Guide de démarrage rapide - Collecte de données pour divers problèmes SD-WAN

Contenu

Introduction

Ce document décrit plusieurs problèmes liés au SD-WAN ainsi que les données pertinentes qui doivent être collectées à l'avance avant d'ouvrir un dossier TAC pour améliorer la vitesse de dépannage et/ou de résolution des problèmes. Ce document est divisé en deux sections techniques principales : Routeurs vManage et Edge. Les sorties et la syntaxe des commandes pertinentes sont fournies en fonction du périphérique en question.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Architecture SDWAN de Cisco
- Compréhension générale de la solution, y compris le contrôleur vManage ainsi que les routeurs cEdge (IOS-XE SD-WAN) et les périphériques vEdge (routeurs ViptelaOS)

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations de base demandées

- Décrire le problème et son impact sur votre réseau et vos utilisateurs : Décrire un comportement attendu.Décrire en détail le comportement observé.Préparez un schéma de topologie avec adressage si possible, même si celui-ci est dessiné à la main.
- Quand le problème a-t-il commencé ? Notez le jour et l'heure où le problème a été observé/remarqué pour la première fois.
- Quel pourrait être le déclencheur potentiel du problème ? Documenter les modifications récentes apportées avant le début du problème.Notez les actions ou événements spécifiques qui ont pu déclencher le problème.Ce problème correspond-il à d'autres événements ou actions réseau ?
- Quelle est la fréquence du problème ? Était-ce un cas unique ?Dans la négative, à quelle fréquence le problème se produit-il ?
- Fournir des informations sur le ou les périphériques en question : Si des périphériques spécifiques sont affectés (pas aléatoires), quels sont leurs points communs ?System-IP et Site-ID pour chaque périphérique.Si le problème se trouve sur un cluster vManage, indiquez les détails du noeud (si ce n'est pas le cas sur tous les noeuds du cluster).Pour les problèmes généraux à l'intérieur de l'interface utilisateur graphique vManage, capturez toutes les captures d'écran dans un fichier qui affiche des messages d'erreur ou d'autres anomalies/disparties qui doivent être étudiées.
- Fournir des informations sur les résultats souhaités du TAC et vos priorités : Voulez-vous récupérer de la panne le plus tôt possible ou connaître la cause première de la panne ?

vManage

Les problèmes ici sont des conditions de problème courantes signalées pour vManage ainsi que des sorties utiles pour chaque problème qui doivent être collectées en plus d'un fichier **admin-tech**. Pour les contrôleurs hébergés dans le cloud, l'ingénieur du centre d'assistance technique (TAC) peut avoir accès à la collecte des sorties **admin-tech** requises pour les périphériques en fonction des commentaires de la section Informations de base demandées si vous y consentez explicitement. Cependant, nous recommandons de capturer les résultats **admin-tech** si les étapes décrites ici pour s'assurer que les données contenues dans sont pertinentes à l'heure du problème. Ceci est particulièrement vrai si le problème n'est pas persistant, ce qui signifie que le problème peut disparaître au moment où le TAC est engagé. Pour les contrôleurs sur site**,** un **admin-tech** doit également être inclus avec chaque ensemble de données ici**.** Pour un cluster vManage, assurez-vous de capturer un **admin-tech** pour chaque noeud du cluster ou uniquement pour le ou les noeuds affectés.

Lenteur/lenteur

Rapport de problème : Lenteur de l'accès à l'interface utilisateur graphique vManage, latence lors de l'exécution d'opérations à l'intérieur de l'interface utilisateur graphique, lenteur ou lenteur

générale constatée dans vManage

Étape 1. Capturez 2 à 3 instances d'une impression de thread, renommez chaque fichier **d'impression de thread** avec une désignation numérique après chaque instance (notez l'utilisation du nom d'utilisateur avec lequel vous vous connectez à vManage dans le chemin d'accès du fichier), par exemple :

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

Étape 2. Connectez-vous à **vshell** et exécutez **vmstat** comme suit :

```
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:~$
```

Étape 3. Collecter des détails supplémentaires à partir du **shell** :

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

Étape 4. Capturez tous les diagnostics des services 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
```

Défaillances/problèmes de l'API

Rapport de problème : Les appels API ne peuvent pas renvoyer les données ou les données correctes, problèmes généraux lors de l'exécution des requêtes

Étape 1. Vérifiez la mémoire 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:~$
```

Étape 2. Capturez 2 à 3 instances d'une impression de thread avec un intervalle de 5 secondes entre les deux, renommez chaque fichier **d'impression de thread** avec une désignation numérique après chaque exécution de la commande (notez l'utilisation du nom d'utilisateur avec lequel vous

vous connectez à vManage dans le chemin d'accès du fichier) :

```
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
```

Étape 3. Collecter les détails de toutes les sessions HTTP actives :

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

Étape 4. Fournissez les détails suivants :

1. Appels API exécutés

2. Fréquence d'appel

3. Méthode de connexion (c'est-à-dire utilisation d'un jeton unique pour exécuter les appels API suivants ou utilisation de l'authentification de base pour exécuter l'appel, puis déconnexion)

4. Le JSESSIONID est-il réutilisé ?

> **Remarque** À partir du logiciel vManage 19.2, seule l'authentification basée sur un jeton est prise en charge pour les appels API. Pour plus d'informations sur la génération, le délai d'attente et l'expiration des jetons, consultez ce lien.

Statistiques DPI (Deep Packet Inspection)/Lenteur

Rapport de problème : Lorsque le protocole DPI est activé, le traitement des statistiques peut être lent ou introduire une lenteur dans l'interface graphique de vManage.

Étape 1. Vérifiez la taille de disque allouée pour DPI à l'intérieur de vManage en accédant à **Administration > Settings > Statistics Database > Configuration**.

Étape 2. Vérifiez l'intégrité de l'index en exécutant la commande CLI suivante à partir de vManage :

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

Étape 3. Confirmer si des appels API liés aux statistiques DPI sont exécutés en externe.

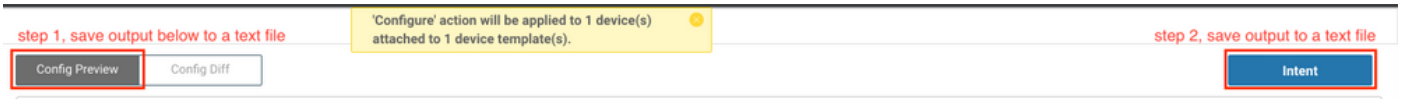
Étape 4. Vérifiez les statistiques d'E/S du disque à l'aide de cette commande CLI de vManage :

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

Échecs de transmission de modèle

Rapport de problème : Échec ou expiration de la mise à jour du modèle ou du modèle de périphérique.

Étape 1. Capturez la configuration **Aperçu de la configuration** et **intention** à partir de vManage avant de cliquer sur le bouton **Configurer les périphériques** (exemple de navigation fourni ici) :



Étape 2. Activez **viptela.enable.rest.log** à partir de la page **logsettings** (cette option doit être désactivée après avoir capturé les informations requises) :

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

Étape 3. Si l'échec de transmission du modèle implique un problème ou une erreur NETCONF, activez **viptela.enable.device.netconf.log** en plus du journal REST à l'étape 1. Notez que ce journal doit également être désactivé après la capture des sorties des étapes 3 et 4.

Étape 4. Tentative de connexion du modèle ayant échoué à nouveau à partir de vManage et capture d'un **admin-tech** à l'aide de cette CLI (capture ceci pour chaque noeud de pour un cluster) :

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

Étape 5. Fournissez des captures d'écran de la tâche dans vManage et Config Diff pour confirmer les détails de l'échec ainsi que les fichiers CSV utilisés pour le modèle.

Étape 6. Incluez des détails sur l'échec et la tâche, y compris l'heure de l'échec de la transmission, l'adresse **ip système** du périphérique qui a échoué, et le message d'erreur que vous voyez dans l'interface graphique de vManage.

Étape 7. Si un échec de transmission de modèle se produit avec un message d'erreur signalé pour la configuration par le périphérique lui-même, collectez également un **admin-tech** à partir du périphérique.

Problèmes liés aux clusters

Rapport de problème : Instabilité du cluster entraînant des délais d'attente, une lenteur ou d'autres anomalies dans l'interface utilisateur graphique.

Étape 1. Capturez le résultat de **server_configs.json** à partir de chaque noeud vManage du cluster. Exemple :

```
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"
}
```


Étape 2. Capturez les détails sur les services activés ou désactivés pour chaque noeud. Pour cela, accédez à **Administration > Cluster Management** dans l'interface graphique de vManage.

Étape 3. Confirmez l'accessibilité de la sous-couche sur l'interface de cluster. Pour cela, exécutez **ping <adresse_ip>** de chaque noeud vManage dans VPN 0 vers l'adresse IP de l'interface de cluster des autres noeuds.

Étape 4. Collecter les diagnostics de tous les services NMS pour chaque noeud vManage du 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
```

Périphérie (vEdge/cEdge)

Les problèmes ici sont les conditions de problème courantes signalées pour les périphériques Edge, ainsi que les sorties utiles pour chacun d'entre eux qui doivent être collectées. Assurez-vous que pour chaque problème, un **admin-tech** est collecté pour tous les périphériques Edge nécessaires et pertinents. Pour les contrôleurs hébergés dans le cloud, le centre d'assistance technique peut avoir accès à la collecte des sorties admin-tech requises pour les périphériques en

fonction des commentaires de la section **Informations de base demandées**. Cependant, comme avec vManage, il peut être nécessaire de les capturer avant d'ouvrir un dossier TAC pour s'assurer que les données contenues dans le sont en fonction de l'heure du problème. Ceci est particulièrement vrai si le problème n'est pas persistant, ce qui signifie que le problème peut disparaître au moment où le TAC est engagé.

Contrôler les connexions qui ne se forment pas entre le périphérique et le contrôleur

Rapport de problème : La connexion de contrôle ne se forme pas d'un vEdge/cEdge à un ou plusieurs contrôleurs

Étape 1. Identifiez l'erreur locale/distante de l'échec de la connexion de contrôle :

- Pour vEdge : sortie de la commande **show control connections-history**.
- Pour cEdge : sortie de la commande **show sdwan control connection-history**.

Étape 2. Confirmez l'état du ou des TLOC et vérifiez que tous les éléments sont activés :

- Pour vEdge : sortie de la commande **show control local-properties**.
- Pour cEdge : sortie de la commande **show sdwan control local-properties**.

Étape 3. Pour les erreurs liées aux dépassements de délai ou aux échecs de connexion (par exemple, DCONFAIL ou VM_TMO), prenez des captures de plan de contrôle sur le périphérique de périphérie ainsi que sur le contrôleur en question :

- Pour les contrôleurs :

```
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
```

- Pour 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
```

- Pour cEdge (la capture ci-dessous suppose que le périphérique a été déplacé en mode CLI et qu'une liste de contrôle d'accès appelée **CTRL-CAP** a été créée pour filtrer - voir plus de détails dans l'exemple de capture EPC dans le scénario **Performances applicatives/réseau**) :

```
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
```

Étape 4. Pour d'autres erreurs observées dans les sorties de l'historique des connexions de contrôle et pour plus de détails sur les problèmes décrits, reportez-vous au guide suivant.

Connexions de contrôle oscillant entre le périphérique de périphérie et le contrôleur

Rapport de problème : Une ou plusieurs connexions de contrôle sont bloquées entre un vEdge/cEdge et un ou plusieurs contrôleurs. Cela peut être fréquent, intermittent ou aléatoire.

- Les pannes de connexion de contrôle sont généralement le résultat de problèmes de perte ou de transfert de paquets entre un périphérique et un contrôleur. Souvent, cela sera lié aux erreurs **TMO**, selon la direction de l'échec. Pour vérifier plus en détail, vérifiez d'abord la raison du rabat : Pour vEdge/contrôleurs : sortie de la commande **show control connections-history**.Pour cEdge : sortie de la commande **show sdwan control connection-history**.
- Confirmez l'état du ou des TLOC et vérifiez que tous les TLOC s'affichent lorsque le battement se produit : Pour vEdge : sortie de la commande **show control local-properties**.Pour cEdge : sortie de la commande **show sdwan control local-properties**.
- Collecter les captures de paquets sur le ou les contrôleurs et le périphérique de périphérie. Reportez-vous à la section **Connexions de contrôle non formatrices entre le périphérique et le contrôleur** pour plus de détails sur les paramètres de capture de chaque côté.

Sessions BFD (Bidirectional Forwarding Detection) qui ne se forment pas ou ne battent pas entre les périphériques de périphérie

Rapport de problème : La session BFD est en panne ou est en train de basculer entre deux périphériques de périphérie.

Étape 1. Collecter l'état de la session BFD sur chaque périphérique :

- Pour vEdge : sortie de la commande **show bfd sessions**.
- Pour cEdge : sortie de la commande **show sdwan bfd sessions**.

Étape 2. Collecter le nombre de paquets Rx et Tx sur chaque routeur de périphérie :

- Pour vEdge : sortie de la commande **show tunnel statistics bfd**.
- Pour cEdge : sortie de la commande **show platform hardware qfp active feature bfd datapath sdwan summary**.

Étape 3. Si les compteurs n'augmentent pas pour la session BFD à une extrémité du tunnel dans les sorties ci-dessus, les captures peuvent être prises à l'aide de listes de contrôle d'accès pour confirmer si des paquets sont reçus localement. Vous trouverez plus de détails à ce sujet ainsi que d'autres validations possibles ici .

Crash des périphériques

Rapport de problème : Le périphérique est rechargé de manière inattendue et les problèmes d'alimentation sont exclus. Les indications du périphérique indiquent qu'il est susceptible de s'écraser.

Étape 1. Vérifiez le périphérique pour vérifier si un plantage ou un rechargement inattendu a été observé :

- Pour vEdge : sortie de la commande **show reboot history**.
- Pour cEdge : sortie de la commande **show sdwan reboot history**.
- Vous pouvez également accéder à **Monitor > Network**, sélectionner le périphérique, puis accéder à **System Status > Reboot** pour confirmer si des rechargements inattendus ont été vus.

Étape 2. Si cela est confirmé, capturez un admin-tech à partir du périphérique via vManage en accédant à **Outils > Commandes opérationnelles**. Une fois sur place, sélectionnez le bouton **Options** du périphérique et sélectionnez **Admin Tech**. Assurez-vous que toutes les cases à cocher sont cochées, qui incluront tous les journaux et fichiers principaux sur le périphérique.

Performances des applications/réseaux dégradées ou défaillantes entre les sites

Rapport de problème : L'application ne fonctionne pas/les pages HTTP ne sont pas chargées, la lenteur/la latence des performances, les échecs après avoir effectué des modifications de stratégie ou de configuration

Étape 1. Identifiez la paire IP source/destination d'une application ou d'un flux présentant le problème.

Étape 2. Déterminez tous les périphériques Edge sur le chemin et collectez une **technologie admin** de chacun à travers vManage.

Étape 3. Prenez une capture de paquets sur les périphériques de périphérie de chaque site pour ce flux lorsque le problème est détecté :

- Pour vEdge : Activez le flux de données sous **Administration > Settings** For **Hostname** field, saisissez l'adresse IP système de vManage. Pour **VPN**, saisissez **0**Assurez-vous que HTTPS est activé sous la configuration **allow-service** de l'interface vManage VPN 0.Suivez les étapes ici pour capturer le trafic sur l'interface VPN côté service.
- Pour cEdge : Déplacez le ou les cEdge en mode CLI via **Configuration > Devices > Change Mode > CLI mode**Sur les cEdge, configurez une liste de contrôle d'accès étendue pour qu'elle corresponde au trafic bidirectionnellement. Rendre ceci aussi spécifique que possible pour inclure le protocole et le port pour limiter la taille et les données dans la capture.
- Configurez la capture de paquets intégrée (EPC) pour l'interface côté service dans les deux directions, en utilisant la liste de contrôle d'accès créée à la (b) pour filtrer le trafic. La capture peut être exportée au format PCAP et copiée hors de la zone. Un exemple de configuration

est fourni ici pour GigabitEthernet0/0/0 sur un routeur à l'aide d'une liste de contrôle d'accès nommée **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
```

- Configurez Packet Trace pour le trafic dans les deux directions, à l'aide de la liste de contrôle d'accès créée à la (b) pour filtrer le trafic. Voici un exemple de configuration :

```
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
```

Étape 4. Si possible, répétez l'étape 3 dans un scénario de travail pour la comparaison.

Conseil : s'il n'y a pas d'autres moyens de copier directement les fichiers correspondants hors de cEdge, les fichiers peuvent être copiés dans vManage en utilisant d'abord la méthode décrite ici. Exécutez la commande sur vManage :
request execute scp -P 830 <nom d'utilisateur>@<cEdge system-IP>:/bootflash/<nom de fichier> .
Ce fichier sera ensuite stocké dans le répertoire **/home/<nom d'utilisateur>/** du nom d'utilisateur que vous avez utilisé pour vous connecter à vManage. À partir de là, vous pouvez utiliser le protocole Secure Copy Protocol (SCP) du protocole SFTP (Secure File Transfer Protocol) pour copier un fichier à partir d'un vManage à l'aide d'un client SCP/SFTP tiers ou d'une CLI de machine Linux/Unix avec des utilitaires OpenSSH.