每個VRF RADIUS的IOS故障排除

目錄

簡介

RADIUS大量用作驗證通訊協定，對使用者進行網路存取的驗證。更多管理員使用VPN路由和轉發(VRF)隔離其管理流量。 預設情況下，IOS®上的驗證、授權和計量(AAA)使用預設路由表來傳送封包。本指南介紹當RADIUS伺服器在VRF中時，如何配置並排除RADIUS故障。

必要條件

需求

思科建議您瞭解以下主題：

- RADIUS
- VRF
- AAA

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

功能資訊

實質上，VRF是裝置上的虛擬路由表。當IOS做出路由決策時，如果功能或介面使用VRF，則根據該VRF路由表做出路由決策。否則，該功能將使用全域性路由表。考慮到這一點，以下是將RADIUS設定為使用VRF的方式：

```
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
```

您可以看到，沒有全域性定義的RADIUS伺服器。如果要將伺服器遷移到VRF，可以安全地移除全域性配置的RADIUS伺服器。

故障排除方法

請完成以下步驟：

1. 請確保在AAA組伺服器下具有正確的IPVRF轉發定義，並且為RADIUS流量提供源介面。
2. 檢查VRF路由表，並確儲存在通往RADIUS伺服器的路由。我們將使用上面的示例來顯示VRF路由表：

```
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. 是否能ping通您的RADIUS伺服器？回想一下，這還需要針對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. 您可以使用**test aaa**命令驗證連線(您必須在結尾使用new-code選項；舊版無法使用):

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

USER ATTRIBUTES

username             "cisco"
```

如果路由已建立，且您的RADIUS伺服器沒有看到命中，請確保ACL允許從路由器或交換器連線至伺服器的udp連線埠1645/1646或udp連線埠1812/1813。如果遇到驗證失敗，請正常排除RADIUS故障。VRF功能僅用於封包的路由。

資料分析

如果一切正常，則可啟用**aaa**和**radius debug**命令以解決問題。從以下**debug**指令開始：

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

以下是**debug**的範例，其中某些內容未正確設定，例如（但不限於）：

- 缺少RADIUS源介面
- 源介面下或AAA組伺服器下缺少IP VRF轉發命令
- VRF路由表中沒有到RADIUS伺服器的路由

```
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
```

遺憾的是，使用RADIUS時，逾時和遺失路由之間沒有區別。

以下是成功驗證的範例：

```
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.
```

常見問題

- 最常見的問題是配置問題。管理員會多次放入aaa組伺服器，但不會更新aaa行以指向伺服器組。而不是這樣：

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

  管理員將輸入以下內容：

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

  只需使用正確的伺服器組更新配置即可。
- 第二個常見問題是使用者嘗試在伺服器組下新增IP VRF轉發時將看到此錯誤：

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

  這表示找不到該命令。如果您看到此錯誤，請確保每個VRF RADIUS都支援IOS版本。

相關資訊

- 技術支援與文件 - Cisco Systems