تكوين خادم syslog الخارجي على ISE

المحتويات

المقدمة

يصف هذا وثيقة كيف أن يشكل خارجي syslog نادل على ISE.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- محرك خدمات الهوية (ISE).
- خوادم Syslog

المكونات المستخدمة

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

- إصدار Identity Services Engine (ISE) 3.3.
- Cisco Syslog Server v1.2.1.4

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

معلومات أساسية

.

يتم تجميع رسائل Syslog من ISE وتخزينها بواسطة أدوات تجميع السجلات. ويتم تعيين أدوات تجميع السجلات هذه لمراقبة العقد حتى تقوم MnT بتخزين السجلات التي يتم تجميعها محليا.

لتجميع السجلات خارجيا، تقوم بتكوين خوادم syslog الخارجية، والتي تسمى أهدافا. تصنف السجلات في فئات مختلفة معرفة مسبقا.

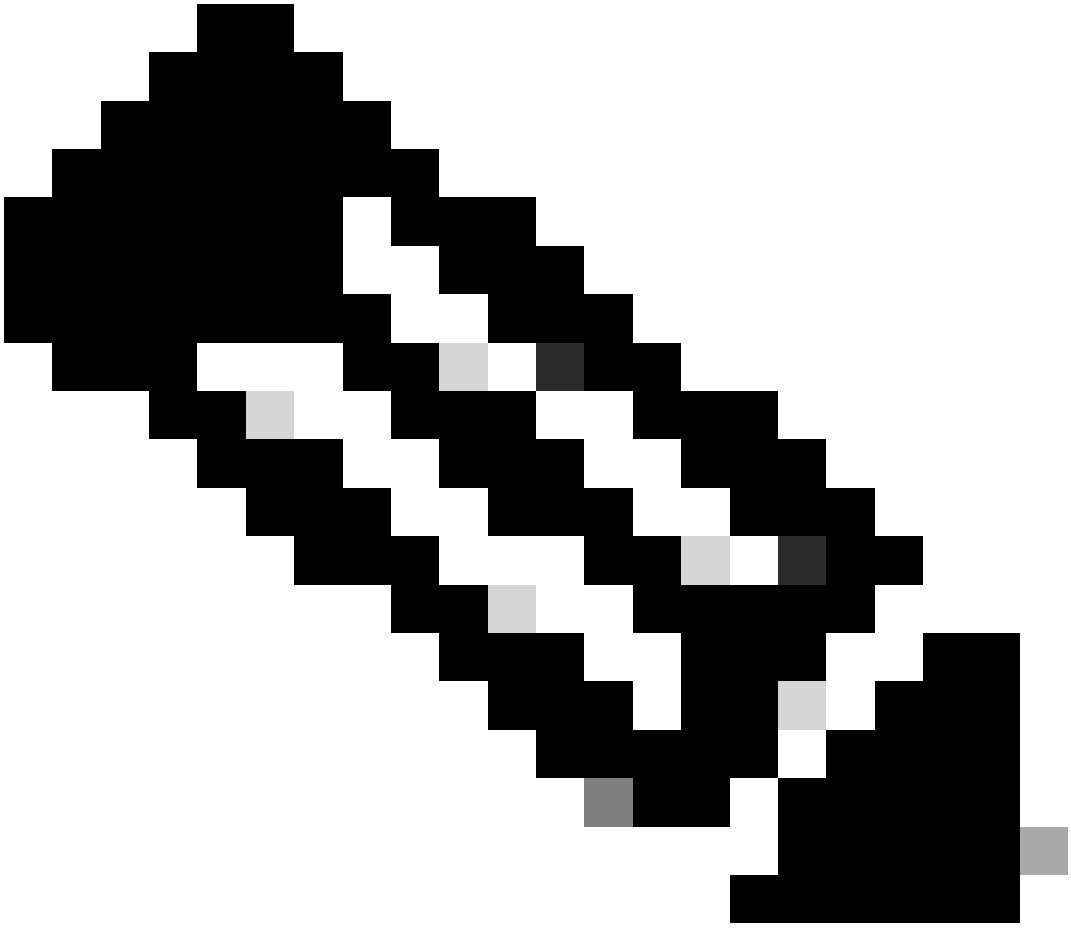
يمكنك تخصيص مخرجات التسجيل من خلال تحرير الفئات فيما يتعلق بأهدافها ومستوى الخطورة وما إلى ذلك.

التكوين

يمكنك إستخدام واجهة الويب لإنشاء أهداف خادم syslog عن بعد التي يتم إرسال رسائل سجل النظام إليها. يتم إرسال رسائل السجل إلى أهداف خادم syslog البعيدة وفقا لمعيار بروتوكول syslog (راجع RFC-3164).

تكوين هدف التسجيل عن بعد (UDP Syslog)

في واجهة المستخدم الرسومية Cisco ISE، انقر فوق الرمز ( ) واختارAdministration>System>التسجيل>أهداف التسجيل عن بعد>>انقر فوق إضافة.



ملاحظة: يعتمد مثال التكوين التالي على لقطة شاشة باسم: تكوين هدف التسجيل عن بعد.

- اسم ك Remote_Kiwi_Syslog، يمكنك هنا إدخال اسم خادم syslog البعيد، ويتم إستخدام هذا الاسم لأغراض وصفية.
- النوع الهدف ك UDP Syslog، في مثال التكوين هذا، يتم إستخدام UDP Syslog؛ ومع ذلك، يمكنك تكوين المزيد من الخيارات من القائمة المنسدلة نوع الهدف:

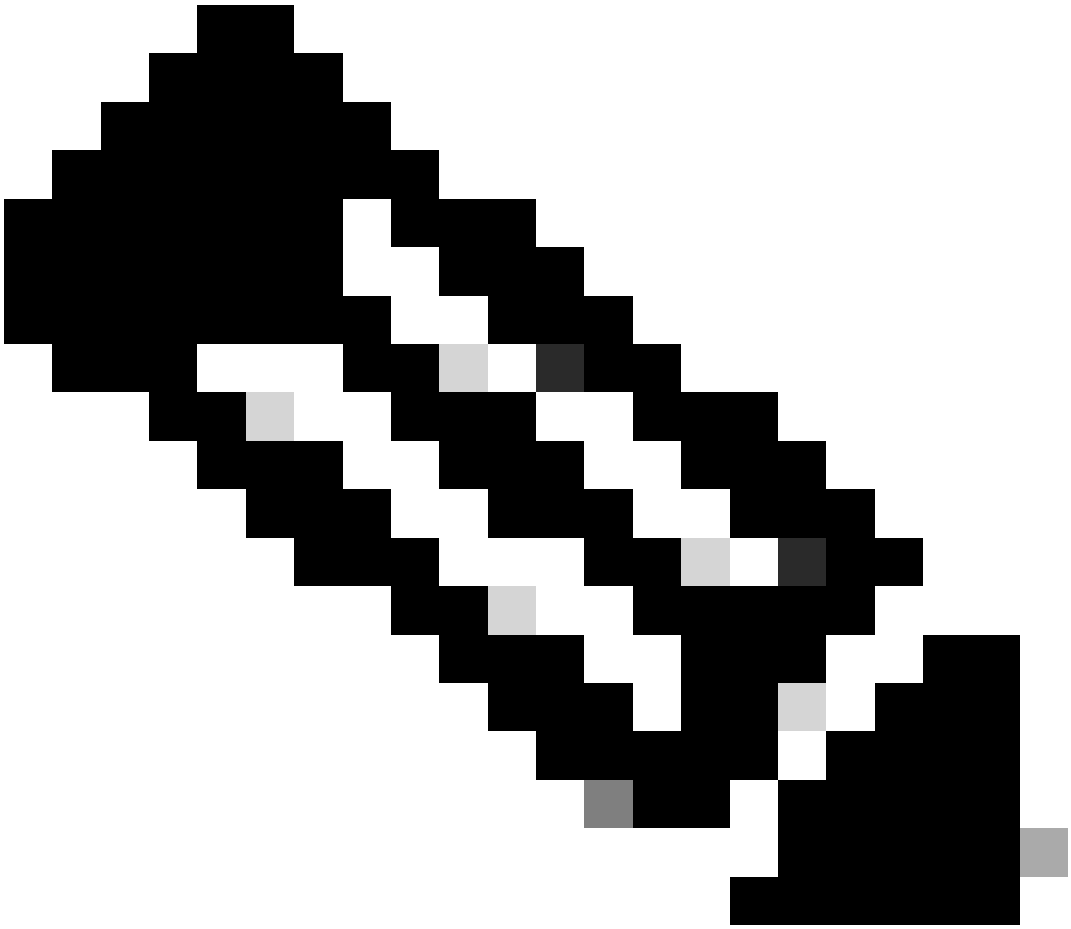
UDP Syslog: يستخدم لإرسال رسائل syslog عبر بروتوكول UDP، المناسب للتسجيل السريع وخفيف الوزن.

بروتوكول TCP syslog: يستخدم لإرسال رسائل syslog عبر TCP، والذي يوفر موثوقية مع إمكانيات التحقق من الأخطاء وإعادة الإرسال.

syslog الآمن: يشير إلى رسائل syslog التي يتم إرسالها عبر TCP باستخدام تشفير TLS، مما يضمن تكامل البيانات وسريتها.

- حالة التمكين، يجب عليك إختيارEnabled من القائمة المنسدلةStatusdrop.

- الوصف، يمكنك إختياريا إدخال وصف موجز للهدف الجديد.
- المضيف / عنوان IP، هنا تقوم بإدخال عنوان IP أو اسم المضيف للخادم الوجهة الذي يقوم بتخزين السجلات.يدعم Cisco ISE تنسيقات IPv4 و IPv6 للتسجيل.



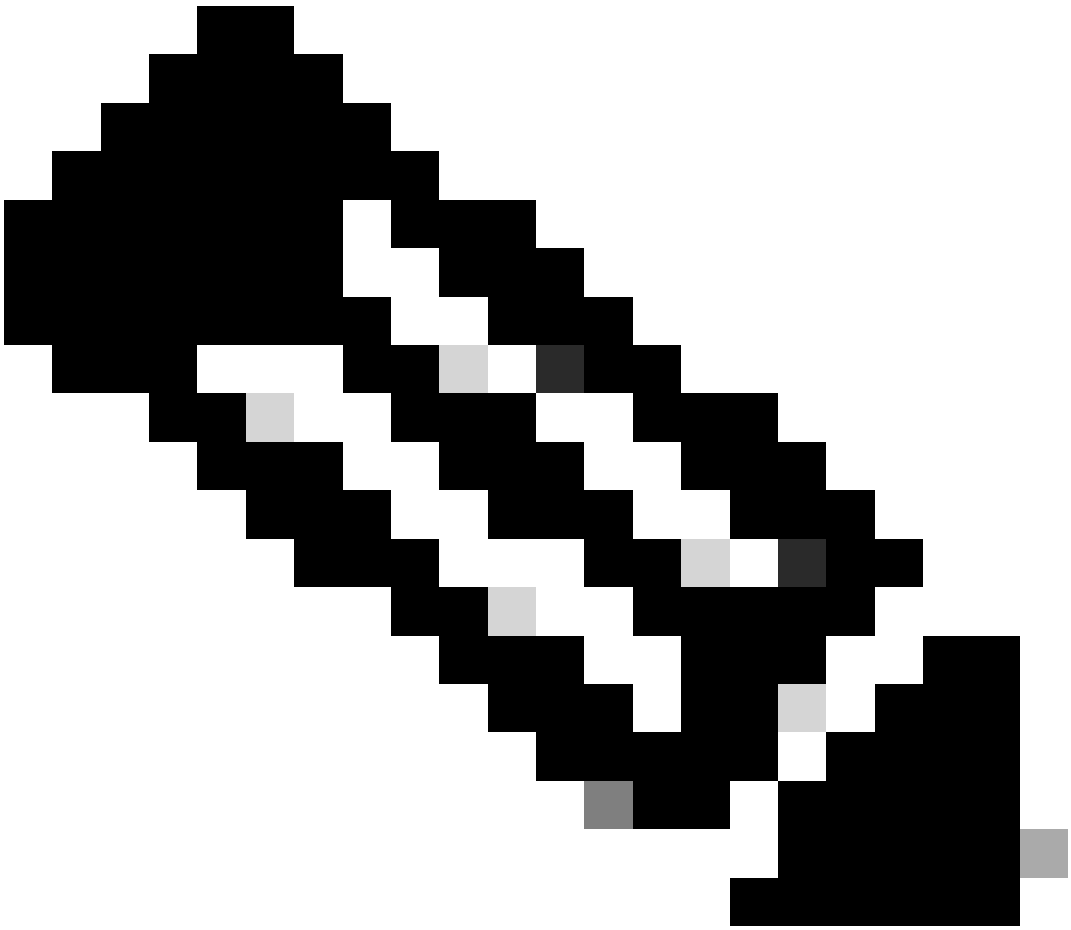
ملاحظة: من الضروري ذكر أنه إذا كنت تريد تكوين خادم syslog باستخدام FQDN، فيجب إعداد التخزين المؤقت ل DNS لتجنب التأثير على الأداء. بدون التخزين المؤقت ل DNS، يستعلم ISE عن خادم DNS في كل مرة يجب إرسال حزمة syslog إلى هذه التسجيل عن بعد الذي تم تكوينه باستخدام FQDN. ويؤثر ذلك بشدة على أداء ISE.

أستخدم الأمرservice cache enableفي جميع شبكات PSN الخاصة بالنشر للتغلب على ما يلي:

مثال

```
ise/admin(config)# service cache enable hosts ttl 180
```

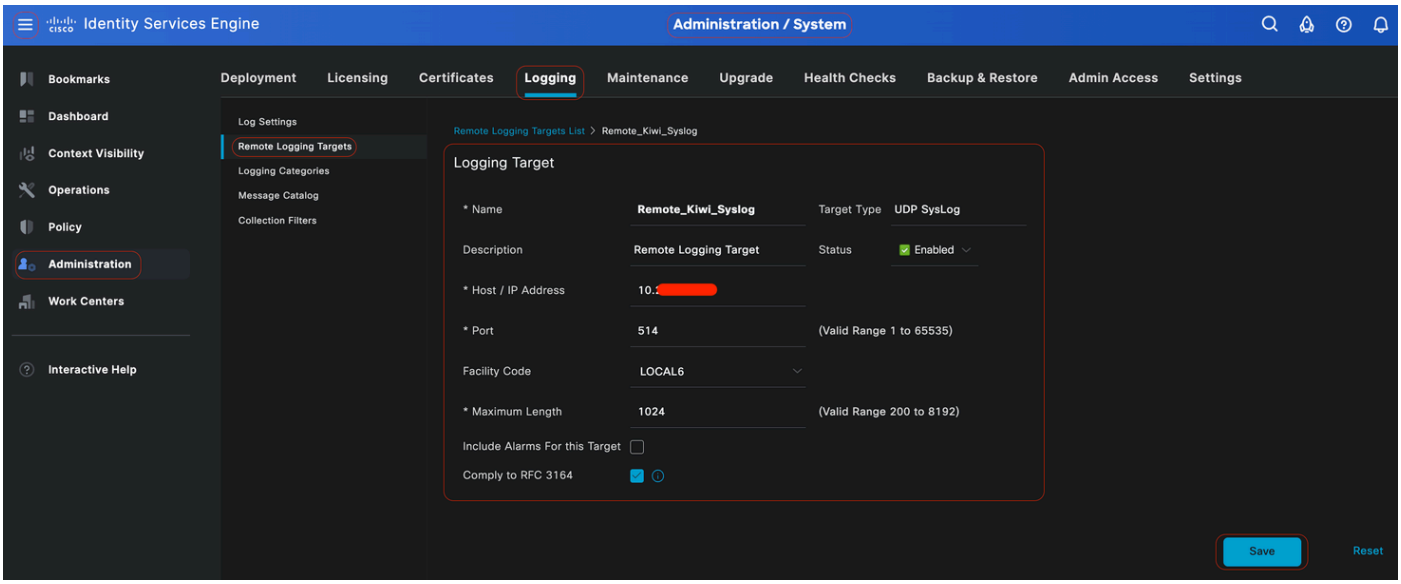
- ميناء as 514، في هذا تشكيل مثال، الـ Kiwi syslog دان لديستمع في ميناء 514 أي يكون التقصير ميناء لـ UDP syslog رسالة. مهم، مستعمل يستطيع غير تذا ميناء رقم إلى أي قيمة بين 1 و 65535.تأكد أن ميناءك بـ الـ يتم حظره من قبل أي جدار حماية.
- رمز المرفق كـ LOCAL6، يمكنك إختيار رمز مرفق syslog الذي يجب إستخدامه للتسجيل، من القائمة المنسدلة. الخيارات الصالحة هي Local0 through Local7.
- الحد الأقصى للطول كـ 1024، يمكنك هنا إدخال الحد الأقصى لطول رسائل هدف السجل البعيد. تم تعيين الحد الأقصى للطول على 1024 افتراضي إصدار ISE 3.3، القيم من 200 إلى 8192 بايت.



ملاحظة: لتجنب إرسال رسائل مقتطعة إلى الهدف البعيد، يمكنك تعديل الحد الأقصى للطول على 8192.

- تضمين تنبيهات لهذا الهدف، إلى بقائه بسيطا، في مثال التكوين هذا، الـ يتم التحقق من تضمين تنبيهات لهذا الهدف؛ ومع ذلك، عند تحديد خانة الاختيار هذه، يتم إرسال رسائل التنبيه إلى الخادم البعيد أيضا.

- التوافق مع RFC 3164 محدد، عندما تقوم بتحديد خانة الاختيار هذه، الفواصل (، ؛ { } \ \) في رسائل syslog التي يتم إرسالها إلى الخوادم البعيدة ال يتم نهبها حتى إذا تم إستخدام شرطة مائلة عكسية (\).
- بمجرد انتهاء التكوين، انقر فوق حفظ.
- بمجرد الحفظ، سيقوم النظام بعرض هذا التحذير: لقد أخترت إنشاء اتصال غير آمن (TCP/UDP) بالخادم. هل تريد بالتأكيد المتابعة؟، انقر فوق نعم.



تكوين الهدف البعيد

تكوين الهدف البعيد ضمن فئات التسجيل

يرسل Cisco ISE أحداث قابلة للتدقيق إلى هدف syslog. بمجرد تكوين هدف التسجيل عن بعد الخاص بك، تحتاج بعد ذلك إلى تعيين هدف التسجيل عن بعد إلى الفئات المقصودة لإعادة توجيه الأحداث القابلة للتدقيق.

يمكن بعد ذلك تعيين أهداف التسجيل لكل فئة من فئات التسجيل هذه. يتم إنشاء سجلات الأحداث من فئات السجل هذه فقط من عقد PSN ويمكن تكوينها لإرسال السجلات ذات الصلة إلى خادم syslog البعيد استنادا إلى الخدمات التي يتم تمكينها على هذه العقد:

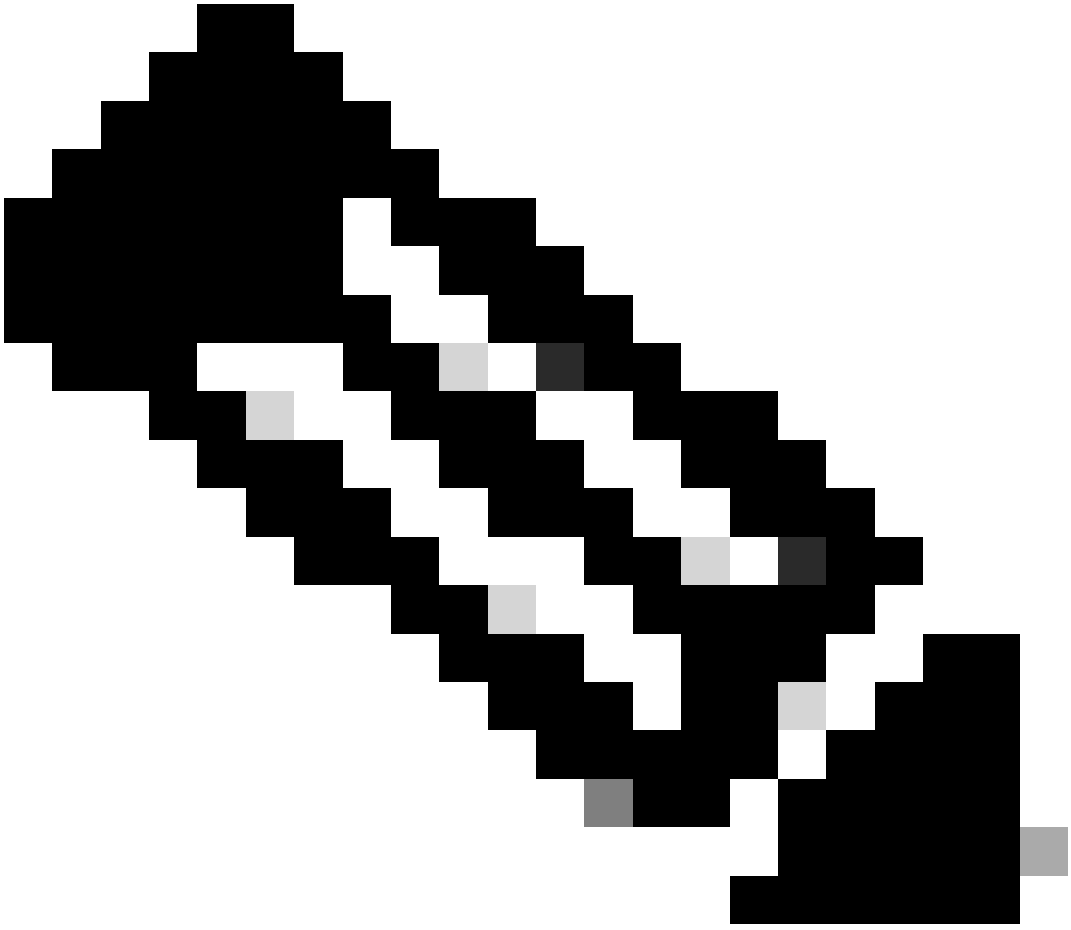
- تدقيق المصادقة والتفويض والمحاسبة (AAA)
- تشخيصات AAA
- الحسابات
- MDM الخارجي
- معرف الخامل
- تدقيق Posture و Client Provisioning
- تشخيصات Posture و Client Provisioning

- محلل

يتم إنشاء سجلات الأحداث من فئات السجل هذه من جميع العقد في النشر ويمكن تكوينها لإرسال السجلات ذات الصلة إلى خادم syslog عن بعد:

- مراجعة الحسابات الإدارية والتشغيلية
- تشخيصات النظام
- إحصائيات النظام

في مثال التكوين هذا، ستقوم بتكوين الهدف البعيد ضمن أربع فئات تسجيل، وهذه الفئات الثلاث لإرسال سجلات حركة مرور المصادقة: عمليات المصادقة التي تم تمريرها، والمحاولات الفاشلة ومحاسبة RADIUS، وهذه الفئة لحركة مرور تسجيل مسؤول ISE:



ملاحظة: يعتمد مثال التكوين التالي على لقطة شاشة باسم: تكوين هدف التسجيل عن بعد

في واجهة المستخدم الرسومية Cisco ISE، انقر فوق الرمز ( ) واختر Administration>System>Logging>فئات التسجيل، وانقر فوق الفئة المطلوبة (المصادقات التي تم تمريرها والمحاولات الفاشلة ومحاسبة RADIUS).

الخطوة 1- مستوى خطورة السجل:ترتبط رسالة حدث بمستوى خطورة، مما يسمح للمسؤول بتصفية الرسائل وترتيبها حسب الأولوية. حدد مستوى خطورة السجل كما هو مطلوب. بالنسبة لبعض فئات التسجيل، يتم تعيين هذه القيمة بشكل افتراضي، ولا يمكنك تحريرها. بالنسبة لبعض فئات التسجيل، يمكنك إختيار أحد مستويات الخطورة التالية من القائمة المنسدلة:

- مميت: مستوى الطوارئ. هذا المستوى يعني أنه لا يمكنك إستخدام Cisco ISE ويجب عليك إتخاذ الإجراء اللازم على الفور.
- الخطأ : يشير هذا المستوى إلى حالة خطأ فادح.
- تحذير: يشير هذا المستوى إلى حالة عادية ولكن هامة. هذا هو المستوى الافتراضي الذي تم تعيينه للعديد من فئات التسجيل.
- المعلومات: يشير هذا المستوى إلى رسالة إعلامية.
- تصحيح الأخطاء: يشير هذا المستوى إلى رسالة خطأ تشخيصية.

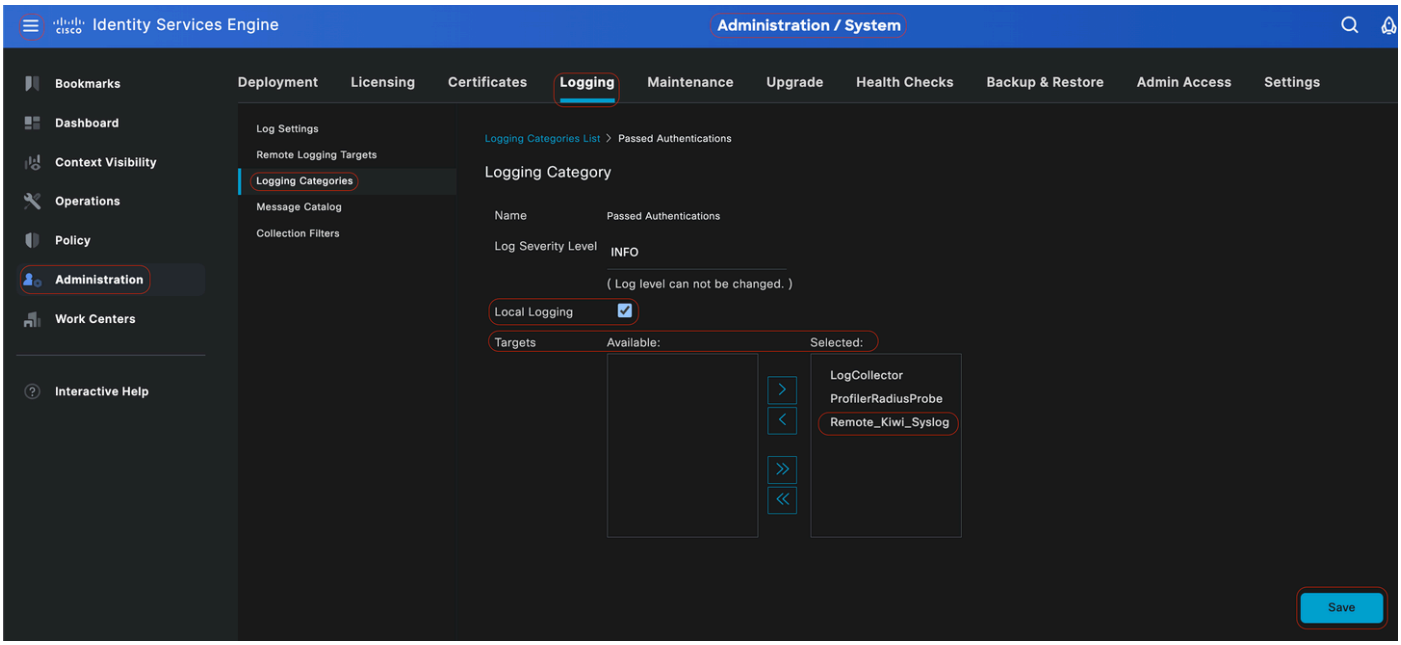
الخطوة 2- التسجيل المحلي: يتيح خانة الاختيار هذه إنشاء السجل المحلي. بمعنى أن السجلات التي تم إنشاؤها بواسطة PSNs يتم حفظها على PSN المحدد الذي يقوم بإنشاء السجل أيضا. نوصي بالاحتفاظ بالتكوين الافتراضي

الخطوة 3- الأهداف: تسمح لك هذه المنطقة باختيار الأهداف لفئة تسجيل عن طريق نقل الأهداف بين AvailableArea و SelectAreas باستخدام رموز الأسهم الأيمن والأيسر.

تحتوي AvailableArea على أهداف التسجيل الموجودة، المحلية (المحددة مسبقا) والخارجية (المحددة من قبل المستخدم).

ثم يعرض Selectedarea، الذي يكون فارغا في البداية، الأهداف التي تم إختيارها للفئة.

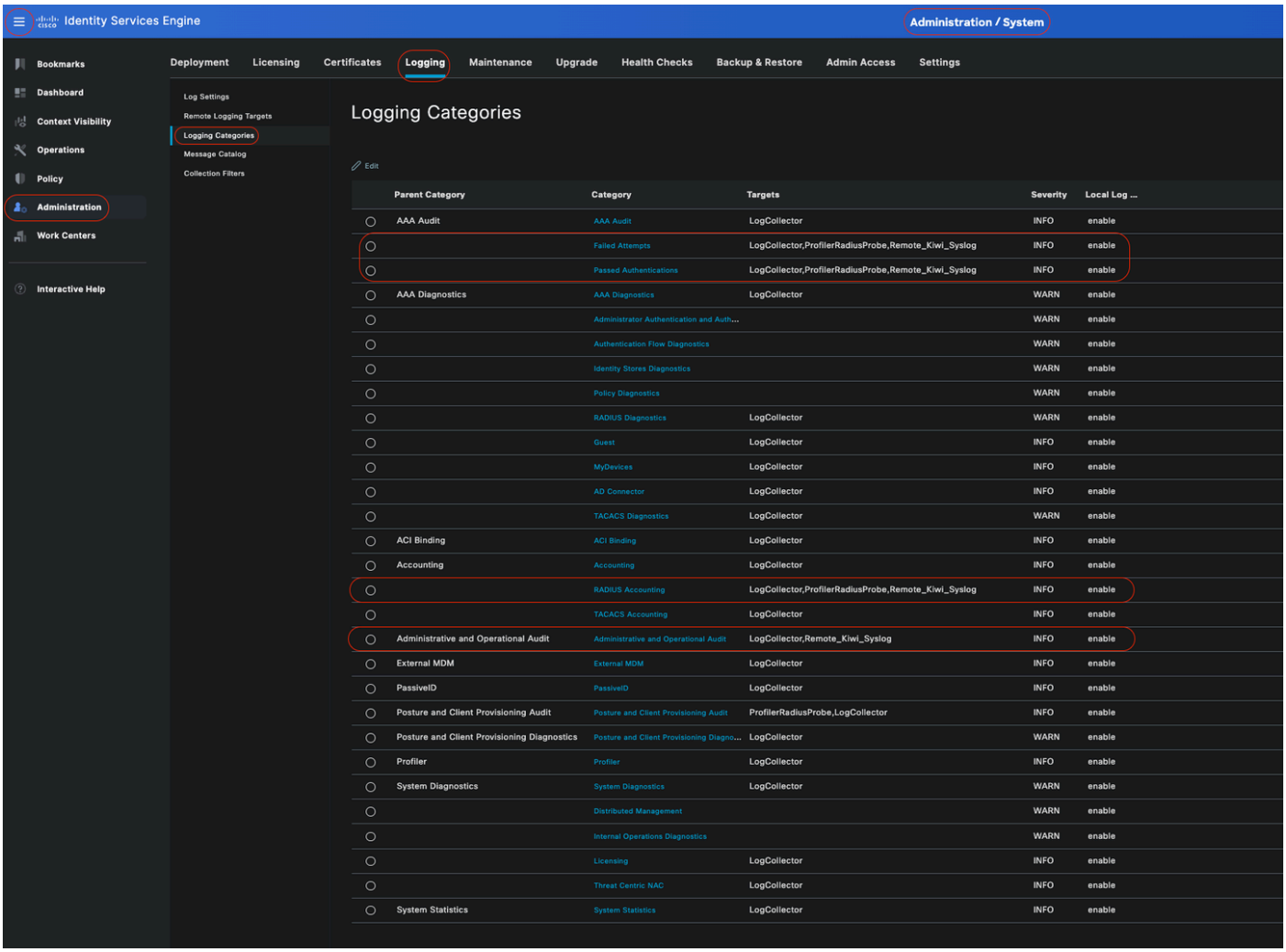
الخطوة 4- كرر الخطوة من الخطوة 1 إلى الخطوة 3 لإضافة الهدف البعيد ضمن فئات محاولات فاشلة ومحاسبة RADIUS.



تعيين الأهداف البعيدة إلى الفئات المقصودة

الخطوة 5- تأكد من أن الهدف البعيد ضمن الفئات المطلوبة.يجب أن تكون قادرا على رؤية الهدف البعيد الذي أضفته للتو.

في لقطة الشاشة هذه، يمكنك رؤية الهدف البعيد Remote_Kiwi_Syslog المعين إلى الفئات المطلوبة.



التحقق من الفئات

فهم الفئات

يتم إنشاء رسالة عند حدوث حدث. هناك أنواع مختلفة من رسائل الحدث التي يتم توليدها من منشآت متعددة مثل kernel، البريد، مستوى المستخدم، وهكذا.

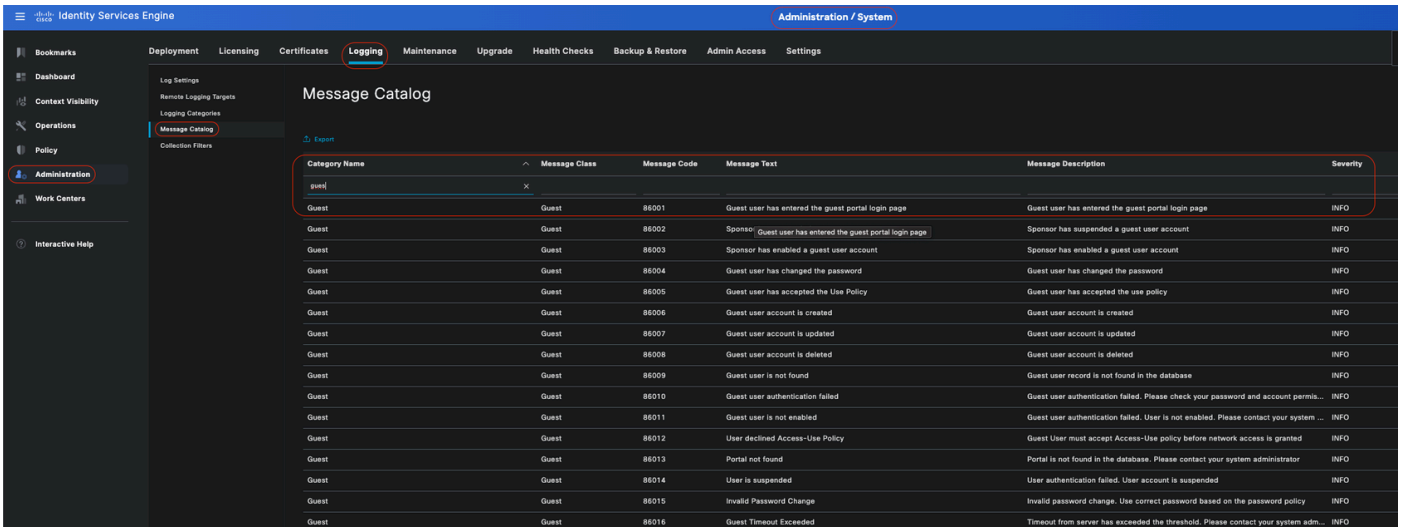
ويتم تصنيف هذه الأخطاء ضمن "كتالوج الرسائل" ويتم تنظيم هذه الأحداث أيضا بشكل هرمي إلى فئات.

تحتوي هذه الفئات على فئات أصلية تحتوي على فئة أو بعض الفئات.

الفئة الأصلية	الفئة
تدقيق المصادقة والتفويض والمحاسبة (AAA)	تدقيق المصادقة والتفويض والمحاسبة (AAA) محاولات فاشلة المصادقة التي تم تمريرها
تشخيصات AAA	تشخيصات AAA

مصادقة المسؤول والتفويض تشخيصات تدفق المصادقة تشخيصات مخزن الهوية تشخيصات السياسة تشخيصات RADIUS ضيف	
الحسابات محاسبة RADIUS	الحسابات
مراجعة الحسابات الإدارية والتشغيلية	مراجعة الحسابات الإدارية والتشغيلية
تدقيق Client Provisioning و Posture	تدقيق Client Provisioning و Posture
تشخيصات Client Provisioning و Posture	تشخيصات Client Provisioning و Posture
محلل	محلل
تشخيصات النظام الإدارة الموزعة تشخيصات العمليات الداخلية	تشخيصات النظام
إحصائيات النظام	إحصائيات النظام

في لقطة الشاشة هذه، يمكنك أن ترى أن Guest عبارة عن فئة رسائل وتم تصنيفها كفئة ضيف. تحتوي فئة Guest هذه على فئة أصل تسمى تشخيصات AAA.



كتالوج الرسائل

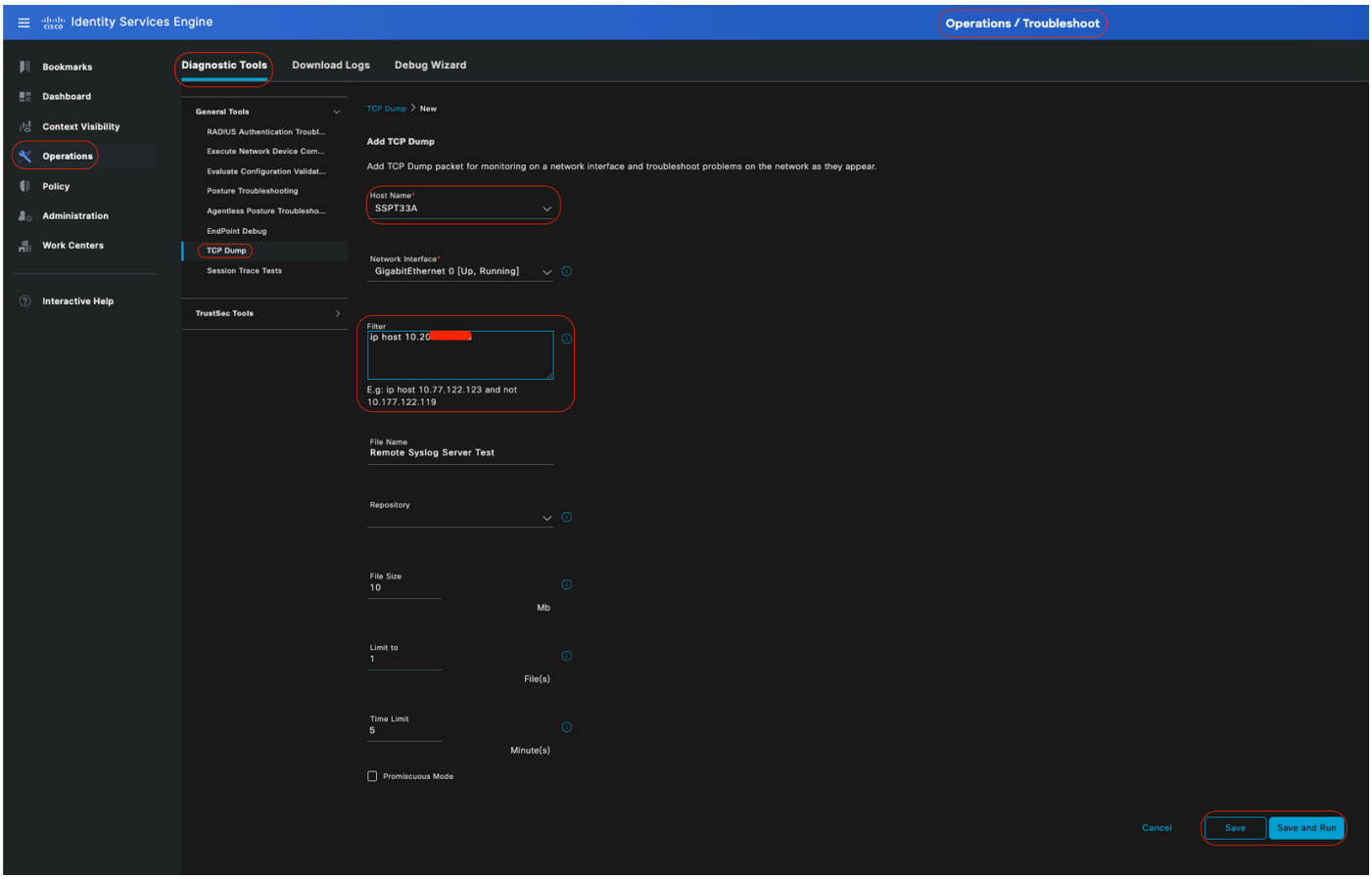
التحقق من الصحة واستكشاف الأخطاء وإصلاحها

يعد إجراء عملية تفريغ TCP مقابل هدف التسجيل عن بعد أسرع خطوة لاستكشاف الأخطاء وإصلاحها والتحقق من صحتها لتأكيد ما إذا كان يتم إرسال أحداث السجل أم لا.

يجب أخذ الالتقاط من PSN الذي يصادق المستخدم لأن PSN سيقوم بإنشاء رسائل السجل وسيتم إرسال هذه الرسائل إلى الهدف البعيد

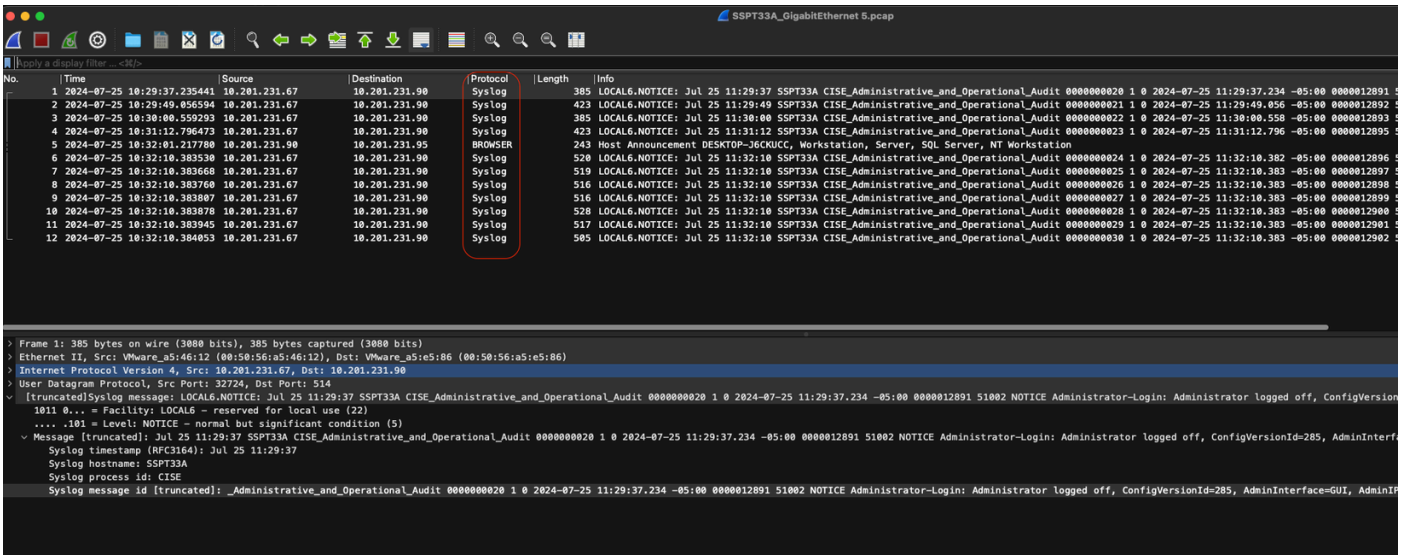
في واجهة المستخدم الرسومية Cisco ISE، انقر فوق الرمز ( ) واخترت عملية>تحريت>TCP تفريغ>طقطقت علي إضافة.

- يجب تصفية حركة المرور، وإضافة حقل تصفية <remote_target_ip_addres> لمضيف ip.
- يجب التقاط التقاط من مصادقة معالجة PSN.



تفريغ TCP

في لقطة الشاشة هذه، يمكنك رؤية كيف يقوم ISE بإرسال رسائل Syslog لحركة مرور تسجيل مسؤول ISE.



حركة مرور Syslog

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).