目次

概要

TACACS+ は認証プロトコルとして頻繁に使用されますネットワークデバイスにユーザを認証するために。 さらに多くの管理者は VPN Routing and Forwarding （ VRF ）を使用してマネジメントトラフィックを分離しています。 デフォルトで、IOS の AAA はパケットを送信するのにデフォルト ルーティング ルーティング· テーブルを使用します。 サーバが VRF にあるときこの資料に TACACS+ を設定し解決する方法を記述されています。

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。

- TACACS+
- VRF

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。

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 はデバイスのバーチャルルーティング ルーティング· テーブルです。 機能かインターフェイスが VRF を使用している場合 IOS がルーティング決定を作るとき、ルーティング決定はその VRF ルーティング テーブルに対してなされます。 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。 これを念頭において、ここに VRF （太字の関係のある構成）を使用するために TACACS+ をどのように設定するかです:

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

見てわかるように、グローバルに定義された TACACS+ サーバがありません。 VRF にサーバを移行する場合、安全にグローバルに設定された TACACS+ サーバを削除できます。

トラブルシューティング方法

1. AAA グループ サーバの下で定義、また TACACS+ トラフィックのためのソースインターフェイスを転送する適切な IP VRF を持つために確かめて下さい。
2. VRF ルーティング テーブルをチェックし、ルートが TACACS+ サーバへあることを確かめて下さい。 上述の例が VRF ルーティング テーブルを表示するのに使用されています: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. TACACS+ サーバを ping できますか。 これが VRF 仕様である同様に必要があることを覚えていて下さい: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. 接続（端、レガシーで作業新コード オプションを使用して下さい）を確認する**テスト aaa コマンドを**使用できます: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
```

ルーティングがきちんと整っていたらおよび TACACS+ サーバのヒットを見なかったら、ACL が TCPポート 49 がルータからのサーバに達するか、または切り替えるようにしていることを確かめて下さい。 認証失敗を得たら標準として TACACS+ を、VRF 機能ですパケットのルーティングのためちょうど解決して下さい。

データ分析

外観の上のすべてが訂正する場合問題を解決するために、AAA および tacacs デバッグは有効にすることができます。 これらのデバッグから開始して下さい:

- debug tacacs
- debug aaa authentication

何かが正しく設定されないデバッグの例はのような限られたにここにありません:

- 抜けている TACACS+ ソースインターフェイス
- ソースインターフェイスまたは AAA グループ サーバの下の抜けた ip vrf forwarding コマンド
- VRF ルーティング テーブルの TACACS+ サーバへのルート無し

```
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
```

接続の成功はここにあります:

```
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
```

一般的な問題

最も 一般的 な 問題は設定です。 admin は何倍も AAA グループ サーバに置きますが、サーバグループを指すために AAA 行をアップデートしません。 の代り:

```
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 はに置いてしまいます:

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

正しいサーバ グループで設定を更新するだけです。

第 2 よくある問題はサーバグループの下で転送する IP VRF を追加することを試みるときユーザ受け取りますこのエラーをです:

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

これはコマンドが見つからなかったことを意味します。 これが発生したら IOSバージョン サポート毎 VRF TACACS+ を確かめて下さい。 いくつかのよくある最小バージョンはここにあります:

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

関連情報

- テクニカルサポートとドキュメント - Cisco Systems