أستكشاف أخطاء IOS لكل VRF TACACS+ وإصلاحها

المحتويات

المقدمة

يتم إستخدام TACACS+ بشدة كبروتوكول مصادقة لمصادقة المستخدمين على أجهزة الشبكة. يقوم المزيد والمزيد من المسؤولين بفصل حركة مرور الإدارة الخاصة بهم باستخدام توجيه وإعادة توجيه الشبكة الخاصة الظاهرية (VRF). بشكل افتراضي، يستخدم AAA على IOS جدول التوجيه الافتراضي لإرسال الحزم. يوضح هذا المستند كيفية تكوين TACACS+ واستكشاف أخطائه وإصلاحها عندما يكون الخادم في وضع VRF.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- TACACS+
- VRFs

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

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. بوضع هذا الأمر في الاعتبار، فيما يلي كيفية تكوين TACACS+ لاستخدام VRF (تكوين ذو صلة بالخط الغامق):

```
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
```

كما ترى، لا توجد خوادم TACACS+ معرفة بشكل عام. إذا كنت تقوم بترحيل الخوادم إلى نظام VRF، فيمكنك إزالة

خوادم TACACS+ التي تم تكوينها بشكل آمن.

منهجية أستكشاف الأخطاء وإصلاحها

1. تأكد من أن لديك تعريف إعادة توجيه IP VRF المناسب تحت خادم مجموعة AAA وكذلك واجهة المصدر لحركة مرور TACACS+.
2. تحقق من جدول توجيه VRF الخاص بك وتأكد من وجود مسار إلى خادم TACACS+. يتم إستخدام المثال أعلاه لعرض جدول توجيه 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 203.0.0.0/24
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 TACACS+؟ تذكر أن هذا يحتاج أن يكون خاص بالترددات اللاسلكية الظاهرية (VRF) أيضا:

```
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. يمكنك إستخدام الأمر **test aaa** للتحقق من الاتصال (يجب أن تستخدم خيار التعليمات البرمجية الجديدة في النهاية، لا يعمل القديم):

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

                                        USER ATTRIBUTES

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

إذا كانت الموجهات في موضعها ولم ترى أي نتائج على خادم TACACS+، فتأكد من أن قوائم التحكم في الوصول (ACLs) تسمح لمنفذ TCP رقم 49 بالوصول إلى الخادم من الموجه أو المحول. إذا حصلت على فشل مصادقة في أستكشاف أخطاء TACACS+ وإصلاحها كأمر عادي، فإن ميزة VRF تكون فقط لتوجيه الحزمة.

تحليل البيانات

إذا بدا كل شيء أعلاه صحيحا، يمكن تمكين تصحيح أخطاء AAA و tacacs لاستكشاف المشكلة وإصلاحها. ابدأ بتصحيح الأخطاء التالية:

- debug tacacs
- تصحيح أخطاء مصادقة aaa (المصادقة والتفويض والمحاسبة)

فيما يلي مثال على تصحيح الأخطاء حيث لا يتم تكوين شيء بشكل صحيح، على سبيل المثال لا الحصر:

- واجهة مصدر TACACS+ مفقودة
- أوامر إعادة توجيه IP VRF مفقودة تحت الواجهة المصدر أو تحت خادم مجموعة AAA
- لا يوجد مسار إلى خادم TACACS+ في جدول توجيه 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
```

فيما يلي اتصال ناجح:

```
   '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
```

مشاكل مشتركة

المشكلة الأكثر شيوعا هي التكوين. عدة مرات يضعها المسؤول في خادم مجموعة AAA، ولكنه لا يقوم بتحديث بنود AAA للإشارة إلى مجموعة الخوادم. بدلا من:

```
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:

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

ما عليك سوى تحديث التكوين باستخدام مجموعة الخوادم الصحيحة.

المشكلة الشائعة الثانية هي أن المستخدم يستقبل 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 حدث هذا الأمر، فتأكد من أن إصدار IOS يدعم بروتوكول TACACS+ لكل VRF. فيما يلي بعض الإصدارات الدنيا الشائعة:

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

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).