viptela.enable.rest.log** desde la **página logsettings** (debe desactivarse después de capturar la información necesaria):

```
https://<vManage IP>:8443/logsettings.html
```

Paso 3. Si la falla de inserción de la plantilla implica un problema o error de NETCONF, habilite **viptela.enable.device.netconf.log** además del registro REST en el Paso 1. Tenga en cuenta que este registro también se debe inhabilitar después de que se capturen los resultados de los pasos 3 y 4.

Paso 4. Intente asociar de nuevo la plantilla defectuosa de vManage y capture un **admin-tech** usando esta CLI (capture esto para cada nodo de para un clúster):

```
vManage# request admin-tech
```

Paso 5. Proporcione capturas de pantalla de la tarea en vManage y la Diff de configuración para confirmar los detalles de la falla junto con cualquier archivo CSV utilizado para la plantilla.

Paso 6. Incluya detalles sobre la falla y la tarea, incluida la hora de la inserción fallida, **system-ip** del dispositivo que falló y el mensaje de error que ve en la GUI de vManage.

Paso 7. Si se produce una falla en el envío de una plantilla con un mensaje de error informado para la configuración por el propio dispositivo, recopile un **admin-tech** del dispositivo también.

Problemas relacionados con el clúster

Informe de problemas: La inestabilidad del clúster provoca tiempos de espera de la GUI, lentitud u otras anomalías.

Paso 1. Capture el resultado de **server_configs.json** de cada nodo vManage del clúster. Por ejemplo:

```
vmanage# vshell
vmanage:~$ cd /opt/web-app/etc/
vmanage:/opt/web-app/etc$ more server_configs.json | python -m json.tool
{
"clusterid": "",
"domain": "",
"hostsEntryVersion": 12,
"mode": "SingleTenant",
"services": {
"cloudAgent": {
"clients": {
"0": "localhost:8553"
},
"deviceIP": "localhost:8553",
"hosts": {
"0": "localhost:8553"
},
"server": true,
"standalone": false
},
```

```
"container-manager": {
"clients": {
"0": "169.254.100.227:10502"
},
"deviceIP": "169.254.100.227:10502",
"hosts": {
"0": "169.254.100.227:10502"
},
"server": true,
"standalone": false
},
"elasticsearch": {
"clients": {
"0": "169.254.100.227:9300",
"1": "169.254.100.254:9300",
"2": "169.254.100.253:9300"
},
"deviceIP": "169.254.100.227:9300",
"hosts": {
"0": "169.254.100.227:9300",
"1": "169.254.100.254:9300",
"2": "169.254.100.253:9300"
},
"server": true,
"standalone": false
},
"kafka": {
"clients": {
"0": "169.254.100.227:9092",
"1": "169.254.100.254:9092",
"2": "169.254.100.253:9092"
},
"deviceIP": "169.254.100.227:9092",
"hosts": {
"0": "169.254.100.227:9092",
"1": "169.254.100.254:9092",
"2": "169.254.100.253:9092"
},
"server": true,
"standalone": false
},
"neo4j": {
"clients": {
"0": "169.254.100.227:7687",
"1": "169.254.100.254:7687",
"2": "169.254.100.253:7687"
},
"deviceIP": "169.254.100.227:7687",
"hosts": {
"0": "169.254.100.227:5000",
"1": "169.254.100.254:5000",
"2": "169.254.100.253:5000"
},
"server": true,
"standalone": false
},
"orientdb": {
"clients": {},
"deviceIP": "localhost:2424",
"hosts": {},
"server": false,
"standalone": false
},
"wildfly": {
```

```
"clients": {
"0": "169.254.100.227:8443",
"1": "169.254.100.254:8443",
"2": "169.254.100.253:8443"
},
"deviceIP": "169.254.100.227:8443",
"hosts": {
"0": "169.254.100.227:7600",
"1": "169.254.100.254:7600",
"2": "169.254.100.253:7600"
},
"server": true,
"standalone": false
},
"zookeeper": {
"clients": {
"0": "169.254.100.227:2181",
"1": "169.254.100.254:2181",
"2": "169.254.100.253:2181"
},
"deviceIP": "169.254.100.227:2181",
"hosts": {
"0": "169.254.100.227:2888:3888",
"1": "169.254.100.254:2888:3888",
"2": "169.254.100.253:2888:3888"
},
"server": true,
"standalone": false
}
},
"vmanageID": "0"
}
```


Paso 2. Capture detalles sobre qué servicios están habilitados o desactivados para cada nodo. Para ello, navegue hasta **Administration > Cluster Management** en la GUI de vManage.

Paso 3. Confirme el alcance de la capa subyacente en la interfaz del clúster. Para esto, ejecute **ping <ip-address>** desde cada nodo vManage en VPN 0 a la IP de la interfaz de clúster de los otros nodos.

Paso 4. Recopile diagnósticos de todos los servicios NMS para cada nodo vManage del clúster:

```
vManage# request nms application-server diagnostics
vManage# request nms configuration-db diagnostics
vManage# request nms messaging-server diagnostics
vManage# request nms coordination-server diagnostics
vManage# request nms statistics-db diagnostics
```

Perímetro (vEdge/CEdge)

Los problemas aquí descritos son las condiciones de problemas habituales notificadas para los dispositivos periféricos, junto con salidas útiles para cada una de las que se deben recopilar. Asegúrese de que para cada problema se recopile un **administrador-técnico** para todos los dispositivos Edge necesarios y relevantes. Para los controladores alojados en la nube, el TAC puede tener acceso para recopilar las salidas de tecnología de administración necesarias para los dispositivos según los comentarios de la sección **Información básica solicitada**. Sin embargo, al igual que con vManage, puede ser necesario capturarlos antes de abrir un caso del TAC para asegurarse de que los datos contenidos en el sean relevantes para el momento del problema. Esto es específicamente cierto si el problema no es persistente, lo que significa que el problema

puede desaparecer para el momento en que se contrate el TAC.

Conexiones de control que no se forman entre el dispositivo y el controlador

Informe de problemas: Conexión de control que no se está formando de un vEdge/cEdge a uno o más controladores

Paso 1. Identifique el error local/remoto de la falla de conexión de control:

- Para vEdge: salida del comando **show control connections-history**.
- Para cEdge: salida del comando **show sdwan control connection-history**.

Paso 2. Confirme el estado de los TLOC y que todos y cada uno aparezcan 'up':

- Para vEdge: salida del comando **show control local-properties**.
- Para cEdge: salida del comando **show sdwan control local-properties**.

Paso 3. Para los errores relacionados con los tiempos de espera o las fallas de conexión (es decir, DCONFAIL o VM_TMO), tome capturas del plano de control tanto en el dispositivo de borde como en el controlador en cuestión:

- Para controladores:

```
vManage# tcpdump vpn 0 interface eth1 options "-vvvvvv host 192.168.44.6"
tcpdump -p -i eth1 -s 128 -vvvvvv host 192.168.44.6 in VPN 0
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 128 bytes
20:02:07.427064 IP (tos 0xc0, ttl 61, id 50139, offset 0, flags [DF], proto UDP (17), length
168)
192.168.44.6.12346 > 192.168.40.1.12346: UDP, length 140
20:02:07.427401 IP (tos 0xc0, ttl 64, id 37220, offset 0, flags [DF], proto UDP (17), length
210)
192.168.40.1.12346 > 192.168.44.6.12346: UDP, length 182
```

- Para vEdge:

```
vEdge-INET-Branch2# tcpdump vpn 0 interface ge0/2 options "-vvvvvv host 192.168.40.1"
tcpdump -p -i ge0_2 -vvvvvv host 192.168.40.1 in VPN 0
tcpdump: listening on ge0_2, link-type EN10MB (Ethernet), capture size 262144 bytes
20:14:16.136276 IP (tos 0xc0, ttl 64, id 55858, offset 0, flags [DF], proto UDP (17), length
277)
10.10.10.1 > 192.168.40.1.12446: [udp sum ok] UDP, length 249
20:14:16.136735 IP (tos 0xc0, ttl 63, id 2907, offset 0, flags [DF], proto UDP (17), length 129)
192.168.40.1.12446 > 10.10.10.1.12346: [udp sum ok] UDP, length 101
```

- Para cEdge (la captura siguiente supone que el dispositivo se movió al modo CLI y se creó una lista de control de acceso (ACL) llamada **CTRL-CAP** para filtrar; vea más detalles en el ejemplo de captura de EPC en el **escenario Rendimiento de la Aplicación/Red**):

```
cEdge-Branch1#config-transaction
cEdge-Branch1(config)# ip access-list extended CTRL-CAP
cEdge-Branch1(config-ext-nacl)# 10 permit ip host 10.10.10.1 host 192.168.40.1
cEdge-Branch1(config-ext-nacl)# 20 permit ip host 192.168.40.1 host 10.10.10.1
cEdge-Branch1(config-ext-nacl)# commit
cEdge-Branch1(config-ext-nacl)# end

cEdge-Branch1#monitor capture CAP control-plane both access-list CTRL-CAP buffer size 10
cEdge-Branch1#monitor capture CAP start
```

```
cEdge-Branch1#show monitor capture CAP buffer brief
------------------------------------------------------------------------
# size timestamp source destination dscp protocol
------------------------------------------------------------------------
0 202 0.000000 192.168.20.1 -> 50.50.50.3 48 CS6 UDP
1 202 0.000000 192.168.20.1 -> 50.50.50.4 48 CS6 UDP
2 220 0.000000 50.50.50.3 -> 192.168.20.1 48 CS6 UDP
3 66 0.000992 192.168.20.1 -> 50.50.50.3 48 CS6 UDP
4 220 0.000992 50.50.50.4 -> 192.168.20.1 48 CS6 UDP
5 66 0.000992 192.168.20.1 -> 50.50.50.4 48 CS6 UDP
6 207 0.015991 50.50.50.1 -> 12.12.12.1 48 CS6 UDP
```

Paso 4. Para ver otros errores observados en los resultados del historial de conexiones de control y para obtener más detalles sobre los problemas descritos, consulte la siguiente guía .

Control de las conexiones que se alternan entre el dispositivo de borde y el controlador

Informe de problemas: Una o más conexiones de control se alternan entre un vEdge/cEdge y uno o más controladores. Esto puede ser frecuente, intermitente o aleatorio por naturaleza.

- Las inestabilidades de la conexión de control son generalmente el resultado de la pérdida de paquetes o los problemas de reenvío entre un dispositivo y un controlador. A menudo, esto estará ligado a errores **TMO**, dependiendo de la direccionalidad de la falla. Para comprobar esto más a fondo, primero verifique el motivo de la inestabilidad: Para vEdge/controladores: salida del comando **show control connections-history**.Para cEdge: salida del comando **show sdwan control connection-history**.
- Confirme el estado de los TLOC y que todos y cada uno aparezcan 'up' cuando se produzca la inestabilidad: Para vEdge: salida del comando **show control local-properties**.Para cEdge: salida del comando **show sdwan control local-properties**.
- Recopile capturas de paquetes tanto en el controlador o los dispositivos periféricos. Consulte la sección **Conexiones de control que no se forman entre el dispositivo y el controlador** para obtener detalles sobre los parámetros de captura para cada lado.

Sesiones de detección de reenvío bidireccional (BFD) que no se forman ni se inmutan entre dispositivos periféricos

Informe de problemas: La sesión BFD está inactiva o se está inestabilizando entre dos dispositivos periféricos.

Paso 1. Recopile el estado de la sesión BFD en cada dispositivo:

- Para vEdge: salida del comando **show bfd sessions**.
- Para cEdge: resultado del comando **show sdwan bfd sessions**.

Paso 2. Recopile los recuentos de paquetes Rx y Tx en cada router de borde:

- Para vEdge: salida del comando **show tunnel statistics bfd**.
- Para cEdge: salida del comando **show platform hardware qfp active feature bfd datapath sdwan summary**.

Paso 3. Si los contadores no aumentan para la sesión BFD en un extremo del túnel en los resultados anteriores, las capturas se pueden realizar usando ACL para confirmar si los paquetes

se reciben localmente. Puede encontrar más detalles sobre esto junto con otras validaciones que se pueden hacer aquí .

Desperfectos del dispositivo

Informe de problemas: El dispositivo se recarga de forma inesperada y se descartan los problemas de alimentación. Las indicaciones del dispositivo son que se ha estrellado potencialmente.

Paso 1. Verifique el dispositivo para confirmar si se observó un desperfecto o una recarga inesperada:

- Para vEdge: salida del comando **show reboot history**.
- Para cEdge: salida del comando **show sdwan reboot history**.
- De manera alternativa, navegue hasta **Monitor > Network**, seleccione el dispositivo y luego navegue hasta **System Status > Reboot** para confirmar si se vieron recargas inesperadas.

Paso 2. Si se confirma, capture un admin-tech del dispositivo a través de vManage navegando a **Herramientas > Comandos Operativos**. Una vez allí, seleccione el botón **Opciones** para el dispositivo y seleccione **Admin Tech**. Asegúrese de que todas las casillas de verificación estén marcadas, que incluirán todos los registros y archivos de núcleo del dispositivo.

Rendimiento de la aplicación/red degradado o que falla entre sitios

Informe de problemas: La aplicación no funciona/las páginas HTTP no se cargan, la lentitud/latencia en el rendimiento, las fallas después de realizar cambios de política o configuración

Paso 1. Identifique el par IP de origen/destino para una aplicación o flujo que muestra el problema.

Paso 2. Determine todos los dispositivos Edge en la trayectoria y recopile un **admin-tech** de cada uno a través de vManage.

Paso 3. Tome una captura de paquetes en los dispositivos de borde en cada sitio para este flujo cuando se vea el problema:

- Para vEdge: Habilite el flujo de datos en el campo **Administration > Settings** For **Hostname**, ingrese la IP del sistema de vManage. Para **VPN**, ingrese **0**Asegúrese de que HTTPS esté habilitado bajo la configuración **allow-service** de la interfaz vManage VPN 0.Siga los pasos aquí para capturar el tráfico en la interfaz VPN del lado del servicio.
- Para cEdge: Mueva el/los borde(s) a modo CLI a través de **Configuration > Devices > Change Mode > CLI mode**En el borde(s) de la red, configure una ACL extendida para que coincida el tráfico bidireccionalmente. Haga esto lo más específico posible para incluir protocolo y puerto para limitar el tamaño y los datos en la captura.
- Configure la captura de paquetes integrada (EPC) para la interfaz del lado del servicio en ambas direcciones, utilizando la ACL creada en (b) para filtrar el tráfico. La captura puede exportarse al formato PCAP y copiarse del cuadro. Aquí se proporciona una configuración de ejemplo para GigabitEthernet0/0/0 en un router mediante una ACL denominada **BROKEN-FLOW**:

```
monitor capture CAP interface GigabitEthernet0/0/0 both access-list BROKEN-FLOW buffer size 10
monitor capture CAP start

show monitor capture CAP parameter
show monitor capture CAP buffer [brief]

monitor capture CAP export bootflash:cEdge1-Broken-Flow.pcap
```

- Configure Packet Trace para el tráfico en ambas direcciones, usando la ACL creada en (b) para filtrar el tráfico. Abajo se brinda un ejemplo de configuración:

```
debug platform packet-trace packet 2048 fia-trace
debug platform packet-trace copy packet input l3 size 2048
debug platform condition ipv4 access-list BROKEN-FLOW both
debug platform condition start

show platform packet-trace summary
show platform packet-trace packet all | redirect bootflash:cEdge1-PT-OUTPUT.txt
```

Paso 4. Si es posible, repita el paso 3 en un escenario en funcionamiento para la comparación.

Sugerencia: si no hay otras formas de copiar directamente los archivos correspondientes de cEdge, los archivos se pueden copiar en vManage primero mediante el método descrito aquí. Ejecute el comando en vManage:
request execute scp -P 830 <username>@<cEdge system-IP>:/bootflash/<filename> .
Este archivo se guardará en el directorio **/home/<username>/** para el nombre de usuario que utilizó para iniciar sesión en vManage. A partir de ahí, puede utilizar el protocolo de copia segura (SCP) del protocolo de transferencia segura de archivos (SFTP) para copiar un archivo de vManage mediante un cliente SCP/SFTP de terceros o una CLI de máquina Linux/Unix con utilidades OpenSSH.