تحليل سلوك إدارة جهاز AAA ل ASA

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
الرسم التخطيطي للشبكة
التكوين
الحالة 1: مصادقة ASA التي تم تكوينها عبر خادم AAA
الحالة 2: مصادقة ASA وتفويض EXEC الذي تم تكوينه عبر خادم AAA
الحالة 3: مصادقة ASA وتفويض EXEC وتفويض الأوامر التي تم تكوينها عبر خادم AAA
الحالة 4: مصادقة ASA، تفويض EXEC باستخدام "التمكين التلقائي" وتفويض الأوامر الذي تم تكوينه عبر خادم AAA
معلومات ذات صلة

المقدمة

يصف هذا المستند سلوك إدارة الجهاز عند تكوين ASA للمصادقة والتفويض باستخدام خادم AAA. يوضح هذا المستند إستخدام محرك خدمة الهوية (ISE) من Cisco كخادم AAA مع Active Directory كمخزن الهوية الخارجي. TACACS+ هو بروتوكول AAA المستخدم.

تمت المساهمة بواسطة ديني شودجيل وبونام غارغ، مهندسو Cisco HTS

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية ب ASA CLI و ASDM
- الاتصال بين خادم ASA و AAA
- تكوين AAA على Cisco ISE للمصادقة والتفويض

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدار البرنامج التالي:

- ASAv جار 9.9(2)
- Cisco Identity Service Engine، الإصدار 2.6

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

معلومات أساسية

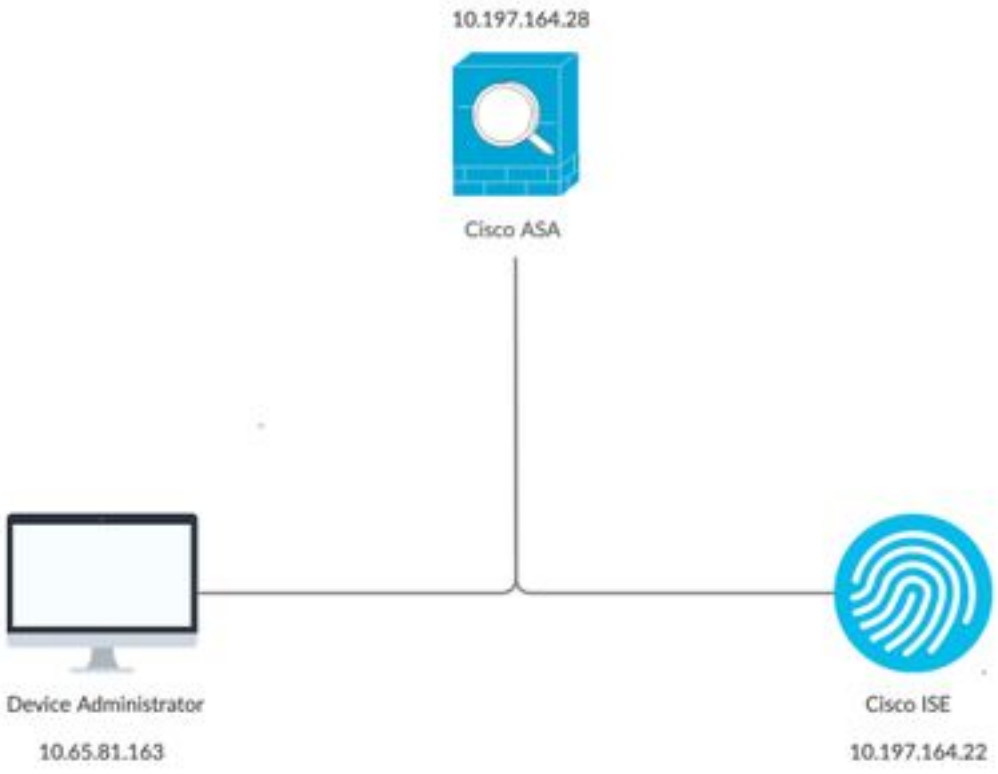
يدعم ASA من Cisco مصادقة الجلسات الإدارية باستخدام قاعدة بيانات مستخدم محلية أو خادم RADIUS أو خادم TACACS+. يمكن أن يتصل المسؤول ب Cisco ASA عبر:

- Telnet
- القشرة الآمنة (SSH)
- اتصال وحدة التحكم التسلسلية
- مدير أجهزة ASA (ASDM) من Cisco

في حالة الاتصال عبر برنامج Telnet أو SSH، يمكن للمستخدم إعادة محاولة المصادقة ثلاث مرات في حالة حدوث خطأ للمستخدم. بعد المرة الثالثة، يتم إغلاق جلسة المصادقة والاتصال ب Cisco ASA.

قبل بدء التكوين، يجب تحديد قاعدة بيانات المستخدم التي ستستخدمها (خادم AAA المحلي أو الخارجي). إذا كنت تستخدم خادم AAA خارجي، كما تم تكوينه في هذا المستند، فعليك تكوين مجموعة خوادم AAA والمضيف كما هو موضح في الأقسام التالية. يمكنك إستخدام أوامر مصادقة AAA وتفويض AAA لطلب المصادقة والتحقق من التفويض على التوالي عند الوصول إلى Cisco ASA للإدارة.

الرسم التخطيطي للشبكة



التكوين

هذه هي المعلومات المستخدمة لجميع الأمثلة الواردة في هذا المستند.

أ) تهيئة ASA:

```
aaa-server ISE protocol tacacs+
aaa-server ISE (internet) host 10.197.164.22
key *****
```

ب) تكوين AAA:

يتم إجراء المصادقة على خادم AAA مقابل تسلسل مخزن الهويات الذي يتكون من AD وقاعدة البيانات المحلية

الحالة 1: مصادقة ASA التي يتم تكوينها عبر خادم AAA

في ASA:

```
aaa authentication ssh console ISE LOCAL
```

على خادم AAA:

نتائج التخويل:

أ) ملف تعريف الصدفة

امتياز افتراضي: 1
الحد الأقصى للامتياز: 15

ب) مجموعة الأوامر
السماح للجميع

سلوك المسؤول:

```
Connection to 10.197.164.28 closed.
DMOUDGIL-M-N1D9:~ dmoudgil$
DMOUDGIL-M-N1D9:~ dmoudgil$
DMOUDGIL-M-N1D9:~ dmoudgil$ ssh ASA_priv1@10.197.164.28
ASA_priv1@10.197.164.28's password:
User ASA_priv1 logged in to ciscoasa
Logins over the last 9 days: 11. Last login: 12:59:51 IST May 7 2020 from 10.65.81.163
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
ciscoasa#
ciscoasa# show curpriv
Username : enable_15
Current privilege level : 15
```

```
Current Mode/s : P_PRIV
```

سجلات ASA:

```
May 07 2020 12:57:26: %ASA-6-113008: AAA transaction status ACCEPT : user = ASA_priv1
May 07 2020 12:57:26: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 07 2020 12:57:26: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 07 2020 12:57:26: %ASA-6-605005: Login permitted from 10.65.81.163/56048 to
internet:10.197.164.28/ssh for user "ASA_priv1"
May 07 2020 12:57:30: %ASA-7-111009: User 'enable_15' executed cmd: show logging
May 07 2020 12:57:40: %ASA-5-502103: User priv level changed: Uname: enable_15 From: 1 To: 15
May 07 2020 12:57:40: %ASA-5-111008: User 'ASA_priv1' executed the 'enable' command.
```

ملاحظات:

1. يتم إجراء مصادقة جلسة SSH عبر خادم AAA
2. يتم إجراء التفويض محليا بغض النظر عن الامتياز الذي تم تكوينه على خادم AAA في نتيجة التفويض
3. بعد مصادقة المستخدم عبر خادم AAA، عندما يدخل المستخدم الكلمة الأساسية "enable" (والتي ليس لها كلمة مرور معينة بشكل افتراضي) أو يدخل كلمة مرور enable (في حالة تكوينها)، يكون اسم المستخدم المتطابق المستخدم هو **enable_15**

```
May 07 2020 12:57:40: %ASA-5-502103: User priv level changed: Uname: enable_15 From: 1 To: 15
```

4. التقصير امتياز ل enable كلمة 15 ام لم يعين أنت يمكن كلمة مع امتياز خاص. على سبيل المثال:

```
enable password C!sco123 level 9
```

5. إذا كنت تستخدم enable مع امتياز مختلف، ال يمائل username أن يأتي على ASA **enable_x** (حيث x يكون الامتياز)

```
May 07 2020 13:20:49: %ASA-5-502103: User priv level changed: Uname: enable_8 From: 1 To: 8
```

الحالة 2: مصادقة ASA وتفويض EXEC الذي يتم تكوينه عبر خادم AAA

في ASA:

```
aaa authentication ssh console ISE LOCAL
aaa authorization exec authentication-server
```

على خادم AAA:

نتائج التخويل:

أ) ملف تعريف الصدفة

امتياز افتراضي: 1
الحد الأقصى للامتياز: 15

ب) مجموعة الأوامر
السماح للجميع

سلوك المستخدم:

```
DMOUDGIL-M-N1D9:~ dmoudgil$ ssh ASA_priv1@10.197.164.28
ASA_priv1@10.197.164.28's password:
User ASA_priv1 logged in to ciscoasa
Logins over the last 1 days: 8. Last login: 14:12:52 IST May 7 2020 from 10.65.81.163
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ciscoasa> show curpriv
Username : ASA_priv1
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa> enable
Password:
ciscoasa# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
```

سجلات ASA:

```
May 07 2020 13:59:54: %ASA-6-113004: AAA user authentication Successful : server = 10.197.164.22
: user = ASA_priv1
May 07 2020 13:59:54: %ASA-6-302013: Built outbound TCP connection 75 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/49068
(10.197.164.28/49068)
May 07 2020 13:59:54: %ASA-6-113004: AAA user authorization Successful : server = 10.197.164.22
: user = ASA_priv1
May 07 2020 13:59:54: %ASA-6-113008: AAA transaction status ACCEPT : user = ASA_priv1
May 07 2020 13:59:54: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 07 2020 13:59:54: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 07 2020 13:59:54: %ASA-6-605005: Login permitted from 10.65.81.163/57671 to
internet:10.197.164.28/ssh for user "ASA_priv1"
May 07 2020 13:59:59: %ASA-5-502103: User priv level changed: Uname: enable_15 From: 1 To: 15
May 07 2020 13:59:59: %ASA-5-111008: User 'ASA_priv1' executed the 'enable' command.
```

ملاحظات:

1. يتم إجراء المصادقة وتفويض EXEC عبر خادم AAA
2. يحكم تفويض EXEC امتياز المستخدم لجميع طلبات إتصالات وحدة التحكم (SSH، و telnet، و enable) التي تم تكوينها للمصادقة

ملاحظة: لا يشمل ذلك الاتصال التسلسلي بهيئة المعايير الفدرالية

3. يتم تكوين خادم AAA بطريقة توفر الامتياز الافتراضي 1 والامتياز الأقصى البالغ 15

نتيجة للتخويل
4. عندما يقوم المستخدم بتسجيل الدخول إلى ASA عبر بيانات اعتماد +TACACS التي تم تكوينها على خادم AAA، يتم منح المستخدم في البداية امتياز 1 بواسطة خادم AAA
5. أو (إن لم يكن يشكل ملكة) ثانوية يدخل "enable"، المفتاح الكلمة المستعمل يدخل أن يمكن ما إن 15 إلى يتغير الامتياز حيث امتياز ذو الوضع إلى يدخلون هم ،(إن يشكل) ملكة enable يدخل

الحالة 3: مصادقة ASA وتفويض EXEC وتفويض الأوامر التي يتم تكوينها عبر خادم AAA

في ASA:

```
aaa authentication ssh console ISE LOCAL
aaa authorization exec authentication-server
aaa authorization command ISE LOCAL
```

على خادم AAA:

نتائج التخويل:

أ) ملف تعريف الصدفة

  امتياز افتراضي: 1
  الحد الأقصى للامتياز: 15

ب) مجموعة الأوامر
  السماح للجميع

سلوك المسؤول:

```
DMOUDGIL-M-N1D9:~ dmoudgil$ ssh ASA_priv1@10.197.164.28
ASA_priv1@10.197.164.28's password:
User ASA_priv1 logged in to ciscoasa
Logins over the last 1 days: 7. Last login: 17:12:23 IST May 9 2020 from 10.65.81.163
Failed logins since the last login: 0. Last failed login: 17:12:21 IST May 9 2020 from
10.65.81.163
Type help or '?' for a list of available commands.
ciscoasa> show curpriv
Username : ASA_priv1
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa> enable
Password:
ciscoasa# show curpriv
Command authorization failed
```

سجلات ASA:

```
May 09 2020 17:13:05: %ASA-6-113004: AAA user authentication Successful : server = 10.197.164.22
: user = ASA_priv1
May 09 2020 17:13:05: %ASA-6-302013: Built outbound TCP connection 170 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/21275
(10.197.164.28/21275)
May 09 2020 17:13:05: %ASA-6-302014: Teardown TCP connection 169 for internet:10.197.164.22/49
```

```
to identity:10.197.164.28/30256 duration 0:00:00 bytes 67 TCP Reset-I from internet
May 09 2020 17:13:05: %ASA-6-113004: AAA user authorization Successful : server = 10.197.164.22
: user = ASA_priv1
May 09 2020 17:13:05: %ASA-6-113008: AAA transaction status ACCEPT : user = ASA_priv1
May 09 2020 17:13:05: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 09 2020 17:13:05: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 09 2020 17:13:05: %ASA-6-605005: Login permitted from 10.65.81.163/49218 to
internet:10.197.164.28/ssh for user "ASA_priv1"
May 09 2020 17:13:05: %ASA-6-302014: Teardown TCP connection 170 for internet:10.197.164.22/49
to identity:10.197.164.28/21275 duration 0:00:00 bytes 61 TCP Reset-I from internet
May 09 2020 17:13:05: %ASA-7-609002: Teardown local-host internet:10.197.164.22 duration 0:00:00
May 09 2020 17:13:07: %ASA-7-609001: Built local-host internet:10.197.164.22
May 09 2020 17:13:07: %ASA-6-302013: Built outbound TCP connection 171 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/53081
(10.197.164.28/53081)
May 09 2020 17:13:07: %ASA-7-111009: User 'ASA_priv1' executed cmd: show curpriv
May 09 2020 17:13:08: %ASA-6-302014: Teardown TCP connection 171 for internet:10.197.164.22/49
to identity:10.197.164.28/53081 duration 0:00:00 bytes 82 TCP Reset-I from internet
May 09 2020 17:13:08: %ASA-7-609002: Teardown local-host internet:10.197.164.22 duration 0:00:00
May 09 2020 17:13:10: %ASA-5-502103: User priv level changed: Uname: enable_15 From: 1 To: 15
May 09 2020 17:13:10: %ASA-5-111008: User 'ASA_priv1' executed the 'enable' command.
May 09 2020 17:13:12: %ASA-7-609001: Built local-host internet:10.197.164.22
May 09 2020 17:13:12: %ASA-6-302013: Built outbound TCP connection 172 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/46803
(10.197.164.28/46803)
May 09 2020 17:13:12: %ASA-6-113016: AAA credentials rejected : reason = Unspecified : server =
10.197.164.22 : user = ***** : user IP = 10.65.81.163
May 09 2020 17:13:12: %ASA-6-302014: Teardown TCP connection 172 for internet:10.197.164.22/49
to identity:10.197.164.28/46803 duration 0:00:00 bytes 82 TCP Reset-I from internet
May 09 2020 17:13:12: %ASA-7-609002: Teardown local-host internet:10.197.164.22 duration 0:00:00
May 09 2020 17:13:20: %ASA-7-609001: Built local-host internet:10.197.164.22
May 09 2020 17:13:20: %ASA-6-302013: Built outbound TCP connection 173 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/6934 (10.197.164.28/6934)
May 09 2020 17:13:20: %ASA-6-113016: AAA credentials rejected : reason = Unspecified : server =
10.197.164.22 : user = ***** : user IP = 10.65.81.163
```

تاظحالم:

1. متي ءارجإ ضيوفتو ةقداصملا EXEC ربع AAA مداخ
2. متي ضيوفت مكحت EXEC زايتما مدختسملل عيمجل تابلط تالاصتإ ةدحو مكحتلا (SSH، و telnet، و enable) يتلا مت اهنيوكت ةقداصملل
3. متي ذيفنت ضيوفتلا رماوألا رمأ" AAA ISE ضيوفت رمأ" مادختساب ةطساوب مداخ AAA LOCAL"

ةظحالم: ال لمشي كلذ لاصتالا يلسلستلا ةئيهب رييعاملا ةيدارفإلا

4. امدنع موقي مدختسملا ليجستب لوخدلا ىلإ ASA ربع تانايب دامتعا TACACS+ يتلا مت اهنيوكت ىلع مداخ AAA، متي حنم مدختسملا يف ةيادبلا زايتما 1 ةطساوب مداخ AAA
5. ام نإ لخدي مدختسملا لمعتسملا ةملكلا حاتفملا "enable"، لخدي ةيناث (نإ نكمي ةملك ال لكشي وأ (لكشي نإ) ةملك enable لخدي) مه نولخدي ىلإ عضولا وذ زايتما ثيح زايتمالا ريغتي ىلإ 15
6. لشفي ضيوفت رماوألا يف اذه ويرانيسلا ثيح متي ضرعي رمألا يذلا ءارجإ مداخ AAA نأل نيوكتلا هرادصإ مدختسملا مسا ةطساوب "enable_15" الدب نم مدختسملا يذلا مت ليجست هلوخد ايلعف يذلاو تمت هتقداصم.
7. لشفيس رماوألا ضيوفت ببسب اضيأ ةدوجوم ةسلج يف هذيفنت متي رمأ يأ
8. ةجلاعمل هذه ةلكشملا، مق ءاشنإب مدختسم مساب "enable_15" ىلع مداخ AAA وأ ىلع AD و ASA (خسنلل ةيطايتحالا ةيلحملا) مادختساب ةملك رورم ةيئاوشع

بمجرد تكوين المستخدم على خادم AAA أو AD، يتم ملاحظة السلوك التالي:

i. للتحقق من المصادقة الأولية، يتحقق خادم AAA من اسم المستخدم الحقيقي للمستخدم الذي قام بتسجيل الدخول
ii. بمجرد إدخال كلمة مرور enable ، يتم التحقق منها محليا على ASA لأن enable authentication تم تكوينه في AAA إلى إشارة الخادم
iii. بعد تكوين كلمة المرور، يتم تنفيذ جميع الأوامر باستخدام اسم المستخدم "enable_15" وتسمح المصادقة والتفويض والمحاسبة (AAA) بهذه الأوامر بموجب وجود اسم المستخدم هذا على خادم AAA أو AD

بمجرد تكوين المستخدم "enable_15"، يتم السماح للمؤول بالانتقال من وضع الامتيازات إلى وضع التكوين على ASA.

سلوك المؤول:

```
DMOUDGIL-M-N1D9:~ dmoudgil$ ssh ASA_priv1@10.197.164.28
ASA_priv1@10.197.164.28's password:
User ASA_priv1 logged in to ciscoasa
Logins over the last 1 days: 2. Last login: 16:50:42 IST May 9 2020 from 10.65.81.163
Failed logins since the last login: 5. Last failed login: 16:53:55 IST May 9 2020 from
10.65.81.163
Type help or '?' for a list of available commands.
ciscoasa> show curpriv
Username : ASA_priv1
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa> enable
Password:
ciscoasa# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
ciscoasa# configure terminal
```

سجلات ASA:

```
May 09 2020 17:05:29: %ASA-6-113004: AAA user authentication Successful : server = 10.197.164.22
: user = ASA_priv1
May 09 2020 17:05:29: %ASA-6-302013: Built outbound TCP connection 113 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/31109
(10.197.164.28/31109)
May 09 2020 17:05:29: %ASA-6-113004: AAA user authorization Successful : server = 10.197.164.22
: user = ASA_priv1
May 09 2020 17:05:29: %ASA-6-113008: AAA transaction status ACCEPT : user = ASA_priv1
May 09 2020 17:05:29: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 09 2020 17:05:29: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 09 2020 17:05:29: %ASA-6-302014: Teardown TCP connection 112 for internet:10.197.164.22/49
to identity:10.197.164.28/7703 duration 0:00:00 bytes 67 TCP Reset-I from internet
May 09 2020 17:05:29: %ASA-6-605005: Login permitted from 10.65.81.163/65524 to
internet:10.197.164.28/ssh for user "ASA_priv1"
May 09 2020 17:05:29: %ASA-6-302014: Teardown TCP connection 113 for internet:10.197.164.22/49
to identity:10.197.164.28/31109 duration 0:00:00 bytes 61 TCP Reset-I from internet
May 09 2020 17:05:29: %ASA-7-609002: Teardown local-host internet:10.197.164.22 duration 0:00:00
```

```
May 09 2020 17:05:32: %ASA-7-609001: Built local-host internet:10.197.164.22
May 09 2020 17:05:32: %ASA-6-302013: Built outbound TCP connection 114 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/64339
(10.197.164.28/64339)
May 09 2020 17:05:32: %ASA-7-111009: User 'ASA_priv1' executed cmd: show curpriv
May 09 2020 17:05:32: %ASA-6-302014: Teardown TCP connection 114 for internet:10.197.164.22/49
to identity:10.197.164.28/64339 duration 0:00:00 bytes 82 TCP Reset-I from internet
May 09 2020 17:05:32: %ASA-7-609002: Teardown local-host internet:10.197.164.22 duration 0:00:00
May 09 2020 17:05:35: %ASA-5-502103: User priv level changed: Uname: enable_15 From: 1 To: 15
May 09 2020 17:05:35: %ASA-5-111008: User 'ASA_priv1' executed the 'enable' command.
May 09 2020 17:05:37: %ASA-7-609001: Built local-host internet:10.197.164.22
May 09 2020 17:05:37: %ASA-6-302013: Built outbound TCP connection 115 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/4236 (10.197.164.28/4236)
May 09 2020 17:05:37: %ASA-7-111009: User 'enable_15' executed cmd: show curpriv
May 09 2020 17:05:37: %ASA-6-302014: Teardown TCP connection 115 for internet:10.197.164.22/49
to identity:10.197.164.28/4236 duration 0:00:00 bytes 82 TCP Reset-I from internet
May 09 2020 17:05:37: %ASA-7-609002: Teardown local-host internet:10.197.164.22 duration 0:00:00
May 09 2020 17:05:44: %ASA-7-609001: Built local-host internet:10.197.164.22
May 09 2020 17:05:44: %ASA-6-302013: Built outbound TCP connection 116 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/27478
(10.197.164.28/27478)
May 09 2020 17:05:44: %ASA-5-111007: Begin configuration: 10.65.81.163 reading from terminal
May 09 2020 17:05:44: %ASA-5-111008: User 'enable_15' executed the 'configure terminal' command.
May 09 2020 17:05:44: %ASA-5-111010: User 'enable_15', running 'CLI' from IP 10.65.81.163,
executed 'configure terminal'
```

ةظحالم: اذإ مت نيوكت ضيوفت رماوألا ربع TACACS ىلع ASA، نمف يمازلإلا دوجو "يلحم" ةميقك ةيطايتحإ امدنع نوكي مداخ AAA ريغ لباق لوصولل هيلإ. كلذو نأل ضيوفت رماوألا قبطي ىلع عيمج تاسلج لمع ASA (ةدحو مكحتلا ةيلسلستلا، SSH، telnet) ىتح دنع مدع نيوكت ةقداصملا ةدحول مكحتلا ةيلسلستلا. يف هذه ةلاحلا يتلا نوكي اهيف مداخ AAA ريغ لباق لوصولل مدختسملاو "enable_15" ريغ دوجوم يف ةدعاق تانايبلا ةيلحملا، لصحي لوؤسملا ىلع أطخلا يلاتلا:

ليوختلا يطايتحالا. مسا مدختسملا 'enable_15' ريغ دوجوم يف ةدعاق تانايبلا ةيلحملا لشف ضيوفت رماوألا

تالجس ASA:

```
%ASA-4-409023: Attempting AAA Fallback method LOCAL for Authentication request for user cisco :
Auth-server group ISE unreachable
%ASA-6-113012: AAA user authentication Successful : local database : user = cisco
%ASA-4-409023: Attempting AAA Fallback method LOCAL for Authentication request for user cisco :
Auth-server group ISE unreachable
%ASA-6-113004: AAA user authorization Successful : server = LOCAL : user = cisco
%ASA-6-113008: AAA transaction status ACCEPT : user = cisco
%ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163, Uname: cisco
%ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163, Uname: cisco
%ASA-6-605005: Login permitted from 10.65.81.163/65416 to internet:10.197.164.28/ssh for user
"cisco"
%ASA-5-502103: User priv level changed: Uname: enable_15 From: 1 To: 15
%ASA-5-111008: User 'cisco' executed the 'enable' command.
%ASA-4-409023: Attempting AAA Fallback method LOCAL for Authorization request for user enable_15
: Auth-server group ISE unreachable
%ASA-5-111007: Begin configuration: 10.65.81.163 reading from terminal
%ASA-5-111008: User 'enable_15' executed the 'configure terminal' command.
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 10.65.81.163, executed 'configure
terminal'
```

```
%ASA-4-409023: Attempting AAA Fallback method LOCAL for Authorization request for user enable_15
: Auth-server group ISE unreachable
```

ملاحظة: باستخدام التكوين المذكور أعلاه، سيعمل تفويض الأوامر ولكن ستظل عملية محاسبة الأوامر تعرض اسم المستخدم "enable_15" بدلا من اسم المستخدم الحقيقي للمستخدم الذي قام بتسجيل الدخول. ويصبح من الصعب على المسؤولين تحديد المستخدم الذي نفذ أي أمر معين على ASA.

لمعالجة هذه المشكلة المحاسبية المتعلقة بمستخدم "enable_15":

1. أستخدم الكلمة الأساسية **auto-enable** في أمر تفويض EXEC على ASA
2. قم بتعيين المايتاز الافتراضي والأقصى إلى 15 في ملف تعريف طبقة TACACS المعين للمستخدم المصدق عليه

الحالة 4: مصادقة ASA، تفويض EXEC باستخدام "التمكين التلقائي" وتفويض الأوامر الذي تم تكوينه عبر خادم AAA

في ASA:

```
aaa authentication ssh console ISE LOCAL
aaa authorization exec authentication-server auto-enable
aaa authorization command ISE LOCAL
```

على خادم AAA:

نتائج التخويل:

أ) ملف تعريف الصدفة

المايتاز الافتراضي: 15
الحد الأقصى للمايتاز: 15

ب) مجموعة الأوامر
السماح للجميع

سلوك المسؤول:

```
DMOUDGIL-M-N1D9:~ dmoudgil$ ssh ASA_priv1@10.197.164.28
ASA_priv1@10.197.164.28's password:
User ASA_priv1 logged in to ciscoasa
Logins over the last 1 days: 8. Last login: 17:13:05 IST May 9 2020 from 10.65.81.163
Failed logins since the last login: 0. Last failed login: 17:12:21 IST May 9 2020 from
10.65.81.163
Type help or '?' for a list of available commands.
ciscoasa# show curpriv
Username : ASA_priv1
Current privilege level : 15
Current Mode/s : P_PRIV
ciscoasa# configure terminal
ciscoasa(config)#
```

سجلات ASA:

```
May 09 2020 17:40:04: %ASA-6-113004: AAA user authentication Successful : server = 10.197.164.22
: user = ASA_priv1
May 09 2020 17:40:04: %ASA-6-302013: Built outbound TCP connection 298 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/57617
(10.197.164.28/57617)
May 09 2020 17:40:04: %ASA-6-113004: AAA user authorization Successful : server = 10.197.164.22
: user = ASA_priv1
May 09 2020 17:40:04: %ASA-6-113008: AAA transaction status ACCEPT : user = ASA_priv1
May 09 2020 17:40:04: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 09 2020 17:40:04: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 09 2020 17:40:04: %ASA-6-605005: Login permitted from 10.65.81.163/49598 to
internet:10.197.164.28/ssh for user "ASA_priv1"
May 09 2020 17:40:04: %ASA-6-302014: Teardown TCP connection 297 for internet:10.197.164.22/49
to identity:10.197.164.28/6083 duration 0:00:00 bytes 67 TCP Reset-I from internet
May 09 2020 17:40:04: %ASA-7-609001: Built local-host internet:139.59.219.101
May 09 2020 17:40:04: %ASA-6-302015: Built outbound UDP connection 299 for
internet:139.59.219.101/123 (139.59.219.101/123) to mgmt-gateway:192.168.100.4/123
(10.197.164.28/195)
May 09 2020 17:40:04: %ASA-6-302014: Teardown TCP connection 298 for internet:10.197.164.22/49
to identity:10.197.164.28/57617 duration 0:00:00 bytes 61 TCP Reset-I from internet
May 09 2020 17:40:04: %ASA-7-609002: Teardown local-host internet:10.197.164.22 duration 0:00:00
May 09 2020 17:40:09: %ASA-7-609001: Built local-host internet:10.197.164.22
May 09 2020 17:40:09: %ASA-6-302013: Built outbound TCP connection 300 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/4799 (10.197.164.28/4799)
May 09 2020 17:40:09: %ASA-7-111009: User 'ASA_priv1' executed cmd: show curpriv
May 09 2020 17:40:09: %ASA-6-302014: Teardown TCP connection 300 for internet:10.197.164.22/49
to identity:10.197.164.28/4799 duration 0:00:00 bytes 82 TCP Reset-I from internet
May 09 2020 17:40:09: %ASA-7-609002: Teardown local-host internet:10.197.164.22 duration 0:00:00
May 09 2020 17:40:14: %ASA-5-111007: Begin configuration: 10.65.81.163 reading from terminal
May 09 2020 17:40:14: %ASA-5-111008: User 'ASA_priv1' executed the 'configure terminal' command.
May 09 2020 17:40:14: %ASA-5-111010: User 'ASA_priv1', running 'CLI' from IP 10.65.81.163,
executed 'configure terminal'
```

ملاحظات:

1. يتم إجراء المصادقة وتفويض EXEC عبر خادم AAA
2. يحكم تفويض EXEC المتياز المستخدم لجميع طلبات إتصالات وحدة التحكم (telnet و ssh) و enable) التي تم تكوينها للمصادقة

ملاحظة: ال يشمل ذلك الاتصال التسلسلي بهيئة المعايير الإفرادية

3. يتم تنفيذ تفويض الأوامر بواسطة خادم AAA باستخدام الأمر "أمر تفويض AAA ISE LOCAL"
4. عندما يقوم المستخدم بتسجيل الدخول إلى ASA عبر بيانات اعتماد TACACS+ التي تم تكوينها على خادم AAA، يحصل المستخدم على المتياز 15 بواسطة خادم AAA وبالتالي يسجل الدخول إلى وضع الامتيازات
5. باستخدام التكوين المذكور أعلاه، ال يلزم على المستخدم إدخال enable password، و ال يلزم تكوين المستخدم "enable_15" على خادم ASA أو AAA.
6. سيقوم خادم AAA الآن بالإبلاغ عن طلب تفويض الأوامر الوارد من اسم المستخدم الحقيقي للمستخدم الذي قام بتسجيل الدخول

معلومات ذات صلة

فيما يلي بعض المستندات للمرجع المتعلقة بإدارة جهاز AAA ل ASA:

https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId--1046199281

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200207-ISE-2-0-ASA-CLI-TACACS-Authentication.pdf

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).