Configuration de la topologie Hub and Spoke active/en veille sur SD-WAN

Table des matières

[Introduction](#)
[Conditions préalables](#)
[Exigences](#)
[Composants utilisés](#)
[Configurer](#)
[Diagramme du réseau](#)
[Configurations](#)
[Vérifier](#)
[Dépannage](#)
[Informations connexes](#)

Introduction

Ce document décrit les étapes de configuration et de validation d'une topologie Hub and Spoke en veille active sur Cisco SD-WAN.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

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

Composants utilisés

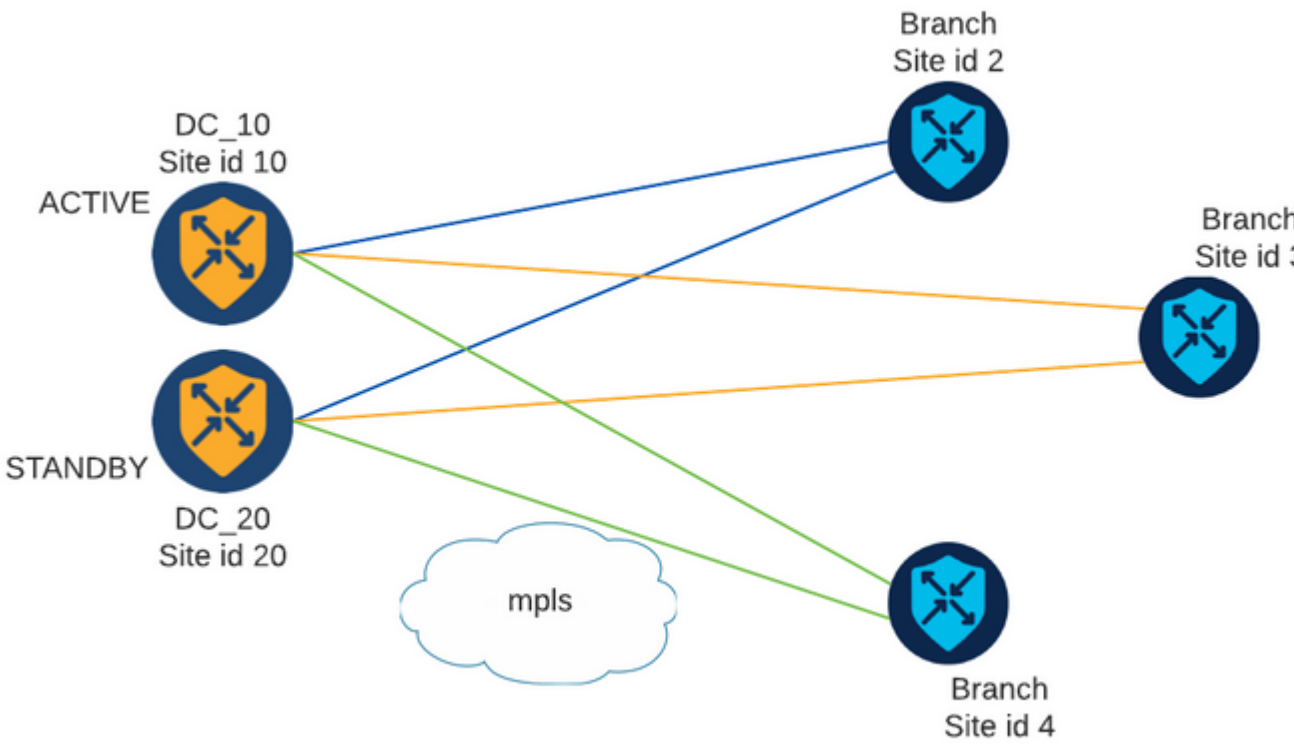
Ce document est basé sur les versions logicielles et matérielles suivantes :

- C8000V version 17.6.3a
- vManage version 20.6.3.1
- vSmart 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 lâ€™incidence possible des commandes.

Configurer

Diagramme du réseau

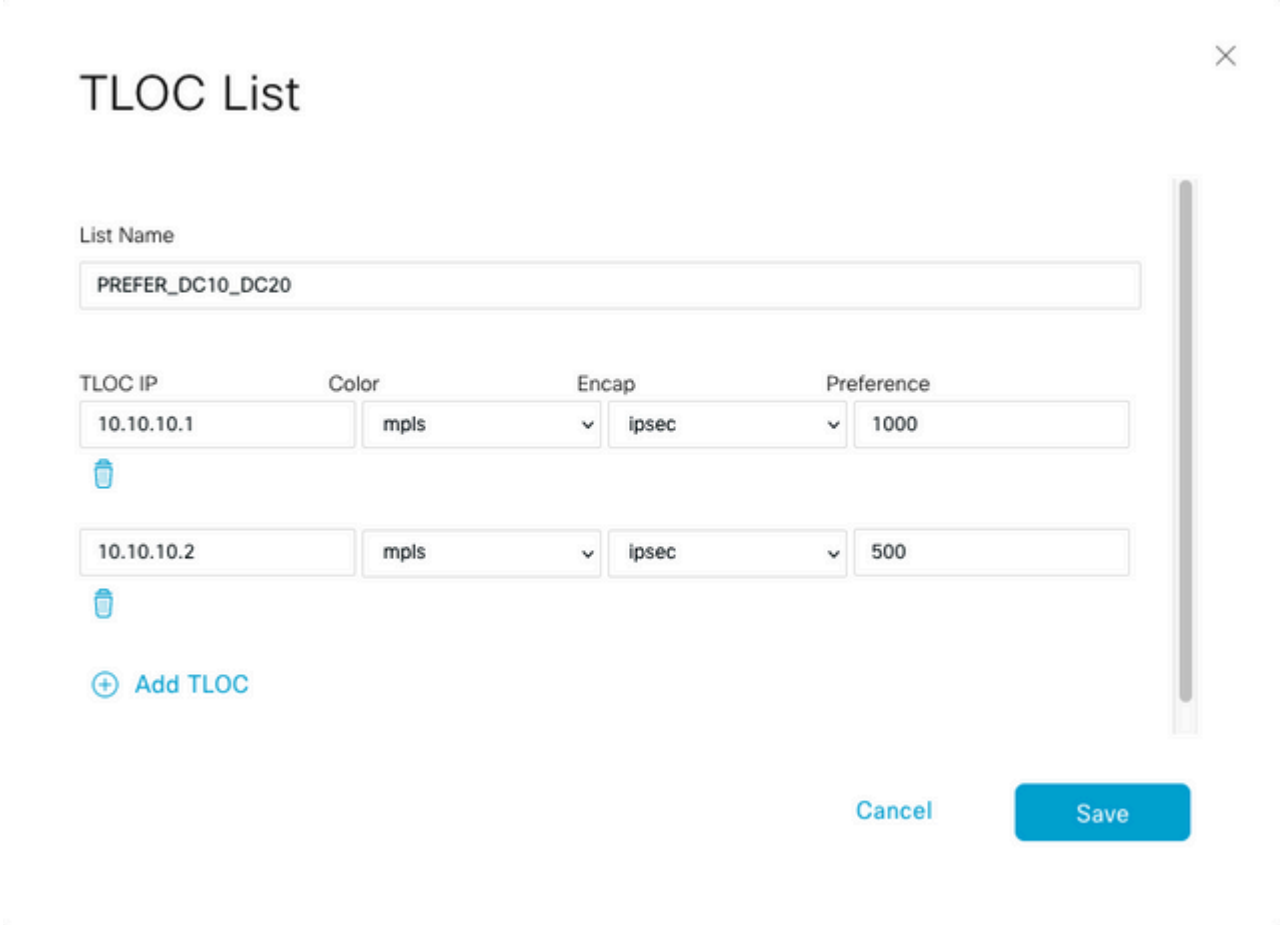


Il existe deux concentrateurs avec les ID de site 10 et 20. L'ID de site 10 fait office de concentrateur actif et l'ID de site 20 de concentrateur de secours. Les filiales peuvent communiquer entre elles, mais toutes les communications doivent passer par le concentrateur. Aucun tunnel ne doit être créé entre les sites de filiale.

Configurations

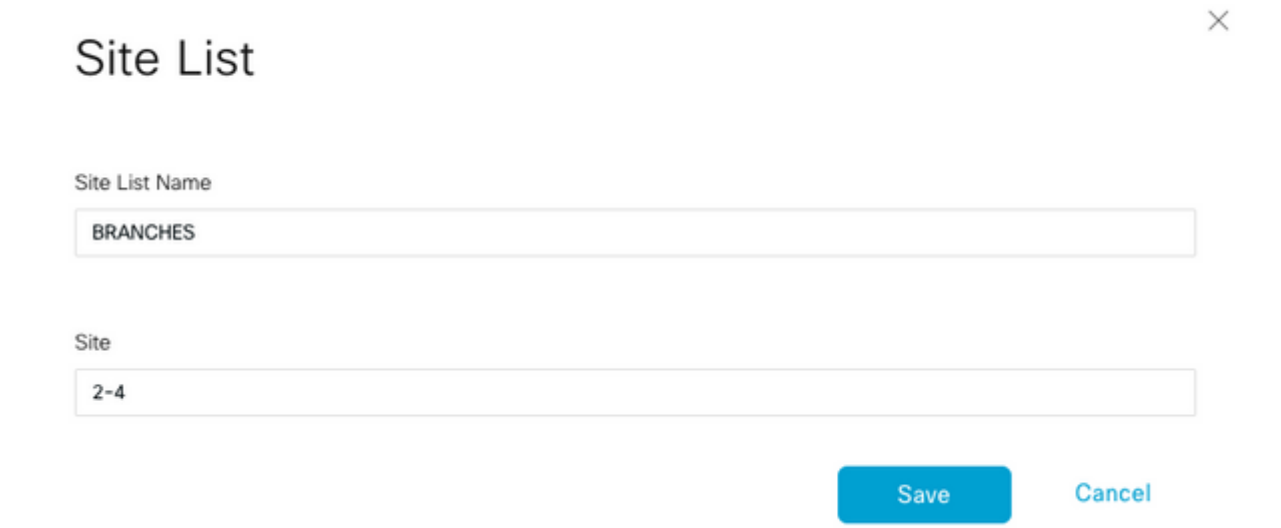
1. Connectez-vous à vManage, accédez à **Configuration > Policies** et cliquez sur **Add Policy**.

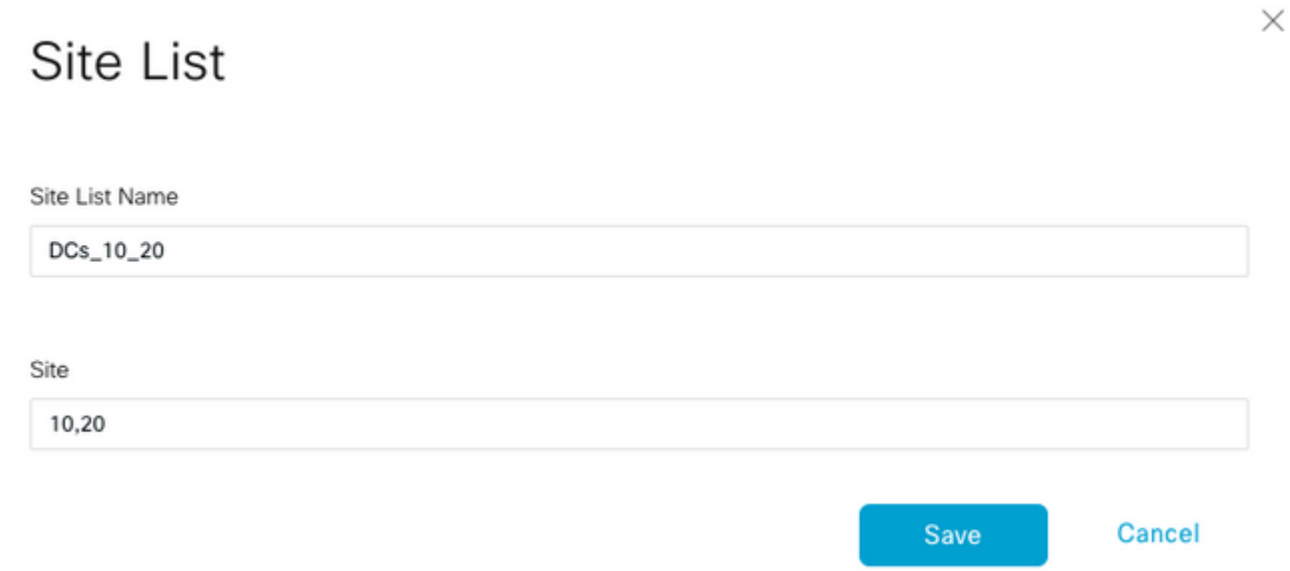
2. Dans la section Créer des groupes d'intérêt, cliquez sur **TLOC > Nouvelle liste TLOC** et ajoutez une entrée pour le concentrateur actif et une entrée pour le concentrateur de secours sur la même liste :



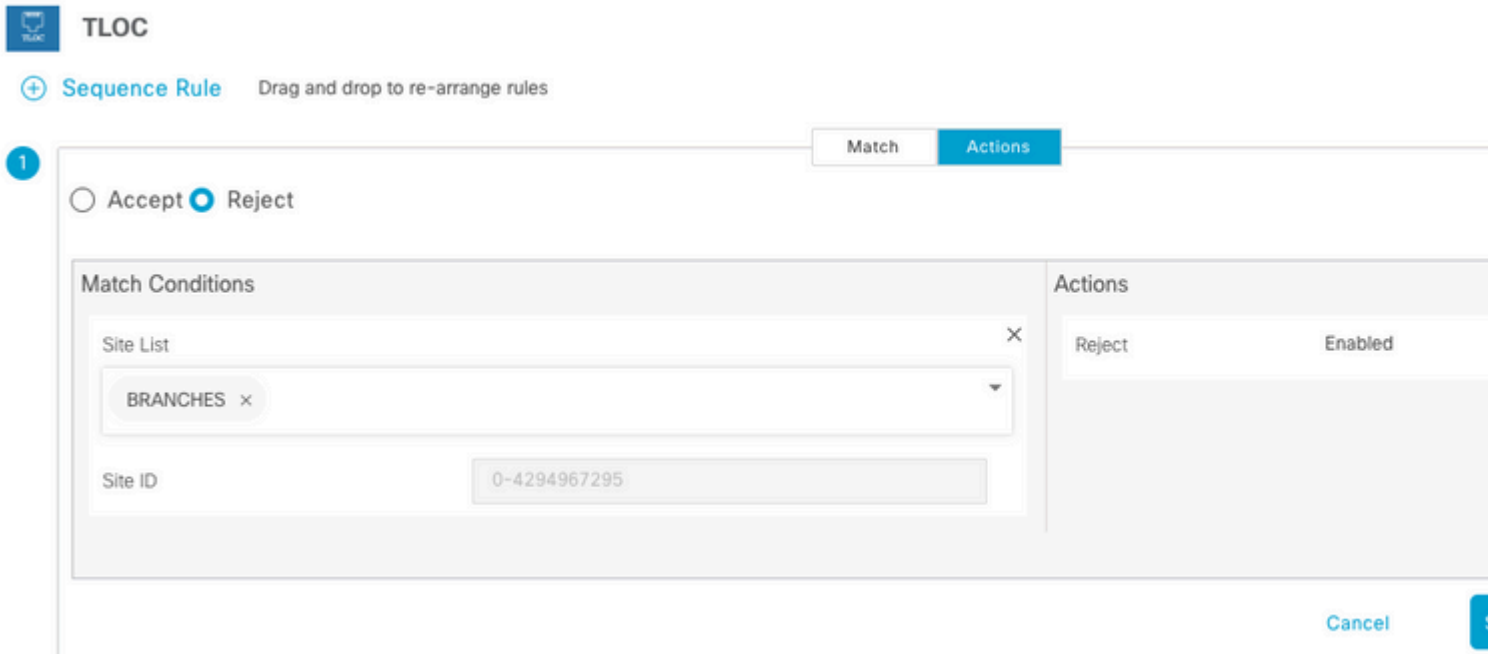
Assurez-vous de définir une préférence supérieure pour le concentrateur actif et une préférence inférieure pour le concentrateur de secours.

3. Accédez à **Site > Nouvelle liste de sites** et créez une liste pour les sites de filiale et une liste pour les sites de concentrateur :

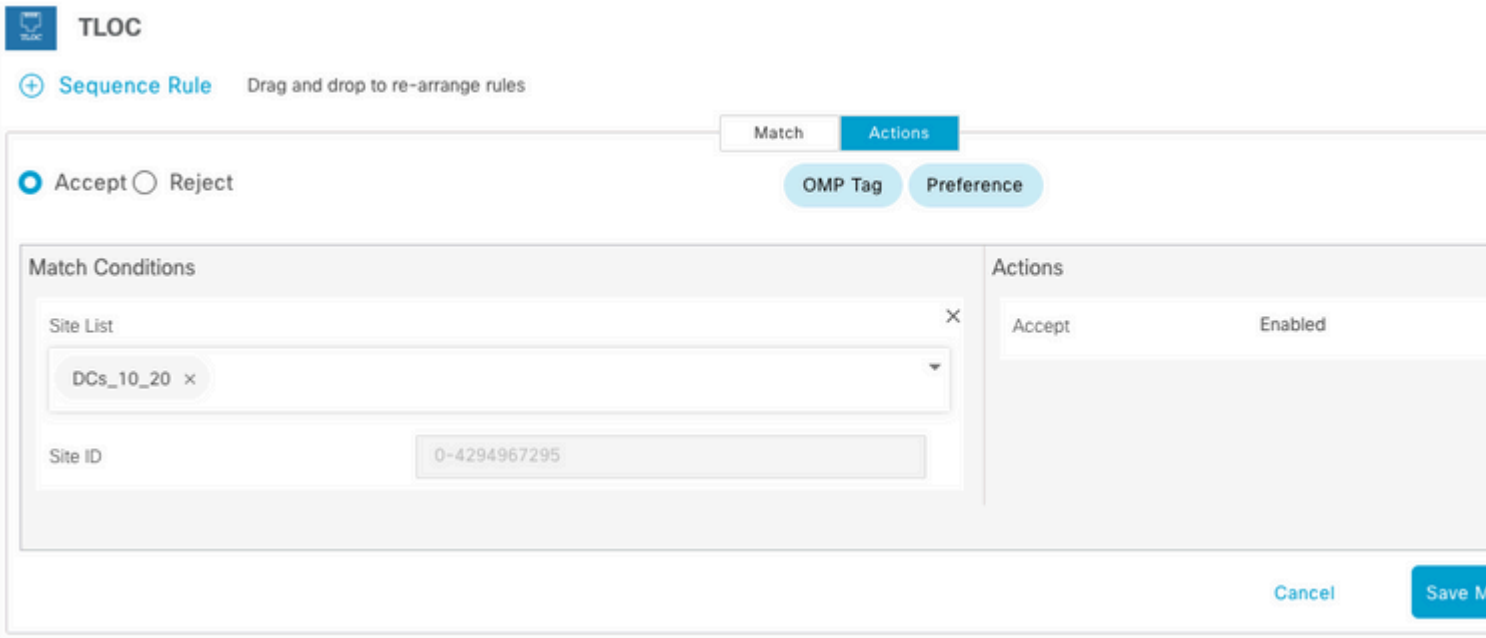




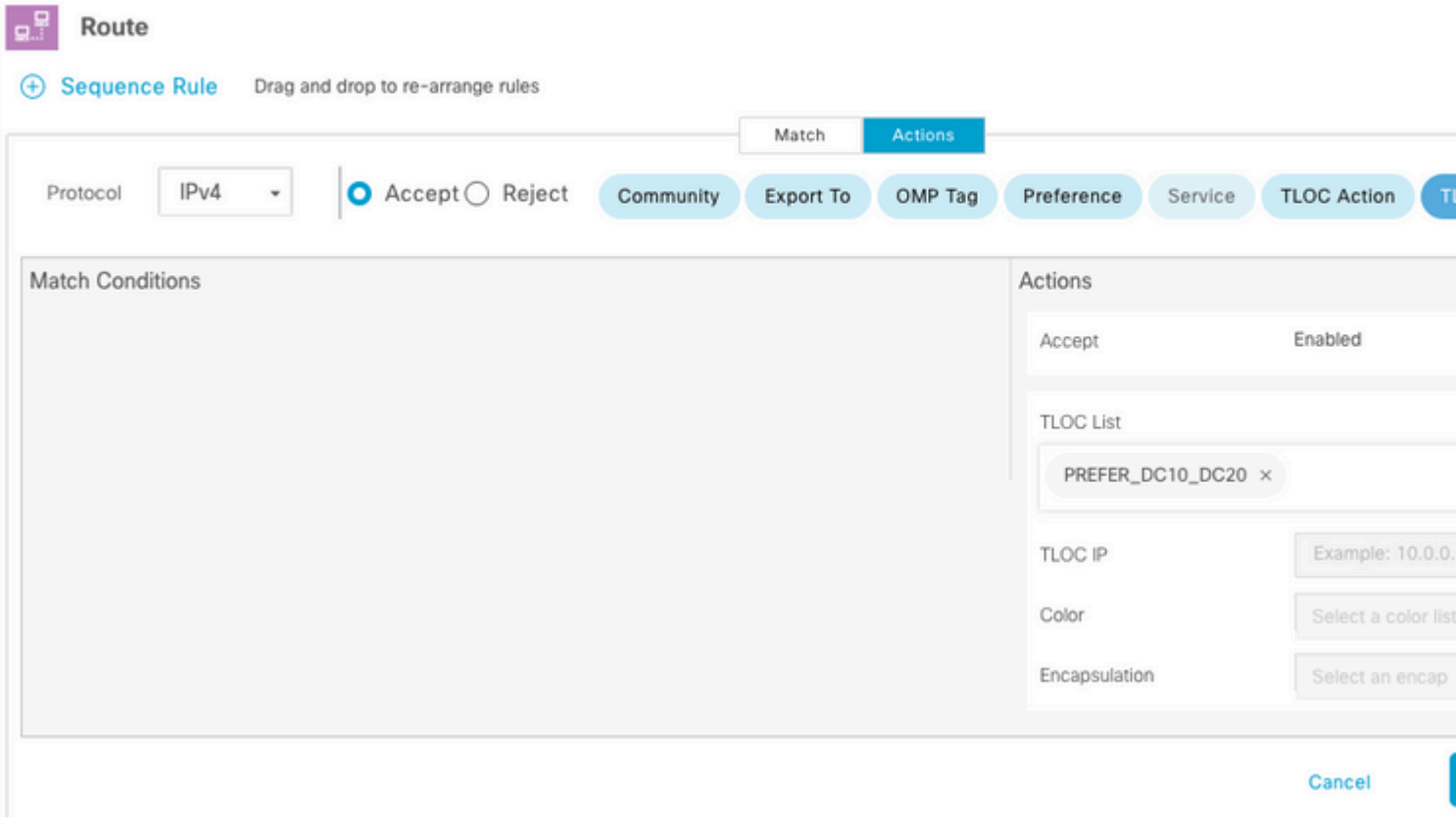
4. Cliquez sur **Suivant**. Dans la section Configurer la topologie et l'appartenance VPN, accédez à **Ajouter une topologie > Contrôle personnalisé**.
5. Ajoutez un nom et une description pour la stratégie.
6. Cliquez sur **Type de séquence > TLOC**, ajoutez une **règle de séquence.**
7. Choisissez **Correspondance > Site** et ajoutez la liste Site pour les branches, puis choisissez **Actions > Rejeter** et cliquez sur **Sauvegarder la correspondance et les actions** :



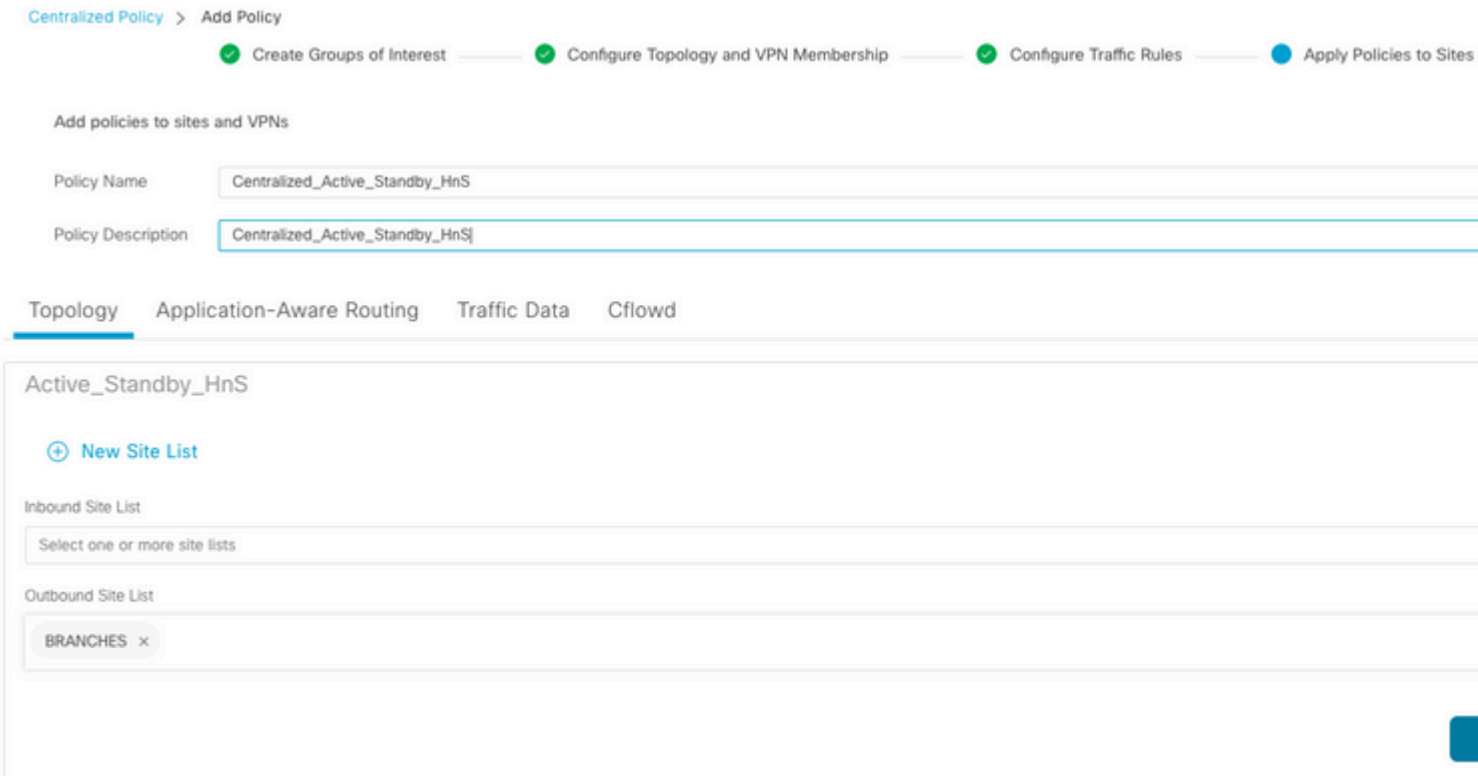
8. Cliquez sur **Sequence Rule**, et ajoutez une entrée correspondant à Hub Sites and Accept :



9. Accédez à **Sequence Type > Route**, ajoutez **Sequence Rule.**
10. Laissez la section de correspondance vide, définissez l'action sur **Accepter**, choisissez **TLOC**, ajoutez la liste TLOC créée précédemment et cliquez sur **Enregistrer la correspondance et les actions** :



11. Cliquez sur **Enregistrer la stratégie de contrôle.**
12. Cliquez sur **Next** jusqu'à ce que la section Apply Policies to Sites and VPNs.
13. Dans la section Topologie, votre stratégie de contrôle s'affiche, cliquez sur **Nouvelle liste de sites**, choisissez la liste Branches pour la liste de sites sortants et cliquez sur **Ajouter** :

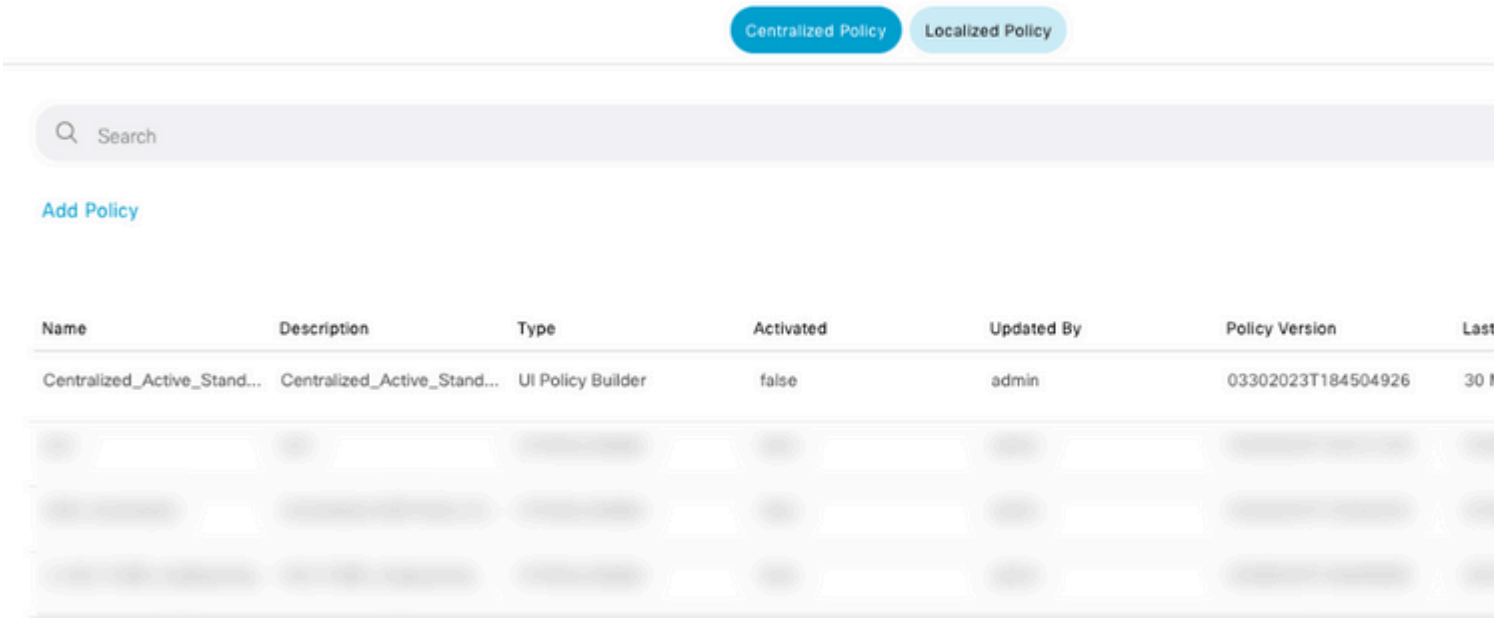


14. Cliquez sur **Aperçu** et vérifiez la stratégie.

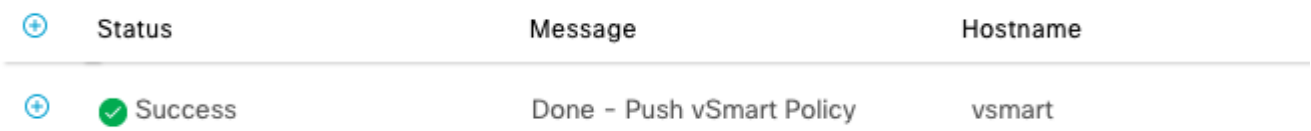
```
viptela-policy:policy
 control-policy Active_Standby_HnS
    sequence 1
     match tloc
      site-list BRANCHES
     !
     action reject
     !
    !
    sequence 11
     match tloc
      site-list DCs_10_20
     !
     action accept
     !
    !
    sequence 21
     match route
      prefix-list _AnyIpv4PrefixList
     !
     action accept
      set
       tloc-list PREFER_DC10_DC20
      !
     !
    !
  default-action reject
 !
 lists
  site-list BRANCHES
   site-id 2-4
  !
```

```
  site-list DCs_10_20
   site-id 10
   site-id 20
  !
  tloc-list PREFER_DC10_DC20
   tloc 10.10.10.1 color mpls encap ipsec preference 1000
   tloc 10.10.10.2 color mpls encap ipsec preference 500
  !
  prefix-list _AnyIpv4PrefixList
   ip-prefix 0.0.0.0/0 le 32
  !
 !
!
apply-policy
 site-list BRANCHES
  control-policy Active_Standby_HnS out
 !
!
```

15. Cliquez sur **Enregistrer la stratégie.**
16. Dans le menu Stratégie centralisée, cliquez sur les 3 points à droite de la nouvelle stratégie créée et sélectionnez **Activer.**



17. Une fois la tâche terminée, l'état Réussite s'affiche.



Vérifier

Vérifiez que la stratégie est créée sur vSmart à l'aide des commandes suivantes :

<#root>

vsmart#

show running-config policy

```
policy
lists
tloc-list PREFER_DC10_DC20
tloc 10.10.10.1 color mpls encap ipsec preference 1000
tloc 10.10.10.2 color mpls encap ipsec preference 500
!
site-list BRANCHES
site-id 2-4
!
site-list DCs_10_20
site-id 10
site-id 20
!
prefix-list _AnyIpv4PrefixList
ip-prefix 0.0.0.0/0 le 32
!
!
control-policy Active_Standby_HnS
sequence 1
match tloc
site-list BRANCHES
!
action reject
!
!
sequence 11
match tloc
site-list DCs_10_20
!
action accept
!
!
sequence 21
match route
prefix-list _AnyIpv4PrefixList
!
action accept
set
tloc-list PREFER_DC10_DC20
!
!
!
default-action reject
!
!
vsmart#
```

show running-config apply-policy

```
apply-policy
site-list BRANCHES
control-policy Active_Standby_HnS out
```

```
!
!
vsmart#
```

> **Remarque** : il s'agit d'une stratégie de contrôle. Il est appliqué et exécuté sur le vSmart et n'est pas poussé dans les périphériques de périphérie. La commande "**show sdwan policy from-vsmart**" n'affiche pas la stratégie sur les périphériques de périphérie.

Dépannage

Commandes utiles pour le dépannage.

Sur vSmart :

```
show running-config policy
show running-config apply-policy
show omp routes vpn <vpn> advertised <detail>
show omp routes vpn <vpn> received <detail>
show omp tlocs advertised <detail>
show omp tlocs received <detail>
```

Sur cEdge :

```
show sdwan bfd sessions
show ip route vrf <service vpn>
show sdwan omp routes vpn <vpn>  <detail>
show sdwan omp tlocs
```

Exemple :

Confirmez que seule la session BFD est formée entre Branch et les concentrateurs :

<#root>

```
Branch_02#
```

show sdwan bfd sessions

```
                         SOURCE TLOC REMOTE TLOC              DST PUBLIC   DST PUBLIC        DETECT
SYSTEM IP   SITE ID STATE COLOR       COLOR       SOURCE IP    IP           PORT       ENCAP  MULTIPLIER
--------------------------------------------------------------------------------------------------------
10.10.10.1  10      up    mpls        mpls        192.168.1.36 192.168.1.30 12386      ipsec  7
10.10.10.2  20      up    mpls        mpls        192.168.1.36 192.168.1.33 12366      ipsec  7
```

Vérifiez que les routes provenant d'autres filiales sont préférées via le concentrateur actif avec la préférence 1000 :

<#root>

Branch_02#

show sdwan omp route vpn 10 172.16.1.0/24 detail

Generating output, this might take time, please wait ...

---

omp route entries for vpn 10 route 172.16.1.0/24

RECEIVED FROM:
peer 10.1.1.3
path-id 8
label 1002

status C,I,R <-- Chosen, Installed, Received

loss-reason not set
lost-to-peer not set
lost-to-path-id not set
Attributes:
originator 10.3.3.3
type installed

tloc 10.10.10.1, mpls, ipsec <-- Active Hub

ultimate-tloc not set
domain-id not set
overlay-id 1
site-id 3

preference 1000

tag not set
origin-proto connected
origin-metric 0
as-path not set
community not set
unknown-attr-len not set
RECEIVED FROM:
peer 10.1.1.3
path-id 9
label 1003

status R <-- Received

loss-reason preference
lost-to-peer 10.1.1.3
lost-to-path-id 8
Attributes:
originator 10.3.3.3
type installed

tloc 10.10.10.2, mpls, ipsec <-- Backup Hub

```
ultimate-tloc not set
domain-id not set
overlay-id 1
site-id 3
```

`preference 500`

```
tag not set
origin-proto connected
origin-metric 0
as-path not set
community not set
unknown-attr-len not set
```

Informations connexes

Guide de configuration des politiques Cisco SD-WAN, Cisco IOS XE version 17.x

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.