Contenido

Introducción

El TACACS+ es muy usado como el protocolo de autenticación autenticar a los usuarios a los dispositivos de red. Los administradores están segregando cada vez más su tráfico de administración usando el VPN Routing and Forwarding (VRF). Por abandono, el AAA en el IOS utiliza la tabla de ruteo predeterminado para enviar los paquetes. Este documento describe cómo configurar y resolver problemas el TACACS+ cuando el servidor está en un VRF.

prerrequisitos

Requisitos

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

Esencialmente un VRF es una tabla de ruteo virtual en el dispositivo. Cuando el IOS toma una decisión de ruteo si la característica o la interfaz está utilizando un VRF, las decisiones de ruteo

se toman contra esa tabla de ruteo VRF. Si no, la característica utiliza la tabla de Global Routing. Con esto en la mente, aquí es cómo usted configura el TACACS+ para utilizar un VRF (configuración pertinente en intrépido):

```
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
```

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

Metodología de Troubleshooting

1. Aseegurese le tener IP VRF la definición de envío apropiada bajo su servidor del grupo aaa así como interfaz de origen para el tráfico TACACS+.
2. Marque su tabla de ruteo del vrf y aseegurese allí es una ruta a su servidor TACACS+. El ejemplo anterior se utiliza para visualizar la tabla de ruteo del 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. ¿Puede usted hacer ping su servidor TACACS+? Recuerde que éste necesita ser específico VRF también:`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. Usted puede utilizar el **comando aaa de la prueba** de verificar la Conectividad (usted debe utilizar la opción del nuevo-código en el extremo, la herencia no hace trabajo):`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 las rutas existen y usted no ve ningún golpe en su servidor TACACS+, aseegurese que los ACL están permitiendo que el puerto TCP 49 alcanzara el servidor del router o del Switch. Si usted consigue un Troubleshooting TACACS+ de la falla de autenticación como normal, la característica VRF está apenas para la encaminamiento del paquete.

Análisis de datos

Si todo sobre las miradas corrige, los debugs aaa y de los tacacs se pueden habilitar para resolver problemas el problema. Comience con estos debugs:

- haga el debug de los tacacs
- debug aaa authentication

Aquí está un ejemplo de un debug donde algo no se configura correctamente, por ejemplo pero no limitado a:

- Interfaz de origen perdida TACACS+
- Comandos ip vrf forwarding que falta bajo interfaz de origen o bajo el servidor del grupo aaa
- Ninguna ruta al servidor TACACS+ en la tabla de ruteo 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
```

Aquí está una conexión satisfactoria:

```
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
```

Problemas Comunes

El problema más común es la configuración. Muchas veces el admin pone en el servidor del grupo aaa, pero no pone al día las líneas aaa para señalar al grupo de servidores. En vez 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
```

El admin habrá puesto en:

```
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
```

Ponga al día simplemente la configuración con el grupo de servidores correcto.

Un segundo problema común es usuario recibe este error al intentar agregar IP VRF el envío bajo grupo de servidores:

```
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
```

Esto significa que el comando no fue encontrado. Si ocurre esto aseegurese los soportes por-VRF TACACS+ de la versión del IOS. Aquí están algunas 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