Remplacer un routeur RMA cEdge

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

- Étape 1. Mise à niveau du périphérique de rechange ou RMA vers une image compatible SDWAN avec les contrôleurs
- Étape 2 : utilisation de la configuration de base pour que le serveur Edge atteigne les serveurs vBond, vManage et vSmart
- Étape 3. Copie et installation du certificat CA racine dans le serveur Edge de rechange ou RMA
- Étape 4. Synchronisation/téléchargement de la liste des périphériques sous vManage

Processus de remplacement si l'arête utilise un modèle

- Étape 1. Sauvegarde des valeurs actuelles utilisées sous le modèle de périphérique
- Étape 2. Suppression du périphérique défaillant du modèle de périphérique joint
- Étape 3. Invalidation de l'ancien routeur/routeur défaillant
- Étape 4. Envoyer aux contrôleurs
- Étape 5. Enfoncement du modèle dans un routeur de rechange ou RMA

Processus de remplacement si le serveur cEdge est configuré via l'interface CLI

- Étape 1. Sauvegarde de la configuration actuelle
- Étape 2. Invalidation de l'ancien routeur/routeur défaillant
- Étape 3. Envoyer aux contrôleurs
- Étape 4. Placement de la configuration dans le routeur

Informations connexes

Introduction

Ce document décrit comment remplacer une unité cEdge défaillante par une autre.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- 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 :

- cEdge version 17.3.3
- vManage version 20.4.2

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.

Informations générales

Ce processus consiste à utiliser une copie de la configuration du routeur défaillant vers le routeur de remplacement, à supprimer ce cEdge et à ajouter le nouveau routeur au réseau. Ce processus est similaire au remplacement vEdge, mais l'option de copie n'est pas disponible dans vManage for Edge.

Généralement, le remplacement d'une unité cEdge défaillante par une nouvelle est effectué lorsqu'un routeur RMA est reçu en raison d'une défaillance complète de l'ancien routeur cEdge ou d'une défaillance d'un composant du routeur, et le TAC Cisco doit procéder à une RMA.

Avant de remplacer le serveur cEdge, vérifiez certains points afin que le nouveau routeur cEdge établisse correctement des connexions de contrôle.

Étape 1. Mise à niveau du périphérique de rechange ou RMA vers une image compatible SDWAN avec les contrôleurs

Remarque : Assurez-vous que la version actuelle de cEdge est compatible avec les versions du contrôleur. Référez-vous à Matrice de compatibilité.

Remarque : Pour plus d'informations sur le processus de mise à niveau de cEdge via l'interface de ligne de commande, veuillez vous reporter à Installation et mise à niveau du logiciel pour les routeurs Cisco IOS XE.

Étape 2 : utilisation de la configuration de base pour que le serveur Edge atteigne les serveurs vBond, vManage et vSmart

Vérifiez que le serveur cEdge en question a été configuré correctement. Il comprend :

- Certificat valide installé.
- Configurez sous le bloc système :

```
System-IP
Site-ID
Organization-Name
vBond address
```

- Interface de transport VPN 0 configurée avec l'option de tunnel et l'adresse IP.
- Horloge système configurée correctement sur le serveur cEdge et celles qui correspondent aux autres périphériques/contrôleurs.

La commande show clock confirme l'heure actuelle et utilise clock set pour définir l'heure correcte sur le périphérique.

```
show clock
clock set
```

- Assurez-vous que cEdge atteint le vBond. Si un nom de domaine fréquemment qualifié (FQDN) est utilisé pour le vBond, assurez-vous que DNS est configuré sous VPN 0 et qu'il résout le vBond.

⚠ Mise en garde : Pour le nouveau serveur cEdge, utilisez une adresse IP système différente de celle présente dans le routeur d'origine/défaillant. Dans les dernières étapes, l'adresse IP du système est modifiée de la même manière que l'adresse cEdge d'origine.

Étape 3. Copier et installer le certificat CA racine dans le serveur de secours ou RMA Edge

L'autorité de certification racine est saisie par l'interface de ligne de commande de tout contrôleur comme vBond, vSmart ou vManage. Localisez le certificat dans le vshell.

Exemple de vBond :

```
vshell
cd /usr/share/viptela
```

Affichez le contenu du certificat et copiez tout le contenu.

```
ls -l root*
cat root-ca.crt
```

Afin de copier le certificat dans la mémoire flash de démarrage du serveur cEdge, utilisez FTP, SFTP ou un lecteur USB. Si cela n'est pas possible, copiez le certificat manuellement en dernier recours.

Créez le fichier pour la nouvelle autorité de certification racine dans le cEdge RMA.

⚠ Mise en garde : Les lignes de commande contiennent des commentaires qui commencent par « ! ». Supprimez tous les commentaires.

```
tclsh !Hit enter
puts [open "bootflash:root-ca-new.cert" w+] { !Hit enter
!Paste-all-the-previous-content-from-vBond-or-vManage-certificaet-WITHOUT-spaces
}!Hit enter
exit
```

Dans les versions plus récentes de Cisco IOS® XE SD-WAN, la commande tclsh est désactivée par défaut. Afin de l'activer temporairement, la commande service internal est nécessaire.

```
config-t
(config)# service internal
(config)# commit
(config)# end
debug platform software sdwan unlock-ios-cl
```

Désinstallez l'ancienne autorité de certification racine et installez l'autorité de certification racine qui vient d'être ajoutée.

```
request platform software sdwan root-cert-chain uninstall
request platform software sdwan root-cert-chain install bootflash:<RootCAFile>
```

Cochez la case show control connections afin de valider que le périphérique a établi de nouveau des connexions avec les contrôleurs.

Étape 4. Synchronisation/téléchargement de la liste des périphériques sous vManage

Le routeur RMA doit être affiché sous « vManage > Devices ». Si le périphérique n'est pas sous vManage, assurez-vous qu'il est ajouté au portail PnP.

À ce stade, le serveur cEdge dispose de connexions de contrôle jusqu'aux contrôleurs.

Processus de remplacement si l'arête utilise un modèle

Étape 1. Sauvegarde des valeurs actuelles utilisées sous le modèle de périphérique

Sauvegardez les valeurs actuelles utilisées pour le périphérique sous le modèle. Accédez à

vManage > Device Template > Template > ... > Export CSV.

Étape 2. Suppression du périphérique défaillant du modèle de périphérique joint

Sauvegardez d'abord les valeurs des variables.

Remarque : Après la suppression du modèle de périphérique, toutes les valeurs variables du modèle sont perdues. La seule façon de les récupérer est de vérifier la configuration de l'unité défaillante ou d'origine. En outre, il n'est pas possible de détacher un modèle de périphérique si le routeur de périphérie WAN est dans un état inaccessible. Le message « Veuillez corriger la connectivité DTLS, NETCONF entre le périphérique et vManage avant le workflow de tentative de modèle » est présenté dans l'interface graphique utilisateur de vManage. Dans ce cas, veuillez d'abord invalider le périphérique (Configuration> Certificat), puis procéder au détachement du modèle.

Retirez le périphérique de tout modèle de périphérique connecté.

Étape 3. Invalidation de l’ancien routeur/routeur défaillant

Invalidez le routeur défaillant sous vManage > Certificates > Devices.

Remarque : Toutes les connexions de contrôle sont perdues au cours de ces étapes.

Étape 4. Envoyer aux contrôleurs

Sélectionnez Send to controllers afin de pousser les modifications aux contrôleurs.

Mise en garde : Si les informations du routeur invalidé ne sont plus nécessaires et que la même adresse IP système doit être réutilisée sur le routeur RMA, supprimez le routeur invalidé de vManage.

Étape 5. Enfoncement du modèle dans un routeur de rechange ou RMA

Enfoncez le modèle dans un routeur de rechange ou RMA.

Remarque : Utilisez le fichier CSV de l'étape 1 pour renseigner toutes les valeurs requises lorsque le modèle de périphérique est joint.

Processus de remplacement si le serveur cEdge est configuré via l'interface CLI

Étape 1. Sauvegarde de la configuration actuelle

Sauvegardez la configuration actuelle. Accédez à vManage > Device > ... > Running Config.

Si le périphérique est hors ligne, essayez de sélectionner la configuration locale, afin de vérifier s'il y a une sauvegarde de la configuration du périphérique.

Si une configuration est enregistrée dans vManage, extrayez-la du périphérique lui-même.

Utilisez ces commandes sous CLI pour créer un fichier dans Bootflash avec toutes les configurations actuelles :

```
show running-config | redirect bootflash:sdwan/ios.cli
show sdwan running-config | redirect bootflash:sdwan/sdwan.cli
```

Étape 2. Invalidation de l’ancien routeur/routeur défaillant

Invalider l'ancien routeur/le routeur défaillant dans vManage > Certificates > Devices.

Remarque : Une fois le périphérique invalidé, la configuration est perdue. Il n'existe aucun moyen de récupérer la configuration à partir de vManage. La configuration est toujours disponible sur le périphérique défaillant ou d'origine.

Remarque : Toutes les connexions de contrôle sont perdues au cours de ces étapes.

Mise en garde : Si les informations du routeur invalidé ne sont plus nécessaires et que la même adresse IP système doit être réutilisée sur le routeur RMA, supprimez le routeur invalidé de vManage.

Étape 3. Envoyer aux contrôleurs

Sélectionnez Send to controllers afin de pousser les modifications aux contrôleurs.

Étape 4. Placement de la configuration dans le routeur

Placez toutes les configurations dans le routeur. À ce stade, il est possible de modifier l'adresse IP du système pour utiliser l'adresse IP du système à partir du routeur défaillant ou d'origine.

Informations connexes

- Remplacer un routeur vEdge
- 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.