Configurer les paramètres de base pour les connexions de contrôle de formulaire sur cEdge

Contenu

Introduction

Ce document décrit la configuration de base et l'ordre d'engagement correct pour intégrer un cEdge à une superposition de réseau étendu défini par logiciel (SD-WAN).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- SD-WAN Cisco
- Interface de ligne de commande (CLI) de base Cisco IOS® XE

Components Used

Ce document est basé sur les versions logicielles et matérielles suivantes :

- cEdge version 17.6.3
- vManage version 20.6.3

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.

> **Note**: Ce guide suppose que pour les routeurs physiques, le numéro de série cEdge figure déjà dans le portail Cisco Network Plug & Play (PnP) et est synchronisé avec la liste des

périphériques vManage ; et pour les arêtes virtuelles, qu'une instance virtuelle est ajoutée au portail Plug and Play et synchronisée avec vManage.

Vérification du mode

Étape 1 : vérification que le routeur est en mode géré par le contrôleur

```
show platform software device-mode
show version | in mode
```

Exemple :

```
Router# show platform software device-mode
Device Operating-mode: Controller-Managed
Device-mode bootup status:
8/03 00:44:16 System is green
Bootup Success

Router# show version | in mode
Router operating mode: Controller-Managed
```

> **Note**: Si le résultat du mode de fonctionnement est Autonome, déplacez le routeur vers Controller-Managed avec **controller-mode enable** erasecat4000_flash:.

Étape 2 : réinitialisation du logiciel

Pour un nouveau périphérique embarqué, il est recommandé de nettoyer le périphérique avec une réinitialisation logicielle, ce qui garantit que toutes les configurations précédentes de la base de données de configuration (CBD) sont supprimées.

```
Router# request platform software sdwan software reset
```

Le périphérique se recharge et démarre avec une configuration vide.

Étape 3. Arrêtez le processus de détection PNP.

Si aucune mise en service automatique (ZTP) n'est requise, arrêtez le processus de détection PNP.

```
Router# pnpa service discovery stop
```

> **Note**: Le processus PNP s'arrête dans 5 à 10 minutes.

Configuration

Deux scénarios sont abordés :

- Interfaces physiques
- Sous-interfaces

Les deux scénarios nécessitent un tunnel IOS XE et un tunnel SD-WAN associé à une interface pour fonctionner et une configuration système SD-WAN de base.

Configuration d'interface physique

La configuration de l'interface et du tunnel pour le VPN 0 ou le VRF global nécessite un ordre spécifique, sinon, il y a des erreurs dans les associations d'interface de tunnel.

Ordre de configuration :

1. Interface physique
2. Route par défaut
3. Valider les modifications
4. Tunnel XE avec une interface physique comme source
5. Tunnel SDWAN XE
6. Valider les modifications

Exemple :

```
!IOS-XE Portion
!
config-transaction
interface GigabitEthernet0/0/0
ip address 192.168.10.2 255.255.255.0
negotiation auto
no shutdown
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
commit    <<<<<<<<<< Commit changes here
!
interface Tunnel0
no shutdown
ip unnumbered GigabitEthernet0/0/0
tunnel source GigabitEthernet0/0/0
tunnel mode sdwan
exit
!
! SD-WAN portion
!
sdwan
interface GigabitEthernet0/0/0
tunnel-interface
encapsulation ipsec
color default
allow-service all
!
commit    <<<<<<<<<< Commit changes here
!
end
```

Si les modifications sont validées dans un ordre différent, une erreur peut se produire car l'interface du tunnel IOS XE n'est pas associée à l'interface du tunnel SDWAN.

```
cEdge(config-if)# commit
Aborted: 'interface Tunnel 0 ios-tun:tunnel': Tunnel interface doesn't have corresponding sdwan
GigabitEthernet0/0/0 interface
```

Dans la direction opposée, si un tunnel SDWAN est tenté d'être supprimé sans le tunnel IOS XE simultanément, il peut entraîner une erreur de référence.

```
cEdge(config)# commit
Aborted: 'sdwan interface GigabitEthernet0/0/0 tunnel-interface' : No Tunnel interface found
with tunnel source set to SDWAN interface
```

Configuration de sous-interface

L'interface physique, la sous-interface et la configuration de tunnel pour VPN 0 ou VRF global nécessitent un ordre spécifique, sinon, il y a des erreurs dans les associations d'interface de tunnel.

Ordre de configuration :

1. Interface physique
2. Sous-Interface
3. Route par défaut
4. Valider les modifications
5. Tunnel XE avec une sous-interface comme source
6. Tunnel SDWAN XE
7. Valider les modifications

Exemple :

```
!IOS-XE Portion
!
config-transaction
interface GigabitEthernet0/0/0
no shutdown
no ip address
ip mtu 1500
mtu 1500
!
interface GigabitEthernet0/0/0.100
no shutdown
encapsulation dot1Q 100
ip address 192.168.10.2 255.255.255.0
ip mtu 1496
mtu 1496
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
commit      <<<<<<<<<< Commit changes here
!
interface Tunnel0
no shutdown
ip unnumbered GigabitEthernet0/0/0.100
tunnel source GigabitEthernet0/0/0.100
tunnel mode sdwan
exit
!
! SD-WAN portion
!
sdwan
interface GigabitEthernet0/0/0.100
tunnel-interface
```

```
encapsulation ipsec
color default
allow-service all
!
commit      <<<<<<<<<< Commit changes here
!
end
```

> **Note**: Pour prendre en charge le champ de 32 bits ajouté aux paquets par le protocole 802.1Q, le MTU des sous-interfaces doit être inférieur d'au moins 4 octets au MTU de l'interface physique. Il est configuré avec le **mtu** erasecat4000_flash:. La MTU par défaut sur une interface physique est de 1 500 octets, par conséquent la MTU de la sous-interface ne doit pas être supérieure à 1 496 octets. En outre, si la sous-interface nécessite une MTU de 1 500 octets, la MTU de l'interface physique peut être ajustée à 1 504 octets.

Si les modifications sont validées dans un ordre différent, une erreur peut se produire car l'interface du tunnel IOS XE n'est pas associée à l'interface du tunnel SDWAN.

```
cEdge(config)# commit
Aborted: 'sdwan interface GigabitEthernet0/0/0.100 tunnel-interface' : No Tunnel interface found
with tunnel source set to SDWAN interface
```

Configuration système

Pour joindre le fabric SD-WAN, le serveur cEdge a besoin d'informations de superposition de base sous le système afin de pouvoir démarrer l'authentification avec vBond.

1. Adresse IP du système **:** Identificateur unique du serveur cEdge, il est fourni au format octal à points. Il ne s'agit pas d'une adresse IP routable.
2. ID du site : Identificateur unique du site.
3. Nom de l'entreprise : Identificateur unique de la superposition SD-WAN.
4. IP et port vBond : IP et port vBond. Il peut être obtenu à partir du vBond lui-même avec **show sdwan running-config system** erasecat4000_flash:.

Exemple :

```
config-transaction
system
system-ip 10.10.10.1
site-id 10
organization-name SDWAN-OVERLAY
vbond 172.16.120.20 port 12346
!
commit
```

Juste après la validation de la configuration du système, le serveur cEdge contacte le serveur vBond pour l'authentification et commence à établir des connexions de contrôle vers vManage et vSmarts.

Activation des routeurs CSR1000V et C8000V

Les routeurs virtuels cEdge nécessitent une étape supplémentaire pour associer un châssis et un jeton, car ils ne sont pas du matériel réel et l'UUDI (Universal Unique Device Identifier) est virtuel.

Dans l'interface graphique utilisateur vManage, accédez à : **Configuration > Devices** et recherchez une entrée CSR1000v ou C8000v disponible :

Exécutez l'activation et remplacez les numéros de châssis et de série dans la commande.

```
request platform software sdwan vedge_cloud activate chassis-number CHASSIS_NUMBER token
TOKEN_ID
```

Exemple :

```
Router# request platform software sdwan vedge_cloud activate chassis-number 7AD5C8CE-301E-4DA8-
A74E-90A316XXXXXX token 23ffdf400cb14e489332a74b8fXXXXXX
```

Vérification des connexions de contrôle

Vérifiez l'état des connexions de contrôle à l'aide des commandes de vérification.

```
show sdwan control connections
show sdwan control connection-history
```

Informations connexes

- Support et documentation techniques - Cisco Systems
- Dépannage des connexions de contrôle SD-WAN

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.