排除常見的SD-WAN控制和資料平面問題

目錄

簡介

本文檔介紹如何開始排除常見的軟體定義廣域網(SD-WAN)控制和資料平面問題。

必要條件

需求

思科建議您瞭解Cisco Catalyst解決方案。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

本文是設計為Runbook，為調試跨生產環境中的難題提供了一個起點。 每個部分都提供了常見的使用案例和可能的資料點，以便在調試這些常見問題時進行收集或查詢。

基本配置

確定路由器上有基本組態，且重疊中的每台裝置有唯一的裝置特定值：

系統配置

<#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
!
```

介面配置

```
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
```

確保路由器的aroute在路由表中可用以建立與控制器（vBond、vManage和vSmart）的控制連線。您可以使用此命令檢視安裝在路由表中的所有路由：

```
show ip route
```

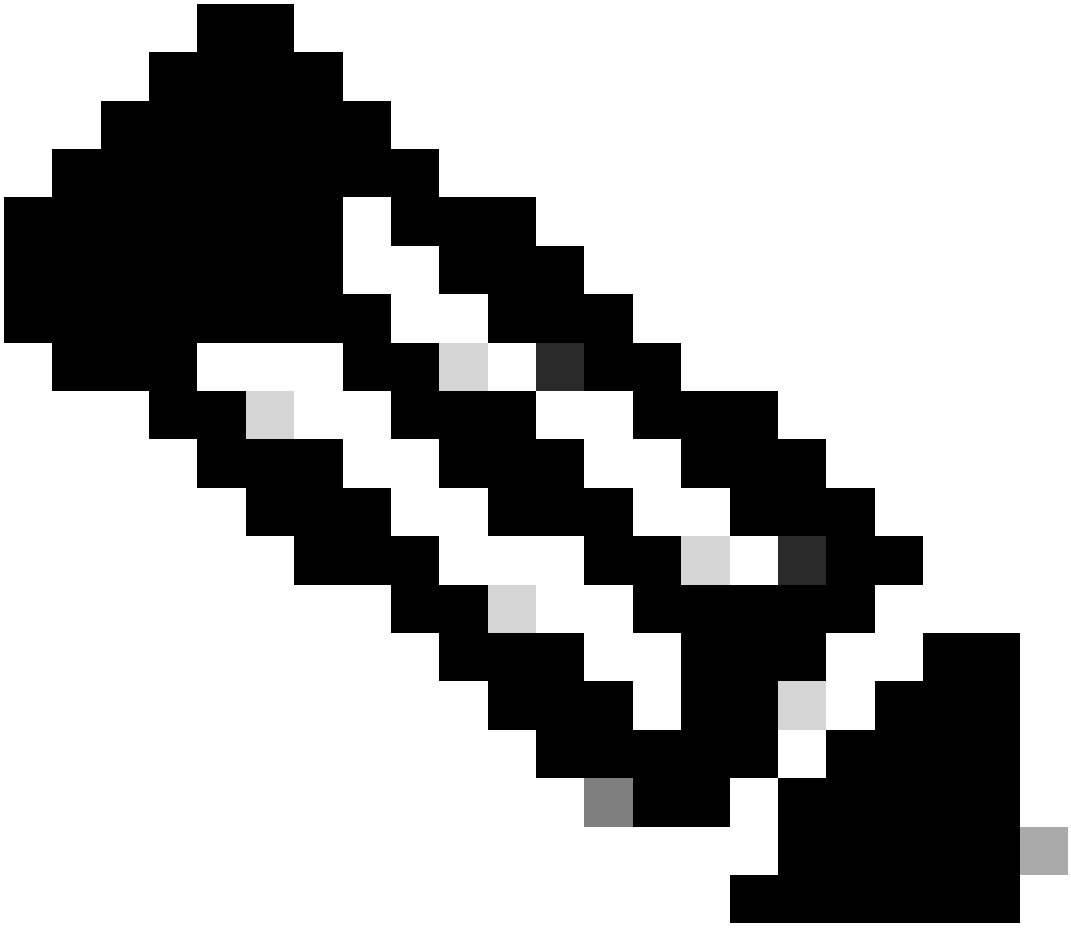
如果使用的是vBond FQDN，請確保配置的DNS伺服器或名稱伺服器具有解析vBond主機名的條目。您可以使用此命令檢查配置的DNS伺服器或名稱伺服器：

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

憑證

使用以下命令驗證路由器上是否已安裝證書：

```
show sdwan certificate installed
```



注意：如果您未使用企業證書，則路由器上已提供該證書。 對於硬體平台，裝置證書內建在路由器硬體中。對於虛擬路由器，vManage充當證書頒發機構並生成雲路由器的證書。

如果您在控制器上使用企業證書，請確保路由器上安裝了企業CA的根證書。

使用以下命令驗證路由器上是否已安裝根證書：

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

檢查show sdwan control local-properties的輸出，確保所需的配置和證書正確。

```
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   ::
```

檢查show sdwan control local-properties的輸出時，請確保滿足以下所有條件：

- 正確反映了organization-name。
- 證書有效性在您檢查輸出時有效。

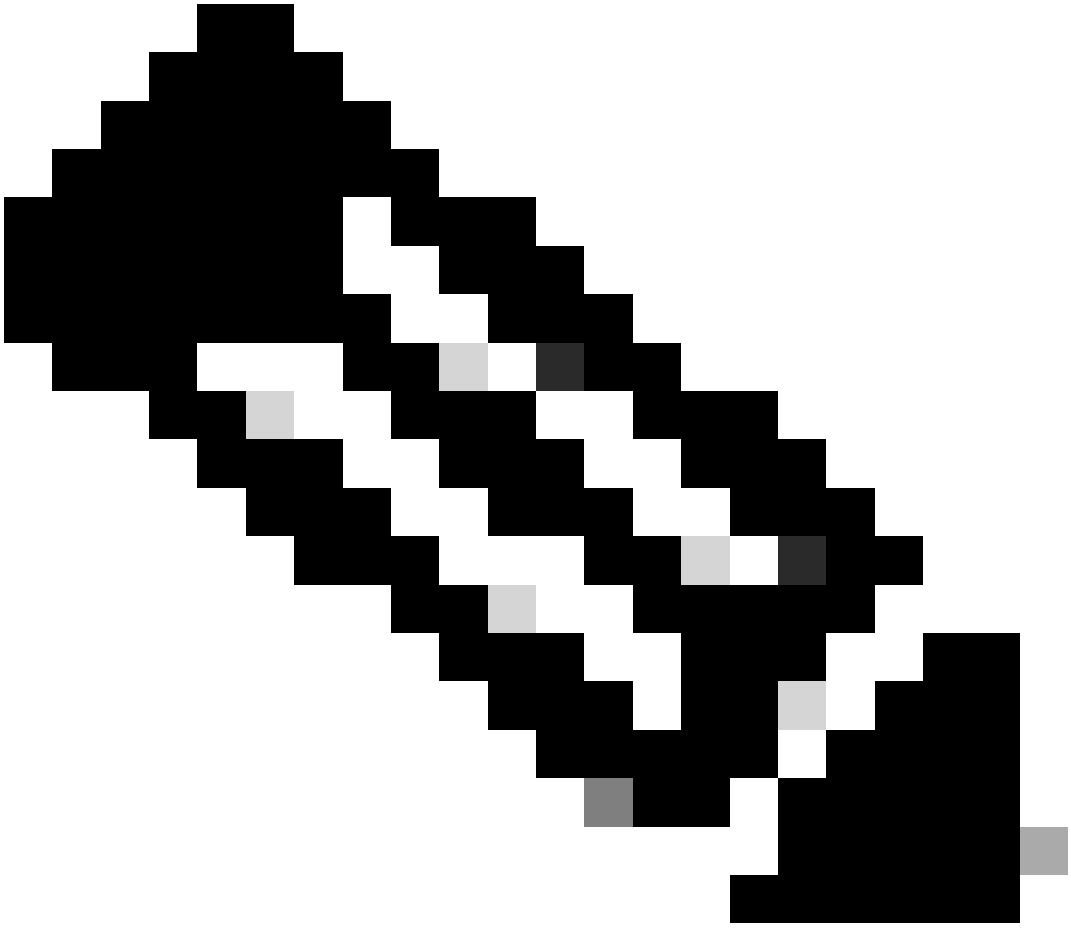
- vBond FQDN/IP地址正確。
- System-ip/Site-id正確。
- vBond IP地址在「number-vbond-peers」條目中顯示。如果未看到vBond IP地址，則使用ping <vBond FQDN>命令檢查DNS是否正在為vBond URL解析。
- 介面用正確的顏色、IP地址進行對映，介面狀態為UP。
- 形成控制連線所需的介面的MAX CNTRL不是0。

控制連線狀態

使用以下命令檢查控制連線的狀態：

```
show sdwan control connection
```

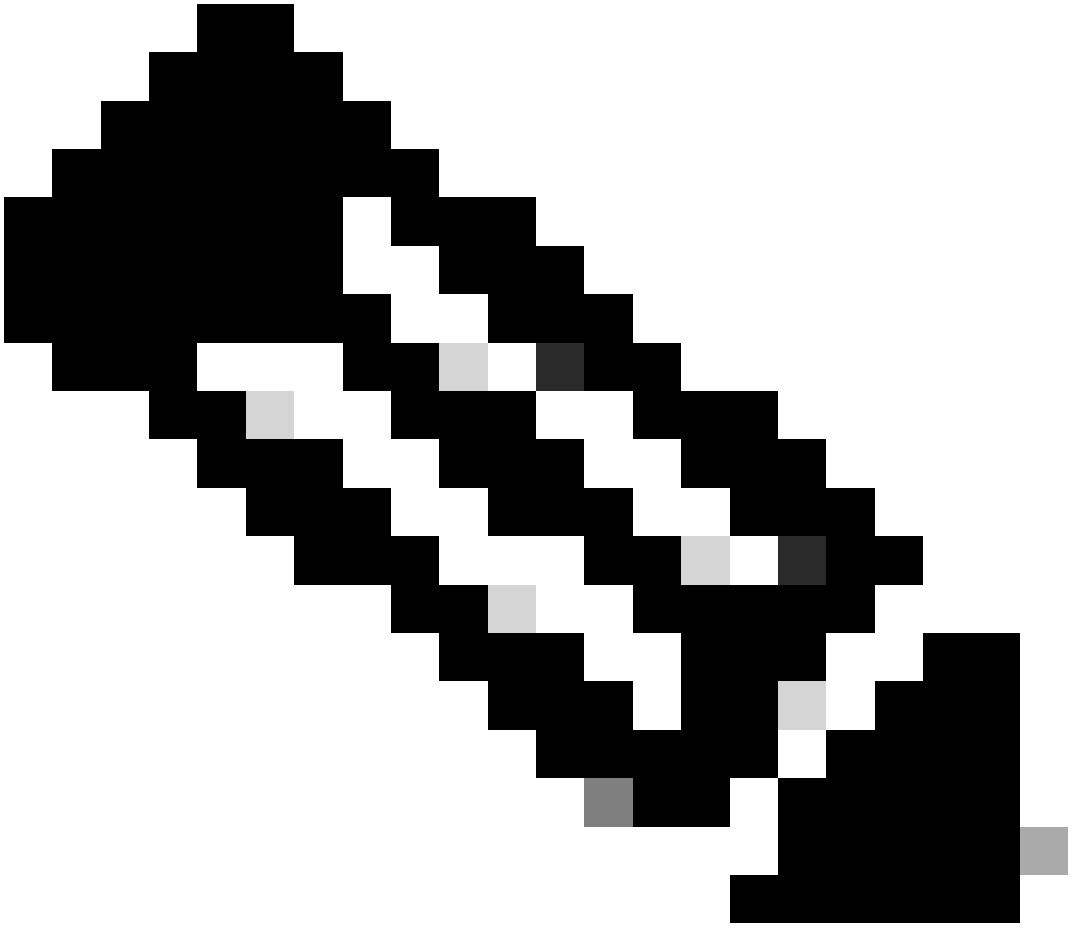
如果所有控制連線都打開，裝置將形成到vBond、vManage和vSmart的控制連線。建立所需的vSmart和vManage連線後，vBond控制連線將關閉。



註：如果覆蓋中只有一個vSmart，並且max-control connections設定為預設值2，則除vManage和vSmart的預期連線外，還將保持一個到vBond的持續控制連線。

此配置在sdwan介面的隧道介面配置部分中提供。您可以使用show sdwan run sdwan命令來檢驗它。如果在介面上將max-control-connection 配置為0，則路由器不會在該介面上形成控制連線。

如果覆蓋中有2個vSmarts，則路由器會在為控制連線配置的每個傳輸定位器(TLOC)顏色上形成與每個vSmart的控制連線。



註：在路由器有多個介面配置為形成控制連線的情況下，僅可在路由器的一個介面顏色上形成與vManage的控制連線。

```
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.
```

控制連線故障排除

在show sdwan control connections的輸出中，如果所需的所有控制連線均未啟動，請驗證show sdwan control connection-history的輸出。

```
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
vbond    dtls     0.0.0.0            0           0      10.106.50.235      12346    10.106.50.235   12346
```

在show sdwan control connection-history輸出中，請檢查以下項：

- 在指定的時間戳記中，控制連線失敗的控制器型別。
- 控制連線失敗時出現的錯誤。 有2個欄分別顯示錯誤、本地錯誤和遠端錯誤。本地錯誤指示路

由器生成的錯誤。Remote Error指示各個控制器生成的錯誤。 輸出的開頭有一個錯誤圖例。

- 重複計數，指示連線失敗次數，原因相同。

常見錯誤代碼故障

- DCONFAIL（DTLS連線故障）：此錯誤表示在路由器和各個控制器之間交換的DTLS資料包丟失，因此DTLS握手無法完成。為了更好地理解這一點，您可以在路由器和各自的控制器上同時設定資料包捕獲。嵌入式資料包捕獲部分介紹了設定資料包捕獲的不同方法。在分析資料包捕獲時，必須確保從一端傳送的資料包在另一端接收，並且不做任何修改。如果從一端傳送的資料包未在另一端接收，則表明襯底電路中存在資料包丟失，需要向服務提供商進行驗證。有關如何捕獲資料包的更多詳細資訊，請參閱底層問題部分。

- BIDNTVRFD（主機板ID未驗證）：此錯誤指示UUID和證書序列號不是控制器vEdge清單中的有效條目。使用以下命令，您可以檢查控制器上有效vedge清單的輸出：

<#root>

vBond:

show orchestrator valid-vedges

vManage/vSmart:

show control valid-vedges

通常，BIDNTVRFD是路由器上的遠端錯誤，因為它在控制器上生成。在各自的控制器上，您可以使用以下命令驗證位於/var/log/tmplog目錄中的vdebug檔案中的日誌：

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

- CRTVERFL（證書驗證失敗）：此錯誤指示無法驗證對等體傳送的證書。

- 如果這是路由器上的本地錯誤，則表示作為DTLS握手一部分傳送的控制器證書無法由路由器驗證。此問題的常見原因之一是，路由器沒有簽署控制器證書的證書頒發機構的根證書。使用以下命令驗證證書的狀態，以確保路由器上存在所需的根證書。

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

- 如果此錯誤是路由器上的遠端錯誤，請使用以下命令檢查相應控制器上的vdebug日誌檔案以

瞭解原因：

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

- VB_TMO（vBond超時）/ VM_TMO（vManage超時）/ VP_TMO（vPeer超時）/ VS_TMO（vSmart超時）：這些錯誤指示裝置之間丟失資料包，這將導致控制連線超時。 為了更好地理解這一點，您可以在路由器和各自的控制器上同時設定資料包捕獲。嵌入式資料包捕獲部分介紹了設定資料包捕獲的不同方法。當分析資料包捕獲時，必須確保一端傳送的資料包在另一端接收，並且不做任何修改。如果從一端傳送的資料包在另一端沒有收到，這表示襯底電路中存在資料包丟失，需要與服務提供商進行驗證

有關如何排除其他控制連線故障錯誤代碼的指導，請參閱以下文檔：

排除SD-WAN控制連線故障

底層問題

用於排除底層中資料包丟失故障的工具因裝置而異。 對於SD-WAN控制器和vEdge路由器，您可以使用tcpdump命令。 對於Catalyst IOS® XE邊緣，請使用嵌入式資料包捕獲(EPC)和功能呼叫陣列(FIA)跟蹤。

要瞭解控制連線失敗的原因並瞭解問題所在，您需要瞭解資料包丟失的發生位置。 例如，如果您的vBond和Edge路由器未形成控制連線，本指南將說明如何隔離問題。

TCP傾印

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

根據資料包的請求和響應，使用者可以瞭解負責丟棄的裝置。tcpdump命令可用於所有控制器和vEdge裝置。

內嵌式封包擷取

在裝置上建立ACL。

```
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>
```

配置並啟動監控捕獲。

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

停止擷取並匯出擷取檔案。

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

檢視wireshark中的檔案內容以瞭解丟棄情況。 有關其他詳細資訊，請參閱在軟體上配置和捕獲嵌入式資料包。

FIA追蹤

配置FIA跟蹤。

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

檢視fia phrase packet輸出。

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

如果存在丟棄，則分析丟棄的資料包的FIA跟蹤輸出。

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

若要瞭解其他FIA追蹤選項，請檢視以下檔案：使用IOS-XE資料路徑封包追蹤功能進行疑難排解

用FIA跟蹤確定Catalyst SD-WAN邊緣上的策略丟棄影片提供了使用FIA跟蹤的示例。

正在生成管理技術

請參閱在SD-WAN環境中收集管理技術並上傳到TAC案例- Cisco

相關資訊

技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。