IOS pro VRF RADIUS-Fehlerbehebung

Inhalt

Einführung

RADIUS wird häufig als Authentifizierungsprotokoll für die Authentifizierung von Benutzern für den Netzwerkzugriff verwendet. Immer mehr Administratoren verwenden VPN Routing and Forwarding (VRF) zur Trennung des Management-Datenverkehrs. Standardmäßig wird bei IOS® die Standard-Routing-Tabelle zum Senden von Paketen verwendet, um Authentifizierung, Autorisierung und Abrechnung (AAA) zu ermöglichen. In dieser Anleitung wird beschrieben, wie RADIUS konfiguriert und Fehler behoben werden, wenn sich der RADIUS-Server in einer VRF-Instanz befindet.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- RADIUS
- VRF
- AAA

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Informationen zu Funktionen

Im Wesentlichen ist eine VRF-Instanz eine virtuelle Routing-Tabelle auf dem Gerät. Wenn IOS eine Routing-Entscheidung trifft und die Funktion oder Schnittstelle eine VRF-Instanz verwendet, werden Routing-Entscheidungen für diese VRF-Routing-Tabelle getroffen. Andernfalls wird die globale Routing-Tabelle verwendet. Im Hinblick darauf wird hier erläutert, wie Sie RADIUS für die Verwendung einer VRF-Instanz konfigurieren:

```
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
```

Wie Sie sehen, gibt es keine global definierten RADIUS-Server. Wenn Sie die Server in eine VRF-Instanz migrieren, können Sie die global konfigurierten RADIUS-Server sicher entfernen.

Fehlerbehebungsmethode

Gehen Sie wie folgt vor:

1. Achten Sie darauf, dass die richtige IPVRF-Weiterleitungsdefinition unter Ihrem AAA-Gruppenserver sowie die Quellschnittstelle für den RADIUS-Datenverkehr vorhanden ist.
2. Überprüfen Sie Ihre VRF-Routing-Tabelle, und stellen Sie sicher, dass eine Route zum RADIUS-Server vorhanden ist. Das obige Beispiel wird verwendet, um die VRF-Routing-Tabelle anzuzeigen:

```
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. Können Sie Ihren RADIUS-Server pingen? Beachten Sie, dass dies auch VRF-spezifisch sein muss:

```
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. Sie können den **Test aaa**-Befehl verwenden, um die Verbindung zu überprüfen (Sie müssen am Ende die Option für den neuen Code verwenden). Legacy funktioniert nicht):

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

USER ATTRIBUTES

username             "cisco"
```

Wenn die Routen vorhanden sind und Sie keine Treffer auf Ihrem RADIUS-Server sehen, stellen Sie sicher, dass die ACLs den udp-Port 1645/1646 oder den udp-Port 1812/1813 zulassen, um den Server vom Router oder Switch zu erreichen. Wenn bei der Authentifizierung ein Fehler auftritt, beheben Sie wie gewohnt RADIUS. Die VRF-Funktion dient lediglich zum Routing des Pakets.

Datenanalyse

Wenn alles korrekt aussieht, können **aaa**- und **Radius-Debugbefehle** aktiviert werden, um das Problem zu beheben. Beginnen Sie mit den folgenden **Debugbefehlen**:

- **Debug-Radius**
- **debuggen aaa authentication**

Hier ein Beispiel für ein **Debuggen**, bei dem etwas nicht richtig konfiguriert ist, z. B.:

- RADIUS-Quellschnittstelle fehlt
- Befehle für die IP-VRF-Weiterleitung unter der Quellschnittstelle oder unter dem AAA-Gruppenserver fehlen
- Keine Route zum RADIUS-Server in der VRF-Routing-Tabelle

```
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
```

Leider gibt es bei RADIUS keinen Unterschied zwischen einem Timeout und einer fehlenden

Route.

Hier ein Beispiel für eine erfolgreiche Authentifizierung:

```
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.
```

Häufige Probleme

- Das häufigste Problem ist die Konfiguration. In vielen Fällen wird der Administrator den AAA-Gruppenserver eingeben, die aaa-Zeilen jedoch nicht aktualisieren, um auf die Servergruppe zu verweisen. Stattdessen:
  ```
  aaa authentication login default group management local
  aaa authorization exec default group management if-authenticated
  ```

```
aaa accounting exec default start-stop group management
```

Der Administrator hat Folgendes eingegeben:

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

Aktualisieren Sie einfach die Konfiguration mit der richtigen Servergruppe.

- Ein zweites häufiges Problem besteht darin, dass ein Benutzer diesen Fehler sieht, wenn er versucht, die IP-VRF-Weiterleitung unter der Servergruppe hinzuzufügen:

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

Dies bedeutet, dass der Befehl nicht gefunden wurde. Wenn Sie diesen Fehler sehen, stellen Sie sicher, dass die IOS-Version pro VRF RADIUS unterstützt.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems