集中型コントロールポリシーのset tloc-actionが機能しない理由

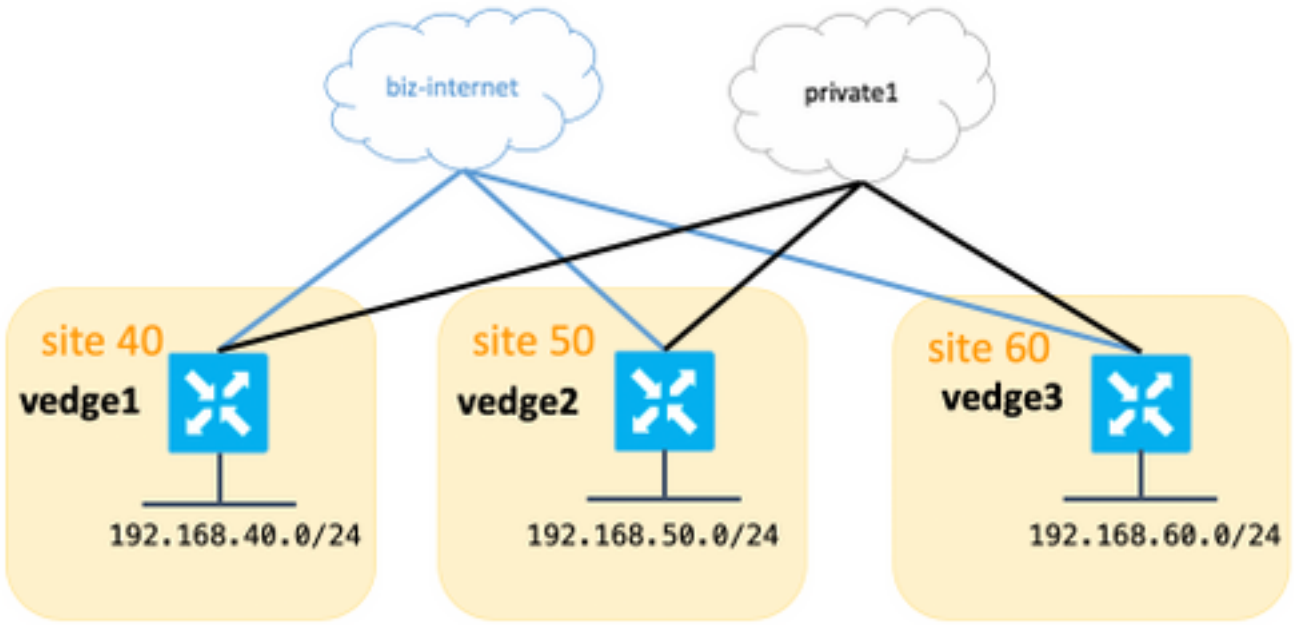
内容

概要

このドキュメントでは、集中制御ポリシーでset tloc-actionコマンドを使用した場合にOverlay Management Protocol(OMP)ルートで発生する問題について説明し、その原因とその解決方法について説明します。

トポロジ

この問題をより深く理解するには、設定を示す次の単純なトポロジ図を参照してください。



コンフィギュレーション

この記事では、vEdgeとコントローラソフトウェアバージョン18.3.5を使用しました。

すべてのサイトがビズー・インターネットとプライベートカラーに接続しています。この表は構成をまとめたものです。

ホスト名	site-id	system-ip	biz-internet link上のip-address	private1リンクのip-address
vEdge1	40	192.168.30.104	192.168.109.181	192.168.110.181
vEdge2	50	192.168.30.105	192.168.109.182	192.168.110.182
vEdge3	60	192.168.30.106	192.168.109.183	192.168.110.183
vsmart	1	192.168.30.103		

vEdgeには特別な設定はありません。2つのデフォルトルートを使用した設定は非常に簡単で、ここでは簡略化のために省略しています。

vSmartでは、次の設定が適用されました。

```
 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
     tloc 192.168.30.105 color biz-internet encap ipsec
    !
   !
  !
```

```
  sequence 20
   match route
    prefix-list SITE_60
   !
   action accept
    set
     tloc-action primary
     tloc 192.168.30.105 color biz-internet encap ipsec
    !
   !
  !
  default-action accept
 !
apply-policy
 site-list sites_40_60
  control-policy REDIRECT_VIA_VEDGE2 out
 !
!
```

このポリシーの主な目的は、中間宛先サイト50を経由してサイト40からサイト60にトラフィックをリダイレクトし、好ましくはビズー・インターネットを使用すること。

問題

show omp routesの出力からは、biz-internet経由のルートをvEdge1、vEdge3にインストールできず、ステータスが[無効(Invalid)]および[未解決(Inv,U)]に設定されていることがわかります。

```
vedge1# show omp routes | b PATH
                                          PATH                      ATTRIBUTE
VPN    PREFIX              FROM PEER      ID     LABEL    STATUS    TYPE       TLOC IP
COLOR            ENCAP  PREFERENCE
-----------------------------------------------------------------------------------------------
-------------------------------------
40     192.168.40.0/24     0.0.0.0        68     1002     C,Red,R   installed  192.168.30.104
biz-internet     ipsec  -
                           0.0.0.0        81     1002     C,Red,R   installed  192.168.30.104
private1         ipsec  -
40     192.168.50.0/24     192.168.30.103 4      1002     C,I,R     installed  192.168.30.105
biz-internet     ipsec  -
                           192.168.30.103 10     1002     C,I,R     installed  192.168.30.105
private1         ipsec  -
40 192.168.60.0/24 192.168.30.103 8 1002 Inv,U installed 192.168.30.105 biz-internet ipsec -
192.168.30.103 9 1002 C,I,R installed 192.168.30.106 biz-internet ipsec -

vedge3# show omp routes | b PATH
                                          PATH                      ATTRIBUTE
VPN    PREFIX              FROM PEER      ID     LABEL    STATUS    TYPE       TLOC IP
COLOR            ENCAP  PREFERENCE
-----------------------------------------------------------------------------------------------
-------------------------------------
40 192.168.40.0/24 192.168.30.103 19 1002 Inv,U installed 192.168.30.105 biz-internet ipsec -
192.168.30.103 20 1002 C,I,R installed 192.168.30.104 biz-internet ipsec - 40 192.168.50.0/24
192.168.30.103 16 1002 C,I,R installed 192.168.30.105 biz-internet ipsec - 192.168.30.103 21
1002 C,I,R installed 192.168.30.105 private1 ipsec - 40 192.168.60.0/24 0.0.0.0 68 1002 C,Red,R
installed 192.168.30.106 biz-internet ipsec - 0.0.0.0 81 1002 C,Red,R installed 192.168.30.106
private1 ipsec -
```

同時に、vEdge1とvEdge3の間で動作するビズズ・インターネット上のデータプレーントンネルも表示されます。

```
vedge1# show bfd sessions
                                       SOURCE TLOC      REMOTE TLOC
DST PUBLIC                        DST PUBLIC         DETECT      TX
SYSTEM IP        SITE ID  STATE       COLOR            COLOR           SOURCE IP
IP                                PORT        ENCAP  MULTIPLIER  INTERVAL(msec) UPTIME
TRANSITIONS
-----------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
-------------
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          private1         private1         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          private1         private1         192.168.110.181
192.168.110.183                   12366       ipsec  7           1000           0:00:56:28      0


vedge3# show bfd sessions
                                       SOURCE TLOC      REMOTE TLOC
DST PUBLIC                        DST PUBLIC         DETECT      TX
SYSTEM IP        SITE ID  STATE       COLOR            COLOR           SOURCE IP
IP                                PORT        ENCAP  MULTIPLIER  INTERVAL(msec) UPTIME
TRANSITIONS
-----------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
-------------
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          private1         private1         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          private1         private1         192.168.110.183
192.168.110.182                   12366       ipsec  7           1000           0:00:57:26      0
```

show omp route detailed出力では、tlocが正しく設定され、unestimate-tlocが設定されていますが、ステータスがInv、Uで、損失理由が無効です。

```
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
```

注：ultimate-tlocは、中間ホップが最終宛先に到達するためにデータプレーントンネル(IPsecまたはGeneric Routing Encapsulation(GRE))を構築するTLOCです。

> **注：tloc-actionは、サイトから中間ホップ、および中間ホップから最終宛先までのトランスポートの色が同じ場合にのみ、エンドツーエンドでサポートされます。サイトから中間ホップに到達するために使用したトランスポートが、最終的な宛先に到達するために中間ホップから使用したトランスポートと異なる色である場合、tloc-actionに問題が発生します。**

主な目標が達成されず、トラフィックは192.168.40.0/24サブネットからホスト上で確認できる直接パスに従います。

```
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
```

解決方法

根本的な原因として、最初はソフトウェア不具合CSCvm64622 ヒットしたが、追加調査の後、製品ドキュメントがtloc-action要件について明確でなかったために誤設定であることが**判明し**ました。そのため、TLOCのアクションに関するドキュメントセクションは、次のように更新されます。

> **注**：アクションが**set tloc-action**を受け入れる場合は、中間**先にサービス**TEを設定します。

したがって、現在のシナリオで**は、vEdge2で集中型の制御ポリシーを機能させるため**に、トラフィックエンジニアリング(TE)を基本的に任意のパスでステアリングして使用するため、TE設定が必要です。

```
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.
```

vEdge2がTEサービスのアドバタイズを開始するため、コントロールポリシーの問題が解決されます。

```
vsmart1# show omp services | b PATH
                                                    PATH
VPN    SERVICE  ORIGINATOR      FROM PEER        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とvEdge3はルートを正常にインストールします。ステータスが**C、I、Rに設定されています**。

```
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
```