

# Configurazione della topologia hub e spoke attivo/standby su SD-WAN

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene descritto come configurare e convalidare una topologia Hub e Spoke in standby attivo su Cisco SD-WAN.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco SD-WAN
- Interfaccia CLI (Command Line Interface) Cisco IOS-XE® di base

### Componenti usati

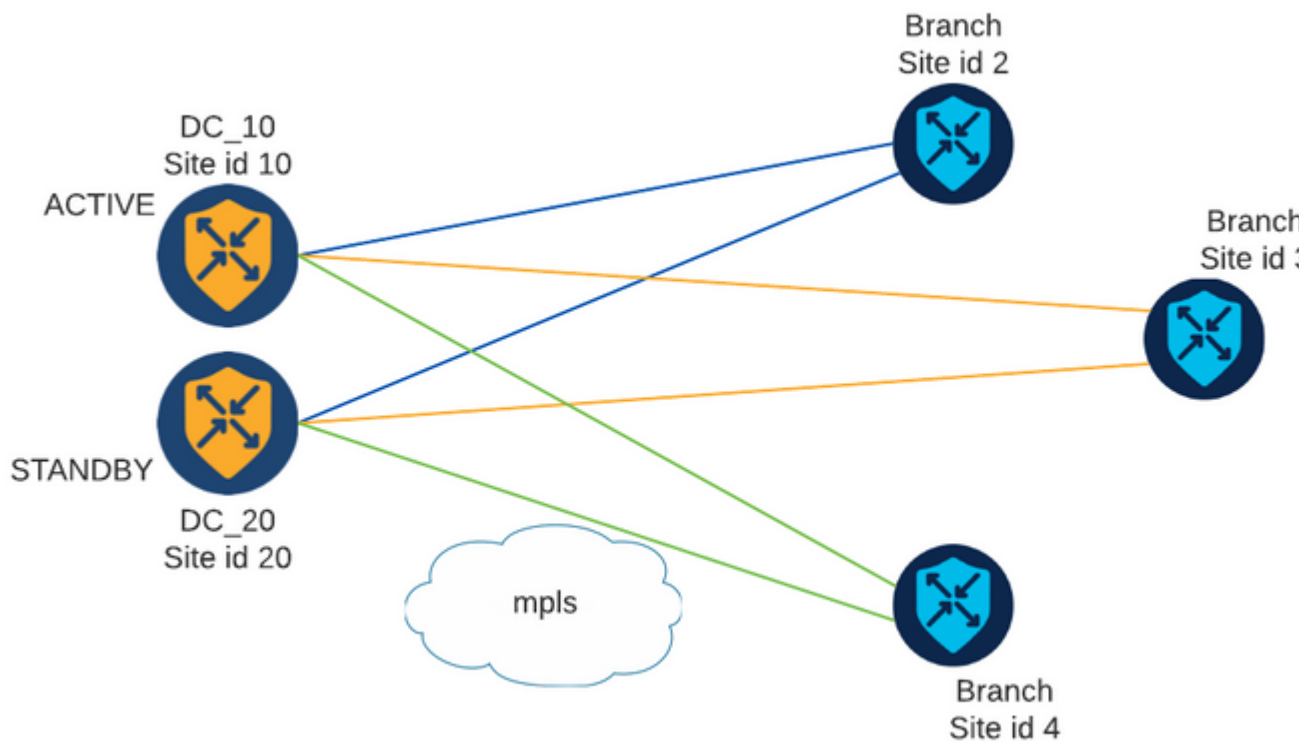
Questo documento si basa sulle seguenti versioni software e hardware:

- C800V versione 17.6.3a
- vManage versione 20.6.3.1
- vSmart versione 20.6.3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Configurazione

### Esempio di rete



Sono disponibili due hub con ID sito 10 e 20. L'ID sito 10 funge da hub attivo e l'ID sito 20 da hub di standby. Le diramazioni possono comunicare tra loro, ma tutte le comunicazioni devono passare attraverso l'hub. Non è necessario creare tunnel tra i siti di diramazione.

## Configurazioni

1. Accedere a vManage e selezionare **Configurazione > Criteri**, quindi fare clic su **Aggiungi criterio**.
2. Nella sezione Crea gruppi di interesse, fare clic su **TLOC > Nuovo elenco TLOC** e aggiungere una voce per l'hub attivo e una per l'hub di standby nello stesso elenco:

## TLOC List



List Name

PREFER\_DC10\_DC20

TLOC IP

Color

Encap

Preference

10.10.10.1

mpls

ipsec

1000



10.10.10.2

mpls

ipsec

500



+ Add TLOC

Cancel

Save

Accertarsi di impostare una preferenza maggiore per l'hub attivo e una preferenza minore per l'hub di standby.

3. Passare a **Sito > Nuovo elenco siti** e creare un elenco per i siti di succursale e un elenco per i siti hub:

## Site List



Site List Name

BRANCHES

Site

2-4

Save

Cancel

# Site List



Site List Name

DCs\_10\_20

Site

10,20

Save

Cancel

4. Fare clic su **Avanti**. Nella sezione Configurazione topologia e appartenenza VPN passare a **Aggiungi topologia > Controllo personalizzato**.
5. Aggiungere un nome e una descrizione per il criterio.
6. Fare clic su **Tipo di sequenza > TLOC**, quindi aggiungere una **regola di sequenza**.
7. Scegliere **Confronta > Sito** e aggiungere l'elenco Sito per le filiali, quindi scegliere **Azioni > Rifiuta** e fare clic su **Salva corrispondenza e azioni**:



TLOC

+ Sequence Rule Drag and drop to re-arrange rules

1

Match

Actions

Accept  Reject

Match Conditions

Site List

BRANCHES

Site ID

0-4294967295

Actions

Reject

Enabled

Cancel

8. Fare clic su **Regola sequenza** e aggiungere una voce corrispondente ai siti hub e Accetta:

**TLOC**

**Sequence Rule** Drag and drop to re-arrange rules

Match **Actions**

Accept  Reject

OMP Tag Preference

Match Conditions

Site List

Site ID

Actions

Accept Enabled

Cancel Save M

9. Passare a **Tipo di sequenza > Ciclo di lavorazione**, aggiungi **regola sequenza**.

10. Lasciare vuota la sezione **Corrispondenza**, impostare l'azione come **Accetta**, scegliere **TLOC**, aggiungere l'elenco TLOC creato in precedenza e fare clic su **Salva corrispondenza e azioni**:

**Route**

**Sequence Rule** Drag and drop to re-arrange rules

Match **Actions**

Protocol   Accept  Reject

Community Export To OMP Tag Preference Service **TLOC Action**

Match Conditions

Actions

Accept Enabled

TLOC List

TLOC IP

Color

Encapsulation

Cancel

11. Fare clic su **Salva criteri di controllo**.

12. Fare clic su **Avanti** fino alla sezione **Applica criteri a siti e VPN**.

13. Nella sezione **Topologia** vengono visualizzati i criteri di controllo, fare clic su **Nuovo elenco siti**, scegliere l'elenco **Rami** per l'elenco dei siti in uscita e fare clic su **Aggiungi**:

Add policies to sites and VPNs

Policy Name

Centralized\_Active\_Standby\_HnS

Policy Description

Centralized\_Active\_Standby\_HnS

Topology

Application-Aware Routing

Traffic Data

Cflowd

Active\_Standby\_HnS

+ New Site List

Inbound Site List

Select one or more site lists

Outbound Site List

BRANCHES x

14. Fare clic su **Anteprima** ed esaminare il criterio.

```

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. Fare clic su **Salva criterio**.

16. Nel menu Criteri centralizzati, fare clic sui 3 punti a destra del nuovo criterio creato e selezionare **Attiva**.

The screenshot shows a web interface for managing policies. At the top, there are two tabs: "Centralized Policy" (selected) and "Localized Policy". Below the tabs is a search bar with a magnifying glass icon and the text "Search". Underneath the search bar is a link labeled "Add Policy". The main part of the interface is a table with the following columns: Name, Description, Type, Activated, Updated By, Policy Version, and Last. The table contains one visible row with the following data:

Name	Description	Type	Activated	Updated By	Policy Version	Last
Centralized_Active_Stand...	Centralized_Active_Stand...	UI Policy Builder	false	admin	03302023T184504926	30 M

17. Una volta completato il task, viene visualizzato lo stato Riuscito.

Status	Message	Hostname
Success	Done - Push vSmart Policy	vsmart

## Verifica

Verificare che il criterio sia stato creato su vSmart con questi comandi:

```
<#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#
```

---

**Nota:** si tratta di un criterio di controllo. Viene applicato ed eseguito su vSmart e non viene inserito nei dispositivi periferici. Il comando "**show sdwan policy from-vsmart**" non visualizza il criterio sui dispositivi Edge.

---

## Risoluzione dei problemi

Comandi utili per la risoluzione dei problemi.

Su 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 tllocs advertised <detail>  
show omp tllocs received <detail>
```

Su cEdge:

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

Esempio:

Confermare che solo la sessione BFD sia formata da un ramo agli hub:

```
<#root>
```

```
Branch_02#
```

```
show sdwan bfd sessions
```

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP	DST PUBLIC IP	DST PUBLIC PORT	ENCAP	DETECT 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

Verificare che le route da altre filiali siano preferite tramite l'hub attivo con preferenza 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

## **Informazioni correlate**

[Guida alla configurazione delle policy Cisco SD-WAN, Cisco IOS XE release 17.x](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).