Resolución de problemas comunes de control SD-WAN y plano de datos

Contenido

Introducción

Este documento describe cómo iniciar la resolución de problemas comunes de control y plano de datos de la red de área extensa definida por software (SD-WAN).

Prerequisites

Requirements

Cisco recomienda que conozca la solución Cisco Catalyst.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

Este artículo se ha diseñado como runbook para proporcionar un punto de partida para los retos de depuración observados en los entornos de producción. Cada sección proporciona casos prácticos comunes y puntos de datos probables para recopilar o buscar al depurar estos problemas frecuentes.

Configuraciones básicas

Asegúrese de que las configuraciones básicas estén presentes en el router y que los valores específicos del dispositivo sean únicos para cada dispositivo en superposición:

Configuraciones del 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
!
```

Configuraciones de interfaz

```
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
```

Asegúrese de que el router tenga una ruta disponible en la tabla de routing para establecer una conexión de control con los controladores (vBond, vManage y vSmart). Puede utilizar este comando para ver todas las rutas instaladas en la tabla de ruteo:

```
show ip route
```

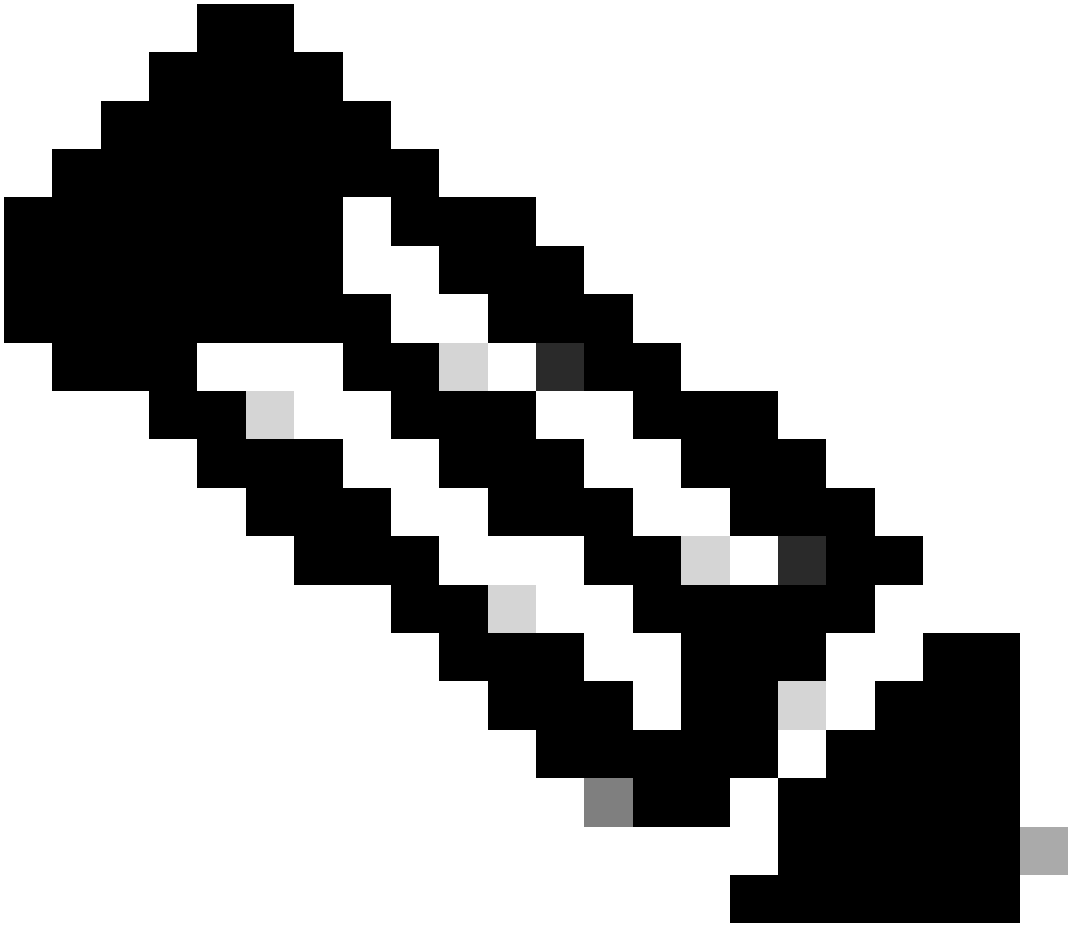
Si utiliza el FQDN de vBond, asegúrese de que el servidor DNS o el servidor de nombres configurado tenga una entrada para resolver el nombre de host de vBond. Puede comprobar qué servidor DNS o servidor de nombres está configurado con este comando:

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

Certificado

Verifique que el certificado esté instalado en el router mediante este comando:

```
show sdwan certificate installed
```



Nota: Si no utiliza certificados de empresa, el certificado ya está disponible en los routers. Para las plataformas de hardware, los certificados de dispositivo están integrados en el hardware del router. En el caso de los routers virtuales, vManage actúa como una autoridad de certificación y genera los certificados para los routers en la nube.

Si utiliza certificados de empresa en los controladores, asegúrese de que el certificado raíz de la CA de empresa está instalado en el router.

Verifique que los certificados raíz estén instalados en el router mediante estos comandos:

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

Verifique el resultado de show sdwan control local-properties para asegurarse de que las configuraciones y los certificados requeridos estén en su 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   ::
```

Al verificar el resultado de show sdwan control local-properties, asegúrese de que se cumplan todos estos criterios:

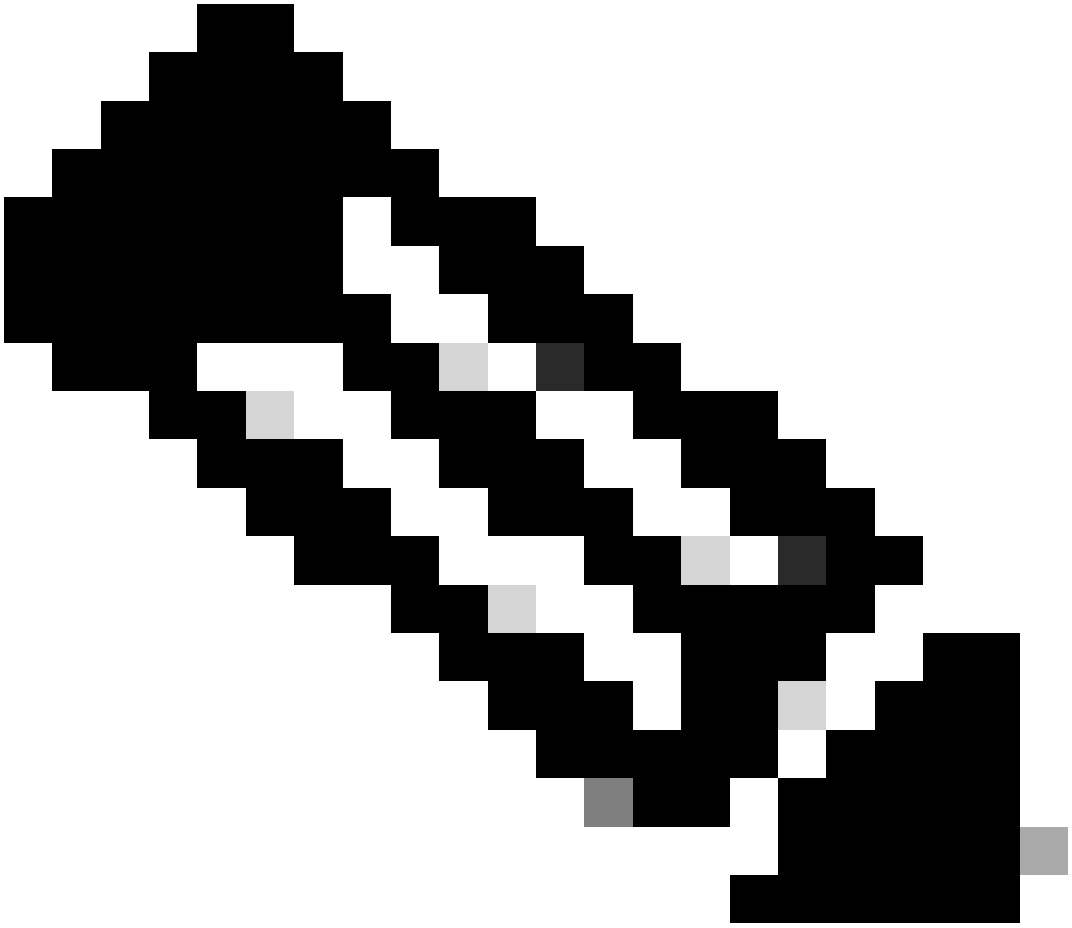
- El nombre de la organización se refleja correctamente.
- La validez del certificado es válida en el momento en que se comprueba el resultado.
- El FQDN/dirección IP de vBond es correcto.
- System-ip/Site-id es correcto.
- La dirección IP de vBond aparece en la entrada correspondiente a "number-vbond-peers". Si no se ve la dirección IP de vBond, compruebe que DNS se resuelve para la URL de vBond mediante el comando ping <vBond FQDN>.
- Las interfaces se asignan con el color correcto, la dirección IP y el estado de la interfaz es UP.
- El MAX CNTRL para la interfaz requerida para formar la conexión de control no es 0.

Estado de las conexiones de control

Verifique el estado de la conexión de control mediante este comando:

```
show sdwan control connection
```

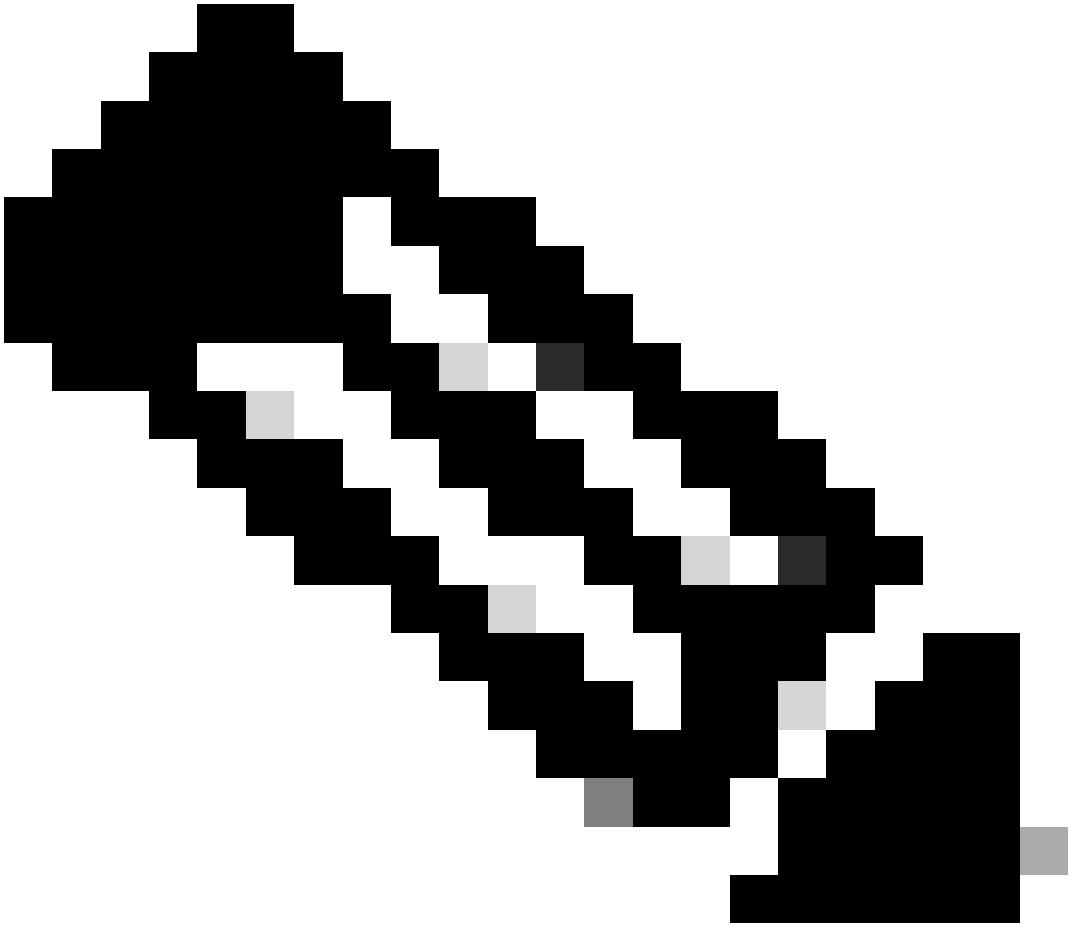
Si todas las conexiones de control están activas, el dispositivo tiene una conexión de control formada por vBond, vManage y vSmart. Una vez establecidas las conexiones vSmart y vManage necesarias, se desactiva la conexión de control vBond.



Nota: si hay un solo vSmart en las conexiones de superposición y max-control se establece en el valor predeterminado de 2, se mantiene una conexión de control persistente a vBond además de la conexión esperada a vManage y vSmart.

Esta configuración está disponible bajo la configuración de la interfaz de túnel de la sección de la interfaz sdwan. Puede verificarlo mediante el comando show sdwan run sdwan. Si max-control-connection se configura en 0 en la interfaz, el router no forma una conexión de control en esa interfaz.

Si hay 2 vSmarts en la superposición, el router forma una conexión de control con cada vSmart en cada color de Transport Locator (TLOC) configurado para las conexiones de control.



Nota: La conexión de control a vManage se forma solamente en un color de interfaz del router en un escenario donde el router tiene varias interfaces configuradas para formar conexiones de control.

```
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.
```

Solución de problemas de conexiones de control

En el resultado de show sdwan control connections, si todas las conexiones de control requeridas

no están activas, verifique el resultado 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
```

En el resultado de show sdwan control connection-history, verifique estos elementos:

- El tipo de controlador al que falla la conexión de control en una marca de tiempo determinada.
- Error que se produce cuando se produce un error en la conexión de control. Hay 2 columnas para los errores, Error local y Error remoto. Error local indica el error generado por el router. Remote Error indica el error generado por el controlador respectivo. Hay una leyenda de errores al principio del resultado.

- Repetir recuento, indica el número de veces, la conexión falló con la misma razón.

Errores comunes de código de error

- DCONFAIL (fallo de conexión DTLS): este error indica que hay una pérdida de paquetes DTLS que se intercambian entre el router y el controlador respectivo debido a la cual no se puede completar el intercambio de señales DTLS. Para entender esto mejor, puede configurar capturas simultáneas de paquetes en el router y en el controlador respectivo. En la sección Captura de Paquetes Integrada se comparten diferentes métodos de configuración de capturas de paquetes. Al analizar las capturas de paquetes, es importante asegurarse de que los paquetes enviados desde un extremo se reciban en el otro extremo sin ninguna modificación. Si el paquete enviado desde un extremo no se recibe en el otro extremo, esto indica que hay una pérdida de paquete en el circuito subyacente que debe verificarse con el proveedor de servicios. Puede encontrar más detalles sobre cómo tomar una captura de paquetes en la sección Problemas Subyacentes.

- BIDNTVRFD (ID de placa no verificada): Este error indica que el UUID y el número de serie del certificado no son entradas válidas en la lista vEdge del controlador. Puede verificar la salida de la lista de vedge válida en los controladores utilizando estos comandos:

<#root>

vBond:

show orchestrator valid-vedges

vManage/vSmart:

show control valid-vedges

Generalmente, BIDNTVRFD es un error remoto en el router porque se genera en el controlador. En el controlador respectivo, puede verificar el registro en el archivo vdebug ubicado en el directorio /var/log/tmplog utilizando estos comandos:

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

- CRTVERFL (Certificate Verification Failed): Este error indica que no se pudo verificar el certificado enviado por el par.
- Si se trata de un error local en el router, indica que el router no pudo verificar el certificado del controlador enviado como parte del protocolo de enlace DTLS. Una de las razones comunes para esto es que el router no tiene el certificado raíz de la autoridad de certificación que firmó el certificado del controlador. Verifique el estado del certificado con estos comandos para asegurarse de que el certificado raíz requerido esté presente en el router.

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

- Si este error es un error remoto en el router, verifique el archivo de registro de depuración en el controlador respectivo para comprender la causa usando estos 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): Estos errores indican que hubo pérdida de paquetes entre los dispositivos, lo que causó que la conexión de control agotara el tiempo de espera. Para entender esto mejor, puede configurar capturas simultáneas de paquetes en el router y en el controlador respectivo. En la sección Captura de Paquetes Integrada se comparten diferentes métodos de configuración de capturas de paquetes. Mientras analiza las capturas de paquetes, es importante asegurarse de que los paquetes enviados desde un extremo se reciban en el otro extremo sin ninguna modificación. Si el paquete enviado desde un extremo no se recibe en el otro extremo, esto indica que hay una pérdida de paquete en el circuito subyacente que debe verificarse con el proveedor de servicios

Para obtener orientación sobre cómo resolver problemas de otros códigos de error de falla de conexión de control, puede consultar este documento:

Solucionar problemas de conexiones de control SD-WAN

Problemas subyacentes

Las herramientas usadas para resolver problemas de pérdida de paquetes en la capa subyacente difieren entre los diferentes dispositivos. Para los controladores SD-WAN y el router vEdges, puede utilizar el comando tcpdump. Para los extremos de Catalyst IOS® XE, utilice el seguimiento de Captura de paquetes integrada (EPC) y Matriz de invocación de características (FIA).

Para comprender por qué fallan las conexiones de control y saber dónde radica el problema, debe saber dónde se produce la pérdida de paquetes. Por ejemplo, si tiene un router vBond y Edge que no forma una conexión de control, esta guía ilustra cómo aislar el problema.

Volcado de TCP

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

Según la solicitud y la respuesta de los paquetes, el usuario puede entender el dispositivo responsable de las caídas. El comando tcpdump se puede utilizar en todos los controladores y dispositivos vEdge.

Captura de paquetes integrada

Cree una ACL en el 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 la captura del monitor.

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

Detenga la captura y exporte el archivo de captura.

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

Vea el contenido del archivo en wireshark para comprender las caídas. Puede encontrar detalles adicionales en Configure and Capture Embedded Packet on Software .

Seguimiento FIA

Configure el seguimiento FIA.

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

Ver las salidas del paquete de frases fia.

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

Si hay un descarte, analice el resultado de seguimiento de FIA para el paquete descartado.

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

Para comprender las opciones de seguimiento FIA adicionales, vea este documento: Solución de Problemas con la Función de Seguimiento de Paquetes de Ruta de Datos IOS-XE

El video Determinación de caídas de políticas en Catalyst SD-WAN Edge con FIA Trace proporciona un ejemplo del uso de la traza FIA.

Generación de Admin-Tech

Consulte Recopilación de una Tecnología de Administración en un Entorno SD-WAN y Carga en el Caso TAC - Cisco

Información Relacionada

Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).