Dépannage des connexions de contrôle SD-WAN

Table des matières

Introduction

Informations générales

Scénarios de problèmes

- Échec de la connexion DTLS (DCONFAIL)
- TLOC désactivé (DISTLOC)
- ID de carte non initialisé (BIDNTPR)
- BDSGVERFL - Échec de signature d'ID de carte
- Coincé dans Connect : Problèmes de routage
- Erreurs de socket (LISFD)
- Problème de délai d'attente d'homologue (VM_TMO)
- Numéro(s) de série absent(s) (CRTREJSER, BIDNTVRFD)
- Non-concordance d'organisation (CTORGNMMIS)
- Certificat vEdge/vSmart révoqué/invalidé (VSCRTREV/CRTVERFL)
- Modèle vEdge non joint dans vManage
- Conditions transitoires (DISCVBD, SYSIPCHNG)
- Échec DNS

Informations connexes

Introduction

Ce document décrit quelques-unes des causes probables qui conduisent à un problème avec les Connexions de contrôle et comment les résoudre.

Informations générales

> Remarque : La plupart des sorties de commande présentées dans ce document proviennent de routeurs vEdge. Cependant, l'approche est la même pour les routeurs qui exécutent le logiciel SD-WAN Cisco IOS® XE. Entrez le mot **sdwan** clé afin d'obtenir les mêmes résultats sur le logiciel Cisco IOS XE SD-WAN. Par exemple, **show sdwan control connections** au lieu de **show control connections**.

Avant de procéder au dépannage, assurez-vous que le périphérique WAN en question a été

configuré correctement.

Il comprend :

- Un certificat valide qui est installé.
- Ces configurations sont mises en place sous le system bloc :
  - System-IP
  - ID du site
  - Nom de l'entreprise
  - Adresse vBond
- Interface de transport VPN 0 configurée avec l'option de tunnel et l'adresse IP.
- Horloge système configurée correctement sur le serveur vEdge et celles qui correspondent à d'autres périphériques/contrôleurs :

La **show clock** commande confirme l'heure actuelle définie.

Entrez la **clock set** commande afin de définir l'heure correcte sur le périphérique.

Pour tous les cas mentionnés précédemment, assurez-vous que le localisateur de transport (TLOC) est activé. Vérifiez cela à l'aide de la **show control local-properties** commande.

Un exemple de résultat valide est présenté ici :

<#root>

```
branch-vE1#

show control local-properties

personality                   vedge
organization-name             vIPtela Inc Regression
certificate-status            Installed
root-ca-chain-status          Installed

certificate-validity          Valid
certificate-not-valid-before Sep 06 22:39:01 2018 GMT
certificate-not-valid-after  Sep 06 22:39:01 2019 GMT

dns-name                      vbond-dns-name.cisco.com
site-id                       10
domain-id                     1
protocol                      dtls
tls-port                      0
system-ip                     10.1.10.1
chassis-num/unique-id         66cb2a8b-2eeb-479b-83d0-0682b64d8190
serial-num                    12345718
vsmart-list-version           0
keygen-interval               1:00:00:00
```

```
retry-interval               0:00:00:17
no-activity-exp-interval     0:00:00:12
dns-cache-ttl                0:00:02:00
port-hopped                  TRUE
time-since-last-port-hop     20:16:24:43
number-vbond-peers           2

INDEX   IP                  PORT
------------------------------
0       10.3.25.25          12346
1       10.4.30.30          12346

number-active-wan-interfaces 2

 PUBLIC      PUBLIC  PRIVATE     PRIVATE                                    RESTRICT/   LAST         MAX
INTERFACE  IPv4        PORT    IPv4        PORT     VS/VM COLOR       CARRIER  STATE CONTROL     CONNEC
-------------------------------------------------------------------------------------------------------
ge0/1      10.1.7.11    12346   10.1.7.11    12346     2/1  gold        default  up      no/yes    0:00
ge0/2      10.2.9.11    12366   10.2.9.11    12366     2/0  silver      default  up      no/yes    0:00
```

Dans le logiciel vEdge version 16.3 et ultérieure, le résultat comporte quelques champs supplémentaires :

```
number-vbond-peers           1
number-active-wan-interfaces 1


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               PRIVATE                          MAX
INTERFACE  IPv4          PORT   IPv4         IPv6                  PORT   VS/VM COLOR         STATE CN
                                                                                              STUN
-------------------------------------------------------------------------------------------------------
ge0/4  172.16.0.20   12386  192.168.0.20  2601:647:4380:ca75::c2  12386  2/1  public-internet  up   2
```

Scénarios de problèmes

Échec de la connexion DTLS (DCONFAIL)

C'est l'un des problèmes courants de connectivité de contrôle qui ne se pose pas. Les causes probables incluent un pare-feu ou d'autres problèmes de connectivité.

Il se peut que certains ou tous les paquets soient abandonnés/filtrés quelque part. L'exemple avec les plus grands est donné dans**tcpdump** les résultats ici.

- Le routeur de tronçon suivant (NH) n'est pas accessible.
- La passerelle par défaut n'est pas installée dans la base d'informations de routage (RIB).
- Le port DTLS (Datagram Transport Layer Security) n'est pas ouvert dans les contrôleurs.

Les commandes show suivantes peuvent être utilisées :

<#root>

```
#Check that Next hop

show ip route vpn 0


#Check ARP table for Default GW

show arp


#Ping default GW
ping <...>
#Ping Google DNS
ping 8.8.8.8
#Ping vBond if ICMP is allowed on vBond
ping <vBond IP>
#Traceroute to vBond DNS
traceroute <...>
```

Lorsque vous rencontrez un échec de connexion DTLS, vous pouvez le voir dans le résultat de la **show control connections-history** commande.

```
                                                                                    PEER
         PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP
-------------------------------------------------------------------------------------------------------
0        vsmart   tls      10.0.1.5          160000000   1      10.0.2.73        23456    10.0.2.73
```

Voici ce qui se produit lorsque de gros paquets n'atteignent pas vEdge lorsque vous utilisez, par exemple, **tcpdump**,du côté SD-WAN (vSmart) :

```
tcpdump vpn 0 interface eth1 options "host 198.51.100.162 -n"

13:51:35.312109 IP 198.51.100.162.9536 > 172.18.10.130.12546: UDP, length 140 <<<< 1 (packet number)
13:51:35.312382 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 1024 <<< not reached vEdege
13:51:35.318654 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 1024 <<< not reached vEdege
13:51:35.318726 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 853 <<< not reached vEdege
13:51:36.318087 IP 198.51.100.162.9536 > 172.18.10.130.12546: UDP, length 140 <<<< 5
13:51:36.318185 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 79 <<<< 6
```

```
13:51:36.318233 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 1024 << not reached vEdege
13:51:36.318241 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 879 << not reached vEdege
13:51:36.318257 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 804 << not reached vEdege
13:51:36.318266 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 65 <<<< 10
13:51:36.318279 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 25 <<<< 11
```

Un exemple du côté vEdge est illustré ici :

```
tcpdump vpn 0 interface ge0/1 options "host 203.0.113.147 -n"

13:51:35.250077 IP 198.51.100.162.12426 > 203.0.113.147.12746: UDP, length 140 <<<< 1
13:51:36.257490 IP 198.51.100.162.12426 > 203.0.113.147.12746: UDP, length 140 <<<< 5
13:51:36.325456 IP 203.0.113.147.12746 > 198.51.100.162.12426: UDP, length 79 <<<< 6
13:51:36.325483 IP 203.0.113.147.12746 > 198.51.100.162.12426: UDP, length 65 <<<< 10
13:51:36.325538 IP 203.0.113.147.12746 > 198.51.100.162.12426: UDP, length 25 <<<< 11
```

Remarque : Sur le logiciel Cisco IOS XE SD-WAN, vous pouvez utiliser Embedded Packet Capture (EPC) au lieu de **tcpdump**.

Vous pouvez également utiliser **traceroute** ou des **nping** utilitaires pour générer du trafic avec différentes tailles de paquets et des marques DSCP (Differentiated Services Code Point) afin de vérifier la connectivité, car votre fournisseur de services peut rencontrer des problèmes avec la livraison de paquets UDP plus volumineux, de paquets UDP fragmentés (en particulier de petits fragments UDP) ou de paquets marqués DSCP. Voici un exemple de connexion **nping** réussie lorsque la connectivité est établie.

Depuis vSmart :

<#root>

```
vSmart#

tools nping vpn 0 198.51.100.162 options "--udp -p 12406 -g 12846 --source-ip 172.18.10.130 --df --data-

Nping in VPN 0
Starting Nping 0.6.47 ( http://nmap.org/nping ) at 2019-05-17 23:28 UTC
SENT (0.0220s) UDP 172.18.10.130:12846 > 198.51.100.162:12406 ttl=64 id=16578 iplen=583
SENT (1.0240s) UDP 172.18.10.130:12846 > 198.51.100.162:12406 ttl=64 id=16578 iplen=583
```

Un exemple de vEdge est présenté ici :

<#root>

```
vEdge#

tcpdump vpn 0 interface ge0/1 options "-n host 203.0.113.147 and udp"

tcpdump -i ge0_1 -s 128 -n host 203.0.113.147 and udp in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_1, link-type EN10MB (Ethernet), capture size 128 bytes
18:29:43.492632 IP 203.0.113.147.12846 > 198.51.100.162.12406: UDP, length 555
18:29:44.494591 IP 203.0.113.147.12846 > 198.51.100.162.12406: UDP, length 555
```

Et voici un exemple d'échec de connectivité avec la **traceroute** commande (qui s'exécute à partir de vShell) sur vSmart :

```
<#root>

vSmart$

traceroute 198.51.100.162 1400 -F -p 12406 -U -t 192 -n -m 20

traceroute to 198.51.100.162.162 (198.51.100.162.162), 20 hops max, 1400 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  10.65.14.177  0.435 ms 10.65.13.225  0.657 ms  0.302 ms
 7  10.10.28.115  0.322 ms 10.93.28.127  0.349 ms 10.93.28.109  1.218 ms
 8  * * *
 9  * * *
10  * 10.10.114.192  4.619 ms *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  10.68.72.61  2.162 ms * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```

vEdge ne reçoit pas les paquets envoyés par vSmart (uniquement certains autres trafics ou fragments) :

<#root>

vEdge#

tcpdump vpn 0 interface ge0/1 options "-n host 203.0.113.147 and udp"

```
tcpdump -i ge0_1 -s 128 -n host 203.0.113.147 and udp in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_1, link-type EN10MB (Ethernet), capture size 128 bytes
18:16:30.232959 IP 203.0.113.147.12846 > 198.51.100.162.12386: UDP, length 65
18:16:30.232969 IP 203.0.113.147.12846 > 198.51.100.162.12386: UDP, length 25
18:16:33.399412 IP 203.0.113.147.12846 > 198.51.100.162.12386: UDP, length 16
18:16:34.225796 IP 198.51.100.162.12386 > 203.0.113.147.12846: UDP, length 140
18:16:38.406256 IP 203.0.113.147.12846 > 198.51.100.162.12386: UDP, length 16
18:16:43.413314 IP 203.0.113.147.12846 > 198.51.100.162.12386: UDP, length 16
```

TLOC désactivé (DISTLOC)

Les déclencheurs des messages TLOC Disabled peuvent être dus aux causes probables suivantes :

- Effacer les connexions de contrôle
- Modifier la couleur sur TLOC
- Modification de l'adresse IP du système

Changement dans l'une des configurations mentionnées dans le bloc système ou dans les propriétés de tunnel dans**show control connections-history**la sortie de commande.

```
                                                                    PEER                    PEER
PEER     PEER     PEER             SITE        DOMAIN PEER         PRIVATE  PEER           PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP   PORT     PUBLIC IP      PORT
-------------------------------------------------------------------------------------------------
vmanage  dtls     192.168.30.101   1           0      192.168.20.101   12346    192.168.20.101   12346
vsmart   dtls     192.168.30.103   1           1      192.168.20.103   12346    192.168.20.103   12346
vbond    dtls     0.0.0.0          0           0      192.168.20.102   12346    192.168.20.102   12346
```

ID de carte non initialisé (BIDNTPR)

Dans un réseau très instable, où les connexions réseau sont constamment instables, vous pouvez"TXCHTOBD - failed to send a challenge to Board ID failed"voir et/ou « RDSIGFBD - Read Signature from Board ID failed ». En outre, parfois en raison de problèmes de verrouillage, une demande envoyée à l'ID de carte échoue et lorsque cela se produit, réinitialisez l'ID de carte et réessayez. Cela n'arrive pas souvent et cela retarde la forme des connexions de contrôle. Ceci est corrigé dans les versions ultérieures.

```
                                                                                PEER                    P
PEER     PEER     PEER             SITE        DOMAIN      PEER               PRIVATE  PEER            P
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP         PORT     PUBLIC IP       P
-------------------------------------------------------------------------------------------------------
vbond    dtls     -                0           0           203.0.113.109      12346    203.0.113.109   1
vbond    dtls     -                0           0           203.0.113.56       12346    203.0.113.56    1
```

BDSGVERFL - Échec de signature d'ID de carte

Cela indique que le numéro de châssis/ID unique/numéro de série vEdge est rejeté par le vBond. Dans ce cas, confirmez les informations vEdge affichées dans le résultat de la **show control local-properties** commande et comparez ce résultat à **show orchestrator valid-vedges** sur le vBond.

Si aucune entrée n'existe pour le vEdge, assurez-vous que vous disposez des éléments suivants :

- Ajout du vEdge au compte Smart.
- Téléchargez ce fichier correctement dans vManage.

Cliquez **Send to Controllers** sous **Configuration** > **Certificates**.

Si tel est le cas, vérifiez les entrées en double dans le tableau des serveurs vEdge valides et contactez le centre d'assistance technique Cisco (TAC) pour résoudre ce problème

Coincé dans Connect : Problèmes de routage

Les connexions de contrôle ne s'activent pas en cas de problèmes de routage sur le réseau. Assurez-vous qu'il existe une route valide dans le RIB avec le NH/TLOC correct.

Exemples :

- Une route plus spécifique vers vBond dans le RIB pointe vers un NH/TLOC qui n'est pas utilisé pour établir des connexions de contrôle.
- L'adresse IP TLOC est divulguée entre le fournisseur de services en amont, ce qui entraîne un routage incorrect.

Entrez ces commandes pour la vérification :

```
show ip route
```

```
show ip routes vpn 0 <prefix/mask>
ping <vBond IP>
```

Recherchez la valeur de distance et le protocole du préfixe IP.

vEdge tente d'établir une connexion de contrôle sans succès ou les connexions aux contrôleurs continuent de battre.

Vérifiez à l'aide des **show control connections** et/ou des **show sdwan control connections-history** commandes.

<#root>

```
vedge1#

show control connections
```

```
                                                                                    PEER
PEER    PEER PEER            SITE       DOMAIN PEER                                 PRIV  PEER
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                           PORT  PUBLIC IP
-------------------------------------------------------------------------------------------------
vbond   dtls 0.0.0.0         0          0      192.168.20.102                       12346 192.168.20
```

Erreurs de socket (LISFD)

S'il existe une adresse IP dupliquée sur le réseau, les connexions de contrôle ne s'activent pas. Vous voyez le "LISFD - Listener Socket FD Error" message. Cela peut également se produire pour d'autres raisons, telles que la corruption de paquets, une réinitialisation, une non-correspondance entre vEdge et les contrôleurs sur les ports TLS par rapport aux ports DTLS, si les ports FW ne sont pas ouverts, etc.

La cause la plus fréquente est une adresse IP de transport dupliquée. Vérifiez la connectivité et assurez-vous que les adresses sont uniques.

```
                                                                    PEER                  P
PEER     PEER     PEER             SITE        DOMAIN      PEER    PRIVATE  PEER         P
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP PORT   PUBLIC IP    P
-------------------------------------------------------------------------------------------
vbond    dtls     -                0           0           203.0.113.21 12346 203.0.113.21 1
```

Problème de délai d'attente d'homologue (VM_TMO)

Une condition de délai d'attente d'homologue est déclenchée lorsqu'un vEdge perd l'accessibilité au contrôleur en question.

Dans cet exemple, il capture un élément**v**Manage Timeout msg (peer VM_TMO). « Autres » qui inclut les délais d'attente vBond, vSmart et/ou vEdge (VB_TMO, VP_TMO, VS_TMO) des homologues.

Dans le cadre du dépannage, assurez-vous que vous disposez d'une connectivité avec le contrôleur. Utilisez le protocole ICMP (Internet Control Message Protocol) et/ou **traceroute** l'adresse IP en question. Cas où il y a beaucoup de pertes de trafic (perte élevée). Rapide **ping** et s'assurer qu'il est bon.

```
                                                                                  PEER                      P
PEER     PEER     PEER             SITE        DOMAIN      PEER              PRIVATE  PEER              P
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP        PORT     PUBLIC IP         P
-------------------------------------------------------------------------------------------------------------
vmanage  tls      10.0.1.3          3           0           10.0.2.42         23456    203.0.113.124     2
```

En outre, vérifiez le résultat de la **show control connections-history detail** commande afin de regarder les statistiques de contrôle TX/RX pour voir s'il y a une différence significative dans les compteurs. Notez dans le résultat la différence entre les numéros de paquets Hello RX et TX.

```
----------------------------------------------------------------------------------------
 LOCAL-COLOR- biz-internet SYSTEM-IP- 192.168.30.103   PEER-PERSONALITY- vsmart
----------------------------------------------------------------------------------------
site-id             1
domain-id           1
protocol            dtls
private-ip          192.168.20.103
private-port        12346
public-ip           192.168.20.103
public-port         12346
UUID/chassis-number 4fc4bf2c-f170-46ac-b217-16fb150fef1d
state               tear_down [Local Err: ERR_DISABLE_TLOC] [Remote Err: NO_ERROR]
downtime            2019-06-01T14:52:49+0200
repeat count        5
previous downtime   2019-06-01T14:43:11+0200

  Tx Statistics-
  --------------
    hello                   597
    connects                0
    registers               0
    register-replies        0
    challenge               0
    challenge-response      1
    challenge-ack           0
    teardown                1
    teardown-all            0
    vmanage-to-peer         0
    register-to-vmanage     0
```

```
  Rx Statistics-
  --------------
    hello                   553
    connects                0
    registers               0
    register-replies        0
    challenge               1
    challenge-response      0
    challenge-ack           1
    teardown                0
    vmanage-to-peer         0
    register-to-vmanage     0
```

Numéro(s) de série absent(s) (CRTREJSER, BIDNTVRFD)

Si le numéro de série n'est pas présent sur les contrôleurs d'un périphérique donné, les connexions de contrôle échouent.

Il peut être vérifié avec des **show controllers [valid-vsmarts | valid-vedges]** sorties et fixé la plupart du temps. Accédez aux **Configuration > Certificates > Send to Controllers or Send to vBond** boutons à partir des onglets vManage. Sur vBond, vérifiez **show orchestrator valid-vedges/show orchestrator valid-vsmarts.**

Dans les journaux sur vBond, vous observez ces messages avec raison ERR_BID_NOT_VERIFIED:

```
messages:local7 info: Dec 21 01:13:31 vBond-1 VBOND[1677]: %Viptela-vBond-1-vbond_0-6-INFO-1400002: Not
y-level:major host-name:"vBond-1" system-ip:10.0.1.11 uuid:"11OG301234567" organization-name:"Example_O
```

Lorsque vous dépannez un tel problème, assurez-vous que le numéro de série et le modèle de périphérique corrects ont été configurés et mis en service sur le portail Plug and Play (software.cisco.com) et sur vManage.

Afin de vérifier le numéro de châssis et le numéro de série du certificat, cette commande peut être utilisée sur les routeurs vEdge :

<#root>

```
vEdge1#
```

```
show control local-properties | include  "chassis-num|serial-num"
```

```
chassis-num/unique-id        11OG528180107
serial-num                   1001247E
```

Sur un routeur qui exécute le logiciel Cisco IOS XE SD-WAN, entrez cette commande :

```
<#root>

cEdge1#

show sdwan control local-properties | include chassis-num|serial-num

chassis-num/unique-id            C1111-4PLTEEA-FGL223911LK
serial-num                       016E9999
```

Ou cette commande :

```
<#root>

Router#

show crypto pki certificates CISCO_IDEVID_SUDI | s ^Certificate

Certificate
  Status: Available
  Certificate Serial Number (hex): 016E9999
  Certificate Usage: General Purpose
  Issuer:
    o=Cisco
    cn=High Assurance SUDI CA
  Subject:
    Name: C1111-4PLTEEA
    Serial Number: PID:C1111-4PLTEEA SN:FGL223911LK
    cn=C1111-4PLTEEA
    ou=ACT-2 Lite SUDI
    o=Cisco
    serialNumber=PID:C1111-4PLTEEA SN:FGL223911LK
  Validity Date:
    start date: 15:33:46 UTC Sep 27 2018
    end   date: 20:58:26 UTC Aug 9 2099
  Associated Trustpoints: CISCO_IDEVID_SUDI
```

Pour les problèmes liés à vEdge/vSmart

Voici comment l'erreur se présente sur vEdge/vSmart dans le résultat de la **show control connections-history** commande :

```
                                                                    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      192.168.0.231    12346    192.168.0.231    12346
```

Sur vBond dans le résultat de la **show orchestrator connections-history** commande :

```
                                                                                                  PEER     PEER
         PEER     PEER     PEER             SITE        DOMAIN      PEER             PEER      PRIVATE  PEER
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT      PUBLIC IP
-------------------------------------------------------------------------------------------------------------
0        unknown  dtls     -                0           0           ::               0         192.168.1
```

En outre, le numéro de série du périphérique sur vBond ne figure pas dans la liste des vEdge valides :

<#root>

```
vbond1#
```

show orchestrator valid-vedges | i 11OG528180107

Pour les problèmes avec les contrôleurs

Si le fichier série entre les contrôleurs lui-même ne correspond pas, l'erreur locale sur vBond est le numéro de série qui n'est pas présent par rapport au certificat révoqué pour vSmarts/vManage.

Sur vBond :

```
                                                                                                  PEER     PEER
         PEER     PEER     PEER             SITE        DOMAIN      PEER             PEER      PRIVATE  PEER
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT      PUBLIC IP
-------------------------------------------------------------------------------------------------------------
0        unknown  dtls     -                0           0           ::               0         192.168.0
```

<#root>

```
vbond1#
```

show orchestrator valid-vsmarts

```
SERIAL
NUMBER  ORG
-----------------------
0A      SAMPLE - ORGNAME
```

```
0B      SAMPLE - ORGNAME
0C      SAMPLE - ORGNAME
0D      SAMPLE - ORGNAME
```

Sur vSmart/vManage affecté :

```
                                                                                    PEER
          PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
INSTANCE  TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP
-------------------------------------------------------------------------------------------------
0         vbond    dtls     0.0.0.0          0           0      192.168.0.231    12346    192.168.0.231
```

<#root>

```
vsmart#
```

show control local-properties| i serial-num

```
serial-num                      0F
```

En outre, vous voyez des messages ORPTMO sur le vSmart affecté en ce qui concerne vEdge :

```
                                                                                    PEER
          PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
INSTANCE  TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP
-------------------------------------------------------------------------------------------------
0         unknown  tls      -                0           0      ::               0        192.168.10.238
0         unknown  tls      -                0           0      ::               0        192.168.10.238
0         unknown  tls      -                0           0      ::               0        198.51.100.100
0         unknown  tls      -                0           0      ::               0        198.51.100.100
0         unknown  tls      -                0           0      ::               0        192.168.10.240
```

Sur vEdge affecté vSmart, dans le résultat, **show control connections-history** l'erreur SERNTPRES est vue :

```
                                                                                PEER                    PEER
PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER                    PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP               PORT
-------------------------------------------------------------------------------------------------------------
vsmart   tls      10.10.10.229     1           1      192.168.0.229    23456    192.168.0.229           23456
vsmart   tls      10.10.10.229     1           1      192.168.0.229    23456    192.168.0.229           23456
```

Numéro De Châssis/ID Unique Incorrect

Un autre exemple de la même erreur CRTREJSER/NOERR peut être vu si le mauvais ID de produit (modèle) est utilisé sur le portail PnP. Exemple :

```
<#root>
vbond#
show orchestrator valid-vedges | include ASR1002
ASR1002-HX-DNA-JAE21050110            014EE30A                          valid     Cisco SVC N1
```

Cependant, le modèle réel de l'appareil est différent (notez que le préfixe ADN n'est pas dans le nom) :

```
<#root>
ASR1k#
show sdwan control local-properties | include chassis-num
chassis-num/unique-id        ASR1002-HX-JAE21050110
```

Non-concordance d'organisation (CTORGNMMIS)

Le nom de l'organisation est un composant essentiel pour activer la connexion de contrôle. Pour une superposition donnée, le nom de l'organisation doit correspondre sur tous les contrôleurs et sur toutes les arêtes afin que les connexions de contrôle puissent être établies.

Si ce n'est pas le cas, il existe un « organisme de certification ». name mismatch" comme indiqué ici :

```
                                                                    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      203.0.113.197 12346    203.0.113.197  12346
vbond    dtls     -                0           0      198.51.100.137 12346   198.51.100.137 12346
```

Certificat vEdge/vSmart révoqué/invalidé (VSCRTREV/CRTVERFL)

Si le certificat est révoqué sur les contrôleurs ou si le numéro de série vEdge est invalidé, un message de révocation de la certification vSmart ou vEdge, respectivement, s'affiche.

Voici des exemples de résultats de messages de révocation de certificat vSmart. Il s'agit du certificat qui est révoqué sur vSmart :

```
                                                                                PEER                    PEER
         PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP
-------------------------------------------------------------------------------------------------------
0        vbond    dtls     0.0.0.0          0           0      192.168.0.231    12346    192.168.0.231
1        vbond    dtls     0.0.0.0          0           0      192.168.0.231    12346    192.168.0.231
```

De même, sur un autre vSmart dans la même superposition, c'est ainsi qu'il voit le vSmart dont le certificat est révoqué :

```
                                                                              PEER                    PEER
         PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP
-------------------------------------------------------------------------------------------------------
0        vsmart   tls      10.10.10.229     1           1      192.168.0.229    23456    192.168.0.229
```

Et voici comment vBond voit cela :

```
                                                                                    PEER     PEER
         PEER     PEER     PEER             SITE        DOMAIN      PEER           PRIVATE  PEER
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP     PORT     PUBLIC IP
-------------------------------------------------------------------------------------------------------
0        vsmart   dtls     10.10.10.229     1           1           192.168.0.229  12346    192.168.0
```

L'échec de la vérification de la certification se produit lorsque le certificat ne peut pas être vérifié avec le certificat racine installé :

1. Vérifiez l'heure avec la **show clock** commande. Elle doit être au moins comprise dans la plage de validité du certificat vBond (vérifiez à l'aide de la **show orchestrator local-properties** commande).

2. Cela peut être causé par la corruption du certificat racine sur vEdge.

Ensuite, **show control connections-history** la commande sur le routeur vEdge affiche un résultat similaire :

```
                                                                                    PEER                    P
PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE  PEER            P
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT     PUBLIC IP       P
-------------------------------------------------------------------------------------------------------------
vbond    dtls     -                0           0           203.0.113.82     12346    203.0.113.82    1
vbond    dtls     -                0           0           203.0.113.81     12346    203.0.113.81    1
```

Dans ce cas, vEdge ne peut pas non plus valider le certificat du contrôleur. Afin de résoudre ce problème, vous pouvez réinstaller la chaîne de certificats racine. Si l'autorité de certification Symantec est utilisée, vous pouvez copier la chaîne de certificats racine à partir du système de fichiers en lecture seule :

<#root>

```
vEdge1#

vshell

vEdge1:~$

cp /rootfs.ro/usr/share/viptela/root-ca-sha1-sha2.crt /home/admin/

vEdge1:~$

exit

exit
vEdge1#

request root-cert-chain install /home/admin/root-ca-sha1-sha2.crt

Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/root-ca-sha1-sha2.crt via VPN 0
Installing the new root certificate chain
Successfully installed the root certificate chain
```

Modèle vEdge non joint dans vManage

Au moment où le périphérique est activé si le périphérique n'est pas connecté à un modèle sur vManage, le message d'"NOVMCFG - No Config in vManage for device"erreur s'affiche.

```
                                                                    PEER                    PEER
```

```
PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER             PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP        PORT
-------------------------------------------------------------------------------------------------------
vmanage  dtls     10.0.1.1          1           0      10.0.2.80        12546    203.0.113.128    12546
```

Conditions transitoires (DISCVBD, SYSIPCHNG)

Voici quelques conditions transitoires dans lesquelles les connexions de contrôle sont instables. Ils incluent :

- L'adresse IP système a changé sur le serveur vEdge.
- Message de démontage vers vBond (la connexion de contrôle vers vBond est transitoire).

```
                                                                PEER                     PEER
PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER             PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP        PORT
-------------------------------------------------------------------------------------------------------
vmanage  dtls     10.0.0.1          1           0      198.51.100.92    12646    198.51.100.92    12646
```

Échec DNS

Lorsqu'aucune tentative de connexion n'apparaît dans la **show control connection-history** commande, vous pouvez vérifier l'échec de la résolution DNS vers le vBond en procédant comme suit :

- Envoyez une requête ping vers l'adresse DNS du vBond.

```
ping vbond-dns-name.cisco.com
ping vbond-dns-name.cisco.com: Temporary failure in name resolution
```

- Envoyez une requête ping à google DNS (8.8.8.8) à partir de l'interface source pour vérifier l'accessibilité à Internet.

```
ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
```

- Capture de paquets intégrée pour le trafic DNS sur le port 53 pour vérifier le trafic DNS envoyé et reçu.

```
monitor capture mycap interface <interface that forms control>
monitor capture mycap match ipv4 <source IP> <vBond IP>
```

Document de référence : Capture de paquets intégrée.

Démarrez la capture de surveillance et laissez-la s'exécuter pendant quelques minutes, puis arrêtez la capture. Examinez la capture de paquets pour voir si les requêtes DNS sont envoyées et reçues.

Informations connexes

- Configuration des paramètres de base pour former les connexions de contrôle sur le routeur de périphérie Cisco
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.