Configurer l'entrée d'hôte pour le contrôleur vBond SDWAN

Table des matières

[Introduction](#)

[Conditions préalables](#)

- [Exigences](#)
- [Composants utilisés](#)
- [Portée](#)
- [Considérations](#)

[Problème : Scénarios DNS avec entrée FQDN](#)

- [Scénario 1. Entrée DNS avec FQDN, la résolution fonctionne](#)
- [Scénario 2. Entrée DNS avec FQDN, échec de la résolution](#)

[Solution : Configuration de l'entrée DNS avec IP statique](#)

- [Configuration pour vEdge](#)
- [Configuration des contrôleurs](#)
- [Configuration du routeur de périphérie Cisco](#)
- [Configuration supplémentaire](#)
- [Problèmes de configuration courants](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer l'entrée d'hôte pour l'authentificateur SD-WAN (Software Defined Wide Area Network).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Authentificateur SD-WAN Cisco
- Réseau étendu défini par logiciel (SD-WAN) de Cisco

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Manager 20.12.8.1
- Logiciel du contrôleur 20.12.8.1
- Logiciel Authenticator 20.12.8.1
- Logiciel du routeur Cisco Edge (cEdge) 17.12.8
- Logiciel du routeur Viptela Edge (vEdge) 20.9.10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Portée

Configurez l'entrée d'hôte vBond en cas de problèmes de serveur de noms de domaine (DNS) tels que, mais sans s'y limiter :

- Connectivité DNS
- Impossible de traduire le nom de domaine complet (FQDN)

Considérations

Ce document suppose :

- Les routeurs WAN SD-WAN Edge sont entièrement fonctionnels
- La configuration de base est appliquée aux contrôleurs
- Les contrôleurs et les routeurs de périphérie ont une connectivité entre eux
- Le réseau comporte un authentificateur, un gestionnaire et des contrôleurs qui sont opérationnels et en bon état

---

Problème : Scénarios DNS avec entrée FQDN

Scénario 1. Entrée DNS avec FQDN, la résolution fonctionne

Voici un exemple de configuration courante avec FQDN :

```
vedge# show running-config system vbond
system
 vbond vbond.lab.sdwan
!
vedge# show running-config vpn 0 dns
vpn 0
 dns 192.168.1.11 primary
!
```

Voici le résultat attendu lorsque la traduction DNS fonctionne correctement :

```
vedge# nslookup vbond.lab.sdwan
nslookup in VPN 0:
Server:    192.168.1.11
Address 1: 192.168.1.11

Name:      vbond.lab.sdwan
Address 1: 192.168.2.1 vbond.lab.sdwan
Address 2: 192.168.2.2 vbond.lab.sdwan

vedge# ping vbond.lab.sdwan
Ping in VPN 0
PING vbond.lab (192.168.2.1) 56(84) bytes of data.
64 bytes from vbond.lab (192.168.2.1): icmp_seq=1 ttl=63 time=26.1 ms
```

Scénario 2. Entrée DNS avec FQDN, échec de la résolution

Cette configuration est la même que dans le scénario précédent :

```
vedge# show running-config system vbond
system
 vbond vbond.lab.sdwan
!
vedge# show running-config vpn 0 dns
vpn 0
 dns 192.168.1.11 primary
!
```

Cette fois, la résolution DNS échoue :

```
vedge#nslookup vbond.lab.sdwan
nslookup in VPN 0:
Server: 192.168.1.11
Address 1: 192.168.1.11
nslookup: can't resolve 'vbond.lab.sdwan'
vedge#
vedge# ping vpn 0 vbond.lab.sdwan
Ping in VPN 0
ping: vbond.lab.sdwan: Name or service not known
vedge#
```

Solution : Configuration de l'entrée DNS avec IP statique

Configuration pour vEdge

Configurez la commande host avec les adresses IP FQDN et vBond :

```
vedge# show running-config vpn 0 host
vpn 0
 host vbond.lab.sdwan ip 192.168.2.1 192.168.2.2
!
vedge#
```

Exécutez la commande nslookup à des fins de validation :

```
vedge# nslookup vbond.lab.sdwan
nslookup in VPN 0:
Server: 192.168.1.11
Address 1: 192.168.1.11

Name: vbond.lab.sdwan
Address 1: 192.168.2.1 vbond.lab.sdwan
Address 2: 192.168.2.2 vbond.lab.sdwan
```

Conseil : Vous pouvez analyser les journaux du fichier vDebug à partir de admin-tech si la résolution vBond échoue.

Configuration des contrôleurs

La configuration est identique à celle des périphériques vEdge. Voici un exemple du contrôleur :

```
vsmart# show running-config system vbond
system
 vbond vbond.lab.sdwan
!
vsmart# show running-config vpn 0 dns
vpn 0
 dns 192.168.1.11 primary
!
vsmart# show running-config vpn 0 host
vpn 0
 host vbond.lab.sdwan ip 192.168.2.1 192.168.2.2
!
vsmart#
```

Configuration du routeur de périphérie Cisco

Voici la configuration du routeur de périphérie Cisco :

```
cedge#show sdwan run system | include vbond
vbond vbond-list
cedge#
cedge#show sdwan run | include host
ip host vbond-list 192.168.2.1 192.168.2.2
cedge#
```

Exécutez ICMP à des fins de validation :

```
cedge#ping vbond-list
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.149, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 27/29/31 ms
cedge#
```

Configuration supplémentaire

Définissez les serveurs DNS principal et secondaire comme méthode de redondance. Dans ce cas, un serveur tombe en panne et l'autre forme une résolution DNS.

L'exemple suivant s'applique à vEdge, Manager et Controller :

```
VM# show running-config vpn 0 dns
vpn 0
 dns 192.168.1.11 secondary
 dns 192.168.1.12 primary
!
```

L'exemple suivant s'applique à cEdge :

```
cedge#show run | i name
ip name-server 192.168.30.32 192.168.48.89
cedge#
```

Problèmes de configuration courants

- Adresses IP d'authentificateur incorrectes.
- Résolution de noms incohérente entre les contrôleurs et les routeurs de périphérie WAN.
- Utilisez la même adresse IP dans l'authentificateur. Chaque authentificateur doit avoir sa propre adresse IP configurée en tant que commande locale vBond.
- Vous pouvez disposer de plusieurs interfaces WAN, telles que Gigabitethernet1 et Gigabitethernet2. Toutefois, le serveur DNS n'est accessible que via Gigabitethernet1, ce qui entraîne l'échec de la connexion de contrôle.

Informations connexes

- Entrée hôte pour la version SD-WAN version 20.15
- Collecter Admin-Tech
- 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.