اهحالصإو VRF لكل IOS ءاطخأ فاشكتسأ

المحتويات

المقدمة

يستخدم RADIUS بشكل مكثف كبروتوكول مصادقة لمصادقة المستخدمين للوصول إلى الشبكة. يقوم المزيد من المسؤولين بفصل حركة مرور الإدارة الخاصة بهم باستخدام توجيه وإعادة توجيه الشبكة الخاصة الظاهرية (VPN). بشكل افتراضي، تستخدم المصادقة والتفويض والمحاسبة (AAA) على IOS® جدول التوجيه الافتراضي لإرسال الحزم. يصف هذا الدليل كيفية تكوين RADIUS واستكشاف أخطائه وإصلاحها عندما يكون خادم RADIUS في VRF.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- RADIUS
- VRF
- AAA

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات الميزة

أساسا، VRF هو جدول توجيه ظاهري على الجهاز. عندما يتخذ IOS قرارا للتوجيه، إذا كانت الميزة أو الواجهة تستخدم التردد اللاسلكي (VRF)، يتم إتخاذ قرارات التوجيه مقابل جدول توجيه التردد اللاسلكي (VRF) هذا. وإلا، تستخدم الميزة جدول التوجيه العام. مع وضع هذا في الاعتبار، هنا كيف أنت تشكل RADIUS لاستخدام 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
```

كما ترى، لا توجد خوادم RADIUS معرفة بشكل عام. إذا كنت تقوم بترحيل الخوادم إلى نظام VRF، فيمكنك إزالة خوادم RADIUS التي تم تكوينها بشكل عام بأمان.

منهجية أستكشاف الأخطاء وإصلاحها

أكمل الخطوات التالية:

1. تأكد من أن لديك تعريف إعادة توجيه IPVRF المناسب تحت خادم مجموعة AAA وكذلك واجهة المصدر لحركة مرور RADIUS.
2. تحقق من جدول توجيه VRF الخاص بك وتأكد من وجود مسار إلى خادم RADIUS. سنستخدم المثال أعلاه. لعرض جدول توجيه التردد اللاسلكي (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
                    is variably subnetted, 2 subnets, 2 masks 203.0.113.0/8
                C        203.0.113.0/24 is directly connected, GigabitEthernet0/0
                L        203.0.113.2/32 is directly connected, GigabitEthernet0/0
```

3. هل يمكنك إختبار اتصال خادم RADIUS؟ تذكر أن هذا يجب أن يكون محددا بالترددات اللاسلكية الظاهرية أيضا:

```
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. يمكنك إستخدام الأمر **test aaa** للتحقق من الاتصال (يجب أن تستخدم خيار الرمز الجديد في النهاية؛ لن يعمل القديم):

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

USER ATTRIBUTES

"username              "cisco
```

إذا كانت الموجهات في موضعها ولم ترى أي نقاط وصول على خادم RADIUS، فتأكد من أن قوائم التحكم في الوصول (ACL) تسمح لمنفذ UDP 1645/1646 أو منفذ UDP 1812/1813 بالوصول إلى الخادم من الموجه أو المحول. إذا حدث فشل في المصادقة، فقم باستكشاف أخطاء RADIUS وإصلاحها كأمر عادي. ال VRF سمة فقط للتوجيه من الربط.

تحليل البيانات

إذا بدا كل شيء صحيحا، يمكن تمكين أوامر **aaa** و**radius debug** لاستكشاف الأخطاء وإصلاحها. ابدأ بهذه الأوامر **debug**:

- **تصحيح أخطاء radius**
- **تصحيح أخطاء مصادقة aaa (المصادقة والتفويض والمحاسبة)**

هنا مثال على **تصحيح** الأخطاء حيث لا يتم تكوين شيء بشكل صحيح، مثل وليس على سبيل المثال:

- واجهة مصدر RADIUS مفقودة
- أوامر إعادة توجيه IP VRF المفقودة تحت واجهة المصدر أو تحت خادم مجموعة AAA
- لا يوجد مسار إلى خادم RADIUS في جدول توجيه 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
                                                      FA 38 59 9C 5F D3 3A 33
                 *  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
```

ولسوء الحظ، مع RADIUS لا يوجد تمييز بين المهلة والمسار المفقود.

فيما يلي مثال على مصادقة ناجحة:

```
'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
                                                                  len 51 ,1645/1

- 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
```

مشاكل مشتركة

- والمشكلة الأكثر شيوعا هي مشكلة التكوين. في كثير من الأحيان، سيضع المسؤول في خادم مجموعة AAA ولكنه لا يقوم بتحديث بنود AAA للإشارة إلى مجموعة الخوادم. بدلا من هذا:

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

سيكون المسؤول قد وضع هذا في:

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

ما عليك سوى تحديث التكوين باستخدام مجموعة الخوادم الصحيحة.

- والمشكلة الشائعة الثانية هي أن المستخدم سيرى هذا الخطأ عند محاولة إضافة إعادة توجيه IP VRF تحت مجموعة الخوادم:

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

وهذا يعني أنه لم يتم العثور على الأمر. إذا رأيت هذا الخطأ، فتأكد من إصدار دعم IOS لكل VRF RADIUS.

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).