Konfiguration einer Hub-and-Spoke-Topologie für aktiven/Standby-Modus im SD-WAN

Inhalt

Einleitung

In diesem Dokument werden die Schritte zur Konfiguration und Validierung einer aktiven Standby-Hub- und -Spoke-Topologie auf dem Cisco SD-WAN beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Cisco SD-WAN
- Grundlegende Cisco IOS-XE® Kommandozeile

Verwendete Komponenten

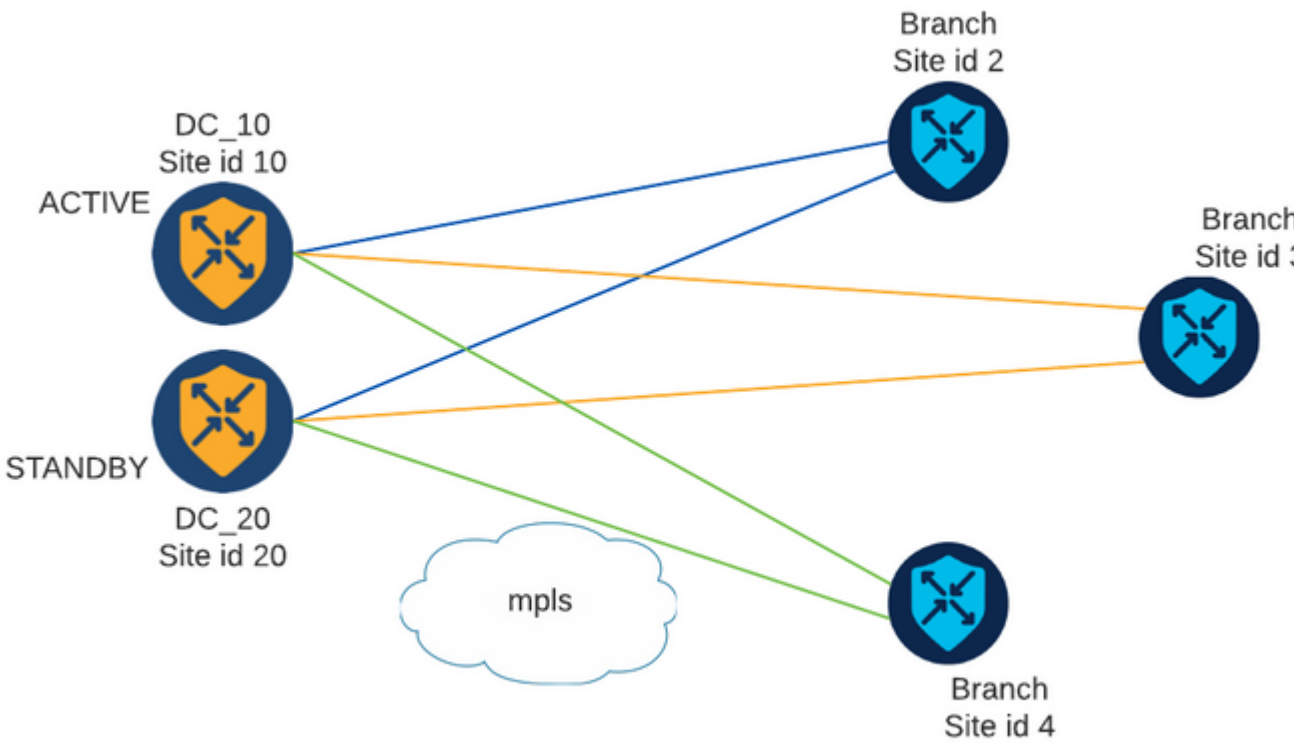
Dieses Dokument basiert auf den folgenden Software- und Hardwareversionen:

- C8000V Version 17.6.3a
- vManage, Version 20.6.3.1
- vSmart Version 20.6.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Netzwerkdiagramm

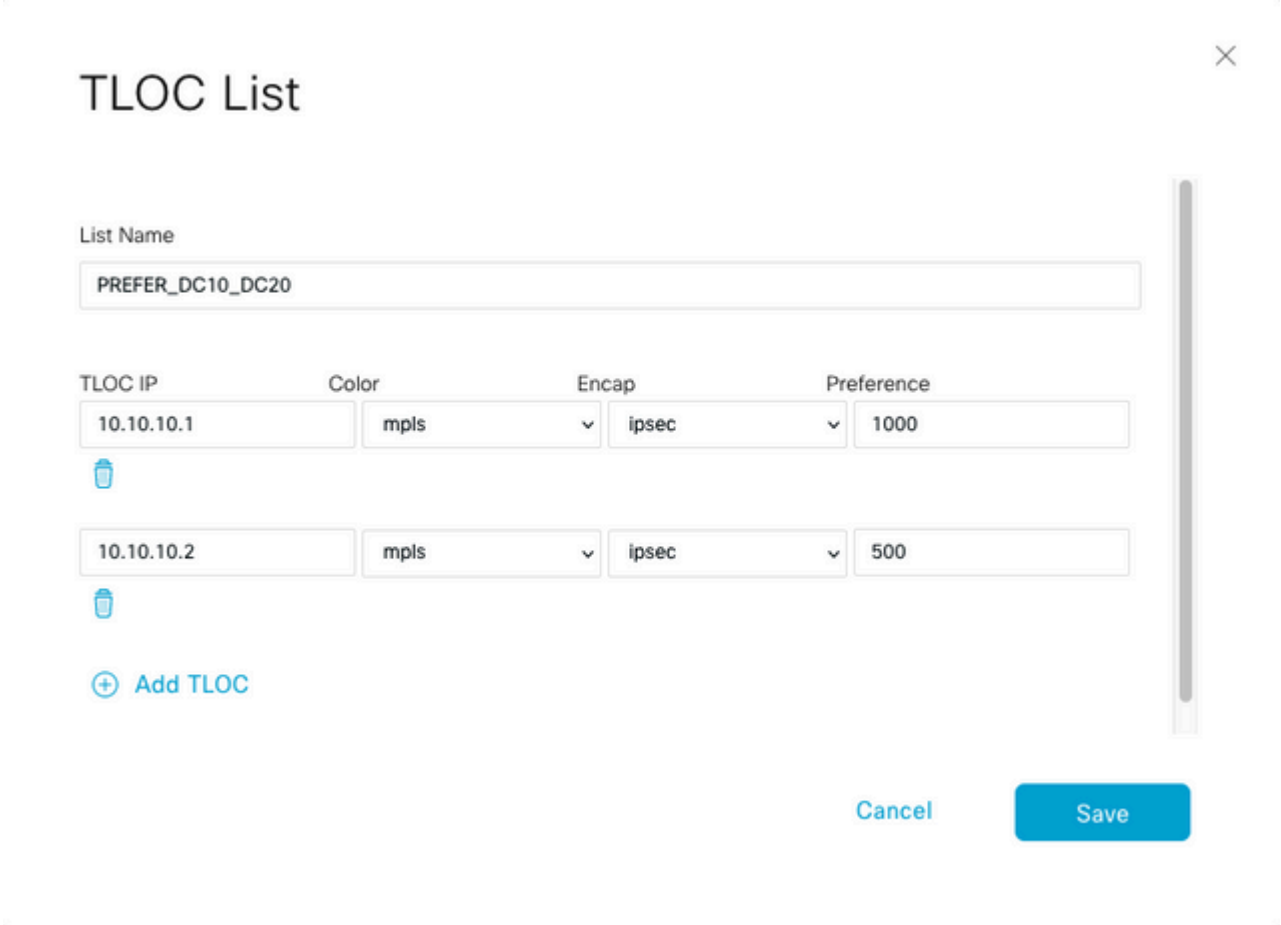


Es gibt zwei Hubs mit Standort-ID 10 und 20. Standort-ID 10 fungiert als aktiver Hub und Standort-ID 20 als Standby-Hub. Die Außenstellen können miteinander kommunizieren, aber die gesamte Kommunikation muss über den Hub erfolgen. Zwischen den Außenstellen dürfen keine Tunnel erstellt werden.

Konfigurationen

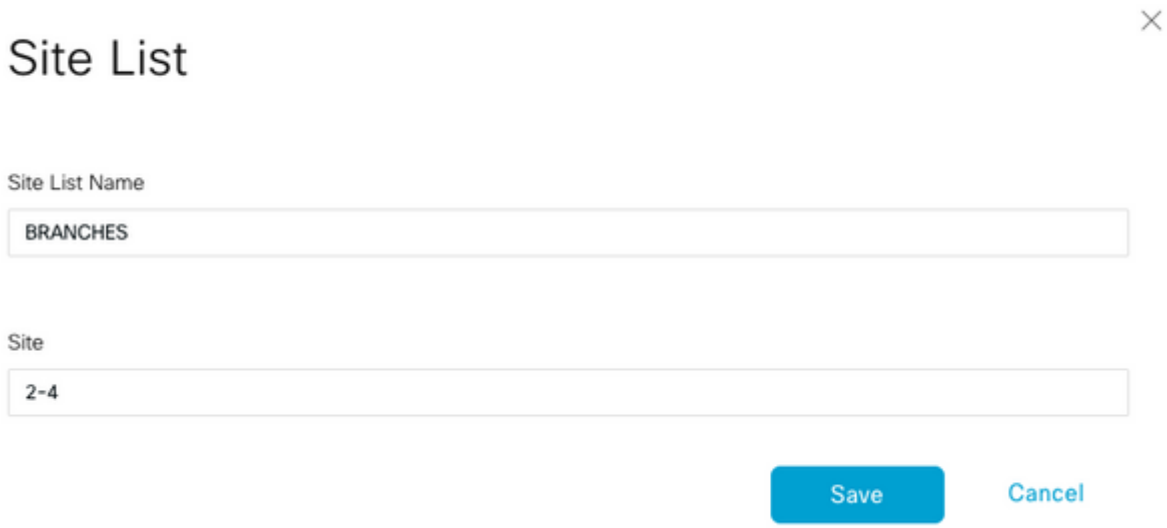
1. Melden Sie sich bei vManage an, navigieren Sie zu **Configuration > Policies**, und klicken Sie auf **Add Policy**.

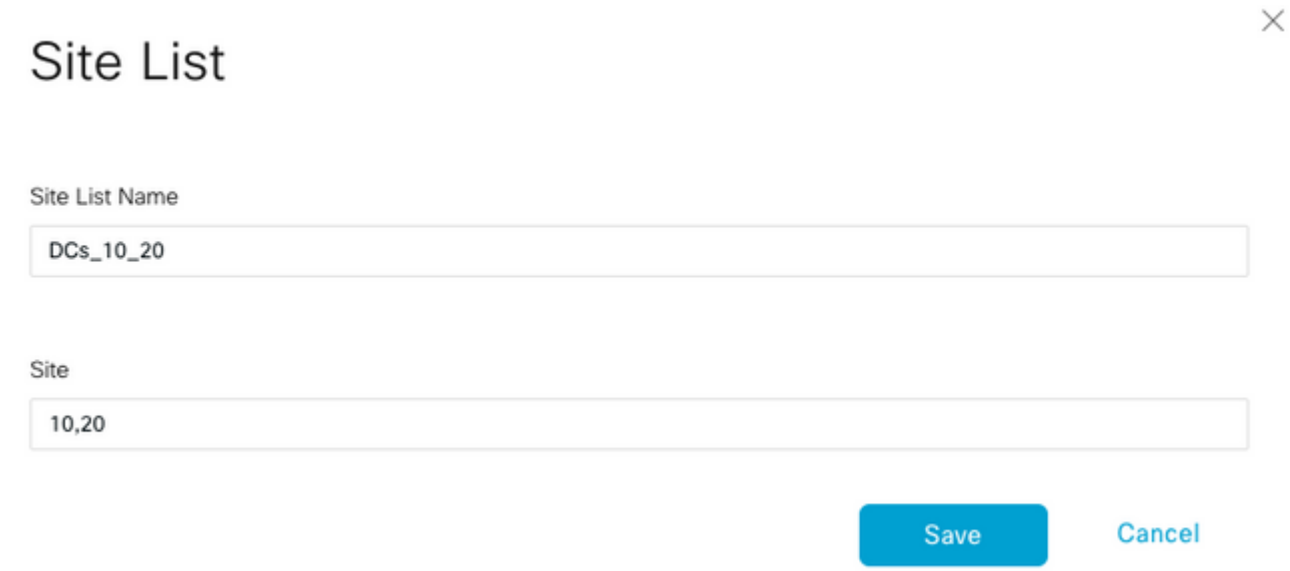
2. Klicken Sie im Abschnitt "Create Groups of Interest" (Interessengruppen erstellen) auf **TLOC > New TLOC List (TLOC > Neue TLOC-Liste)**, und fügen Sie in derselben Liste einen Eintrag für den aktiven Hub und einen Eintrag für den Standby-Hub hinzu:



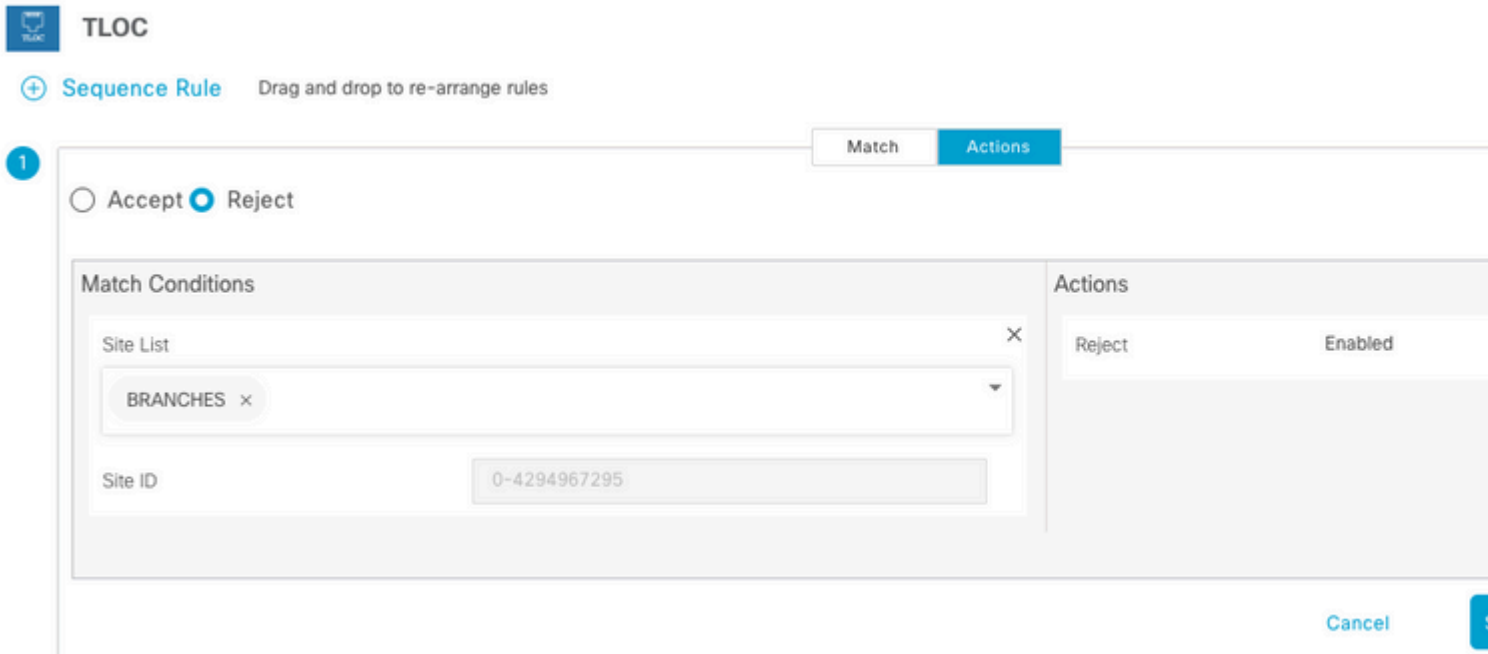
Stellen Sie sicher, dass Sie eine höhere Präferenz für den aktiven Hub und eine niedrigere Präferenz für den Standby-Hub festlegen.

3. Navigieren Sie zu **Site > New Site List** (Website > Neue Standortliste), und erstellen Sie eine Liste für die Außenstellen und eine Liste für die Hub-Standorte:

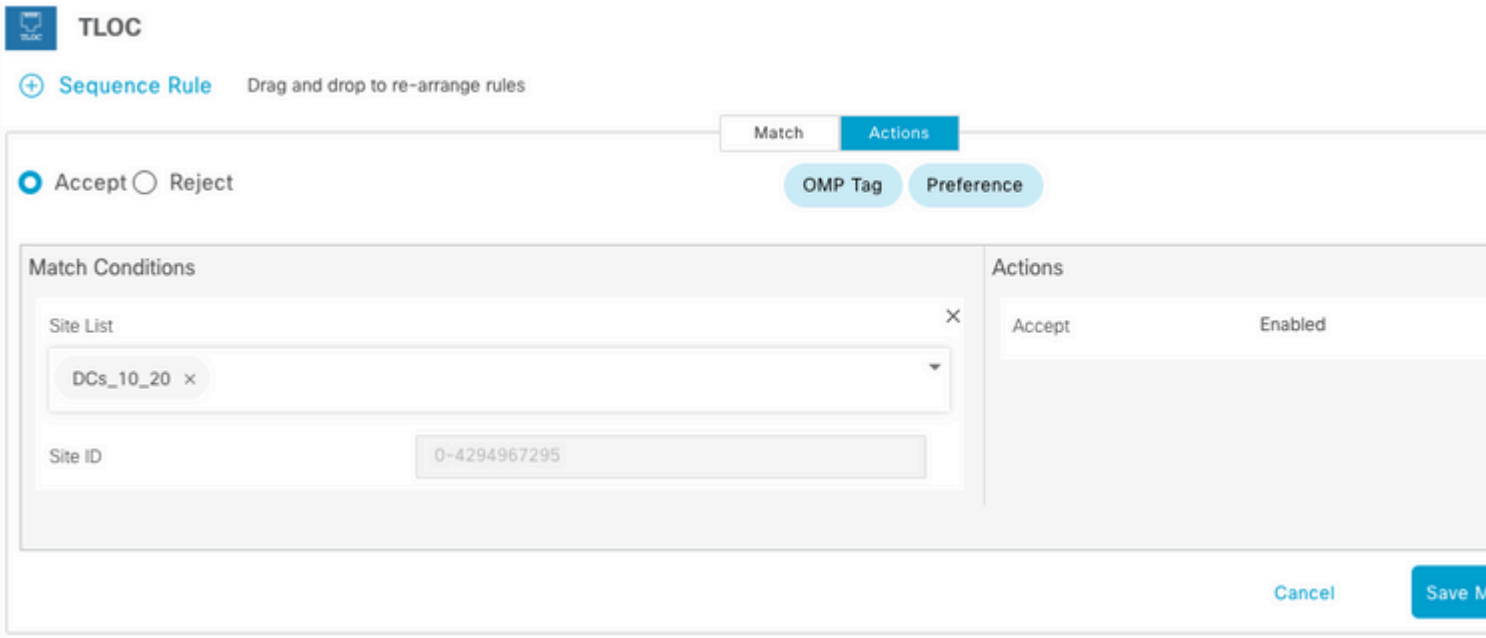




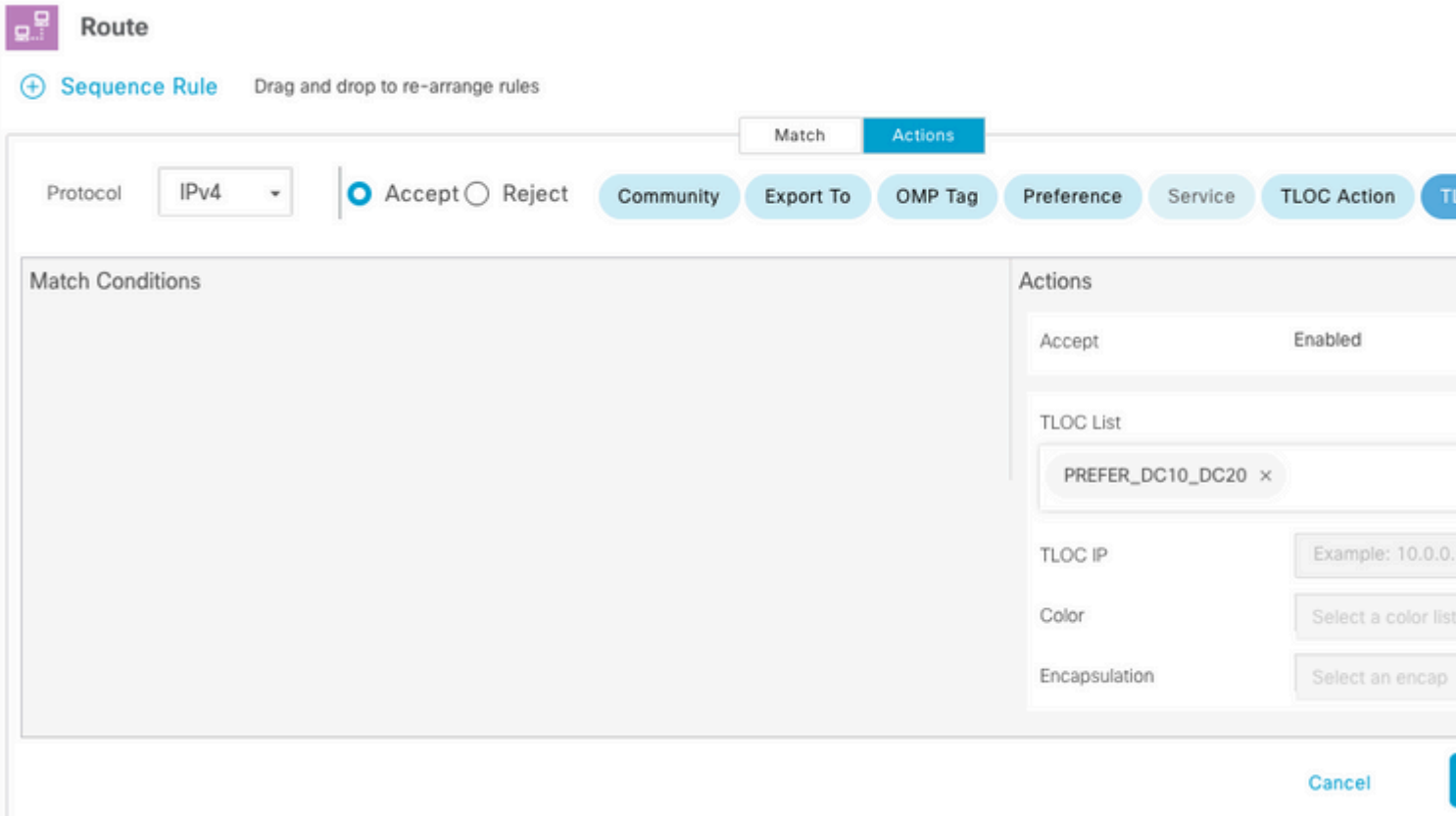
4. Klicken Sie auf **Weiter**. Navigieren Sie im Abschnitt "Topologie konfigurieren und VPN-Mitgliedschaft" zu **Topologie hinzufügen > Benutzerdefiniertes Steuerelement**.
5. Fügen Sie einen Namen und eine Beschreibung für die Richtlinie hinzu.
6. Klicken Sie auf **Sequenztyp > TLOC**, fügen Sie eine **Sequenzregel hinzu.**
7. Wählen Sie **Zuordnen > Standort** und fügen Sie die Liste Standort für die Verzweigungen hinzu, wählen Sie dann **Aktionen > Ablehnen** und klicken Sie auf **Zuordnen und Aktionen speichern**:



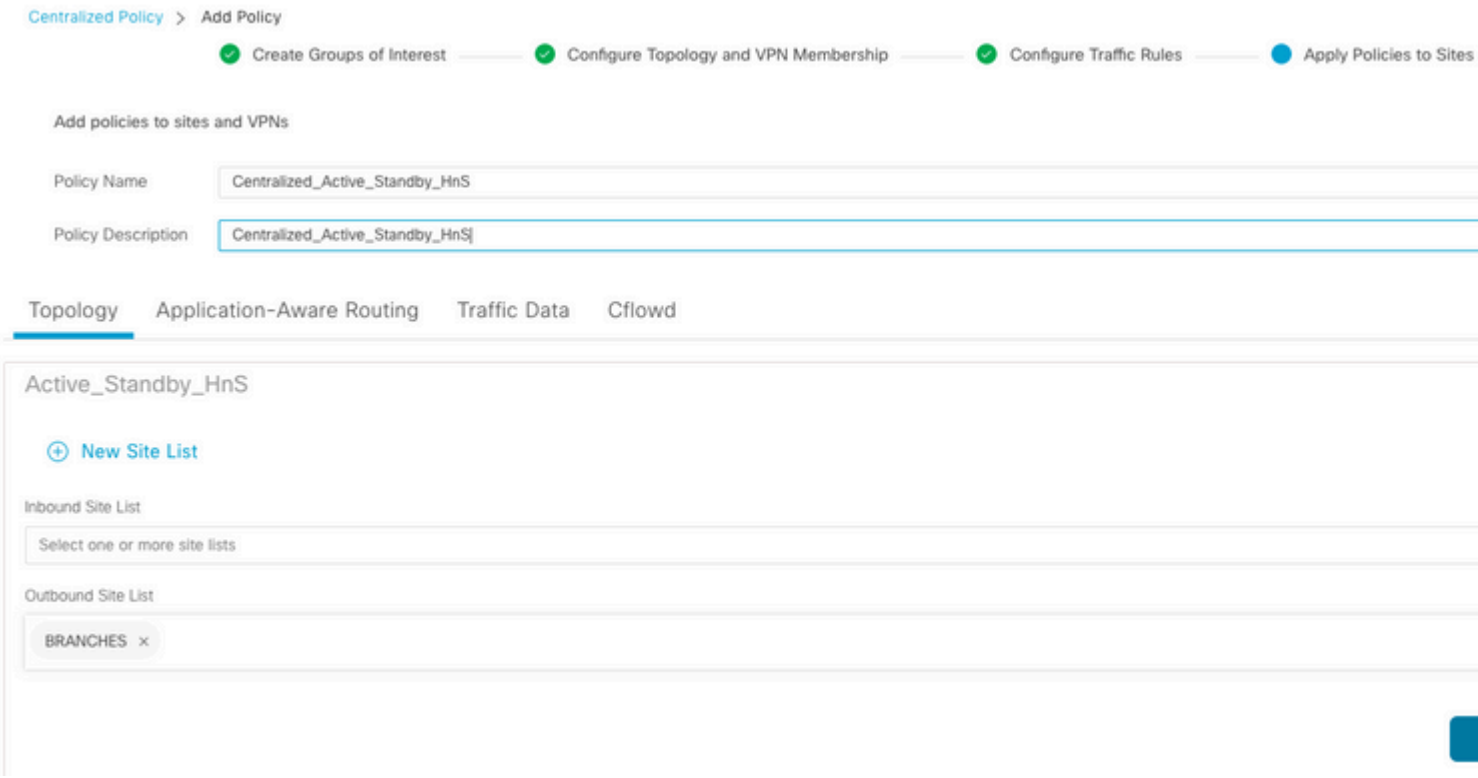
8. Klicken Sie auf **Sequence Rule (Sequenzregel)**, und fügen Sie einen Eintrag hinzu, der mit den Hub-Standorten und Accept (Akzeptieren) übereinstimmt:



9. Navigieren Sie zu **Sequenzart > Weiterleiten, und** fügen Sie eine **Sequenzregel hinzu.**
10. Lassen Sie den Übereinstimmungsabschnitt leer, legen Sie die Aktion auf **Akzeptieren fest**, wählen Sie **TLOC,** fügen Sie die zuvor erstellte TLOC-Liste hinzu, und klicken Sie auf **Übereinstimmende Aktionen speichern**:



11. Klicken Sie auf **Save Control Policy (Steuerungsrichtlinie speichern).**
12. Klicken Sie auf **Weiter**, bis der Abschnitt "Apply Policies to Sites and VPNs" (Richtlinien auf Standorte und VPNs anwenden) angezeigt wird.
13. Im Abschnitt "Topologie" wird die Kontrollrichtlinie angezeigt. Klicken Sie auf "**Neue Standortliste",** wählen Sie die Liste der Verzweigungen für die Liste der ausgehenden Standorte aus, und klicken Sie auf **Hinzufügen**:

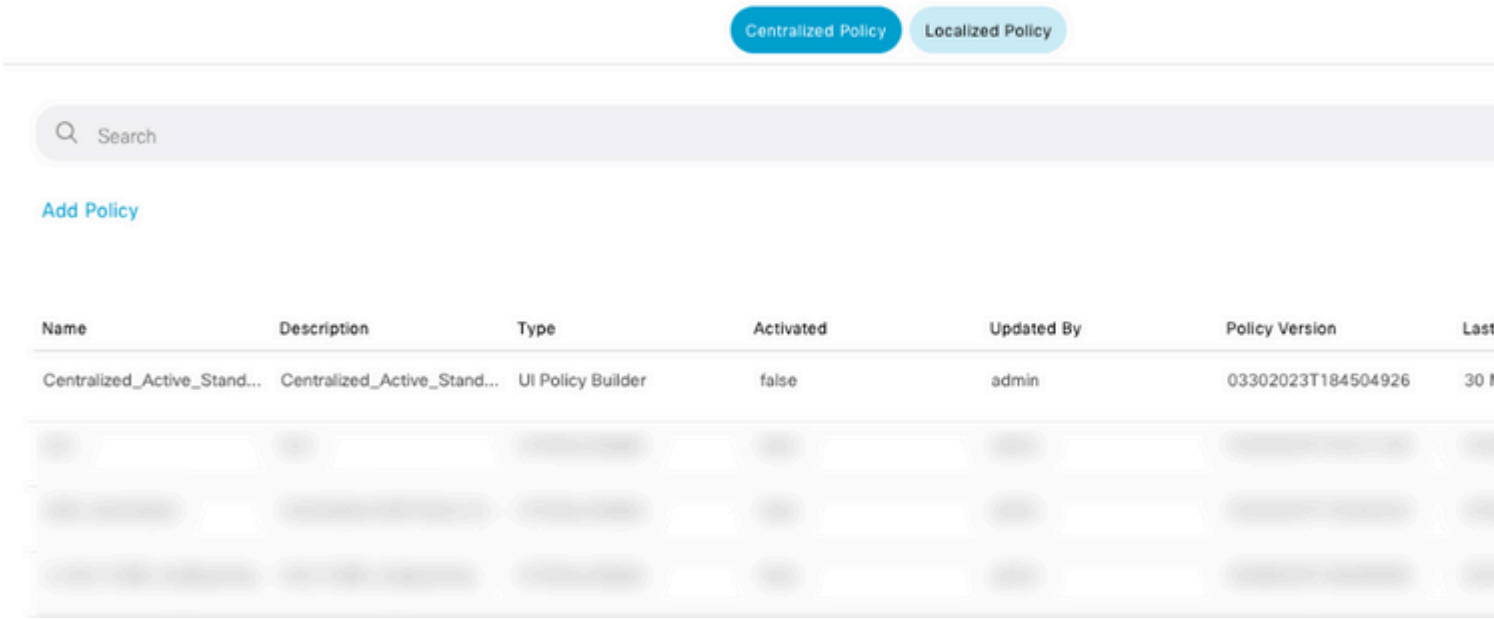


14. Klicken Sie auf **Vorschau**, und überprüfen Sie die Richtlinie.

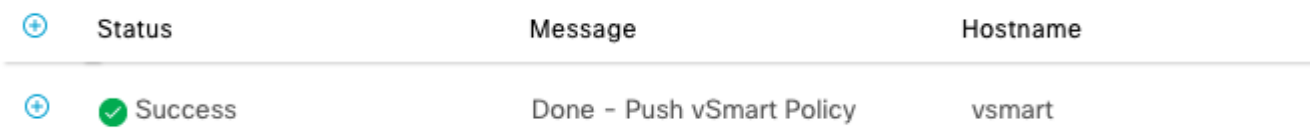
```
viptela-policy:policy
 control-policy Active_Standby_HnS
    sequence 1
     match tloc
      site-list BRANCHES
     !
     action reject
     !
    !
    sequence 11
     match tloc
      site-list DCs_10_20
     !
     action accept
     !
    !
    sequence 21
     match route
      prefix-list _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. Klicken Sie auf **Richtlinie speichern.**
16. Klicken Sie im Menü Centralized Policy (Zentrale Richtlinie) auf die 3 Punkte rechts neben der neu erstellten Richtlinie, und wählen Sie **Activate (Aktivieren) aus.**



17. Sobald die Aufgabe abgeschlossen ist, wird der Status Erfolgreich angezeigt.



Überprüfung

Vergewissern Sie sich, dass die Richtlinie auf vSmart mit den folgenden Befehlen erstellt wird:

<#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#
```

> **Hinweis**: Dies ist eine Kontrollrichtlinie. Sie wird auf den vSmart angewendet und ausgeführt und nicht in die Edge-Geräte verschoben. "**show sdwan policy from-vsmart**" zeigt die Richtlinie nicht auf den Edge-Geräten an.

Fehlerbehebung

Hilfreiche Befehle zur Fehlerbehebung.

Bei 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>
```

Am cEdge:

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

Beispiel:

Vergewissern Sie sich, dass nur die BFD-Sitzung von der Außenstelle zu den Hubs gebildet wird:

<#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
```

Überprüfen Sie, ob Routen von anderen Zweigstellen über den aktiven Hub mit der Präferenz 1000 bevorzugt werden:

<#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
```

Zugehörige Informationen

Konfigurationsleitfaden für Cisco SD-WAN-Richtlinien, Cisco IOS XE Version 17.x

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.