Problemen met veelvoorkomende SD-WAN controle- en dataplane oplossen

Inhoud

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen met de SD-WAN-controle (Common Software Defined Wide Area Network) en problemen met het dataplatform.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van Cisco Catalyst-oplossing.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële

impact van elke opdracht begrijpt.

Overzicht

Dit artikel is ontworpen als een runbook om een startplaats te bieden voor het debuggen van uitdagingen in verschillende productieomgevingen. Elke sectie biedt veelvoorkomende gebruikscases en waarschijnlijke datapunten om te verzamelen of te zoeken wanneer u deze vaak geziene problemen zuivert.

Basisconfiguraties

Zorg ervoor dat de basisconfiguraties op de router aanwezig zijn en dat de apparaat-specifieke waarden voor elk apparaat in bekleding uniek zijn:

Systeemconfiguraties

<#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
!
```

Interfaceconfiguraties

```
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
```

Zorg ervoor dat de router een route heeft beschikbaar is in de routeringstabel om een controleverbinding met de controllers tot stand te brengen (vBond, vManager en vSmart). U kunt dit bevel gebruiken om alle routes te zien die in de routeringstabel worden geïnstalleerd:

```
show ip route
```

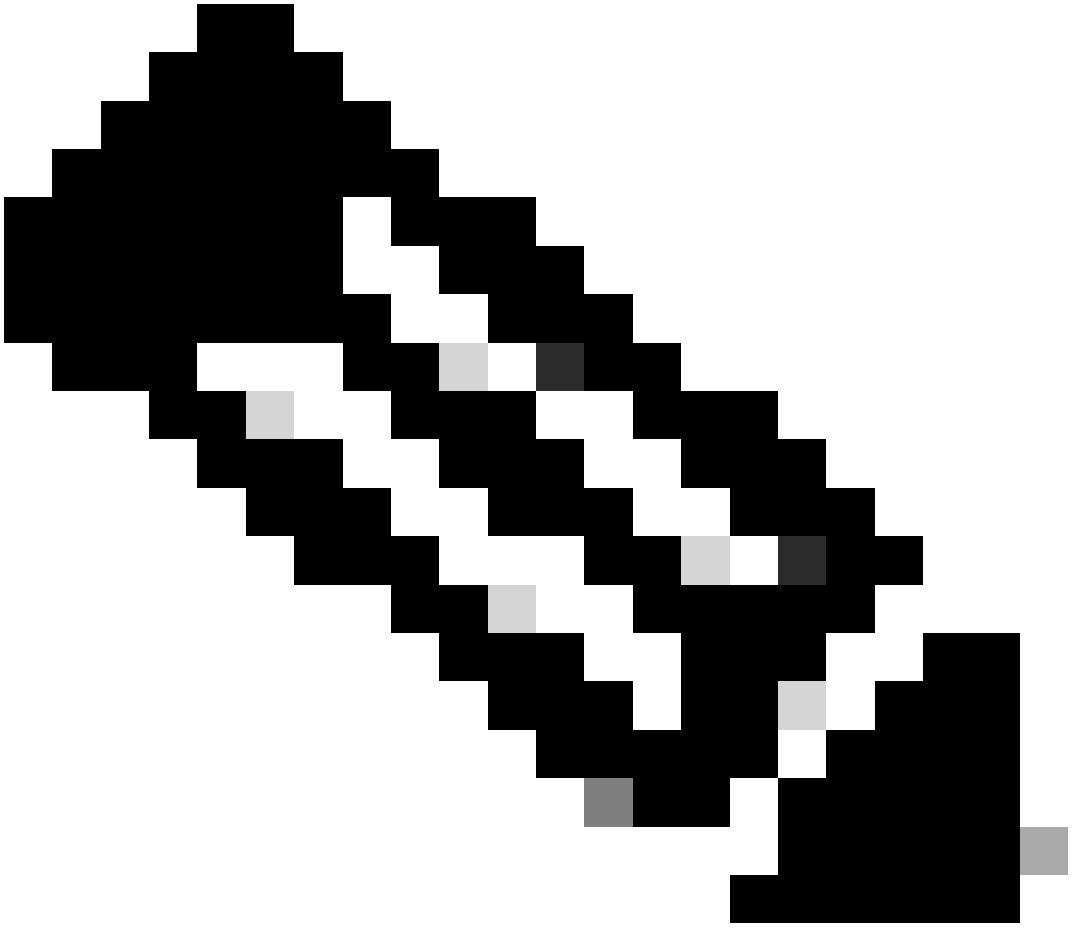
Als u vBond FQDN gebruikt, zorg er dan voor dat de DNS-server of naamserver geconfigureerd een ingang heeft om vBond hostname op te lossen. U kunt controleren welke DNS-server of naamserver met deze opdracht is geconfigureerd:

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

Certificaat

Controleer dat het certificaat op de router is geïnstalleerd met deze opdracht:

```
show sdwan certificate installed
```



Opmerking:Als u geen Enterprise-certificaten gebruikt, is het certificaat al beschikbaar op de routers. Voor hardwareplatforms, zijn de apparatencertificaten ingebouwde aan de routerhardware. Voor virtuele routers fungeert vManager als certificeringsinstantie en genereert het de certificaten voor cloudrouters.

Als u Enterprise-certificaten op de controllers gebruikt, zorg er dan voor dat het basiscertificaat van de Enterprise CA op de router is geïnstalleerd.

Controleer of de basiscertificaten op de router zijn geïnstalleerd met deze opdrachten:

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

Controleer de uitvoer van show sdwan control local-Properties om er zeker van te zijn dat de vereiste configuraties en certificaten aanwezig zijn.

```
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   ::
```

Bij het controleren van de output van show sdwan control local-Properties, zorg ervoor dat al deze criteria worden voldaan:

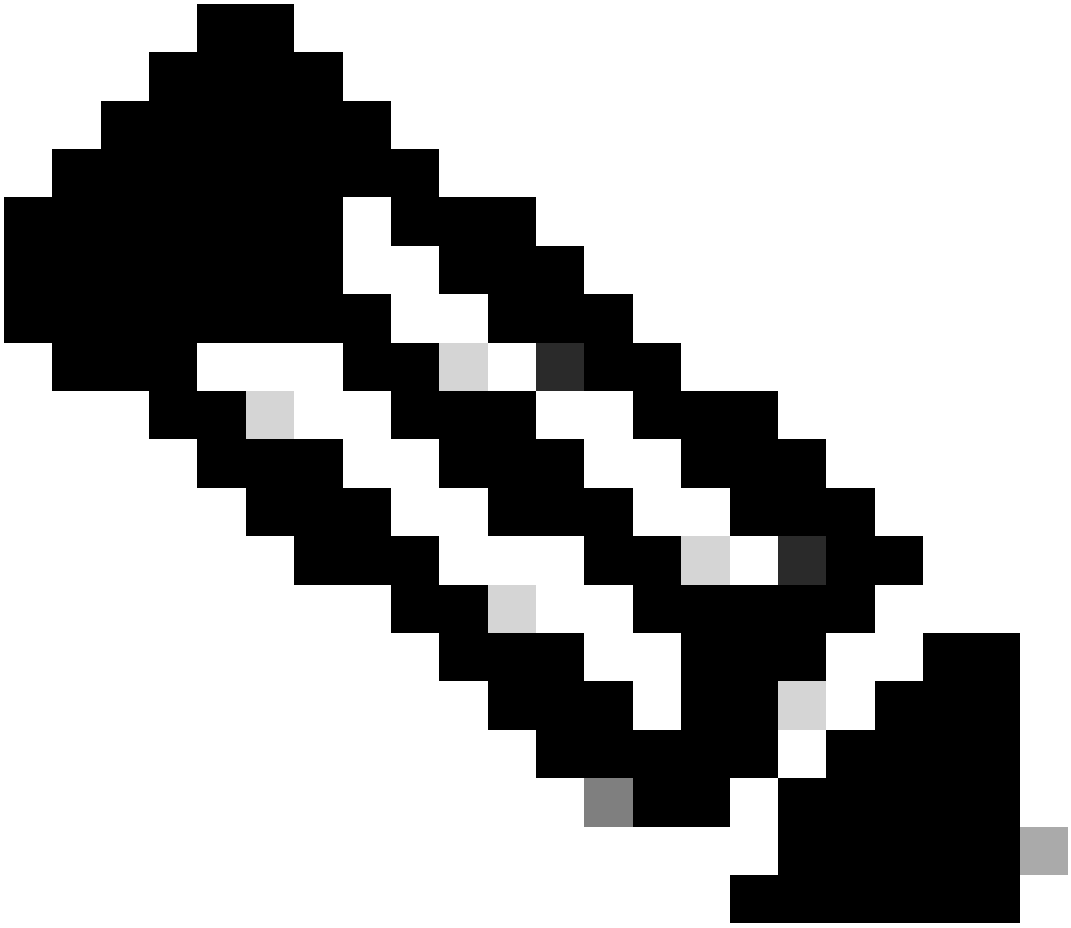
- De naam van de organisatie wordt correct weergegeven.
- De geldigheid van het certificaat is geldig op het moment dat u de uitvoer controleert.
- Het FQDN/IP-adres van de vBond is correct.
- Systeemip/Site-id is correct.
- Het IP-adres van vBond wordt weergegeven in de vermelding voor "number-vbond-peers". Als het IP-adres van de vBond niet wordt weergegeven, controleert u of DNS voor de vBond-URL wordt opgelost met behulp van de opdracht ping <vBond FQDN>.
- De interfaces worden in kaart gebracht met de juiste kleur, IP-adres en de status van de interface is UP.
- De MAX CNTRL die nodig is om een verbinding te vormen is niet 0.

Status van Control Connections

Controleer de status van de besturingsverbinding met behulp van deze opdracht:

```
show sdwan control connection
```

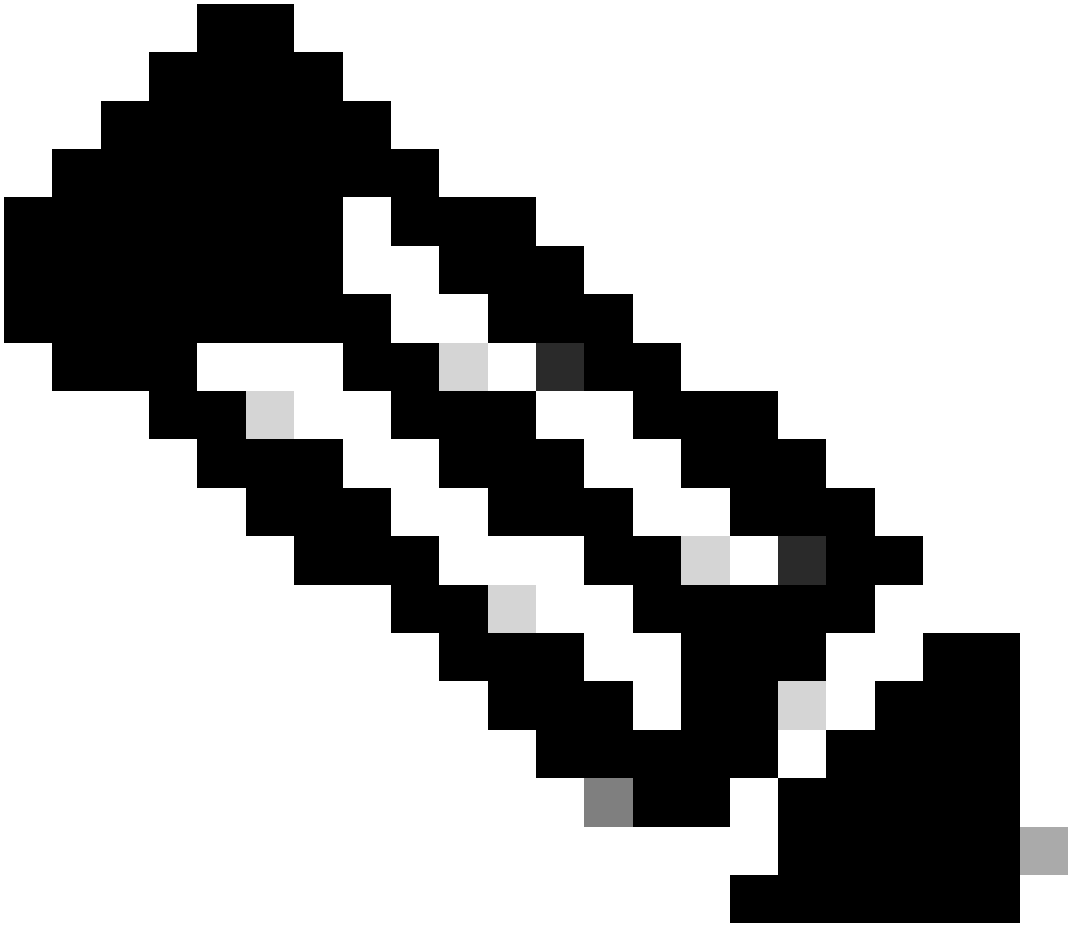
Als alle besturingsverbindingen zijn ingeschakeld, is op het apparaat een besturingsverbinding tot stand gebracht met vBond, vManager en vSmart. Zodra de vereiste vSmart- en vManager-verbindingen zijn gemaakt, wordt de vBond-besturingsverbinding verbroken.



Opmerking: als er slechts één vSmart in de overlay-out is en de max-control-verbindingen zijn ingesteld op de standaardwaarde van 2, blijft er naast de verwachte verbinding met vManager en vSmart een persistente besturingsverbinding met vBond behouden.

Deze configuratie is beschikbaar onder de tunnelinterfaceconfiguratie van de sdwan interfacesectie. U kunt het verifiëren met behulp van de opdracht show sdwan run sdwan. Als max-control-connection is ingesteld op 0 op de interface, vormt de router geen control-verbinding op die interface.

Als er 2 vSmarts zijn in de overlay, vormt de router een besturingsverbinding met elke vSmart op elke TLOC-kleur (Transport Locator) die is geconfigureerd voor besturingsverbindingen.



Opmerking: de besturingsverbinding met vManager wordt alleen gevormd op één interfacekleur van de router in een scenario waarin de router meerdere interfaces heeft geconfigureerd om besturingsverbindingen te vormen.

```
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.
```

Aansluitingen voor probleemoplossing

In de output van show sdwan control connections, als alle vereiste control connecties niet omhoog

zijn, verifieer de output van 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 r
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
vbond    dtls     0.0.0.0          0           0      10.106.50.235    12346    10.106.50.235     12346
```

Controleer in de uitvoer van de verbindingsgeschiedenis van de vertragingscontrole van de show

deze items:

- Het type controller waarop de besturingsverbinding op een gegeven tijdstempel niet werkt.
- De fout die is opgetreden tijdens het uitvallen van de besturingsverbinding. Er zijn 2 kolommen voor fouten, lokale fout en externe fout. Lokale fout geeft de fout aan die door de router is gegenereerd. Remote Error geeft de fout aan die door de betreffende controller is gegenereerd. Er is een legende van fouten aan het begin van de output.

- Herhaal de telling, geeft het aantal keren aan dat de verbinding om dezelfde reden is mislukt.

Veelvoorkomende fouten in foutcodes

- DCONFAIL (DTLS-verbindingsfout): Deze fout geeft aan dat er DTLS-pakketten verloren gaan die worden uitgewisseld tussen de router en de respectieve controller, waardoor de DTLS-handdruk niet kan worden voltooid. Om dit beter te begrijpen, kunt u gelijktijdige pakketopnamen op router en respectieve controller instellen. Verschillende methoden voor het instellen van pakketopnamen worden gedeeld in de sectie Ingesloten pakketvastlegging. Terwijl het analyseren van het pakket vangt, is het belangrijk om ervoor te zorgen de pakketten die van één eind worden verzonden aan het andere eind zonder enige wijzigingen worden ontvangen. Als het pakket dat van één eind wordt verzonden niet aan het andere eind wordt ontvangen, wijst dit op er pakketverlies in de ondergrondse kring is die met de dienstverlener moet worden geverifieerd. Meer informatie over het nemen van een pakketopname is te vinden in de sectie Onderliggende problemen.

- BIDNTVRFD (Board ID niet geverifieerd): Deze fout geeft aan dat de UUID en het serienummer van het certificaat geen geldige vermelding zijn in de vEdge-lijst van de controller. U kunt de output van de geldige randlijst op de controllers controleren met behulp van deze opdrachten:

<#root>

vBond:

show orchestrator valid-vedges

vManage/vSmart:

show control valid-vedges

Gewoonlijk is BIDNTVRFD een externe fout op de router omdat het op de controller is gegenereerd. Op de respectieve controller kunt u de login van het vdebug bestand in de map /var/log/tmplog verifiëren met behulp van deze opdrachten:

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

- CRTVERFL (certificaatverificatie mislukt): Deze fout geeft aan dat het door de peer verzonden certificaat niet kon worden geverifieerd.
- Als dit een lokale fout op de router is, dan wijst het op het certificaat van het controlemechanisme dat als deel van handdruk DTLS wordt verzonden kon niet door de router worden geverifieerd. Een van de gemeenschappelijke redenen hiervoor is router heeft niet het basiscertificaat van de certificeringsinstantie die het controllercertificaat heeft ondertekend. Controleer de status van het certificaat met deze opdrachten om er zeker van te zijn dat het vereiste basiscertificaat op de router aanwezig is.

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

- Als deze fout een externe fout op de router is, controleer het vdebug logbestand op de betreffende controller om de oorzaak te begrijpen met deze opdrachten:

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

- VB_TMO (vBond Timeout) / VM_TMO (vManager Timeout) / VP_TMO (vPeer Timeout) / VS_TMO (vSmart Timeout): Deze fouten duiden erop dat er pakketverlies tussen de apparaten was, wat ervoor zorgt dat de besturingsverbinding uitviel. Om dit beter te begrijpen, kunt u gelijktijdige pakketopnamen op de router en respectieve controller instellen. Verschillende methoden voor het instellen van pakketopnamen worden gedeeld in de sectie Ingesloten pakketvastlegging. Terwijl het analyseren van het pakket vangt, is het belangrijk om ervoor te zorgen de pakketten die van één eind worden verzonden aan het andere eind zonder enige wijzigingen worden ontvangen. Als het pakket dat van het ene uiteinde wordt verzonden niet aan het andere uiteinde wordt ontvangen, geeft dit aan dat er pakketverlies in het onderlegcircuit zit dat bij de serviceprovider moet worden geverifieerd

Voor richtlijnen voor het oplossen van foutcodes bij andere fouten in besturingsverbindingen kunt u dit document raadplegen:

Probleemoplossing voor SD-WAN Control Connections

Onderliggende problemen

De tools die worden gebruikt om pakketverlies in de ondergrond op te lossen, verschillen van apparaat tot apparaat. Voor SD-WAN controllers en vEdge-router kunt u de opdracht TCP gebruiken. Gebruik voor Catalyst IOS® XE-randen ingesloten pakketvastlegging (EPC) en

functieaanroeping (FIA) om te traceren.

Om te begrijpen waarom de controleverbindingen ontbreken en begrijpen waar het probleem ligt, moet u begrijpen waar het pakketverlies gebeurt. Als u bijvoorbeeld een vBond en Edge-router hebt die geen controleverbinding vormt, wordt in deze handleiding geïllustreerd hoe u het probleem kunt isoleren.

TCP-pomp

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

Op basis van het verzoek en de reactie van de pakketten kan de gebruiker het apparaat dat verantwoordelijk is voor de druppels begrijpen. De opdracht tcpdump kan op alle controllers en vEdge-apparaten worden gebruikt.

Ingesloten pakketvastlegging

Maak een ACL op het apparaat.

```
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>
```

Configureer de monitor en start de opname.

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

Stop de opname en exporteer het opnamebestand.

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

Bekijk de inhoud van het bestand in wireshark om de druppels te begrijpen. U vindt aanvullende

informatie over het configureren en opnemen van ingesloten pakketten op software .

FIA Trace

Configureer het FIA-spoor.

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

Bekijk de fia frase pakketuitgangen.

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

Als er een val is, parse de FIA spooroutput voor het gelaten vallen pakket.

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

Als u meer opties voor FIA-tracering wilt begrijpen, raadpleegt u dit document: Probleemoplossing met de functie IOS-XE Datapath Packet Trace

De Determine Policy Drops op Catalyst SD-WAN Edge met FIA Trace-video biedt een voorbeeld van het gebruik van FIA-spoor.

Admin-Tech genereren

Raadpleeg Admin-Tech in SD-WAN omgeving verzamelen en naar TAC-case uploaden - Cisco

Gerelateerde informatie

Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.