IOS pro VRF TACACS+ Fehlerbehebung

Inhalt

Einführung

TACACS+ wird häufig als Authentifizierungsprotokoll für die Authentifizierung von Benutzern für Netzwerkgeräte verwendet. Immer mehr Administratoren verwenden VPN Routing and Forwarding (VRF) für die Trennung des Verwaltungsdatenverkehrs. Standardmäßig verwendet AAA in IOS die Standard-Routingtabelle, um Pakete zu senden. In diesem Dokument wird beschrieben, wie Sie TACACS+ konfigurieren und Fehler beheben, wenn sich der Server in einer VRF-Instanz befindet.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- TACACS+
- VRFs

Verwendete Komponenten

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

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, wenn die Funktion oder Schnittstelle eine VRF-Instanz verwendet, werden Routing-Entscheidungen für diese VRF-Routing-Tabelle getroffen. Andernfalls wird die globale Routing-Tabelle verwendet. In diesem Zusammenhang zeigen wir Ihnen, wie Sie TACACS+ für die Verwendung einer VRF-Instanz konfigurieren (relevante fett formatierte Konfiguration):

```
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 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 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 TACACS+-Server. Wenn Sie die Server zu einer VRF-Instanz migrieren, können Sie die global konfigurierten TACACS+-Server sicher entfernen.

Fehlerbehebungsmethode

1. Stellen Sie sicher, dass Sie die richtige IP-VRF-Weiterleitungsdefinition unter Ihrem AAA-Gruppenserver sowie die Quellschnittstelle für den TACACS+-Datenverkehr haben.
2. Überprüfen Sie Ihre VRF-Routing-Tabelle, und stellen Sie sicher, dass eine Route zum TACACS+-Server vorhanden ist. Im obigen Beispiel wird die VRF-Routing-Tabelle angezeigt:

```
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
      203.0.0.0/24 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 TACACS+-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 102.0.2.4, 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 aa**-Befehl verwenden, um die Verbindung zu überprüfen (Sie müssen am Ende die Option für den neuen Code verwenden, die Legacy funktioniert nicht):

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

USER ATTRIBUTES

username             "cisco"
reply-message        "password: "
```

Wenn die Routen vorhanden sind und Sie keine Treffer auf Ihrem TACACS+-Server sehen, stellen Sie sicher, dass die ACLs zulassen, dass der TCP-Port 49 den Server vom Router oder Switch aus erreicht. Wenn bei der Fehlerbehebung für TACACS+ ein Authentifizierungsfehler auftritt, dient die VRF-Funktion nur für das Routing des Pakets.

Datenanalyse

Wenn alles oben richtig aussieht, können aaaa und tacacs debugs aktiviert werden, um das Problem zu beheben. Beginnen Sie mit diesen Debuggen:

- Debug-Taktiken
- debuggen aaa authentication

Im Folgenden finden Sie ein Beispiel für ein Debuggen, bei dem etwas nicht richtig konfiguriert ist, z. B.:

- TACACS+-Quellschnittstelle fehlt
- ip vrf Forwarding-Befehle unter der Quellschnittstelle oder unter dem AAA-Gruppenserver fehlen
- Keine Route zum TACACS+-Server in der VRF-Routing-Tabelle

```
Jul 30 20:23:16.399: TPLUS: Queuing AAA Authentication request 0 for processing
Jul 30 20:23:16.399: TPLUS: processing authentication start request id 0
Jul 30 20:23:16.399: TPLUS: Authentication start packet created for 0(cisco)
Jul 30 20:23:16.399: TPLUS: Using server 192.0.2.4
Jul 30 20:23:16.399: TPLUS(00000000)/0: Connect Error No route to host
Jul 30 20:23:16.399: TPLUS: Choosing next server 192.0.2.5
Jul 30 20:23:16.399: TPLUS(00000000)/0: Connect Error No route to host
```

Die Verbindung ist erfolgreich:

```
Jul 30 20:54:29.091: AAA/AUTHEN/LOGIN (00000000): Pick method list 'default'
Jul 30 20:54:29.091: TPLUS: Queuing AAA Authentication request 0 for processing
Jul 30 20:54:29.091: TPLUS: processing authentication start request id 0
Jul 30 20:54:29.091: TPLUS: Authentication start packet created for 0(cisco)
Jul 30 20:54:29.091: TPLUS: Using server 192.0.2.4
Jul 30 20:54:29.091: TPLUS(00000000)/0/NB_WAIT/2B2DC1AC: Started 5 sec timeout
Jul 30 20:54:29.095: TPLUS(00000000)/0/NB_WAIT: socket event 2
Jul 30 20:54:29.095: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request
Jul 30 20:54:29.095: TPLUS(00000000)/0/READ: socket event 1
Jul 30 20:54:29.095: TPLUS(00000000)/0/READ: Would block while reading
Jul 30 20:54:29.099: TPLUS(00000000)/0/READ: socket event 1
Jul 30 20:54:29.099: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 16 bytes data)
Jul 30 20:54:29.099: TPLUS(00000000)/0/READ: socket event 1
Jul 30 20:54:29.099: TPLUS(00000000)/0/READ: read entire 28 bytes response
Jul 30 20:54:29.099: TPLUS(00000000)/0/2B2DC1AC: Processing the reply packet
Jul 30 20:54:29.099: TPLUS: Received authen response status GET_PASSWORD (8)
Jul 30 20:54:29.099: TPLUS: Queuing AAA Authentication request 0 for processing
Jul 30 20:54:29.099: TPLUS: processing authentication continue request id 0
Jul 30 20:54:29.099: TPLUS: Authentication continue packet generated for 0
Jul 30 20:54:29.099: TPLUS(00000000)/0/WRITE/2B2DC1AC: Started 5 sec timeout
Jul 30 20:54:29.099: TPLUS(00000000)/0/WRITE: wrote entire 25 bytes request
Jul 30 20:54:29.103: TPLUS(00000000)/0/READ: socket event 1
Jul 30 20:54:29.103: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 6 bytes data)
Jul 30 20:54:29.103: TPLUS(00000000)/0/READ: socket event 1
Jul 30 20:54:29.103: TPLUS(00000000)/0/READ: read entire 18 bytes response
Jul 30 20:54:29.103: TPLUS(00000000)/0/2B2DC1AC: Processing the reply packet
Jul 30 20:54:29.103: TPLUS: Received authen response status PASS (2)
```

Häufige Probleme

Das häufigste Problem ist die Konfiguration. Oft legt der Administrator den AAA-Gruppenserver ein, aktualisiert die aaa-Zeilen jedoch nicht so, dass sie auf die Servergruppe zeigen. Anstatt:

```
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 tacacs+ local
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting exec default start-stop group tacacs+
```

Aktualisieren Sie einfach die Konfiguration mit der richtigen Servergruppe.

Ein zweites häufiges Problem ist, dass ein Benutzer diesen Fehler erhält, 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 dies der Fall ist, stellen Sie sicher, dass die IOS-Version VRF TACACS+ unterstützt. Hier einige gängige Mindestversionen:

- 12,3(7)T
- 12.2(33)SRA1
- 12.2(33)SXI
- 12.2(33)SXH4
- 12.2(54)SG

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems