每VRF TACACS+的IOS故障排除

目录

简介

TACACS+主要用作向网络设备验证用户身份的身份验证协议。越来越多的管理员使用VPN路由和转发(VRF)来隔离其管理流量。 默认情况下，IOS上的AAA使用默认路由表发送数据包。本文档介绍当服务器在VRF中时如何配置TACACS+并对其进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- TACACS+
- VRF

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

功能信息

VRF本质上是设备上的虚拟路由表。当IOS在功能或接口使用VRF时做出路由决策，则根据该VRF路由表做出路由决策。否则，该功能将使用全局路由表。考虑到这一点，以下是如何配置

TACACS+以使用VRF（相关配置以粗体显示）：

```
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
```

如您所见，没有全局定义的TACACS+服务器。如果将服务器迁移到VRF，则可以安全地删除全局配置的TACACS+服务器。

故障排除方法

1. 确保您在aaa组服务器下具有正确的ip vrf转发定义以及TACACS+流量的源接口。
2. 检查vrf路由表，确保有到TACACS+服务器的路由。上例用于显示vrf路由表：

```
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. 您能ping通TACACS+服务器吗？请记住，这也需要特定于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. 您可以使用**test aaa**命令验证连接（必须在末尾使用new-code选项，旧版不起作用）：

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

USER ATTRIBUTES

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

如果路由已就位，并且您在TACACS+服务器上没有看到任何命中，请确保ACL允许TCP端口49从路由器或交换机到达服务器。如果TACACS+身份验证失败正常，VRF功能仅用于数据包的路由。

数据分析

如果上述所有内容都看起来正确，则可以启用aaa和tacacs调试来排除故障。从以下调试开始：

- debug tacacs
- debug aaa authentication

以下是调试示例，其中某项配置不正确，例如但不限于：

- 缺少TACACS+源接口
- 源接口或aaa组服务器下缺少ip vrf forwarding命令
- 在VRF路由表中没有到TACACS+服务器的路由

```
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
```

以下是成功的连接：

```
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)
```

常见问题

最常见的问题是配置。许多次，管理员放入aaa组服务器，但不更新aaa行以指向服务器组。而不是：

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

管理员将输入：

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

只需使用正确的服务器组更新配置。

第二个常见问题是用户在尝试在服务器组下添加ip vrf转发时收到以下错误：

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

这表示找不到该命令。如果发生这种情况，请确保IOS版本支持每个VRF TACACS+。以下是一些常见的最低版本：

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

相关信息

- 技术支持和文档 - Cisco Systems