Guida introduttiva - Raccolta dei dati per vari problemi di SD-WAN

Sommario

Introduzione

Questo documento descrive vari problemi di SD-WAN e i dati importanti che devono essere raccolti in anticipo prima di aprire una richiesta TAC per migliorare la velocità di risoluzione dei problemi e/o la risoluzione dei problemi. Questo documento è suddiviso in due sezioni tecniche principali: Router vManage e Edge. Gli output pertinenti e la sintassi dei comandi vengono forniti in base al dispositivo in questione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Architettura SDWAN di Cisco
- Conoscenza generale della soluzione, inclusi controller vManage e cEdge (router SD-WAN IOS-XE) e dispositivi vEdge (router ViptelaOS)

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Informazioni di base richieste

- Descrivere il problema e il relativo impatto sulla rete e sugli utenti: Descrive un comportamento previsto.Descrivere nei dettagli il comportamento osservato.Preparare un diagramma della topologia con l'indirizzamento, se possibile, anche se disegnato a mano.
- Quando è iniziato il problema? Annotare il giorno e l'ora in cui il problema è stato osservato/notato per la prima volta.
- Quale potrebbe essere la potenziale causa del problema? Documentare le modifiche recenti apportate prima dell'inizio del problema.Prendere nota di eventuali azioni o eventi specifici che hanno attivato il problema.Il problema corrisponde ad altri eventi o azioni di rete?
- Qual è la frequenza del problema? Si tratta di un caso isolato?In caso negativo, con quale frequenza si verifica il problema?
- Fornire informazioni sui dispositivi in questione: Se sono interessati dispositivi specifici (non casuali), cosa hanno in comune?System-IP e Site-ID per ciascun dispositivo.Se il problema si verifica in un cluster vManage, fornire i dettagli del nodo (se non lo stesso in tutti i nodi del cluster).Per problemi generali all'interno dell'interfaccia grafica di vManage, acquisire tutti gli screenshot in un file che mostri messaggi di errore o altre anomalie/interruzioni che è necessario esaminare.
- Fornire informazioni sui risultati desiderati relativi al TAC e sulle priorità: Ripristinare il sistema il più presto possibile o individuare la causa principale dell'errore?

vManage

I problemi riportati di seguito sono condizioni di problemi comuni per vManage insieme agli output utili per ogni problema che devono essere raccolti oltre a uno o più file **admin-tech**. Per i controller ospitati nel cloud, i tecnici dei centri Cisco TAC (Technical Assistance Center) possono accedere per raccogliere gli output **admin-tech** richiesti per i dispositivi in base al feedback nella sezione Informazioni di base richieste, a condizione che l'utente acconsenta esplicitamente a questa operazione. Tuttavia, si consiglia di acquisire gli output **admin-tech** se le procedure descritte qui per assicurare che i dati contenuti in siano rilevanti per il momento del problema. Ciò è vero in particolare se il problema non è persistente, ossia può scomparire quando viene attivato TAC. Per i controller locali**,** è necessario includere anche un **admin-tech.** Per un cluster vManage, assicurarsi di acquisire un **admin-tech** per ogni nodo del cluster o solo per i nodi interessati.

Lentezza/Lentezza

Segnalazione problema: Lentezza nell'accesso all'interfaccia grafica di vManage, latenza durante l'esecuzione di operazioni all'interno dell'interfaccia, lentezza generale o lentezza rilevata all'interno di vManage

Passaggio 1. Acquisire 2-3 istanze di un thread di stampa, rinominare ogni file di **thread di stampa**

con una designazione numerica dopo ciascuna di esse (notare l'uso del nome utente con cui si accede a vManage nel percorso del file), ad esempio:

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

Passaggio 2. Accedere a **vshell** ed eseguire **vmstat** come indicato di seguito:

```
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:~$
```

Passaggio 3. Raccogliere ulteriori dettagli dalla **shell**:

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

Passaggio 4. Acquisire tutte le informazioni di diagnostica dei servizi 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
```

Errori/problemi API

Segnalazione problema: Le chiamate API non restituiscono dati o i dati corretti, problemi generali durante l'esecuzione delle query

Passaggio 1. Controllare la memoria disponibile:

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

Passaggio 2. Acquisire 2-3 istanze di un thread di stampa con un intervallo di 5 secondi, rinominare ogni file di **thread di stampa** con una designazione numerica dopo ogni esecuzione del comando (notare l'uso del nome utente con cui si accede a vManage nel percorso del file):

```
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
```

Passaggio 3. Raccogliere i dettagli per le sessioni HTTP attive:

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

Passaggio 4. Fornire i seguenti dettagli:

1. Chiamate API eseguite

2. Frequenza di chiamata

3. Metodo di accesso (ad esempio, uso di un singolo token per eseguire chiamate API successive o uso dell'autenticazione di base per eseguire la chiamata e poi la disconnessione)

4. È in corso il riutilizzo di JSESSIONID?

> **Nota** A partire dal software vManage 19.2, per le chiamate API è supportata solo l'autenticazione basata su token. Per ulteriori informazioni sulla generazione, il timeout e la scadenza dei token, vedere questo collegamento.

Statistiche/Lentezza Deep Packet Inspection (DPI)

Segnalazione problema: Con DPI abilitato, l'elaborazione delle statistiche può essere lenta o introdurre lentezza all'interno dell'interfaccia grafica di vManage.

Passaggio 1. Controllare le dimensioni del disco allocate per DPI all'interno di vManage passando a **Amministrazione > Impostazioni > Database statistiche > Configurazione**.

Passaggio 2. Controllare l'integrità dell'indice eseguendo il seguente comando CLI da vManage:

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

Passaggio 3. Verificare se le chiamate API correlate agli stati DPI vengono eseguite esternamente.

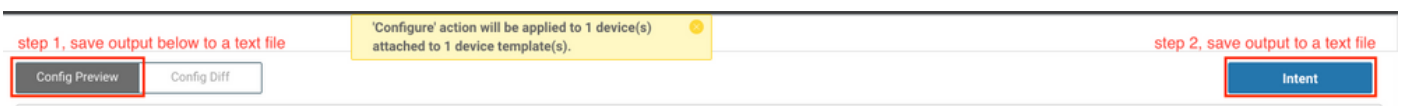
Passaggio 4. Controllare lo stato di I/O del disco con l'aiuto di questo comando CLI da vManage:

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

Errori Push Modello

Segnalazione problema: Push del modello o aggiornamento del modello del dispositivo non riuscito o scaduto.

Passaggio 1. Acquisire **Config Preview** e **Intent** config da vManage prima di fare clic sul pulsante **Configure Devices** (esempio di navigazione fornito qui):



Passaggio 2. Abilitare **viptela.enable.rest.log** dalla pagina **logsettings** (questa opzione deve essere disabilitata dopo aver acquisito le informazioni richieste):

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

Passaggio 3. Se l'errore di push del modello comporta un problema o un errore NETCONF, abilitare **viptela.enable.device.netconf.log** oltre al log REST nel passaggio 1. Tenere presente che questo log deve essere disabilitato anche dopo l'acquisizione degli output dei passaggi 3 e 4.

Passaggio 4. Tentare di collegare nuovamente il modello non riuscito da vManage e acquisire un **admin-tech** utilizzando questa CLI (acquisire questo per ogni nodo di per un cluster):

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

Passaggio 5. Fornire gli screenshot dal task in vManage e il Diff configurazione per confermare i dettagli dell'errore e gli eventuali file CSV utilizzati per il modello.

Passaggio 6. Includere i dettagli relativi all'errore e all'attività, tra cui l'ora del push non riuscito, l'indirizzo di **sistema** del dispositivo che non è riuscito e il messaggio di errore visualizzato nell'interfaccia utente di vManage.

Passaggio 7. Se un errore di push del modello si verifica con un messaggio di errore segnalato per la configurazione dal dispositivo stesso, raccogliere anche un **admin-tech** dal dispositivo.

Problemi correlati ai cluster

Segnalazione problema: Instabilità del cluster con conseguente timeout della GUI, lentezza o altre anomalie.

Passaggio 1. Acquisire l'output da **server_configs.json** da ogni nodo vManage del cluster. Ad esempio:

```
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"
}
```


Passaggio 2. Acquisire i dettagli sui servizi abilitati o disabilitati per ogni nodo. A tale scopo, selezionare **Amministrazione > Gestione cluster** nella GUI di vManage.

Passaggio 3. Confermare la raggiungibilità dell'underlay sull'interfaccia del cluster. A tale scopo, eseguire il comando **ping <indirizzo-ip>** da ogni nodo vManage della VPN 0 all'indirizzo IP dell'interfaccia cluster degli altri nodi.

Passaggio 4. Raccogliere la diagnostica da tutti i servizi NMS per ogni nodo vManage nel 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)

I problemi qui sono comuni condizioni di problema segnalate per i dispositivi Edge insieme a output utili per ciascuno che devono essere raccolti. Verificare che per ogni problema venga raccolto un **admin-tech** per tutti i dispositivi Edge necessari e pertinenti. Per i controller ospitati sul cloud, TAC può avere accesso per raccogliere gli output admin-tech richiesti per i dispositivi in base ai commenti riportati nella sezione **Informazioni di base richieste**. Tuttavia, come per vManage, può essere necessario acquisirle prima di aprire una richiesta TAC per assicurarsi che i dati in essa contenuti siano pertinenti al momento in cui si è verificato il problema. Ciò è vero in particolare se il problema non è persistente, ossia se il problema può scomparire nel momento in cui si attiva TAC.

Controllare le connessioni che non si formano tra dispositivo e controller

Segnalazione problema: Connessione di controllo non formata da un vEdge/cEdge a uno o più controller

Passaggio 1. Identificare l'errore locale/remoto dell'errore della connessione di controllo:

- Per vEdge: output del comando **show control connections-history**.
- Per cEdge: output del comando **show sdwan control connection-history**.

Passaggio 2. Confermare lo stato dei TLOC e che tutti i TLOC vengano visualizzati:

- Per vEdge: output del comando **show control local-properties**.
- Per cEdge: output del comando **show sdwan control local-properties**.

Passaggio 3. Per gli errori relativi a timeout o errori di connessione (ad esempio, DCONFAIL o VM_TMO), acquisire il control-plane sia sul dispositivo periferico che sul controller in questione:

- Per i 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
```

- Per 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
```

- Per cEdge (l'acquisizione riportata di seguito presuppone che il dispositivo sia stato spostato in modalità CLI e che sia stato creato un Access Control List (ACL) denominato **CTRL-CAP** per filtrare. Per ulteriori dettagli, vedere l'esempio relativo all'acquisizione EPC nello scenario **Prestazioni applicazioni/rete**):

```
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
```

Passaggio 4. Per altri errori osservati negli output della cronologia delle connessioni di controllo e per ulteriori dettagli sui problemi descritti, fare riferimento alla seguente guida .

Controllare lo sfarfallio delle connessioni tra il dispositivo Edge e il controller

Segnalazione problema: Una o più connessioni di controllo eseguono il flap tra un vEdge/cEdge e uno o più controller. Ciò può essere frequente, intermittente o casuale.

- I flap di connessione di controllo sono generalmente il risultato di problemi di perdita di pacchetti o di inoltro tra un dispositivo e un controller. Spesso, ciò è legato a errori **TMO**, a seconda della direzionalità del fallimento. Per controllare ulteriormente questo, verificare prima il motivo del flap: Per vEdge/controller: output del comando **show control connections-history**.Per cEdge: output del comando **show sdwan control connection-history**.
- Confermare lo stato dei TLOC e che tutti i TLOC siano visualizzati quando si verifica il flapping: Per vEdge: output del comando **show control local-properties**.Per cEdge: output del comando **show sdwan control local-properties**.
- Raccogli le clip dei pacchetti sui controller e sul dispositivo edge. Fare riferimento alla sezione **Controlla connessioni non formanti tra dispositivo e controller** per i dettagli sui parametri di acquisizione per ciascun lato.

Sessioni BFD (Bidirectional Forwarding Detection) che non si formano o non lampeggiano tra dispositivi Edge

Segnalazione problema: La sessione BFD è interrotta o lampeggia su e giù tra due dispositivi periferici.

Passaggio 1. Raccogliere lo stato della sessione BFD su ciascun dispositivo:

- Per vEdge: output del comando **show bfd session**.
- Per cEdge: output del comando **show sdwan bfd session**.

Passaggio 2. Raccogliere il numero di pacchetti Rx e Tx su ciascun router perimetrale:

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

Passaggio 3. Se i contatori per la sessione BFD non aumentano su un'estremità del tunnel negli output di cui sopra, è possibile acquisire le immagini usando gli ACL per confermare se i pacchetti vengono ricevuti localmente. Qui è possibile trovare ulteriori dettagli su questo e altre convalide.

Arresti anomali del dispositivo

Segnalazione problema: Il dispositivo viene ricaricato in modo imprevisto e i problemi di alimentazione vengono esclusi. È possibile che il dispositivo si sia bloccato.

Passaggio 1. Controllare il dispositivo per verificare se è stato rilevato un arresto anomalo o un ricaricamento imprevisto:

- Per vEdge: output del comando **show reboot history**.
- Per cEdge: output del comando **show sdwan reboot history**.
- In alternativa, selezionare **Monitor > Network** (Monitor > Rete), selezionare il dispositivo, quindi selezionare **System Status** (Stato sistema) > Reboot (Riavvia) per verificare se sono stati rilevati ricaricamenti imprevisti.

Passaggio 2. Se confermato, acquisire un admin-tech dal dispositivo tramite vManage passando a **Strumenti > Comandi operativi**. Quindi, selezionare il pulsante **Options** (Opzioni) per il dispositivo e selezionare **Admin Tech** (Tecnica di amministrazione). Verificare che tutte le caselle di controllo siano selezionate, includendo tutti i registri e i file di base nel dispositivo.

Prestazioni di applicazioni/rete ridotte o con errori tra i siti

Segnalazione problema: L'applicazione non funziona/le pagine HTTP non vengono caricate, le prestazioni rallentate/latenti, gli errori dopo aver apportato modifiche alla configurazione o ai criteri

Passaggio 1. Identificare la coppia IP origine/destinazione per un'applicazione o un flusso che presenta il problema.

Passaggio 2. Determinare tutti i dispositivi Edge nel percorso e raccogliere un **admin-tech** da ciascuno di essi tramite vManage.

Passaggio 3. Acquisire un pacchetto sui dispositivi periferici in ciascun sito per questo flusso quando viene rilevato il problema:

- Per vEdge: Abilitare il flusso di dati in **Amministrazione > Impostazioni** per il campo **Nome host**, immettere l'indirizzo IP di sistema di vManage. Per la **VPN**, immettere **0**Verificare che HTTPS sia abilitato nella configurazione **allow-service** dell'interfaccia vManage VPN 0.Seguire la procedura qui per acquisire il traffico sull'interfaccia VPN del lato servizio.
- Per cEdge: Spostare i cEdge in modalità CLI tramite **Configurazione > Dispositivi > Modifica modalità > Modalità CLI**Sugli cEdge, configurare un ACL esteso in modo che corrisponda bidirezionalmente al traffico. Rendere questa impostazione il più specifica possibile per includere il protocollo e la porta per limitare le dimensioni e i dati nell'acquisizione.
- Configurare l'EPC (Embedded Packet Capture) per l'interfaccia del lato servizio in entrambe le direzioni, usando l'ACL creato in (b) per filtrare il traffico. L'acquisizione può essere esportata in formato PCAP e copiata all'esterno della confezione. Di seguito viene fornita una configurazione di esempio per Gigabit Ethernet0/0/0 su un router che utilizza un ACL denominato **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
```

- Configurare Packet Trace per il traffico in entrambe le direzioni, usando l'ACL creato in (b) per filtrare il traffico. Di seguito è riportata una configurazione di esempio:

```
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
```

Passaggio 4. Se possibile, ripetere il passaggio 3 in uno scenario di lavoro per il confronto.

> **Suggerimento**: se non esistono altri modi per copiare i file corrispondenti direttamente da cEdge, è possibile copiarli prima in vManage utilizzando il metodo descritto di seguito. Eseguire il comando su vManage:
> **request execute scp -P 830 <nomeutente>@<cEdge IP-sistema>:/bootflash/<nomefile> .**
> Il file verrà quindi archiviato nella directory **/home/<nomeutente>/** del nome utente utilizzato per accedere a vManage. Da qui, è possibile utilizzare il protocollo SCP (Secure Copy Protocol) del protocollo SFTP (Secure File Transfer Protocol) per copiare i file da un vManage utilizzando un client SCP/SFTP di terze parti o una CLI di un computer Linux/Unix con utilità OpenSSH.