Dépannage IOS par VRF TACACS+

Contenu

Introduction

TACACS+ est largement utilisé comme protocole d'authentification pour authentifier les utilisateurs sur les périphériques réseau. De plus en plus d'administrateurs séparent leur trafic de gestion à l'aide de VRF (VPN Routing and Forwarding). Par défaut, AAA sur IOS utilise la table de routage par défaut pour envoyer des paquets. Ce document décrit comment configurer et dépanner TACACS+ lorsque le serveur est dans un VRF.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- TACACS+
- VRF

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

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

Informations sur les fonctionnalités

Essentiellement, un VRF est une table de routage virtuelle sur le périphérique. Lorsque l'IOS prend une décision de routage si la fonction ou l'interface utilise un VRF, les décisions de routage sont prises par rapport à cette table de routage VRF. Sinon, la fonction utilise la table de routage globale. Dans cet esprit, voici comment configurer TACACS+ pour utiliser un VRF (configuration appropriée en gras) :

```
version 15.2
service config
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname vrfAAA
!
boot-start-marker
boot-end-marker
!
aaa new-model
!
aaa group server tacacs+ management
 server-private 192.0.2.4 key cisco
 server-private 192.0.2.5 key cisco
 ip vrf forwarding blue
 ip tacacs source-interface GigabitEthernet0/0
!
aaa authentication login default group management local
aaa authorization exec default group management if-authenticated
aaa accounting exec default start-stop group management
!
aaa session-id common
!
no ipv6 cef
!
ip vrf blue
!
no ip domain lookup
ip cef
!
interface GigabitEthernet0/0
 ip vrf forwarding blue
 ip address 203.0.113.2 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1
!
line con 0
line aux 0
line vty 0 4
 transport input all
```

Comme vous pouvez le voir, il n'existe aucun serveur TACACS+ défini globalement. Si vous migrez les serveurs vers un VRF, vous pouvez supprimer en toute sécurité les serveurs TACACS+ configurés globalement.

Méthodologie de dépannage

1. Assurez-vous d'avoir la définition de transfert ip vrf appropriée sous votre serveur de groupe aaa ainsi que l'interface source pour le trafic TACACS+.
2. Vérifiez votre table de routage vrf et assurez-vous qu'il existe une route vers votre serveur TACACS+. L'exemple ci-dessus est utilisé pour afficher la table de routage vrf :

```
vrfAAA#show ip route vrf blue

Routing Table: blue
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 203.0.113.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 203.0.113.1
      203.0.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        203.0.113.0/24 is directly connected, GigabitEthernet0/0
L        203.0.113.2/32 is directly connected, GigabitEthernet0/0
```

3. Pouvez-vous envoyer une requête ping à votre serveur TACACS+ ? N'oubliez pas que ceci doit également être spécifique à VRF :

```
vrfAAA#ping vrf blue 192.0.2.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 102.0.2.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

4. Vous pouvez utiliser la commande **test aaa** pour vérifier la connectivité (vous devez utiliser l'option new-code à la fin, l'héritage ne fonctionne pas) :

```
vrfAAA#test aaa group management cisco Cisco123 new-code
Sending password
User successfully authenticated

USER ATTRIBUTES

username             "cisco"
reply-message        "password: "
```

Si les routes sont en place et que vous ne voyez aucun accès sur votre serveur TACACS+, assurez-vous que les listes de contrôle d'accès permettent au port TCP 49 d'atteindre le serveur à partir du routeur ou du commutateur. Si vous obtenez un échec d'authentification dépannez TACACS+ comme d'habitude, la fonctionnalité VRF est juste pour le routage du paquet.

Analyse des données

Si tout ce qui précède semble correct, les débogages aaa et tacacs peuvent être activés pour résoudre le problème. Commencez par les débogages suivants :

- debug tacacs
- debug aaa authentication

Voici un exemple de débogage où quelque chose n'est pas configuré correctement, par exemple, mais sans s'y limiter :

- Interface source TACACS+ manquante
- Commandes ip vrf forwarding manquantes sous l'interface source ou sous le serveur de groupe aaa
- Aucune route vers le serveur TACACS+ dans la table de routage VRF

```
Jul 30 20:23:16.399: TPLUS: Queuing AAA Authentication request 0 for processing
Jul 30 20:23:16.399: TPLUS: processing authentication start request id 0
Jul 30 20:23:16.399: TPLUS: Authentication start packet created for 0(cisco)
Jul 30 20:23:16.399: TPLUS: Using server 192.0.2.4
Jul 30 20:23:16.399: TPLUS(00000000)/0: Connect Error No route to host
Jul 30 20:23:16.399: TPLUS: Choosing next server 192.0.2.5
Jul 30 20:23:16.399: TPLUS(00000000)/0: Connect Error No route to host
```

Voici une connexion réussie :

```
Jul 30 20:54:29.091: AAA/AUTHEN/LOGIN (00000000): Pick method list 'default'
Jul 30 20:54:29.091: TPLUS: Queuing AAA Authentication request 0 for processing
Jul 30 20:54:29.091: TPLUS: processing authentication start request id 0
Jul 30 20:54:29.091: TPLUS: Authentication start packet created for 0(cisco)
Jul 30 20:54:29.091: TPLUS: Using server 192.0.2.4
Jul 30 20:54:29.091: TPLUS(00000000)/0/NB_WAIT/2B2DC1AC: Started 5 sec timeout
Jul 30 20:54:29.095: TPLUS(00000000)/0/NB_WAIT: socket event 2
Jul 30 20:54:29.095: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request
Jul 30 20:54:29.095: TPLUS(00000000)/0/READ: socket event 1
Jul 30 20:54:29.095: TPLUS(00000000)/0/READ: Would block while reading
Jul 30 20:54:29.099: TPLUS(00000000)/0/READ: socket event 1
Jul 30 20:54:29.099: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 16 bytes data)
Jul 30 20:54:29.099: TPLUS(00000000)/0/READ: socket event 1
Jul 30 20:54:29.099: TPLUS(00000000)/0/READ: read entire 28 bytes response
Jul 30 20:54:29.099: TPLUS(00000000)/0/2B2DC1AC: Processing the reply packet
Jul 30 20:54:29.099: TPLUS: Received authen response status GET_PASSWORD (8)
Jul 30 20:54:29.099: TPLUS: Queuing AAA Authentication request 0 for processing
Jul 30 20:54:29.099: TPLUS: processing authentication continue request id 0
Jul 30 20:54:29.099: TPLUS: Authentication continue packet generated for 0
Jul 30 20:54:29.099: TPLUS(00000000)/0/WRITE/2B2DC1AC: Started 5 sec timeout
Jul 30 20:54:29.099: TPLUS(00000000)/0/WRITE: wrote entire 25 bytes request
Jul 30 20:54:29.103: TPLUS(00000000)/0/READ: socket event 1
Jul 30 20:54:29.103: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 6 bytes data)
Jul 30 20:54:29.103: TPLUS(00000000)/0/READ: socket event 1
Jul 30 20:54:29.103: TPLUS(00000000)/0/READ: read entire 18 bytes response
Jul 30 20:54:29.103: TPLUS(00000000)/0/2B2DC1AC: Processing the reply packet
Jul 30 20:54:29.103: TPLUS: Received authen response status PASS (2)
```

Problèmes courants

Le problème le plus courant est la configuration. Souvent, l'administrateur place dans le serveur de groupe aaa, mais ne met pas à jour les lignes aaa pour pointer vers le groupe de serveurs. Au lieu de :

```
aaa authentication login default group management local
aaa authorization exec default group management if-authenticated
```

```
aaa accounting exec default start-stop group management
```
L'administrateur aura ajouté :

```
aaa authentication login default grout tacacs+ local
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting exec default start-stop group tacacs+
```
Il vous suffit de mettre à jour la configuration avec le groupe de serveurs approprié.

Un deuxième problème courant est qu'un utilisateur reçoit cette erreur lors de la tentative d'ajout d'ip vrf forwarding sous le groupe de serveurs :

```
% Unknown command or computer name, or unable to find computer address
```
Cela signifie que la commande est introuvable. Si cela se produit, assurez-vous que la version d'IOS prend en charge chaque VRF TACACS+. Voici quelques versions minimales courantes :

- 12.3(7)T
- 12.2(33)SRA1
- 12.2(33)SXI
- 12.2(33)SXH4
- 12.2(54)SG

Informations connexes

- Support et documentation techniques - Cisco Systems