IOS per VRF-probleemoplossing bij TACACS+

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Conventies](#)
[Functieinformatie](#)
[Methode voor probleemoplossing](#)
[Gegevensanalyse](#)
[Vaak voorkomende problemen](#)
[Gerelateerde informatie](#)

Inleiding

TACACS+ is sterk gebruikt als het authenticatieprotocol om gebruikers aan netwerkapparaten te authentiseren. Steeds meer beheerders segregeren hun beheerverkeer via VPN Routing en Forwarding (VRF's). Standaard gebruikt AAA op IOS de standaard routingtabel om pakketten te verzenden. Dit document beschrijft hoe u TACACS+ kunt configureren en problemen kunt oplossen wanneer de server in een VRF staat.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- TACACS+
- VRF's

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Functieinformatie

In wezen is een VRF een virtuele routingtabel op het apparaat. Wanneer IOS een routebesluit neemt als de eigenschap of de interface een VRF gebruikt, worden de routeringsbesluiten genomen tegen die VRF-routingtabel. Anders gebruikt de functie de globale routingtabel. Met dit in gedachten, is hier hoe u TACACS+ configureren om een VRF te gebruiken (relevante configuratie in vet):

```
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
```

Zoals u kunt zien, zijn er geen wereldwijd gedefinieerde TACACS+ servers. Als u de servers naar een VRF migreert, kunt u de wereldwijd geconfigureerd TACACS+ servers veilig verwijderen.

Methode voor probleemoplossing

1. Zorg ervoor dat u de juiste ip vrf door:sturen definitie onder uw a groepsserver evenals de broninterface voor het TACACS+ verkeer hebt.
2. Controleer uw vrf-routingtabel en controleer of er een route naar uw TACACS+ server is. Het bovenstaande voorbeeld wordt gebruikt om de vrf-routingtabel weer te geven:
```
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. Kun je je TACACS+ server pingelen? Vergeet niet dat dit ook VRF-specifiek moet zijn:
```
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. U kunt de opdracht **testgebied** gebruiken om de connectiviteit te verifiëren (u moet de nieuwe-code optie aan het eind gebruiken, de erfenis werkt niet):
```
vrfAAA#test aaa group management cisco Cisco123 new-code
Sending password
User successfully authenticated

USER ATTRIBUTES

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

Als de routes op zijn plaats zijn en u geen treffers op uw TACACS+ server ziet, zorg ervoor dat ACLs TCP poort 49 toestaat om de server van de router of de schakelaar te bereiken. Als u een problemen met TACACS+ als normaal hebt bij een verificatiestoring krijgt, is de VRF-functie alleen voor de routing van het pakket.

Gegevensanalyse

Als alles boven lijkt te kloppen, kunnen a en tacacs debugs in staat zijn om het probleem op te lossen. Begin met deze debugs:

- tacacs debug
- debug van verificatie

Hier is een voorbeeld van een debug waar iets niet goed ingesteld is, zoals maar niet beperkt tot:

- Ontbrekende interface voor TACACS+ bron
- Ontbrekende ip vrf-verzendopdrachten onder de broninterface of onder de AAA-groepsserver
- Geen route naar de TACACS+ server in de VRF-routing

```
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
```

Dit is een geslaagde verbinding:

```
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)
```

Vaak voorkomende problemen

Het meest voorkomende probleem is de configuratie. Vaak voert de admin de a groep server in, maar werkt niet de a lijnen bij om naar de server groep te wijzen. In plaats van:

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

De beheerder heeft:

```
aaa authentication login default grout tacacs+ local
aaa authorization exec default group tacacs+ if-authenticated
```

```
aaa accounting exec default start-stop group tacacs+
```
update de configuratie eenvoudig met de juiste servergroep.

Een tweede algemeen probleem is een gebruiker ontvangt deze fout wanneer hij probeert om ip vrf verzenden toe te voegen onder de servergroep:

```
% Unknown command or computer name, or unable to find computer address
```
Dit betekent dat de opdracht niet gevonden is. Als dit voorkomt zorg de versie van IOS steunt per-VRF TACACS+. Hier zijn een aantal veelvoorkomende minimum versies:

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

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems