Solucionar problemas comuns de controle de SD-WAN e plano de dados

Contents

Introdução

Este documento descreve como iniciar a solução de problemas comuns de controle de Rede de Longa Distância Definida por Software (SD-WAN) e problemas de plano de dados.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento da solução Cisco Catalyst.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Overview

Este artigo foi desenvolvido como um runbook para fornecer um ponto de partida para os desafios de depuração vistos em ambientes de produção. Cada seção fornece casos de uso comuns e pontos de dados prováveis para coletar ou procurar quando você estiver depurando esses problemas comuns.

Configurações básicas

Verifique se as configurações básicas estão presentes no roteador e se os valores específicos do dispositivo são exclusivos para cada dispositivo na sobreposição:

Configurações do 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
!
```

Configurações de interface

```
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
```

Certifique-se de que o roteador tenha uma rota disponível na tabela de roteamento para estabelecer uma conexão de controle com os controladores (vBond, vManage e vSmart). Você pode usar este comando para ver todas as rotas instaladas na tabela de roteamento:

```
show ip route
```

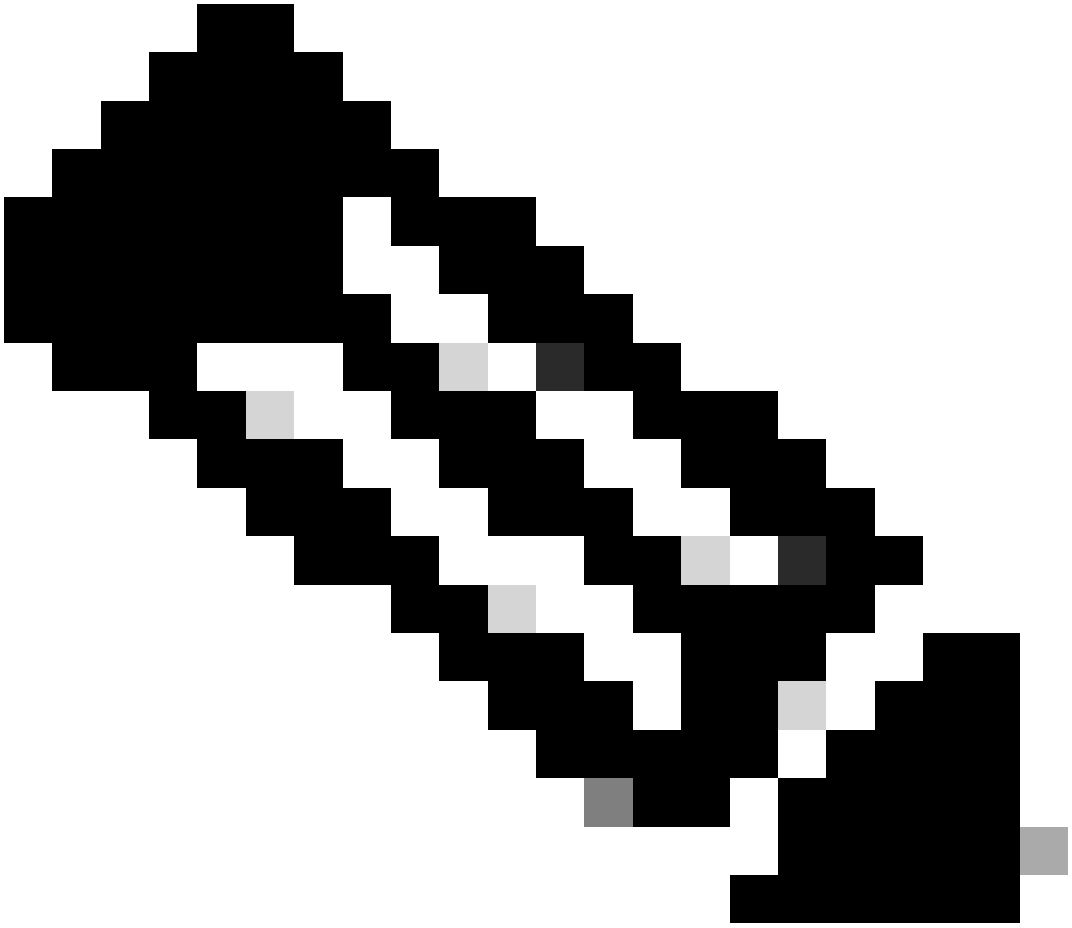
Se você estiver usando o FQDN vBond, certifique-se de que o servidor DNS ou o servidor de nomes configurado tenha uma entrada para resolver o nome de host vBond. Você pode verificar qual servidor DNS ou servidor de nomes está configurado com este comando:

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

Certificado

Verifique se o certificado está instalado no roteador usando este comando:

```
show sdwan certificate installed
```



Nota:Se você não estiver usando certificados Enterprise, o certificado já estará disponível nos roteadores. Para plataformas de hardware, os certificados do dispositivo são incorporados ao hardware do roteador. Para roteadores virtuais, o vManage atua como uma autoridade de certificação e gera os certificados para roteadores de nuvem.

Se você estiver usando certificados Enterprise nos controladores, verifique se o certificado raiz da CA Enterprise está instalado no roteador.

Verifique se os certificados raiz estão instalados no roteador usando estes comandos:

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

Verifique a saída de show sdwan control local-properties para certificar-se de que as configurações e os certificados necessários estão no lugar.

```
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   ::
```

Ao verificar a saída de show sdwan control local-properties, certifique-se de que todos estes critérios sejam atendidos:

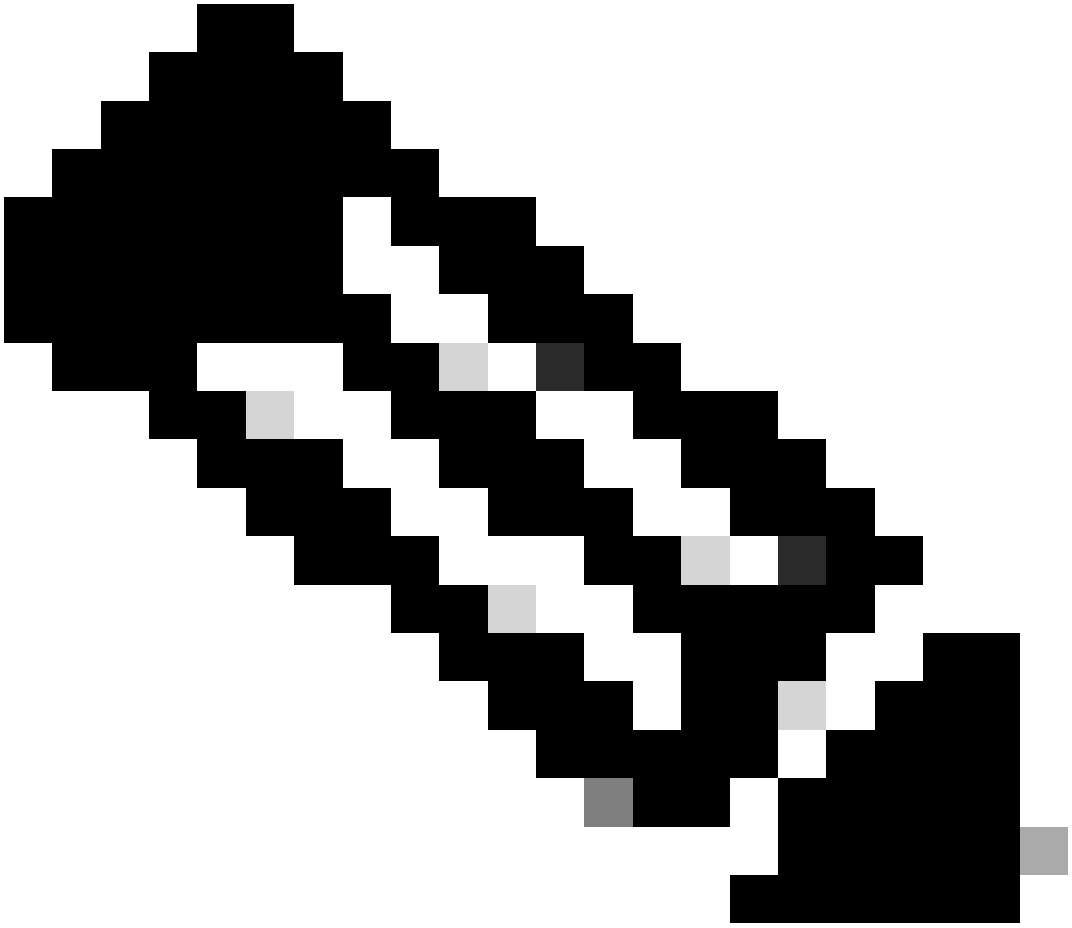
- O nome da organização está refletido corretamente.
- A validade do certificado é válida no momento em que você está verificando a saída.
- O endereço IP/FQDN do vBond está correto.
- System-ip/Site-id está correto.
- O endereço IP do vBond é visto na entrada de "number-vbond-peers". Se o endereço IP do vBond não for visto, verifique se o DNS está resolvendo para o URL do vBond usando o comando ping <vBond FQDN>.
- As interfaces são mapeadas com a cor correta, o endereço IP e o status da interface é UP.
- O MAX CNTRL da interface necessária para formar a conexão de controle não é 0.

Status das Conexões de Controle

Verifique o status da conexão de controle que está usando este comando:

```
show sdwan control connection
```

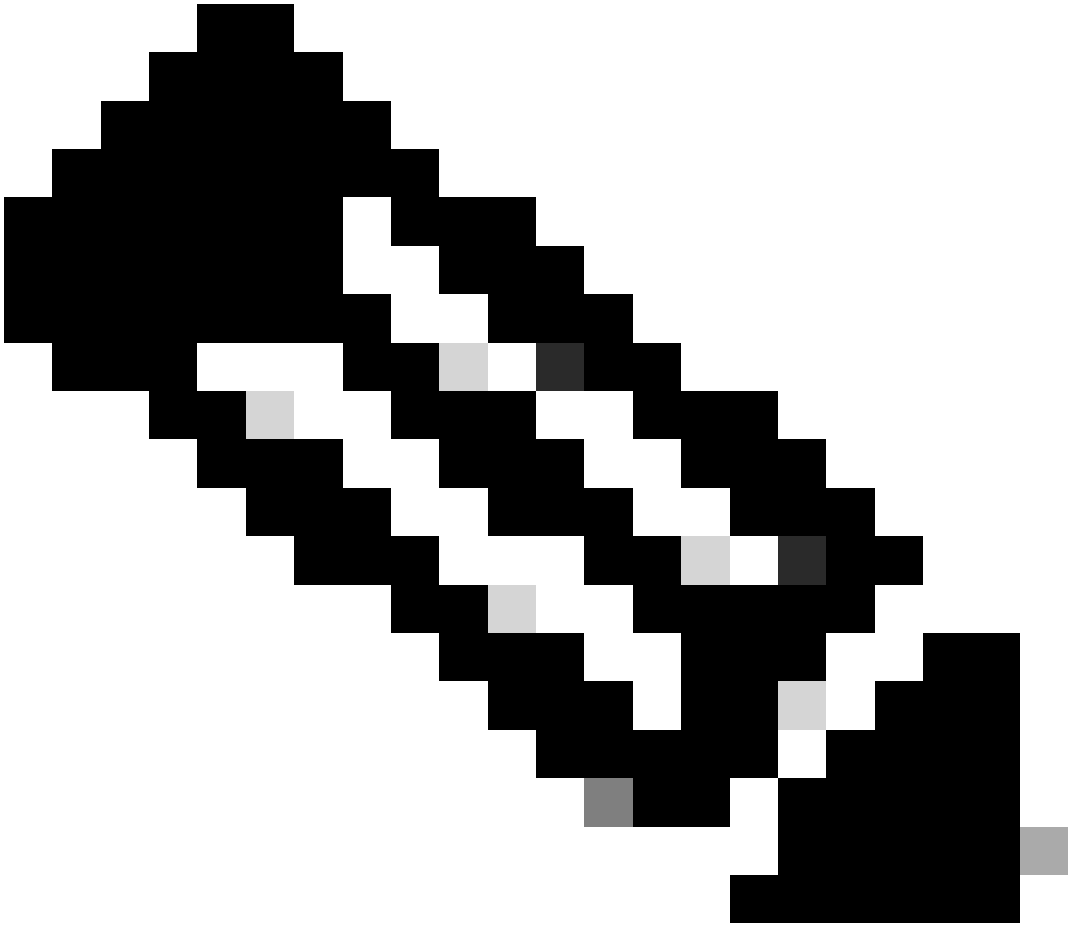
Se todas as conexões de controle estiverem ativas, o dispositivo terá uma conexão de controle formada para vBond, vManage e vSmart. Uma vez estabelecidas as conexões vSmart e vManage necessárias, a conexão de controle vBond é interrompida.



Observação: se houver apenas um vSmart na sobreposição e as conexões de controle máximo estiverem definidas com o valor padrão de 2, uma conexão de controle persistente será mantida no vBond, além da conexão esperada com o vManage e o vSmart.

Essa configuração está disponível na configuração tunnel-interface da seção de interface sdwan. Você pode verificá-lo usando o comando show sdwan run sdwan. Se max-control-connection estiver configurado como 0 na interface, o roteador não forma conexão de controle nessa interface.

Se houver 2 vSmarts na sobreposição, o roteador formará uma conexão de controle para cada vSmart em cada cor do Transport Locator (TLOC) configurada para conexões de controle.



Observação: a conexão de controle para o vManage é formada apenas em uma cor de interface do roteador em um cenário em que o roteador tem várias interfaces configuradas para formar conexões de controle.

```
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.
```

Troubleshooting de Conexões de Controle

Na saída de show sdwan control connections, se todas as conexões de controle necessárias não

estiverem ativas, verifique a saída de 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
```

Na saída show sdwan control connection-history, verifique estes itens:

- O tipo de controlador com o qual a conexão de controle está falhando em um determinado carimbo de data/hora.
- Erro visto quando a conexão de controle falhou. Há 2 colunas para erros, Erro local e Erro remoto. Erro local indica o erro gerado pelo roteador. Remote Error indica o erro gerado pelo respectivo controlador. Há uma legenda de erros no início da saída.
- A contagem de repetição indica o número de vezes em que a conexão falhou pelo mesmo motivo.

Falhas Comuns de Código de Erro

- DCONFAIL (Falha de conexão DTLS): este erro indica que há uma perda de pacotes DTLS que são trocados entre o roteador e o respectivo controlador, devido à qual o handshake DTLS não pode ser concluído. Para entender isso melhor, você pode configurar capturas simultâneas de pacotes no roteador e no respectivo controlador. Diferentes métodos de configuração de capturas de pacotes são compartilhados na seção Captura de pacotes incorporada. Ao analisar as capturas de pacotes, é importante certificar-se de que os pacotes enviados de uma extremidade sejam recebidos na outra extremidade sem nenhuma modificação. Se o pacote enviado de uma extremidade não for recebido na outra extremidade, isso indica que há perda de pacote no circuito subjacente que precisa ser verificado com o provedor de serviços. Mais detalhes sobre como capturar um pacote podem ser encontrados na seção Problemas subjacentes.
- BIDNTVRFD (Board ID Not Verified, ID da placa não verificada): esse erro indica que o UUID e o número de série do certificado não é uma entrada válida na lista vEdge do controlador. Você pode verificar a saída da lista de vetor válida nas controladoras usando estes comandos:

<#root>

vBond:

show orchestrator valid-vedges

vManage/vSmart:

show control valid-vedges

Geralmente, BIDNTVRFD é um erro remoto no roteador porque é gerado no controlador. No controlador respectivo, você pode verificar o log no arquivo vdebuglocalizado no diretório /var/log/tmplog usando estes comandos:

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

- CRTVERFL (Falha na Verificação de Certificado): Este erro indica que o certificado enviado pelo par não pôde ser verificado.
- Se este for um erro local no roteador, ele indicará que o certificado do controlador enviado como parte do handshake DTLS não pôde ser verificado pelo roteador. Um dos motivos comuns para isso é que o roteador não tem o certificado raiz da autoridade de certificação que assinou o certificado do controlador. Verifique o status do certificado com esses comandos para garantir que o certificado raiz necessário esteja presente no roteador.

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

- Se esse erro for um erro remoto no roteador, verifique o arquivo de log vdebug no respectivo controlador para entender a causa usando estes comandos:

```
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): Esses erros indicam que houve perda de pacotes entre os dispositivos, o que faz com que a conexão de controle expire. Para entender isso melhor, você pode configurar capturas simultâneas de pacotes no roteador e no respectivo controlador. Diferentes métodos de configuração de capturas de pacotes são compartilhados na seção Captura de pacotes incorporada. Ao analisar as capturas de pacotes, é importante certificar-se de que os pacotes enviados de uma extremidade sejam recebidos na outra extremidade sem nenhuma modificação. Se o pacote enviado de uma extremidade não for recebido na outra, isso indica que há perda de pacote no circuito subjacente que precisa ser verificada com o provedor de serviços

Para obter orientação sobre como solucionar problemas de outros códigos de erro de falha de conexão de controle, consulte este documento:

Solucionar problemas de conexões de controle SD-WAN

Problemas subjacentes

As ferramentas usadas para solucionar problemas de perda de pacotes na subjacência diferem entre os diferentes dispositivos. Para controladores SD-WAN e roteadores de Bordas, você pode usar o comando tcpdump. Para Catalyst IOS® XE Edges, use o rastreamento EPC (Embedded Packet Capture) e FIA (Feature Invocation Array).

Para entender por que as conexões de controle estão falhando e onde está o problema, você

precisa entender onde está ocorrendo a perda de pacotes. Por exemplo, se você tiver um vBond e um roteador de borda que não está formando uma conexão de controle, este guia ilustra como isolar o problema.

Despejo TCP

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

Com base na solicitação e na resposta dos pacotes, o usuário pode entender o dispositivo responsável pelos descartes. O comando tcpdump pode ser usado em todos os controladores e dispositivos vEdge.

Captura de pacotes incorporada

Crie uma ACL no 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>
```

Configure e inicie a captura do monitor.

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

Pare a captura e exporte o arquivo de captura.

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

Exiba o conteúdo do arquivo no Wireshark para entender as gotas. Você pode encontrar detalhes adicionais em Configurar e Capturar Pacote Incorporado no Software .

Rastreamento FIA

Configure o rastreamento FIA.

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

Exibir as saídas do pacote de frases do fia.

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

Se houver um descarte, analise a saída do rastreamento FIA para o pacote descartado.

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

Para entender as opções adicionais de rastreamento FIA, consulte este documento: Solução de problemas com o recurso IOS-XE Datapath Packet Trace

O vídeo Determine Policy Drops on Catalyst SD-WAN Edge with FIA Trace fornece um exemplo de uso do rastreamento FIA.

Geração de tecnologia administrativa

Consulte Coletar um Admin-Tech no Ambiente SD-WAN e Fazer Upload no Caso TAC - Cisco

Informações Relacionadas

Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.