Risoluzione dei problemi TACACS+ IOS per VRF

Sommario

Introduzione

TACACS+ è ampiamente utilizzato come protocollo di autenticazione per autenticare gli utenti sui dispositivi di rete. Un numero sempre maggiore di amministratori sta segregando il traffico di gestione utilizzando VRF (VPN Routing and Forwarding). Per impostazione predefinita, AAA su IOS usa la tabella di routing predefinita per inviare i pacchetti. In questo documento viene descritto come configurare TACACS+ e risolvere i relativi problemi quando il server è in un VRF.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- TACACS+
- VRF

Componenti usati

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

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 questo, ecco come configurare TACACS+ per l'uso di un VRF (configurazione pertinente in grassetto):

```
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
```

Come si può vedere, non esistono server TACACS+ definiti a livello globale. Se si sta eseguendo la migrazione dei server a un VRF, è possibile rimuovere in modo sicuro i server TACACS+ configurati globalmente.

Metodologia di risoluzione dei problemi

1. Verificare di avere la definizione di inoltro ip vrf corretta nel server del gruppo aaa e l'interfaccia di origine del traffico TACACS+.
2. Controllare la tabella di routing vrf e verificare che sia disponibile un percorso al server TACACS+. L'esempio precedente viene usato per visualizzare la tabella di routing vrf:

```
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. Èpossibile eseguire il ping del server TACACS+? Tenere presente che questa impostazione deve essere specifica anche per VRF:

```
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. Èpossibile utilizzare il comando **test aaa** per verificare la connettività (è necessario utilizzare l'opzione new-code alla fine, la versione precedente non funziona):

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

USER ATTRIBUTES

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

Se le route sono attive e non si rilevano accessi al server TACACS+, verificare che gli ACL consentano alla porta TCP 49 di raggiungere il server dal router o dallo switch. Se si riceve un errore di autenticazione durante la risoluzione normale dei problemi relativi a TACACS+, la funzione VRF serve solo per il routing del pacchetto.

Analisi dei dati

Se tutto quanto sopra sembra corretto, è possibile abilitare i debug aaa e tacacs per risolvere il

problema. Inizia con questi debug:

- debug tacacs
- debug autenticazione aaa

Di seguito è riportato un esempio di debug in cui qualcosa non è configurato correttamente, ad esempio ma senza limitazioni:

- Interfaccia di origine TACACS+ mancante
- Comandi di inoltro ip vrf mancanti nell'interfaccia di origine o nel server del gruppo aaa
- Nessuna route al server TACACS+ nella tabella di routing VRF

```
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
```

Connessione riuscita:

```
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)
```

Problemi comuni

Il problema più comune è la configurazione. Molte volte l'amministratore inserisce nel server del gruppo aaa, ma non aggiorna le righe aaa in modo che puntino al gruppo di server. Anziché:

```
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 avrà inserito:

```
aaa authentication login default grout tacacs+ local
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting exec default start-stop group tacacs+
```
Èsufficiente aggiornare la configurazione con il gruppo di server corretto.

Un secondo problema comune è che un utente riceve 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. In questo caso, verificare che la versione di IOS supporti TACACS+ per VRF. Di seguito sono riportate alcune versioni minime comuni:

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

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems