Résolution des problèmes courants de contrôle SD-WAN et de plan de données

Table des matières

Introduction

Ce document décrit comment commencer à dépanner les problèmes courants de contrôle et de plan de données du réseau étendu défini par logiciel (SD-WAN).

Conditions préalables

Exigences

Cisco vous recommande de connaître la solution Cisco Catalyst.

Composants utilisés

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.

Aperçu

Cet article est conçu comme un Runbook pour fournir un point de départ pour les défis de débogage rencontrés dans les environnements de production. Chaque section présente des exemples d'utilisation courants et des points de données probables à collecter ou à rechercher lorsque vous déboguez ces problèmes courants.

Configurations de base

Assurez-vous que les configurations de base sont présentes sur le routeur et que les valeurs spécifiques au périphérique sont uniques pour chaque périphérique dans la superposition :

Configurations du système

<#root>

```
system
 system-ip <system –ip>
 site-id <site-id>
 admin-tech-on-failure
 organization-name <organization name>
 vbond <vbond-ip>
!
```

Example:

```
system
 system-ip 10.2.2.1
 site-id 2
 admin-tech-on-failure
 organization-name "TAC - 22201"
 vbond 10.106.50.235
!
```

Configurations des interfaces

```
interface Tunnel0
 no shutdown
 ip unnumbered GigabitEthernet0/0/0
 tunnel source GigabitEthernet0/0/0
 tunnel mode sdwan
exit

sdwan
 interface GigabitEthernet0/0/0
  tunnel-interface
   encapsulation ipsec
   color blue restrict
```

```
   no allow-service all
   no allow-service bgp
   no allow-service dhcp
   no allow-service dns
   no allow-service icmp
   allow-service sshd
   allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
exit
```

Assurez-vous que le routeur dispose d'une route disponible dans la table de routage pour établir une connexion de contrôle avec les contrôleurs (vBond, vManage et vSmart). Vous pouvez utiliser cette commande pour afficher toutes les routes installées dans la table de routage :

```
show ip route
```

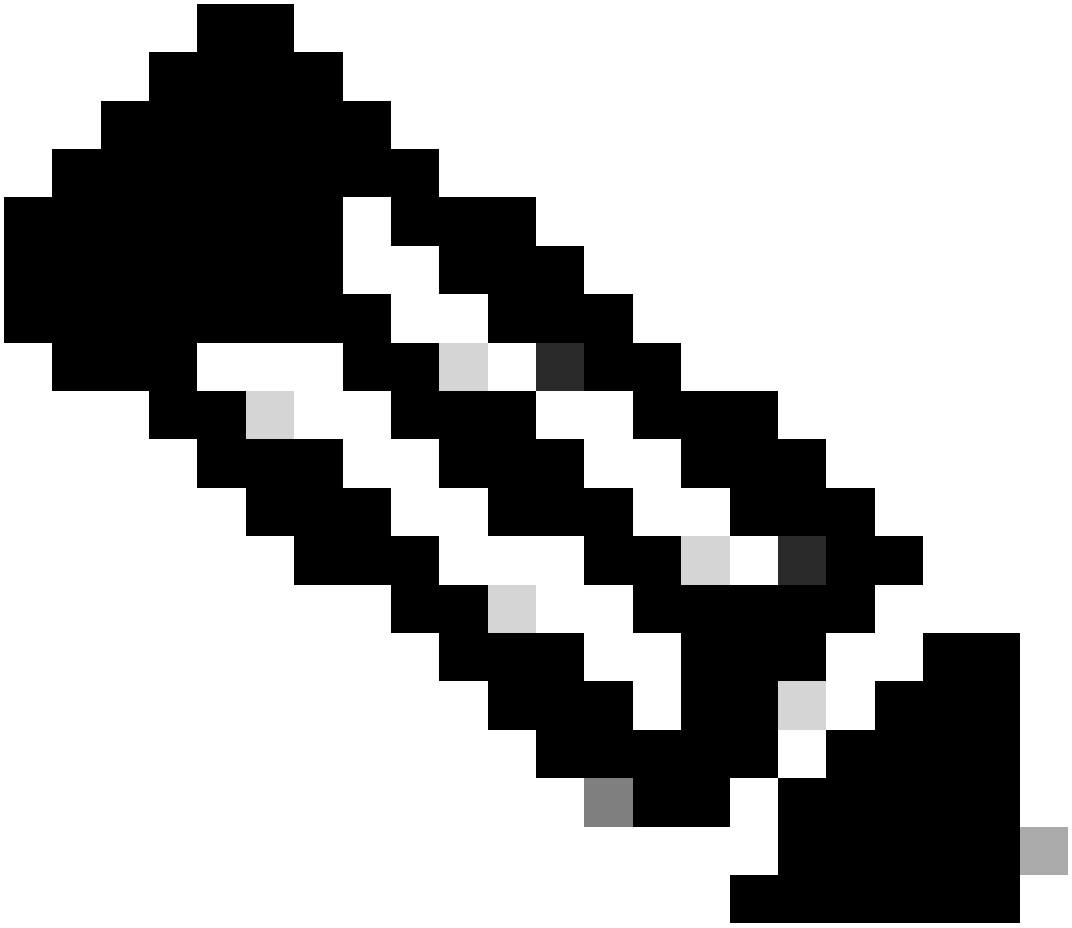
Si vous utilisez le nom de domaine complet vBond, assurez-vous que le serveur DNS ou le serveur de noms configuré dispose d'une entrée pour résoudre le nom d'hôte vBond. Vous pouvez vérifier quel serveur DNS ou serveur de noms est configuré avec cette commande :

```
show run | in ip name-server
```

Certificat

Vérifiez que le certificat est installé sur le routeur à l'aide de la commande suivante :

```
show sdwan certificate installed
```



Remarque : si vous n'utilisez pas de certificats d'entreprise, le certificat est déjà disponible sur les routeurs. Pour les plates-formes matérielles, les certificats de périphérique sont intégrés au matériel du routeur. Pour les routeurs virtuels, vManage agit en tant qu'autorité de certification et génère les certificats pour les routeurs cloud.

Si vous utilisez des certificats d'entreprise sur les contrôleurs, assurez-vous que le certificat racine de l'autorité de certification d'entreprise est installé sur le routeur.

Vérifiez que les certificats racine sont installés sur le routeur à l’aide des commandes suivantes :

```
show sdwan certificate root-ca-cert
show sdwan certificate root-ca-cert | inc Issuer
```

Vérifiez le résultat de show sdwan control local-properties pour vous assurer que les configurations et certificats requis sont en place.

```
SD-WAN-Router#show sdwan control local-properties
personality                          vedge
sp-organization-name                 TAC - 22201
organization-name                    TAC - 22201
root-ca-chain-status                 Installed

certificate-status                   Installed
certificate-validity                 Valid
certificate-not-valid-before         Nov 23 07:21:37 2015 GMT
certificate-not-valid-after          Nov 23 07:21:37 2025 GMT



enterprise-cert-status               Not-Applicable
enterprise-cert-validity             Not Applicable
enterprise-cert-not-valid-before     Not Applicable
enterprise-cert-not-valid-after      Not Applicable

dns-name                             10.106.50.235
site-id                              2
domain-id                            1
protocol                             dtls
tls-port                             0
system-ip                            10.2.2.1
chassis-num/unique-id                ASR1001-X-JAE194707HJ
serial-num                           983558
subject-serial-num                   JAE194707HJ
enterprise-serial-num                No certificate installed
token                                -NA-
keygen-interval                      1:00:00:00
retry-interval                       0:00:00:18
no-activity-exp-interval             0:00:00:20
dns-cache-ttl                        0:00:02:00
port-hopped                          TRUE
time-since-last-port-hop             0:00:01:26
embargo-check                        success
number-vbond-peers                   1

INDEX   IP                                       PORT
------------------------------------------------------
0       10.106.50.235                            12346

number-active-wan-interfaces         2


 NAT TYPE: E -- indicates End-point independent mapping
           A -- indicates Address-port dependent mapping
           N -- indicates Not learned
           Note: Requires minimum two vbonds to learn the NAT type

                           PUBLIC          PUBLIC PRIVATE         PRIVATE

INTERFACE                  IPv4            PORT   IPv4            IPv6

-------------------------------------------------------------------------------------------------------------
GigabitEthernet0/0/0          10.197.240.4    12426  10.197.240.4    ::
GigabitEthernet0/0/1          10.197.242.10   12406  10.197.242.10   ::
```

Lors de la vérification du résultat de show sdwan control local-properties, assurez-vous que tous ces critères sont remplis :

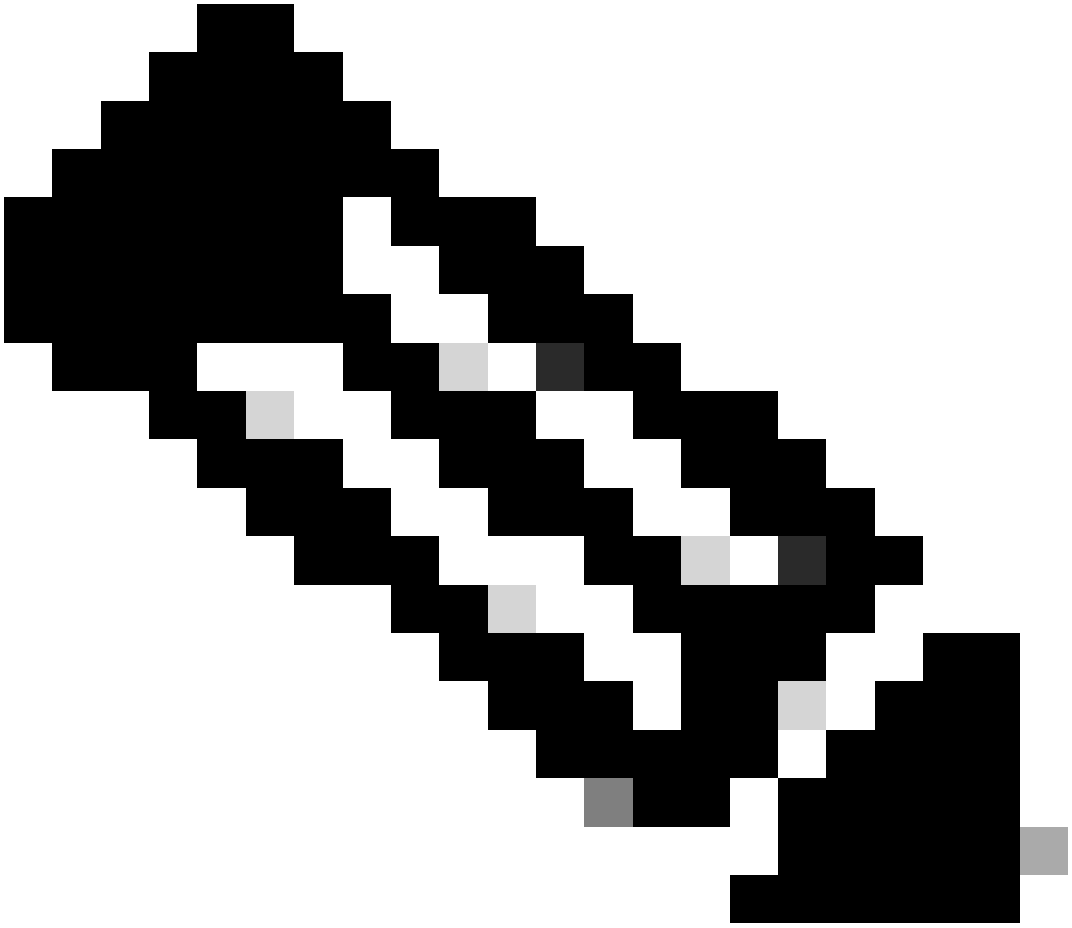
- Le nom de l'organisation apparaît correctement.
- La validité du certificat est valide au moment où vous vérifiez le résultat.
- L'adresse FQDN/IP vBond est correcte.
- System-ip/Site-id est correct.
- L'adresse IP vBond apparaît dans l'entrée « number-vbond-peers ». Si l'adresse IP vBond n'est pas vue, vérifiez que DNS résout l'URL vBond à l'aide de la commande ping <vBond FQDN>.
- Les interfaces sont mappées avec la couleur et l'adresse IP correctes et l'état de l'interface est UP.
- Le MAX CONTROL pour l'interface requise pour former la connexion de contrôle n'est pas 0.

État des connexions de contrôle

Vérifiez l'état de la connexion de contrôle à l'aide de cette commande :

```
show sdwan control connection
```

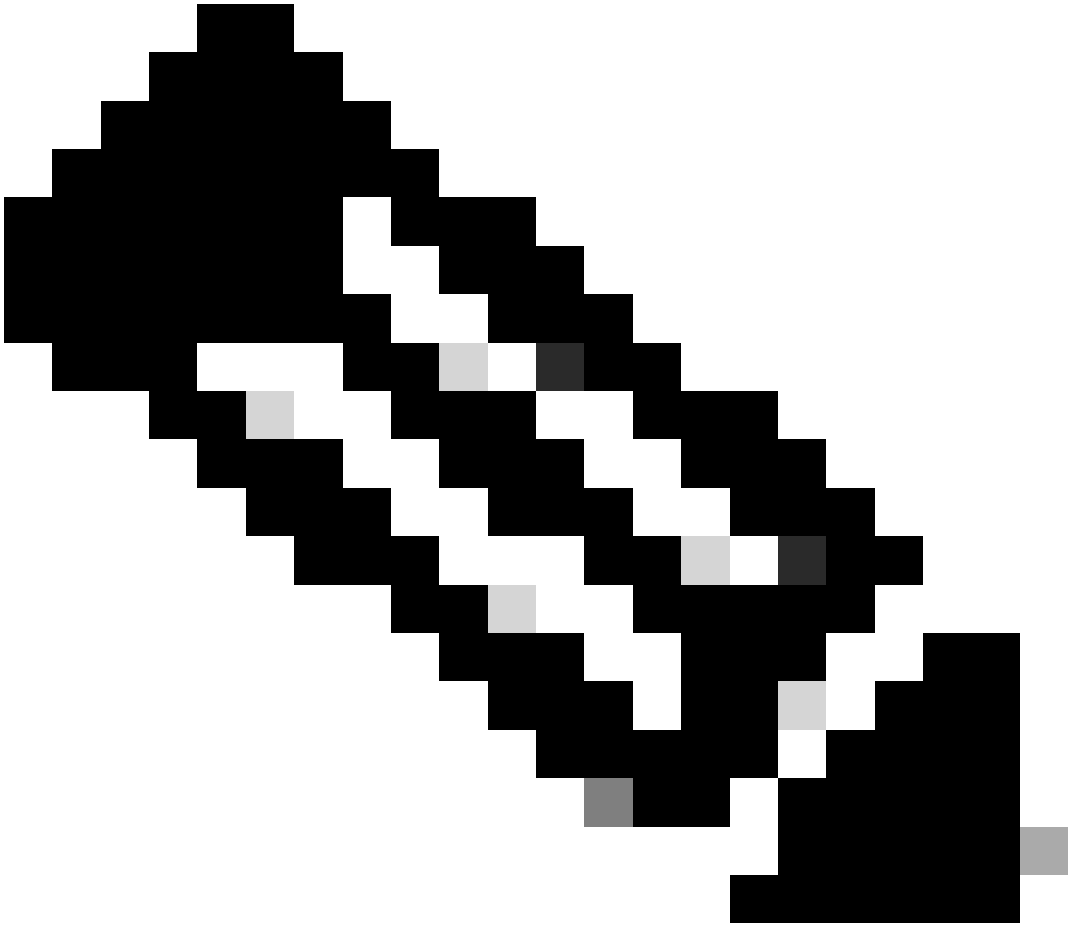
Si toutes les connexions de contrôle sont activées, le périphérique dispose d'une connexion de contrôle formée avec vBond, vManage et vSmart. Une fois les connexions vSmart et vManage requises établies, la connexion de contrôle vBond est interrompue.



Remarque : s'il n'y a qu'un seul vSmart dans la superposition et que max-control connections est défini sur la valeur par défaut de 2, une connexion de contrôle permanente est maintenue vers vBond en plus de la connexion attendue vers vManage et vSmart.

Cette configuration est disponible sous la configuration tunnel-interface de la section sdwan interface. Vous pouvez le vérifier à l'aide de la commande show sdwan run sdwan. Si max-control-connection est configuré à 0 sur l'interface, le routeur ne forme pas de connexion de contrôle sur cette interface.

S'il y a 2 vSmarts dans la superposition, le routeur forme une connexion de contrôle à chaque vSmarts sur chaque couleur TLOC (Transport Locator) configurée pour les connexions de contrôle.



Remarque : la connexion de contrôle à vManage est formée sur une seule couleur d'interface du routeur dans un scénario où le routeur a plusieurs interfaces configurées pour former des connexions de contrôle.

```
SD-WAN-Router#show sdwan control connections
                                                                                                PEER
PEER    PEER PEER            SITE       DOMAIN PEER                                            PRIV  PEER
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                                      PORT  PUBLIC IP
-------------------------------------------------------------------------------------------------------------
vsmart  dtls 10.1.1.3        1          1      10.106.50.254                                   12346 10.106.50.
vbond   dtls  0.0.0.0        0          0      10.106.50.235                                   12346 10.106.50.
vmanage dtls 10.1.1.2        1          0      10.106.65.182                                   12346 10.106.65.
```

Dépannage des connexions de contrôle

Dans le résultat de show sdwan control connections, si toutes les connexions de contrôle requises

ne sont pas activées, vérifiez le résultat de show sdwan control connection-history.

```
SD-WAN-Router#show sdwan control connection-history

Legend for Errors

ACSRREJ    - Challenge rejected by peer.              NOVMCFG   - No cfg in vmanage for device.
BDSGVERFL  - Board ID Signature Verify Failure.       NOZTPEN   - No/Bad chassis-number entry in ZTP.
BIDNTPR    - Board ID not Initialized.                OPERDOWN  - Interface went oper down.
BIDNTVRFD  - Peer Board ID Cert not verified.         ORPTMO    - Server's peer timed out.
BIDSIG    - Board ID signing failure.                 RMGSPR    - Remove Global saved peer.
CERTEXPRD  - Certificate Expired                      RXTRDWN   - Received Teardown.
CRTREJSER  - Challenge response rejected by peer.     RDSIGFBD  - Read Signature from Board ID failed.
CRTVERFL   - Fail to verify Peer Certificate.         SERNTPRES - Serial Number not present.
CTORGNMMIS - Certificate Org name mismatch.           SSLNFAIL  - Failure to create new SSL context.
DCONFAIL   - DTLS connection failure.                 STNMODETD - Teardown extra vBond in STUN server
DEVALC     - Device memory Alloc failures.            SYSIPCHNG - System-IP changed.
DHSTMO     - DTLS HandShake Timeout.                  SYSPRCH   - System property changed
DISCVBD    - Disconnect vBond after register reply.   TMRALC    - Timer Object Memory Failure.
DISTLOC    - TLOC Disabled.                           TUNALC    - Tunnel Object Memory Failure.
DUPCLHELO  - Recd a Dup Client Hello, Reset Gl Peer.  TXCHTOBD  - Failed to send challenge to BoardID.
DUPSER     - Duplicate Serial Number.                 UNMSGBDRG - Unknown Message type or Bad Register
DUPSYSIPDEL- Duplicate System IP.                     UNAUTHEL  - Recd Hello from Unauthenticated peer
HAFAIL     - SSL Handshake failure.                   VBDEST    - vDaemon process terminated.
IP_TOS     - Socket Options failure.                  VECRTREV  - vEdge Certification revoked.
LISFD      - Listener Socket FD Error.                VSCRTREV  - vSmart Certificate revoked.
MGRTBLCKD  - Migration blocked. Wait for local TMO.   VB_TMO    - Peer vBond Timed out.
MEMALCFL   - Memory Allocation Failure.               VM_TMO    - Peer vManage Timed out.
NOACTVB    - No Active vBond found to connect.        VP_TMO    - Peer vEdge Timed out.
NOERR      - No Error.                                VS_TMO    - Peer vSmart Timed out.
NOSLPRCRT  - Unable to get peer's certificate.        XTVMTRDN  - Teardown extra vManage.
NEWVBNOVMNG- New vBond with no vMng connections.      XTVSTRDN  - Teardown extra vSmart.
NTPRVMINT  - Not preferred interface to vManage.      STENTRY    - Delete same tloc stale entry.
HWCERTREN  - Hardware vEdge Enterprise Cert Renewed   HWCERTREV - Hardware vEdge Enterprise Cert Revok
EMBARGOFAIL - Embargo check failed

                                                                          PEER                    PEER
PEER     PEER     PEER            SITE       DOMAIN PEER               PRIVATE  PEER           PUBLIC
TYPE     PROTOCOL SYSTEM IP       ID         ID     PRIVATE IP         PORT     PUBLIC IP      PORT
-------------------------------------------------------------------------------------------------------
vbond    dtls     0.0.0.0         0          0      10.106.50.235      12346    10.106.50.235  12346
vbond    dtls     0.0.0.0         0          0      10.106.50.235      12346    10.106.50.235  12346
vbond    dtls     0.0.0.0         0          0      10.106.50.235      12346    10.106.50.235  12346
vbond    dtls     0.0.0.0         0          0      10.106.50.235      12346    10.106.50.235  12346
vmanage  dtls    10.1.1.2         1          0      10.106.65.182      12346    10.106.65.182  12346
vsmart   dtls    10.1.1.3         1          1      10.106.50.254      12346    10.106.50.254  12346
vbond    dtls     0.0.0.0         0          0      10.106.50.235      12346    10.106.50.235  12346
vbond    dtls     0.0.0.0         0          0      10.106.50.235      12346    10.106.50.235  12346
vbond    dtls     0.0.0.0         0          0      10.106.50.235      12346    10.106.50.235  12346
vbond    dtls     0.0.0.0         0          0      10.106.50.235      12346    10.106.50.235  12346
vbond    dtls     0.0.0.0         0          0      10.106.50.235      12346    10.106.50.235  12346
vbond    dtls     0.0.0.0         0          0      10.106.50.235      12346    10.106.50.235  12346
vbond    dtls     0.0.0.0         0          0      10.106.50.235      12346    10.106.50.235  12346
```

Dans la sortie show sdwan control connection-history, vérifiez ces éléments :

- Type de contrôleur auquel la connexion de contrôle échoue à un horodatage donné.
- Erreur constatée lors de l'échec de la connexion de contrôle. Il existe 2 colonnes pour les erreurs, Erreur locale et Erreur distante. L'erreur locale indique l'erreur générée par le routeur. Remote Error indique l'erreur générée par le contrôleur respectif. Il y a une légende d'erreurs au début de la sortie.

- Repeat count, indique le nombre de fois où la connexion a échoué pour la même raison.

Échecs courants de code d'erreur

- DCONFAIL (DTLS connection Failure) : cette erreur indique une perte de paquets DTLS qui sont échangés entre le routeur et le contrôleur respectif en raison de laquelle la connexion DTLS ne peut pas être effectuée. Pour mieux comprendre cela, vous pouvez configurer des captures de paquets simultanées sur le routeur et le contrôleur respectif. Différentes méthodes de configuration des captures de paquets sont partagées dans la section Embedded Packet Capture. Lors de l'analyse des captures de paquets, il est important de s'assurer que les paquets envoyés d'une extrémité sont reçus à l'autre extrémité sans aucune modification. Si le paquet envoyé d'une extrémité n'est pas reçu à l'autre extrémité, cela indique qu'il y a une perte de paquet dans le circuit sous-jacent qui doit être vérifiée auprès du fournisseur de services. Pour plus de détails sur la façon de prendre une capture de paquets, consultez la section Problèmes sous-jacents.

- BIDNTVRFD (ID de carte non vérifié) : cette erreur indique que l'UUID et le numéro de série du certificat ne sont pas une entrée valide dans la liste vEdge du contrôleur. Vous pouvez vérifier la sortie de la liste des bords valides sur les contrôleurs en utilisant ces commandes :

<#root>

vBond:

show orchestrator valid-vedges

vManage/vSmart:

show control valid-vedges

Généralement, BIDNTVRFD est une erreur distante sur le routeur car elle est générée sur le contrôleur. Sur le contrôleur respectif, vous pouvez vérifier le journal dans le fichier vdebug situé dans le répertoire /var/log/tmplog en utilisant ces commandes :

```
vmanage# vshell
vmanage:~$ cd /var/log/tmplog/
vmanage:/var/log/tmplog$ tail -f vdebug
```

- CRTVERFL (Certificate Verification Failed) : cette erreur indique que le certificat envoyé par

l'homologue n'a pas pu être vérifié.

- S'il s'agit d'une erreur locale sur le routeur, alors il indique que le certificat du contrôleur envoyé dans le cadre de la connexion DTLS n'a pas pu être vérifié par le routeur. L'une des raisons courantes de cette situation est que le routeur ne possède pas le certificat racine de l'autorité de certification qui a signé le certificat du contrôleur. Vérifiez l'état du certificat à l'aide de ces commandes pour vous assurer que le certificat racine requis est présent sur le routeur.

```
show sdwan certificate root-ca-cert
show sdwan certificate root-ca-cert | inc Issuer
```

- Si cette erreur est une erreur distante sur le routeur, vérifiez le fichier journal vdebug sur le contrôleur respectif pour comprendre la cause à l'aide de ces commandes :

```
vmanage# vshell
vmanage:~$ cd /var/log/tmplog/
vmanage:/var/log/tmplog$ tail -f vdebug
```

- VB_TMO (vBond Timeout) / VM_TMO (vManage Timeout) / VP_TMO (vPeer Timeout) / VS_TMO (vSmart Timeout) : ces erreurs indiquent qu'il y a eu une perte de paquets entre les périphériques, ce qui entraîne l'expiration de la connexion de contrôle. Pour mieux comprendre cela, vous pouvez configurer des captures de paquets simultanées sur le routeur et le contrôleur respectif. Différentes méthodes de configuration des captures de paquets sont partagées dans la section Embedded Packet Capture. Lors de l'analyse des captures de paquets, il est important de s'assurer que les paquets envoyés d'une extrémité sont reçus à l'autre extrémité sans aucune modification. Si le paquet envoyé d'une extrémité n'est pas reçu à l'autre extrémité, cela indique qu'il y a une perte de paquet dans le circuit sous-jacent qui doit être vérifiée auprès du fournisseur de services

Pour obtenir des conseils sur la façon de dépanner d'autres codes d'erreur d'échec de connexion de contrôle, vous pouvez vous reporter à ce document :

Dépannage des connexions de contrôle SD-WAN

Problèmes sous-jacents

Les outils utilisés pour dépanner la perte de paquets dans le sous-réseau diffèrent selon les périphériques. Pour les contrôleurs SD-WAN et les routeurs vEdge, vous pouvez utiliser la commande tcpdump. Pour les périphériques Catalyst IOS® XE, utilisez Embedded Packet Capture (EPC) et la trace FIA (Feature Invocation Array).

Pour comprendre pourquoi les connexions de contrôle échouent et pour comprendre où se situe le

problème, vous devez comprendre où se produit la perte de paquets. Par exemple, si vous disposez d'un routeur vBond et Edge ne formant pas de connexion de contrôle, ce guide explique comment isoler le problème.

Dépôt TCP

```
tcpdump vpn 0 interface ge0/0 options "host 10.1.1.x -vv"
```

En fonction de la demande et de la réponse des paquets, l'utilisateur peut comprendre le périphérique responsable des abandons. La commande tcpdump peut être utilisée sur tous les contrôleurs et périphériques vEdge.

Capture de paquets intégrée

Créez une liste de contrôle d’accès sur le périphérique.

```
ip access-list extended TAC
10 permit ip host <edge-private-ip> host <controller-public-ip>
20 permit ip host <controller-public-ip> host <edge-private-ip>
```

Configurez et démarrez la capture de surveillance.

```
monitor capture CAP access-list TAC bidirectional
monitor capture CAP start
```

Arrêtez la capture et exportez le fichier de capture.

```
monitor capture CAP stop
monitor capture CAP export bootflash:<filename>
```

Affichez le contenu du fichier dans wireshark pour comprendre les pertes. Pour plus d'informations, consultez Configurer et capturer un paquet intégré sur le logiciel .

FIA Trace

Configurez la trace FIA.

```
debug platform condition ipv4 <ip> both
debug platform packet-trace packet 2048 fia-trace data-size 4096
debug platform condition start
```

Affichez les sorties du paquet de phrases fia.

```
debug platform condition stop
show platform packet-trace summary
show platform packet-trace summary | i DROP
```

En cas d'abandon, analysez le résultat de la commande FIA trace pour le paquet abandonné.

```
show platform packet-trace packet <packet-no> decode
```

Pour comprendre les options de trace FIA supplémentaires, consultez ce document : Dépannage avec la fonctionnalité de trace de paquet de datapath IOS-XE

La vidéo Déterminer les abandons de politique sur Catalyst SD-WAN Edge avec FIA Trace fournit un exemple d'utilisation de FIA Trace.

Génération de Admin-Tech

Reportez-vous à Collecter un Admin-Tech dans un environnement SD-WAN et Télécharger vers le cas TAC - Cisco

Informations connexes

Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.