Solução de problemas IOS por TACACS+ de VRF

Contents

Introduction

TACACS+ é usado como protocolo de autenticação para autenticar usuários em dispositivos de rede. Cada vez mais administradores estão segregando seu tráfego de gerenciamento usando VPN Routing and Forwarding (VRFs). Por padrão, o AAA no IOS usa a tabela de roteamento padrão para enviar pacotes. Este documento descreve como configurar e solucionar problemas do TACACS+ quando o servidor está em um VRF.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- TACACS+
- VRFs

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações do recurso

Essencialmente, um VRF é uma tabela de roteamento virtual no dispositivo. Quando o IOS toma uma decisão de roteamento se o recurso ou a interface está usando um VRF, as decisões de roteamento são tomadas em relação a essa tabela de roteamento VRF. Caso contrário, o recurso usa a tabela de roteamento global. Com isso em mente, aqui está como você configura o TACACS+ para usar um VRF (configuração relevante em negrito):

```
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 você pode ver, não há servidores TACACS+ definidos globalmente. Se estiver migrando os servidores para um VRF, você poderá remover com segurança os servidores TACACS+ configurados globalmente.

Metodologia de solução de problemas

1. Verifique se você tem a definição de encaminhamento ip vrf adequada em seu servidor de grupo aaa, bem como a interface de origem para o tráfego TACACS+.
2. Verifique sua tabela de roteamento vrf e certifique-se de que haja uma rota para seu servidor TACACS+. O exemplo acima é usado para exibir a tabela de roteamento 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. Você pode fazer ping no servidor TACACS+? Lembre-se de que isso também precisa ser específico do 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. Você pode usar o comando **test aaa** para verificar a conectividade (você deve usar a opção new-code no final, o legado não funciona):

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

USER ATTRIBUTES

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

Se as rotas estiverem estabelecidas e você não vir nenhum acerto no servidor TACACS+, certifique-se de que as ACLs estejam permitindo que a porta TCP 49 acesse o servidor do roteador ou switch. Se você obtiver uma falha de autenticação, solucione problemas de TACACS+ como de costume, o recurso VRF é apenas para o roteamento do pacote.

Análise de dados

Se tudo acima parecer correto, as depurações de aaa e tacacs podem ser habilitadas para

solucionar o problema. Comece com estas depurações:

- debug tacacs
- debug aaa authentication

Aqui está um exemplo de depuração em que algo não está configurado corretamente, como, mas não limitado a:

- Falta interface de origem TACACS+
- Falta comandos ip vrf forwarding na interface de origem ou no servidor do grupo aaa
- Nenhuma rota para o servidor TACACS+ na tabela de roteamento 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 é uma conexão bem-sucedida:

```
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 comuns

O problema mais comum é a configuração. Muitas vezes o administrador coloca no servidor do grupo aaa, mas não atualiza as linhas aaa para apontar para o grupo de servidores. Em vez de:

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

```
aaa accounting exec default start-stop group management
```
O administrador terá colocado:

```
aaa authentication login default grout tacacs+ local
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting exec default start-stop group tacacs+
```
Basta atualizar a configuração com o grupo de servidores correto.

Um segundo problema comum é que um usuário recebe esse erro ao tentar adicionar o encaminhamento ip vrf no grupo de servidores:

```
% Unknown command or computer name, or unable to find computer address
```
Isso significa que o comando não foi encontrado. Se isso ocorrer, verifique se a versão do IOS suporta TACACS+ por VRF. Aqui estão algumas versões mínimas comuns:

- 12.3(7)T
- 12,2(33)SRA1
- 12.2(33)SXI
- 12.2(33)SXH4
- 12.2(54)SG

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems