Utilisez EEM avec l'IP SLA pour dépanner des instabilités ou la perte de paquets d'IGP à travers un tunnel VPN

Contenu

Introduction

Beaucoup de valises sont ouvertes avec le symptôme « instabilités EIGRP/OSPF/BGP au-dessus de mon tunnel DMVPN/GRE/sVTI ». Afin de dépanner cette question, la première question qui doit être répondue est, « est ceci un VPN, un protocole de routage ou une question ISP ? »

La manière que ceci peut être testé est de découvrir si le transport sous-jacent fonctionne toujours correctement pendant la période de l'instabilité/de panne. Malheureusement, ces données sont habituellement POST-événement passé en revue et sont impossibles de déterminer cette partie de données. Ce document fournit des informations au sujet de l'utilisation des accords de niveau de service IP (SLA), des objets de piste et du gestionnaire encastré d'événement (EEM) afin de collecter ces informations pendant la période de la question.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- IP SLA
- EEM

Composants utilisés

Les informations dans ce document sont basées sur le code de version de logiciel 15.2(4)M de

Cisco IOS® sur des 881, mais n'importe quel code récent (15.0(1)M ou plus tard) aura ce support.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

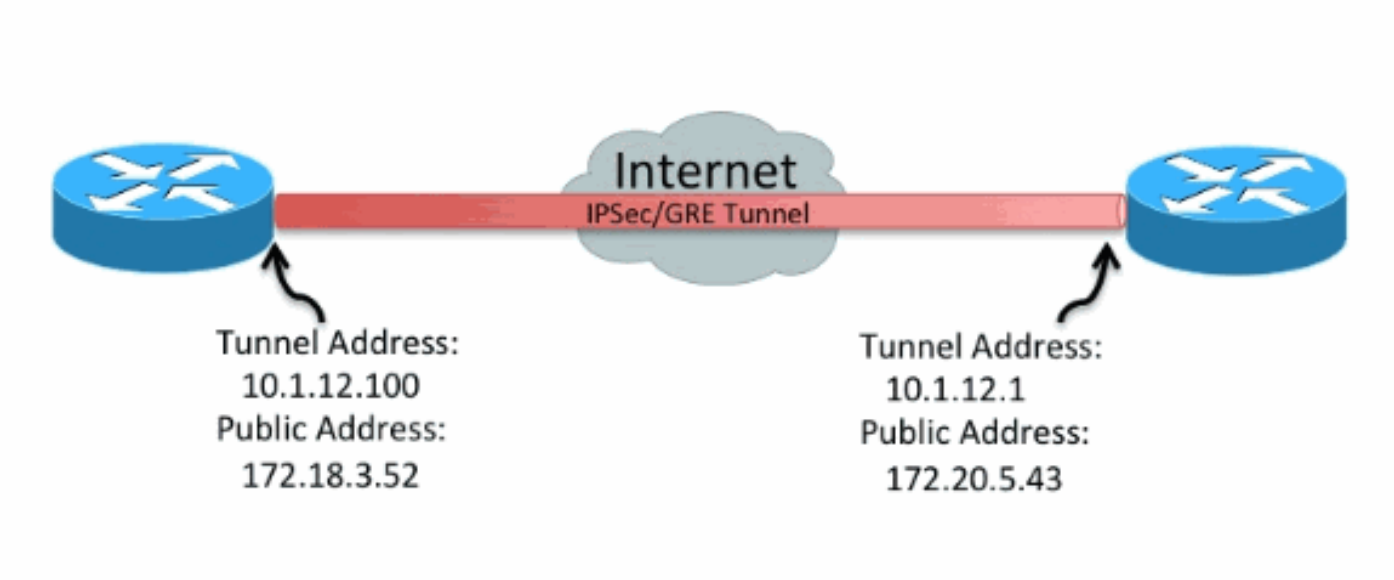
Les informations de caractéristique

IP SLA sont des processus qui fonctionnent sur le routeur à l'arrière-plan qui testent un nombre variable d'états de réseau. Dans cette connectivité IP générale de document est testé utilisant le test de « icmp-echo ».

Ensuite que l'état IP SLA est dépisté utilisant un objet de piste. Puis, utilisant un applet EEM, l'état du réseau dans la mémoire tampon de Syslog peut être enregistré en agissant quand les modifications d'état de l'objet de piste.

L'état de réseau étant inclus en ligne avec les Syslog, vous pouvez rétroactivement comprendre l'état actuel du réseau pendant l'instabilité/panne et déterminer s'il y avait un crypto, le transport, ou la question d'IGP.

Dépannage de la méthodologie



Deux SLA distinct sont utilisés pour dépister chaque couche de connectivité IP :

- Adresse IP publique à l'adresse IP publique (172.18.3.52 ------> 172.20.5.43)`ip sla 100`
  `icmp-echo 172.20.5.43 source-interface FastEthernet4`
  `frequency 5`
  `ip sla schedule 100 life forever start-time now`
- Adresse IP de tunnel pour percer un tunnel l'adresse IP (10.1.12.100 ----> 10.1.12.1)`ip sla 200`
  `icmp-echo 10.1.12.1 source-interface Tunnel100`
  `frequency 5`
  `ip sla schedule 200 life forever start-time now`

Ces le SLA enverra à un paquet simple de ping toutes les 5 secondes aux pairs définis. Si le ping

répond SLA sera « CORRECT » marqué. S'il ne répond pas ce sera « délai d'attente » marqué. Puis, des objets de piste sont utilisés pour dépister l'état de SLA.

- Adresse IP publique à la piste d'adresse IP publique`track 100 ip sla 100`
  `delay down 15 up 15`
- Adresse IP de tunnel pour percer un tunnel la piste d'adresse IP`track 200 ip sla 200`
  `delay down 15 up 15`

Quand l'objet de piste change, un message peut être inséré dans les Syslog.

- Adresse IP publique à la piste d'adresse IP publique`event manager applet ipsla100down`
  `event track 100 state down`
  `action 1.0 syslog msg "Physical SLA probe failed!"`
  `event manager applet ipsla100up`
  `event track 100 state up`
  `action 1.0 syslog msg "Physical SLA probe came up!"`
- Adresse IP de tunnel pour percer un tunnel la piste d'adresse IP`event manager applet ipsla200down`
  `event track 200 state down`
  `action 1.0 syslog msg "Tunnel SLA probe failed!"`
  `event manager applet ipsla200up`
  `event track 200 state up`
  `action 1.0 syslog msg "Tunnel SLA probe came up!"`

Analyse de données

Quand une panne se produit, collectez la sortie du **show log command**.

Recherchez les messages de SLA ci-dessus.

Pendant la panne, si vous voyez :

- Les deux échouer SLA. Ceci signifie :La Connectivité de la couche 3 à travers l'Internet entre les deux pairs a été interrompue. Ceci a besoin de recherches plus approfondies.Il n'y a aucun problème avec le tunnel. Il manque parce que c'est une victime de l'interruption ci-dessus.
- SLA physique n'échoue pas mais SLA de tunnel fait. Ceci signifie :La Connectivité de la couche 3 à travers l'Internet entre les deux pairs fonctionne correctement.Il y a un problème avec le tunnel. Les recherches plus approfondies du tunnel sont nécessaires.
- Ni l'un ni l'autre de l'échouer SLA. Ceci signifie :La Connectivité de la couche 3 à travers l'Internet entre les deux pairs fonctionne correctement.La Connectivité d'unicast de la couche 3 à travers le tunnel entre les deux pairs fonctionne correctement.La connectivité multicast de la couche 3 à travers le tunnel est inconnue. Ceci peut être testé en cinglant l'adresse de multidiffusion utilisée par l'IGP.Si les travaux de test ci-dessus alors ceci indiquent une question d'application (EIGRP/OSFP/BGP). Davantage d'enquête de protocole est nécessaire.

Informations connexes

- Support et documentation techniques - Cisco Systems