Configuration et vérification de DIA NAT Tracker et Fallback

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
  - Restrictions pour NAT DIA Tracker
    - Restrictions pour Cisco IOS XE Catalyst SD-WAN version 17.10.1a et versions antérieures
    - Restrictions pour Cisco IOS XE Catalyst SD-WAN version 17.11.1a
    - Restrictions pour Cisco IOS XE Catalyst SD-WAN version 17.13.1a
  - Interfaces prises en charge pour NAT DIA Tracker
- Configurer
  - Diagramme du réseau
  - Configurations
  - Étape 1 : configuration de NAT DIA Tracker
  - Étape 2. Liaison du traqueur à l'interface de transport
  - Étape 3 : activation de la fonction NAT Fallback sur la stratégie DIA existante
- Vérifier
- Suivi du dépannage
- Informations connexes

Introduction

Ce document décrit comment configurer et vérifier DIA NAT Tracker et Fallback sur les routeurs Cisco IOS® XE à l'aide de l'interface graphique utilisateur de Cisco Catalyst Manager.

Conditions préalables

Exigences

La stratégie NAT DIA de Cisco SD-WAN doit être configurée sur les périphériques des filiales. Consultez la section Informations connexes pour obtenir des instructions sur la façon d'implémenter l'accès Internet direct (DIA) pour SD-WAN.

Composants utilisés

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

- Cisco Catalyst SD-WAN Manager version 20.14.1

- Contrôleur Cisco Catalyst SD-WAN version 20.14.1
- Routeur de périphérie Cisco version 17.14.01a

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.

Restrictions pour NAT DIA Tracker

Restrictions pour Cisco IOS XE Catalyst SD-WAN version 17.10.1a et versions antérieures

- Dans Cisco IOS XE version 17.6.x et antérieure, le traqueur NAT DIA n'est pas pris en charge sur les interfaces de numérotation. À partir de la version 17.7.1a de Cisco IOS XE Catalyst SD-WAN, les sous-interfaces et les interfaces de numérotation prennent en charge les traqueurs de point d'extrémité unique et double.
- Le point de terminaison URL DNS n'est pas pris en charge sur les périphériques SD-WAN Cisco IOS XE Catalyst.
- Vous ne pouvez appliquer qu'un seul suivi ou groupe de suivi à une interface.
- La fonctionnalité de secours NAT est prise en charge uniquement à partir de Cisco IOS XE Catalyst SD-WAN version 17.3.2.
- L'adresse IP du tunnel avec l'adresse 169.254.x.x n'est pas prise en charge pour suivre le point d'extrémité zScaler sur les tunnels manuels.
- Vous devez configurer au moins deux dispositifs de suivi de point de terminaison unique pour configurer un groupe de dispositifs de suivi.
- Un groupe de suivi ne peut incorporer qu'un maximum de deux traqueurs de point d'extrémité.
- Dans Cisco IOS XE version 17.10.1 et les versions précédentes, vous ne pouvez pas configurer IPv4 tracker sur une interface IPv6 ou vice versa. Le traqueur ne sera pas actif.

Restrictions pour Cisco IOS XE Catalyst SD-WAN version 17.11.1a

- Le point de terminaison URL API est pris en charge uniquement sur le traqueur DIA IPv6 et non sur le traqueur DIA IPv4.
- Les trackers IPv4 et IPv6 ne peuvent pas être utilisés dans le même groupe de trackers.
- Vous devez configurer la commande allow service all sous l'interface de tunnel TLOC pour que les trackers IPv6 fonctionnent avec une interface de tunnel TLOC.
- Plusieurs interfaces DIA NAT66 ne sont pas prises en charge.

Restrictions pour Cisco IOS XE Catalyst SD-WAN version 17.13.1a

- Le processus de résolution de nom n'est pas lié à l'interface ET. La résolution de noms utilise la table de routage VPN 0. Il peut quitter n'importe quelle interface active avec un routage approprié.

Interfaces prises en charge pour NAT DIA Tracker

Vous pouvez configurer le traqueur NAT DIA pour les interfaces suivantes :

- Interfaces cellulaires

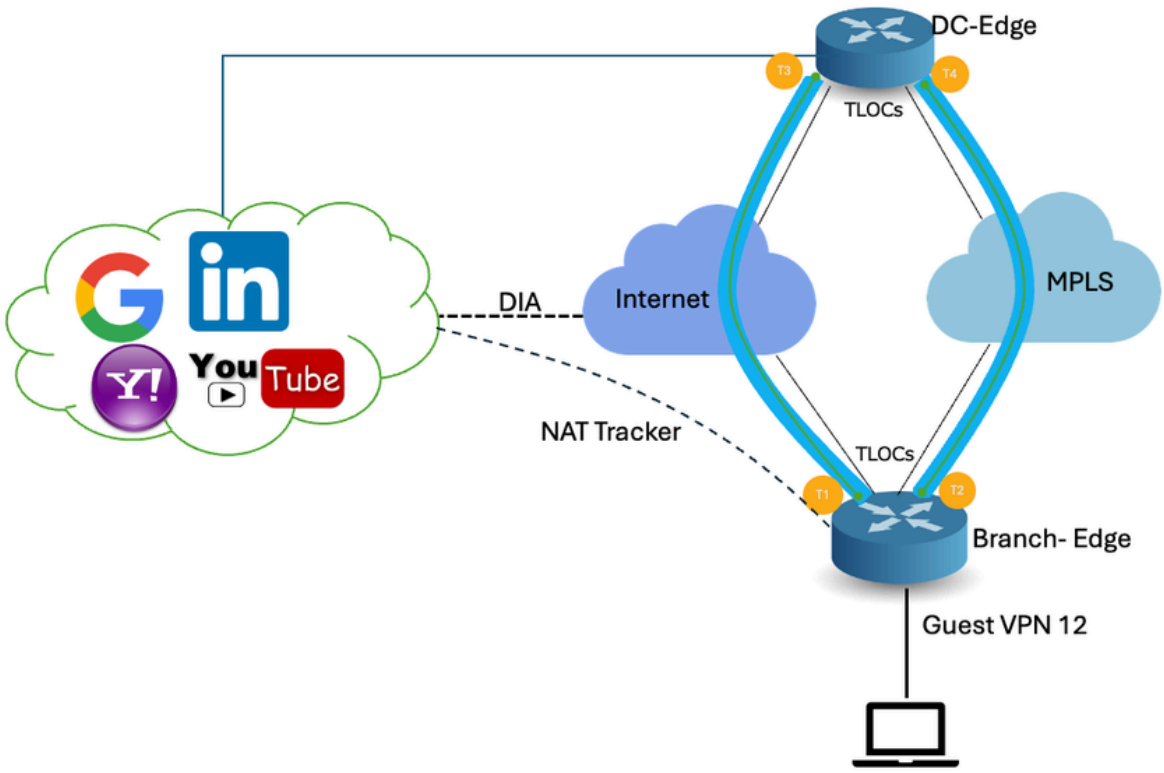
> Remarque : Les interfaces cellulaires ne prennent pas en charge les adresses IP négociées.

- Interfaces Ethernet
- Interfaces Ethernet (PPPoE)
- Sous-interfaces
- Interfaces de numérotation DSL (PPPoE et PPPoA)

> Remarque : Le traqueur DIA NAT IPv6 est pris en charge uniquement sur les interfaces physiques et les sous-interfaces des interfaces Ethernet.

Configurer

Diagramme du réseau



Configurations

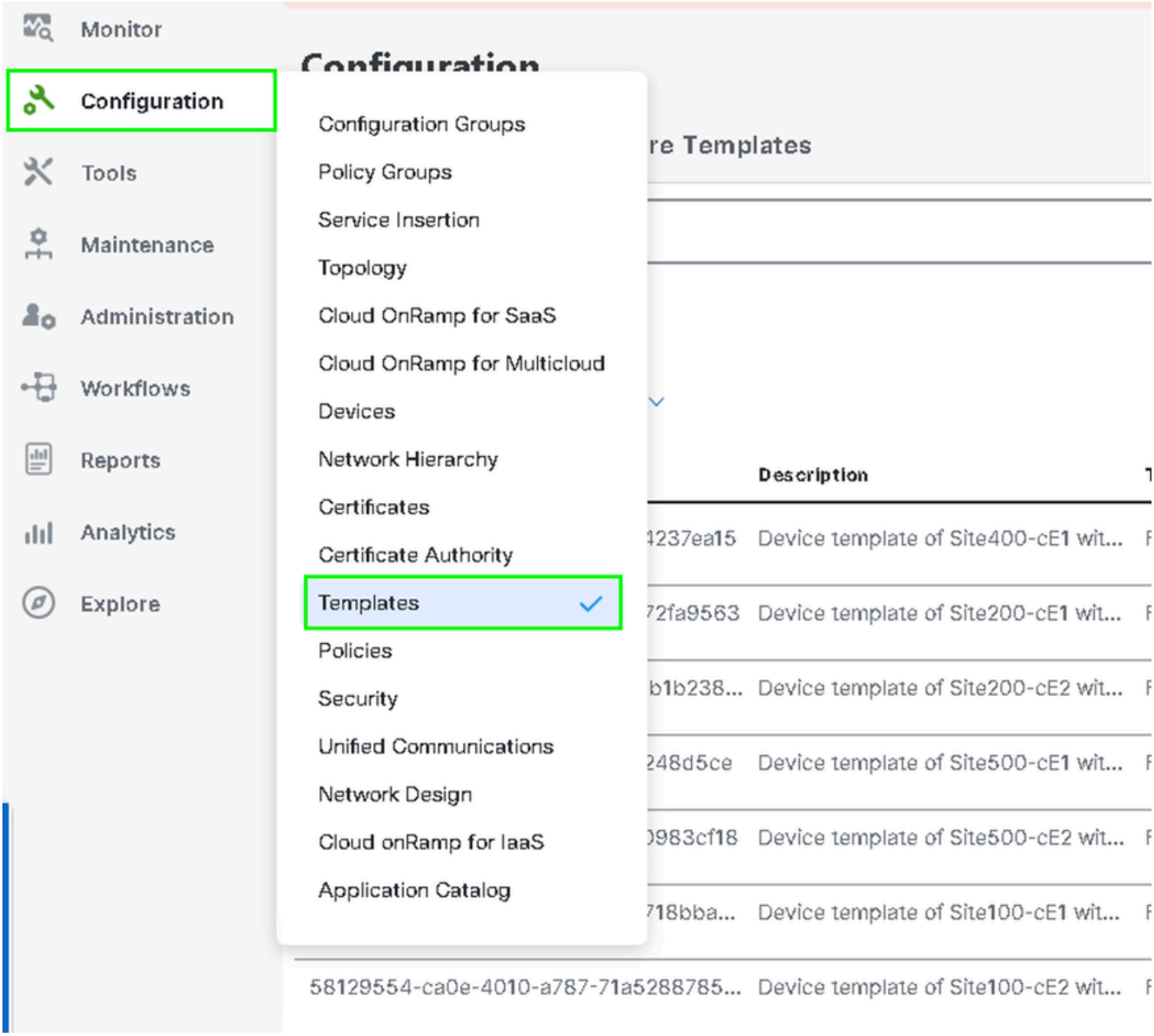
Le traqueur DIA permet de déterminer si Internet ou le réseau externe est devenu indisponible. La

fonction NAT DIA Tracking est utile lorsque la fonction NAT est activée sur une interface de transport dans VPN 0 pour permettre au trafic de données du routeur de sortir directement vers Internet.

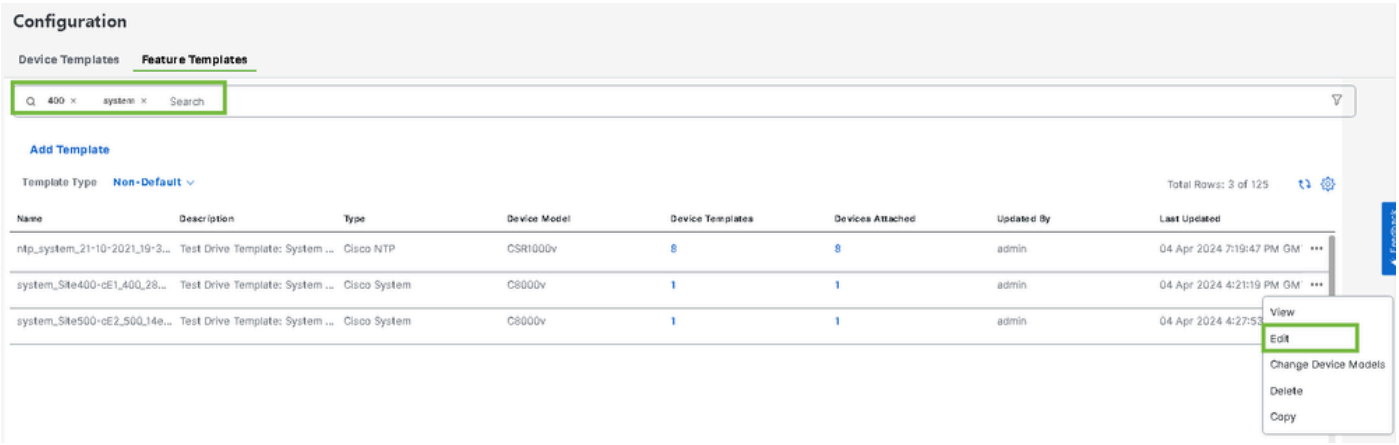
Si Internet ou le réseau externe devient indisponible, le routeur continue à transférer le trafic en fonction de la route NAT dans le VPN de service. Le trafic qui est transféré vers Internet est abandonné. Pour éviter que le trafic Internet ne soit abandonné, configurez le traqueur DIA sur le routeur de périphérie pour suivre l'état de l'interface de transport. Le dispositif de poursuite sonde périodiquement l'interface pour déterminer l'état d'Internet et renvoyer les données aux points d'attache qui sont associés au dispositif de poursuite.

Étape 1 : configuration de NAT DIA Tracker

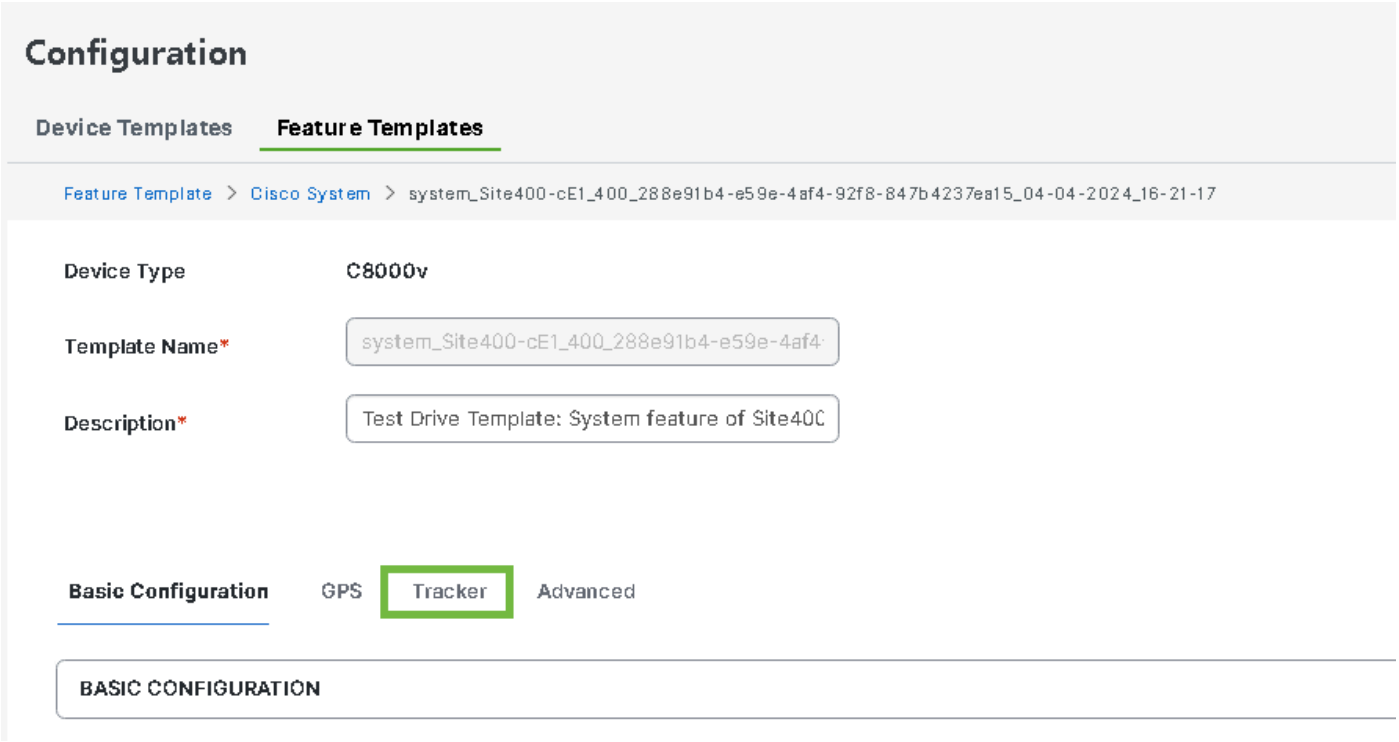
Dans le menu Cisco SD-WAN Manager, accédez à Configuration > Templates.



Cliquez sur Feature Templates. Recherchez le modèle de fonctionnalité Cisco System dans la barre de recherche, cliquez sur les trois points (...), puis cliquez sur Edit pour le modifier.



Dans le modèle de fonctionnalité Système, cliquez sur Tracker.



Cliquez sur New Endpoint Tracker pour configurer les paramètres de suivi.



Entrez les paramètres de suivi et cliquez sur Add.

Name : Nom du traqueur. Le nom peut contenir jusqu'à 128 caractères alphanumériques. Vous pouvez configurer jusqu'à huit trackers.

Seuil : Durée d'attente de la réponse de la sonde avant de déclarer que l'interface de transport est désactivée. Plage: 100 à 1000 millisecondes. Par défaut : 300 millisecondes

Intervalle : Fréquence à laquelle une sonde est envoyée pour déterminer l'état de l'interface de transport. Plage: 20 à 600 secondes. Par défaut : 60 secondes (1 minute).

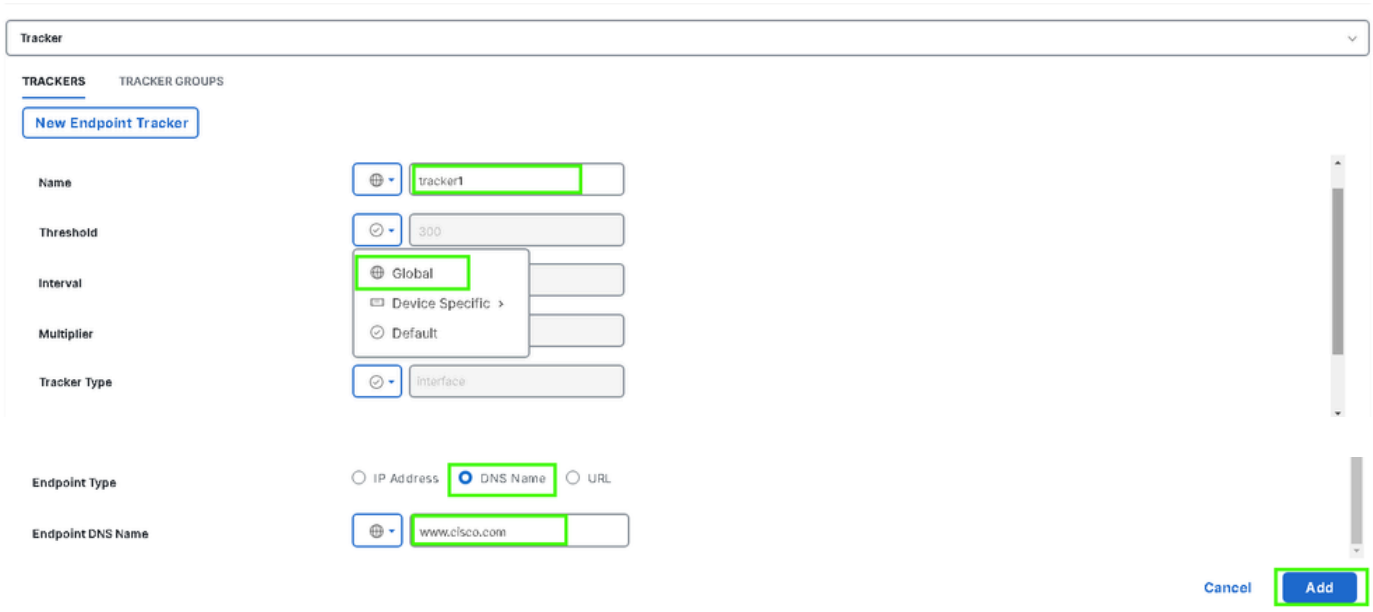
Multiplicateur : Nombre de fois qu'une sonde peut être renvoyée avant de déclarer que l'interface de transport est désactivée. Plage: 1 à 10. Valeur par défaut : 3.

Type de suivi : Choisissez Interface pour configurer le traqueur DIA.

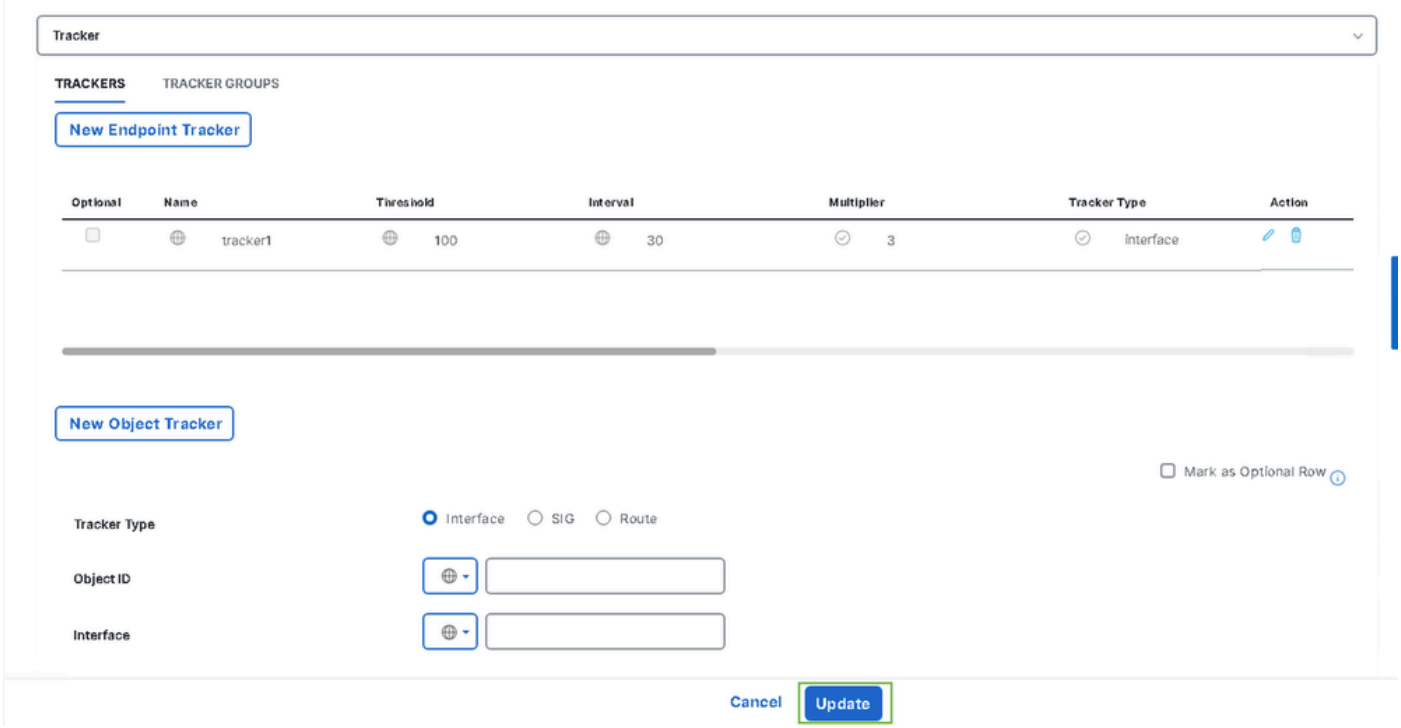
End Point Type : vous pouvez sélectionner l'adresse IP, le nom DNS ou l'URL.

Nom DNS du point de terminaison : Nom DNS du point d'extrémité. Il s'agit de la destination Internet vers laquelle le routeur envoie des sondes pour déterminer l'état de l'interface de transport.

Cliquez sur la liste déroulante et sélectionnez Global pour modifier une valeur par défaut.

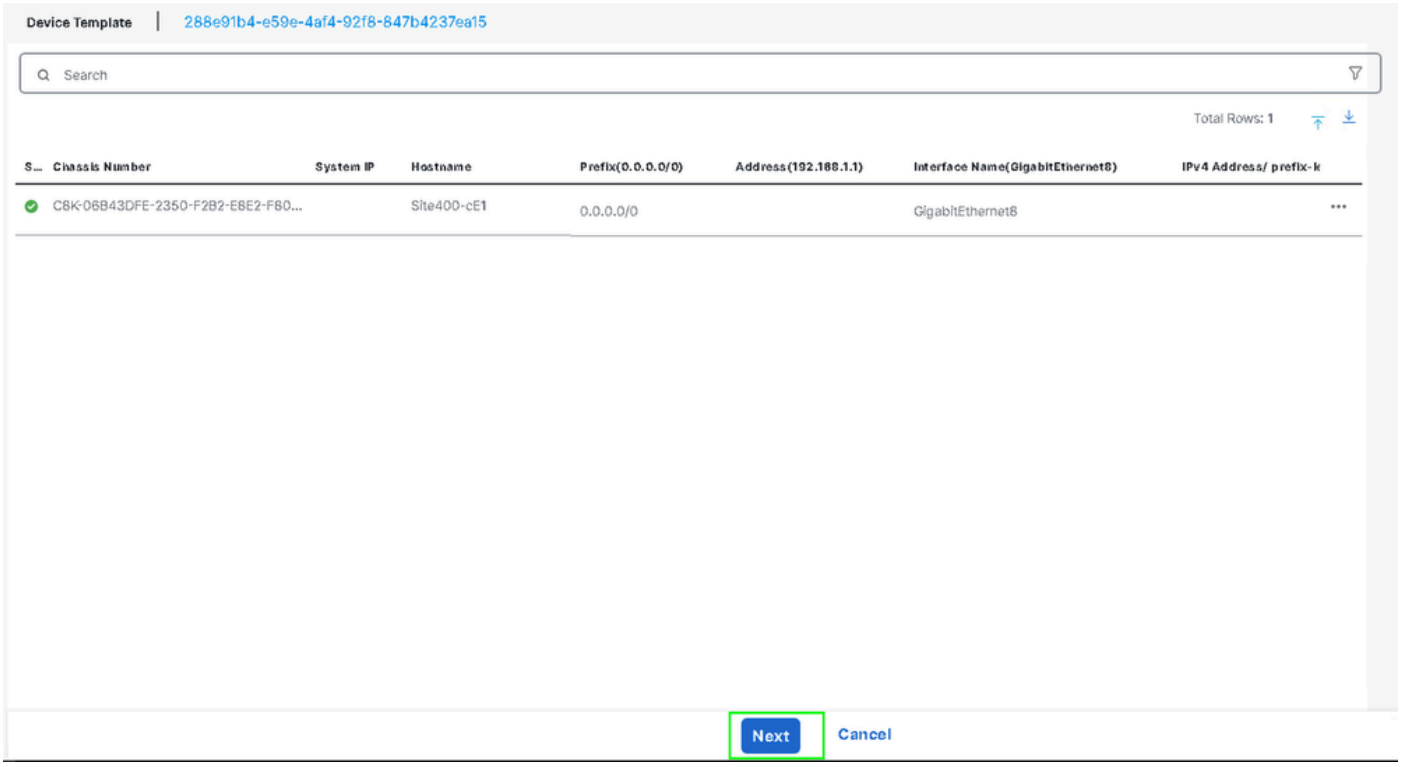


Cliquez sur Update.

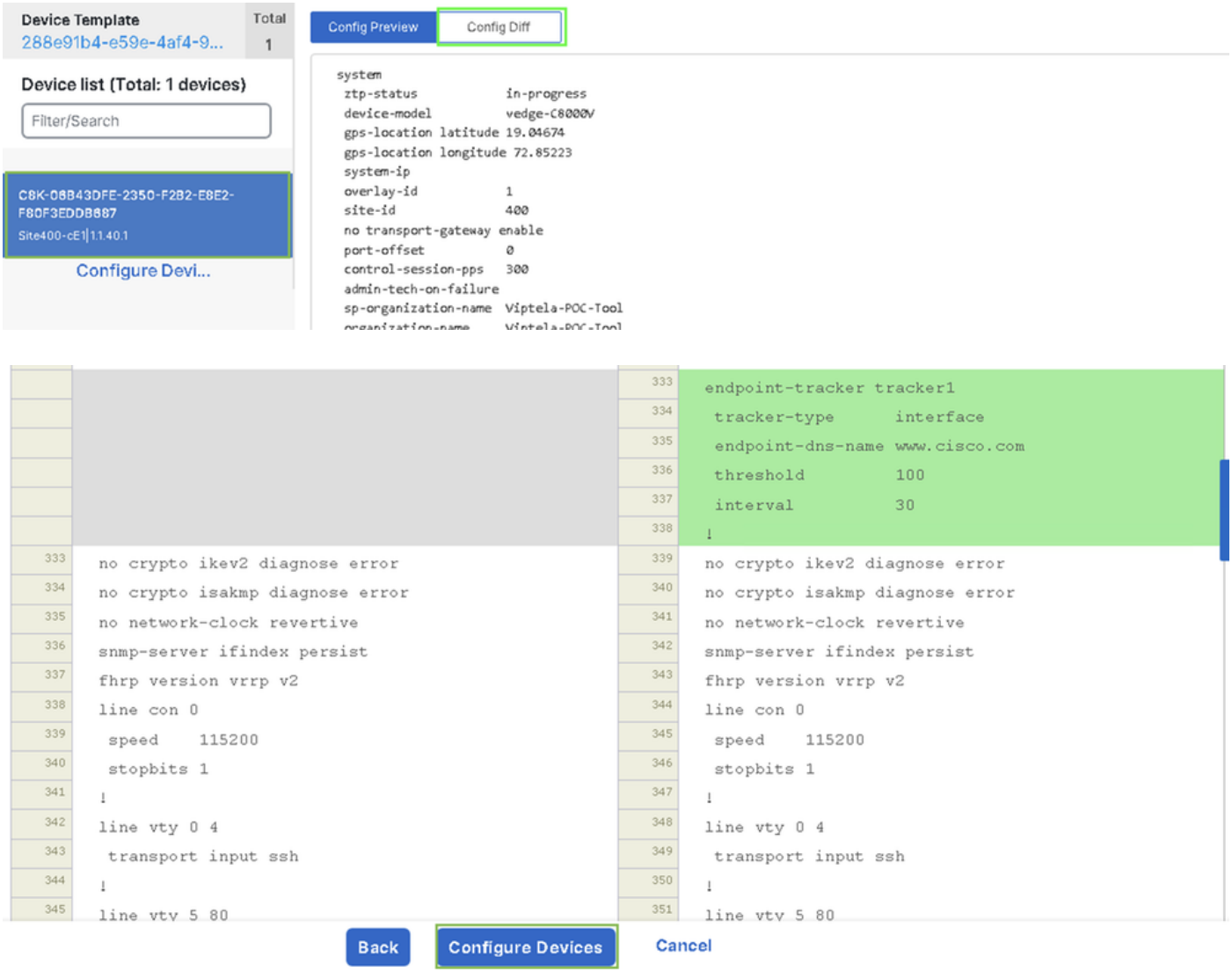


Remarque : avant de configurer un groupe de suivi, assurez-vous d'avoir configuré deux suivis de point d'extrémité uniques.

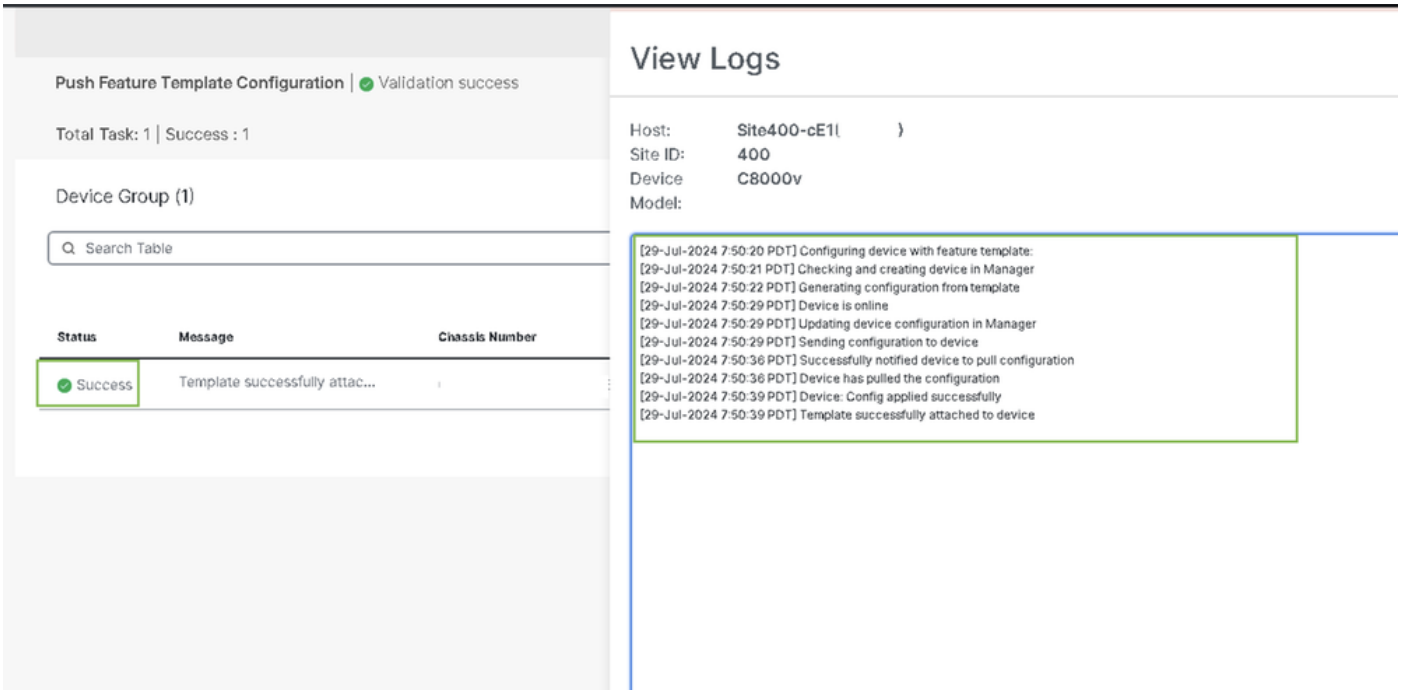
Cliquez sur Next (Suivant).



Cliquez sur devices, et vérifiez que la configuration est correcte. Cliquez sur Config Diff et sur Side by Side Diff. Cliquez sur Configurer les périphériques.

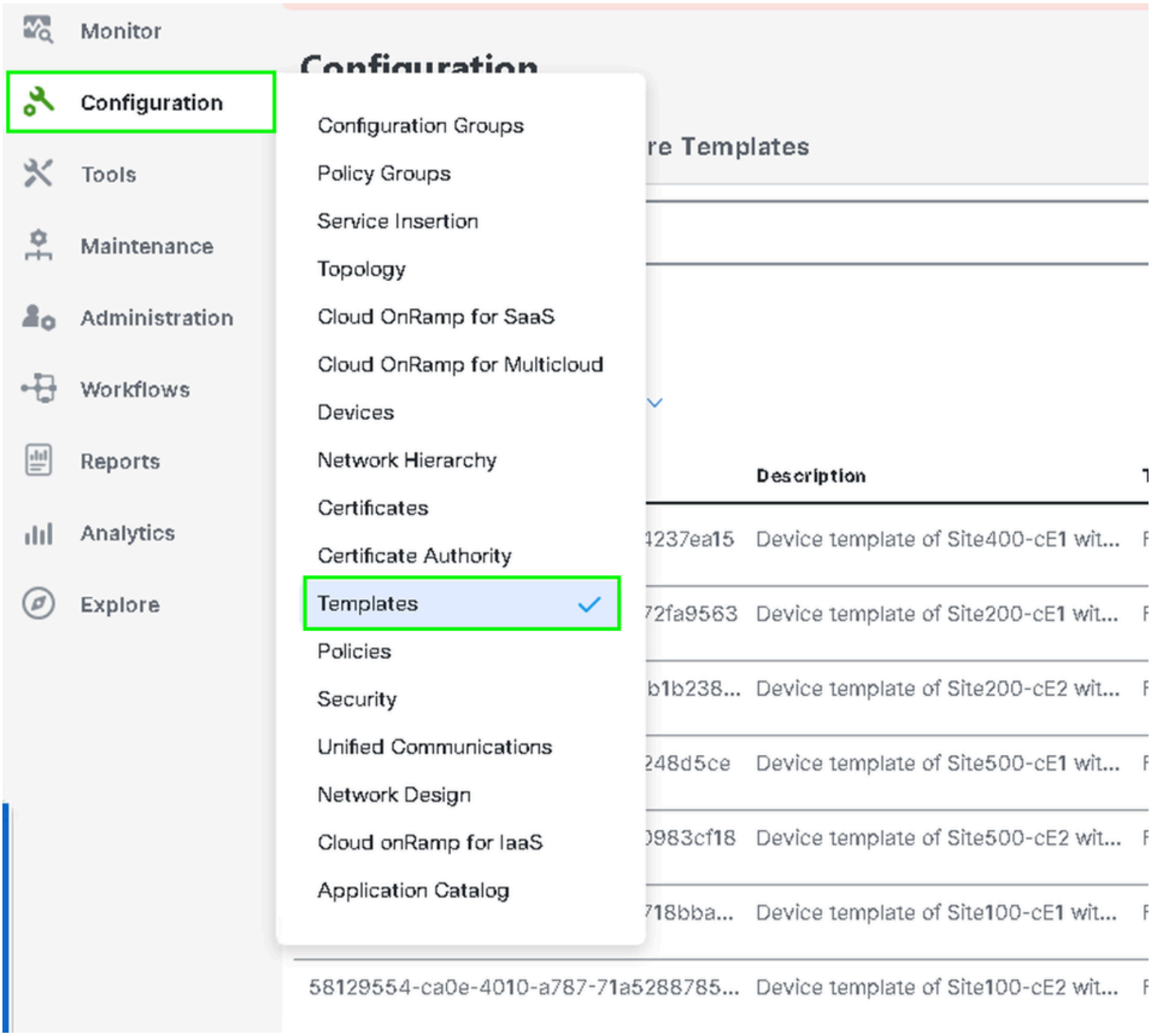


vManage a correctement configuré le modèle de périphérique avec la configuration de suivi.

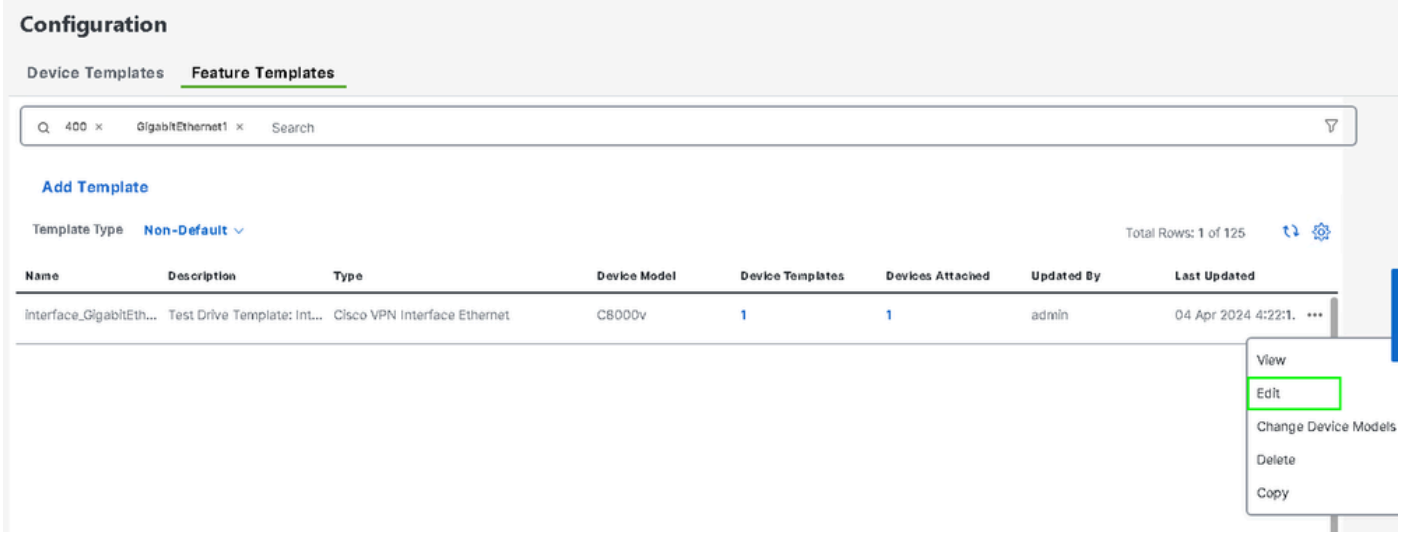


Étape 2. Liaison du traqueur à l’interface de transport

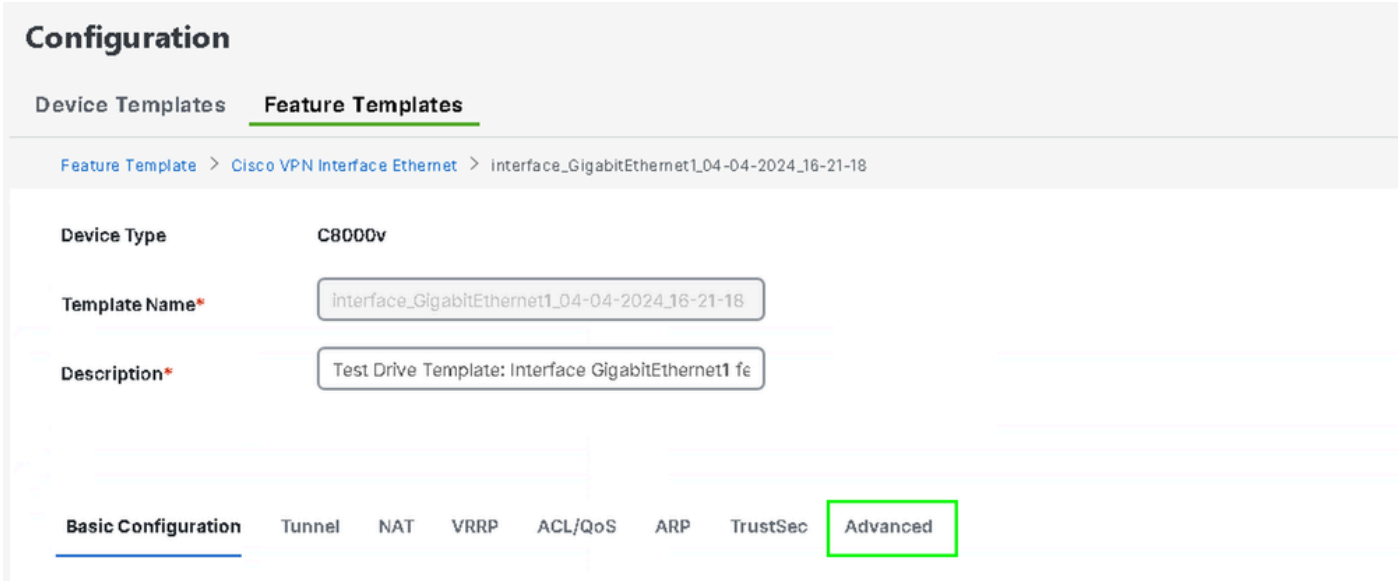
Dans le menu Cisco SD-WAN Manager, accédez à Configuration > Templates.



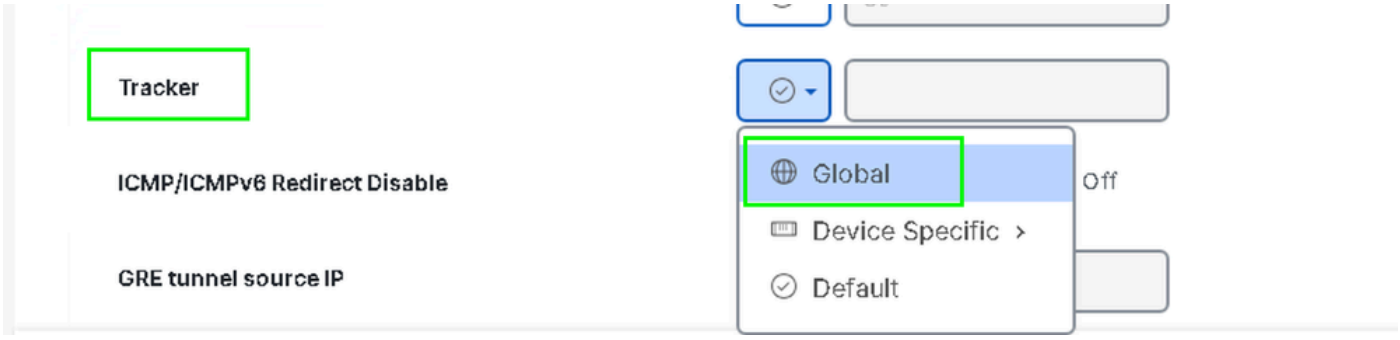
Recherchez le modèle de fonction NAT Transport Interface dans la barre de recherche, cliquez sur les trois points (...), puis cliquez sur Edit pour le modifier.



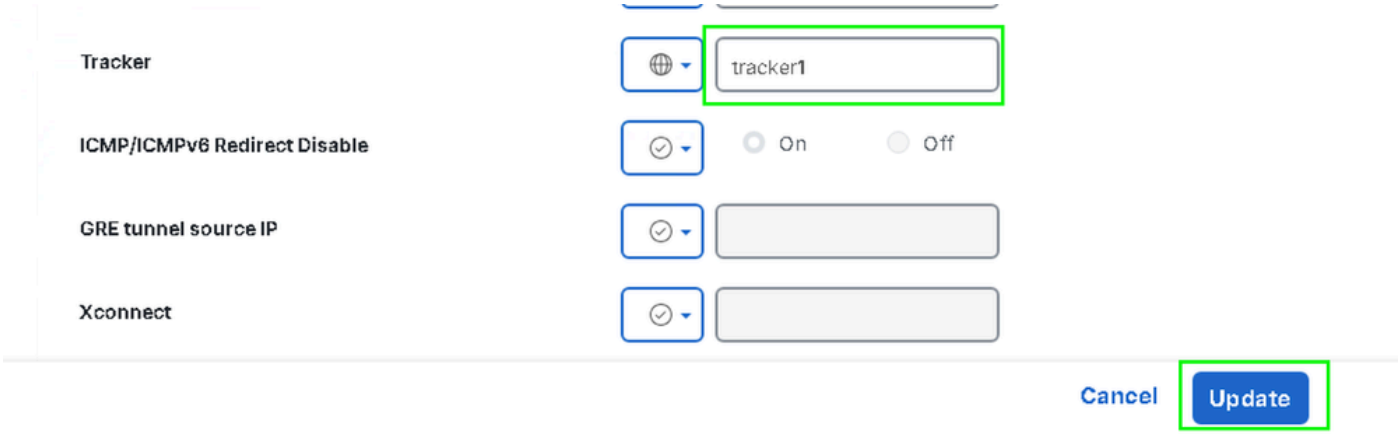
Cliquez sur l'onglet Advanced.



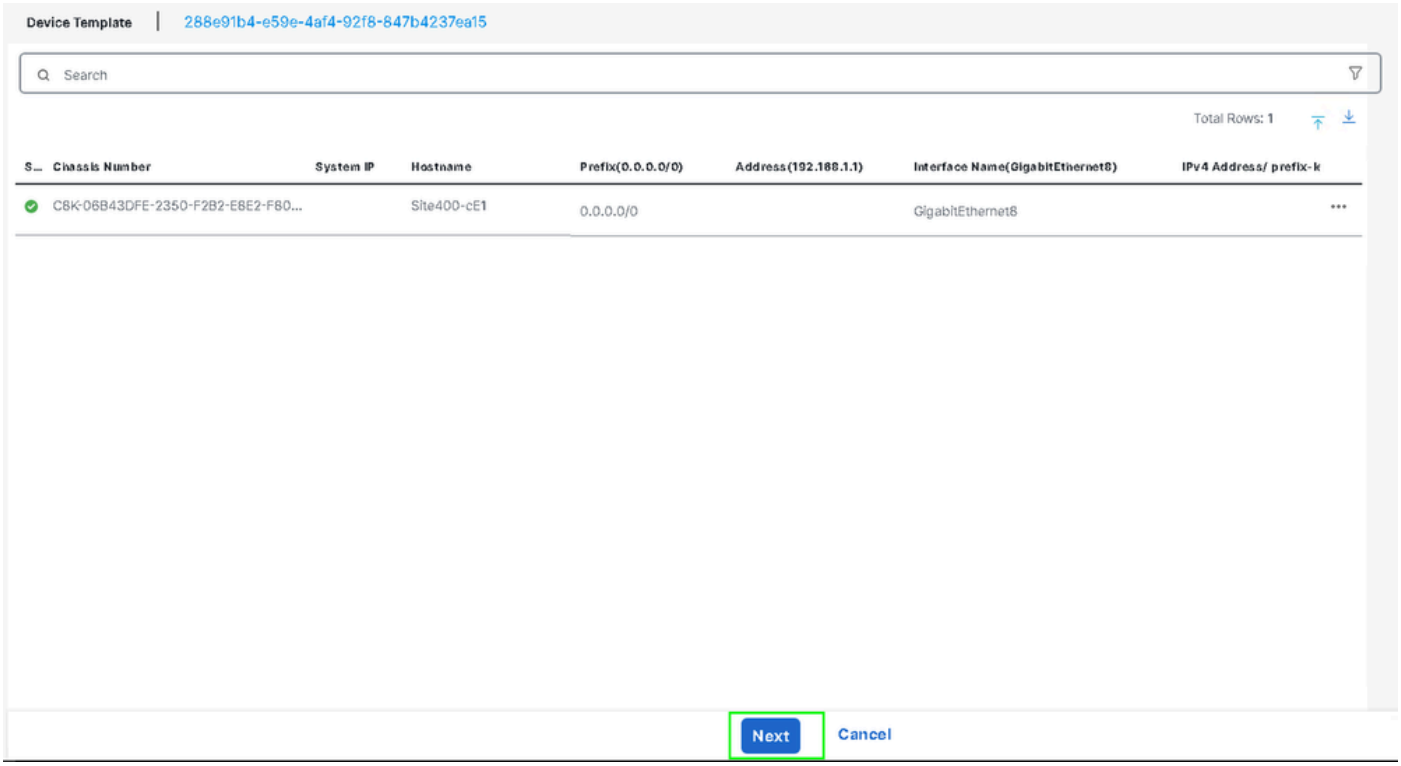
Pour ajouter le nom du traqueur dans le traqueur, sélectionnez Global dans le menu déroulant.



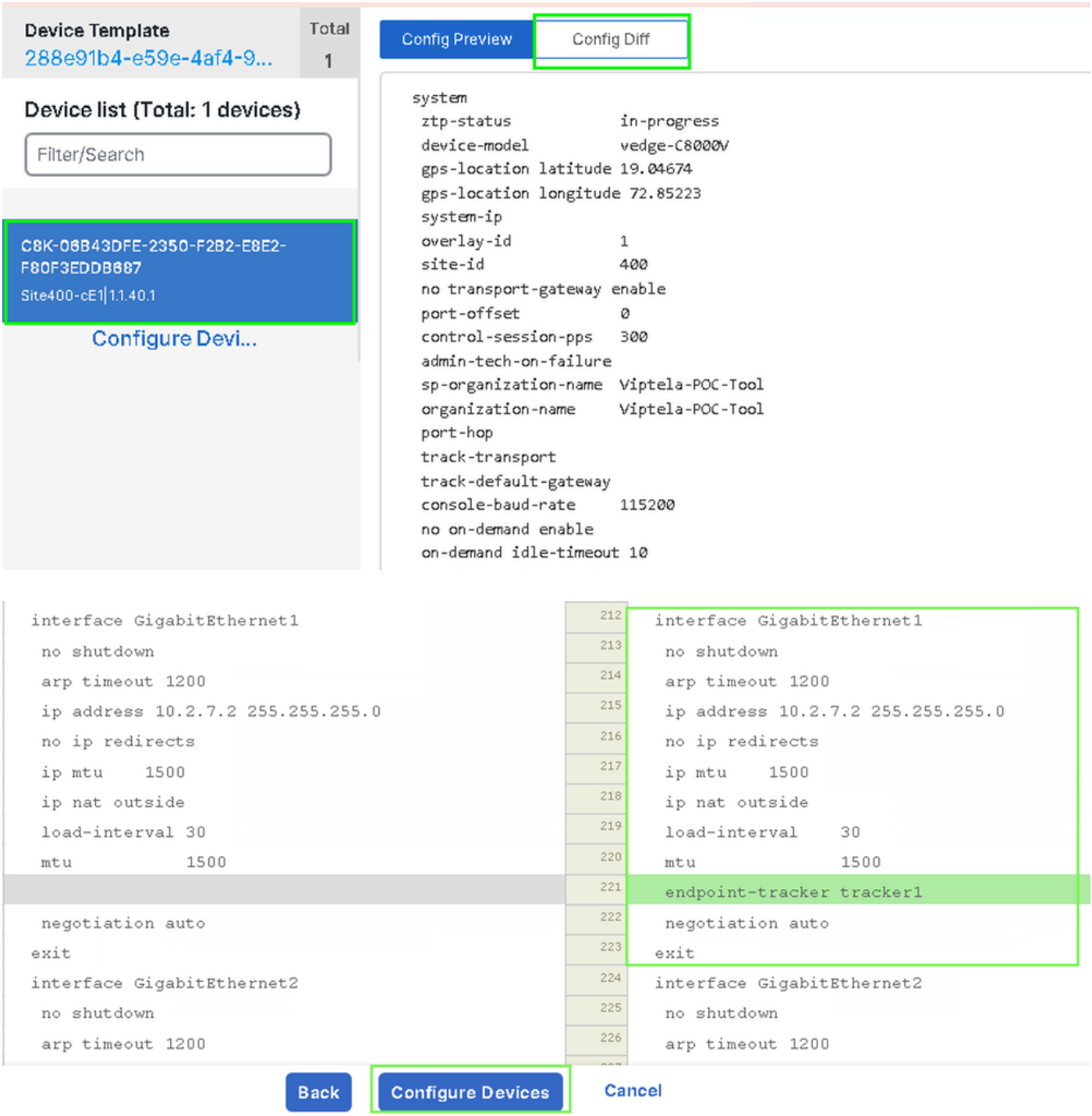
Entrez le nom du traqueur que vous avez créé dans le modèle système et cliquez sur Mettre à jour.



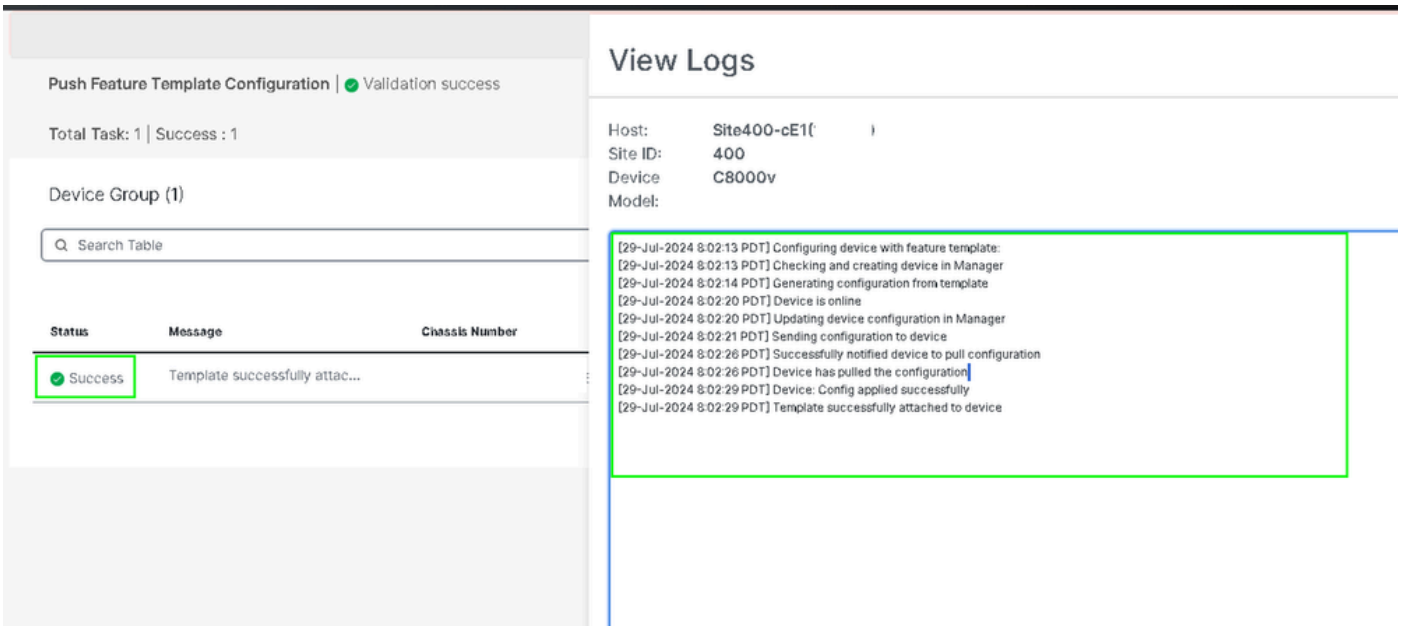
Cliquez sur Next (Suivant).



Cliquez sur devices, et vérifiez que la configuration est correcte. Cliquez sur Config Diff et sur Side by Side Diff. Cliquez sur Configurer les périphériques.



vManage a correctement configuré le modèle de périphérique.

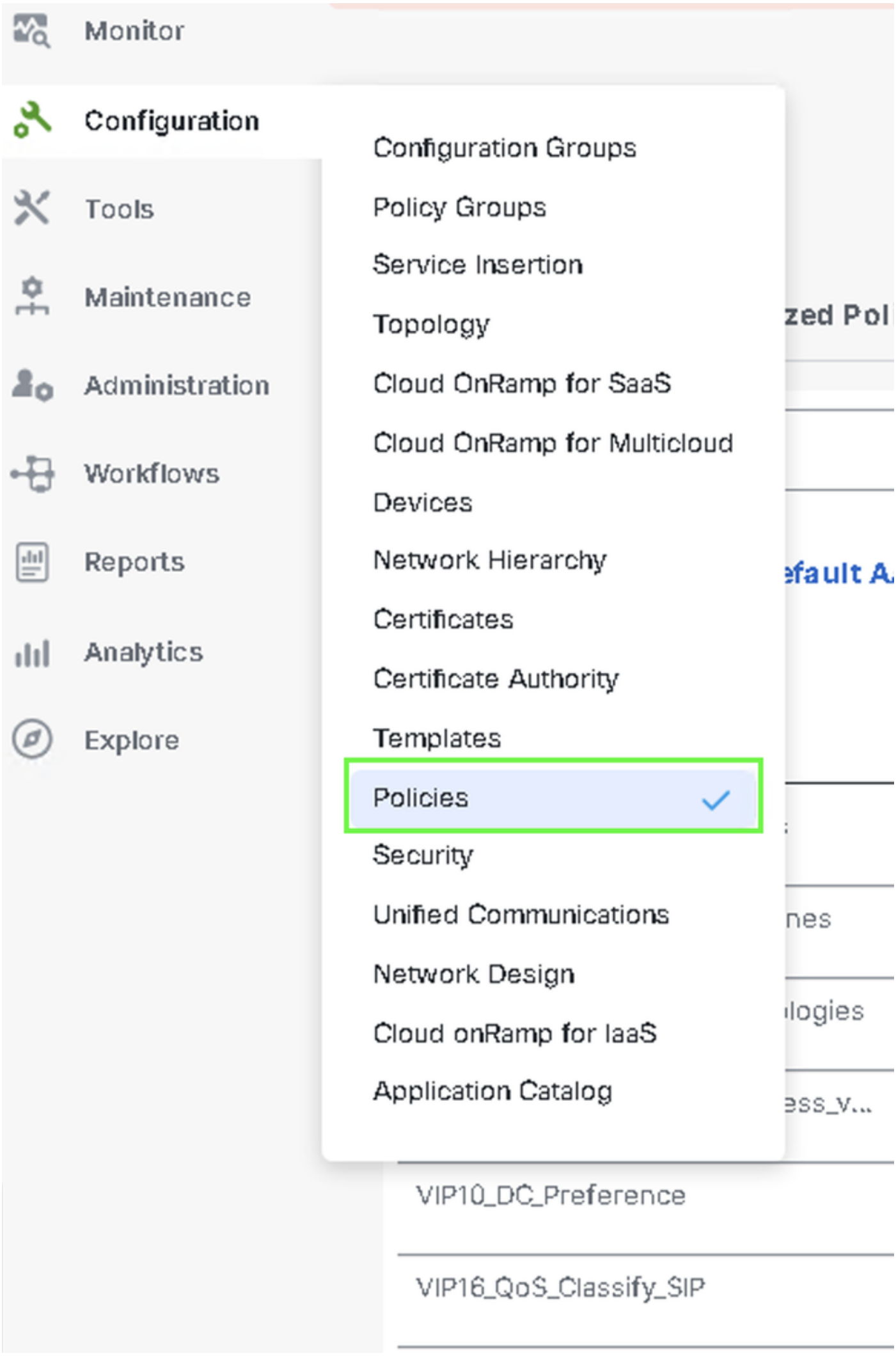


Étape 3 : activation de la fonction NAT Fallback sur la stratégie DIA existante

Les périphériques SD-WAN Cisco IOS XE Catalyst prennent en charge la fonctionnalité de secours NAT pour l'accès Internet direct (DIA). La fonctionnalité de secours NAT permet au trafic d'utiliser un autre chemin si le chemin NAT principal échoue. Cela garantit une connectivité continue même en cas de problèmes avec la configuration NAT principale.

Pour activer la reprise NAT à l'aide de Cisco SD-WAN Manager :

Dans le menu Cisco SD-WAN Manager, accédez à Configuration > Policy.


Monitor
Configuration
Tools
Maintenance
Administration
Workflows
Reports
Analytics
Explore
Configuration Groups
Policy Groups
Service Insertion
Topology
Cloud OnRamp for SaaS
Cloud OnRamp for Multicloud
Devices
Network Hierarchy
Certificates
Certificate Authority
Templates
Policies
Security
Unified Communications
Network Design
Cloud onRamp for IaaS
Application Catalog
VIP10_DC_Preference
VIP16_QoS_Classify_SIP

```
interface GigabitEthernet1
ip address 10.2.7.2 255.255.255.0
no ip redirects
ip nat outside
load-interval 30
negotiation auto
```

endpoint-tracker tracker1

```
arp timeout 1200
end
```

```
Site400-cE1#show sdwan running-config | sec endpoint
endpoint-tracker tracker1
tracker-type interface
endpoint-dns-name www.cisco.com
threshold 100
interval 30
```

Le résultat montre comment vérifier l'état du tracker à l'aide des commandes show endpoint-tracker et show endpoint-tracker GigabitEthernet1.

```
Site400-cE1#show endpoint-tracker
Interface         Record Name   Status   Address Family   RTT in msecs   Probe ID  Next Hop
GigabitEthernet1    tracker1     Up      IPv4              8              6       10.2.7.1

Site400-cE1#show endpoint-tracker interface GigabitEthernet1
Interface          Record Name    Status    Address Family   RTT in msecs   Probe ID  Next Hop
GigabitEthernet1    tracker1       Up        IPv4                8          6        10.2.7.1
```

Le résultat affiche des informations relatives au minuteur sur le traqueur pour aider à déboguer les problèmes liés au traqueur, le cas échéant :

```
Site400-cE1#show endpoint-tracker records
Record Name    Endpoint        EndPoint Type    Threshold(ms)  Multiplier   Interval(s)  Tracker-Type
tracker1       www.cisco.com    DNS_NAME           100            3            30         interface
```

Le résultat de la commande show ip sla summary.

```
Site400-cE1#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
```

```
All Stats are in milliseconds. Stats with u are in microseconds

ID  Type  Destination    Stats  Return   Last
                                Code     Run
------------------------------------------------------------------------
*5  dns    8.8.8.8       RTT=16  OK    16 seconds ago
*6  http   x.x.x.x       RTT=15  OK    3 seconds ago
```

Vérifiez la configuration de secours appliquée sur le périphérique à l'aide de la commande show sdwan policy from-vsmart.

<#root>

```
Site400-cE1#show sdwan policy from-vsmart
from-vsmart data-policy _VPN12_VPN12_DIA
direction from-service
vpn-list VPN12
sequence 1
match
source-data-prefix-list Site400_AllVPN_Prefixes
action accept
nat use-vpn 0
```

nat fallback

```
no nat bypass
default-action drop
```

Suivi du dépannage

Activez ces débogages sur le périphérique de périphérie pour vérifier comment le routeur envoie des sondes afin de déterminer l'état de l'interface de transport.

- Pour surveiller la façon dont le routeur envoie des sondes et détermine l'état des interfaces de transport, utilisez la commande debug platform software sdwan tracker qui est prise en charge jusqu'à la version 17.12.x.
- À partir de la version 17.13.x, pour surveiller les journaux des sondes, activez ces débogages.
  - set platform software trace ios R0 sdwanrp-tracker debug
  - set platform software trace ios R0 sdwanrp-cfg debug

- Activez ces débogages pour vérifier les journaux relatifs aux erreurs et au suivi des opérations IP SLA. Ces journaux indiquent si les opérations IP SLA échouent.
  - debug ip sla trace
  - debug ip sla error

Exécutez ces commandes show et monitor pour vérifier les journaux de débogage :

- show logging profile sdwan internal

- monitor logging profile sdwan internal

```
Site400-cE1#show logging profile sdwan internal
Logging display requested on 2024/08/13 08:10:45 (PDT) for Hostname: [Site400-cE1], Model: [C8000V], Ve

Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds
executing cmd on chassis local ...
Unified Decoder Library Init .. DONE
Found 1 UTF Streams

2024/08/13 08:02:28.408998337 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 s
2024/08/13 08:02:28.409061529 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.409086404 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE: Sla sync
2024/08/13 08:02:28.409160541 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE: Sla sync
2024/08/13 08:02:28.409182208 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Sta
2024/08/13 08:02:28.409197024 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Qu
2024/08/13 08:02:28.409215496 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 DN
2024/08/13 08:02:28.409242243 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 So
2024/08/13 08:02:28.409274690 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 De
2024/08/13 08:02:28.409298157 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 So
2024/08/13 08:02:28.409377223 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Ne
2024/08/13 08:02:28.409391034 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Re
2024/08/13 08:02:28.409434969 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 ac
2024/08/13 08:02:28.409525831 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Pr
2024/08/13 08:02:28.426966448 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Qu
2024/08/13 08:02:28.427004143 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Re
2024/08/13 08:02:28.427029754 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 RT
2024/08/13 08:02:28.427161550 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427177727 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427188035 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427199147 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427208941 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 IP
2024/08/13 08:02:28.427219960 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427238042 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427301952 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427316275 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427326235 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): Received IPSLA sta
2024/08/13 08:02:28.427328425 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): DNS status callbac
2024/08/13 08:02:28.427341452 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): DNS query valid TR
2024/08/13 08:02:28.427343152 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): DNS resolved addre
2024/08/13 08:02:28.427344332 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): DNS probe handler
2024/08/13 08:02:28.427349194 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427359268 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427370416 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427555382 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427565670 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427577691 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427588947 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427600567 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427611465 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427620724 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427645035 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:55.599896668 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 sl
2024/08/13 08:02:55.599966240 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 St
2024/08/13 08:02:55.599981173 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Sta
2024/08/13 08:02:55.600045761 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Nex
2024/08/13 08:02:55.600111585 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 DNS
2024/08/13 08:02:55.600330868 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 sla
2024/08/13 08:02:55.610693565 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Soc
2024/08/13 08:02:55.610717011 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Wai
```

```
2024/08/13 08:02:55.610777327 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Sen
2024/08/13 08:02:55.610788233 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Wai
2024/08/13 08:02:55.618534651 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Soc
2024/08/13 08:02:55.618685838 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 HTT
2024/08/13 08:02:55.618697389 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sc
2024/08/13 08:02:55.618706090 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sc
2024/08/13 08:02:55.618714316 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sc
2024/08/13 08:02:55.618723915 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sc
2024/08/13 08:02:55.618732815 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 IPS
2024/08/13 08:02:55.618821650 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:55.618833396 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:55.618857012 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
```

Informations connexes

[Implémenter un accès direct à Internet (DIA) pour SD-WAN]

[Guide de configuration de la fonction NAT SD-WAN de Cisco Catalyst]

[Reprise NAT sur les périphériques SD-WAN Cisco IOS XE Catalyst]

[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.