Configuration de SD-WAN Cloud OnRamp pour SaaS

Table des matières

Introduction

Ce document décrit la configuration de Cloud OnRamp pour le logiciel en tant que service (SaaS) à l'aide de la sortie locale de la filiale.

Conditions préalables

Exigences

Cisco recommande que vous ayez connaissance du 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 :

- Cisco vManage version 20.9.4
- Routeur de périphérie WAN Cisco version 17.9.3a

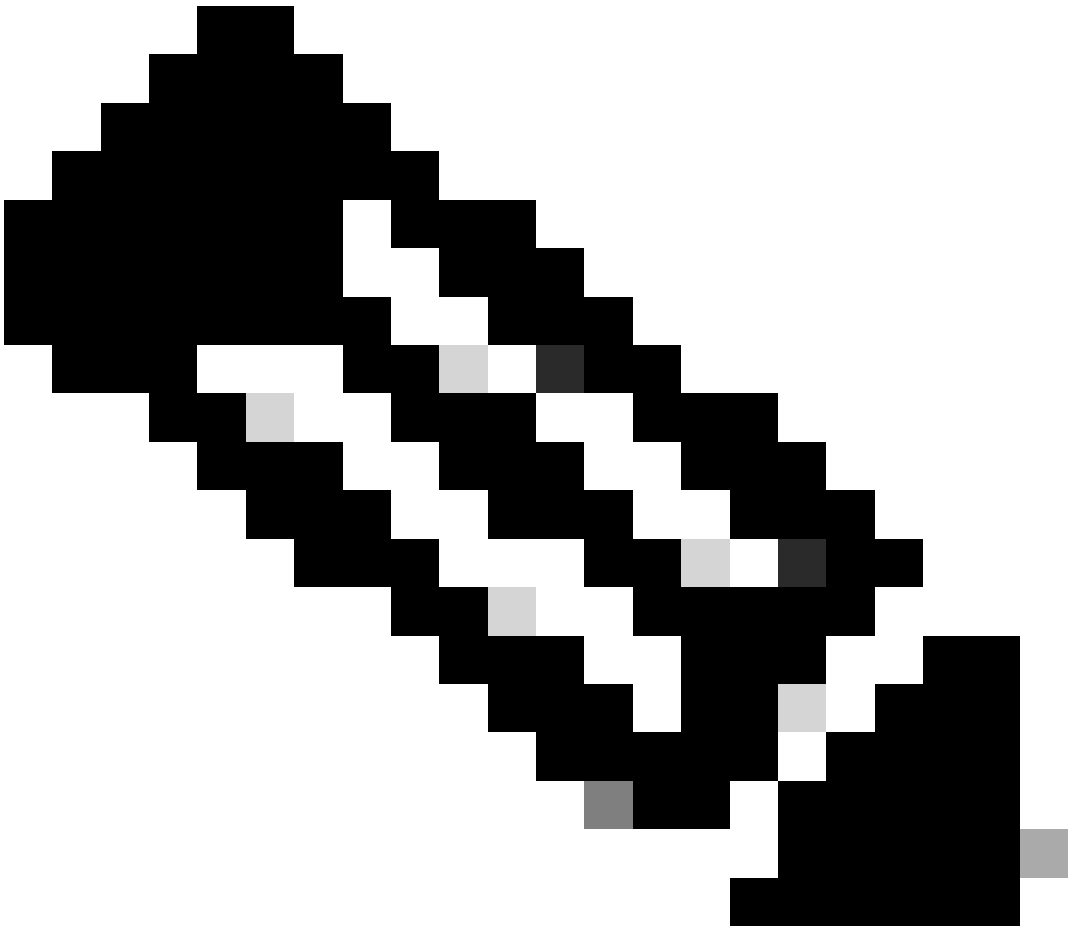
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Pour une entreprise utilisant le SD-WAN, un site de filiale achemine généralement le trafic des applications SaaS par défaut sur des liaisons de superposition SD-WAN vers un data center. À partir du data center, le trafic SaaS atteint le serveur SaaS.

Par exemple, dans une grande entreprise disposant d'un data center central et de sites de filiale, les employés peuvent utiliser Office 365 sur un site de filiale. Par défaut, le trafic Office 365 d'une filiale est acheminé via une liaison de superposition SD-WAN vers un data center centralisé et, à partir de la sortie DIA, vers le serveur cloud Office 365.

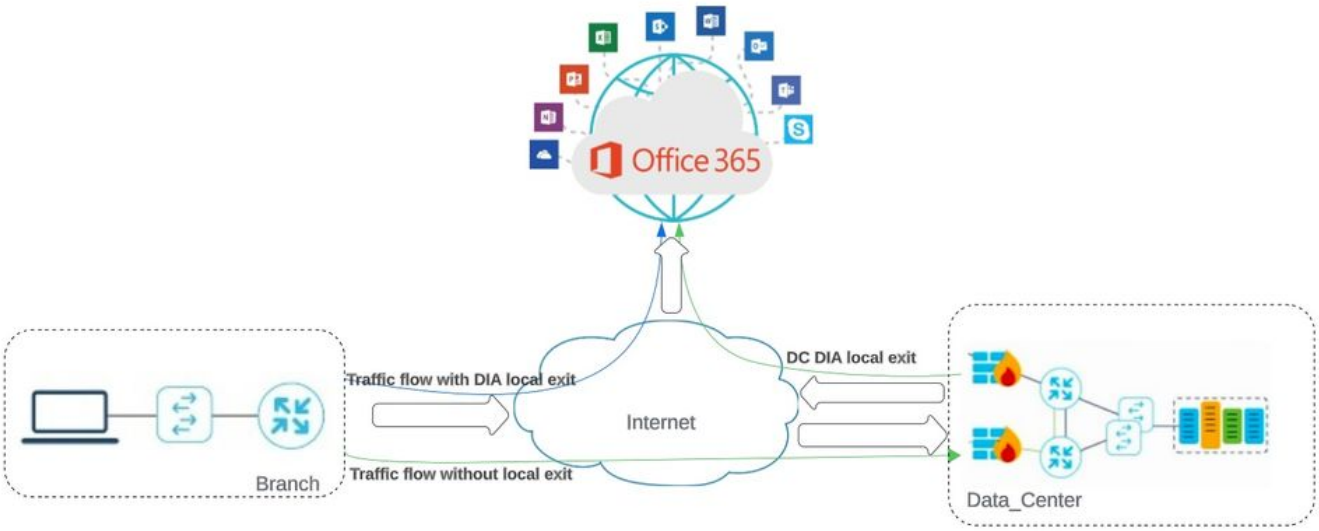
Ce document couvre ce scénario : Si le site de la filiale dispose d'une connexion d'accès direct à Internet (DIA), vous pouvez améliorer les performances en acheminant le trafic SaaS via le DIA local, en contournant le centre de données.



Remarque : la configuration de Cloud OnRamp pour SaaS lorsqu'un site utilise un bouclage comme interface de localisation de transport (TLOC) n'est pas prise en charge.

Configurer

Diagramme du réseau

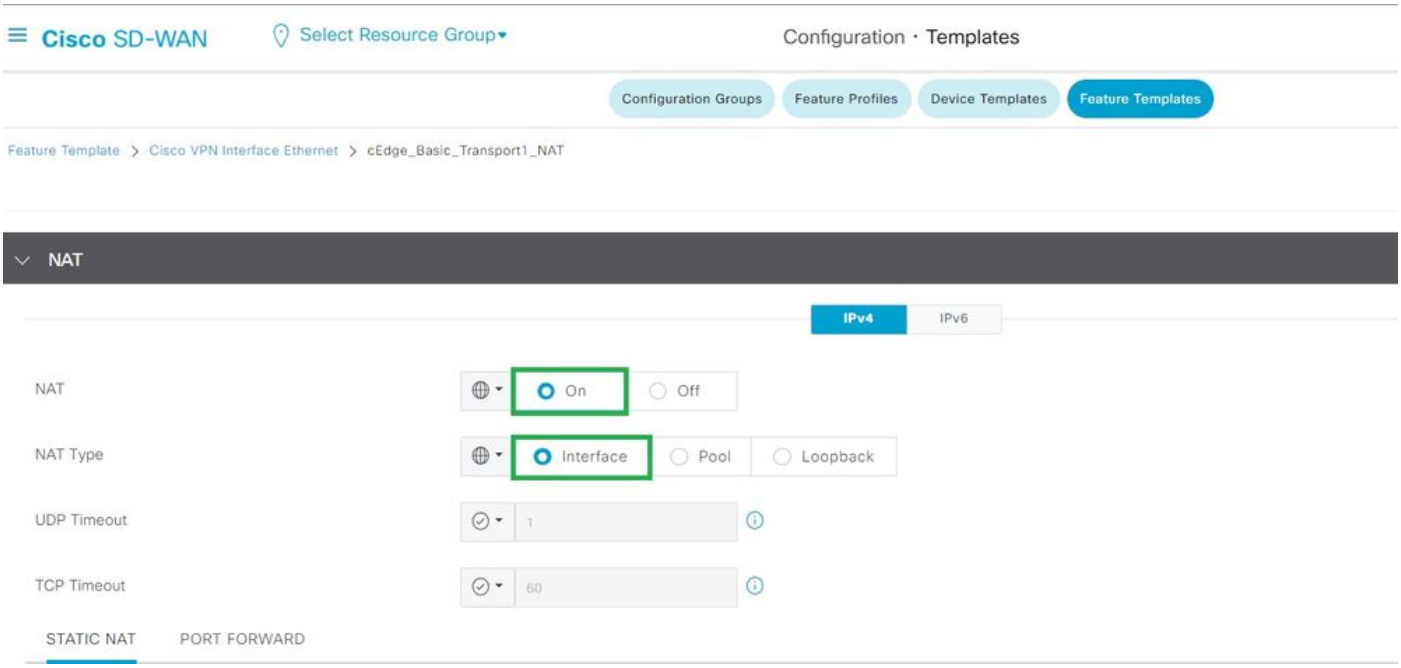


Topologie du réseau

Configurations

Activer NAT sur l'interface de transport

Accédez à Feature Template . Sélectionnez le **Transport VPN interface** modèle et **Activer NAT**.



Activer l'interface NAT

Configuration CLI équivalente :

interface GigabitEthernet2
ip nat outside

ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload
ip nat translation tcp-timeout 3600
ip nat translation udp-timeout 60

Créer une politique AAR centralisée

Pour établir une stratégie centralisée, vous devez suivre la procédure suivante :

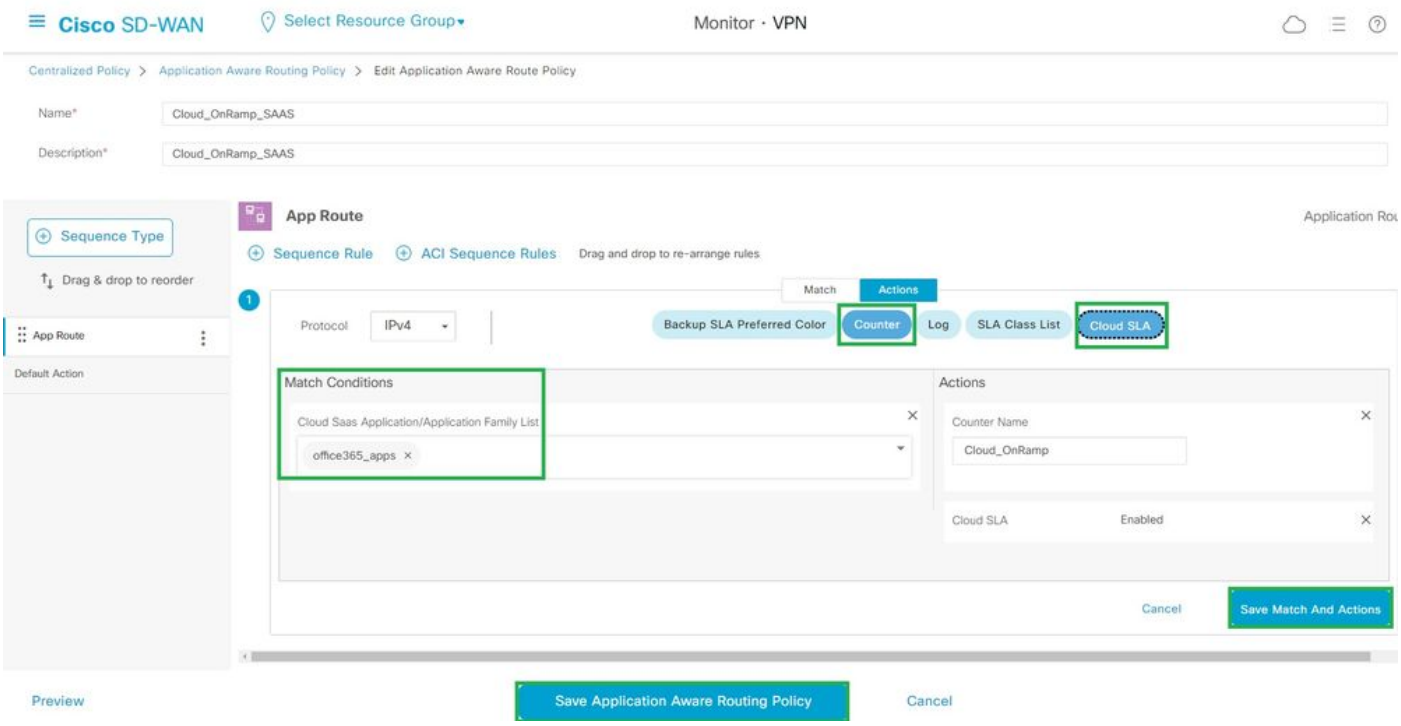
Étape 1. Créer une liste de sites :

Modèle NAT d'interface VPN

Étape 2. Créer une liste VPN :

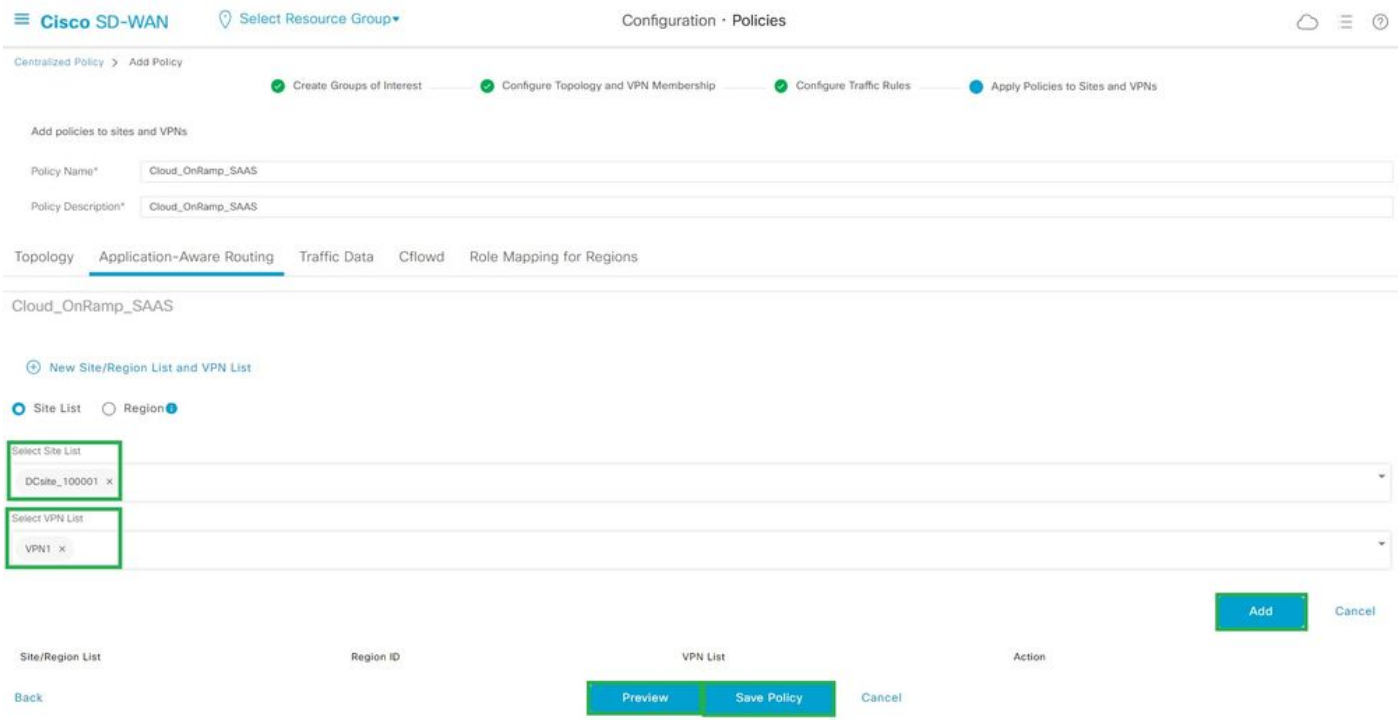
Liste des sites personnalisés de stratégie centralisée

Étape 3. Configurez le Traffic Rules et créez le Application Aware Routing Policy.



Stratégie de routage sensible aux applications

Étape 4. Ajoutez la stratégie à la stratégie souhaitéeSites et VPN:



Ajouter des stratégies aux sites et aux VPN

Politique d'équivalence CLI :

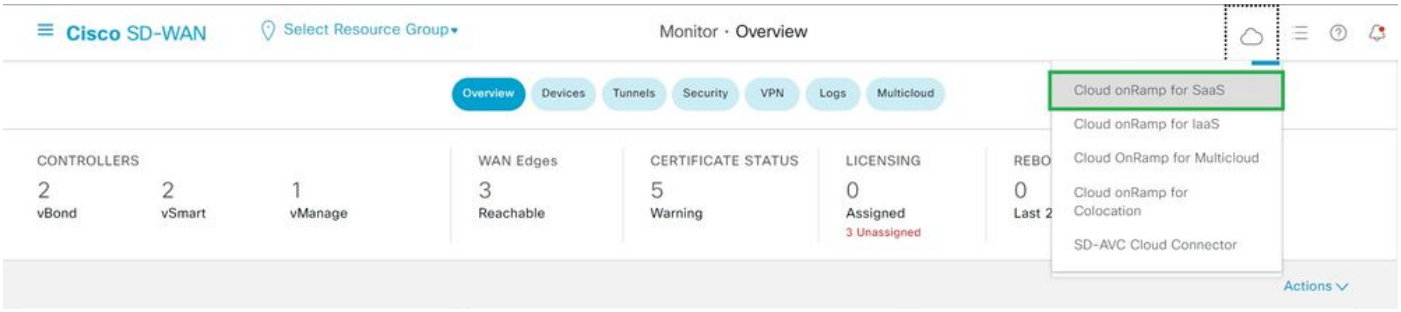
```
viptela-policy:policy
app-route-policy _VPN1_Cloud_OnRamp_SAAS
vpn-list VPN1
sequence 1
```

match
cloud-saas-app-list office365_apps
source-ip 0.0.0.0/0
!
action
count Cloud_OnRamp_-92622761
!
!
!
lists
app-list office365_apps
app skype
app ms_communicator
app windows_marketplace
app livemail_mobile
app word_online
app excel_online
app onedrive
app yammer
app sharepoint
app ms-office-365
app hockeyapp
app live_hotmail
app live_storage
app outlook-web-service
app skydrive
app ms_teams
app skydrive_login
app sharepoint_admin
app ms-office-web-apps
app ms-teams-audio
app share-point
app powerpoint_online
app ms-lync-video
app live_mesh
app ms-lync-control
app groove
app ms-live-accounts
app office_docs
app owa
app ms_sway
app ms-lync-audio
app live_groups
app office365
app windowslive
app ms-lync
app ms-services
app ms_translator
app microsoft
app sharepoint_blog
app ms_onenote
app ms-teams-video
app ms-update
app ms-teams-media
app ms_planner
app lync
app outlook
app sharepoint_online
app lync_online

app sharepoint_calendar
app ms-teams
app sharepoint_document
!
site-list DCsite_100001
site-id 100001
!
vpn-list VPN1
vpn 1
!
!
!
apply-policy
site-list DCsite_100001
app-route-policy _VPN1_Cloud_OnRamp_SAAS
!
!

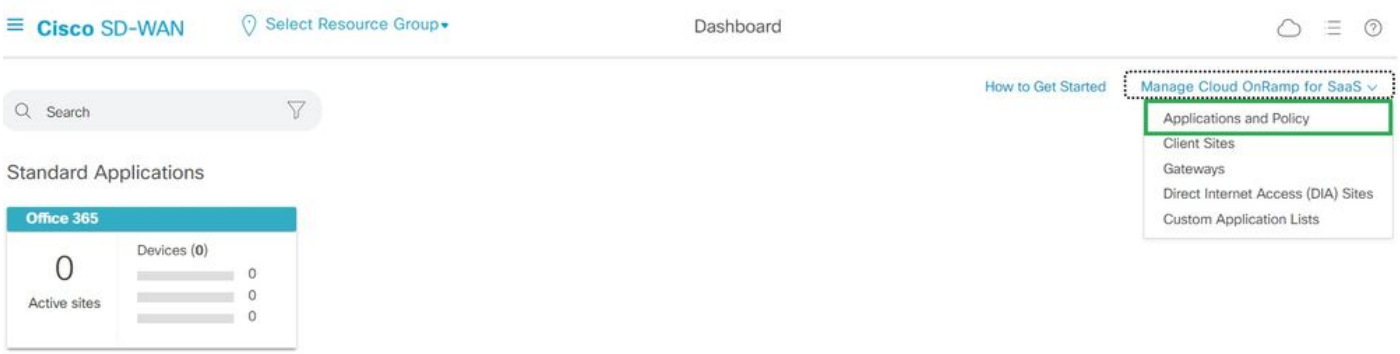
Activer l'application et l'accès Internet direct dans vManage

Étape 1. Accédez à Cloud OnRamp for SaaS.



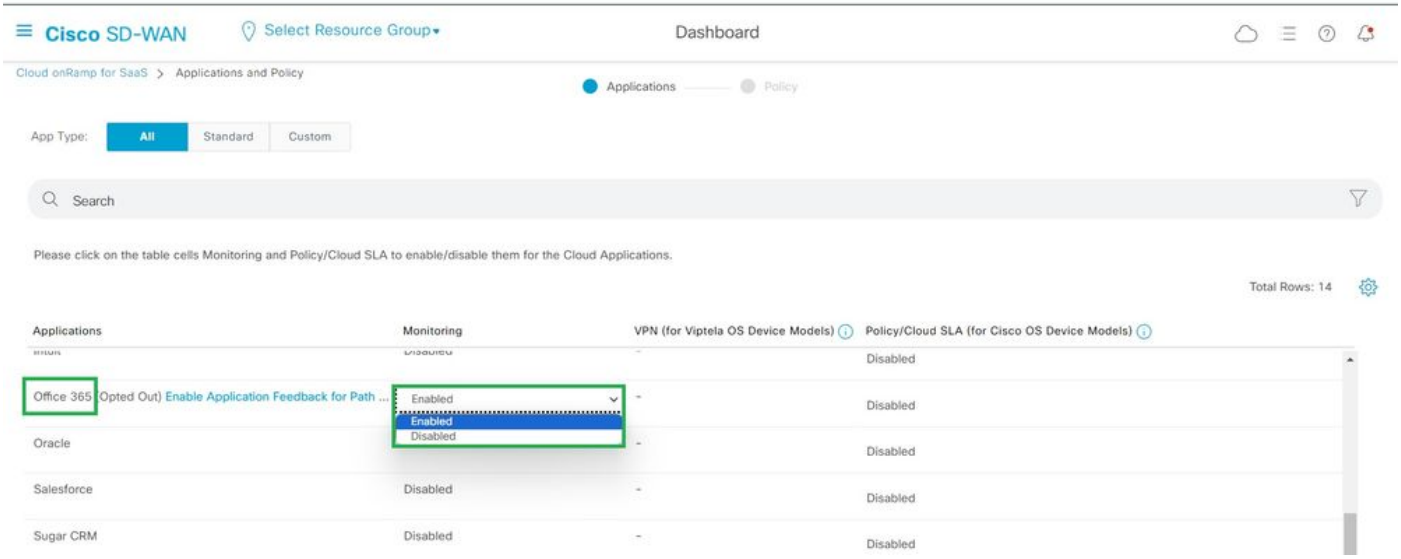
Sélectionner Cloud onRamp pour SaaS

Étape 2. Accédez à Applications and Policy.



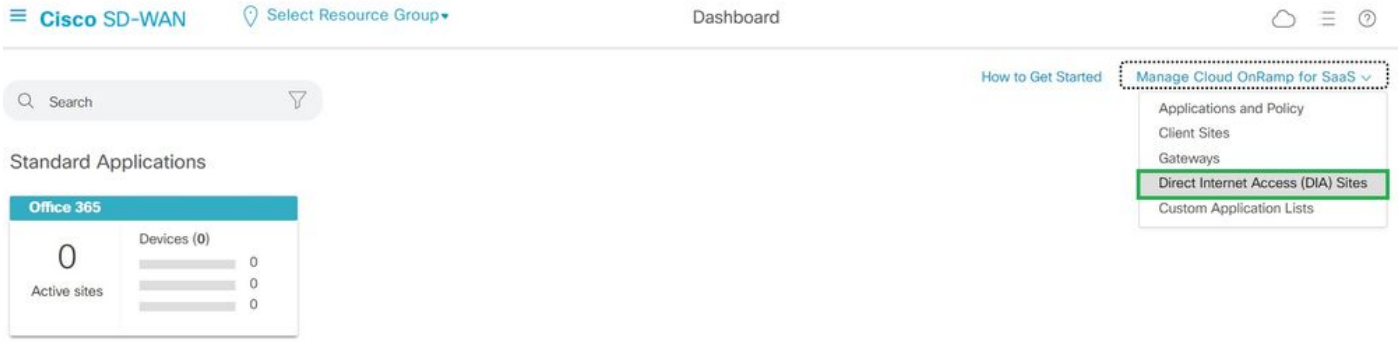
Sélectionner les applications et la stratégie

Étape 3. Accédez à Application > Enableet Save. Cliquez ensuite sur Next.



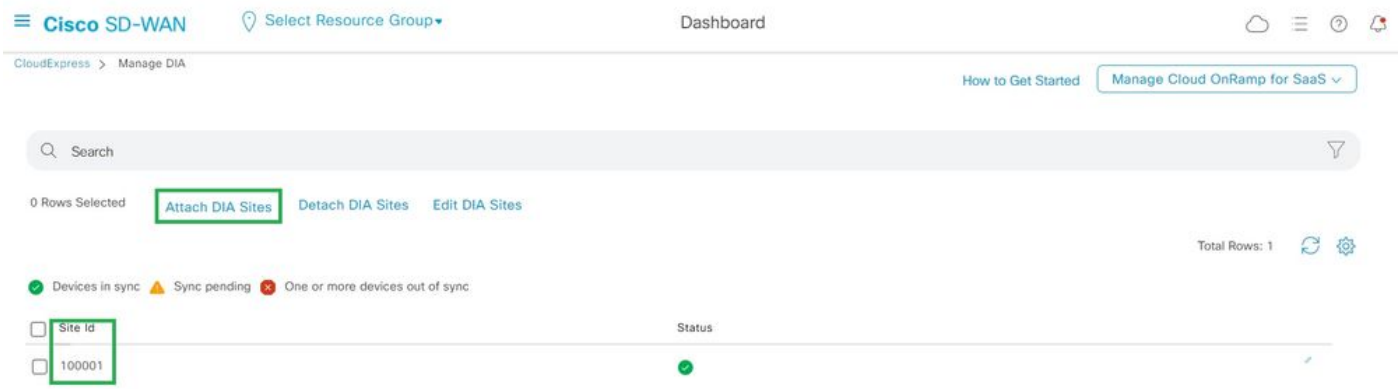
Sélectionner des applications et activer la surveillance

Étape 4. Accédez à Direct Internet Access (DIA) Sites.



Sélectionner des sites d'accès Internet direct

Étape 5. Naviguez jusqu'Attach DIA Sites aux sites et sélectionnez-les.



Joindre des sites DIA

Vérification

Cette section décrit les résultats afin de vérifier le Cloud OnRamp pour SaaS.

- Ce résultat montre Cloudexpress local-exits :

```
cEdge_West-01#sh sdwan cloudexpress local-exits
cloudexpress local-exits vpn 1 app 2 type app-group subapp 0 GigabitEthernet2
application office365
latency 6
loss 0
```

- Ce résultat montre les applications Cloudexpress :

```
cEdge_West-01#sh sdwan cloudexpress applications
cloudexpress applications vpn 1 app 2 type app-group subapp 0
application office365
exit-type local
interface GigabitEthernet2
latency 6
loss 0
```

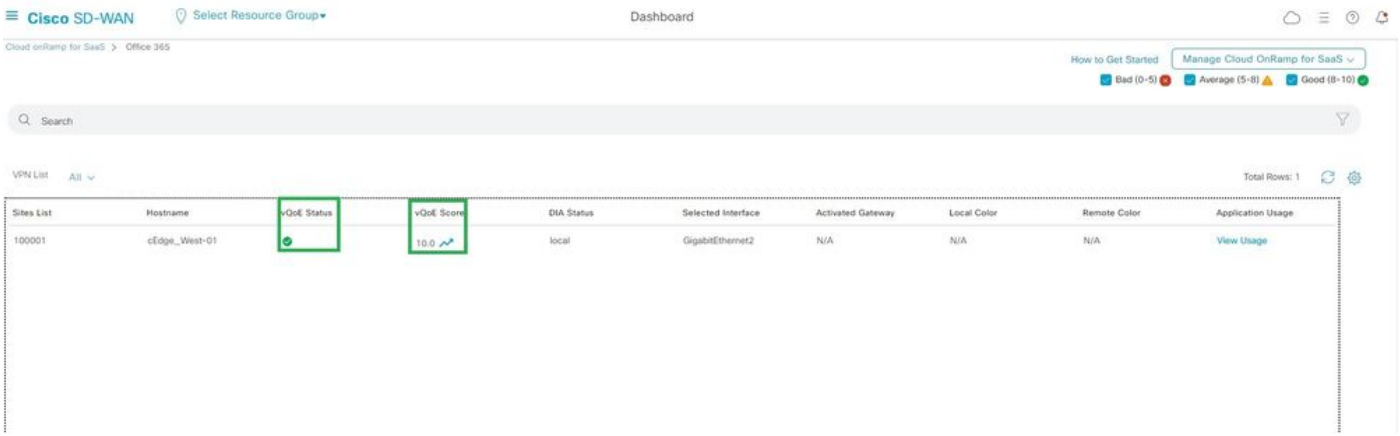
- Ce résultat montre les compteurs incrémentés pour le trafic intéressé :

<#root>

```
cEdge_West-01#sh sdwan policy app-route-policy-filter
NAME                       NAME         COUNTER NAME                          PACKETS      BYTES
-------------------------------------------------------------------------------------------------
_VPN1_Cloud_OnRamp_SAAS    VPN1         default_action_count                  640          66303
```

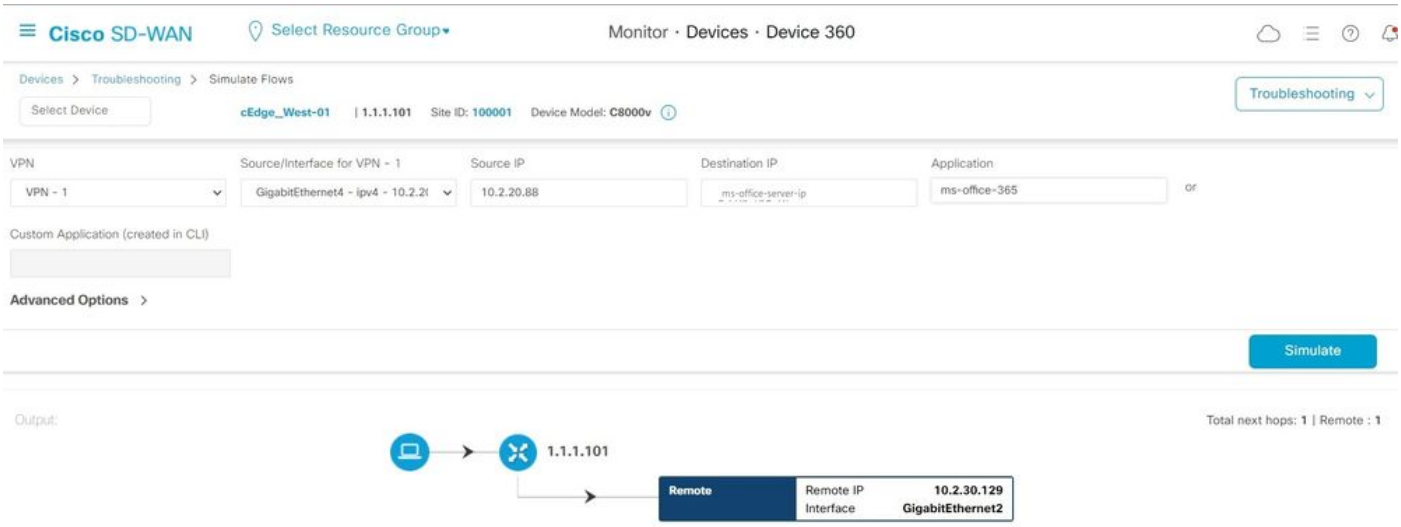
Cloud_OnRamp_-403085179 600 432292

- Ce résultat montre l'état et le score de la vQoE :



État et score vQoE

- Ce résultat montre le chemin de service de l'interface graphique utilisateur vManage :



Chemin de service

- Ce résultat montre le chemin de service de l'interface de ligne de commande du périphérique :

```
cEdge_West-01#sh sdwan policy service-path vpn 1 interface GigabitEthernet4 source-ip 10.2.20.70 dest-i
Next Hop: Remote
Remote IP: 10.2.30.129, Interface GigabitEthernet2 Index: 8
```

Informations connexes

- Guide de configuration de Cisco Catalyst SD-WAN Cloud OnRamp
- Assistance technique de Cisco et téléchargements

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.