Guia de início rápido - Coleta de dados para vários problemas de SD-WAN

Contents

Introduction

Este documento descreve vários problemas de SD-WAN junto com dados relevantes que devem ser coletados antecipadamente antes de você abrir um caso de TAC para melhorar a velocidade da solução de problemas e/ou resolução de problemas. Este documento está dividido em duas seções técnicas principais: Roteadores vManage e Edge. As saídas relevantes e a sintaxe de comando são fornecidas dependendo do dispositivo em questão.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Arquitetura SDWAN da Cisco
- Compreensão geral da solução, incluindo o controlador vManage, bem como o cEdge (roteadores IOS-XE SD-WAN) e os dispositivos vEdge (roteadores ViptelaOS)

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações básicas solicitadas

- Descrever o problema e seu impacto na rede e nos usuários: Descrever um comportamento esperado.Descrever em detalhes o comportamento observado.Prepare um diagrama de topologia com endereçamento, se possível, mesmo que ele seja desenhado à mão.
- Quando o problema começou? Observe o dia e a hora em que o problema foi observado/observado pela primeira vez.
- O que poderia ser um possível desencadeador do problema? Documente todas as alterações recentes feitas antes de quando o problema começou.Observe todas as ações ou eventos específicos que possam ter disparado o problema para ser iniciado.Esse problema corresponde a outros eventos ou ações de rede?
- Qual é a frequência do problema? Foi uma ocorrência única?Em caso negativo, com que frequência o problema ocorre?
- Forneça informações sobre o(s) dispositivo(s) em questão: Se dispositivos específicos são afetados (não aleatórios), o que eles têm em comum?System-IP e Site-ID para cada dispositivo.Se o problema estiver em um cluster vManage, forneça os detalhes do nó (se não for o mesmo em todos os nós do cluster).Para problemas gerais dentro da GUI do vManage, capture todas as capturas de tela em um arquivo que mostre mensagens de erro ou outras anomalias/dispartes que precisam ser investigadas.
- Forneça informações sobre os resultados desejados do TAC e suas prioridades: Deseja se recuperar da falha o mais rápido possível ou descobrir a causa raiz da falha?

vManage

Os problemas aqui são condições comuns de problemas relatadas para o vManage, juntamente com saídas úteis para cada problema que deve ser coletado além de um arquivo **admin-tech**. Para controladores hospedados na nuvem, o engenheiro do Technical Assistance Center (TAC) pode ter acesso para coletar as saídas **administrativas necessárias** para os dispositivos com base no feedback na seção Informações básicas solicitadas, se você fornecer consentimento explícito para isso. No entanto, recomendamos capturar as saídas **de tecnologia administrativa** se as etapas descritas aqui para garantir que os dados contidos no são relevantes para o momento do problema. Isso é especificamente verdade se o problema não for persistente, o que significa que o problema pode desaparecer quando o TAC estiver ativado. Para controladores no local**,** um **admin-tech** também deve ser incluído em cada conjunto de dados aqui**.** Para um cluster vManage, certifique-se de capturar um **admin-tech** para cada nó no cluster ou apenas para o(s) nó(s) afetado(s).

Lentidão/Sonolência

Relatório de problemas: Lentidão no acesso à GUI do vManage, latência ao executar operações dentro da GUI, lentidão geral ou lentidão observados no vManage

Etapa 1. Capturar de 2 a 3 instâncias de uma impressão de thread, renomeie cada arquivo **de impressão de thread** com uma designação numérica após cada (observe o uso do nome de usuário com o qual você faz login no vManage no caminho do arquivo), exemplo:

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

Etapa 2. Faça login no **vshell** e execute **vmstat** como abaixo:

```
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:~$
```

Etapa 3. Colete detalhes adicionais do **vshell**:

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

Etapa 4. Capturar todos os diagnósticos de serviços do 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
```

Falhas/Problemas de API

Relatório de problemas: As chamadas de API não retornam nenhum dado ou os dados corretos, problemas gerais que executam consultas

Etapa 1. Verifique a memória disponível:

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

Etapa 2. Capturar 2 a 3 instâncias de uma impressão de thread com um intervalo de 5 segundos entre elas, renomeie cada arquivo **de impressão de thread** com uma designação numérica após cada execução do comando (observe o uso do nome de usuário com o qual você faz login no vManage no caminho do arquivo):

```
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
```

Etapa 3. Coletar detalhes para quaisquer sessões HTTP ativas:

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

Etapa 4. Forneça estes detalhes:

1. Chamadas de API executadas

2. Frequência de chamada

3. Método de login (ou seja, uso de um único token para executar chamadas de API subsequentes ou uso da autenticação básica para executar a chamada e, em seguida, fazer logoff)

4. O JSESSIONID está sendo reutilizado?

> **Observação** A partir do software vManage 19.2, somente a autenticação baseada em token é suportada para chamadas de API. Para obter mais detalhes sobre geração de token, tempo limite e expiração, consulte este link.

Estatísticas de inspeção profunda de pacotes (DPI)/lentidão

Relatório de problemas: Com o DPI ativado, o processamento de estatísticas pode ser lento ou introduzir lentidão dentro da GUI do vManage.

Etapa 1. Verifique o tamanho do disco alocado para DPI dentro do vManage navegando até **Administration > Settings > Statistics Database > Configuration**.

Etapa 2. Verifique a integridade do índice executando o seguinte comando CLI no vManage:

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

Etapa 3. Confirme se as chamadas de API relacionadas às estatísticas de DPI são executadas externamente.

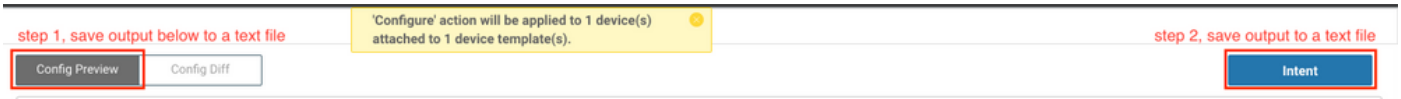
Etapa 4. Verifique as estatísticas de E/S do disco com a ajuda deste comando CLI do vManage:

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

Falhas de envio de modelo

Relatório de problemas: O envio de modelo ou a atualização de modelo de dispositivo falham ou expiram.

Etapa 1. Capture o **Config Preview** e o **Intent** config do vManage antes de clicar no botão **Configurar dispositivos** (exemplo de navegação fornecido aqui):



Etapa 2. Ative **viptela.enable.rest.log** na página **logsettings** (isso deve ser desativado após a captura das informações necessárias):

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

Etapa 3. Se a falha de envio do modelo envolver um problema ou erro NETCONF, ative **viptela.enable.device.netconf.log** além do registro REST na Etapa 1. Observe que esse log também deve ser desativado depois que as saídas das Etapas 3 e 4 forem capturadas.

Etapa 4. Tente anexar o modelo com falha novamente a partir do vManage e capture um **admin-tech** usando esta CLI (capture isso para cada nó de para um cluster):

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

Etapa 5. Forneça capturas de tela da tarefa no vManage e no Config Diff para confirmar os detalhes da falha, juntamente com todos os arquivos CSV usados para o modelo.

Etapa 6. Inclua detalhes sobre a falha e a tarefa, incluindo o tempo do envio com falha, o **system-ip** do dispositivo que falhou e a mensagem de erro exibida na GUI do vManage.

Passo 7. Se uma falha de envio de modelo ocorrer com uma mensagem de erro relatada para a configuração pelo próprio dispositivo, colete um **admin-tech** também do dispositivo.

Problemas relacionados ao cluster

Relatório de problemas: Instabilidade de cluster que leva a timeouts de GUI, lentidão ou outras anomalias.

Etapa 1. Capture a saída de **server_configs.json** de cada nó do vManage no cluster. Por exemplo:

```
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"
}
```


Etapa 2. Capture detalhes sobre quais serviços estão habilitados ou desabilitados para cada nó. Para isso, navegue até **Administration > Cluster Management** na GUI do vManage.

Etapa 3. Confirme a acessibilidade da base na interface do cluster. Para isso, execute **ping <ip-address>** de cada nó do vManage na VPN 0 para o IP da interface de cluster dos outros nós.

Etapa 4. Colete diagnósticos de todos os serviços NMS para cada nó do vManage no cluster:

```
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
```

Borda (vEdge/cEdge)

Os problemas aqui são condições comuns de problemas relatadas para dispositivos Edge, juntamente com saídas úteis para cada um que deve ser coletado. Certifique-se de que, para cada problema, um **admin-tech** seja coletado para todos os dispositivos Edge necessários e relevantes. Para controladores hospedados na nuvem, o TAC pode ter acesso para coletar as saídas administrativas necessárias para os dispositivos com base no feedback na seção **Informações básicas solicitadas**. No entanto, como no vManage, pode ser necessário capturá-los antes de abrir um caso do TAC para garantir que os dados contidos no sejam relevantes para o momento do problema. Isso é especificamente verdade se o problema não for persistente, o que significa que o problema pode desaparecer quando o TAC estiver ativado.

Conexões de controle não formadas entre dispositivo e controlador

Relatório de problemas: Conexão de controle que não está formando de um vEdge/cEdge para um ou mais dos controladores

Etapa 1. Identifique o erro local/remoto da falha de conexão de controle:

- Para vEdge: saída do comando **show control connections-history**.
- Para cEdge: saída do comando **show sdwan control connection-history**.

Etapa 2. Confirme o estado das TLOCs e se todas e quaisquer mostram 'up':

- Para vEdge: saída do comando **show control local-properties**.
- Para cEdge: saída do comando **show sdwan control local-properties**.

Etapa 3. Para erros em relação a falhas de tempo limite ou de conexão (ou seja, DCONFAIL ou VM_TMO), faça capturas de plano de controle no dispositivo de borda e no controlador em questão:

- 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 o cEdge (a captura abaixo assume que o dispositivo foi movido para o modo CLI e uma ACL (Access Control List, lista de controle de acesso) chamada **CTRL-CAP** foi criada para filtrar - consulte mais detalhes no exemplo de captura EPC no cenário **Desempenho de aplicativo/rede**):

```
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
```

Etapa 4. Para outros erros observados nas saídas do histórico de conexões de controle e para obter mais detalhes sobre os problemas descritos, consulte o seguinte guia .

Conexões de controle oscilando entre o dispositivo de borda e o controlador

Relatório de problemas: Uma ou mais conexões de controle oscilam entre um vEdge/cEdge e um ou mais controladores. Isso pode ser de natureza frequente, intermitente ou aleatória.

- Os flaps de conexão de controle são geralmente o resultado de problemas de perda ou encaminhamento de pacotes entre um dispositivo e um controlador. Muitas vezes, isso será associado a erros **de TMO**, dependendo da diretoria da falha. Para verificar mais detalhadamente, primeiro verifique o motivo da aba: Para vEdge/controladores: saída do comando **show control connections-history**.Para cEdge: saída do comando **show sdwan control connection-history**.
- Confirme o estado das TLOCs e que todas e todas aparecem como 'up' quando a oscilação está ocorrendo: Para vEdge: saída do comando **show control local-properties**.Para cEdge: saída do comando **show sdwan control local-properties**.
- Colete capturas de pacotes no(s) controlador(es) e no dispositivo de borda. Consulte a seção **Conexões de controle não formando entre dispositivo e controlador** para obter detalhes sobre os parâmetros de captura de cada lado.

Sessões Bidirecionais de Detecção de Encaminhamento (BFD - Bidirectional Forming) que não se formam nem oscilam entre dispositivos de borda

Relatório de problemas: A sessão de BFD está inoperante ou está oscilando para cima e para baixo entre dois dispositivos de borda.

Etapa 1. Colete o estado da sessão BFD em cada dispositivo:

- Para vEdge: saída do comando **show bfd sessions**.
- Para cEdge: saída do comando **show sdwan bfd sessions**.

Etapa 2. Coletar contagens de pacotes Rx e Tx em cada roteador de borda:

- Para vEdge: saída do comando **show tunnel statistics bfd**.
- Para cEdge: saída do comando **show platform hardware qfp ative feature bfd datapath sdwan summary**.

Etapa 3. Se os contadores não aumentam para a sessão BFD em uma extremidade do túnel nas saídas acima, as capturas podem ser feitas usando ACLs para confirmar se os pacotes estão sendo recebidos localmente. Mais detalhes sobre isso, juntamente com outras validações que podem ser feitas, podem ser encontrados aqui .

Travamentos de dispositivo

Relatório de problemas: Dispositivo recarregado inesperadamente e problemas com energia estão excluídos. As indicações do dispositivo são que ele pode ter travado.

Etapa 1. Verifique o dispositivo para confirmar se um travamento ou recarga inesperada foi observada:

- Para vEdge: saída do comando **show reboot history**.
- Para cEdge: saída do comando **show sdwan reboot history**.
- Como alternativa, navegue para **Monitor > Rede**, selecione o dispositivo e navegue até **Status do sistema > Reinicialização** para confirmar se alguma recarga inesperada foi detectada.

Etapa 2. Se confirmado, capture um admin-tech do dispositivo através do vManage navegando para **Ferramentas > Comandos operacionais**. Depois disso, selecione o botão **Opções** do dispositivo e selecione **Admin Tech**. Verifique se todas as caixas de seleção estão marcadas, o que incluirá todos os registros e arquivos principais no dispositivo.

Desempenho de aplicativo/rede degradado ou com falha entre locais

Relatório de problemas: O aplicativo não funciona/as páginas HTTP não são carregadas, lentidão/latência no desempenho, falhas depois de fazer alterações na política ou na configuração

Etapa 1. Identifique o par IP origem/destino de um aplicativo ou fluxo que exibe o problema.

Etapa 2. Determine todos os dispositivos Edge no caminho e colete um **admin-tech** de cada um através do vManage.

Etapa 3. Faça uma captura de pacotes nos dispositivos de borda de cada local para esse fluxo quando o problema for visto:

- Para vEdge: Ative o fluxo de dados no campo **Administration > Settings** for **Hostname**, insira o IP do sistema do vManage. Para **VPN**, digite **0**Certifique-se de que o HTTPS esteja ativado na configuração **allow-service** da interface do vManage VPN 0.Siga as etapas aqui para capturar o tráfego na interface VPN do lado do serviço.
- Para cEdge: Mova o(s) cEdge(s) para o modo CLI via **Configuration > Devices > Change Mode > CLI mode**No(s) cEdge(s), configure uma ACL estendida para corresponder o tráfego bidirecionalmente. Tornar isso o mais específico possível para incluir protocolo e porta para limitar o tamanho e os dados na captura.
- Configure Embedded Packet Capture (EPC) para a interface do lado do serviço em ambas as direções, usando a ACL criada em (b) para filtrar o tráfego. A captura pode ser exportada para o formato PCAP e copiada da caixa. Um exemplo de configuração é fornecido aqui para GigabitEthernet0/0/0 em um roteador usando uma ACL chamada **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 o Packet Trace para o tráfego em ambas as direções, usando a ACL criada em (b) para filtrar o tráfego. Uma configuração de exemplo é fornecida a seguir:

```
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
```

Etapa 4. Se possível, repita a Etapa 3 em um cenário de trabalho para comparação.

Dica: se não houver outras maneiras de copiar os arquivos correspondentes diretamente do cEdge, os arquivos poderão ser copiados para o vManage primeiro usando o método descrito aqui. Execute o comando no vManage:
request execute scp -P 830 <username>@<cEdge system-IP>:/bootflash/<filename> .
Esse arquivo será armazenado no diretório **/home/<nome de usuário>/** do nome de usuário usado para fazer login no vManage. A partir daí, você pode usar o protocolo de cópia segura (SCP - Secure Copy Protocol) do protocolo de transferência de arquivos seguros (SFTP - Secure File Transfer Protocol) para copiar o arquivo de um vManage usando um cliente SCP/SFTP de terceiros ou uma CLI da máquina Linux/Unix com utilitários OpenSSH.