Fehlerbehebung bei allgemeinen Problemen mit der SD-WAN-Steuerung und Datenebene

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie mit der Fehlerbehebung für allgemeine Probleme mit der Steuerung und Datenebene eines Software-defined Wide Area Network (SD-WAN) beginnen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der Cisco Catalyst-Lösung verfügen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Dieser Artikel wurde als Runbook entwickelt, um einen Ausgangspunkt für das Debuggen von Herausforderungen in Produktionsumgebungen zu bieten. Jeder Abschnitt enthält allgemeine Anwendungsfälle und mögliche Datenpunkte, die beim Debuggen dieser häufig auftretenden Probleme erfasst oder gesucht werden müssen.

Basiskonfigurationen

Vergewissern Sie sich, dass die Basiskonfigurationen auf dem Router vorhanden sind und dass die gerätespezifischen Werte für jedes Gerät im Overlay eindeutig sind:

Systemkonfigurationen

<#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
!
```

Schnittstellenkonfigurationen

```
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
```

Stellen Sie sicher, dass der Router über Routing in der Routing-Tabelle verfügt, um eine Steuerungsverbindung mit den Controllern (vBond, vManage und vSmart) herzustellen. Mit diesem Befehl können Sie alle in der Routing-Tabelle installierten Routen anzeigen:

```
show ip route
```

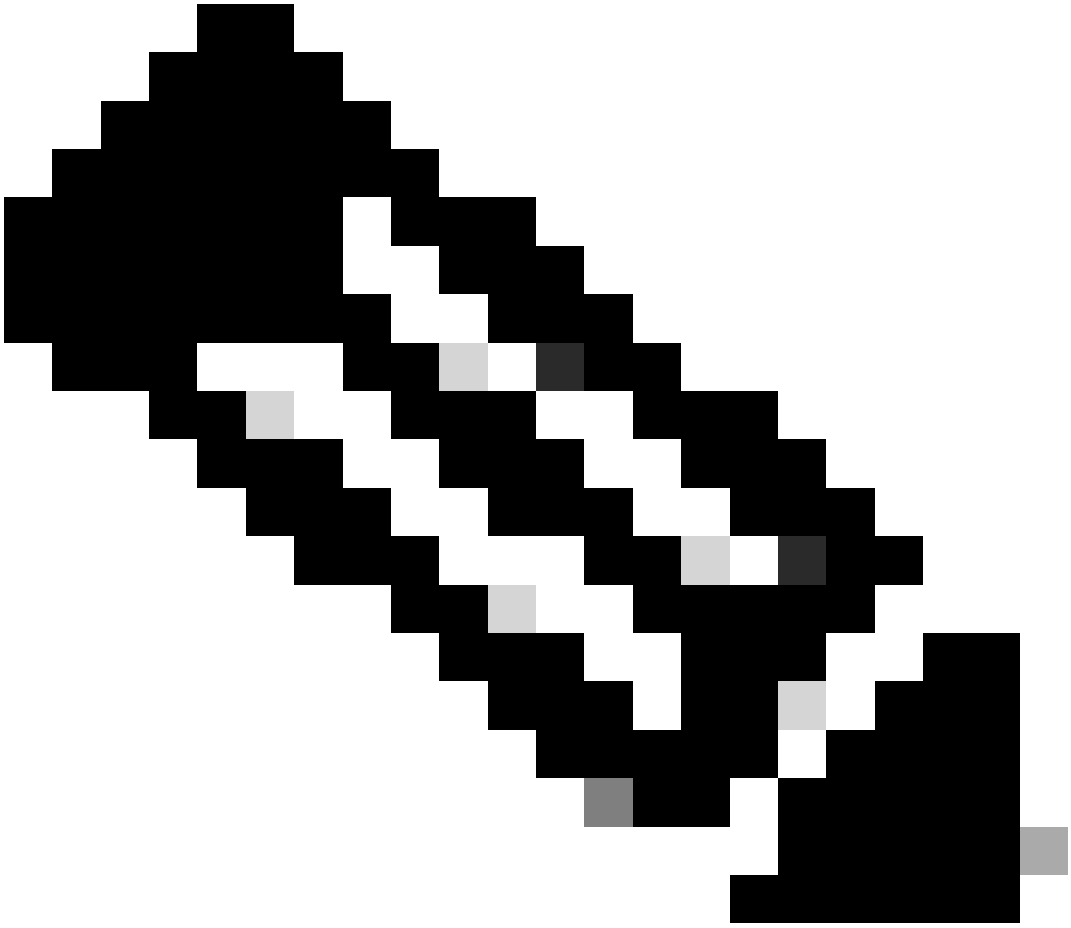
Wenn Sie vBond FQDN verwenden, stellen Sie sicher, dass der konfigurierte DNS-Server oder Namensserver über einen Eintrag zum Auflösen des vBond-Hostnamens verfügt. Mit dem folgenden Befehl können Sie überprüfen, welcher DNS-Server oder Name-Server konfiguriert ist:

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

Zertifikat

Stellen Sie sicher, dass das Zertifikat mit dem folgenden Befehl auf dem Router installiert ist:

```
show sdwan certificate installed
```



Hinweis: Wenn Sie keine Enterprise-Zertifikate verwenden, ist das Zertifikat auf den Routern bereits verfügbar. Bei Hardwareplattformen sind die Gerätezertifikate in die Router-Hardware integriert. Bei virtuellen Routern fungiert vManage als Zertifizierungsstelle und generiert die Zertifikate für Cloud-Router.

Wenn Sie Enterprise-Zertifikate auf den Controllern verwenden, stellen Sie sicher, dass das Stammzertifikat der Enterprise-CA auf dem Router installiert ist.

Stellen Sie sicher, dass die Stammzertifikate auf dem Router installiert sind. Verwenden Sie hierzu die folgenden Befehle:

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

Überprüfen Sie die Ausgabe von show sdwan control local-properties, um sicherzustellen, dass

die erforderlichen Konfigurationen und Zertifikate vorhanden sind.

```
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   ::
```

Wenn Sie die Ausgabe von show sdwan control local-properties überprüfen, stellen Sie sicher, dass alle folgenden Kriterien erfüllt sind:

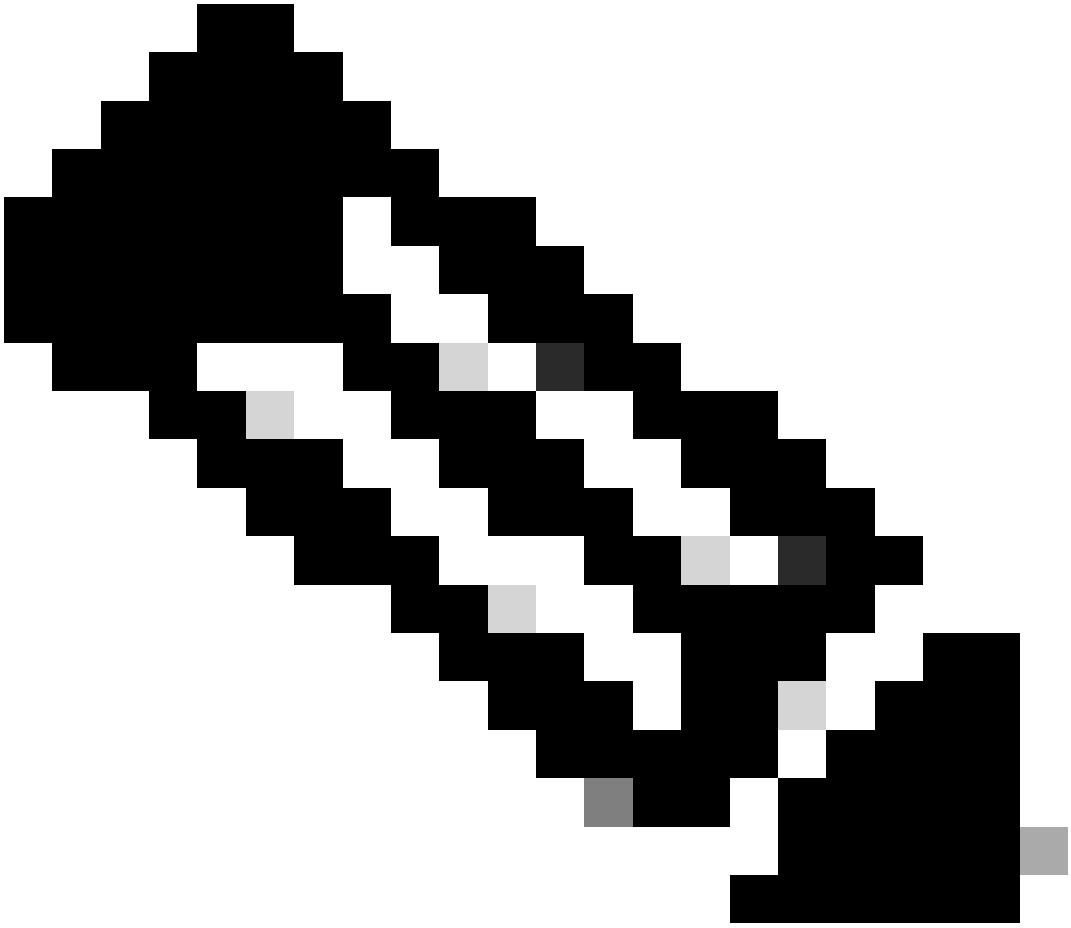
- Der Organisationsname wird korrekt wiedergegeben.
- Die Gültigkeit des Zertifikats ist zum Zeitpunkt der Überprüfung der Ausgabe gültig.
- Die vBond-FQDN/IP-Adresse ist richtig.
- System-IP/Standort-ID ist korrekt.
- Die vBond-IP-Adresse wird im Eintrag für "number-vbond-peers" angezeigt. Wenn die vBond-IP-Adresse nicht angezeigt wird, überprüfen Sie, ob DNS die Auflösung für die vBond-URL mit dem Befehl ping <vBond FQDN> durchführt.
- Die Schnittstellen werden mit der richtigen Farbe und IP-Adresse zugeordnet, und der Status der Schnittstelle lautet UP.
- Die MAX STRG für die erforderliche Schnittstelle zum Herstellen der Steuerverbindung ist nicht 0.

Status der Steuerverbindungen

Überprüfen Sie den Status der Steuerungsverbindung mithilfe des folgenden Befehls:

```
show sdwan control connection
```

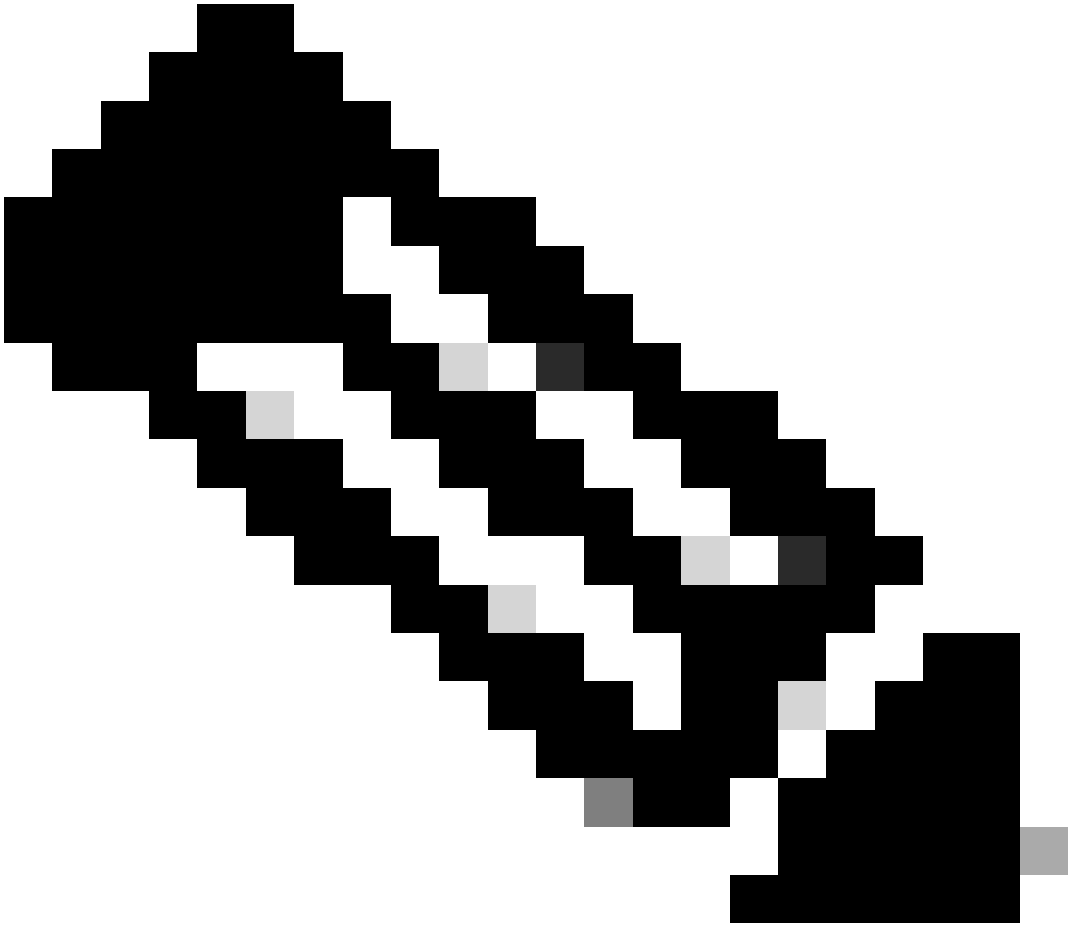
Wenn alle Steuerungsverbindungen aktiv sind, verfügt das Gerät über eine Steuerungsverbindung mit vBond, vManage und vSmart. Sobald die erforderlichen vSmart- und vManage-Verbindungen hergestellt sind, wird die vBond-Steuerverbindung getrennt.



Hinweis: Wenn nur ein vSmart im Overlay vorhanden ist und für die maximale Anzahl an Steuerverbindungen der Standardwert 2 festgelegt ist, wird eine permanente Steuerverbindung zu vBond aufrechterhalten, zusätzlich zur erwarteten Verbindung zu vManage und vSmart.

Diese Konfiguration steht im Abschnitt zur Tunnelschnittstellenkonfiguration des SDWAN-Schnittstellenabschnitts zur Verfügung. Sie können dies mit dem Befehl show sdwan run sdwan überprüfen. Wenn max-control-connection für die Schnittstelle auf 0 konfiguriert ist, stellt der Router an dieser Schnittstelle keine Steuerverbindung her.

Wenn das Overlay zwei vSmarts enthält, stellt der Router für jedes vSmart eine Steuerverbindung in jeder für Steuerverbindungen konfigurierten Farbe des Transport Locator (TLOC) her.



Hinweis: Die Steuerverbindung zu vManage wird nur in einer Schnittstellenfarbe des Routers hergestellt, wenn der Router mehrere Schnittstellen aufweist, die so konfiguriert sind, dass sie Steuerverbindungen bilden.

```
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.
```

Fehlerbehebung bei Steuerverbindungen

Wenn in der Ausgabe von show sdwan control connections nicht alle erforderlichen

Steuerverbindungen aktiv sind, überprüfen Sie die Ausgabe von 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
vbond    dtls     0.0.0.0             0           0      10.106.50.235    12346    10.106.50.235     12346
```

Aktivieren Sie in der Ausgabe show sdwan control connection-history die folgenden Optionen:

- Der Controller-Typ, mit dem die Steuerverbindung bei einem bestimmten Zeitstempel fehlschlägt.
- Der Fehler, der beim Ausfall der Steuerelementverbindung aufgetreten ist. Es gibt zwei Spalten für Fehler, Lokale Fehler und Remote-Fehler. Der lokale Fehler zeigt den vom Router generierten Fehler an. Remote Error (Remote-Fehler) gibt den vom jeweiligen Controller generierten Fehler an. Am Anfang der Ausgabe befindet sich eine Fehlerlegende.

- Anzahl der Wiederholungen: Gibt die Anzahl der fehlgeschlagenen Verbindungen mit demselben Grund an.

Häufige Fehlercodefehler

- DCONFAIL (DTLS Connection Failure): Dieser Fehler weist auf einen Verlust von DTLS-Paketen hin, die zwischen Router und jeweiligem Controller ausgetauscht werden, wodurch der DTLS-Handshake nicht abgeschlossen werden kann. Um dies besser zu verstehen, können Sie die gleichzeitige Paketerfassung auf dem Router und dem jeweiligen Controller einrichten. Im Abschnitt "Embedded Packet Capture" (Integrierte Paketerfassung) werden verschiedene Methoden zum Einrichten von Paketerfassungen gemeinsam genutzt. Bei der Analyse der Paketerfassung muss sichergestellt werden, dass die von einem Ende gesendeten Pakete am anderen Ende ohne Änderungen empfangen werden. Wenn das von einem Ende gesendete Paket nicht am anderen Ende empfangen wird, weist dies auf einen Paketverlust in der Underlay-Schaltung hin, der mit dem Service Provider überprüft werden muss. Weitere Informationen zur Durchführung einer Paketerfassung finden Sie im Abschnitt Underlay Issues (Underlay-Probleme).

- BIDNTVRFD (Motherboard-ID nicht verifiziert): Dieser Fehler weist darauf hin, dass die UUID und die Seriennummer des Zertifikats kein gültiger Eintrag in der vEdge-Liste des Controllers sind. Sie können die Ausgabe der gültigen vedge-Liste auf den Controllern mit den folgenden Befehlen überprüfen:

<#root>

vBond:

show orchestrator valid-vedges

vManage/vSmart:

show control valid-vedges

In der Regel ist BIDNTVRFD ein Remote-Fehler auf dem Router, da er auf dem Controller generiert wird. Auf dem entsprechenden Controller können Sie das Protokoll in der vdebug-Datei im Verzeichnis /var/log/tmplog mithilfe der folgenden Befehle überprüfen:

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

- CRTVERFL (Certificate Verification Failed): Dieser Fehler weist darauf hin, dass das vom Peer gesendete Zertifikat nicht verifiziert werden konnte.
- Wenn es sich um einen lokalen Fehler auf dem Router handelt, weist dies darauf hin, dass das Zertifikat des Controllers, das als Teil des DTLS-Handshakes gesendet wurde, vom Router nicht verifiziert werden konnte. Einer der häufigsten Gründe dafür ist, dass der Router nicht über das Stammzertifikat der Zertifizierungsstelle verfügt, die das Controller-Zertifikat signiert hat. Überprüfen Sie mit diesen Befehlen den Status des Zertifikats, um sicherzustellen, dass das erforderliche Root-Zertifikat auf dem Router vorhanden ist.

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

- Wenn es sich bei diesem Fehler um einen Fernfehler auf dem Router handelt, überprüfen Sie die vdebug-Protokolldatei auf dem entsprechenden Controller, um die Ursache mithilfe der folgenden Befehle zu ermitteln:

```
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): Diese Fehler weisen auf einen Paketverlust zwischen den Geräten hin, der zu einem Timeout der Steuerverbindung führt. Um dies besser zu verstehen, können Sie die gleichzeitige Paketerfassung auf dem Router und dem jeweiligen Controller einrichten. Im Abschnitt "Embedded Packet Capture" (Integrierte Paketerfassung) werden verschiedene Methoden zum Einrichten von Paketerfassungen gemeinsam genutzt. Bei der Analyse der Paketerfassungen muss sichergestellt werden, dass die von einem Ende gesendeten Pakete am anderen Ende ohne Änderungen empfangen werden. Wenn das von einem Ende gesendete Paket am anderen Ende nicht empfangen wird, weist dies auf einen Paketverlust in der Underlay-Schaltung hin, der mit dem Service Provider überprüft werden muss

Hinweise zur Fehlerbehebung bei anderen Verbindungsfehlercodes finden Sie in diesem Dokument:

Fehlerbehebung bei SD-WAN-Steuerverbindungen

Underlay-Probleme

Die Tools, die zur Fehlerbehebung bei Paketverlusten im Underlay verwendet werden, sind von Gerät zu Gerät unterschiedlich. Für SD-WAN-Controller und vEdges-Router können Sie den Befehl tcpdump verwenden. Verwenden Sie für Catalyst IOS® XE-Edges Embedded Packet Capture (EPC) und Feature Invocation Array (FIA) trace.

Um zu verstehen, warum die Steuerungsverbindungen fehlschlagen, und um zu verstehen, wo das Problem liegt, müssen Sie verstehen, wo der Paketverlust stattfindet. Wenn Sie beispielsweise einen vBond- und Edge-Router haben, der keine Steuerverbindung herstellt, wird in diesem Handbuch erläutert, wie Sie das Problem isolieren können.

TCP-Dump

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

Je nach Anforderung und Antwort der Pakete kann der Benutzer das Gerät verstehen, das für die Löschvorgänge verantwortlich ist. Der Befehl tcpdump kann auf allen Controllern und vEdge-Geräten verwendet werden.

Integrierte Paketerfassung

Erstellen Sie eine ACL auf dem Gerät.

```
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>
```

Konfigurieren Sie die Monitorerfassung, und starten Sie sie.

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

Beenden Sie die Erfassung, und exportieren Sie die Erfassungsdatei.

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

Zeigen Sie den Inhalt der Datei in Wireshark an, um die Drops zu verstehen. Weitere Informationen finden Sie unter Konfigurieren und Erfassen von eingebetteten Paketen auf Software .

FIA-Ablaufverfolgung

Konfigurieren der FIA-Ablaufverfolgung

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

Anzeigen der Ausgabe der endgültigen Phrase.

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

Wenn ein Verwerfen auftritt, analysieren Sie die FIA-Ablaufverfolgungsausgabe für das verworfene Paket.

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

Weitere FIA-Ablaufverfolgungsoptionen finden Sie in diesem Dokument: Fehlerbehebung mit der IOS-XE DataPath Packet Trace-Funktion

Das Video Determine Policy Drops on Catalyst SD-WAN Edge with FIA Trace bietet ein Beispiel für die Verwendung von FIA Trace.

Erstellen von Admin-Tech

Weitere Informationen finden Sie unter Collect an Admin-Tech in SD-WAN Environment und Upload to TAC Case - Cisco

Zugehörige Informationen

Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.