Risoluzione dei problemi IOS per VRF RADIUS

Sommario

Introduzione

RADIUS viene ampiamente utilizzato come protocollo di autenticazione per autenticare gli utenti per l'accesso alla rete. Un numero sempre maggiore di amministratori sta isolando il traffico di gestione utilizzando il routing e l'inoltro VPN (VRF). Per impostazione predefinita, l'autenticazione, l'autorizzazione e l'accounting (AAA) su IOS® utilizza la tabella di routing predefinita per inviare i pacchetti. In questa guida viene descritto come configurare e risolvere i problemi relativi a RADIUS quando il server RADIUS si trova in un VRF.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- RAGGIO
- VRF
- AAA

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Informazioni sulle funzionalità

Essenzialmente, un VRF è una tabella di routing virtuale sul dispositivo. Quando il sistema operativo IOS prende una decisione di routing, se la funzione o l'interfaccia utilizza un VRF, le decisioni di routing vengono prese in base a tale tabella di routing VRF. In caso contrario, la feature utilizza la tabella di routing globale. Tenendo presente quanto segue, è possibile configurare RADIUS per l'utilizzo di un VRF:

```
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
```

Come si può vedere, non esistono server RADIUS definiti globalmente. Se si esegue la migrazione dei server in un VRF, è possibile rimuovere in modo sicuro i server RADIUS configurati globalmente.

Metodologia di risoluzione dei problemi

Attenersi alla seguente procedura:

1. Verificare di disporre della definizione di inoltro IPVRF corretta nel server del gruppo AAA, nonché dell'interfaccia di origine del traffico RADIUS.
2. Controllare la tabella di routing VRF e verificare che esista un percorso verso il server RADIUS. Per visualizzare la tabella di routing VRF, utilizzeremo l'esempio riportato sopra:

```
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. Èpossibile eseguire il ping del server RADIUS? Ricordate che questo deve essere specifico per 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. Èpossibile usare il comando **test aaa** per verificare la connettività (è necessario usare l'opzione new-code alla fine; l'eredità non funzionerà):

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

USER ATTRIBUTES

username             "cisco"
```

Se i percorsi sono corretti e non si notano accessi al server RADIUS, verificare che gli ACL consentano alla porta UDP 1645/1646 o alla porta UDP 1812/1813 di raggiungere il server dal router o dallo switch. Se si verifica un errore di autenticazione, risolvere il problema normalmente. La funzione VRF serve solo per il routing del pacchetto.

Analisi dei dati

Se tutto sembra corretto, è possibile abilitare i comandi **aaa** e **radius debug** per risolvere il problema. Avviare con questi comandi **di debug**:

- **raggio di debug**
- **debug autenticazione aaa**

Di seguito è riportato un esempio di **debug** in cui un elemento non è configurato correttamente, ad esempio ma non limitato a:

- Interfaccia di origine RADIUS mancante
- Comandi di inoltro VRF IP mancanti nell'interfaccia di origine o nel server del gruppo AAA
- Nessuna route al server RADIUS nella tabella di routing VRF

```
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
```

Sfortunatamente, con RADIUS non vi è distinzione tra timeout e route mancante.

Di seguito è riportato un esempio di autenticazione riuscita:

```
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.
```

Problemi comuni

- Il problema più comune è quello della configurazione. Molte volte l'amministratore inserirà nel server del gruppo aaa ma non aggiornerà le righe aaa in modo che puntino al gruppo di server. Invece di questo:
  ```
  aaa authentication login default group management local
  aaa authorization exec default group management if-authenticated
  aaa accounting exec default start-stop group management
  ```
  L'amministratore inserirà quanto segue:

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

Èsufficiente aggiornare la configurazione con il gruppo di server corretto.

- Un secondo problema comune è che un utente vedrà questo errore quando tenta di aggiungere l'inoltro VRF IP nel gruppo di server:

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

Comando non trovato. Se viene visualizzato questo errore, verificare che la versione di IOS supporti per VRF RADIUS.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems