

Pourquoi définir tloc-action dans une stratégie de contrôle centralisée ne fonctionne pas ?

Contenu

[Introduction](#)

[Topologie](#)

[Configuration](#)

[Problème](#)

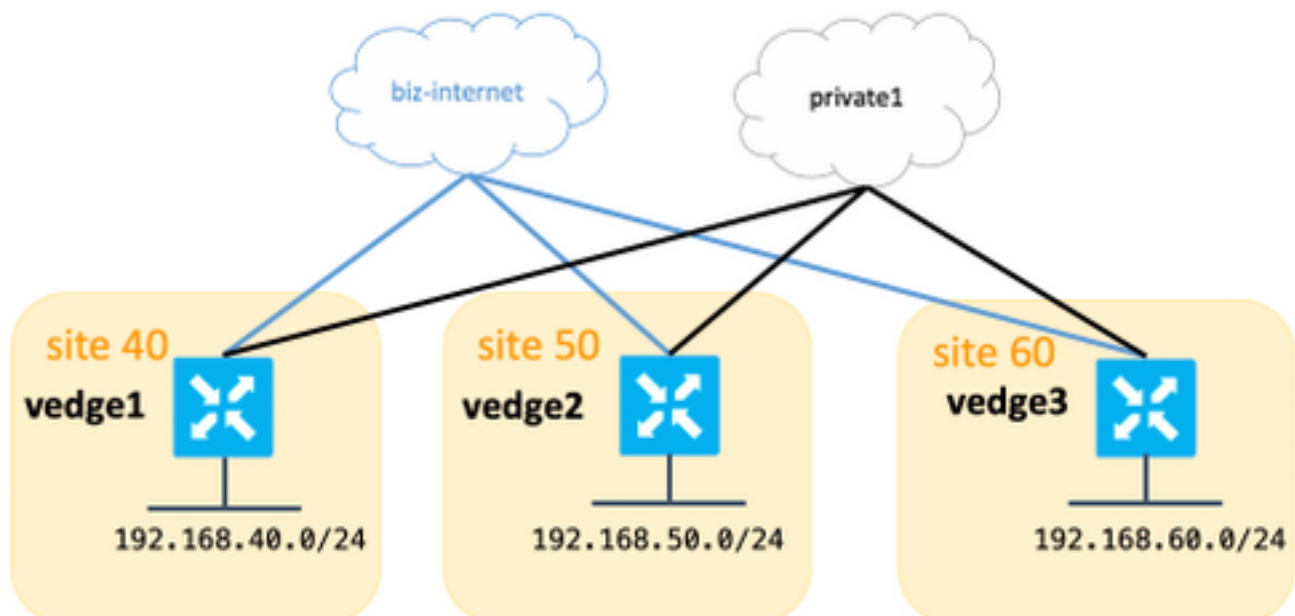
[Solution](#)

Introduction

Ce document décrit le problème qui se produit avec les routes OMP (Overlay Management Protocol) si la commande **set tloc-action** dans la stratégie de contrôle centralisé est utilisée et explique pourquoi cela se produit et comment le résoudre.

Topologie

Afin de mieux comprendre le problème, référez-vous à ce schéma de topologie simple qui décrit la configuration :



Configuration

Aux fins de cet article, vEdge et le logiciel Controllers version 18.3.5 ont été utilisés.

Tous les sites ont une connexion à **biz-internet** et **privé** couleurs, ce tableau résume la

configuration.

nom de l'hôte	id-site	system-ip	adresse IP sur le lien interne	adresse IP sur la liaison privée
vEdge1	40	192.168.30.104	192.168.10.181	192.168.110.181
vEdge2	50	192.168.30.105	192.168.10.182	192.168.110.182
vEdge3	60	192.168.30.106	192.168.10.183	192.168.110.183
vSmart	1	192.168.30.103		

Il n'existe aucune configuration spéciale sur les contours. La configuration avec deux routes par défaut est assez simple et omise ici pour plus de concision.

Sur vSmart, cette configuration a été appliquée :

```
lists
vpn-list VPN_40
  vpn 40
!
site-list sites_40_60
  site-id 40
  site-id 60
!
prefix-list SITE_40
  ip-prefix 192.168.40.0/24
!
prefix-list SITE_60
  ip-prefix 192.168.60.0/24
!
!
control-policy REDIRECT_VIA_VEDGE2
sequence 10
match route
  prefix-list SITE_40
!
action accept
set
  tloc-action primary
```


privatel ipsec -

En même temps, des tunnels de plan de données sur **biz-internet** fonctionnent et fonctionnent entre vEdge1 et vEdge3 :

vedge1# show bfd sessions

DST PUBLIC SYSTEM IP IP TRANSITIONS	SITE ID	STATE	DST PUBLIC PORT	SOURCE TLOC COLOR ENCAP	DETECT MULTIPLIER	REMOTE TLOC TX INTERVAL(msec)	SOURCE IP	UPTIME	
192.168.30.105	50	up		biz-internet			biz-internet	192.168.109.181	
192.168.109.182			12366	ipsec	7		1000		0:02:52:22 0
192.168.30.105	50	up		privatel			privatel	192.168.110.181	
192.168.110.182			12366	ipsec	7		1000		0:00:00:12 1
192.168.30.106	60	up		biz-internet			biz-internet	192.168.109.181	
192.168.109.183			12366	ipsec	7		1000		0:02:52:22 0
192.168.30.106	60	up		privatel			privatel	192.168.110.181	
192.168.110.183			12366	ipsec	7		1000		0:00:56:28 0

vedge3# show bfd sessions

DST PUBLIC SYSTEM IP IP TRANSITIONS	SITE ID	STATE	DST PUBLIC PORT	SOURCE TLOC COLOR ENCAP	DETECT MULTIPLIER	REMOTE TLOC TX INTERVAL(msec)	SOURCE IP	UPTIME	
192.168.30.104	40	up		biz-internet			biz-internet	192.168.109.183	
192.168.109.181			12366	ipsec	7		1000		0:02:54:25 0
192.168.30.104	40	up		privatel			privatel	192.168.110.183	
192.168.110.181			12366	ipsec	7		1000		0:00:58:30 0
192.168.30.105	50	up		biz-internet			biz-internet	192.168.109.183	
192.168.109.182			12366	ipsec	7		1000		0:02:54:25 0
192.168.30.105	50	up		privatel			privatel	192.168.110.183	
192.168.110.182			12366	ipsec	7		1000		0:00:57:26 0

Dans la sortie détaillée show omp route, vous voyez le **tloc** défini correctement et aussi le **ultimate-tloc** est défini, mais l'état est **Inv,U** et la raison de perte est **non valide** :

vedge3# show omp routes 192.168.40.0/24 detail

```
-----  
omp route entries for vpn 40 route 192.168.40.0/24  
-----  
RECEIVED FROM:  
peer 192.168.30.103  
path-id 19  
label 1002 status Inv,U loss-reason invalid lost-to-peer 192.168.30.103 lost-to-path-id 20  
Attributes: originator 192.168.30.104 type installed tloc 192.168.30.105, biz-internet, ipsec  
ultimate-tloc 192.168.30.104, biz-internet, ipsec -- primary domain-id not set overlay-id 1  
site-id 40 preference not set tag not set origin-PROTO connected origin-metric 0 as-path not set  
unknown-attr-len not set RECEIVED FROM: peer 192.168.30.103 path-id 20 label 1002 status C,I,R  
loss-reason not set lost-to-peer not set lost-to-path-id not set Attributes: originator  
192.168.30.104 type installed tloc 192.168.30.104, biz-internet, ipsec ultimate-tloc not set
```

```
domain-id not set overlay-id 1 site-id 40 preference not set tag not set origin-proto connected
origin-metric 0 as-path not set unknown-attr-len not set
```

Note: Un TLOC ultime est le TLOC auquel le saut intermédiaire construit le tunnel de plan de données (IPsec ou Generic Routing Encapsulation (GRE)) afin d'atteindre la destination finale.

Note: tloc-action n'est pris en charge de bout en bout que si la couleur de transport est identique d'un site au saut intermédiaire et du saut intermédiaire à la destination finale. Si le transport utilisé pour atteindre le saut intermédiaire à partir d'un site est d'une couleur différente du transport utilisé à partir du saut intermédiaire pour atteindre la destination finale, cela créera un problème avec l'action tloc.

Vous pouvez voir que l'objectif principal n'est pas atteint et que le trafic suit un chemin direct comme on peut le voir sur l'hôte à partir du sous-réseau 192.168.40.0/24 :

```
traceroute -n 192.168.60.20
traceroute to 192.168.60.20 (192.168.60.20), 30 hops max, 60 byte packets
 1 192.168.40.104 0.288 ms 0.314 ms 0.266 ms
 2 192.168.60.106 0.911 ms 1.045 ms 1.140 ms
 3 192.168.60.20 1.213 ms !X 1.289 ms !X 1.224 ms !X
```

Solution

En tant que cause première, on a d'abord suspecté un défaut logiciel [CSCvm64622](#) a été touché, mais après une enquête supplémentaire, il a été constaté qu'il s'agissait d'une mauvaise configuration en raison du fait que la documentation du produit n'était pas claire au sujet des exigences d'action tloc. Ainsi, la section [documentation](#) relative à l'action TLOC est mise à jour avec ceci :

Remarque : Si l'action est **acceptez set tloc-action**, configurez le **service TE** sur la destination intermédiaire.

Par conséquent, dans le scénario courant, la configuration **du service TE** est requise sur vEdge2 afin de rendre la politique de contrôle centralisé efficace parce que vous utilisez l'ingénierie de trafic (TE) essentiellement par la direction via un chemin arbitraire :

```
vedge2(config)# vpn 40
vedge2(config-vpn-40)# service ?
Possible completions:
  FW  IDP  IDS  TE  netsvc1  netsvc2  netsvc3  netsvc4
vedge2(config-vpn-40)# service TE
vedge2(config-vpn-40)# commit
Commit complete.
```

Il résout le problème avec la stratégie de contrôle depuis que vEdge2 commence à annoncer le service TE :

```
vsmart1# show omp services | b PATH
```

VPN	SERVICE	ORIGINATOR	FROM PEER	PATH ID	LABEL	STATUS

```

40    VPN      192.168.30.104  192.168.30.104  68    1002    C,I,R
                                192.168.30.104  81    1002    C,I,R
40    VPN      192.168.30.105  192.168.30.105  68    1002    C,I,R
                                192.168.30.105  81    1002    C,I,R
40    VPN      192.168.30.106  192.168.30.106  68    1002    C,I,R
                                192.168.30.106  81    1002    C,I,R
40    TE 192.168.30.105 192.168.30.105 68 1007 C,I,R 192.168.30.105 81 1007 C,I,R

```

vEdge1 et vEdge3 installent les routes avec succès maintenant, notez que l'état est défini sur C, I, R :

```
vedge3# show omp routes 192.168.40.0/24 detail
```

```

-----
omp route entries for vpn 40 route 192.168.40.0/24
-----
                RECEIVED FROM:
peer                192.168.30.103
path-id            19 label 1002 status C,I,R loss-reason not set lost-to-peer not set lost-to-path-id
not set Attributes: originator 192.168.30.104 type installed tloc 192.168.30.105, biz-internet,
ipsec ultimate-tloc 192.168.30.104, biz-internet, ipsec -- primary domain-id not set overlay-id
1 site-id 40 preference not set tag not set origin-proto connected origin-metric 0 as-path not
set unknown-attr-len not set RECEIVED FROM: peer 192.168.30.103 path-id 20 label 1002 status R
loss-reason tloc-action lost-to-peer 192.168.30.103 lost-to-path-id 19 Attributes: originator
192.168.30.104 type installed tloc 192.168.30.104, biz-internet, ipsec ultimate-tloc not set
domain-id not set overlay-id 1 site-id 40 preference not set tag not set origin-proto connected
origin-metric 0 as-path not set unknown-attr-len not set vedge3# show ip routes 192.168.40.0/24
| b PROTOCOL PROTOCOL NEXTHOP NEXTHOP NEXTHOP VPN PREFIX PROTOCOL SUB TYPE IF NAME ADDR VPN TLOC
IP COLOR ENCAP STATUS -----
----- 40 192.168.40.0/24 omp - - -
- 192.168.30.105 biz-internet ipsec F,S

```