解决常见的SD-WAN控制和数据平面问题

目录

简介

本文档介绍如何开始排除常见的软件定义广域网(SD-WAN)控制和数据平面问题。

先决条件

要求

Cisco建议您应具备Cisco Catalyst解决方案知识。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

本文设计为操作手册，为调试跨生产环境的挑战提供一个起点。 每个部分提供常见使用案例和可能的数据点，以便在调试这些常见问题时收集或查找。

基本配置

确保路由器上存在基本配置，并且重叠中每台设备的设备特定值是唯一的：

系统配置

<#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
!
```

接口配置

```
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
```

确保路由器的aroute在路由表中可用，以建立与控制器（vBond、vManage和vSmart）的控制连接。您可以使用此命令查看安装在路由表中的所有路由：

```
show ip route
```

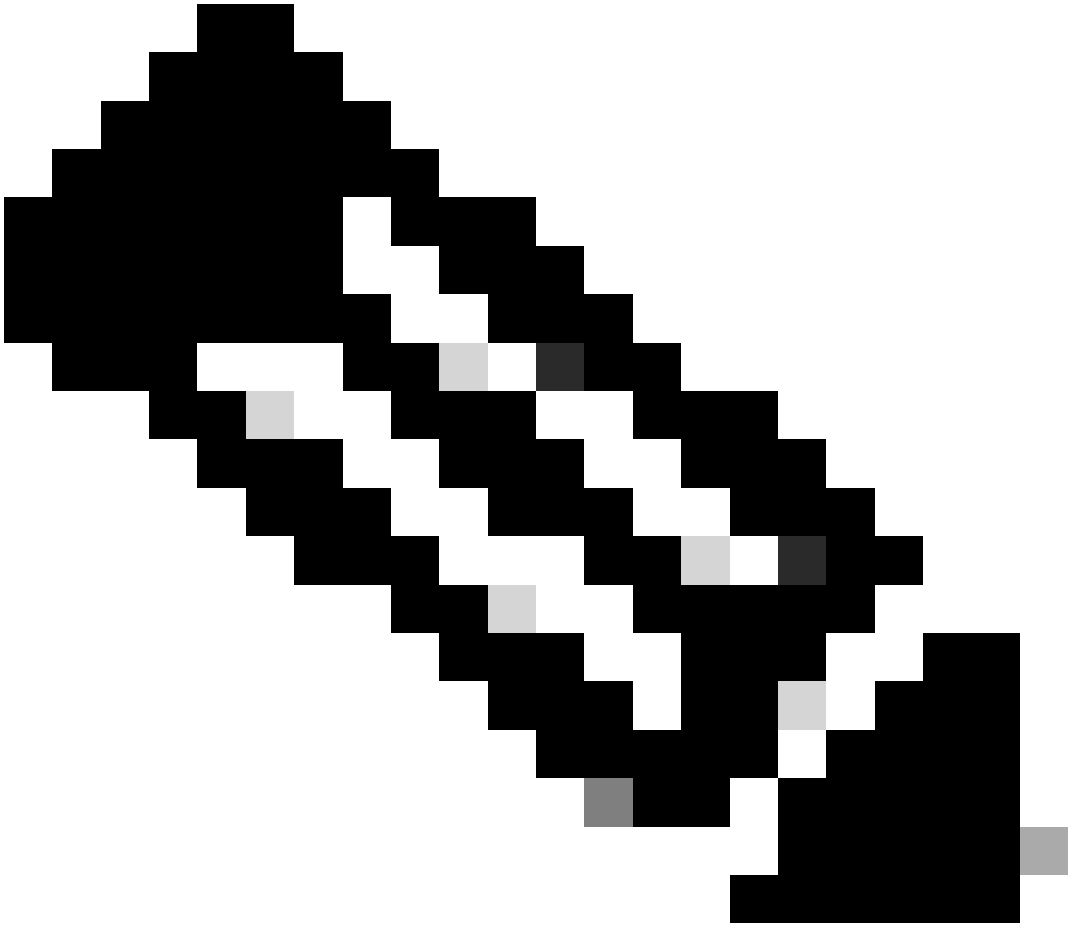
如果使用的是vBond FQDN，请确保配置的DNS服务器或名称服务器具有解析vBond主机名的条目。您可以使用以下命令检查配置了哪个DNS服务器或名称服务器：

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

证书

使用以下命令验证路由器上是否安装了证书：

```
show sdwan certificate installed
```



注意：如果不使用企业证书，则路由器上已提供该证书。 对于硬件平台，设备证书内置在路由器硬件中。对于虚拟路由器，vManage充当证书颁发机构并生成云路由器的证书。

如果您在控制器上使用企业证书，请确保在路由器上安装企业CA的根证书。

使用以下命令验证路由器上是否安装了根证书：

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

检查show sdwan control local-properties的输出，以确保所需的配置和证书已就位。

```
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   ::
```

检查show sdwan control local-properties的输出时，请确保满足以下所有条件：

- 正确反映了organization-name。
- 当您检查输出时，证书有效性有效。

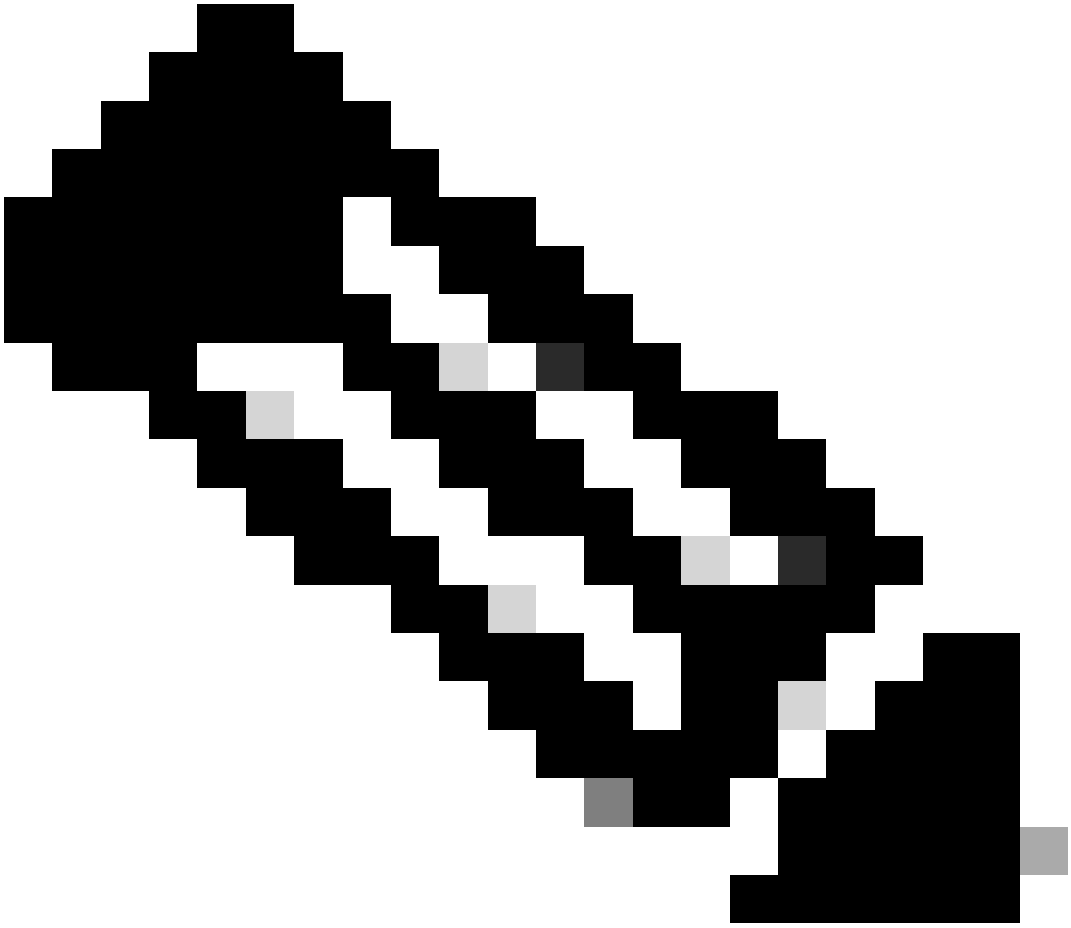
- vBond FQDN/IP地址正确。
- System-ip/Site-id正确。
- vBond IP地址可在“number-vbond-peers”条目中看到。如果未看到vBond IP地址，则使用ping <vBond FQDN>命令检查vBond URL的DNS是否已解析。
- 接口使用正确的颜色、IP地址进行映射，并且接口状态为UP。
- 形成控制连接所需的接口的MAX CNTRL不是0。

控制连接的状态

使用以下命令检查控制连接的状态：

```
show sdwan control connection
```

如果所有控制连接均开启，设备将形成与vBond、vManage和vSmart的控制连接。建立所需的vSmart和vManage连接后，vBond控制连接将断开。



注意：如果重叠中只有一个vSmart，并且max-control connections设置为默认值2，则除vManage和vSmart的预期连接外，将保持到vBond的持续控制连接。

此配置在sdwan接口的隧道接口配置部分提供。使用命令show sdwan run sdwan可以验证这一点。如果在接口上将max-control-connection配置为0，则路由器将不会在该接口上形成控制连接。

如果重叠中存在2个vSmarts，则路由器会在为控制连接配置的每个传输定位器(TLOC)颜色上形成与每个vSmart的控制连接。

注意：如果路由器配置了多个接口以形成控制连接，则仅在路由器的一种接口颜色上形成到vManage的控制连接。

```
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.
```

排除控制连接故障

在show sdwan control connections的输出中，如果所需的所有控制连接均未启动，请验证show sdwan control connection-history的输出。

```
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 输出中，选中以下项目：

- 在给定时间戳上控制连接失败的控制器类型。
- 当控制连接失败时看到的错误。 错误列、本地错误列和远程错误列。本地错误表示路由器生

成的错误。Remote Error指示各个控制器生成的错误。 输出开头有一个错误图例。

- 重复计数，指示连接失败次数，原因相同。

常见错误代码故障

- DCONFAIL（DTLS连接故障）：此错误指示在路由器和相应控制器之间交换的DTLS数据包丢失，因此无法完成DTLS握手。为了更好地理解这一点，您可以在路由器和相应控制器上设置同步数据包捕获。嵌入式数据包捕获部分介绍了设置数据包捕获的不同方法。在分析数据包捕获时，确保从一端发送的数据包在另一端接收而不作任何修改非常重要。如果从一端发送的数据包在另一端没有收到，则表明衬底电路中存在数据包丢失，需要与服务提供商进行验证。有关如何捕获数据包的更多详细信息，请参阅底层问题部分。

- BIDNTVRFD(Board ID Not Verified)：此错误指示UUID和证书序列号不是控制器vEdge列表中的有效条目。可以使用以下命令检查控制器上有效边界列表的输出：

<#root>

vBond:

show orchestrator valid-vedges

vManage/vSmart:

show control valid-vedges

通常，BIDNTVRFD是路由器上的远程错误，因为BIDNTVRFD是在控制器上生成的。在各自的控制器上，可以使用以下命令验证/var/log/tmplog目录中的vdebug文件中的日志：

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

- CRTVERFL（证书验证失败）：此错误指示无法验证对等体发送的证书。

- 如果这是路由器上的本地错误，则它指示作为DTLS握手的一部分发送的控制器的证书无法由路由器验证。出现这种情况的常见原因之一是，路由器没有签署了控制器证书的证书颁发机构的根证书。使用这些命令验证证书的状态，以确保路由器上存在所需的根证书。

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

- 如果此错误是路由器上的远程错误，请使用以下命令检查相应控制器上的vdebug日志文件以

了解原因：

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

- VB_TMO（vBond超时）/VM_TMO（vManage超时）/VP_TMO（vPeer超时）/VS_TMO（vSmart超时）：这些错误表明设备之间存在数据包丢失，从而导致控制连接超时。 为了更好地理解这一点，您可以在路由器和相应控制器上设置同步数据包捕获。嵌入式数据包捕获部分介绍了设置数据包捕获的不同方法。在分析数据包捕获时，必须确保从一端发送的数据包在另一端接收，并且未进行任何修改。如果从一端发送的数据包在另一端没有收到，这表示衬底电路中存在数据包丢失，需要与服务提供商进行验证

有关如何对其他控制连接故障错误代码进行故障排除的指导，请参阅以下文档：

排除SD-WAN控制连接故障

底层问题

用于排除底层数据包丢失故障的工具因设备而异。 对于SD-WAN控制器和vEdge路由器，可以使用tcpdump命令。 对于Catalyst IOS® XE边缘，请使用嵌入式数据包捕获(EPC)和功能调用阵列(FIA)跟踪。

要了解控制连接失败的原因并了解问题所在，您需要了解数据包丢失发生在哪里。 例如，如果您有vBond和Edge路由器未形成控制连接，本指南将说明如何隔离问题。

TCP转储

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

根据数据包的请求和响应，用户可以了解负责丢弃的设备。tcpdump命令可用于所有控制器和vEdge设备。

嵌入式数据包捕获

在设备上创建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>
```

配置并开始监控捕获。

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

停止捕获并导出捕获文件。

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

查看Wireshark中文件的内容，以了解丢弃情况。 有关其他详细信息，请参阅在软件上配置和捕获嵌入式数据包。

FIA跟踪

配置FIA跟踪。

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

查看fia phrase数据包输出。

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

如果存在丢包，请解析已丢弃数据包的FIA跟踪输出。

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

要了解其他FIA跟踪选项，请查看以下文档：使用IOS-XE数据路径数据包跟踪功能进行故障排除

用FIA跟踪确定Catalyst SD-WAN边缘上的策略丢弃视频提供了使用FIA跟踪的示例。

正在生成管理技术

请参阅在SD-WAN环境中收集管理技术并上传到TAC支持请求- Cisco

相关信息

技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。