

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informação da característica](#)

[Metodologia de Troubleshooting](#)

[Análise de dados](#)

[Problemas comuns](#)

[Informações Relacionadas](#)

[Introdução](#)

O RADIUS é usado pesadamente como o protocolo de autenticação para autenticar usuários para o acesso de rede. Mais admins estão segregando seu tráfego de gerenciamento usando o VPN Routing and Forwarding (VRF). À revelia, o Authentication, Authorization, and Accounting (AAA) no IOS® usa a tabela de roteamento padrão a fim enviar pacotes. Este guia descreve como configurar e pesquisar defeitos o RADIUS quando o servidor Radius está em um VRF.

[Pré-requisitos](#)

[Requisitos](#)

A Cisco recomenda que você tenha conhecimento destes tópicos:

- RADIUS
- VRF
- AAA

[Componentes Utilizados](#)

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

[Convenções](#)

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Caracterize a informação

Essencialmente, um VRF é uma tabela de roteamento virtual no dispositivo. Quando os IO fazem uma decisão de roteamento, se a característica ou a relação estão usando um VRF, as decisões de roteamento são feitas contra essa tabela de roteamento VRF. Se não, a característica usa a tabela de roteamento global. Com isto em mente, é aqui como você configura o RAI0 para usar um VRF:

Como você pode ver, não há nenhum servidor Radius globalmente definido. Se você está migrando os server em um VRF, você pode com segurança remover globalmente os servidores radius configurados.

Metodologia de Troubleshooting

Conclua estes passos:

1. Certifique-se de você ter a definição apropriada da transmissão IPVRF sob seu server do grupo AAA assim como a interface de origem para o tráfego de radius.
2. Verifique sua tabela de roteamento VRF e certifique-se que há uma rota a seu servidor Radius. Nós usaremos o exemplo acima a fim indicar a tabela de roteamento

```
VRF:vrfAAA#show ip route vrf blueRouting Table: blueCodes: 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 overrideGateway of last resort is 203.0.113.1 to network 0.0.0.0S* 0.0.0.0/0 [1/0] via 203.0.113.1 203.0.113.0/8 is variably subnetted, 2 subnets, 2 masksC 203.0.113.0/24 is directly connected, GigabitEthernet0/0L 203.0.113.2/32 is directly connected, GigabitEthernet0/0
```

3. Pode você sibilar seu servidor Radius? Recorde que este precisa de ser específico VRF também:

```
vrfAAA#ping vrf blue 192.0.2.4Type escape sequence to abort.Sending 5, 100-byte ICMP Echos to 192.0.2.4, 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 **aaa do teste** a fim verificar a Conectividade (você deve usar a opção do novo-código na extremidade; o legado não trabalho):

```
vrfAAA#test aaa group management cisco Cisco123 new-codeUser successfully authenticatedUSER ATTRIBUTESusername "cisco"
```

Se as rotas são no lugar e você não vê nenhuma batida em seu servidor Radius, certifique-se de que os ACL estão permitindo que a porta 1645/1646 UDP ou a porta 1812/1813 UDP alcançassem o server do roteador ou do interruptor. Se você obtém uma falha de autenticação, pesquise defeitos o RAI0 como o normal. A característica VRF é apenas para o roteamento do pacote.

Análise de dados

Se tudo olha correto, os comandos **debug aaa** e de **raio** podem ser permitidos a fim pesquisar defeitos a edição. Comece com estes comandos **debug**:

- debug radius
- debug aaa authentication

Está aqui um exemplo **debugar** onde algo não é configurado corretamente, como mas não limitado a:

- Interface de origem faltante do RAIO
 - Comandos ip vrf forwarding faltantes sob a interface de origem ou sob o server do grupo AAA
 - Nenhuma rota ao servidor Radius na tabela de roteamento VRF
- ```
vrfAAA#test aaa group management cisco Cisco123 new-codeUser successfully authenticatedUSER ATTRIBUTEUsername "cisco"
```

Infelizmente, com RAIO não há nenhuma distinção entre um intervalo e uma rota faltante.

Está aqui um exemplo de uma autenticação bem sucedida:

```
vrfAAA#test aaa group management cisco Cisco123 new-codeUser successfully authenticatedUSER ATTRIBUTEUsername "cisco"
```

## Problemas comuns

- O problema mais comum é aquele da configuração. Muitas vezes o admin porá no server do grupo aaa mas não atualizará as linhas aaa para apontar ao grupo de servidor. Em vez disto:

```
vrfAAA#test aaa group management cisco Cisco123 new-codeUser successfully authenticatedUSER ATTRIBUTEUsername "cisco"
```

O admin terá posto neste:

```
vrfAAA#test aaa group management cisco Cisco123 new-codeUser successfully authenticatedUSER ATTRIBUTEUsername "cisco"
```

Atualize simplesmente a configuração com o grupo de servidor correto.
- Um segundo problema comum é que um usuário verá este erro ao tentar adicionar o VRF IP que envia sob o grupo de servidor:

```
vrfAAA#test aaa group management cisco Cisco123 new-codeUser successfully authenticatedUSER ATTRIBUTEUsername "cisco"
```

Isto significa que o comando não esteve encontrado. Se você vê este erro, certifique-se dos apoios da versão de IOS pelo RAIO VRF.

## Informações Relacionadas

- [Suporte Técnico e Documentação - Cisco Systems](#)