

# 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[機能情報](#)

[トラブルシューティング方法](#)

[データ分析](#)

[一般的な問題](#)

[関連情報](#)

## 概要

RADIUS は、ネットワークにアクセスするユーザを認証する、認証プロトコルとして多用されています。多くの管理者が、VPN ルーティングおよび転送 (VRF) を使用して管理トラフィックを分離しています。IOS® の認証、認可、アカウントिंग (AAA) はパケットを送信するためにデフォルトのルーティング テーブルを使用します。このガイドでは、RADIUS サーバが VRF にある場合の RADIUS の設定およびトラブルシューティング方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- RADIUS
- VRF
- [AAA]

### 使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

### 表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

## 機能情報

基本的に、VRF はデバイス上の仮想ルーティング テーブルです。IOS がルーティングを決定する際に、機能またはインターフェイスが VRF を使用している場合、ルーティングの決定はその VRF ルーティング テーブルに対して行われます。これ以外の場合、機能はグローバル ルーティング テーブルを使用します。このことを念頭において、次に、VRF を使用するように RADIUS を設定する方法を示します。

出力結果からわかるように、グローバルに定義された RADIUS サーバはありません。サーバを VRF に移行する場合、グローバルに設定された RADIUS サーバを安全に削除することができます。

## トラブルシューティング方法

次の手順を実行します。

1. AAA グループ サーバに、RADIUS トラフィックの送信元インターフェイスと適切な IPVRF 転送定義があることを確認します。
2. VRF ルーティング テーブルをチェックし、RADIUS サーバへのルートがあることを確認します。VRF ルーティング テーブルの表示に上記の例を使用します。`vrfAAA#show ip route vrf blue`  
Routing 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 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, GigabitEthernet0/0L  
203.0.113.2/32 is directly connected, GigabitEthernet0/0
3. RADIUS サーバに ping できますか。また VRF 専用でなければなりません。`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. `test aaa` コマンドを使用して接続をテストできます (最後に [new-code] オプションをつける必要があります。レガシーは機能しません)。`vrfAAA#test aaa group management cisco Cisco123 new-code`  
User successfully authenticatedUSER ATTRIBUTESusername "cisco"

ルートが設定されているにもかかわらず RADIUS サーバにヒットしない場合、ルータまたはスイッチからサーバに到達できるように ACL で UDP ポート 1645/1646、または UDP ポート 1812/1813 が許可されていることを確認してください。認証エラーが発生した場合、通常通り RADIUS のトラブルシューティングを実施します。VRF の機能は、パケットをルーティングするだけのものです。

## データ分析

すべてが正常に機能しているように見えるのであれば、問題のトラブルシューティングのために `aaa` および `radius debug` コマンドを有効にします。次の `debug` コマンドを使用して開始します。

- `debug radius`
- `debug aaa authentication`

次の例のように何かが正しく設定されていない場合のデバッグの例を示します。

- RADIUS の送信元インターフェイスがない
  - 送信元インターフェイスまたは AAA グループ サーバに IP VRF 転送コマンドがない
  - VRF ルーティング テーブルに RADIUS サーバへのルートがない
- ```
vrfAAA#test aaa group management cisco Cisco123 new-codeUser successfully authenticatedUSER ATTRIBUTEUsername "cisco"
```

残念ながら、RADIUS ではタイムアウトとルートがない場合の区別ができません。

次に正常な認証の例を示します。

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

## 一般的な問題

- 最も一般的な問題は、設定に関するものです。管理者は AAA グループ サーバを何度も設定しますが、AAA 行をサーバグループをポイントするように更新しません。次の代わりに、

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

管理者は次を設定します。

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

正しいサーバグループで設定を更新するだけです。
- 2 つめの一般的な問題は、ユーザがサーバグループに IP VRF 転送を追加しようとした場合に、次のエラーが表示されることです。

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

これはコマンドが見つからなかったことを意味します。このエラーが発生した場合、IOS のバージョンが VRF RADIUS をサポートしていることを確認してください。

## 関連情報

- [テクニカルサポートとドキュメント - Cisco Systems](#)