إنشاء لوحات معلومات وتنبيهات مخصصة على Splunk باستخدام Syslogs من FTD

المحتويات

المقدمة

يصف هذا المستند المشي خطوة بخطوة لتكوين FTD لإرسال syslogs إلى التقسيم واستخدام هذه السجلات لإنشاء لوحات معلومات وتنبيهات مخصصة.

المتطلبات الأساسية

المتطلبات

توصي cisco أن يتلقى أنت معرفة من هذا موضوع قبل أن يمر من خلال هذا تشكيل مرشد:

- Syslog
- معرفة أساسية بلغة معالجة البحث في Splunk (SPL)

يفترض هذا المستند أيضا أن لديك بالفعل مثيل Splunk Enterprise مثبت على خادم ولديك حق الوصول إلى واجهة الويب.

المكونات المستخدمة

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

- Cisco Firepower Threat Defense (FTD) قيد التشغيل على الإصدار 7.2.4
- مركز إدارة Cisco Firepower (FMC) يعمل على الإصدار 7.2.4
- مثيل Splunk Enterprise (الإصدار 9.4.3) قيد التشغيل على جهاز Windows

تم إنشاء المعلومات الواردة في هذه المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذه المستند بتكوين ممسوح (افتراضي).

معلومات أساسية

تقوم أجهزة بروتوكول FTD من Cisco بإنشاء syslogs تفصيلية تغطي أحداث التسلل وسياسات التحكم في الوصول وأحداث الاتصال وغير ذلك الكثير. يتيح دمج هذه السجلات مع إمكانية إجراء تحليل فعال والتنبيه في الوقت الفعلي لعمليات أمان الشبكة.

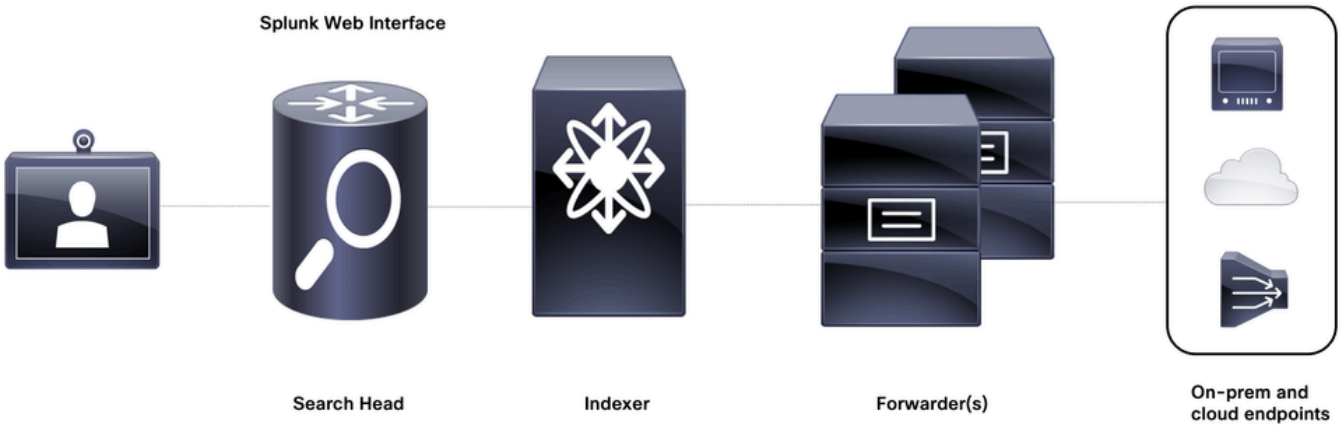
SPLUNK هو نظام تحليلات بيانات في الوقت الفعلي مصمم لاستخراج البيانات التي تم إنشاؤها بواسطة الجهاز وفهرستها والبحث عنها وعرضها. يعتبر SPLUNK فعالا بشكل خاص في بيئات الأمان السيبراني كأداة لإدارة الأحداث ومعلومات الأمان (SIEM) نظرا لقدرته على:

- إدخال بيانات السجل عند القياس
- إجراء عمليات بحث معقدة باستخدام SPL
- إنشاء لوحات معلومات وتنبيهات
- الدمج مع أنظمة الأمن والتوافق مع الحوادث

تقوم عملية Splunk بمعالجة البيانات من خلال تدفقات مهيكلة من أجل جعل بيانات الأجهزة غير مهيكلة أو شبه مهيكلة مفيدة وقابلة للتنفيذ. عادة ما يشار إلى المراحل الأساسية لخط الأنابيب هذا باسم IPIS والتي تمثل:

- الإدخال
- تحليل
- فهرسة
- بحث

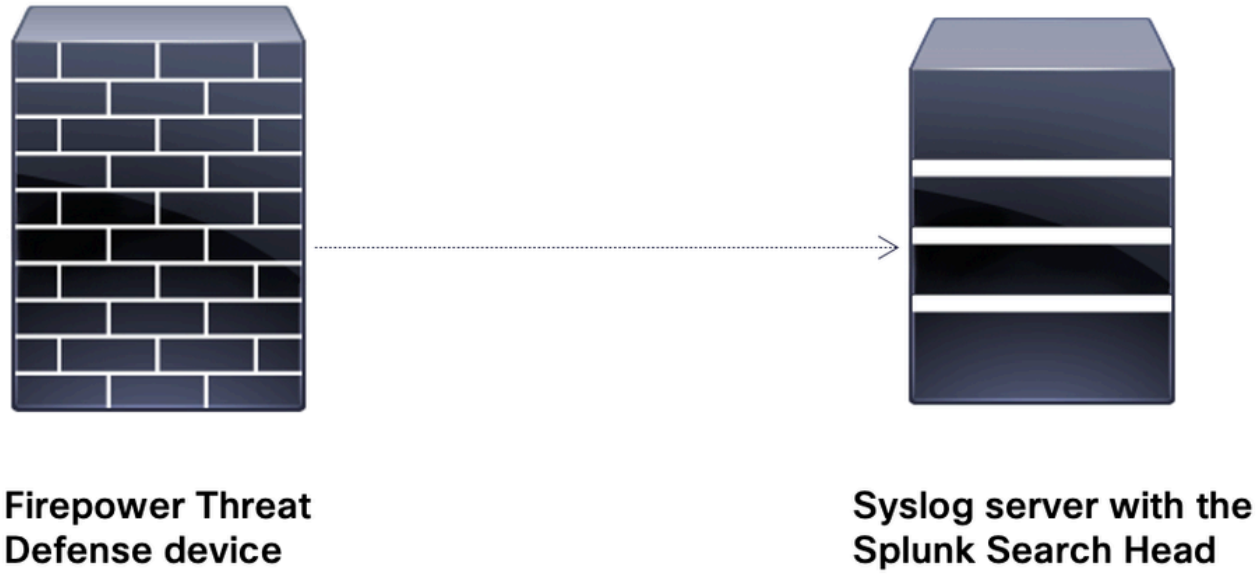
يتم عرض المكونات العامة الرئيسية للبنية الأساسية المستخدمة في تحقيق تدفقات IPIS في هذا الرسم التخطيطي:



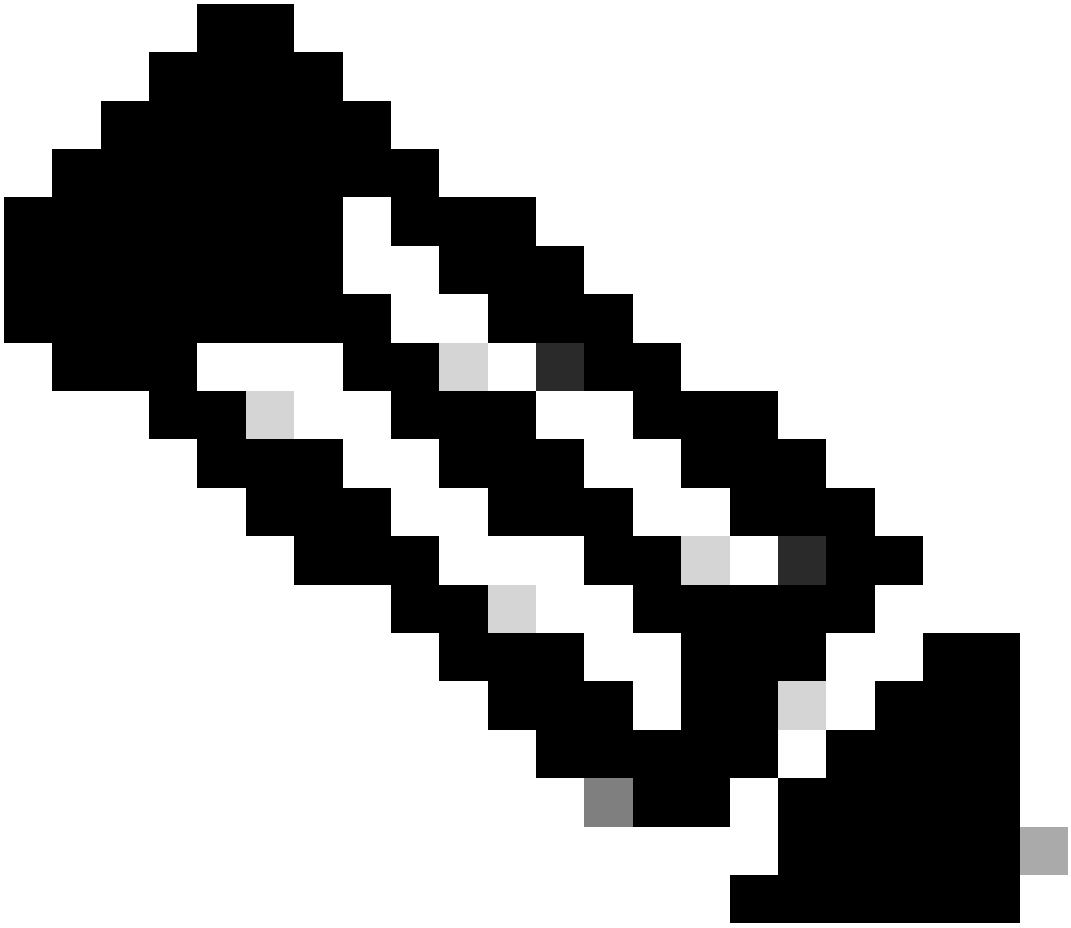
بنية أساسية ضخمة

التكوين

الرسم التخطيطي للشبكة



الرسم التخطيطي للشبكة

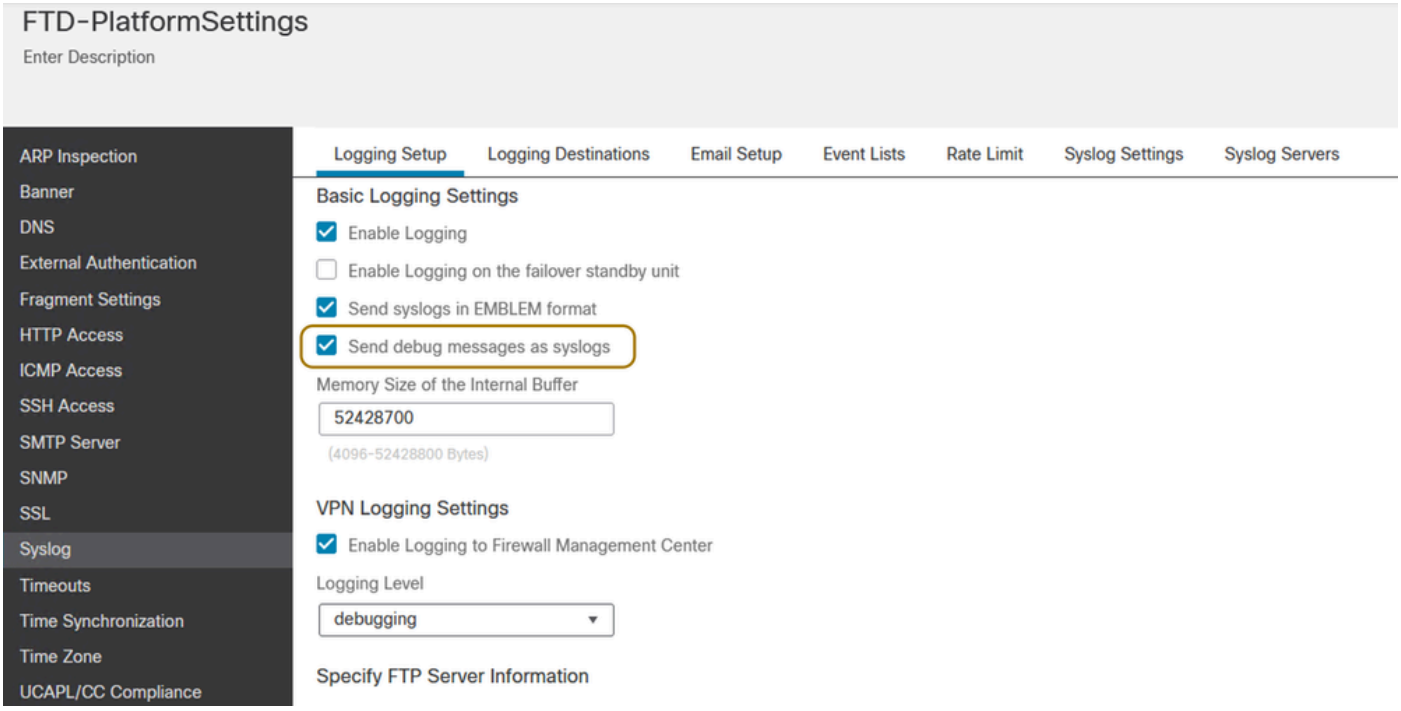


ملاحظة: لا تتطلب بيئة المعمل الخاصة بهذا المستند مثيلات منفصلة للمصدر والمفهرسة. يعمل جهاز Windows، أي خادم syslog الذي تم تثبيت مثيل Splunk Enterprise عليه كمفهرس ورأس بحث.

التكوينات

تكوين إعدادات syslog ل FTD

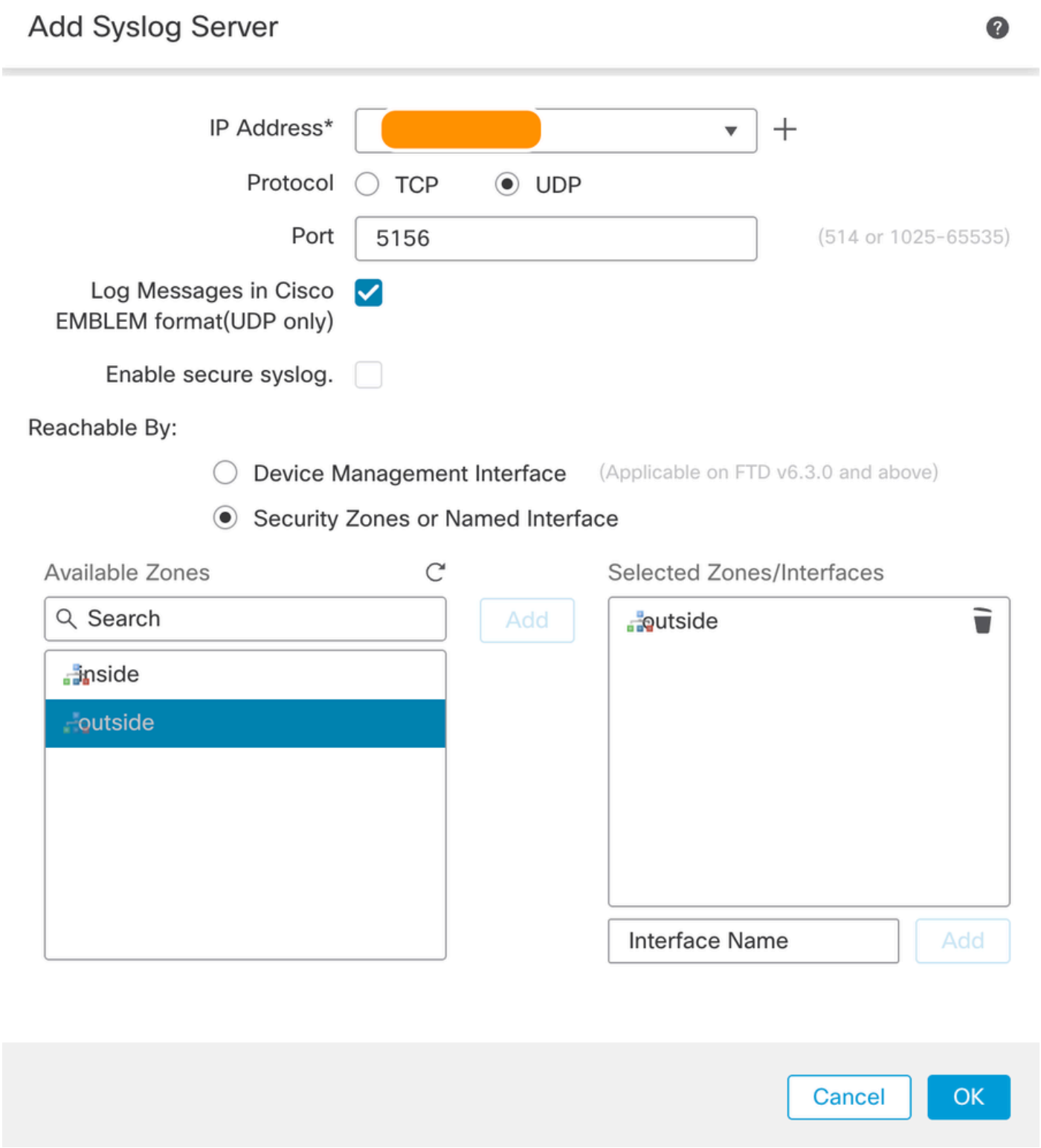
الخطوة 1. قم بتكوين إعدادات syslog الأولية على FMC ل FTD ضمن الأجهزة > إعدادات النظام الأساسي لإرسال السجلات إلى خادم syslog الذي يتم تشغيل مثيل Splunk عليه.



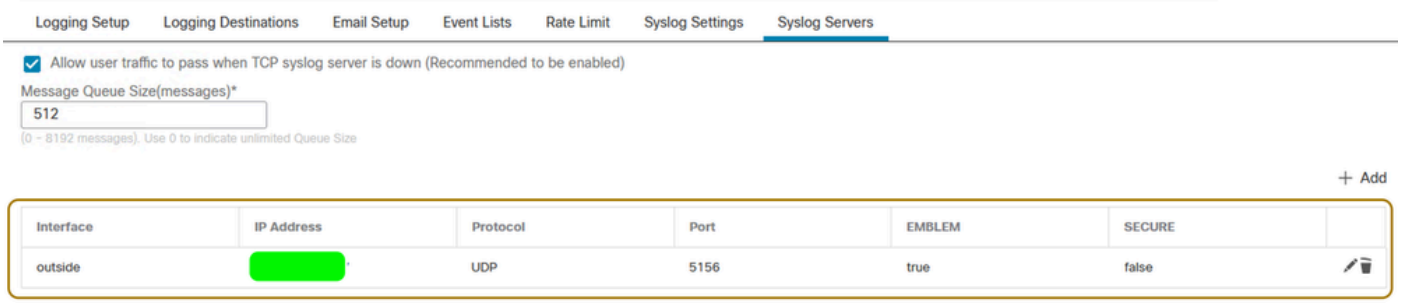
إعدادات النظام الأساسي على FTD - Syslog

الخطوة 2. قم بتكوين عنوان IP للجهاز الذي يتم فيه تثبيت مثيل Splunk Enterprise وتشغيله كخادم syslog. قم بتحديد الحقول كما هو مذكور.

```
IP Address: Fill in the IP address of the host acting as the syslog server
Protocol: TCP/UDP (usually UDP is preferred)
Port: You can choose any random high port. In this case 5156 is being used
Interface: Add the interface(s) through which you have connectivity to the server
```

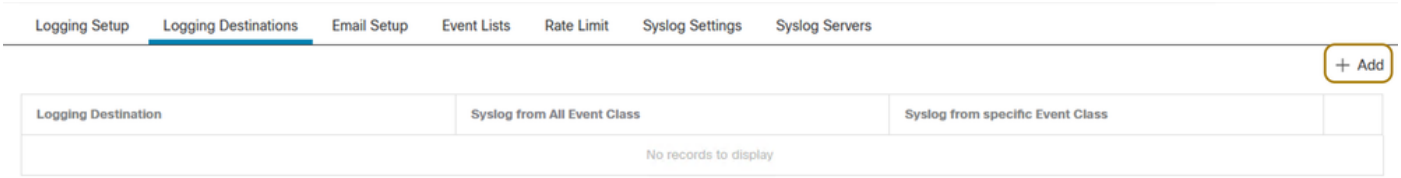


إعدادات النظام الأساسي على FTD - إضافة خادم syslog

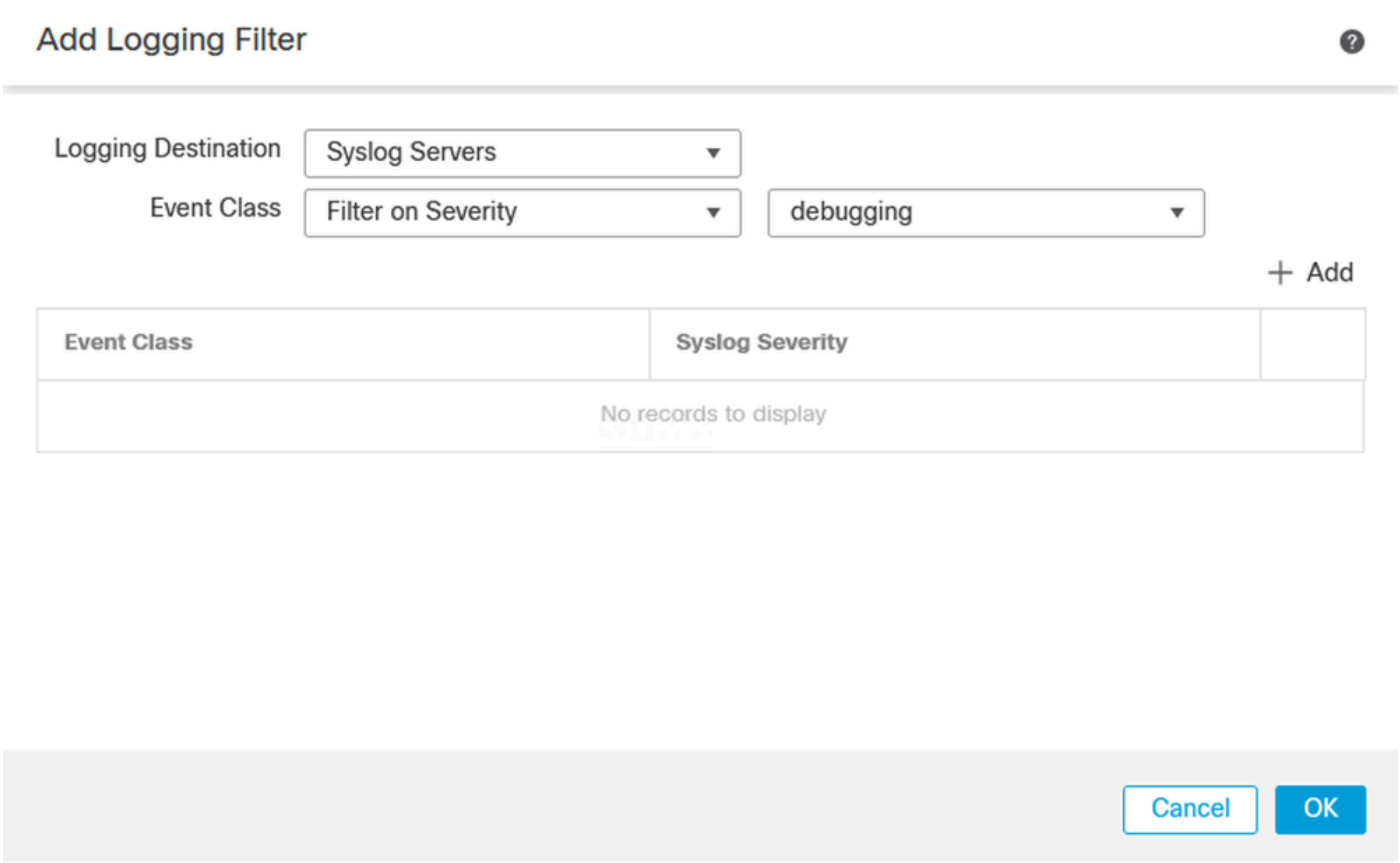


إعدادات النظام الأساسي على FTD - خادم Syslog مضاف

الخطوة 3. أضف وجهة تسجيل لخوادم Syslog. يمكن تعيين مستوى التسجيل وفقا لحالة الاختيار أو الاستخدام الخاصة بك.



إعدادات النظام الأساسي على FTD - إضافة وجهة تسجيل



إعدادات النظام الأساسي على FTD - تعيين مستوى الخطورة لوجهة التسجيل

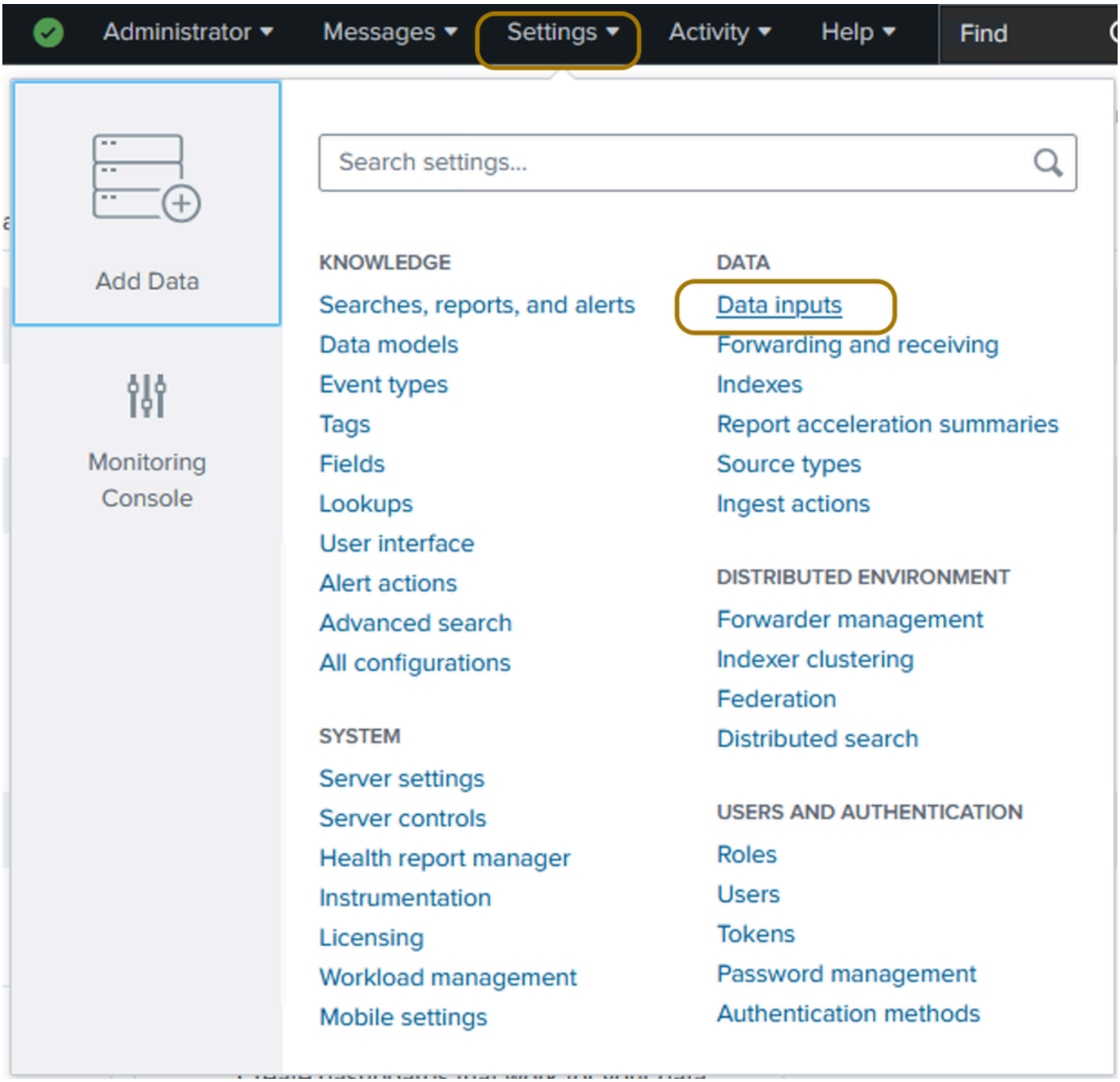
قم بنشر تغييرات إعداد النظام الأساسي على FTD بعد إكمال هذه الخطوات.

تكوين إدخال بيانات على مثيل Splunk Enterprise

الخطوة 1. تسجيل الدخول إلى واجهة ويب مثيل Splunk Enterprise.

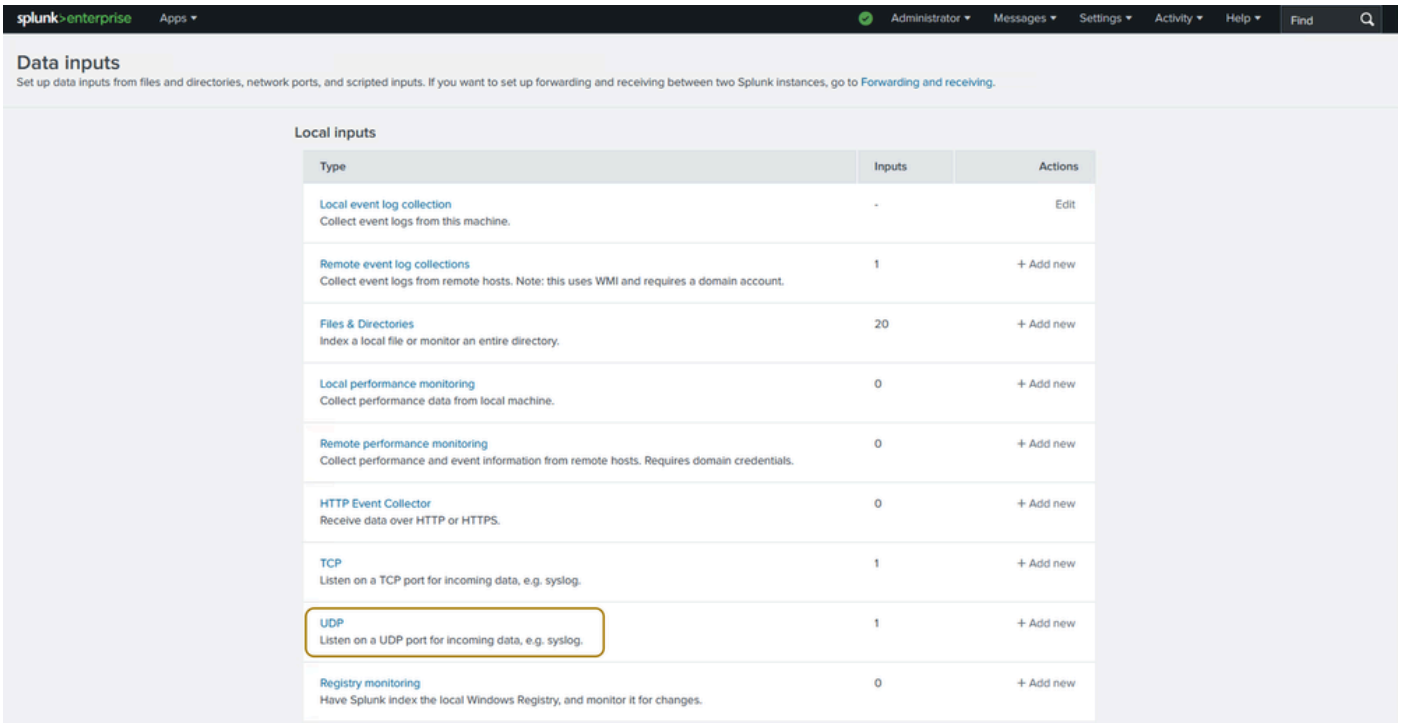
صفحة تسجيل الدخول إلى واجهة ويب SPLUNK

الخطوة 2. يجب تحديد إدخال بيانات حتى يمكنك تخزين وفهرسة syslogs على Splunk. انتقل إلى الإعدادات > البيانات > إدخالات البيانات بعد تسجيل الدخول.

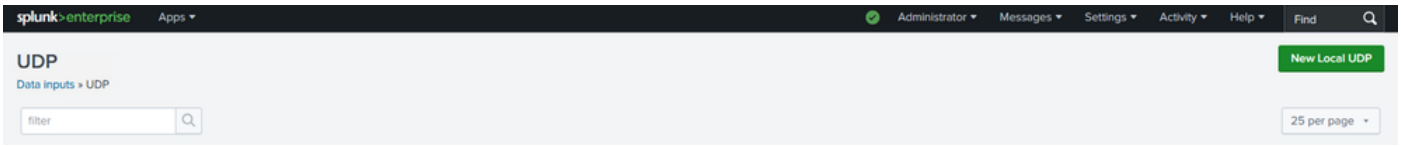


انتقل إلى مدخلات البيانات في Splunk

الخطوة 3. أختر UDP ثم انقر على UDP المحلي الجديد في الصفحة التالية التي تظهر.

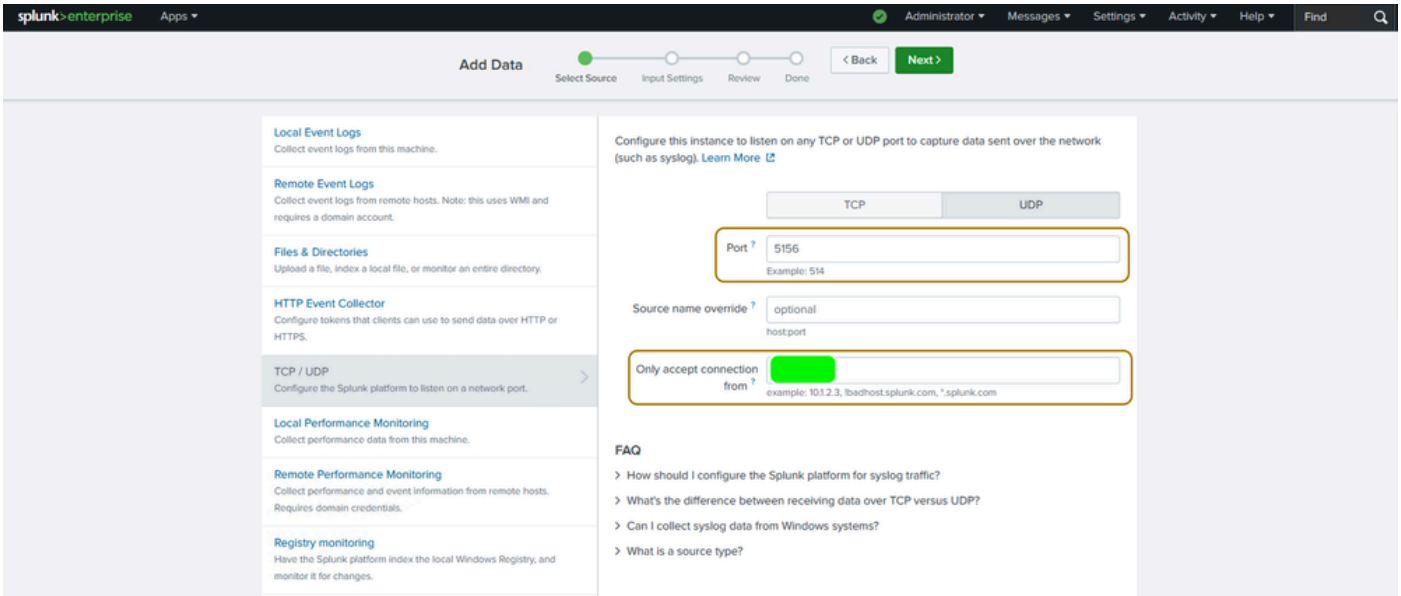


انقر على 'UDP' لإدخال بيانات UDP



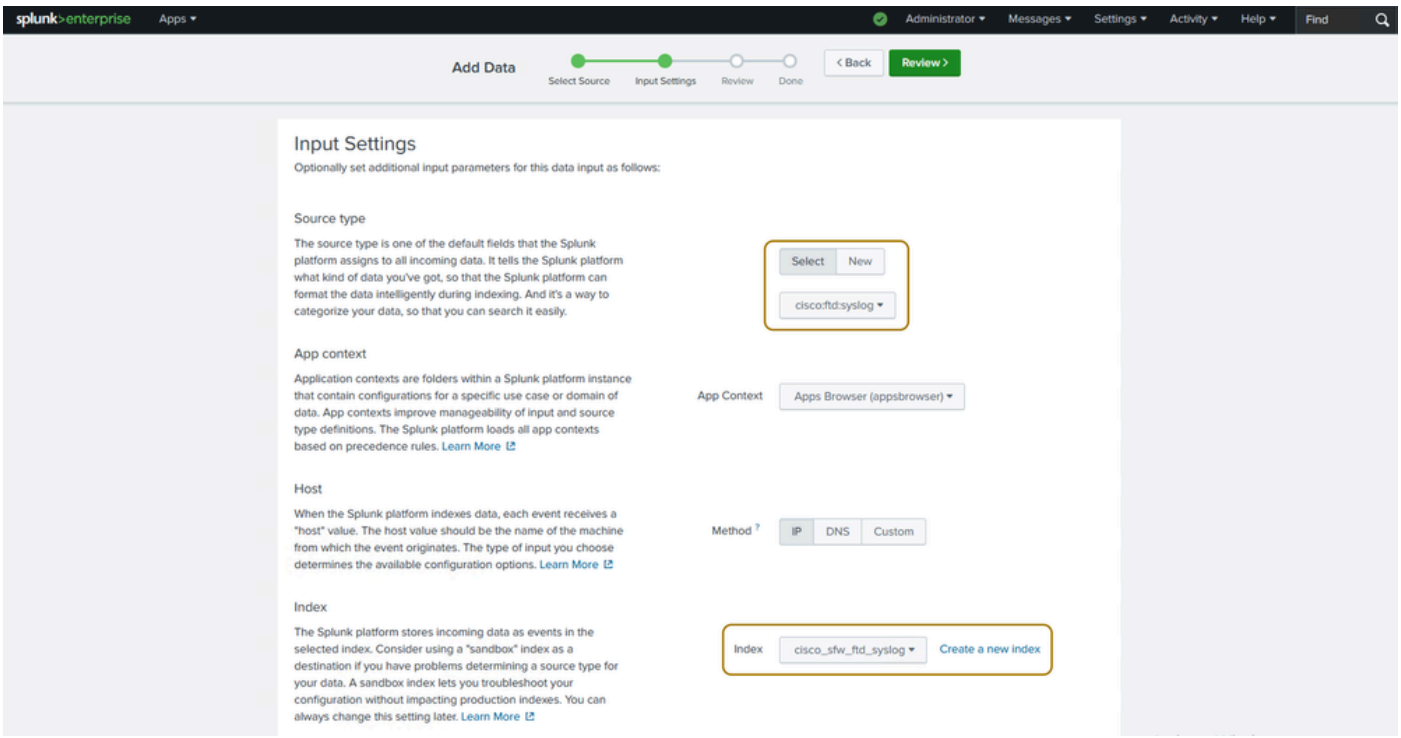
إنشاء إدخال 'UDP محلي جديد'

يدخل خطوة 4. المينا عل أي ال syslogs يكون أرسلت. وه ينبغي كنت ال نفس بما أن المينا يشكل عل ال FTD syslog عملية إعداد، في هذه الحالة 5156. in order to قبلت ال syslogs فقط من واحد مصدر (ال FTD)، ثبتت ال فقط قبول توصيل من مجال إلى ال IP من القارن عل ال FTD أن يكون يتصل مع ال splunk دان. انقر فوق Next (التالي).



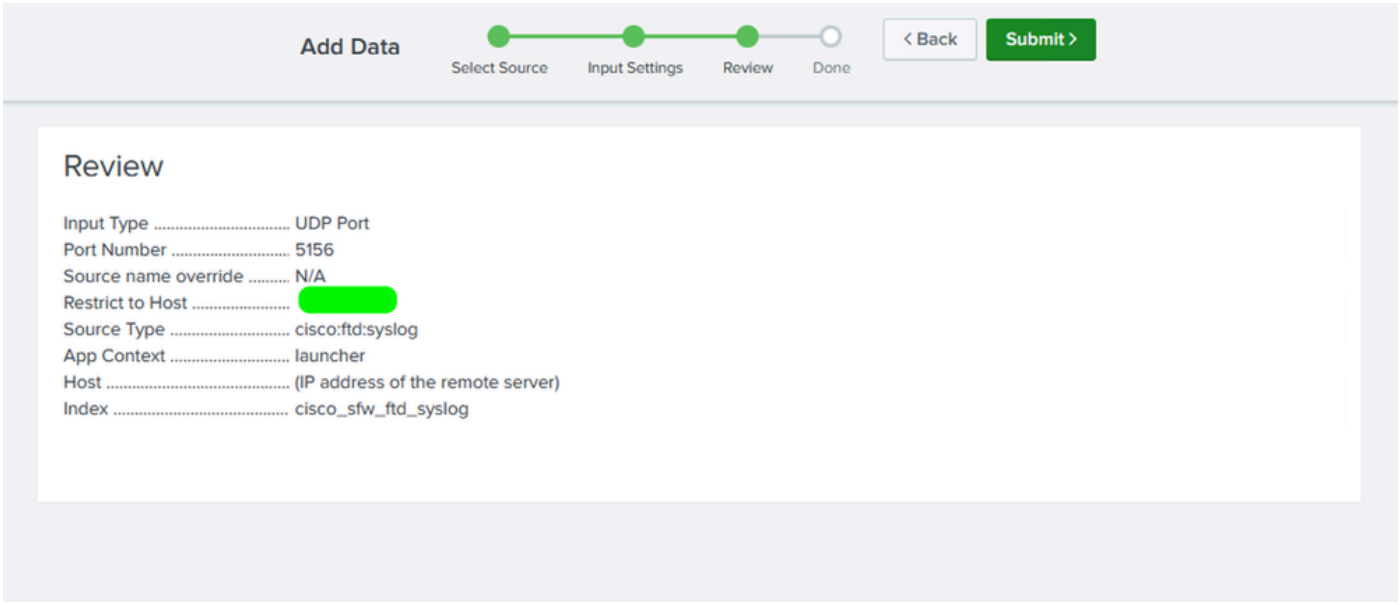
تحديد عنوان IP للمنفذ و FTD

الخطوة 5. يمكنك البحث واختيار نوع المصدر وفهرسة قيم الحقل من تلك المحددة مسبقا على Splunk كما هو مبرز في الصورة التالية. يمكن إستخدام الإعدادات الافتراضية للحقول المتبقية.



تكوين إعدادات إدخال البيانات

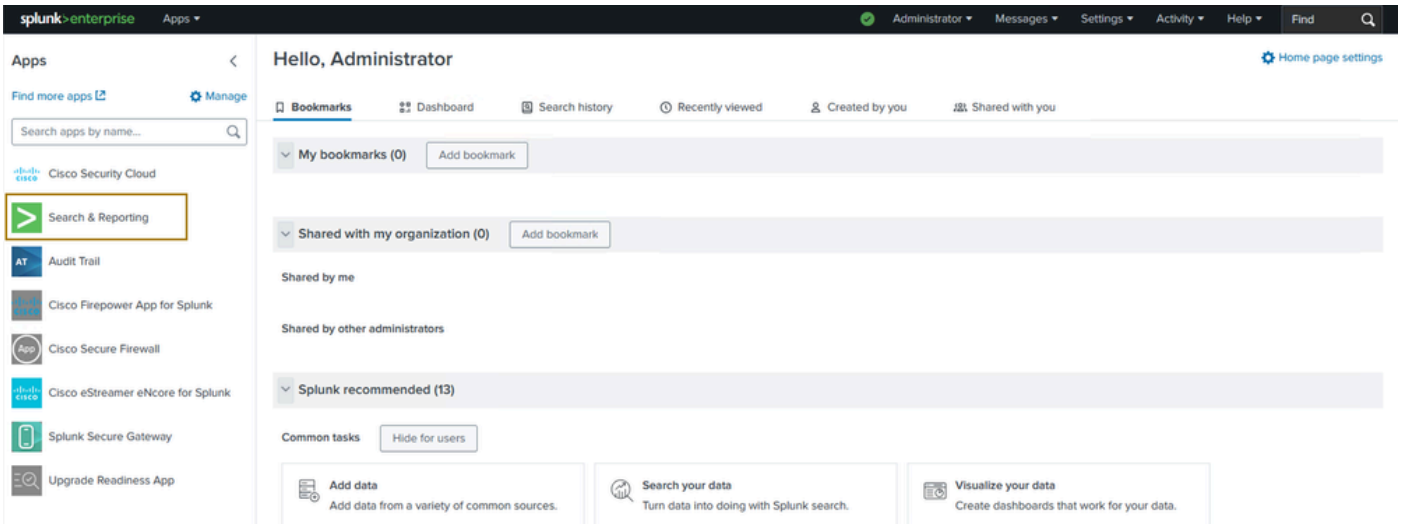
الخطوة 6. راجع الإعدادات وانقر فوق إرسال.



مراجعة إعدادات إدخال البيانات

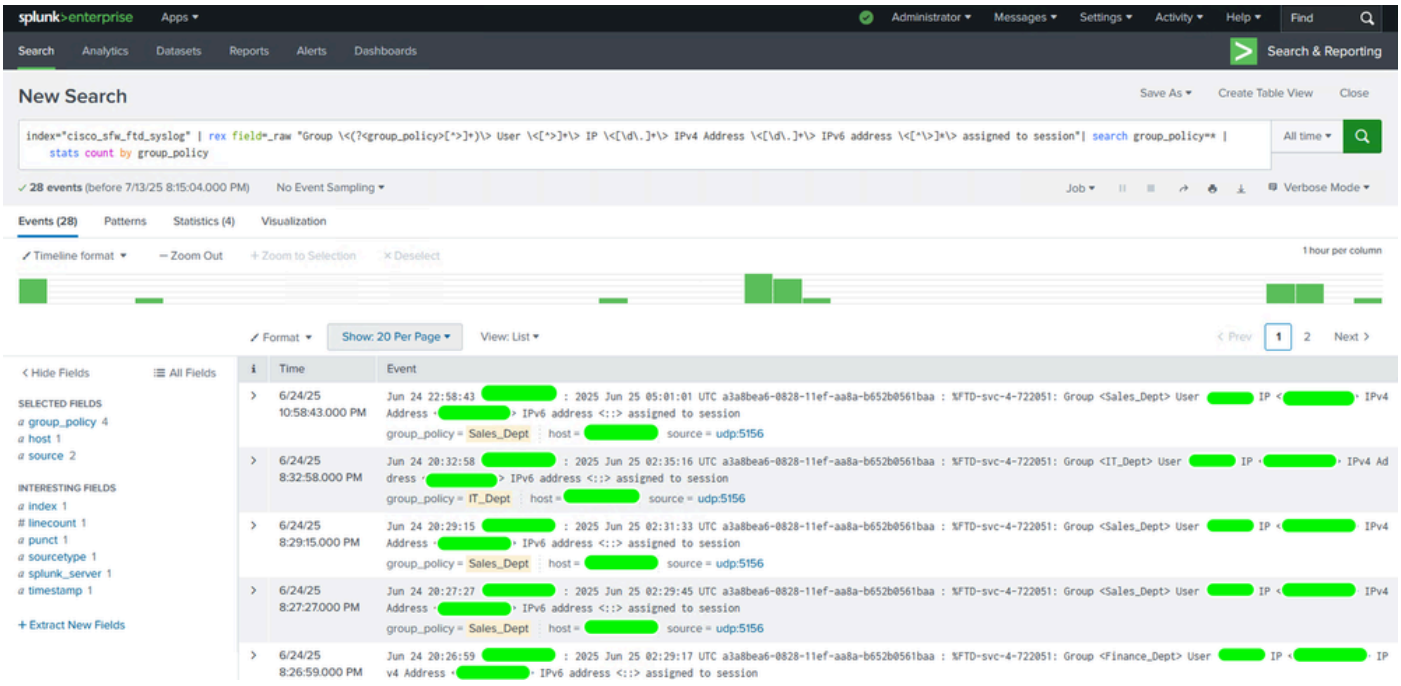
تنفيذ استعلامات SPL وإنشاء لوحات المعلومات

الخطوة 1. انتقل إلى تطبيق البحث وإعداد التقارير على Splunk.

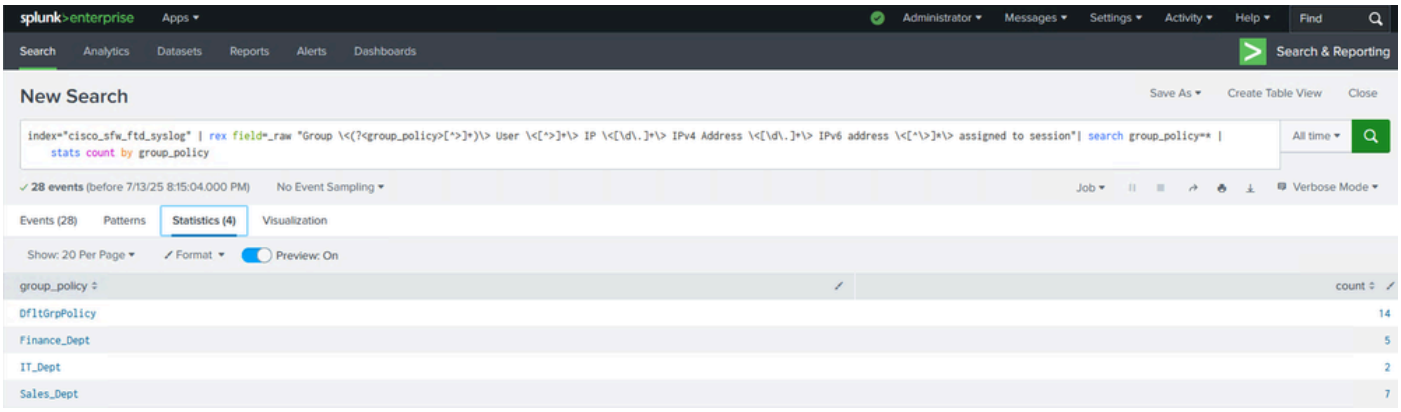


انتقل إلى تطبيق البحث وإعداد التقارير

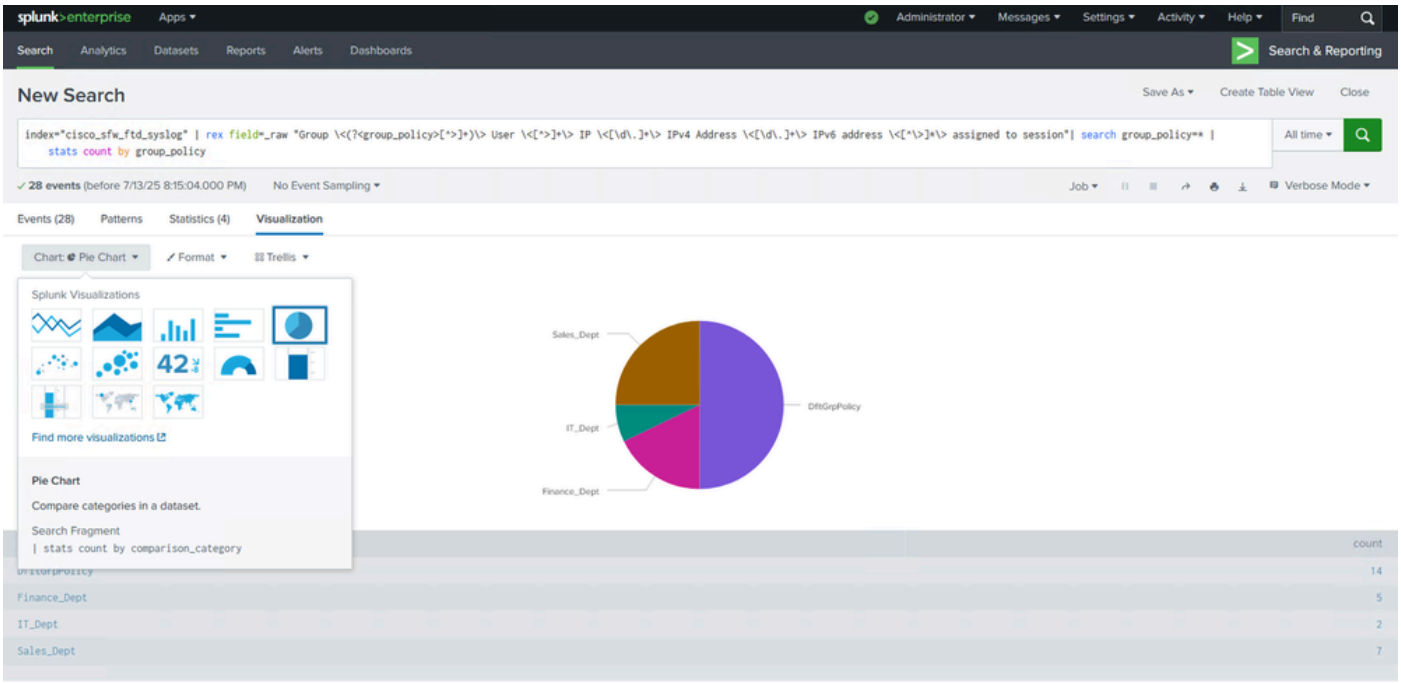
الخطوة 2. قم بصياغة استعلام SPL وتنفيذه وفقا للبيانات التي تريد تصورها. ستتمكن من رؤية كل سجل بشكل كامل (في الوضع المطول) ضمن علامة التبويب الأحداث، وعدد الاتصالات لكل نهج مجموعة في علامة التبويب إحصائيات وعرض هذه البيانات مرئيا باستخدام هذه الإحصائيات ضمن علامة التبويب المرئيات.



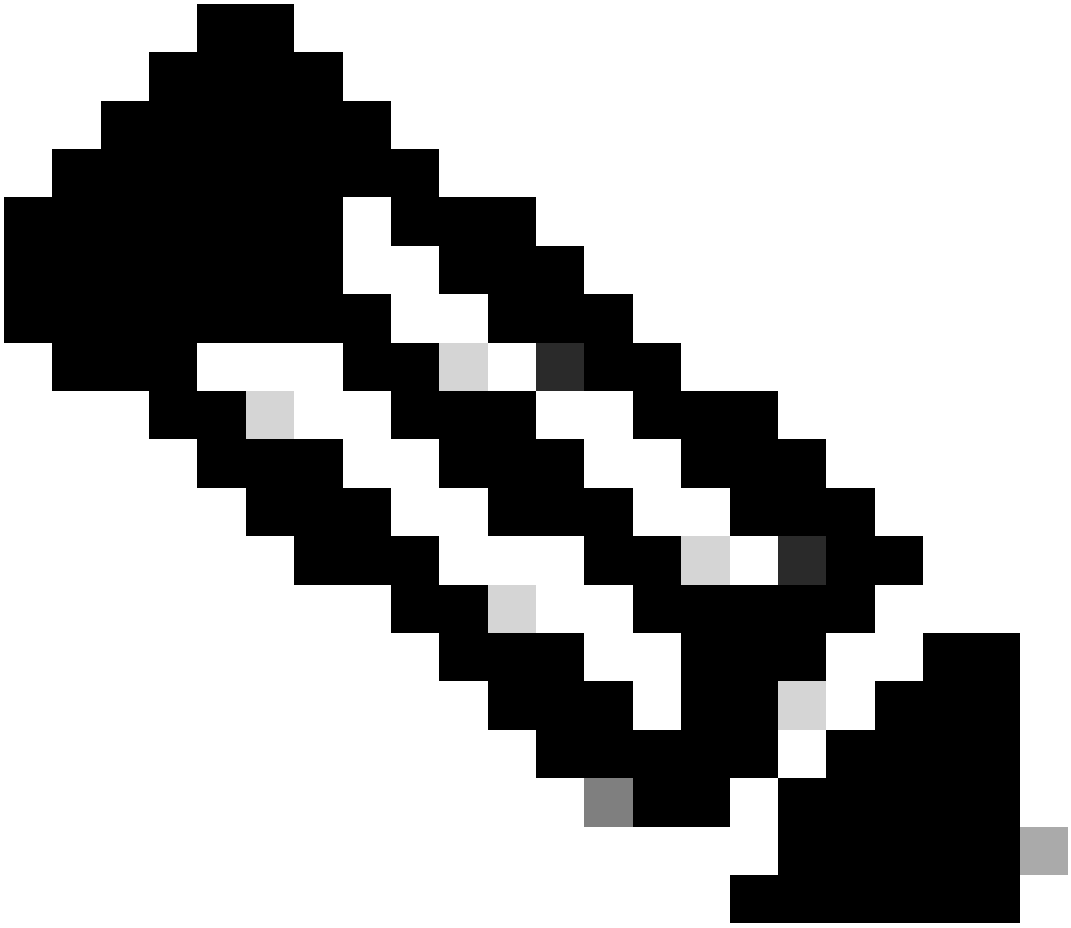
البحث عن أحداث باستخدام استعلامات SPL



تحقق من علامة التبويب الإحصائيات

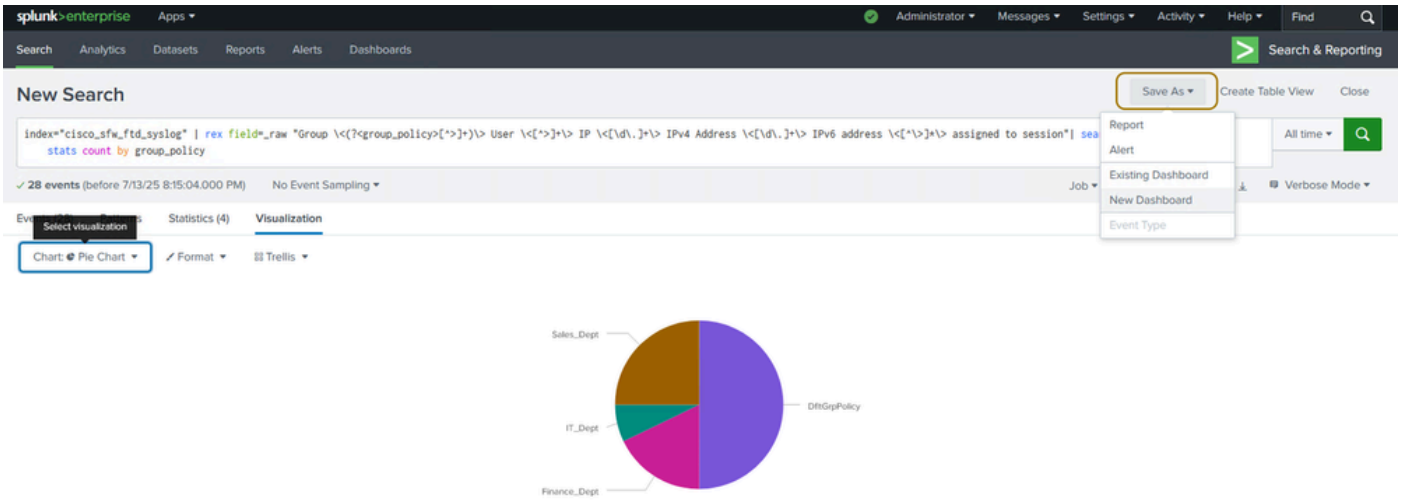


سوف تعرض علامة التبويب المرئيات الرسم البياني/المخطط



ملاحظة: في هذا المثال، يقوم الاستعلام بجلب سجلات اتصالات VPN للوصول عن بعد الناجحة عبر نهج مجموعة مختلفة. تم إستخدام مخطط دائري لعرض عدد الاتصالات الناجحة ونسبتها المئوية لكل نهج مجموعة. بناءا على استيراداتك وتفضيلاتك، يمكنك إختيار إستخدام نوع مختلف من المرئيات مثل الرسم البياني الشريطي كذلك.

الخطوة 3. انقر فوق حفظ باسم واختر لوحة معلومات جديدة أو موجودة وقم إذا كانت لديك لوحة معلومات ترغب إضافة هذه اللوحة إليها أو ترغب إنشاء لوحة معلومات جديدة. تعرض هذه المثلة الأخيرة.



حفظ اللوحة في لوحة معلومات

الخطوة 4. حدد عنوان للوحة المعلومات التي تقوم بإنشائها وأدخل عنوان للوحة التي ستحتوي على المخطط الدائري.

Save Panel to New Dashboard

Dashboard Title: FTD_Dashboard

ftd_dashboard — Edit ID

Description: Optional

Permissions: Private

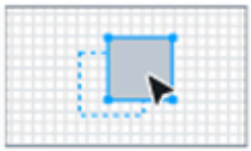
How do you want to build your dashboard? What's this?

Classic Dashboards
The traditional Splunk dashboard builder

Dashboard Studio NEW
A new builder to create visually-rich, customizable dashboards

Select layout mode

Absolute
Full layout control



Grid
Quick organization

Panel Title: Successful RAVPN Connections Per Group Policy

Visualization Type: Pie Chart | Statistics Table

> Advanced Panel Settings

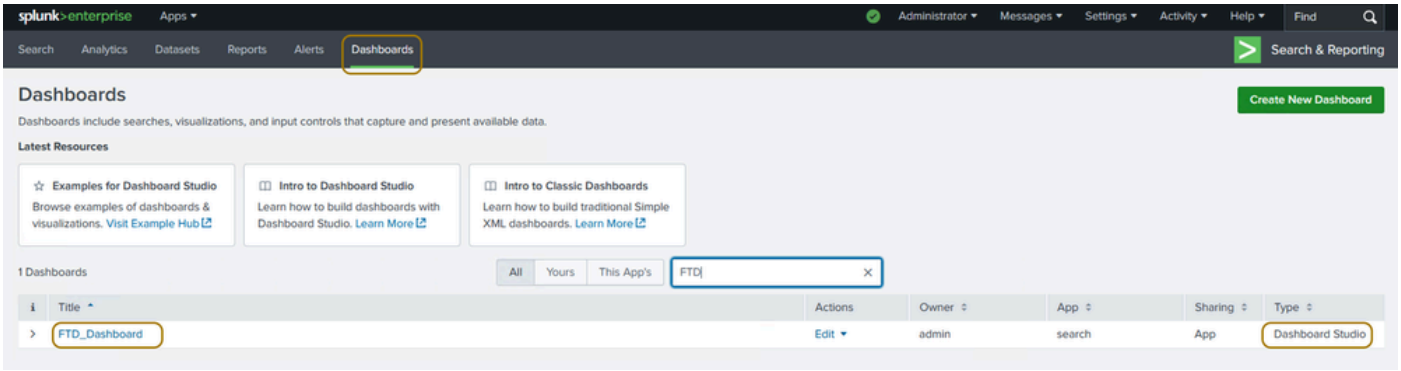
Cancel | Save to Dashboard

إعدادات لوحة المعلومات الجديدة

بناء على ما إذا كان من المفترض عرض لوحة المعلومات فقط أم السماح للمستخدمين الآخرين الذين لديهم حق الوصول إلى مثيل Splunk أيضا. علاوة على ذلك، بناء على ما إذا كنت تريد التحكم متعدد المستويات في إعدادات اللوحة وتخطيط لوحة المعلومات أم لا، أختر الوضع Classic أو Dashboard Studio لإنشاء لوحة المعلومات الخاصة بك.

الخطوة 5 (اختيارية). قم بتنفيذ المزيد من استعلامات SPL وحفظها كلوحات إلى لوحة المعلومات هذه وفقا لمتطلباتك باستخدام الخطوات السابقة المذكورة.

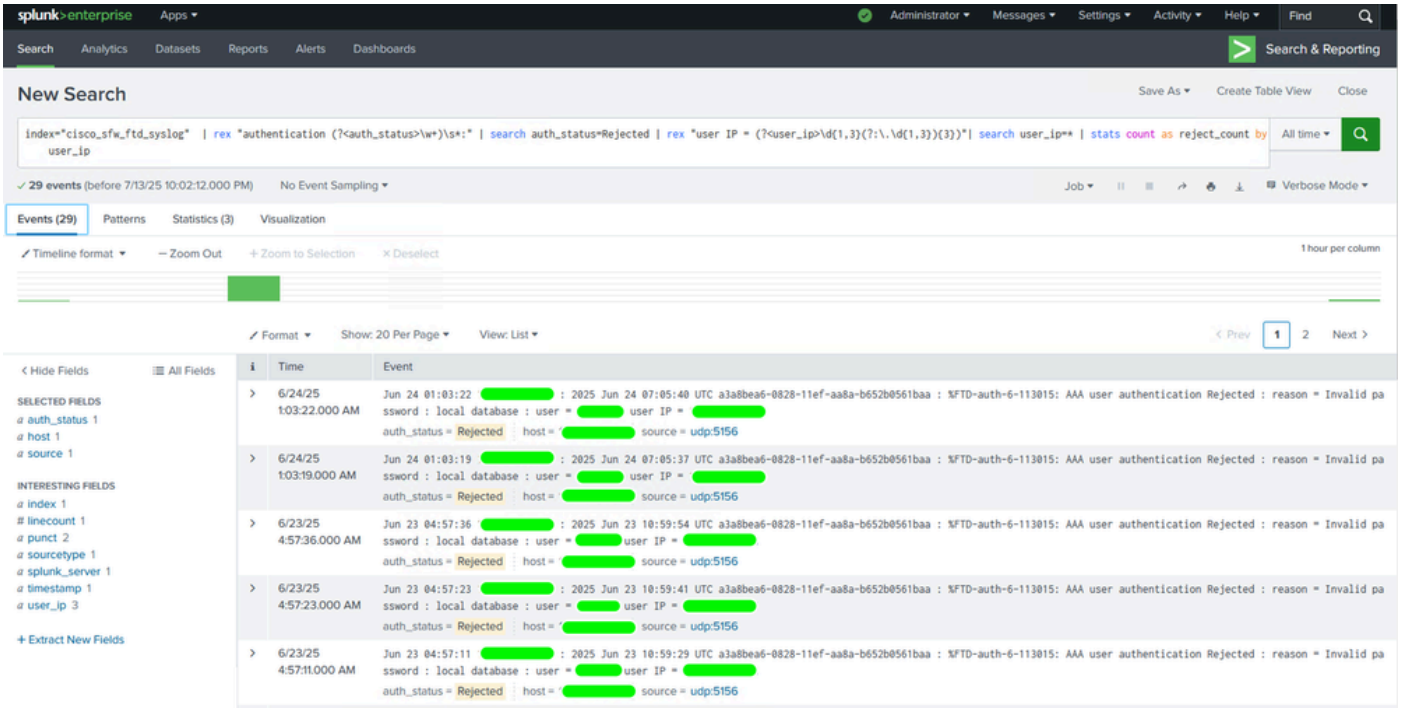
الخطوة 6. انتقل إلى علامة التبويب لوحة المعلومات للبحث في لوحة المعلومات التي قمت بإنشائها واختيار هذه اللوحة. انقر عرض، تحرير، أو إعادة ترتيب لوحاتك.



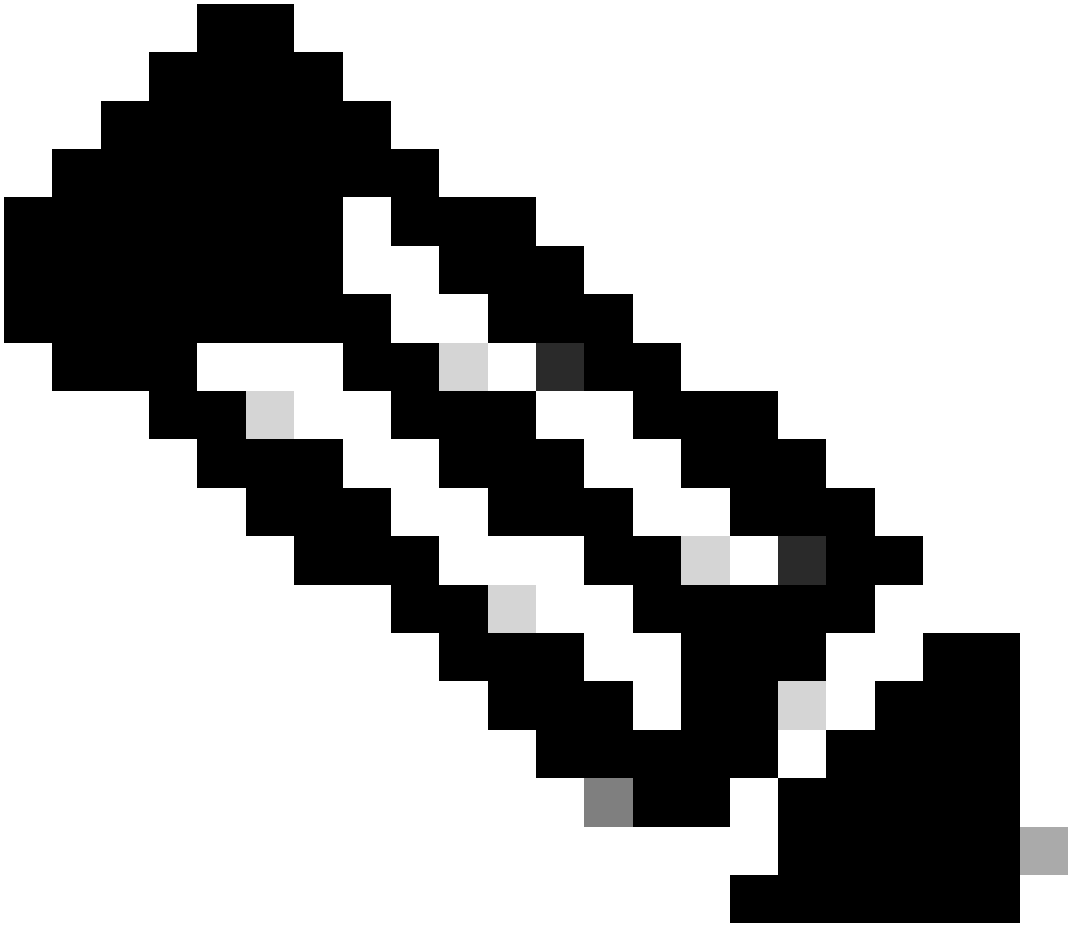
كيفية عرض لوحة المعلومات

تكوين التنبيهات استنادا إلى استعلامات SPL

الخطوة 1. انتقل إلى تطبيق البحث وإعداد التقارير لإنشاء استعلام SPL وتشغيله للتحقق من أنه يجلب السجلات الصحيحة التي سيتم إستخدامها لتشغيل التنبيه.



تشغيل استعلامات SPL لإنشاء تنبيهات خاصة



ملاحظة: في هذا المثال، يتم إستخدام الاستعلام لجلب سجلات المصادقة الفاشلة لشبكة VPN الخاصة بالوصول عن بعد لتشغيل التنبيهات عندما يتجاوز عدد المحاولات الفاشلة حدا معينا خلال فترة زمنية معينة.

الخطوة 3. انقر فوق حفظ باسم واختر تنبيه.

حفظ التنبيه

الخطوة 4. حدد عنوانا لتسمية التنبيه. قم بتعبئة كافة التفاصيل والمرشدات الأخرى المطلوبة لتكوين التنبيه وانقر فوق حفظ. تم ذكر الإعدادات المستخدمة لهذا التنبيه هنا.

<#root>

Permissions: Shared in App.
Alert Type: Real-time (allows failed user authentications in the last 10 minutes can be tracked continu
Trigger Conditions: A

custom

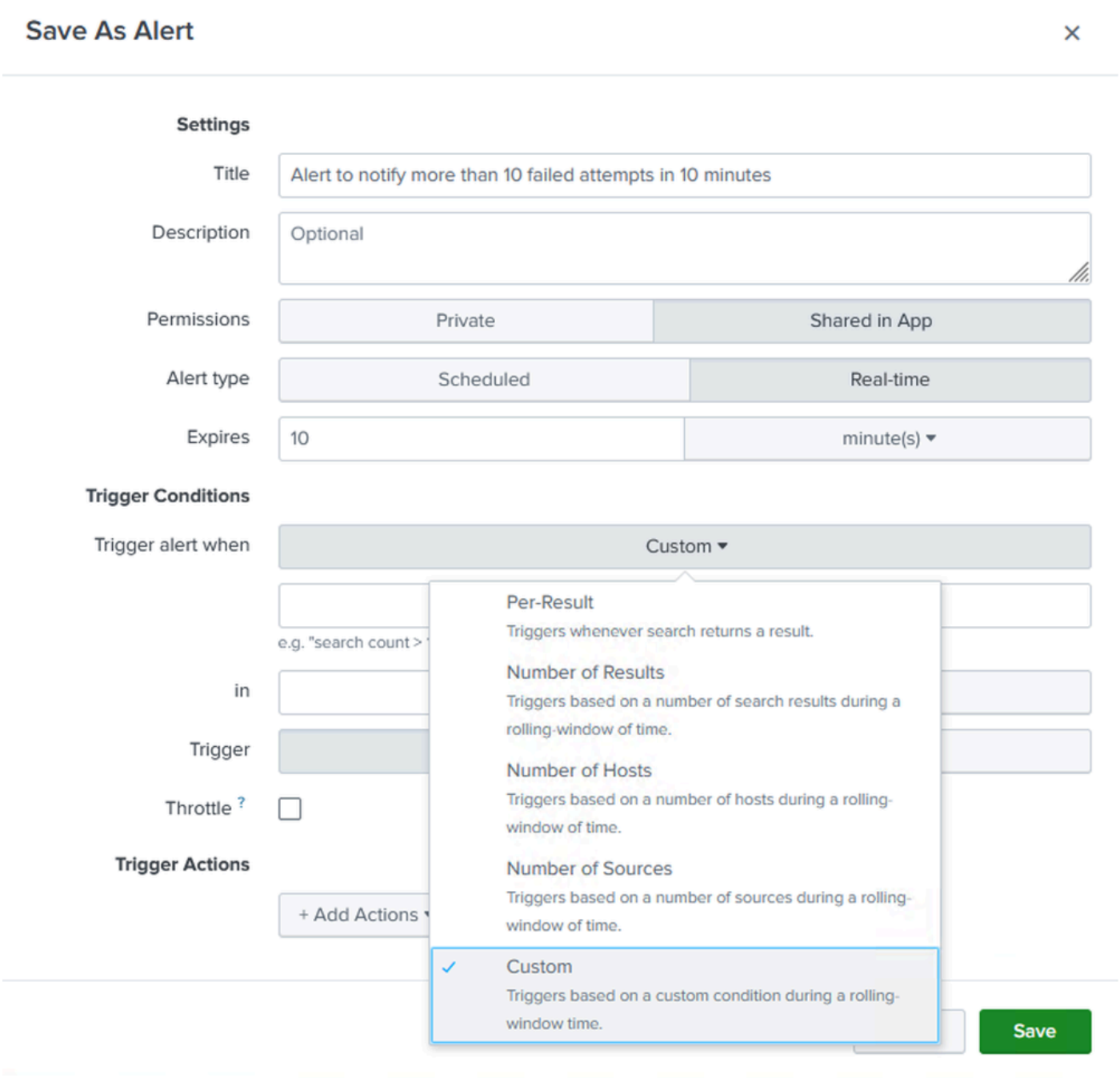
condition is used to search if the

reject_count

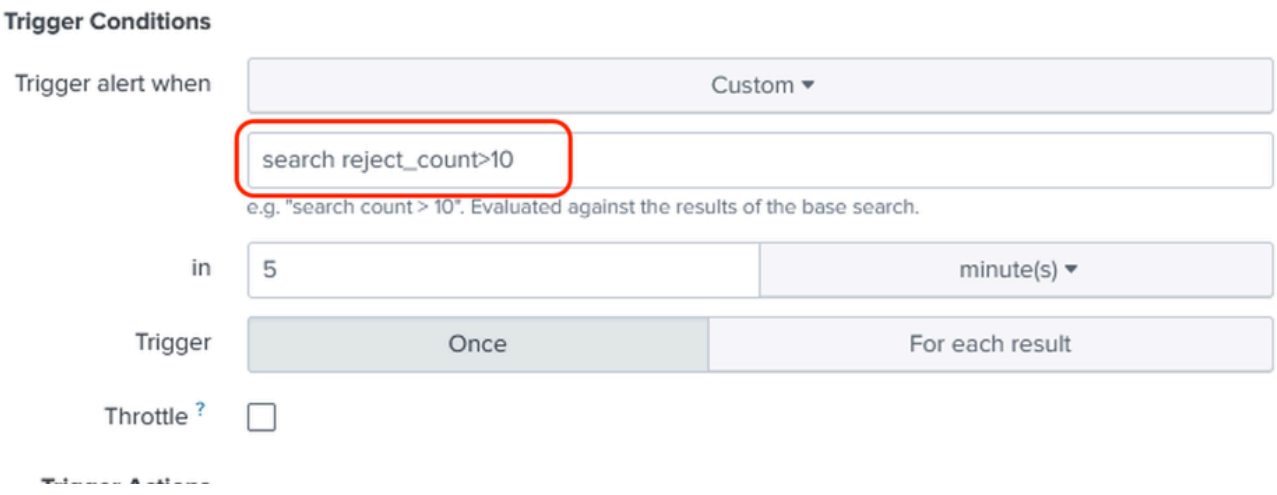
counter from the SPL query has exceeded 10 in the last 5 minutes for any IP address.
Trigger Actions: Set a trigger action such as

Add to Triggered Alerts, Send email, etc.

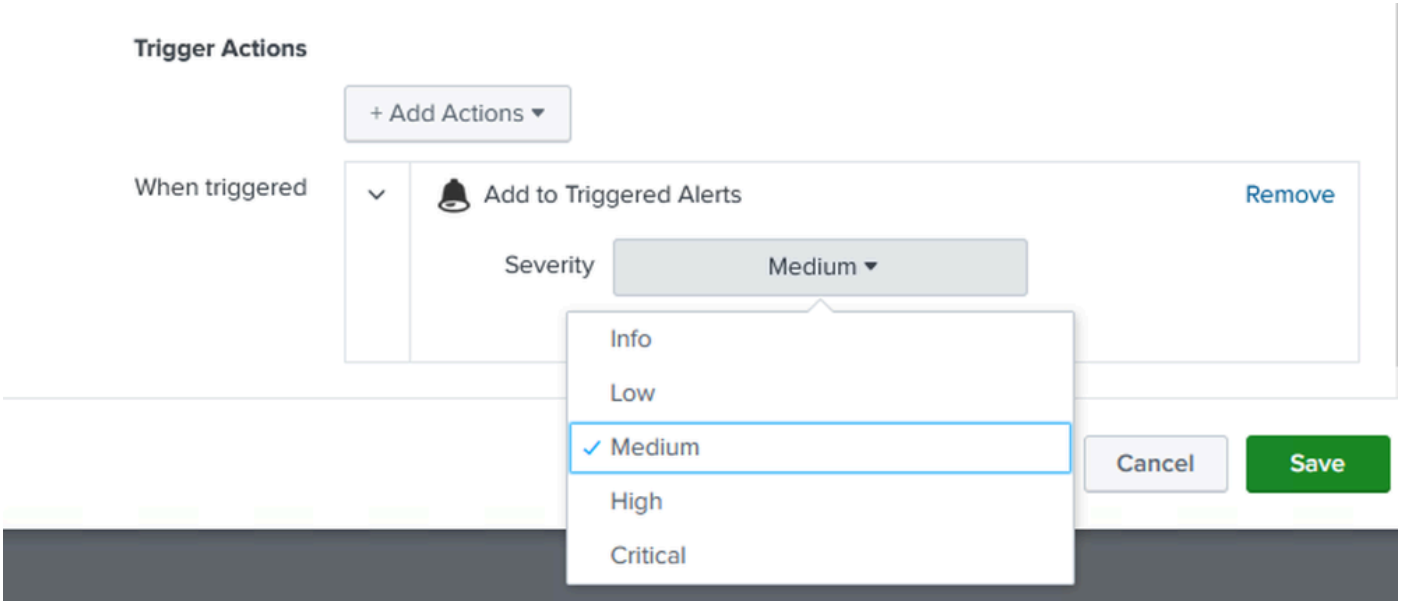
and set the alert severity as per your requirement.



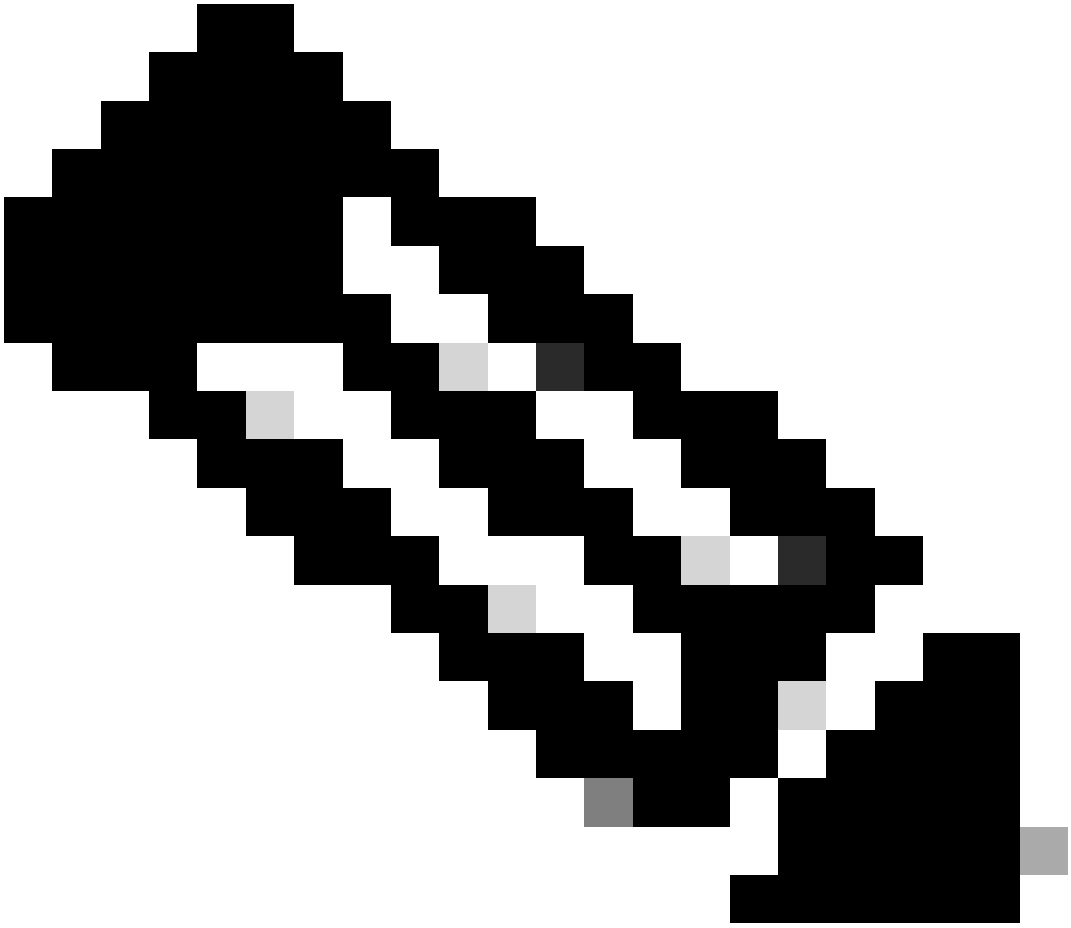
إعدادات إضافية لإنشاء التنبيه



إعدادات إضافية لإنشاء التنبيه



إعدادات إضافية لإنشاء التنبيه



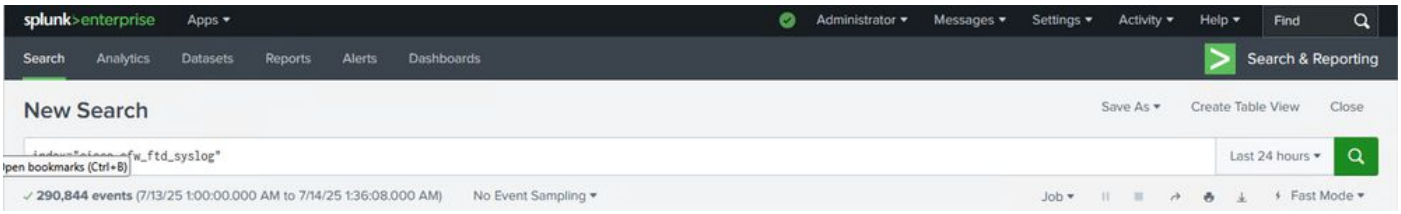
ملاحظة: إذا كنت تريد تشغيل التنبيهات لكل نتيجة، فيجب عليك تحديد إعدادات التحكم وفقا لذلك أيضا.

التحقق من الصحة

بمجرد إنشاء لوحات البيانات والتنبيهات، يمكنك التحقق من التكوينات وتدفق البيانات ولوحات المعلومات والتنبيهات في الوقت الفعلي باستخدام التعليمات الواردة في هذا القسم.

عرض السجلات

يمكنك إستخدام تطبيق البحث لتأكيد ما إذا كانت السجلات التي تم إرسالها بواسطة جدار الحماية قد تم تلقيها وقابليتها للرؤية على رأس بحث جزء كبير من الكتلة. يمكن التحقق من هذا الإجراء من خلال التحقق من أحدث السجلات المفهرسة (فهرس البحث = "cisco_sfw_ftd_syslog") وطابع الوقت المرتبط به.

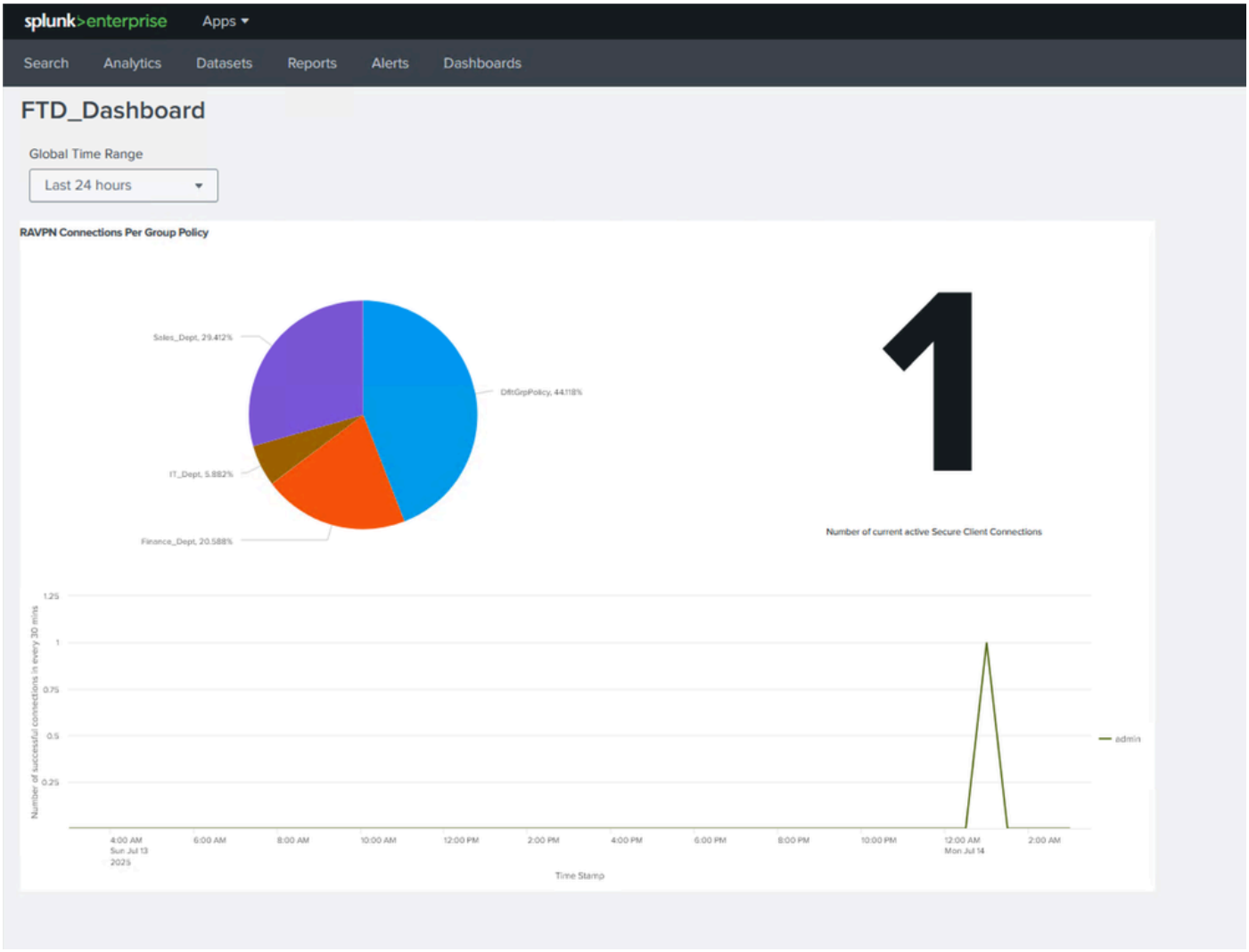


فحص السجلات وعرضها

فحص السجلات وعرضها

عرض لوحات المعلومات في الوقت الفعلي

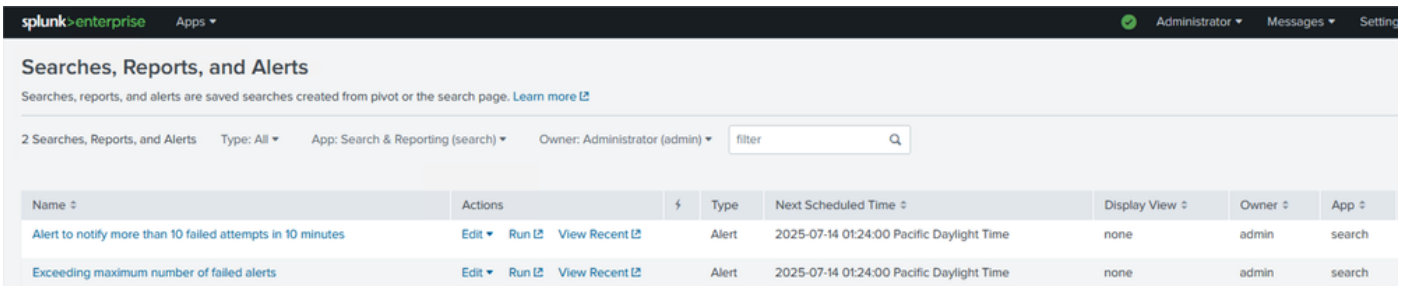
يمكنك الانتقال إلى لوحة المعلومات المخصصة التي قمت بإنشائها ورؤية التغييرات على كل من اللوحات كبيانات وسجلات جديدة يتم إنشاؤها من FTD.



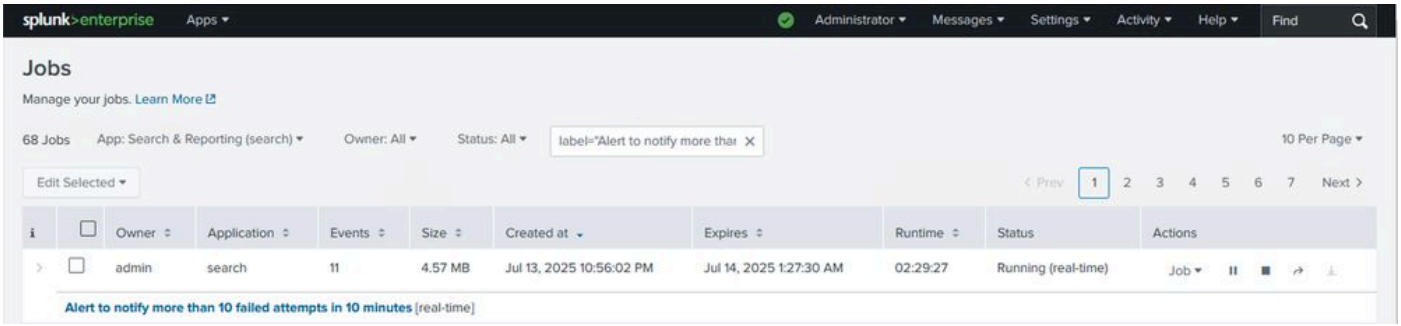
عرض لوحات المعلومات

التحقق من تشغيل أية تنبيهات

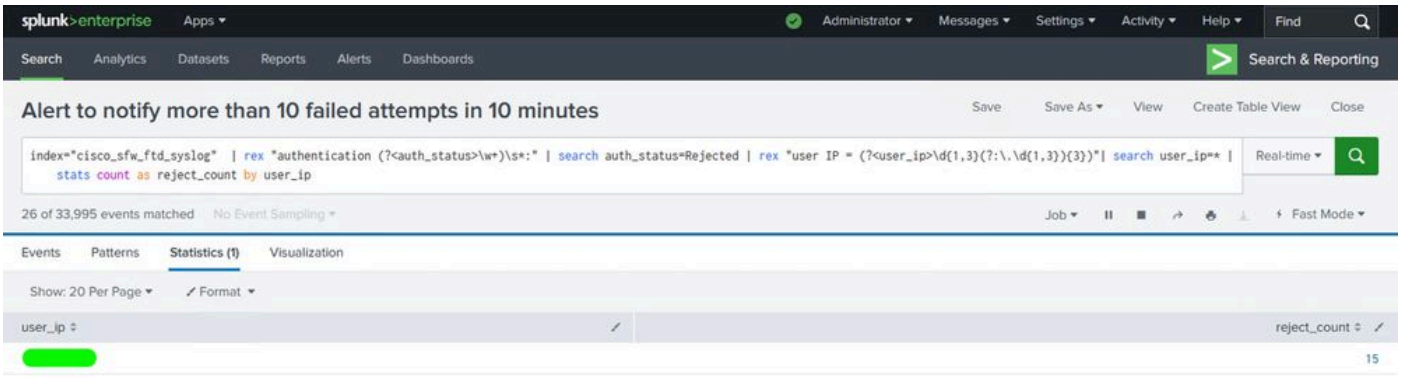
للتحقق من المعلومات حول التنبيهات، يمكنك الانتقال إلى عمليات بحث المقطع والتقارير والتنبيهات للاطلاع على معلومات التنبيه الأخيرة. انقر فوق عرض الأحدث للتحقق أكثر من المهام وعمليات البحث.



التحقق من التنبيهات وعرضها



التحقق من التنبيهات وعرضها



التحقق من الإحصائيات للتنبيه الذي تم تشغيله

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).