一般的なSD-WANコントロールおよびデータプレーンの問題のトラブルシューティング

内容

はじめに

このドキュメントでは、ソフトウェア定義型ワイドエリアネットワーク(SD-WAN)の一般的なコントロールおよびデータプレーンの問題のトラブルシューティングを開始する方法について説明します。

前提条件

要件

Cisco Catalystソリューションに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

この記事は、実稼働環境で発生する問題をデバッグするためのランブックとして作成されています。 各セクションでは、これらの一般的な問題をデバッグする際に収集または検索する一般的な使用例と考えられるデータポイントについて説明します。

基本設定

基本設定がルータ上に存在し、デバイス固有の値がオーバーレイ内の各デバイスに固有であることを確認します。

システム設定

<#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
!
```

インターフェイス設定

```
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
```

コントローラ（vBond、vManage、およびvSmart）との制御接続を確立するために、ルータがルーティングテーブルで利用可能であることを確認します。次のコマンドを使用して、ルーティングテーブルにインストールされているすべてのルートを表示できます。

```
show ip route
```

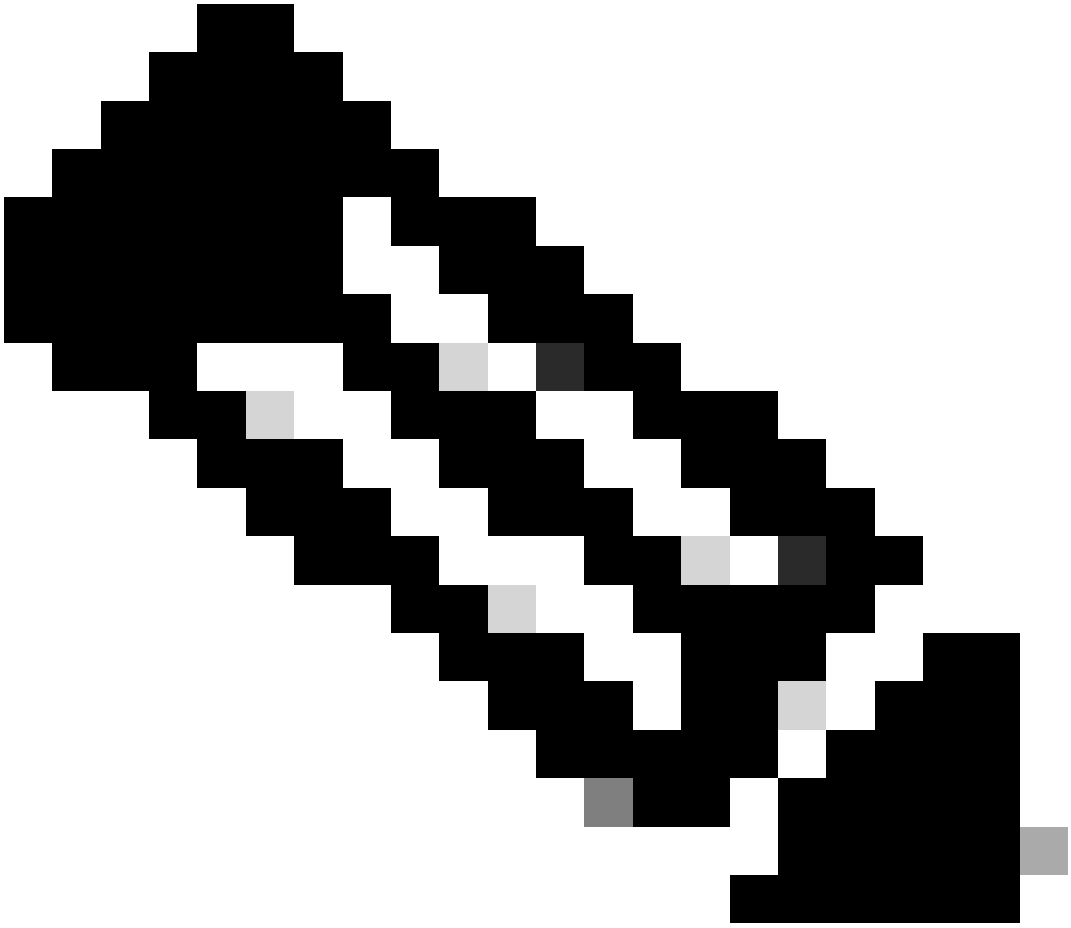
vBond FQDNを使用している場合は、設定されているDNSサーバまたはネームサーバにvBondホスト名を解決するためのエントリがあることを確認します。次のコマンドを使用して、どのDNSサーバまたはネームサーバが設定されているかを確認できます。

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

証明書

次のコマンドを使用して、証明書がルータにインストールされていることを確認します。

```
show sdwan certificate installed
```



注：エンタープライズ証明書を使用していない場合、証明書はすでにルータで使用できます。 ハードウェアプラットフォームの場合、デバイス証明書はルータハードウェアに組み込まれています。仮想ルータの場合、vManageは認証局として機能し、クラウドルータ用の証明書を生成します。

コントローラでエンタープライズ証明書を使用している場合は、エンタープライズCAのルート証明書がルータにインストールされていることを確認します。

次のコマンドを使用して、ルート証明書がルータにインストールされていることを確認します。

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

show sdwan control local-propertiesの出力を調べて、必要な設定と証明書が適切であることを確認します。

```
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   ::
```

show sdwan control local-propertiesの出力をチェックする際は、次の基準がすべて満たされていることを確認してください。

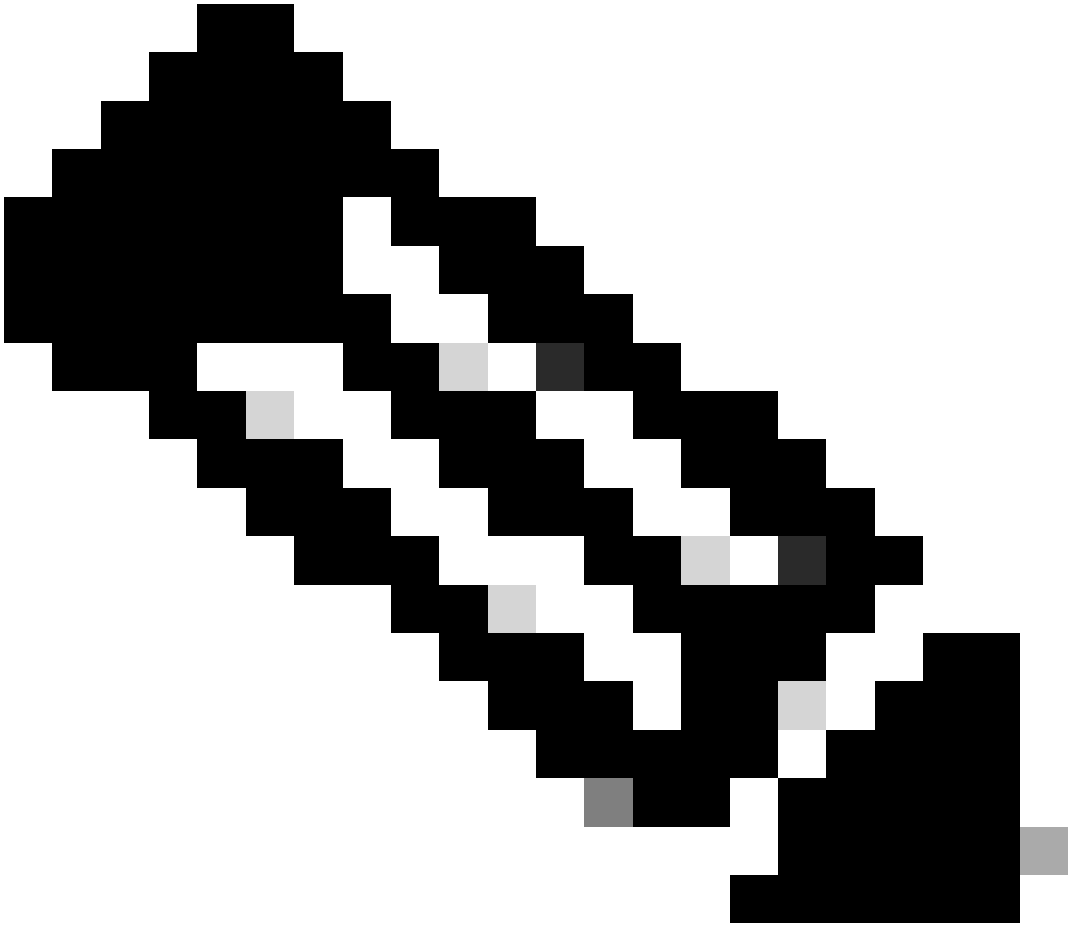
- 組織名は正しく反映されています。
- 証明書の有効性は、出力を確認する時点で有効です。
- vBond FQDN/IPアドレスが正しい。
- System-ip/Site-idが正しいことを確認します。
- vBond IPアドレスは、「number-vbond-peers」のエントリで確認できます。vBond IPアドレスが表示されない場合は、ping <vBond FQDN>コマンドを使用して、vBond URLのDNS解決が行われていることを確認します。
- インターフェイスは正しい色、IPアドレスでマッピングされ、インターフェイスのステータスはUPです。
- コントロール接続を形成するために必要なインターフェイスのMAX CNTRLが0ではありません。

コントロール接続の状態

次のコマンドを使用して、コントロール接続のステータスを確認します。

```
show sdwan control connection
```

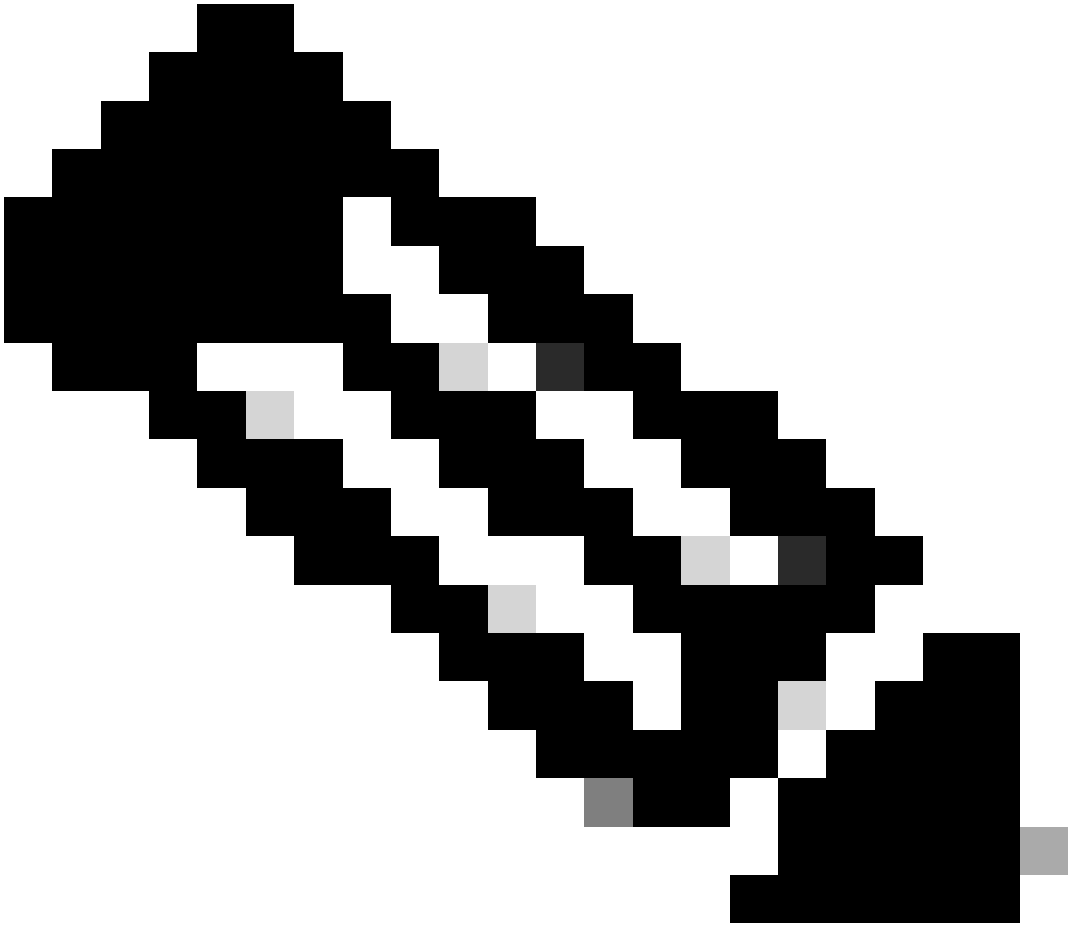
すべての制御接続がアップしている場合、デバイスにはvBond、vManage、およびvSmartへの制御接続が確立されています。必要なvSmartおよびvManage接続が確立されると、vBond制御接続が解除されます。



注：オーバーレイ内にvSmartが1つしかなく、max-control connectionsがデフォルト値の2に設定されている場合、vManageおよびvSmartへの予期される接続に加えて、vBondへの持続的な制御接続が維持されます。

この設定は、sdwanインターフェイスセクションのトンネルインターフェイス設定で使用できます。これは、show sdwan run sdwanコマンドを使用して確認できます。インターフェイスでmax-control-connectionが0に設定されている場合、ルータはそのインターフェイスで制御接続を形成しません。

オーバーレイに2つのvSmartsがある場合、ルータは制御接続用に設定されたすべてのTransport Locator(TLOC)カラーで各vSmartへの制御接続を形成します。



注:vManageへの制御接続は、ルータの1つのインターフェイスカラーでのみ形成されます。これは、ルータに制御接続を形成するように設定された複数のインターフェイスがある場合のシナリオです。

```
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.
```

コントロール接続のトラブルシューティング

show sdwan control connectionsの出力で、必要な制御接続がすべてアップしていない場合は、

show sdwan control connection-historyの出力を確認します。

```
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
```

show sdwan control connection-history の出力で、次の項目を確認します。

- 指定したタイムスタンプでコントロール接続が失敗するコントローラのタイプ。
- コントロール接続が失敗したときに表示されるエラーです。 エラー、ローカルエラー、およびリモートエラー用に2つの列があります。Local errorは、ルータによって生成されたエラーを示します。リモートエラーは、それぞれのコントローラで生成されたエラーを示します。 出力の先頭にエラーの凡例があります。

- 繰り返し回数。同じ理由で接続が失敗した回数を示します。

一般的なエラーコードのエラー

- DCONFAIL（DTLS接続障害）：このエラーは、ルータと各コントローラの間で交換されたDTLSパケットが失われ、DTLSハンドシェイクを完了できないことが原因であることを示します。この点をよりよく理解するために、ルータと各コントローラで同時パケットキャプチャを設定できます。パケットキャプチャのさまざまな設定方法は、「組み込みパケットキャプチャ」セクションで共有されています。パケットキャプチャを分析する際には、一方の端から送信されたパケットが修正されずに他方の端で受信されていることを確認することが重要です。一方の端から送信されたパケットがもう一方の端で受信されない場合は、アンダーレイ回路でパケット損失があり、サービスプロバイダーに確認する必要があります。パケットキャプチャの取得方法の詳細については、「アンダーレイの問題」セクションを参照してください。

- BIDNTVRFD(Board ID Not Verified):このエラーは、UUIDと証明書シリアル番号がコントローラvEdgeリストの有効なエントリではないことを示します。次のコマンドを使用して、コントローラ上の有効なvedgeリストの出力を確認できます。

<#root>

vBond:

show orchestrator valid-vedges

vManage/vSmart:

show control valid-vedges

通常、BIDNTVRFDはコントローラで生成されるため、ルータのリモートエラーです。それぞれのコントローラで、次のコマンドを使用して/var/log/tmplogディレクトリにあるvdebugファイルのログを確認できます。

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

- CRTVERFL(Certificate Verification Failed):このエラーは、ピアから送信された証明書を検証できなかったことを示します。

- これがルータ上のローカルエラーである場合は、DTLSハンドシェイクの一部として送信されたコントローラの証明書がルータで確認できなかったことを示します。この問題の一般的な原因の1つは、コントローラ証明書に署名した認証局(CA)のルート証明書がルータにないことです。次のコマンドを使用して証明書のステータスを確認し、必要なルート証明書がルータにあることを確認します。

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

- このエラーがルータのリモートエラーである場合は、次のコマンドを使用して、それぞれのコントローラのvdebugログファイルを確認し、原因を理解します。

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

- VB_TMO（vBondタイムアウト）/VM_TMO（vManageタイムアウト）/VP_TMO（vPeerタイムアウト）/VS_TMO（vSmartタイムアウト）：これらのエラーは、デバイス間でパケット損失が発生し、制御接続がタイムアウトしたことを示します。 この点をよりよく理解するために、ルータと各コントローラで同時パケットキャプチャを設定できます。パケットキャプチャのさまざまな設定方法は、「組み込みパケットキャプチャ」セクションで共有されています。パケットキャプチャを分析する際には、一方の端から送信されたパケットが、変更を加えることなく他方の端で受信されていることを確認することが重要です。一方の端から送信されたパケットがもう一方の端で受信されない場合は、アンダーレイ回路でパケット損失があり、サービスプロバイダーに確認する必要があります

その他のコントロール接続障害エラーコードのトラブルシューティング方法については、次のドキュメントを参照してください。

SD-WANコントロール接続のトラブルシューティング

アンダーレイの問題

アンダーレイのパケット損失のトラブルシューティングに使用するツールは、デバイスによって異なります。 SD-WANコントローラおよびvEdgeルータの場合は、tcpdumpコマンドを使用できます。 Catalyst IOS® XEエッジの場合は、Embedded Packet Capture(EPC)およびFeature Invocation Array(FIA)トレースを使用します。

コントロール接続が失敗する理由を理解し、問題がどこにあるかを理解するには、パケット損失がどこで発生しているかを理解する必要があります。　たとえば、vBondルータとエッジルータが制御接続を形成していない場合、このガイドでは問題を切り分ける方法を示します。

TCPダンプ

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

パケットの要求と応答に基づいて、ドロップの原因となっているデバイスをユーザが理解できます。tcpdumpコマンドは、すべてのコントローラとvEdgeデバイスで使用できます。

Embedded Packet Capture

デバイスにACLを作成します。

```
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>
```

モニタキャプチャを設定して開始します。

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

キャプチャを停止し、キャプチャファイルをエクスポートします。

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

Wiresharkでファイルの内容を表示して、ドロップについて理解します。 詳細は、『ソフトウェアでの組み込みパケットの設定とキャプチャ』を参照してください。

FIAトレース

FIAトレースを設定します。

```
debug platform condition ipv4 <ip> both
```

```
debug platform packet-trace packet 2048 fia-trace data-size 4096
debug platform condition start
```

fia phraseのパケット出力を表示します。

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

ドロップがある場合、ドロップされたパケットのFIAトレース出力を解析します。

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

その他のFIAトレースオプションについては、「IOS-XEデータパストパケットトレース機能によるトラブルシューティング」を参照してください。

「FIAトレースによるCatalyst SD-WANエッジでのポリシードロップの決定」ビデオは、FIAトレースを使用した例を示しています。

Admin-Techの生成

詳細については、「SD-WAN環境でのAdmin-Techの収集とTACケースへのアップロード：シスコ

関連情報

テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。