Dépannage IOS par VRF RADIUS

Contenu

Introduction

RADIUS est largement utilisé comme protocole d'authentification pour authentifier les utilisateurs pour l'accès au réseau. De plus en plus d'administrateurs séparent leur trafic de gestion à l'aide du routage et transfert VPN (VRF). Par défaut, l'authentification, l'autorisation et la comptabilité (AAA) sur IOS® utilise la table de routage par défaut afin d'envoyer des paquets. Ce guide décrit comment configurer et dépanner RADIUS lorsque le serveur RADIUS se trouve dans un VRF.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- RADIUS
- VRF
- AAA

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations sur les fonctionnalités

Essentiellement, un VRF est une table de routage virtuelle sur le périphérique. Lorsque l'IOS prend une décision de routage, si la fonction ou l'interface utilise un VRF, les décisions de routage sont prises par rapport à cette table de routage VRF. Sinon, la fonction utilise la table de routage globale. Dans cet esprit, voici comment configurer RADIUS pour utiliser 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
```

Comme vous pouvez le voir, il n'existe aucun serveur RADIUS défini globalement. Si vous migrez les serveurs vers un VRF, vous pouvez supprimer en toute sécurité les serveurs RADIUS configurés globalement.

Méthodologie de dépannage

Procédez comme suit :

1. Assurez-vous d'avoir la définition de transfert IPVRF appropriée sous votre serveur de groupe AAA ainsi que l'interface source pour le trafic RADIUS.
2. Vérifiez votre table de routage VRF et assurez-vous qu'il existe une route vers votre serveur RADIUS. Nous allons utiliser l'exemple ci-dessus afin d'afficher la table de routage 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
      203.0.113.0/8 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. Pouvez-vous envoyer une requête ping à votre serveur RADIUS ? Souvenez-vous que ceci doit également être spécifique à 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. Vous pouvez utiliser la commande **test aaa** afin de vérifier la connectivité (vous devez utiliser l'option new-code à la fin ; l'héritage ne fonctionnera pas) :

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

USER ATTRIBUTES

username            "cisco"
```

Si les routes sont en place et que vous ne voyez aucun accès sur votre serveur RADIUS, assurez-vous que les listes de contrôle d'accès permettent au port udp 1645/1646 ou au port udp 1812/1813 d'atteindre le serveur à partir du routeur ou du commutateur. En cas d'échec de

l'authentification, dépannez RADIUS comme normal. La fonctionnalité VRF est uniquement destinée au routage du paquet.

Analyse des données

Si tout semble correct, les commandes **aaa** et **radius debug** peuvent être activées afin de résoudre le problème. Commencez par ces commandes **de débogage** :

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

Voici un exemple de **débogage** où quelque chose n'est pas configuré correctement, par exemple, mais sans s'y limiter :

- Interface source RADIUS manquante
- Commandes de transfert VRF IP manquantes sous l'interface source ou sous le serveur de groupe AAA
- Aucune route vers le serveur RADIUS dans la table de routage 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
```

Malheureusement, avec RADIUS il n'y a aucune distinction entre un délai d'attente et une route manquante.

Voici un exemple d'authentification réussie :

```
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.
```

Problèmes courants

- Le problème le plus courant est celui de la configuration. Souvent, l'administrateur place le serveur de groupe aaa mais ne met pas à jour les lignes aaa pour pointer vers le groupe de serveurs. Au lieu de cela :

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

  L'administrateur aura ajouté ceci :

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

Il vous suffit de mettre à jour la configuration avec le groupe de serveurs approprié.

- Un deuxième problème courant est qu'un utilisateur verra cette erreur lors de la tentative d'ajout de transfert VRF IP sous le groupe de serveurs :

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

Cela signifie que la commande est introuvable. Si vous voyez cette erreur, assurez-vous que la version de l'IOS prend en charge par RADIUS VRF.

Informations connexes

- Support et documentation techniques - Cisco Systems