Schnellstartanleitung - Datenerfassung für verschiedene SD-WAN-Probleme

Inhalt

Einführung

In diesem Dokument werden mehrere SD-WAN-Probleme sowie relevante Daten beschrieben, die vor dem Öffnen eines TAC-Tickets erfasst werden müssen, um die Fehlerbehebung und/oder Problembehebung zu beschleunigen. Dieses Dokument gliedert sich in zwei technische Hauptabschnitte: vManage- und Edge-Router. Relevante Ausgaben und Befehlssyntax werden je nach Gerät bereitgestellt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco SDWAN-Architektur
- Allgemeine Kenntnisse der Lösung, einschließlich vManage-Controller sowie cEdge- (IOS-XE SD-WAN-Router) und vEdge-Geräte (ViptelaOS-Router)

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Basisinformationen angefordert

- Beschreiben Sie das Problem und seine Auswirkungen auf Ihr Netzwerk und Ihre Benutzer: Beschreiben Sie ein erwartetes Verhalten.Beschreiben Sie detailliertes beobachtetes Verhalten.Erstellen Sie ein Topologiediagramm mit der Adressierung, wenn möglich, auch wenn es handgezeichnet ist.
- Wann hat das Problem begonnen? Beachten Sie, wann und an welchem Tag das Problem erstmals beobachtet/bemerkt wurde.
- Was könnte ein potenzieller Auslöser für das Problem sein? Dokumentieren Sie alle vor dem Beginn des Problems vorgenommenen Änderungen.Notieren Sie alle Aktionen oder Ereignisse, die aufgetreten sind und die das Problem möglicherweise zum Starten ausgelöst haben.Entspricht dieses Problem anderen Netzwerkereignissen oder -aktionen?
- Wie häufig tritt das Problem auf? War dies ein einmaliges Ereignis?Falls nicht, wie oft tritt das Problem auf?
- Geben Sie Informationen zu dem bzw. den betreffenden Geräten an: Welche Gemeinsamkeiten haben sie, wenn bestimmte Geräte betroffen sind (nicht zufällig)?System-IP und Standort-ID für jedes Gerät.Wenn sich das Problem auf einem vManage-Cluster befindet, geben Sie die Knotendetails an (wenn nicht alle Knoten im Cluster identisch sind).Bei allgemeinen Problemen innerhalb der vManage-GUI können Sie alle Screenshots in eine Datei aufnehmen, die Fehlermeldungen oder andere Anomalien/Ungleichheiten anzeigt, die untersucht werden müssen.
- Geben Sie Informationen zu den gewünschten Ergebnissen des TAC und Ihren Prioritäten an: Möchten Sie den Ausfall so schnell wie möglich beheben oder die Ursache des Fehlers ermitteln?

vManage

Die Probleme sind allgemeine Problembedingungen, die für vManage gemeldet werden, sowie nützliche Ausgaben für jedes Problem, das zusätzlich zu einer **admin-tech-**Datei(en) erfasst werden muss. Für Cloud-gehostete Controller kann der Techniker des Technical Assistance Center (TAC) auf der Grundlage des Feedbacks im Abschnitt "angeforderte Basisinformationen" die erforderlichen **Admin-Tech-**Ausgaben für die Geräte sammeln, wenn Sie dies ausdrücklich genehmigen. Wir empfehlen jedoch, **admin-tech-**Ausgaben zu erfassen, wenn die hier beschriebenen Schritte sicherstellen, dass die darin enthaltenen Daten für die Zeit des Problems relevant sind. Dies gilt vor allem, wenn das Problem nicht beständig ist, d.h. das Problem kann verschwinden, wenn das TAC aktiviert ist. Für Vor-Ort-Controller muss hier ein **Admin-Tech** mit jedem Datensatz enthalten sein**.** Stellen Sie bei einem vManage-Cluster sicher, dass Sie eine **admin-tech** für jeden Knoten im Cluster oder nur für die betroffenen Knoten erfassen.

Langsamkeit/Langsamkeit

Problembericht: Langsamer Zugriff auf die vManage-GUI, Latenz bei Operationen innerhalb der GUI, allgemeine Langsamkeit oder Langsamkeit bei vManage

Schritt 1: Erfassen Sie 2 bis 3 Instanzen eines Threaddrucks, benennen Sie jede **Threadprint-**Datei mit einer numerischen Bezeichnung nach jedem neu (beachten Sie die Verwendung des Benutzernamens, mit dem Sie sich im Dateipfad bei vManage anmelden), z. B.:

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

Schritt 2: Melden Sie sich bei **vshell an**, und führen Sie **vmstat** wie folgt aus:

```
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:~$
```

Schritt 3: Sammeln Sie weitere Details aus der **vshell**:

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

Schritt 4: Erfassen Sie alle NMS-Servicediagnosen:

```
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
```

API-Fehler/Probleme

Problembericht: API-Aufrufe senden keine Daten oder die richtigen Daten zurück, generelle Probleme beim Durchführen von Abfragen

Schritt 1: Überprüfen Sie den verfügbaren Speicher:

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

Schritt 2: Erfassen Sie 2 bis 3 Instanzen eines Threaddrucks mit einer Lücke von 5 Sekunden dazwischen, und benennen Sie jede **Thread-Print-**Datei nach jedem Ausführen des Befehls mit einer numerischen Bezeichnung um (beachten Sie die Verwendung des Benutzernamens, mit

dem Sie sich im Dateipfad bei vManage anmelden):

```
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
```

Schritt 3: Details zu aktiven HTTP-Sitzungen sammeln:

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

Schritt 4: Machen Sie folgende Angaben:

1. Ausführung von API-Anrufen

2. Häufigkeit der Anrufe

3. Anmeldungsmethode (d. h. Verwendung eines einzigen Tokens zur Ausführung nachfolgender API-Aufrufe oder Verwendung einer Standardauthentifizierung zur Ausführung des Anrufs und anschließender Abmeldung)

4. Wird die JSESSIONID wiederverwendet?

> **Hinweis** Ab der Version 19.2 vManage-Software wird für API-Aufrufe nur die Token-basierte Authentifizierung unterstützt. Weitere Informationen zur Erstellung, zum Timeout und zum Ablauf von Token finden Sie unter diesem Link.

Status/Langsamkeit der Deep Packet Inspection (DPI)

Problembericht: Wenn DPI aktiviert ist, kann die Verarbeitung von Statistiken langsam sein oder zu einer Verlangsamung innerhalb der vManage-GUI führen.

Schritt 1: Überprüfen Sie die für DPI in vManage reservierte Festplattengröße, indem Sie zu **Administration > Settings > Statistics Database > Configuration** navigieren.

Schritt 2: Überprüfen Sie den Indexzustand, indem Sie den folgenden CLI-Befehl von vManage ausführen:

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

Schritt 3: Überprüfen Sie, ob API-Aufrufe im Zusammenhang mit DPI-Statistiken extern ausgeführt werden.

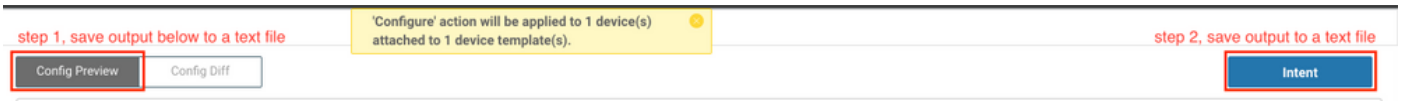
Schritt 4: Überprüfen Sie die Datenträger-E/A-Statistiken mithilfe dieses CLI-Befehls von vManage:

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

Vorlagenpush-Fehler

Problembericht: Vorlagenpush oder Gerätevorlagenaktualisierung schlägt fehl oder ist abgelaufen.

Schritt 1: Erfassen Sie die **Konfigurationsvorschau** und die Intent-Konfiguration von vManage, bevor Sie auf die Schaltfläche **Geräte konfigurieren klicken** (Navigationsbeispiel hier):



Schritt 2: Aktivieren Sie **viptela.enable.rest.log** von der **Anmeldesettings-**Seite (dieser muss nach dem Erfassen der erforderlichen Informationen deaktiviert werden):

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

Schritt 3: Wenn bei dem Vorlagenpush-Fehler ein NETCONF-Problem oder -Fehler auftritt, aktivieren Sie **viptela.enable.device.netconf.log** zusätzlich zum REST-Protokoll in Schritt 1. Beachten Sie, dass dieses Protokoll auch deaktiviert werden muss, nachdem die Ausgaben aus Schritt 3 und Schritt 4 erfasst wurden.

Schritt 4: Versuchen Sie, die ausgefallene Vorlage erneut über vManage anzufügen und mithilfe dieser CLI einen **Admin-Techniker** zu erfassen (erfassen Sie diesen für jeden Knoten von für einen Cluster):

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

Schritt 5: Geben Sie Screenshots von der Aufgabe in vManage und im Konfigurationsdiff an, um die Fehlerdetails sowie alle für die Vorlage verwendeten CSV-Dateien zu bestätigen.

Schritt 6: Enthalten sind Details zum Ausfall und zur Aufgabe, einschließlich der Uhrzeit des fehlgeschlagenen Push-Vorgangs, der **System-IP-Adresse** des Geräts, das ausgefallen ist, und der Fehlermeldung, die Sie in der vManage-GUI sehen.

Schritt 7: Wenn ein Vorlagenpush-Fehler auftritt und eine Fehlermeldung angezeigt wird, die das Gerät selbst für die Konfiguration gemeldet hat, holen Sie auch einen **Admin-Tech** vom Gerät ein.

Cluster-bezogene Probleme

Problembericht: Instabilität der Cluster führt zu GUI-Timeouts, Verzögerungen oder anderen Anomalien.

Schritt 1: Erfassen Sie die Ausgabe von **server_configs.json** von jedem vManage-Knoten im Cluster. Beispiel:

```
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"
}
```


Schritt 2: Erfassen Sie Details, welche Services für jeden Knoten aktiviert oder deaktiviert sind. Navigieren Sie hierzu in der vManage-GUI zu **Administration > Cluster Management**.

Schritt 3: Bestätigen Sie die Erreichbarkeit des Basisbereichs auf der Cluster-Schnittstelle. Führen Sie dazu **ping <ip-address>** von jedem vManage-Knoten in VPN 0 zur Cluster-Schnittstellen-IP der anderen Knoten aus.

Schritt 4: Sammeln Sie Diagnosen von allen NMS-Services für jeden vManage-Knoten im 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
```

Edge (vEdge/cEdge)

Die Probleme sind die allgemeinen Problembedingungen, die für Edge-Geräte gemeldet werden, sowie nützliche Ausgaben für alle Geräte, die erfasst werden müssen. Stellen Sie sicher, dass für jedes Problem ein **Admin-Tech** für alle erforderlichen und relevanten Edge-Geräte erfasst wird. Für Cloud-gehostete Controller kann das TAC auf der Grundlage des Feedbacks im Abschnitt

"Basisinformationen angefordert" die erforderlichen Admin-Tech-Ausgaben für die Geräte erfassen. Wie bei vManage kann es jedoch notwendig sein, diese zu erfassen, bevor Sie ein TAC-Ticket eröffnen, um sicherzustellen, dass die darin enthaltenen Daten für den Zeitpunkt des Problems relevant sind. Dies gilt vor allem, wenn das Problem nicht beständig ist, d.h. das Problem kann verschwinden, wenn das TAC aktiviert ist.

Keine Steuerungsverbindungen zwischen Gerät und Controller

Problembericht: Steuerungsverbindung nicht vom vEdge/cEdge zu einem oder mehreren Controllern

Schritt 1: Identifizieren des lokalen/Remote-Fehlers der Bedienungsanbindung:

- Für vEdge: Ausgabe des Befehls **show control connections-history**.
- Für cEdge: Ausgabe des Befehls **show sdwan control connection-history**.

Schritt 2: Bestätigen Sie den Status der TLOC(s) und ob alle Einträge "up" (aktiv) angezeigt werden:

- Für vEdge: Ausgabe des Befehls **show control local-properties**.
- Für cEdge: Ausgabe des Befehls **show sdwan control local-properties**.

Schritt 3: Bei Fehlern in Bezug auf Zeitüberschreitungen oder Verbindungsausfälle (d. h. DCONFAIL oder VM_TMO) sollten sowohl auf der Kontrollebene als auch auf dem betreffenden Controller erfasst werden:

- Für Controller:

```
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
```

- Für 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
```

- Für cEdge (Erfassung unten geht davon aus, dass das Gerät in den CLI-Modus verschoben wurde und eine Zugriffskontrollliste (ACL) mit dem Namen **STRG-CAP** zum Filtern erstellt wurde - weitere Details finden Sie im EPC-Erfassungsbeispiel im **Anwendungs-/Netzwerkleistungs-**Szenario):

```
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
```

Schritt 4: Weitere Fehler, die in den Ausgaben für den Steuerungsverbindungsverlauf beobachtet wurden, sowie weitere Informationen zu den beschriebenen Problemen finden Sie im folgenden Leitfaden.

Steuerungsverbindungen, die zwischen Edge-Gerät und Controller flattern

Problembericht: Eine oder mehrere Steuerungsanschlüsse klappen zwischen einem vEdge/cEdge und einem oder mehreren Controllern. Dies kann häufig, zeitweilig oder zufällig erfolgen.

- Kontrollverbindungs-Flaps sind im Allgemeinen das Ergebnis von Paketverlusten oder Weiterleitungsproblemen zwischen einem Gerät und einem Controller. Häufig ist dies auf **TMO-**Fehler zurückzuführen, abhängig von der Richtung des Fehlers. Überprüfen Sie zunächst den Grund für die Klappe: Für vEdge/Controller: Ausgabe des Befehls **show control connections-history**.Für cEdge: Ausgabe des Befehls **show sdwan control connection-history**.
- Bestätigen Sie den Zustand der TLOC(s), und dass alle TLOCs bei einem Flapping als "up" (aktiv) angezeigt werden: Für vEdge: Ausgabe des Befehls **show control local-properties**.Für cEdge: Ausgabe des Befehls **show sdwan control local-properties**.
- Sammeln Sie Paketerfassungen sowohl auf dem Controller als auch auf dem Edge-Gerät. Einzelheiten zu den Erfassungsparametern für jede Seite finden Sie im Abschnitt **Nicht zwischen Gerät und Controller** gebildete **Steuerungsverbindungen**.

BFD-Sitzungen (Bidirectional Forwarding Detection; bidirektionale Weiterleitungserkennung), bei denen keine oder keine Flapping zwischen Edge-Geräten stattfindet

Problembericht: Die BFD-Sitzung ist abgebrochen, oder die Verbindung zwischen zwei Edge-Geräten wird unterbrochen bzw. es kommt zu einem Flapping.

Schritt 1: Erfassen Sie den Status der BFD-Sitzung auf jedem Gerät:

- Für vEdge: Ausgabe des Befehls **show bfd sessions**.
- Für cEdge: Ausgabe des Befehls **show sdwan bfd sessions**.

Schritt 2: Sammeln von Rx- und Tx-Paketzählungen für jeden Edge-Router:

- Für vEdge: Ausgabe des Befehls **show tunnel statistics bfd**.
- Für cEdge: Ausgabe des Befehls **show platform hardware qfp active feature bfd datapath sdwan summary**.

Schritt 3: Wenn die Zähler für die BFD-Sitzung an einem Ende des Tunnels in den oben angegebenen Ausgaben nicht ansteigen, können mithilfe von ACLs erfasst werden, um zu überprüfen, ob Pakete lokal empfangen werden. Weitere Einzelheiten hierzu sowie weitere Validierungen, die durchgeführt werden können, finden Sie hier.

Geräteabstürze

Problembericht: Geräte werden unerwartet neu geladen und Probleme mit der Stromversorgung sind ausgeschlossen. Das Gerät weist darauf hin, dass es möglicherweise abgestürzt ist.

Schritt 1: Überprüfen Sie das Gerät, um sicherzustellen, dass ein Absturz oder ein unerwartetes erneutes Laden festgestellt wurde:

- Für vEdge: Ausgabe des Befehls **show reboot history**.
- Für cEdge: Ausgabe des Befehls **show sdwan reboot history**.
- Sie können auch zu **Monitor > Network** (**Überwachung > Netzwerk**) wechseln, das Gerät auswählen und zu **System Status > Reboot (Systemstatus > Neustart) wechseln**, um zu überprüfen, ob unerwartete Ladevorgänge aufgetreten sind.

Schritt 2: Wenn dies bestätigt wird, können Sie über vManage eine Admin-Technologie vom Gerät erfassen, indem Sie zu **Tools > Operational Commands (Tools > Betriebliche Befehle)** navigieren. Wählen Sie dort die Schaltfläche **Optionen** für das Gerät aus, und wählen Sie **Admin Tech** aus. Stellen Sie sicher, dass alle Kontrollkästchen aktiviert sind, die alle Protokolle und Kerndateien auf dem Gerät enthalten.

Anwendungs-/Netzwerkleistung beeinträchtigt oder fällt zwischen Standorten aus

Problembericht: Anwendung funktioniert nicht/HTTP-Seiten werden nicht geladen, Leistung langsam/Latenz, Fehler nach Durchführung von Richtlinien- oder Konfigurationsänderungen

Schritt 1: Identifizieren Sie das Quell-/Ziel-IP-Paar für eine Anwendung oder einen Flow, in dem das Problem auftritt.

Schritt 2: Bestimmen Sie alle Edge-Geräte im Pfad, und sammeln Sie von jedem Edge bis **zu** vManage einen **Admin-Tech**.

Schritt 3: Nehmen Sie eine Paketerfassung auf den Edge-Geräten an jedem Standort für diesen Fluss vor, wenn das Problem erkannt wird:

- Für vEdge: Aktivieren Sie im Feld **Administration > Settings** For **Hostname** (**Verwaltung > Einstellungen** > Hostname) die System-IP von vManage. Für **VPN** geben Sie **0** ein.Stellen Sie sicher, dass HTTPS unter der **allow-service-**Konfiguration der vManage VPN 0-Schnittstelle aktiviert ist.Folgen Sie den hier beschriebenen Schritten, um den Datenverkehr an der serviceseitigen VPN-Schnittstelle zu erfassen.
- Für cEdge: Versetzen Sie den bzw. die cEdge(s) in den CLI-Modus über **Konfiguration > Geräte > Modus ändern > CLI-Modus.**Konfigurieren Sie auf dem bzw. den cEdge(s) eine erweiterte ACL, um den Datenverkehr bidirektional abzugleichen. Gehen Sie so präzise wie möglich vor, um Protokolle und Ports einzubeziehen, um die Größe und die Daten in der

Erfassung zu begrenzen.

- Konfigurieren Sie Embedded Packet Capture (EPC) für die serviceseitige Schnittstelle in beide Richtungen, und verwenden Sie die unter (b) erstellte ACL zum Filtern des Datenverkehrs. Die Erfassung kann in das PCAP-Format exportiert und aus dem Karton kopiert werden. Hier finden Sie eine Beispielkonfiguration für GigabitEthernet0/0/0 auf einem Router mit einer ACL namens **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
```

- Konfigurieren Sie Packet Trace für den Datenverkehr in beide Richtungen, indem Sie die unter (b) erstellte ACL zum Filtern des Datenverkehrs verwenden. Nachfolgend finden Sie eine Beispielkonfiguration:

```
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
```

Schritt 4: Wiederholen Sie, wenn möglich, Schritt 3 in einem Arbeitsszenario zum Vergleich.

> **Tipp**: Wenn es keine andere Möglichkeit gibt, die entsprechenden Dateien direkt aus dem cEdge zu kopieren, können die Dateien zuerst mithilfe der hier beschriebenen Methode in vManage kopiert werden. Führen Sie den Befehl auf vManage aus: **anfordern scp -P 830 <Benutzername>@<cEdge system-IP>:/bootflash/<Dateiname> auszuführen.**
> Diese Datei wird dann im Verzeichnis **/home/<Benutzername>/** für den Benutzernamen gespeichert, den Sie für die Anmeldung bei vManage verwendet haben. Von dort können Sie Secure Copy Protocol (SCP) von Secure File Transfer Protocol (SFTP) verwenden, um eine Datei von einem vManage mithilfe eines SCP/SFTP-Clients eines Drittanbieters oder einer Linux/Unix-Rechner-CLI mit OpenSSH-Dienstprogrammen zu kopieren.