تكوين مصادقة TACACS+ على محول Arista باستخدام ISE

المحتويات

المقدمة

المتطلبات الأساسية

المكونات المستخدمة

الرسم التخطيطي للشبكة

التكوينات

تكوين TACACS+ على ISE

تكوين محول Arista

الخطوة 1. تمكين مصادقة TACACS+

الخطوة 2. حفظ التكوين

التحقق من الصحة

مراقبة ISE

استكشاف الأخطاء وإصلاحها

المشكلة 1

السبب المحتمل

المشكلة 2

السبب المحتمل

الحل

المقدمة

يوضح هذا المستند كيفية دمج Cisco ISE TACACS+ مع محول Arista للوصول المركزي عبر المصادقة والتفويض والمحاسبة (AAA) لوصول المسؤول.

المتطلبات الأساسية

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- بروتوكول ISE و TACACS+ من Cisco.
- محولات Arista

المكونات المستخدمة

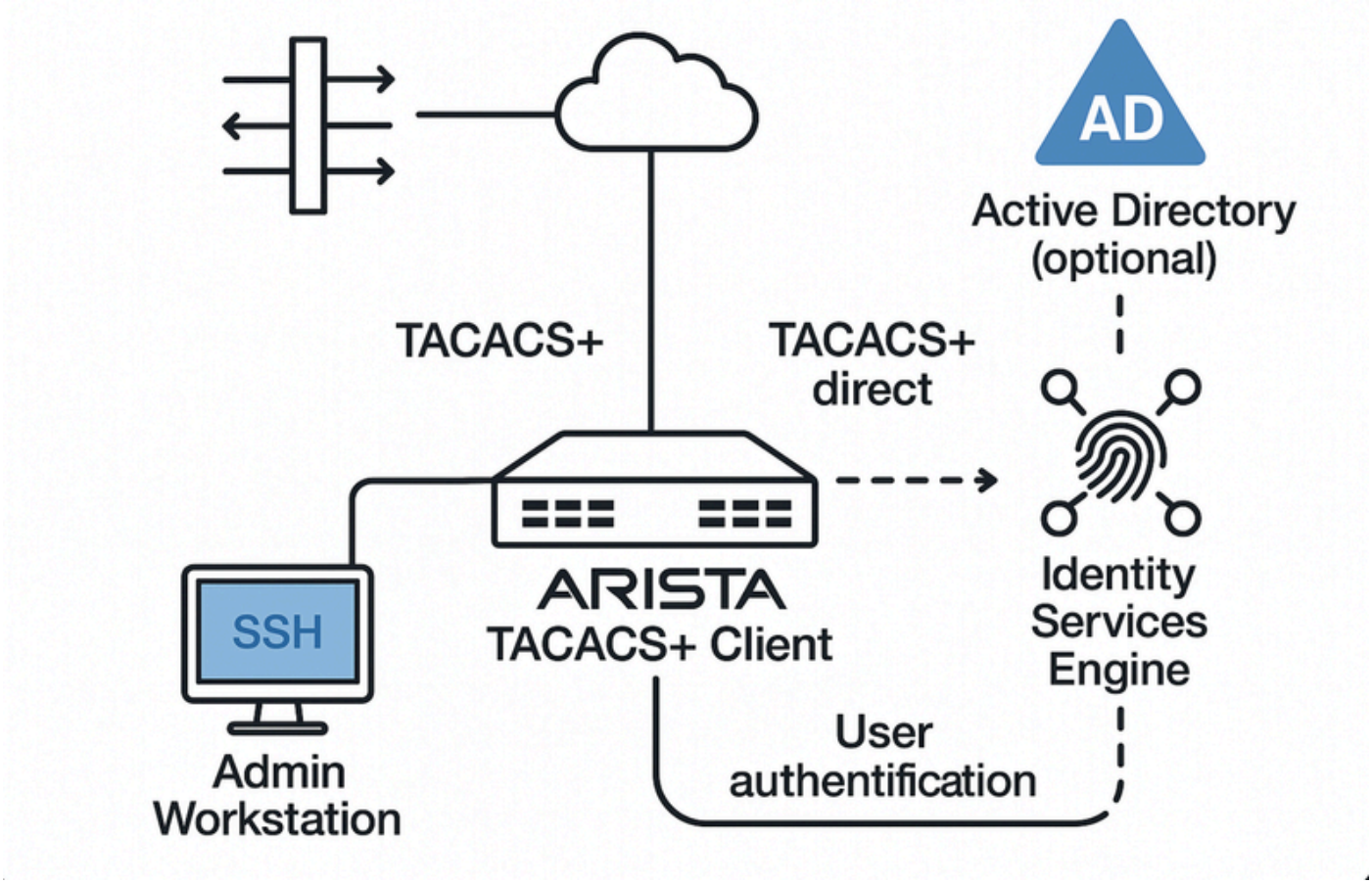
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- إصدار صورة برنامج المحول Arista Switch Software: 4,33,2 درجة فهرنهايت
- Cisco Identity Services Engine (ISE)، الإصدار 3.3 Patch 4

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

الرسم التخطيطي للشبكة

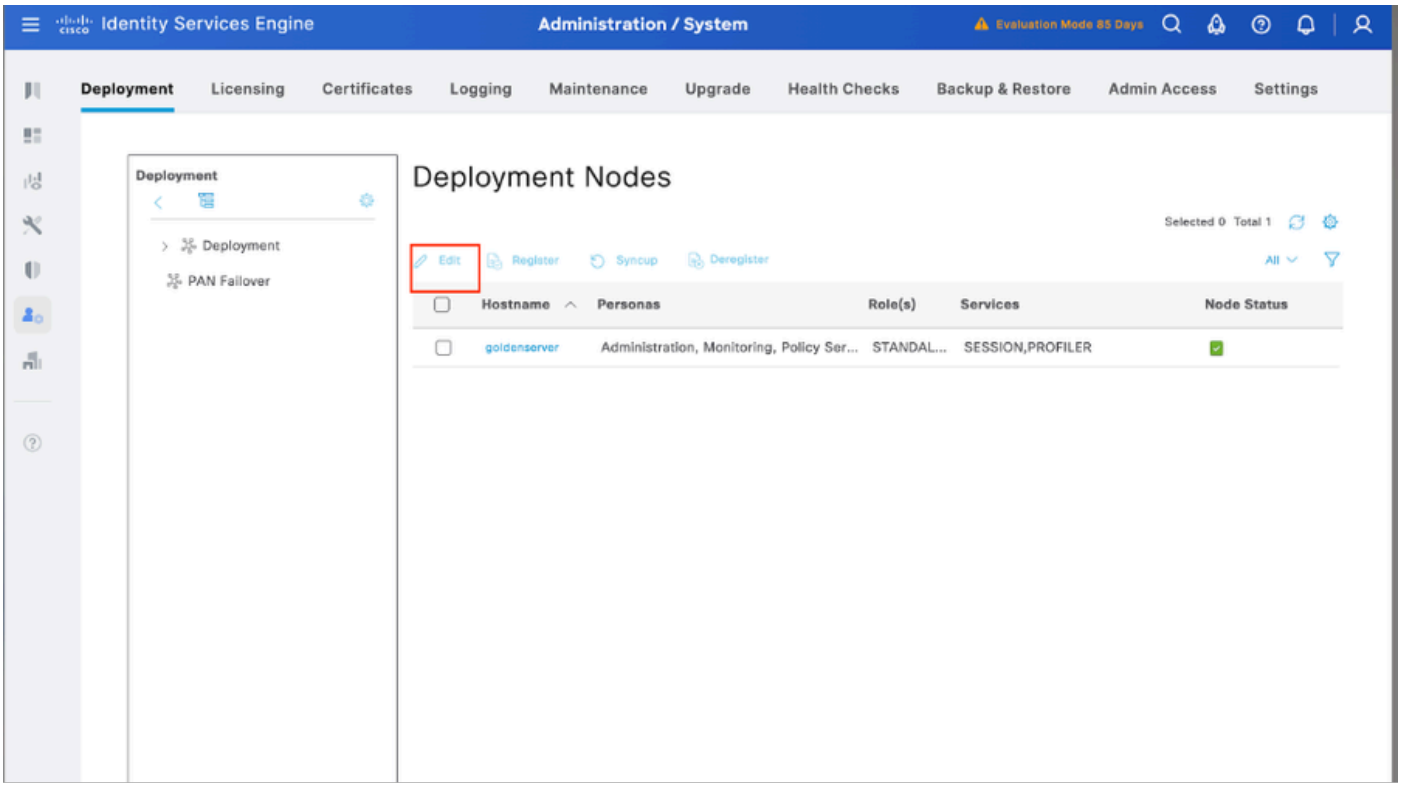


التكوينات

تكوين TACACS+ على ISE

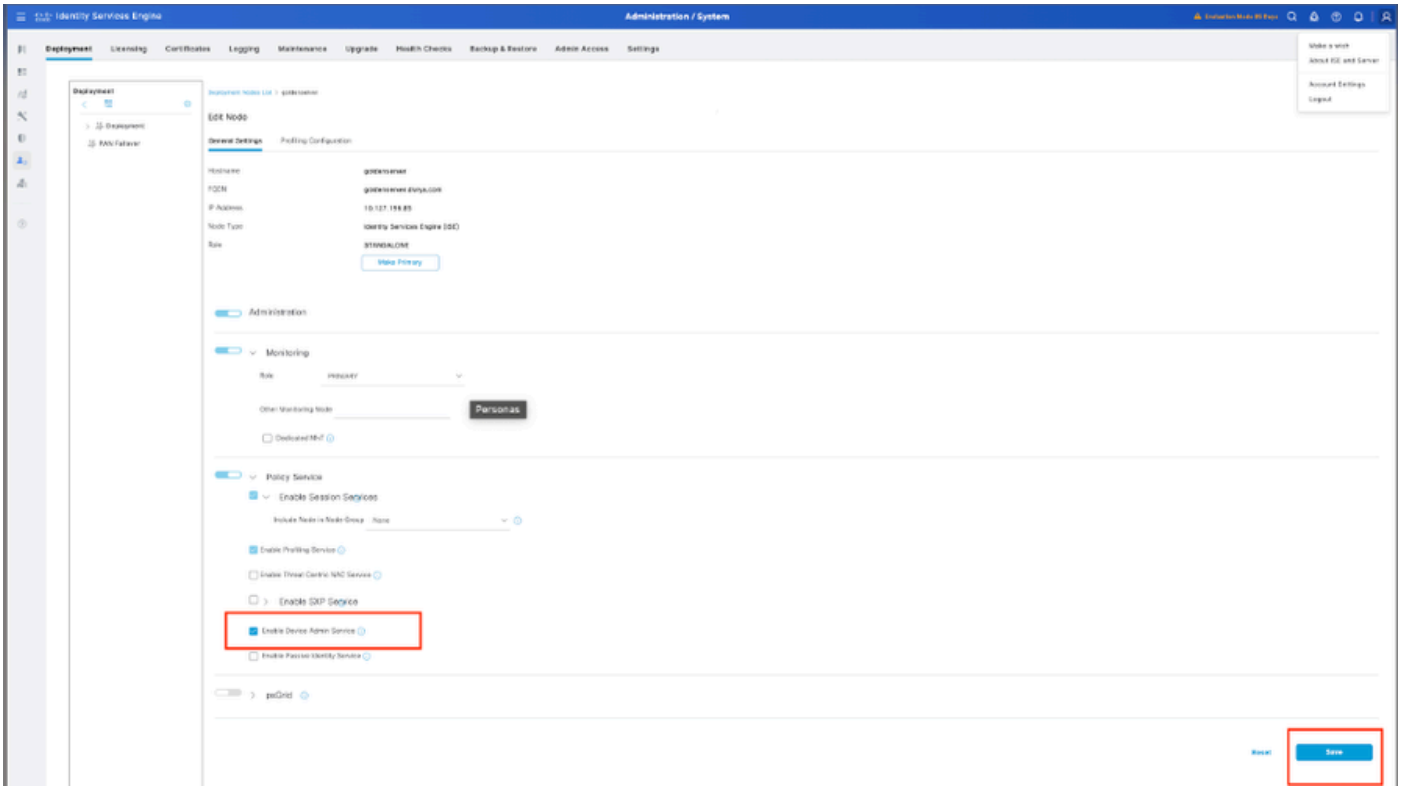
الخطوة 1. تتمثل الخطوة الأولية في التحقق مما إذا كان لدى Cisco ISE القدرات اللازمة لمعالجة مصادقة TACACS+. للقيام بذلك، تأكد من تمكين ميزة "خدمة النهج" (PSN) لعقدة خدمة النهج المطلوبة.

انتقل إلى إدارة > نظام > نشر، وحدد العقدة المناسبة حيث يقوم ISE بمعالجة مصادقة TACACS+، وانقر فوق تحرير لمراجعة التكوين الخاص به.



الخطوة 2. قم بالتمرير لأسفل لتحديد موقع ميزة خدمة إدارة الأجهزة. لاحظ أن تمكين هذه الميزة يتطلب أن يكون شخص خدمة السياسة نشطا على العقدة، إلى جانب ترخيص TACACS+ المتاحة في النشر.

حدد خانة الاختيار لتمكين الميزة، ثم احفظ التكوين.

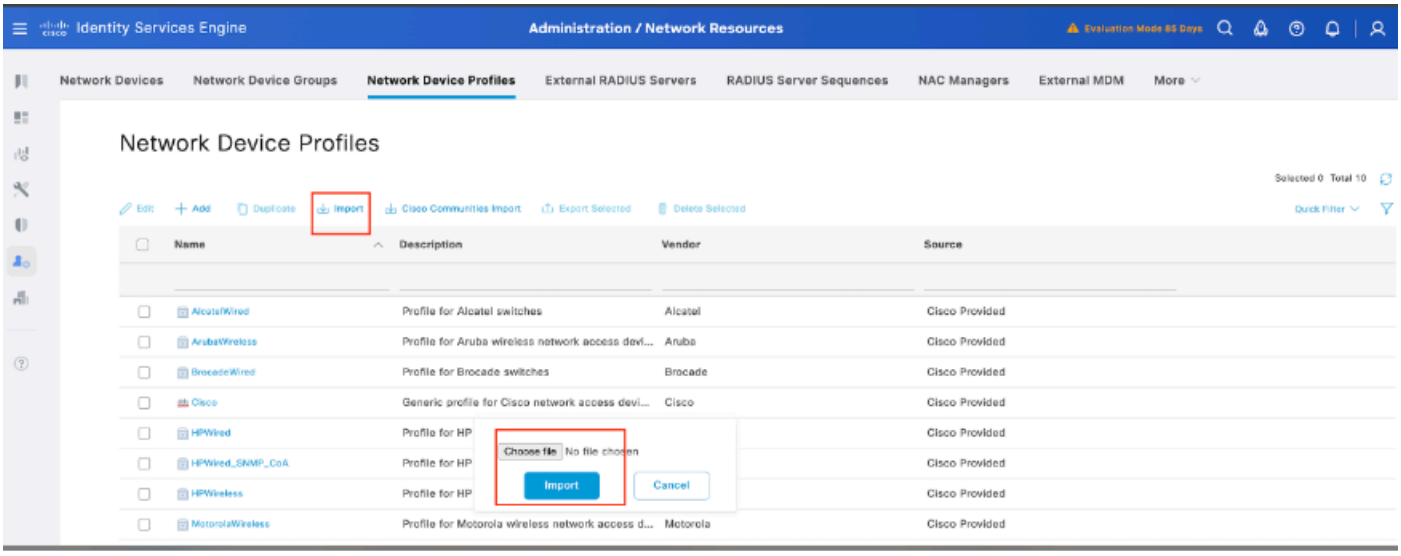


الخطوة 3. الحصول على ملف تعريف جهاز شبكة Arista ل Cisco ISE.

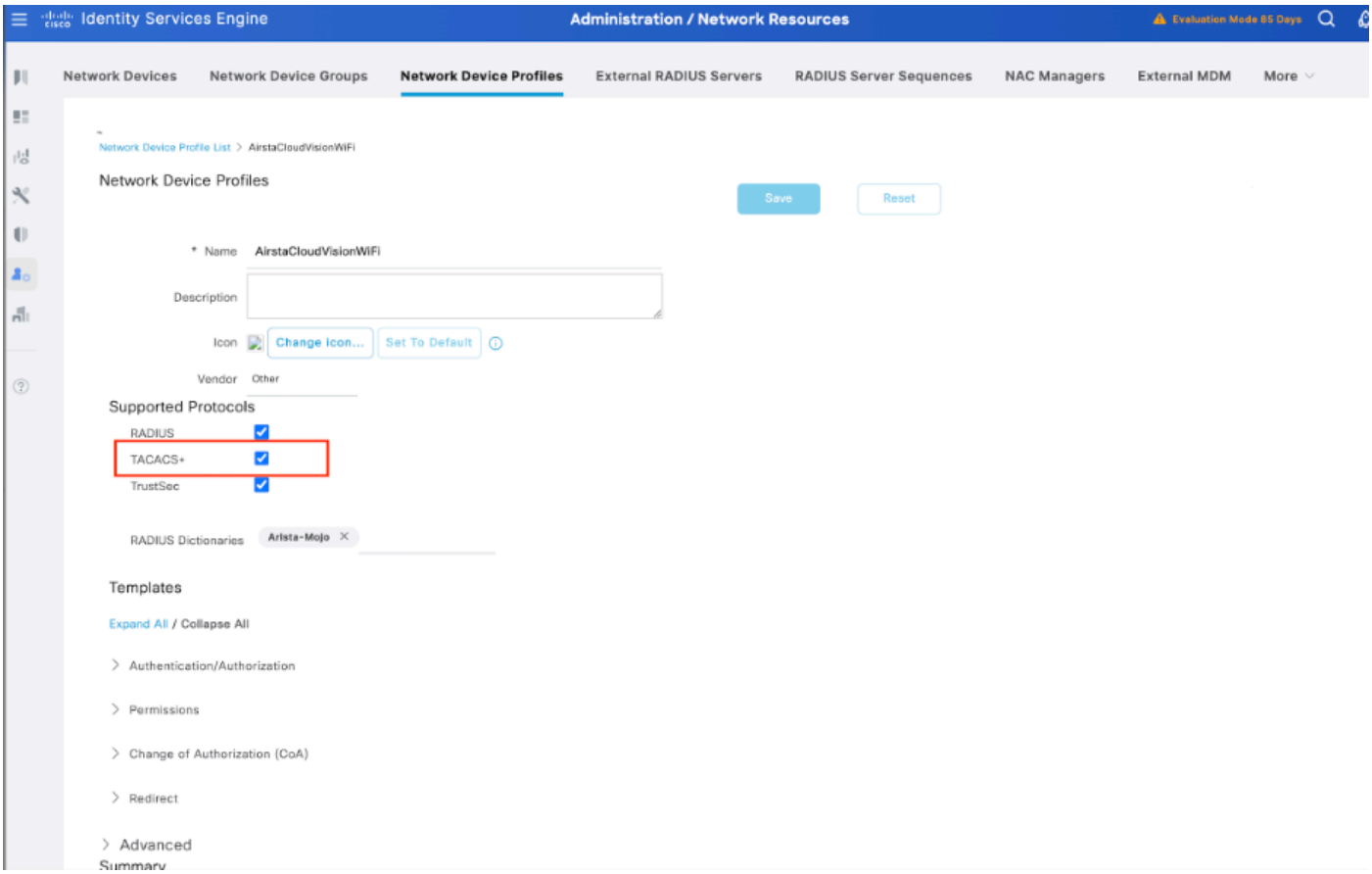
قام مجتمع Cisco بمشاركة ملف تعريف NAD مخصص لأجهزة Arista. يمكن العثور على ملف التعريف هذا مع ملفات القاموس الضرورية في قاموس Arista CloudVision WiFi وتوصيف NAD لتكامل ISE. يؤدي تنزيل هذا الملف التعريفي واستيراده إلى إعداد ISE إلى تسهيل عملية الدمج بشكل أكثر سلاسة

خطوات إستيراد ملف تعريف Arista و AD إلى Cisco ISE:

1. تنزيل ملف التعريف:
   - يمكنك الحصول على ملف تعريف Arista NAD من إرتباط مجتمع Cisco المتوفر أعلاه. مجتمع Cisco
2. الوصول إلى Cisco ISE:
   - سجل الدخول إلى وحدة التحكم الإدارية Cisco ISE الخاصة بك.
3. إستيراد ملف تعريف NAD:
   - انتقل إلى إدارة > موارد الشبكة > توصيفات أجهزة الشبكة
   - انقر فوق الزر إستيراد.
   - قم بتحميل ملف تعريف ARISTA NAD الذي تم تنزيله.

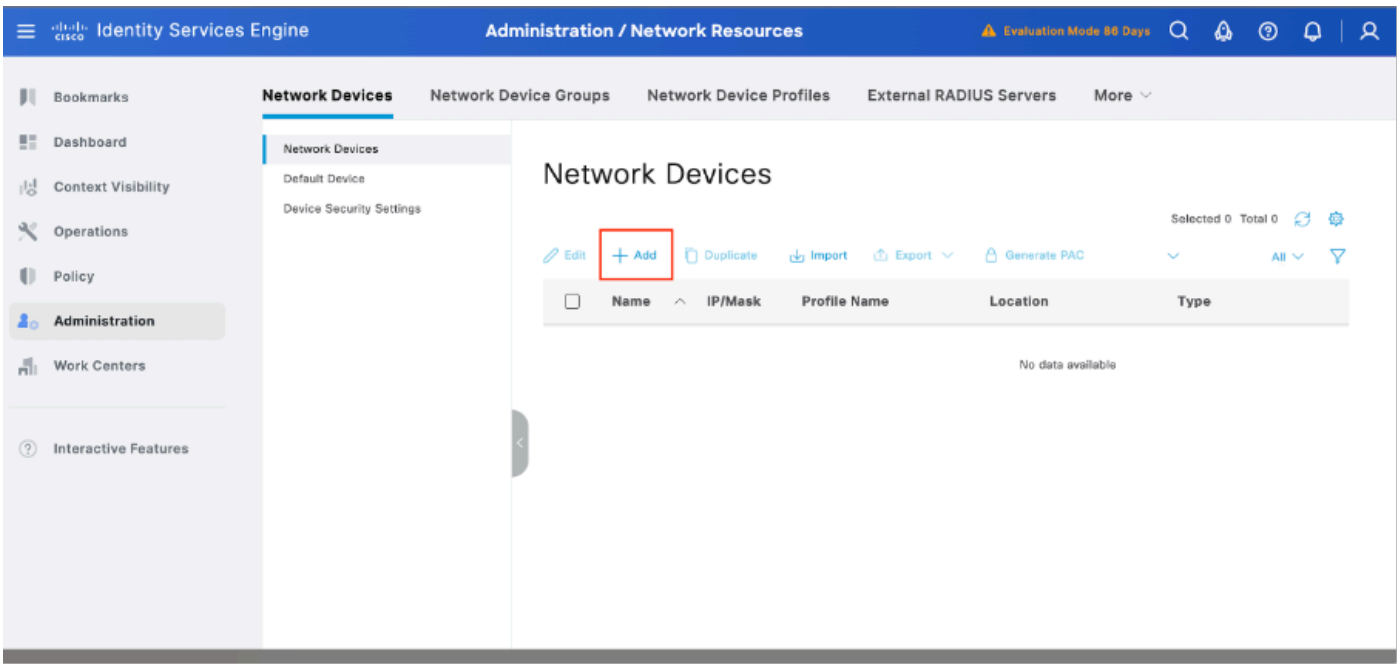


بعد اكتمال التحميل، انتقل إلى خيار التحرير وتمكين TACACS+ كبروتوكول مدعوم.



الخطوة 2: إضافة محول Arista كجهاز شبكة.

1. انتقل إلى إدارة > موارد الشبكة > أجهزة الشبكة> +إضافة:

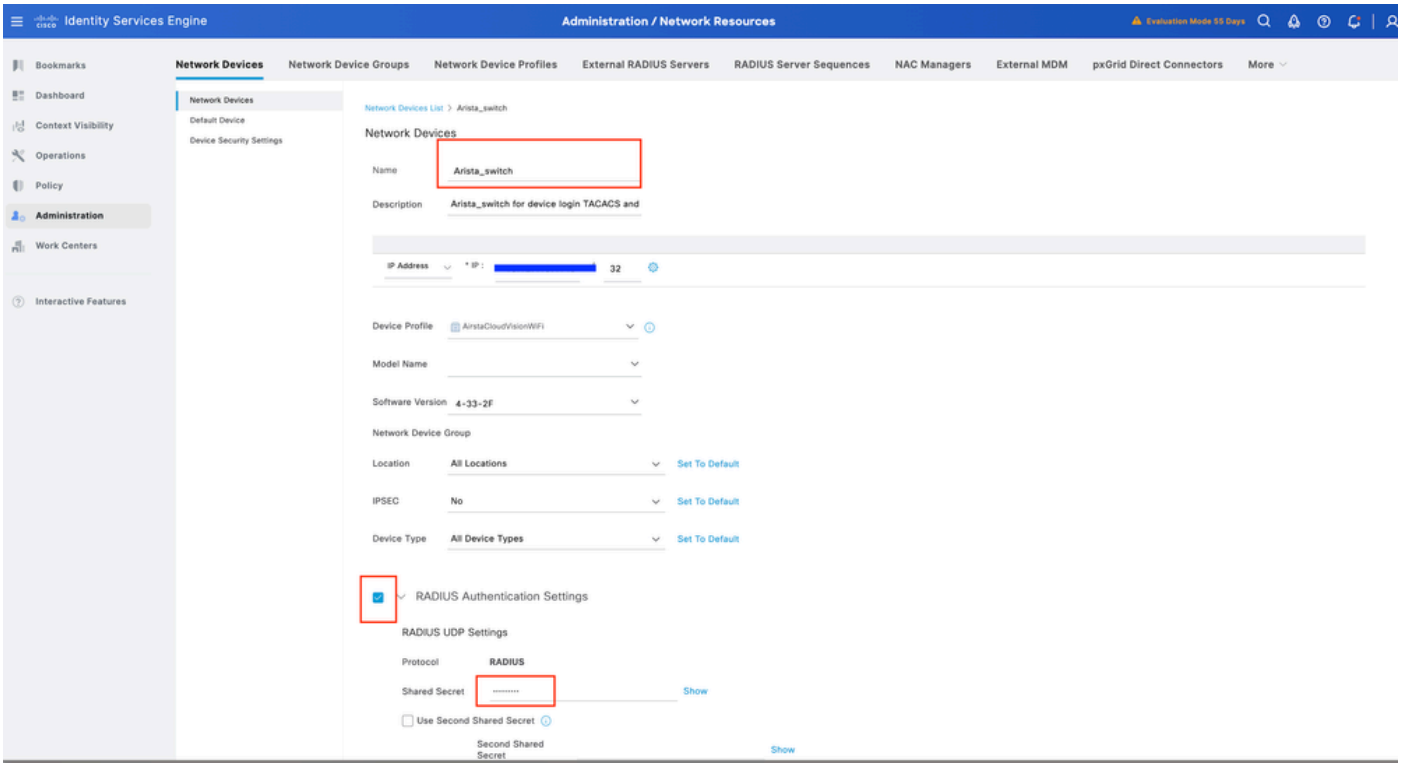


2.انقر فوق إضافة وأدخل التفاصيل التالية:

- عنوان IP: <switch-ip>
- نوع الجهاز: إختيار اتصال سلكي آخر
- ملف تعريف جهاز الشبكة: حدد AirstaCloudVisionWiFi.

- إعدادات مصادقة RADIUS:
  - تمكين مصادقة RADIUS.
  - أدخل السر المشترك (يجب أن يطابق تكوين المحول).

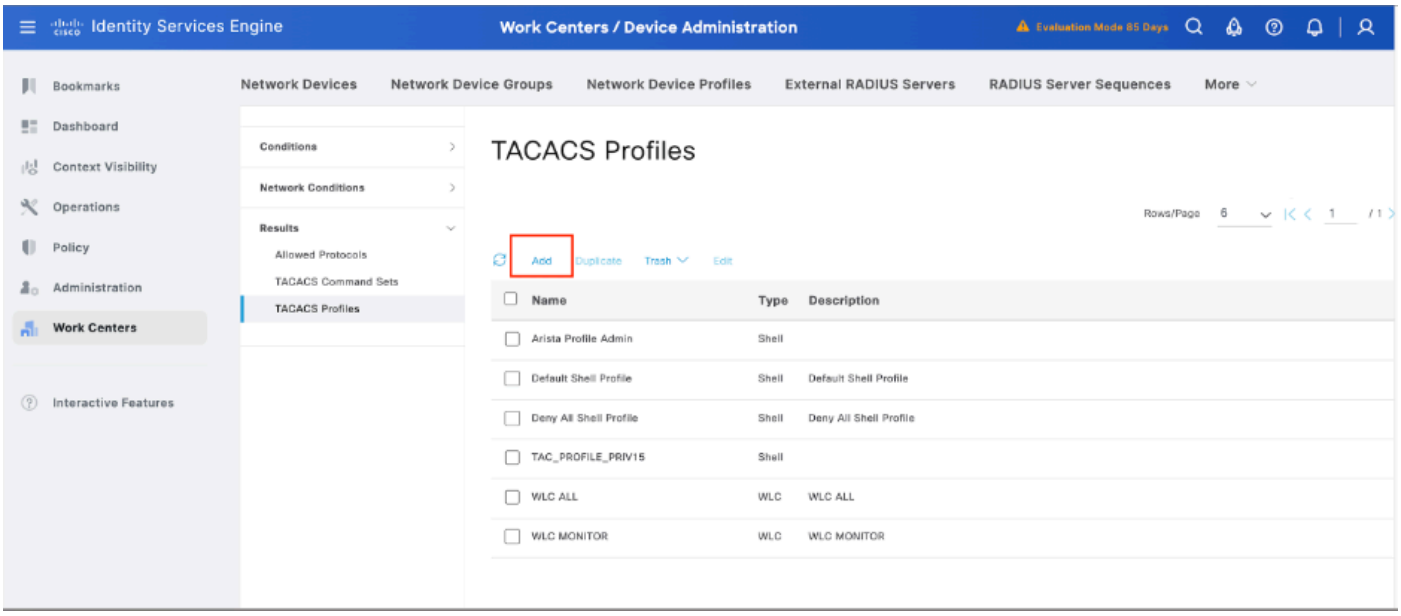
3. انقر فوق حفظ:



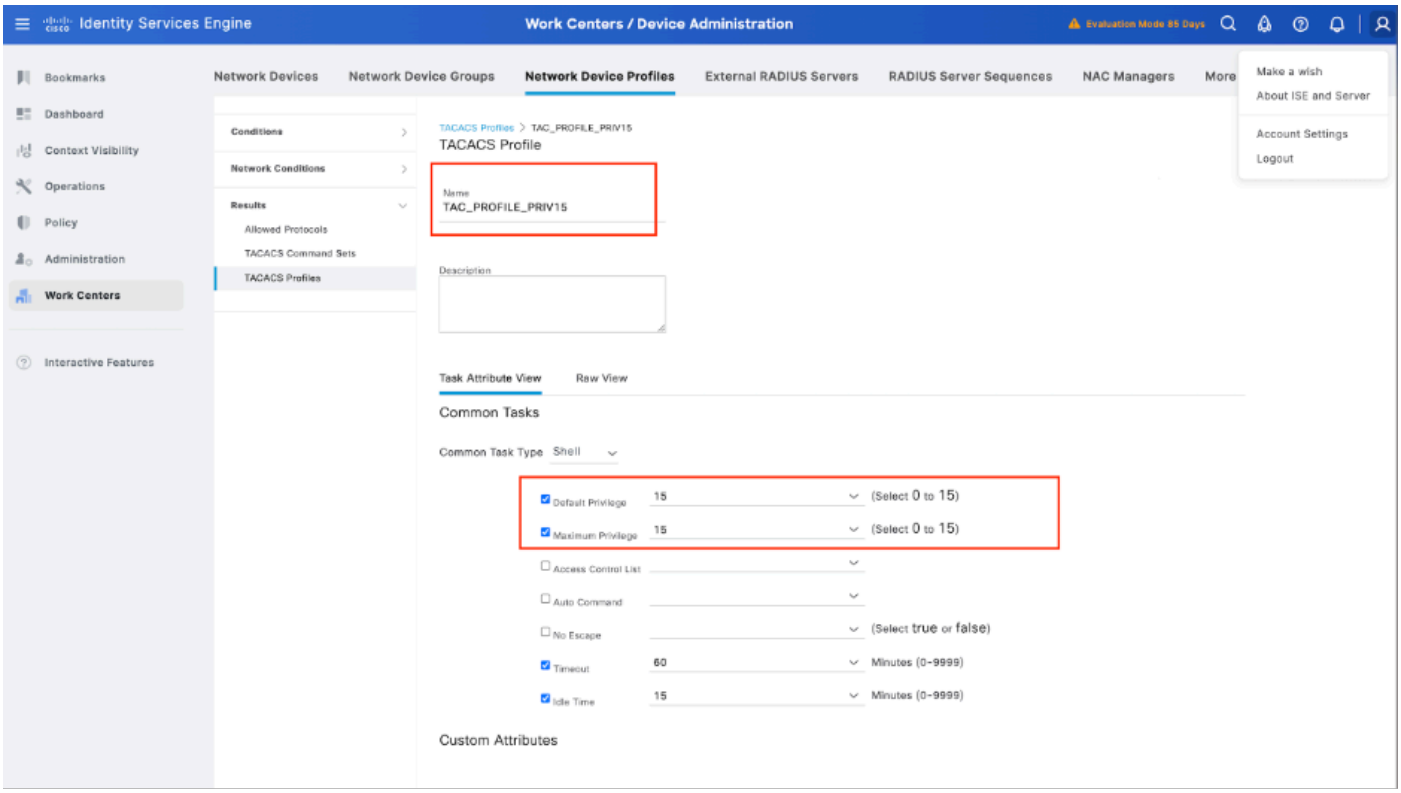
الخطوة 3. التحقق من صحة الجهاز الجديد معروض ضمن أجهزة الشبكة:

الخطوة 4. قم بتكوين ملف تعريف TACACS.

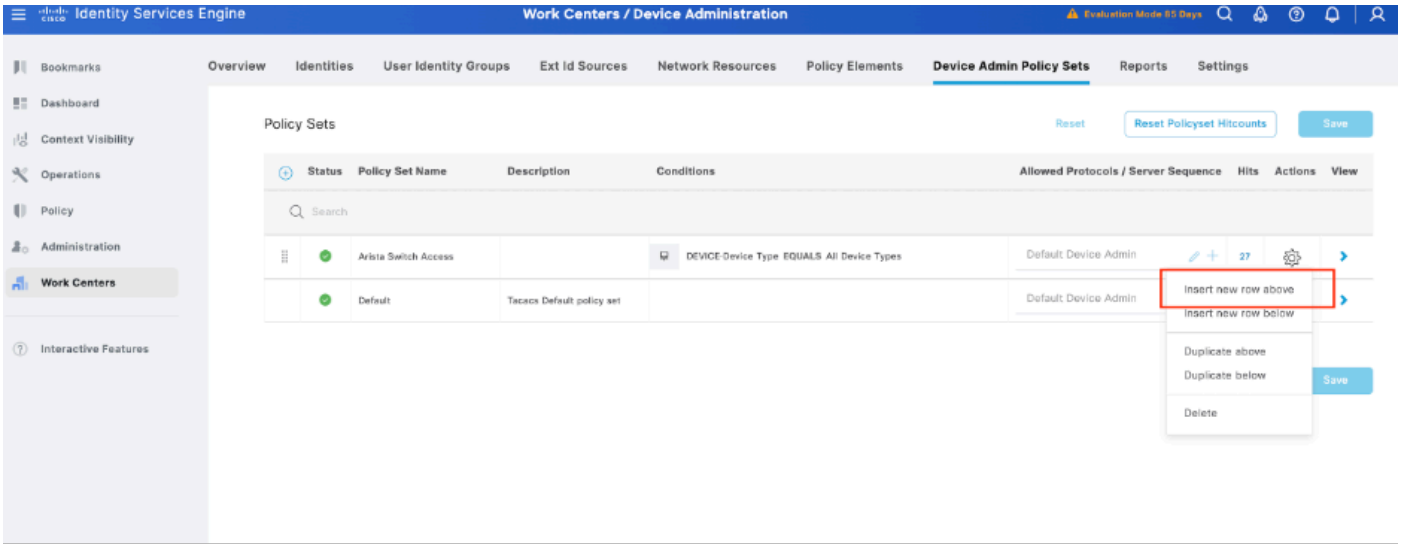
قم بإنشاء ملف تعريف TACACS، انتقل إلى مراكز عمل الهوية > إدارة الجهاز > عناصر السياسة > النتائج > ملفات تعريف TACACS، ثم حدد إضافة:



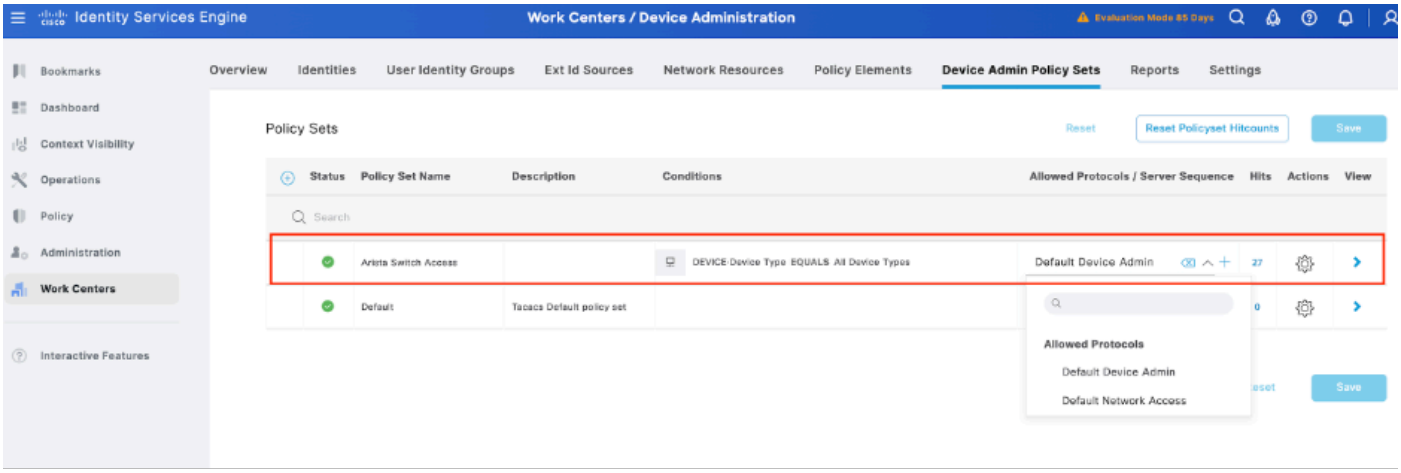
أدخل اسما، ثم حدد خانة الاختيار "الامتياز الافتراضي"، ثم قم بتعيين القيمة إلى 15. بالإضافة إلى ذلك، حدد "الحد الأقصى للامتياز"، وقم بتعيين قيمته إلى 15، وانقر فوق إرسال:



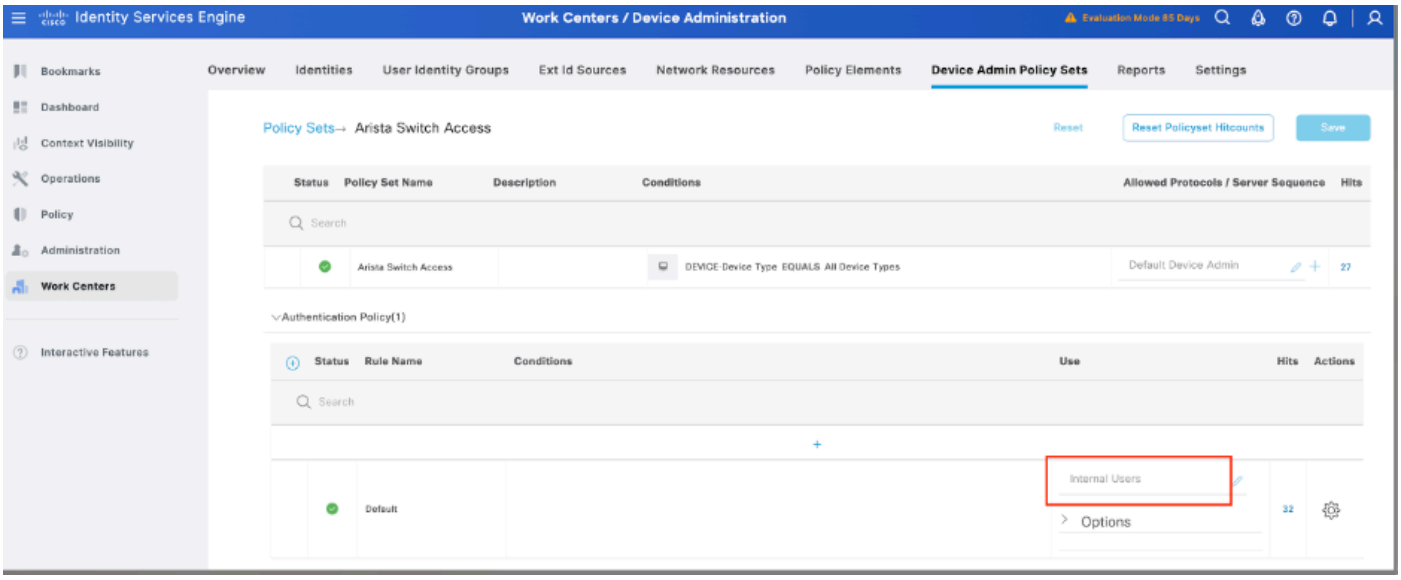
الخطوة 5. قم بإنشاء "مجموعة نهج إدارة الأجهزة" ليتم إستخدامها لمحول Arista، انتقل إلى مراكز العمل القائمة > إدارة الأجهزة > مجموعات نهج إدارة الأجهزة، ثم من مجموعة نهج موجودة حدد أيقونة المعدات ثم حدد إدراج صف جديد أعلاه.



الخطوة 6. قم بتسمية مجموعة النهج الجديدة هذه، وإضافة شروط وفقا لخصائص مصادقة TACACS+ الواردة من المحول Arista، وحدد كبروتوكولات مسموح بها > مسؤول الجهاز الافتراضي، احفظ التكوين الخاص بك.

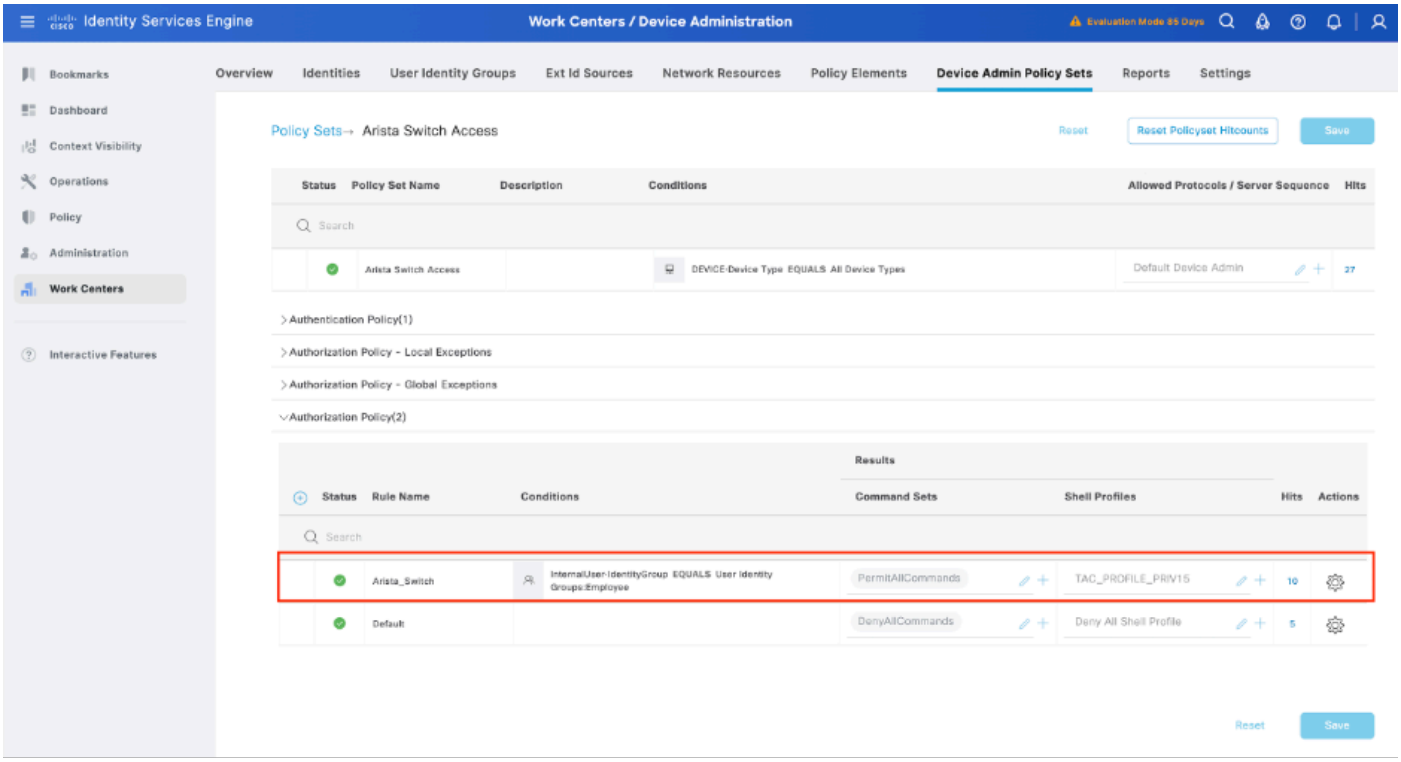


الخطوة 7. حدد في خيار >عرض، ثم في قسم سياسة المصادقة، حدد مصدر الهوية الخارجية الذي يستخدمه Cisco ISE للاستعلام عن اسم المستخدم وبيانات الاعتماد للمصادقة على محول Arista. في هذا المثال، تتطابق بيانات الاعتماد مع المستخدمين الداخليين المخزنين داخل ISE.



الخطوة 8. قم بالتمرير لأسفل حتى القسم المسمى نهج التخويل إلى النهج الافتراضي، وحدد أيقونة العتاد، ثم قم بإدراج قاعدة واحدة أعلاه.

الخطوة 9. قم بتسمية قاعدة التخويل الجديدة، وإضافة شروط تتعلق بالمستخدم الذي تمت مصادقته بالفعل كعضوية في المجموعة، وفي قسم ملفات تعريف Shell قم بإضافة ملف تعريف TACACS الذي قمت بتكوينه مسبقا، احفظ التكوين.



تكوين محول Arista

الخطوة 1. تمكين مصادقة TACACS+

قم بتسجيل الدخول إلى المحول Arista switch وأدخل وضع التكوين:

التكوين

!

tacacs خادم لمضيف <tacacs-secret> مفتاح <ise-ip>

!

AAA خادم مجموعة tacacs+ ISE_TACACS

  خادم <ISE-IP>

!

تسجيل دخول مصادقة AAA المجموعة الافتراضية ISE_TACACS محلي

مجموعة ISE_TACACS المحلية الافتراضية لتفويض AAA

أوامر محاسبة AAA الإصدار 15 default-stop group ise_tacacs

!

نهاية

الخطوة 2. حفظ التكوين

للحفاظ على التكوين عبر عمليات إعادة التمهيد:

ذاكرة الكتابة

أو

copy running-config startup-config

التحقق من الصحة

مراجعة ISE

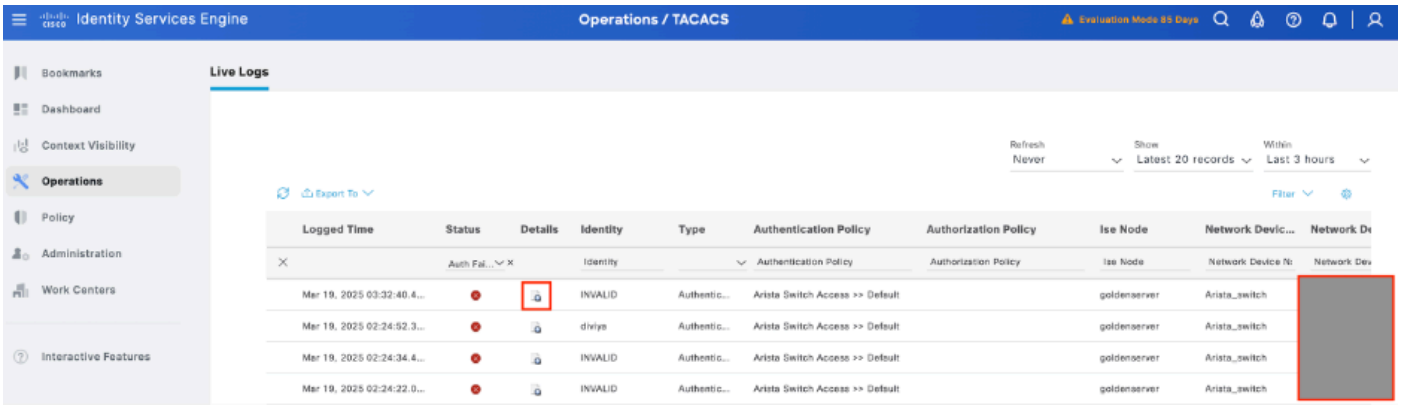
الخطوة 1. راجع إذا كانت خدمة TACACS+ قيد التشغيل، ويمكن إيداع ما يلي:

- GUI: راجع إذا كان لديك العقدة المدرجة مع مسؤول جهاز الخدمة في > النظام > النشر.
- CLI: قم بتشغيل الأمر show ports | يتضمن 49 لتأكيد وجود إتصالات في منفذ TCP تنتمي إلى TACACS+

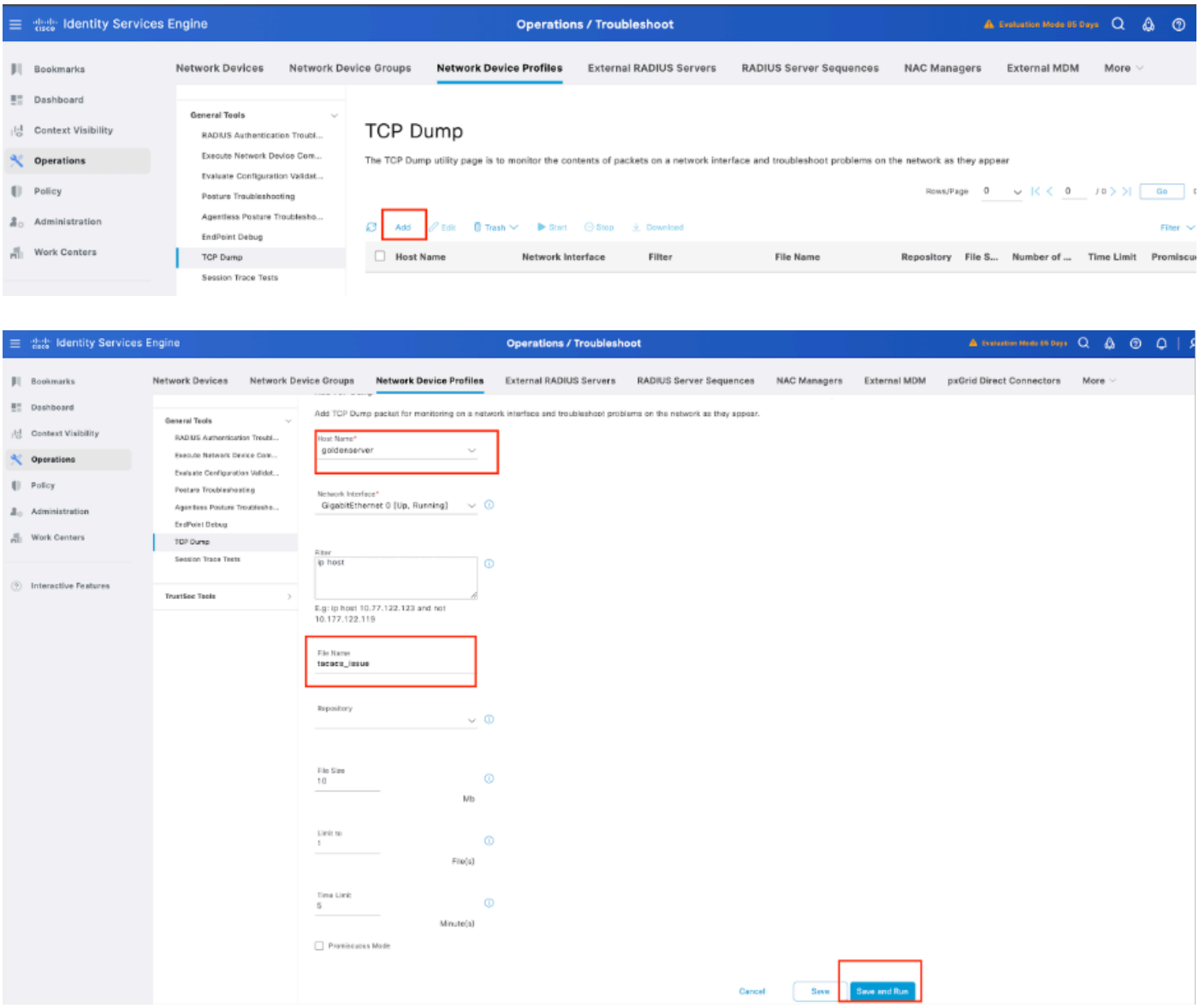
```
goldenserver/admin#show ports | include 49
tcp: [redacted]
```

الخطوة 2. تأكد ما إذا كانت هناك إصابات حية تتعلق بمصدقات TACACS+ : يمكن إيداع هذه في القائمة عمليات > TACACS > سجلات نشطة،

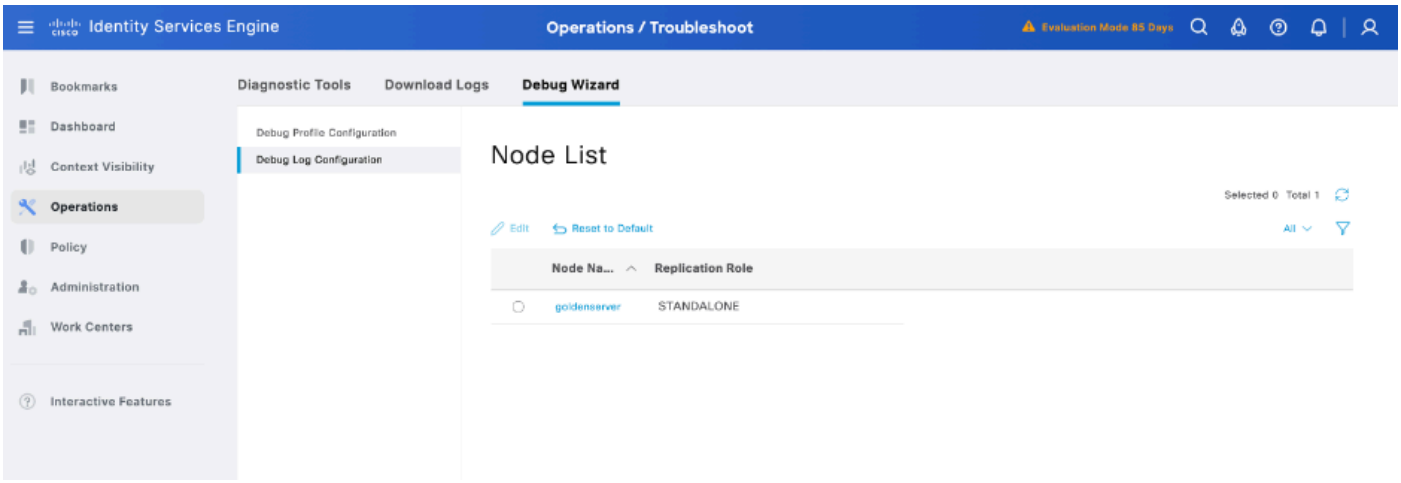
على حسب سبب الفشل يمكنك ضبط التكوين أو معالجة سبب الفشل.

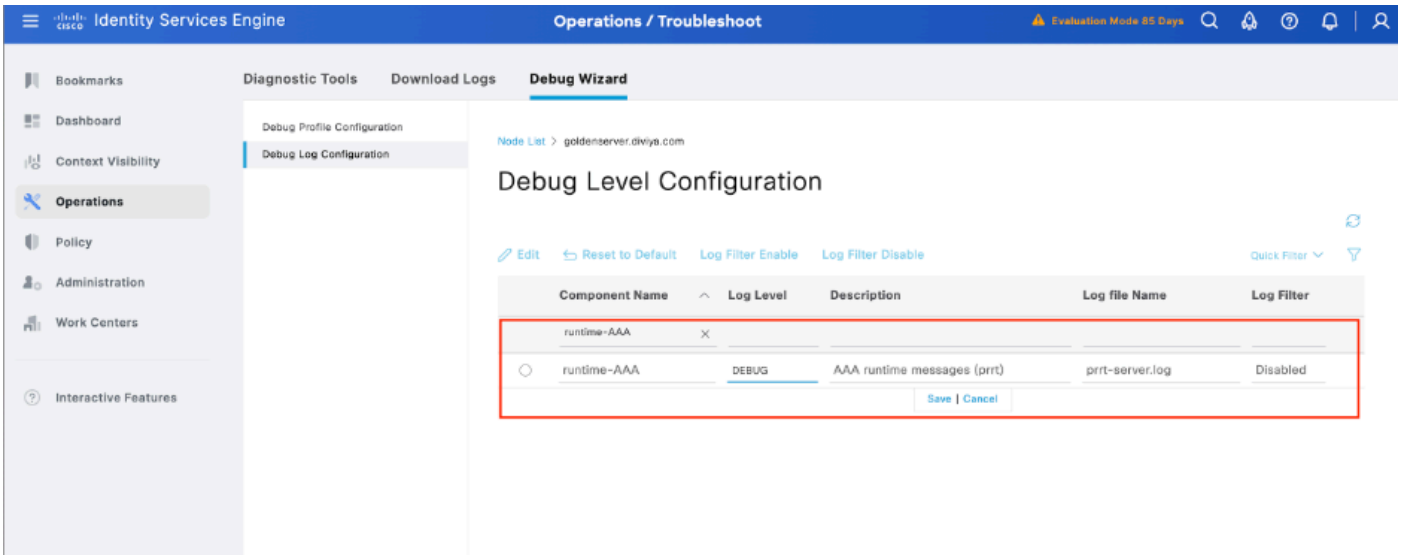


الخطوة 3. في حالة عدم رؤية أي حرف عائم، قم بالمتابعة للتقاط الحزمة. انتقل إلى عمليات القائمة > أستكشاف الأخطاء وإصلاحها > أدوات التشخيص > أدوات عامة > تفريغ TCP ، حدد إضافة:



الخطوة 4. قم بتمكين المكون runtime-AAA في تصحيح الأخطاء ضمن PSN من حيث يتم إجراء المصادقة في العمليات > أستكشاف الأخطاء وإصلاحها > معالج تصحيح الأخطاء > تكوين سجل الأخطاء، حدد عقدة PSN، ثم حدد الزر تحرير:





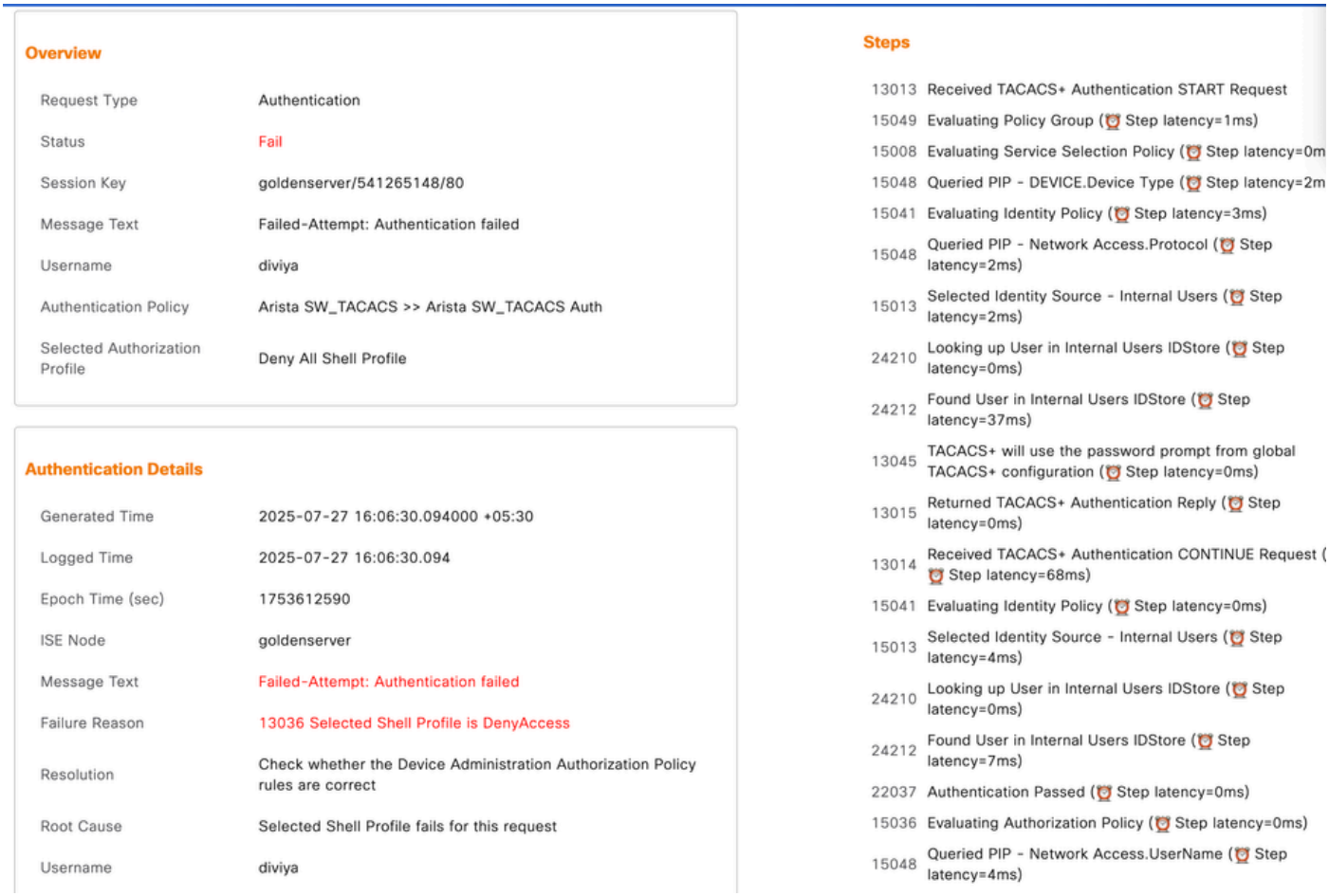
حدد مكون وقت التشغيل AAA، وقم بتعيين مستوى التسجيل الخاص به على تصحيح الأخطاء، وإعادة إنشاء المشكلة، وتحليل السجلات لمزيد من التحقيق.

استكشاف الأخطاء وإصلاحها

المشكلة 1

يفشل مصادقة TACACS+ بين Cisco ISE ومفتاح Arista (أو أي جهاز شبكة) مع رسالة الخطأ:

"ملف تعريف Shell المحدد ل 13036 هو DenyAccess"



يعني الخطأ "13036 ملف تعريف Shell المحدد وه DenyAccess" في Cisco ISE عادة أنه أثناء محاولة إدارة جهاز TACACS+، تطابق سياسة التخويل مع ملف تعريف Shell المعين إلى DenyAccess. ال يكون ذلك عادة نتيجة لملف تعريف Shell نفسه مكون بشكل غير صحيح، ولكنه يشير إلى أنه ال يوجد أي من قواعد التخويل التي تم تكوينها تطابق سمات المستخدم الواردة (مثل عضوية المجموعة أو نوع الجهاز أو الموقع). ونتيجة لذلك، يرجع ISE إلى قاعدة افتراضية أو قاعدة رفض صريحة، مما يؤدي إلى رفض الوصول.

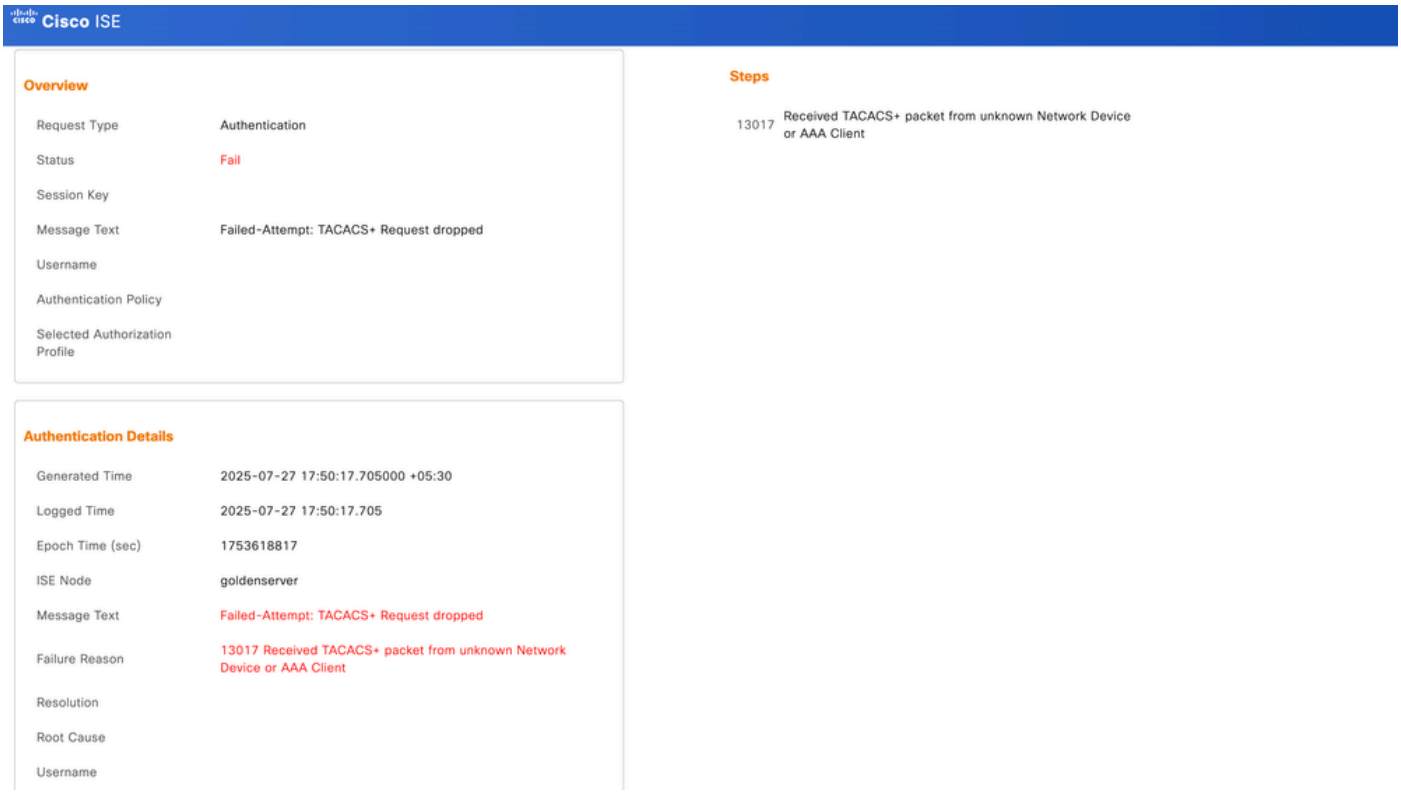
الأسباب المحتملة

- راجع قواعد سياسة التخويل في ISE. تأكد من مطابقة المستخدم أو الجهاز للقاعدة الصحيحة التي تعين ملف تعريف shell المقصود، مثل الذي يسمح بالوصول المناسب.
- تأكد من صحة تعيين AD أو مجموعة المستخدمين الداخلية ومن تحديد شروط النهج بدقة، مثل عضوية مجموعة المستخدمين ونوع الجهاز والبروتوكول.
- أستخدم سجالت ISE المباشرة وتفاصيل المحاولة الفاشلة لمعرفة القاعدة المتطابقة بالضبط والسبب.

المشكلة 2

يفشل مصادقة TACACS+ بين Cisco ISE ومفتاح Arista (أو أي جهاز شبكة) مع رسالة الخطأ:

"تم تلقي 13017 حزمة TACACS+ من جهاز شبكة غير معروف أو عميل AAA"



الأسباب المحتملة

- السبب الأكثر شيوعا وه عدم إضافة عنوان IP للمحول كجهاز شبكة في ISE (تحت الإدارة > موارد الشبكة > أجهزة الشبكة).
- تأكد من تطابق عنوان IP أو نطاقه تماما مع عنوان IP المصدر الذي يتم إستخدامه من قبل محول Arista لإرسال حزم TACACS+.
- إذا كان المحول لديك يستخدم واجهة إدارة، فتحقق من إضافة IP الخاص به (ليس مجرد شبكة فرعية/نطاق) في ISE.

الحل

- انتقل إلى الإدارة > موارد الشبكة > أجهزة الشبكة في واجهة المستخدم الرسومية (GUI) المتوافقة مع معيار ISE.
- تحقق ما إذا كان عنوان IP المصدر المحدد على محول Arista يستخدم لاتصال TACACS+ (غالبا ما يكون عنوان واجهة الإدارة IP).
- حدد السر المشترك (يجب أن يطابق ما تم ضبطه على مفتاح Arista).

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).