# Solução de problemas de RADIUS do IOS por VRF

## Contents



## Introduction

O RADIUS é usado pesadamente como protocolo de autenticação para autenticar usuários para acesso à rede. Mais administradores estão segregando seu tráfego de gerenciamento usando o VPN Routing and Forwarding (VRF). Por padrão, a autenticação, autorização e contabilização (AAA) no IOS® usa a tabela de roteamento padrão para enviar pacotes. Este guia descreve como configurar e solucionar problemas de RADIUS quando o servidor RADIUS está em um VRF.

## Prerequisites

### Requirements

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.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## 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 estiver 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 RADIUS para usar um VRF:

```
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 radius management
 server-private 192.0.2.4 key cisco
 server-private 192.0.2.5 key cisco
 ip vrf forwarding blue
 ip radius 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 RADIUS definidos globalmente. Se estiver migrando os servidores para um VRF, você poderá remover com segurança os servidores RADIUS configurados globalmente.

## Metodologia de solução de problemas

Conclua estes passos:

1. Verifique se você tem a definição de encaminhamento IPVRF adequada em seu servidor de grupo AAA, bem como a interface de origem para o tráfego RADIUS.
2. Verifique sua tabela de roteamento VRF e certifique-se de que haja uma rota para seu servidor RADIUS. Usaremos o exemplo acima 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
      203.0.113.0/8 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 consegue fazer ping no servidor RADIUS? 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 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 **test aaa** para verificar a conectividade (você deve usar a opção new-code no final; legado não funcionará):

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

USER ATTRIBUTES

username             "cisco"
```

Se as rotas estiverem estabelecidas e você não vir nenhum acerto no servidor RADIUS, certifique-se de que as ACLs estejam permitindo que a porta udp 1645/1646 ou a porta udp 1812/1813 acesse o servidor a partir do roteador ou switch. Se você tiver uma falha de autenticação, solucione problemas de RADIUS normalmente. O recurso VRF é apenas para o roteamento do pacote.

## Análise de dados

Se tudo parecer correto, os comandos **aaa** e **radius debug** podem ser ativados para solucionar o problema. Comece com estes comandos **debug**:

- **debug radius**
- **debug aaa authentication**

Aqui está um exemplo de uma **depuração** onde algo não está configurado corretamente, como, mas não limitado a:

- Falta interface de origem RADIUS
- Falta comandos de encaminhamento de VRF IP na interface de origem ou no servidor de grupo AAA
- Nenhuma rota para o servidor RADIUS na tabela de roteamento VRF

```
Aug  1 13:39:28.571: AAA/AUTHEN/LOGIN (00000000): Pick method list 'default'
Aug  1 13:39:28.571: RADIUS/ENCODE(00000000):Orig. component type = Invalid
Aug  1 13:39:28.571: RADIUS/ENCODE(00000000): dropping service type,
   "radius-server attribute 6 on-for-login-auth" is off
Aug  1 13:39:28.571: RADIUS(00000000): Config NAS IP: 203.0.113.2
Aug  1 13:39:28.571: RADIUS(00000000): Config NAS IPv6: ::
Aug  1 13:39:28.571: RADIUS(00000000): sending
Aug  1 13:39:28.575: RADIUS(00000000): Send Access-Request to 192.0.2.4:1645
   id 1645/2, len 51
Aug  1 13:39:28.575: RADIUS:  authenticator 12 C8 65 2A C5 48 B8 1F -
   33 FA 38 59 9C 5F D3 3A
Aug  1 13:39:28.575: RADIUS:  User-Password       [2]   18  *
Aug  1 13:39:28.575: RADIUS:  User-Name           [1]   7   "cisco"
Aug  1 13:39:28.575: RADIUS:  NAS-IP-Address      [4]   6   203.0.113.2
Aug  1 13:39:28.575: RADIUS(00000000): Sending a IPv4 Radius Packet
Aug  1 13:39:28.575: RADIUS(00000000): Started 5 sec timeout
Aug  1 13:39:32.959: RADIUS(00000000): Request timed out
Aug  1 13:39:32.959: RADIUS: Retransmit to (192.0.2.4:1645,1646) for id 1645/2
Aug  1 13:39:32.959: RADIUS(00000000): Started 5 sec timeout
Aug  1 13:39:37.823: RADIUS(00000000): Request timed out
Aug  1 13:39:37.823: RADIUS: Retransmit to (192.0.2.4:1645,1646) for id 1645/2
Aug  1 13:39:37.823: RADIUS(00000000): Started 5 sec timeout
Aug  1 13:39:42.199: RADIUS(00000000): Request timed out
Aug  1 13:39:42.199: RADIUS: Retransmit to (192.0.2.4:1645,1646) for id 1645/2
Aug  1 13:39:42.199: RADIUS(00000000): Started 5 sec timeout
Aug  1 13:39:47.127: RADIUS(00000000): Request timed out
Aug  1 13:39:47.127: RADIUS: Fail-over to (192.0.2.5:1645,1646) for id 1645/2
Aug  1 13:39:47.127: RADIUS(00000000): Started 5 sec timeout
Aug  1 13:39:51.927: RADIUS(00000000): Request timed out
Aug  1 13:39:51.927: RADIUS: Retransmit to (192.0.2.5:1645,1646) for id 1645/2
Aug  1 13:39:51.927: RADIUS(00000000): Started 5 sec timeout
Aug  1 13:39:56.663: RADIUS(00000000): Request timed out
Aug  1 13:39:56.663: RADIUS: Retransmit to (192.0.2.5:1645,1646) for id 1645/2
Aug  1 13:39:56.663: RADIUS(00000000): Started 5 sec timeout
Aug  1 13:40:01.527: RADIUS(00000000): Request timed out
Aug  1 13:40:01.527: RADIUS: Retransmit to (192.0.2.5:1645,1646) for id 1645/2
Aug  1 13:40:01.527: RADIUS(00000000): Started 5 sec timeoutUser rejected
```

Infelizmente, com o RADIUS, não há distinção entre um tempo limite e uma rota ausente.

Aqui está um exemplo de uma autenticação bem-sucedida:

```
Aug  1 13:35:51.791: AAA/AUTHEN/LOGIN (00000000): Pick method list 'default'

Aug  1 13:35:51.791: RADIUS/ENCODE(00000000):Orig. component type = Invalid

Aug  1 13:35:51.791: RADIUS/ENCODE(00000000): dropping service type,
   "radius-server attribute 6 on-for-login-auth" is off

Aug  1 13:35:51.791: RADIUS(00000000): Config NAS IP: 203.0.113.2

Aug  1 13:35:51.791: RADIUS(00000000): Config NAS IPv6: ::

Aug  1 13:35:51.791: RADIUS(00000000): sending

Aug  1 13:35:51.791: RADIUS(00000000): Send Access-Request to 192.0.2.4:1645 id
   1645/1, len 51

Aug  1 13:35:51.791: RADIUS:  authenticator F4 E3 00 93 3F B7 79 A9 -
   2B DC 89 18 8D B9 FF 16

Aug  1 13:35:51.791: RADIUS:  User-Password       [2]   18  *

Aug  1 13:35:51.791: RADIUS:  User-Name           [1]   7   "cisco"

Aug  1 13:35:51.791: RADIUS:  NAS-IP-Address      [4]   6   203.0.113.2

Aug  1 13:35:51.791: RADIUS(00000000): Sending a IPv4 Radius Packet

Aug  1 13:35:51.791: RADIUS(00000000): Started 5 sec timeout

Aug  1 13:35:51.799: RADIUS: Received from id 1645/1 14.36.142.31:1645,
   Access-Accept, len 62

Aug  1 13:35:51.799: RADIUS:  authenticator B0 0B AA FF B1 27 17 BD -
   3F AD 22 30 C6 03 5C 2D

Aug  1 13:35:51.799: RADIUS:  User-Name           [1]   7   "cisco"

Aug  1 13:35:51.799: RADIUS:  Class               [25]  35

Aug  1 13:35:51.799: RADIUS:   43 41 43 53 3A 6A 65 64 75 62 6F 69 73 2D 61 63
   [CACS:ACS1]

Aug  1 13:35:51.799: RADIUS:   73 2D 35 33 2F 31 33 32 34 35 33 37 33 35 2F 33
   [s-53/132453735/3]

Aug  1 13:35:51.799: RADIUS:   38                 [ 8]

Aug  1 13:35:51.799: RADIUS(00000000): Received from id 1645/1.
```

## Problemas comuns

- O problema mais comum é o da configuração. Muitas vezes, o administrador colocará no servidor do grupo aaa, mas não atualizará as linhas aaa para apontar para o grupo de servidores. Em vez disso:

  ```
  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 isso:

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

Basta atualizar a configuração com o grupo de servidores correto.

- Um segundo problema comum é que um usuário verá esse erro ao tentar adicionar o encaminhamento de VRF IP no grupo de servidores:

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

Isso significa que o comando não foi encontrado. Se você vir esse erro, verifique se a versão do IOS suporta por VRF RADIUS.

## Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems