Risoluzione dei problemi comuni relativi al controllo SD-WAN e al piano dati

Sommario

Introduzione

Questo documento descrive come avviare la risoluzione dei problemi comuni relativi al controllo SD-WAN (Software Defined Wide Area Network) e al piano dati.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza della soluzione Cisco Catalyst.

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.

Panoramica

Questo articolo è stato concepito come un runbook per fornire un punto di partenza per le sfide di debug rilevate in tutti gli ambienti di produzione. Ogni sezione fornisce casi di utilizzo comuni e punti dati probabili da raccogliere o cercare quando si esegue il debug di questi problemi comuni.

Configurazioni di base

Verificare che le configurazioni di base siano presenti sul router e che i valori specifici del dispositivo siano univoci per ogni dispositivo sovrapposto:

Configurazioni del sistema

<#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
!
```

Configurazioni interfaccia

```
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
```

Accertarsi che il router disponga di routing disponibile nella tabella di routing per stabilire una connessione di controllo con i controller (vBond, vManage e vSmart). È possibile utilizzare questo comando per visualizzare tutte le route installate nella tabella di routing:

```
show ip route
```

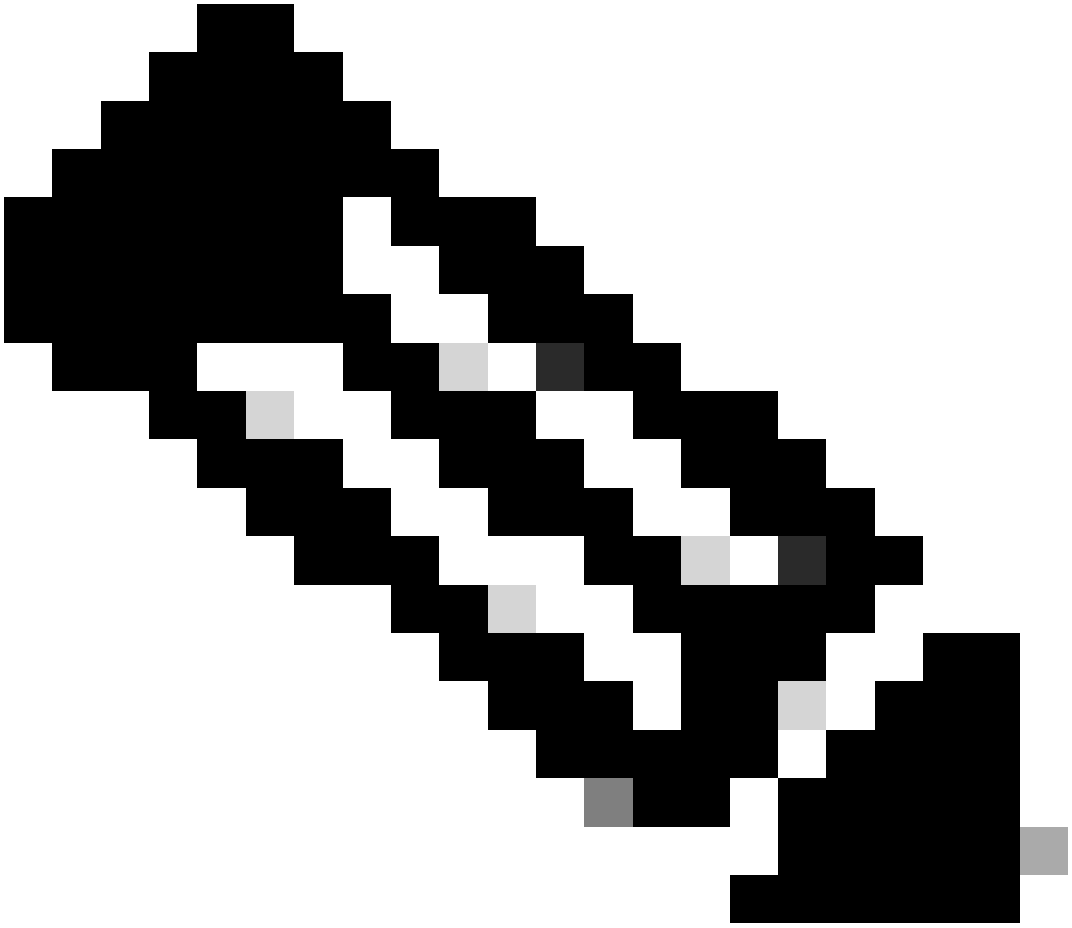
Se si utilizza l'FQDN vBond, verificare che il server DNS o il server dei nomi configurato disponga di una voce per risolvere il nome host vBond. È possibile verificare quale server DNS o server dei nomi è configurato con questo comando:

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

Certificato

Verificare che il certificato sia installato sul router utilizzando questo comando:

```
show sdwan certificate installed
```



Nota: se non si utilizzano certificati Enterprise, il certificato è già disponibile sui router. Per le piattaforme hardware, i certificati dei dispositivi sono incorporati nell'hardware del router. Per i router virtuali, vManage funge da autorità di certificazione e genera i certificati per i router cloud.

Se si utilizzano certificati Enterprise nei controller, verificare che il certificato radice della CA Enterprise sia installato nel router.

Verificare che i certificati radice siano installati sul router utilizzando questi comandi:

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

Controllare l'output di show sdwan control local-properties per assicurarsi che le configurazioni e i certificati richiesti siano presenti.

```
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   ::
```

Quando si controlla l'output di show sdwan control local-properties, verificare che siano soddisfatti tutti i seguenti criteri:

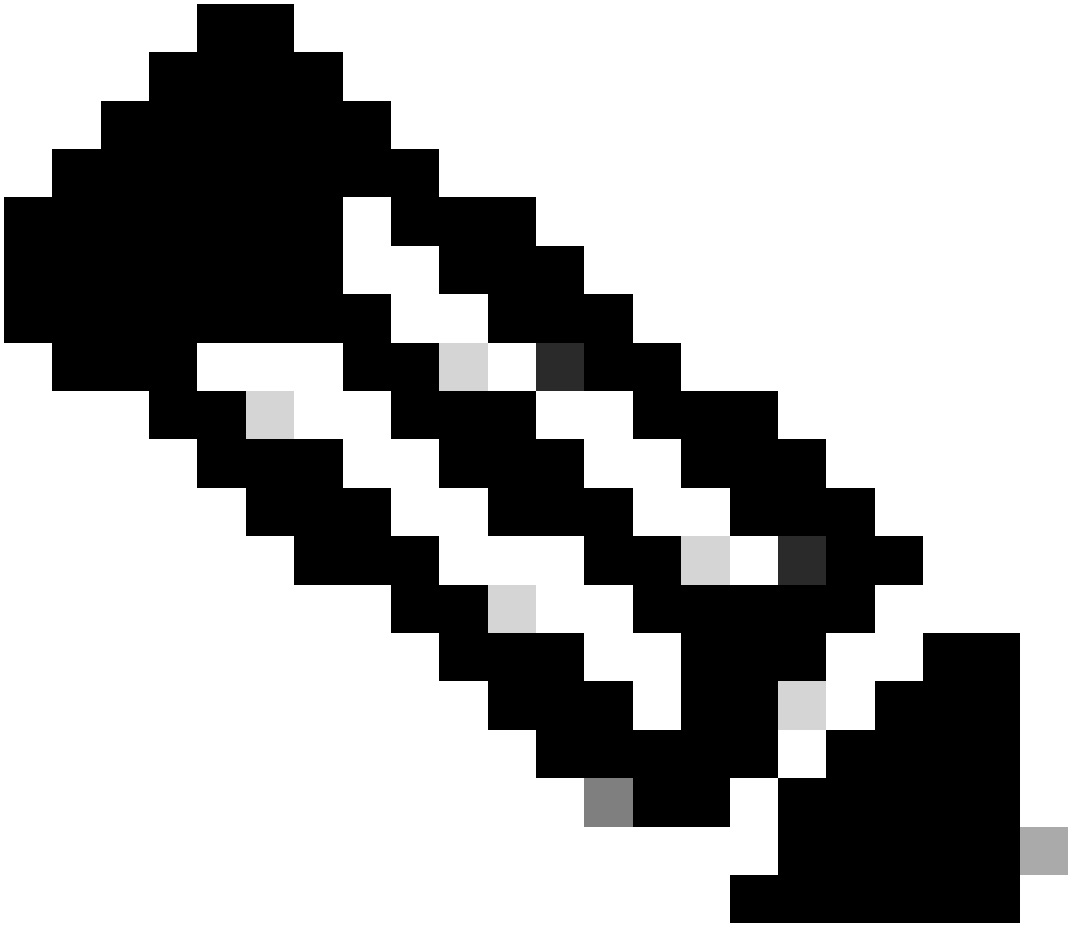
- Il nome dell'organizzazione viene riflesso correttamente.
- La validità del certificato è valida al momento del controllo dell'output.
- L'indirizzo IP/FQDN vBond è corretto.
- System-ip/Site-id è corretto.
- L'indirizzo IP vBond è indicato nella voce "number-vbond-peers". Se l'indirizzo IP vBond non viene visualizzato, verificare che DNS stia eseguendo la risoluzione dell'URL vBond utilizzando il comando ping <FQDN vBond>.
- Le interfacce sono mappate con il colore corretto, l'indirizzo IP e lo stato dell'interfaccia è ATTIVO.
- Il valore di MAX CNTRL per l'interfaccia necessaria a formare la connessione di controllo non è 0.

Stato delle connessioni di controllo

Verificare lo stato della connessione di controllo utilizzando questo comando:

```
show sdwan control connection
```

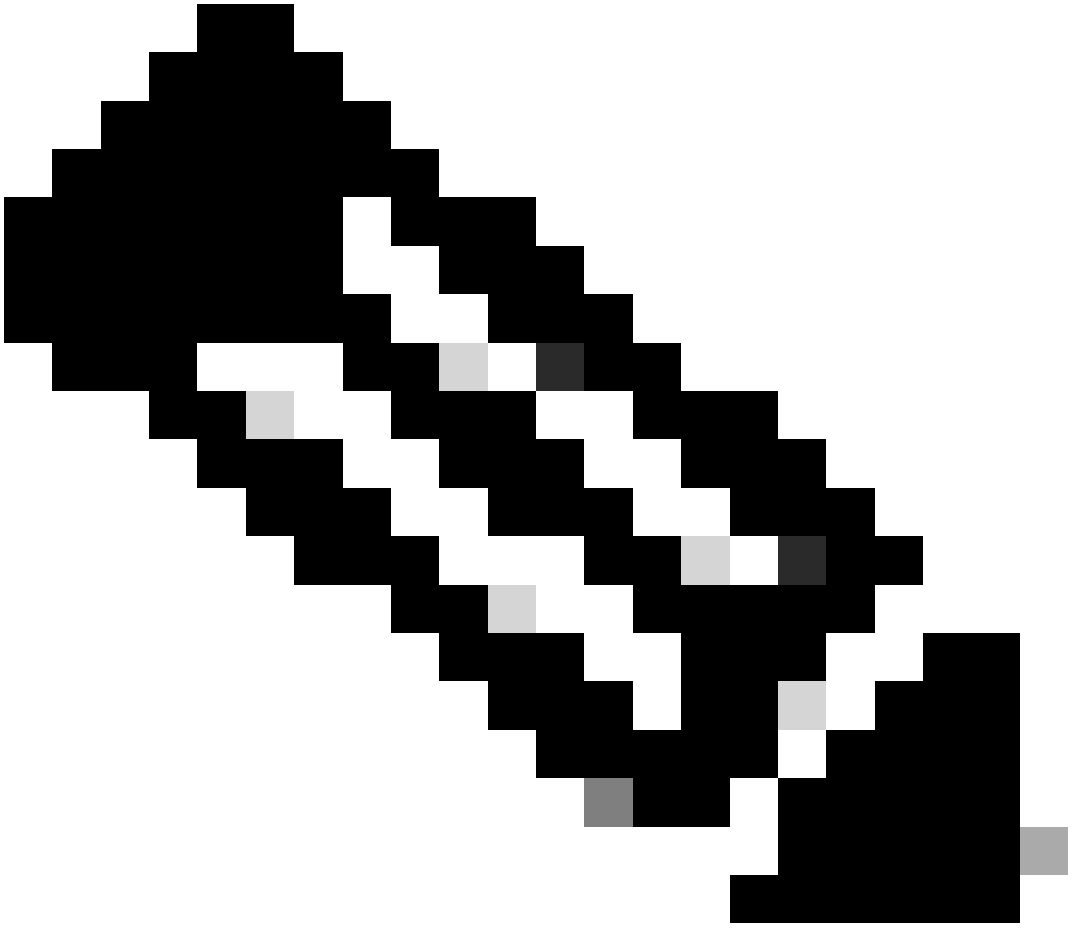
Se tutte le connessioni di controllo sono attive, il dispositivo dispone di una connessione di controllo formata da vBond, vManage e vSmart. Una volta stabilite le connessioni vSmart e vManage necessarie, la connessione di controllo vBond viene disattivata.



Nota: se nella sovrapposizione è presente un solo vSmart e max-control connections è impostato sul valore predefinito di 2, oltre alla connessione prevista a vManage e vSmart viene mantenuta una connessione di controllo persistente a vBond.

Questa configurazione è disponibile nella configurazione dell'interfaccia tunnel della sezione dell'interfaccia sdwan. Per verificarlo, usare il comando show sdwan run sdwan. Se max-control-connection è configurato su 0 sull'interfaccia, il router non crea una connessione di controllo su quell'interfaccia.

Se nella sovrapposizione sono presenti 2 vSmarts, il router forma una connessione di controllo a ciascun vSmart su ogni colore Transport Locator (TLOC) configurato per le connessioni di controllo.



Nota: la connessione di controllo a vManage è formata solo su un colore di interfaccia del router in uno scenario in cui il router dispone di più interfacce configurate per formare connessioni di controllo.

```
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.
```

Risoluzione dei problemi relativi alle connessioni di controllo

Nell'output di show sdwan control connections, se tutte le connessioni di controllo necessarie non

sono attive, verificare l'output di 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
```

Nell'output show sdwan control connection-history, verificare i seguenti elementi:

- Tipo di controller a cui si è verificato un errore della connessione del controllo a un determinato timestamp.
- Errore rilevato quando la connessione di controllo non è riuscita. Sono disponibili due colonne per gli errori, Errore locale ed Errore remoto. Errore locale indica l'errore generato dal router. Errore remoto indica l'errore generato dal rispettivo controller. All'inizio dell'output è presente una legenda degli errori.

- Repeat count, indica il numero di volte in cui la connessione non è riuscita per lo stesso motivo.

Errori comuni nei codici di errore

- DCONFAIL (errore di connessione DTLS): questo errore indica che si è verificata una perdita di pacchetti DTLS scambiati tra il router e il rispettivo controller a causa della quale non è possibile completare l'handshake DTLS. Per comprendere meglio questa condizione, è possibile configurare le acquisizioni simultanee dei pacchetti sul router e sul rispettivo controller. Nella sezione Embedded Packet Capture vengono condivisi diversi metodi di impostazione delle acquisizioni dei pacchetti. Durante l'analisi delle acquisizioni dei pacchetti, è importante assicurarsi che i pacchetti inviati da un'estremità vengano ricevuti dall'altra estremità senza modifiche. Se il pacchetto inviato da un'estremità non viene ricevuto dall'altra, il circuito sottostante contiene una perdita di pacchetto che deve essere verificata con il provider di servizi. Per ulteriori informazioni su come acquisire un pacchetto, consultare la sezione Problemi di underlay.

- BIDNTVRFD (ID scheda non verificato): questo errore indica che l'UUID e il numero di serie del certificato non sono voci valide nell'elenco vEdge del controller. È possibile controllare l'output dell'elenco vedge valido sui controller utilizzando i seguenti comandi:

<#root>

vBond:

show orchestrator valid-vedges

vManage/vSmart:

show control valid-vedges

In genere, BIDNTVRFD è un errore remoto sul router perché è generato sul controller. Sul rispettivo controller, è possibile verificare il log nel file vdebug che si trova nella directory /var/log/tmplog utilizzando i seguenti comandi:

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

- CRTVERFL (verifica certificato non riuscita): questo errore indica che non è stato possibile verificare il certificato inviato dal peer.
- Se si tratta di un errore locale sul router, indica che il certificato del controller inviato come parte dell'handshake DTLS non può essere verificato dal router. Uno dei motivi più comuni è che il router non dispone del certificato radice dell'autorità di certificazione che ha firmato il certificato del controller. Verificare lo stato del certificato con questi comandi per assicurarsi che il certificato radice richiesto sia presente sul router.

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

- Se l'errore è remoto sul router, controllare il file di registro vdebug sul controller in uso per individuare la causa dell'errore e usare i seguenti comandi:

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

- VB_TMO (Timeout vBond) / VM_TMO (Timeout vManage) / VP_TMO (Timeout vPeer) / VS_TMO (Timeout vSmart): questi errori indicano che si è verificata una perdita di pacchetti tra i dispositivi, che causa il timeout della connessione di controllo. Per comprendere meglio questa condizione, è possibile configurare le acquisizioni simultanee dei pacchetti sul router e sul rispettivo controller. Nella sezione Embedded Packet Capture vengono condivisi diversi metodi di impostazione delle acquisizioni dei pacchetti. Durante l'analisi delle clip dei pacchetti, è importante assicurarsi che i pacchetti inviati da un'estremità vengano ricevuti dall'altra estremità senza modifiche. Se il pacchetto inviato da un'estremità non viene ricevuto dall'altra, significa che si è verificata una perdita di pacchetto nel circuito sottostante, che deve essere verificata con il provider di servizi

Per informazioni sulla risoluzione dei problemi relativi ad altri codici di errore di connessione del controllo, fare riferimento a questo documento:

Risoluzione dei problemi relativi alle connessioni di controllo SD-WAN

Problemi di underlay

Gli strumenti per risolvere i problemi di perdita dei pacchetti nella struttura sottostante variano a seconda del dispositivo. Per i controller SD-WAN e i router vEdge, è possibile usare il comando tcpdump. Per i bordi Catalyst IOS® XE, usare la traccia EPC (Embedded Packet Capture) e FIA (Feature Invocation Array).

Per capire perché le connessioni di controllo non funzionano e capire dove si trova il problema, è

necessario capire dove si sta verificando la perdita di pacchetti. Ad esempio, se un router vBond e Edge non forma una connessione di controllo, questa guida illustra come isolare il problema.

Dump TCP

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

In base alla richiesta e alla risposta dei pacchetti, l'utente può capire il dispositivo responsabile delle cadute. il comando tcpdump può essere usato su tutti i controller e i dispositivi vEdge.

Embedded Packet Capture

Creare un ACL sul dispositivo.

```
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>
```

Configurare e avviare l'acquisizione del monitor.

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

Arrestare l'acquisizione ed esportare il file di acquisizione.

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

Visualizzate il contenuto del file in wireshark per comprendere le gocce. Per ulteriori informazioni, visitare il sito Web all'indirizzo Configure and Capture Embedded Packet on Software.

Traccia FIA

Configurare la traccia FIA.

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

Visualizzare gli output del pacchetto fia phrase.

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

In caso di perdita, analizzare l'output di traccia FIA per il pacchetto perso.

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

Per ulteriori informazioni sulle opzioni di traccia FIA, consultare questo documento: Risoluzione dei problemi relativi alla funzionalità di traccia dei pacchetti datapath IOS-XE

Il video Determine Policy Drops on Catalyst SD-WAN Edge with FIA Trace fornisce un esempio di utilizzo di FIA Trace.

Generazione di Admin-Tech

Fare riferimento alla sezione sulla raccolta di informazioni su Admin-Tech in un ambiente SD-WAN e il caricamento nella richiesta TAC - Cisco

Informazioni correlate

Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).