Troubleshooting de IOS Per VRF TACACS+

Contenido

Introducción

TACACS+ se utiliza intensamente como protocolo de autenticación para autenticar a los usuarios en los dispositivos de red. Cada vez más administradores separan el tráfico de gestión mediante el routing y el reenvío de VPN (VRF). De forma predeterminada, AAA en IOS utiliza la tabla de ruteo predeterminada para enviar paquetes. Este documento describe cómo configurar y resolver problemas de TACACS+ cuando el servidor está en un VRF.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- TACACS+
- VRF

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Información sobre la Función

Básicamente, un VRF es una tabla de ruteo virtual en el dispositivo. Cuando IOS toma una decisión de ruteo si la función o interfaz está utilizando un VRF, las decisiones de ruteo se toman en relación con esa tabla de ruteo VRF. De lo contrario, la función utiliza la tabla de ruteo global. Teniendo esto en cuenta, aquí está cómo configurar TACACS+ para utilizar un VRF (configuración relevante en negrita):

```
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
```

Como puede ver, no hay servidores TACACS+ definidos globalmente. Si está migrando los servidores a un VRF, puede quitar con seguridad los servidores TACACS+ configurados globalmente.

Metodología de solución de problemas

1. Asegúrese de tener la definición de reenvío de vrf ip adecuada en su servidor de grupo aaa, así como la interfaz de origen para el tráfico TACACS+.
2. Verifique su tabla de ruteo vrf y asegúrese de que haya una ruta a su servidor TACACS+. El ejemplo anterior se utiliza para mostrar la tabla de ruteo 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. ¿Puede hacer ping en su servidor TACACS+? Recuerde que esto también debe ser específico de 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. Puede utilizar el comando **test aaa** para verificar la conectividad (debe utilizar la opción new-code al final, el heredado no funciona):

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

USER ATTRIBUTES

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

Si las rutas están en su lugar y no ve ningún resultado en su servidor TACACS+, asegúrese de que las ACL permitan que el puerto TCP 49 llegue al servidor desde el router o el switch. Si obtiene un error de autenticación para resolver problemas de TACACS+ como normal, la función VRF es sólo para el ruteo del paquete.

Análisis de datos

Si todo lo anterior parece correcto, las depuraciones aaa y tacacs se pueden habilitar para

solucionar el problema. Comience con estas depuraciones:

- debug tacacs
- debug aaa authentication

A continuación se muestra un ejemplo de una depuración en la que algo no está configurado correctamente, como pero sin limitarse a:

- Falta la interfaz de origen TACACS+
- Falta el comando ip vrf forwarding en la interfaz de origen o en el servidor de grupo aaa
- No hay ruta al servidor TACACS+ en la tabla de ruteo 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
```

Esta es una conexión correcta:

```
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)
```

Problemas Comunes

El problema más común es la configuración. Muchas veces el administrador coloca el servidor de grupo aaa, pero no actualiza las líneas aaa para apuntar al grupo de servidores. En lugar de:

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

```
aaa accounting exec default start-stop group management
```

El administrador habrá introducido:

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

Simplemente actualice la configuración con el grupo de servidores correcto.

Un segundo problema común es que un usuario recibe este error cuando intenta agregar el reenvío de vrf ip en el grupo de servidores:

```
% Unknown command or computer name, or unable to find computer address
```

Esto significa que no se encontró el comando. Si esto ocurre, asegúrese de que la versión del IOS soporte por VRF TACACS+. Estas son algunas de las versiones mínimas comunes:

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

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems