目录

简介

TACACS+是大量使用的作为认证协议验证用户到网络设备。使用VPN路由与转发(VRF)，越来越多的管理员分离他们的管理数据流。默认情况下，在IOS的AAA使用默认路由路线表发送数据包。当服务器在VRF时，本文描述如何配置和排除故障TACACS+。

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

本质上VRF是在设备的虚拟路由路线表。当IOS做出路由决策时功能或接口是否使用VRF，路由决策做该VRF路由表。否则，功能使用全球路由表。鉴于此，这是您如何配置TACACS+使用VRF (在粗体的相关配置)：

```
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

正如你看到的没有全局定义TACACS+服务器。如果移植服务器到VRF，您能安全删除全局已配置的TACACS+服务器。

故障排除方法

1. 确保您有转发定义在您的aaa组服务器下以及TACACS+流量的适当的IP VRF源接口。
2. 检查您的VRF路由表并且确保那里是路由到您的TACACS+服务器。以上示例用于显示VRF路由表：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. 能否ping您的TACACS+服务器？切记此需要是VRF特定：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. 您能使用**aaa命令的测验**验证连接(您必须使用新代码选项在末端，传统不工作)：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

如果路由到位，并且没看到在您的TACACS+服务器的命中数，请确保ACL允许TCP端口49到达从路由器或交换机的服务器。如果获得认证失败请排除故障TACACS+作为正常， VRF功能是为数据包的路由。

数据分析

如果一切在查找上更正， aaa和TACACS调试可以启用排除故障问题。从这些调试开始：

- debug tacacs

- debug aaa authentication

这是某事没有适当地配置调试的示例，例如，但是没有有限对：

- 缺少TACACS+源接口
- 转发命令的缺少IP VRF在源接口下或在aaa组服务器下
- 对TACACS+服务器的没有路由在VRF路由表里

```
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
```

这是成功的连接：

```
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
```

常见问题

最常见的问题是配置。许多时间admin在aaa组服务器放置，但是不更新aaa线路指向服务器组。而不是：

```
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
```

admin放置在：

```
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
```

请更新与正确服务器组的配置。

第二常见问题是用户收到此错误，当尝试转发在服务器组下时的添加IP 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
```

这意味着未找到命令。如果这发生请确保IOS版本支持每VRF TACACS+。这是一些普通的最低版本：

- 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