Contenu

Introduction

TACACS+ est fortement utilisé comme protocole d'authentification pour authentifier des utilisateurs aux périphériques de réseau. De plus en plus les administrateurs isolent leur trafic d'administration utilisant le routage VPN et l'expédition (vrf). Par défaut, l'AAA sur l'IOS emploie la table de routage par défaut pour envoyer des paquets. Ce document décrit comment configurer et dépanner TACACS+ quand le serveur est dans un VRF.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- TACACS+
- Vrf

Composants utilisés

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.

Les informations de caractéristique

Essentiellement un VRF est une table de routage virtuelle sur le périphérique. Quand l'IOS prend une décision de routage si la caractéristique ou l'interface utilise un VRF, conduisant des décisions sont faits contre cette table de routage de VRF. Autrement, la caractéristique utilise la

table de routage globale. À cet effet, voici comment vous configurez TACACS+ pour utiliser un VRF (configuration appropriée en gras) :

```
version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1!line con 0line aux 0line vty 0 4 transport input all
```

Comme vous pouvez voir, il n'y a aucun serveur globalement défini TACACS+. Si vous migrez les serveurs vers un VRF, vous pouvez sans risque retirer les serveurs globalement configurés TACACS+.

Dépannage de la méthodologie

1. Veillez-vous pour avoir la définition appropriée d'ip vrf forwarding sous votre aaa group server aussi bien que l'interface de source pour le trafic TACACS+.
2. Vérifiez votre table de routage de vrf et assurez-vous qu'il y a une artère à votre serveur TACACS+. L'exemple ci-dessus est utilisé pour afficher la table de routage de vrf :`version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1!line con 0line aux 0line vty 0 4 transport input all`
3. Pouvez-vous cingler votre serveur TACACS+ ? Souvenez-vous ceci doit être particularité de VRF aussi bien :`version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1!line con 0line aux 0line vty 0 4 transport input all`
4. Vous pouvez utiliser la commande d'**AAA de test** de vérifier la Connectivité (vous devez utiliser l'option de nouveau-code à l'extrémité, au legs ne fait pas travail) :`version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0
0.0.0.0 203.0.113.1!line con 0line aux 0line vty 0 4 transport input all
```

Si les artères sont en place et vous ne voyez aucun hit sur votre serveur TACACS+, assurez-vous que l'ACLs permettent au port TCP 49 pour atteindre le serveur du routeur ou du commutateur. Si vous obtenez un échec d'authentification dépannez TACACS+ en tant que normale, la caractéristique de VRF est juste pour le routage du paquet.

Analyse de données

Si tout au-dessus des aspects corrigent, l'AAA et les tacacs met au point peuvent être activés pour dépanner la question. Le début avec ces derniers met au point :

- debug tacacs
- **debug aaa authentication**

Voici un exemple d'un débogage où quelque chose n'est pas configurée correctement, comme mais pas limité à :

- Manquer l'interface de source TACACS+
- L'ip vrf forwarding manquant commande sous l'interface de source ou sous l'aaa group server
- Aucune artère au serveur TACACS+ dans la table de routage de VRF

```
version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime
msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1!line con 0line
aux 0line vty 0 4 transport input all
```

Voici une connexion réussie :

```
version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime
msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1!line con 0line
aux 0line vty 0 4 transport input all
```

Problèmes courants

La plupart de problème courant est la configuration. Beaucoup de fois l'admin met dans l'aaa group server, mais ne met pas à jour les lignes d'AAA pour indiquer le groupe de serveurs. Au lieu de :

```
version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime
msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1!line con 0line
aux 0line vty 0 4 transport input all
```

L'admin aura mis dans :

```
version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime
msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1!line con 0line
aux 0line vty 0 4 transport input all
```

Mettez à jour simplement la configuration avec le groupe de serveurs correct.

Un deuxième problème courant est un utilisateur reçoit cette erreur en essayant d'ajouter l'ip vrf forwarding sous le groupe de serveurs :

```
version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime
msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1!line con 0line
aux 0line vty 0 4 transport input all
```

Ceci signifie que la commande n'a pas été trouvée. Si ceci se produit assurez-vous la version du par-VRF TACACS+ de prises en charge d'IOS. Voici quelques versions minimum communes :

- 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