Creación de paneles y alertas personalizados en Splunk mediante registros del sistema desde FTD

Contenido

Introducción

Este documento describe un tutorial paso a paso para configurar FTD para enviar registros del sistema a Splunk y utilizar esos registros para crear paneles y alertas personalizados.

Prerequisites

Requirements

Cisco recomienda que conozca estos temas antes de seguir esta guía de configuración:

- Syslog
- Conocimiento básico del lenguaje de procesamiento de búsquedas (SPL) de Splunk

En este documento también se supone que ya tiene una instancia de Splunk Enterprise instalada en un servidor y que tiene acceso a la interfaz web.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Firepower Threat Defense (FTD), versión 7.2.4
- Cisco Firepower Management Center (FMC), versión 7.2.4
- Instancia de Splunk Enterprise (versión 9.4.3) que se ejecuta en un equipo con Windows

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada).

Antecedentes

Los dispositivos Cisco FTD generan registros detallados del sistema que abarcan los eventos de intrusión, las políticas de control de acceso, los eventos de conexión y mucho más. La integración de estos registros con Splunk permite un análisis eficaz y alertas en tiempo real para las operaciones de seguridad de la red.

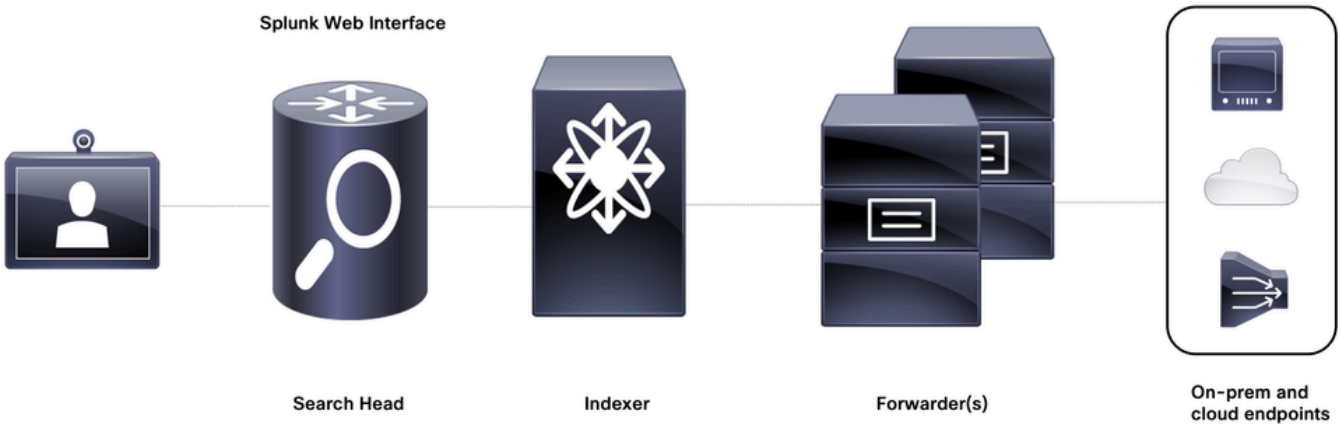
Splunk es una plataforma de análisis de datos en tiempo real diseñada para ingerir, indexar, buscar y visualizar datos generados por máquinas. Splunk es especialmente eficaz en entornos de ciberseguridad como una herramienta de gestión de eventos de seguridad (SIEM) gracias a su capacidad para:

- Ingesta de datos de registro a escala
- Realizar búsquedas complejas con SPL
- Crear paneles y alertas
- Integrarse con la orquestación de seguridad y los sistemas de respuesta ante incidentes

Splunk procesa los datos a través de una canalización estructurada para que los datos de máquinas no estructurados o semiestructurados sean útiles y procesables. Las etapas clave de esta canalización a menudo se denominan IPIS que significa:

- Entrada
- Análisis
- Indexación
- Búsqueda

Los principales componentes generales de la arquitectura subyacente que se utilizan para realizar la canalización IPIS se muestran en este diagrama:



Disminuir la arquitectura subyacente

Configurar

Diagrama de la red

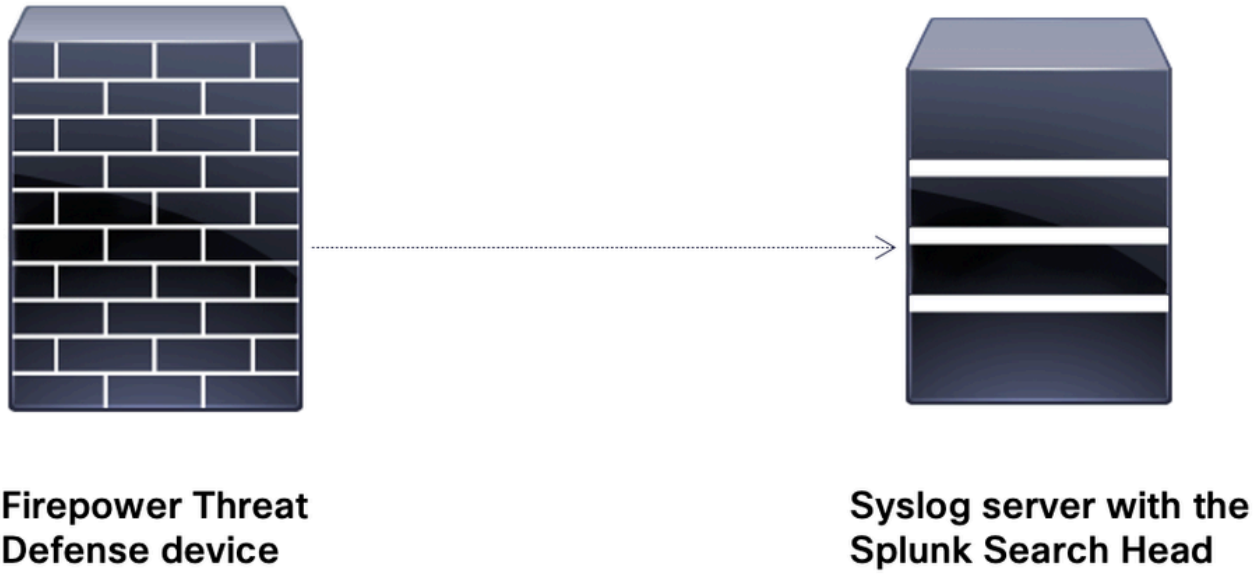
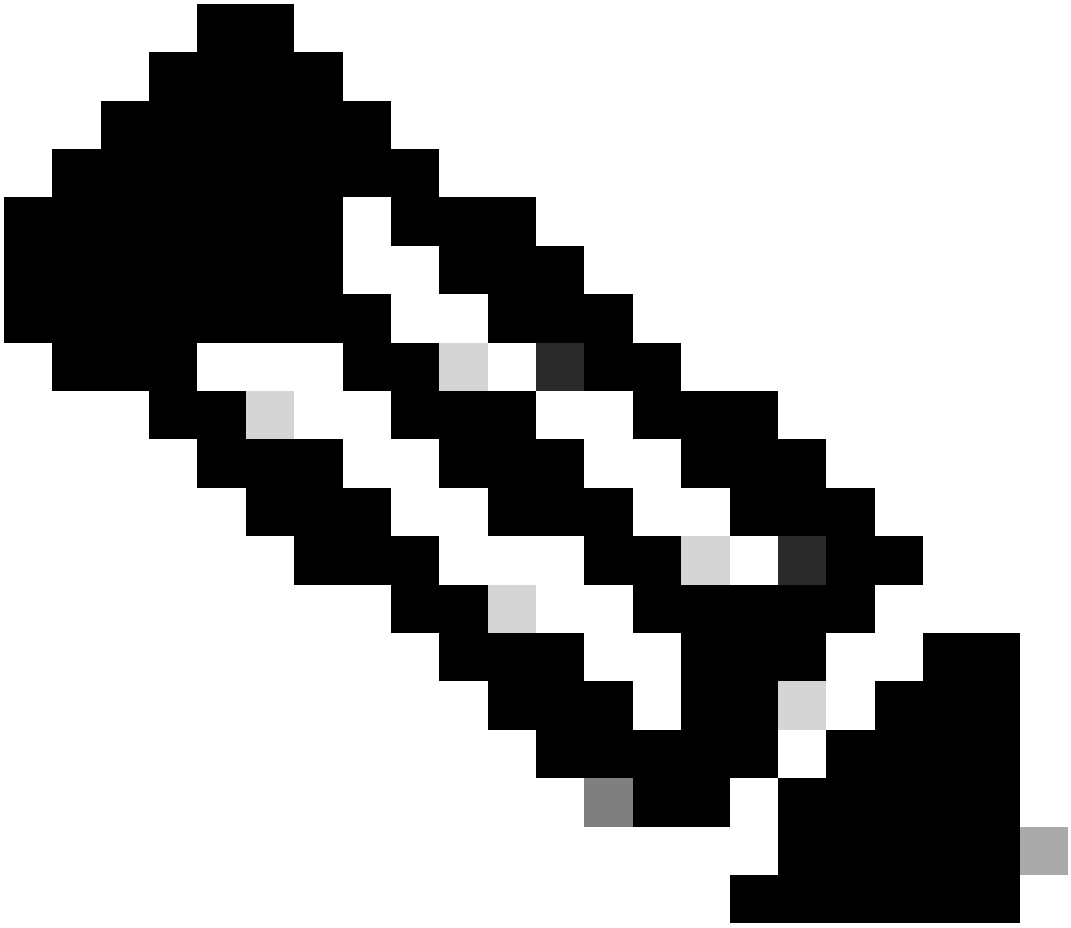


Diagrama de la red

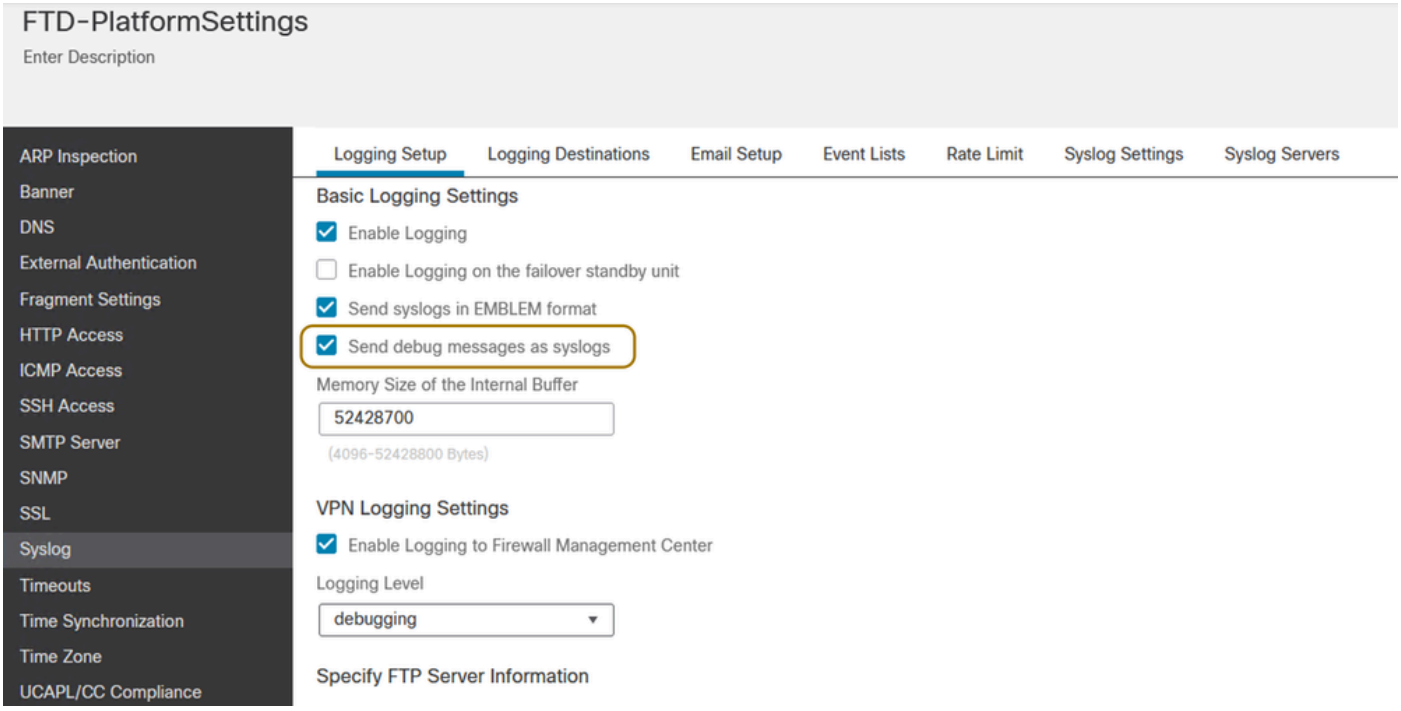


Nota: El entorno de laboratorio para este documento no requiere instancias independientes de reenviador e indizador. El equipo de Windows, es decir, el servidor syslog en el que está instalada la instancia de Splunk Enterprise actúa como indizador y encabezado de búsqueda.

Configuraciones

Configuración de Syslog para el FTD

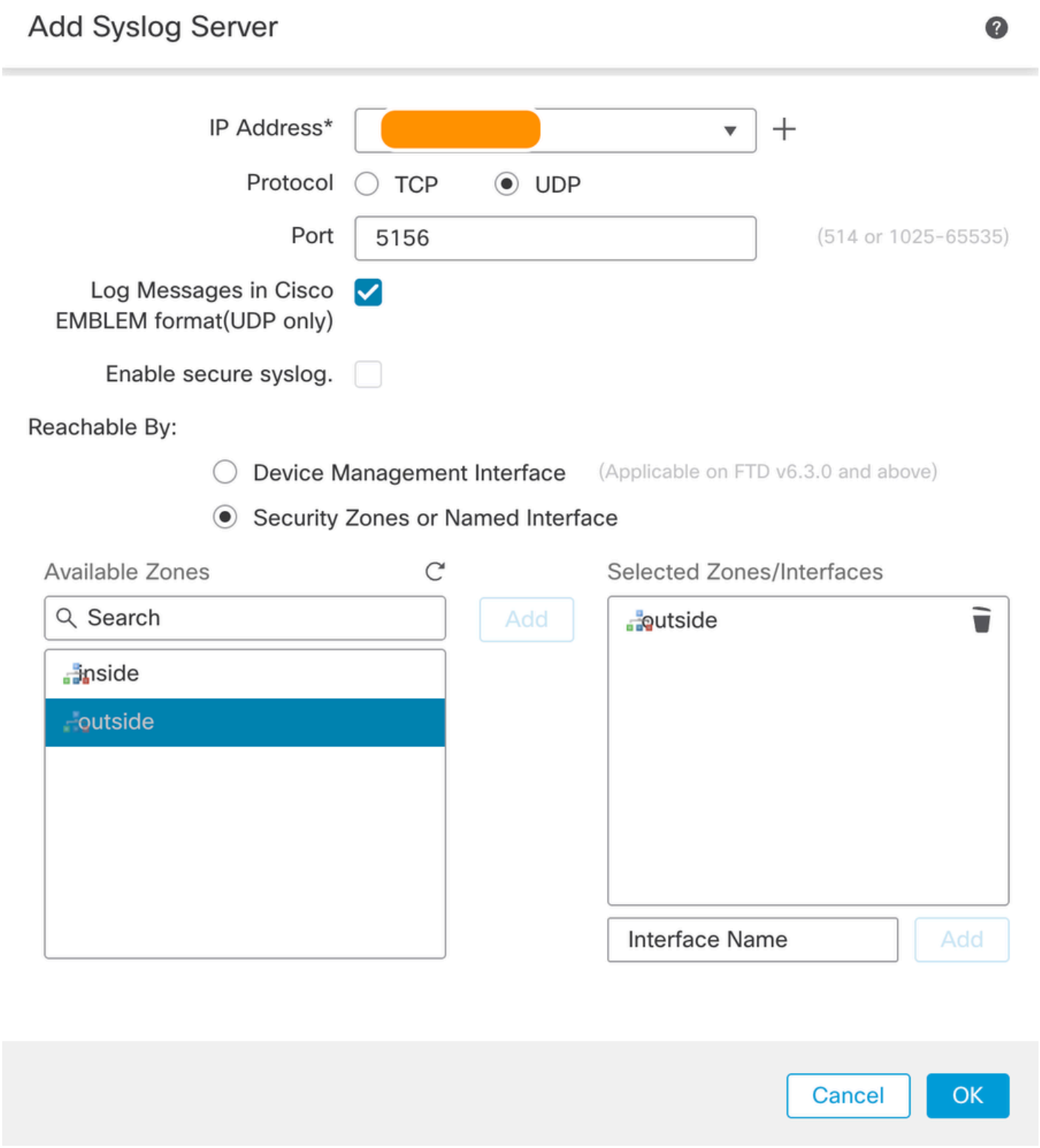
Paso 1. Configure los ajustes preliminares de syslog en FMC para el FTD bajo Devices > Platform Settings para enviar los registros al servidor syslog en el que se está ejecutando la instancia de Splunk.



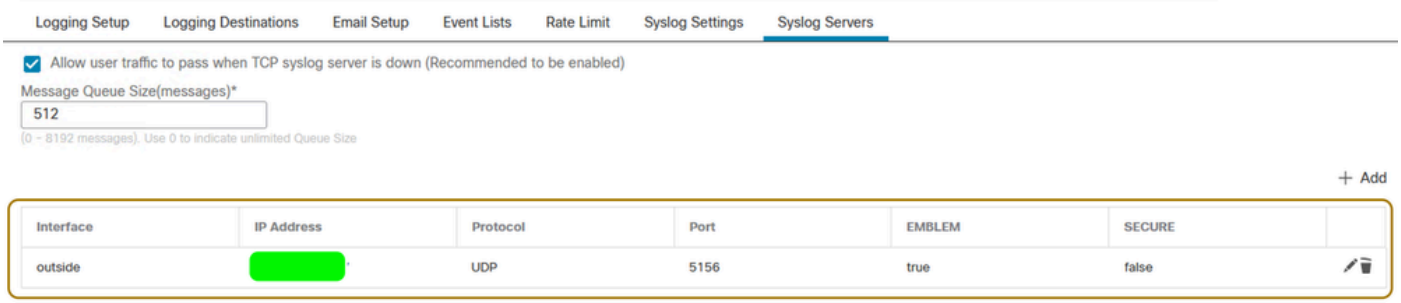
Configuración de la plataforma en FTD - Syslog

Paso 2. Configure la dirección IP de la máquina en la que está instalada la instancia de Splunk Enterprise y se está ejecutando como servidor Syslog. Defina los campos como se ha mencionado.

```
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
```

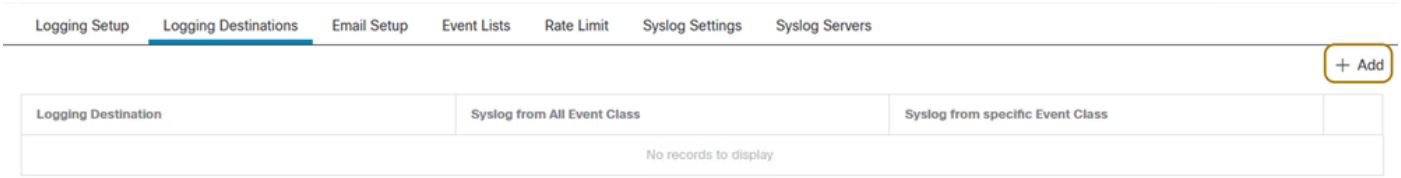


Configuración de la plataforma en FTD - Agregar servidor Syslog

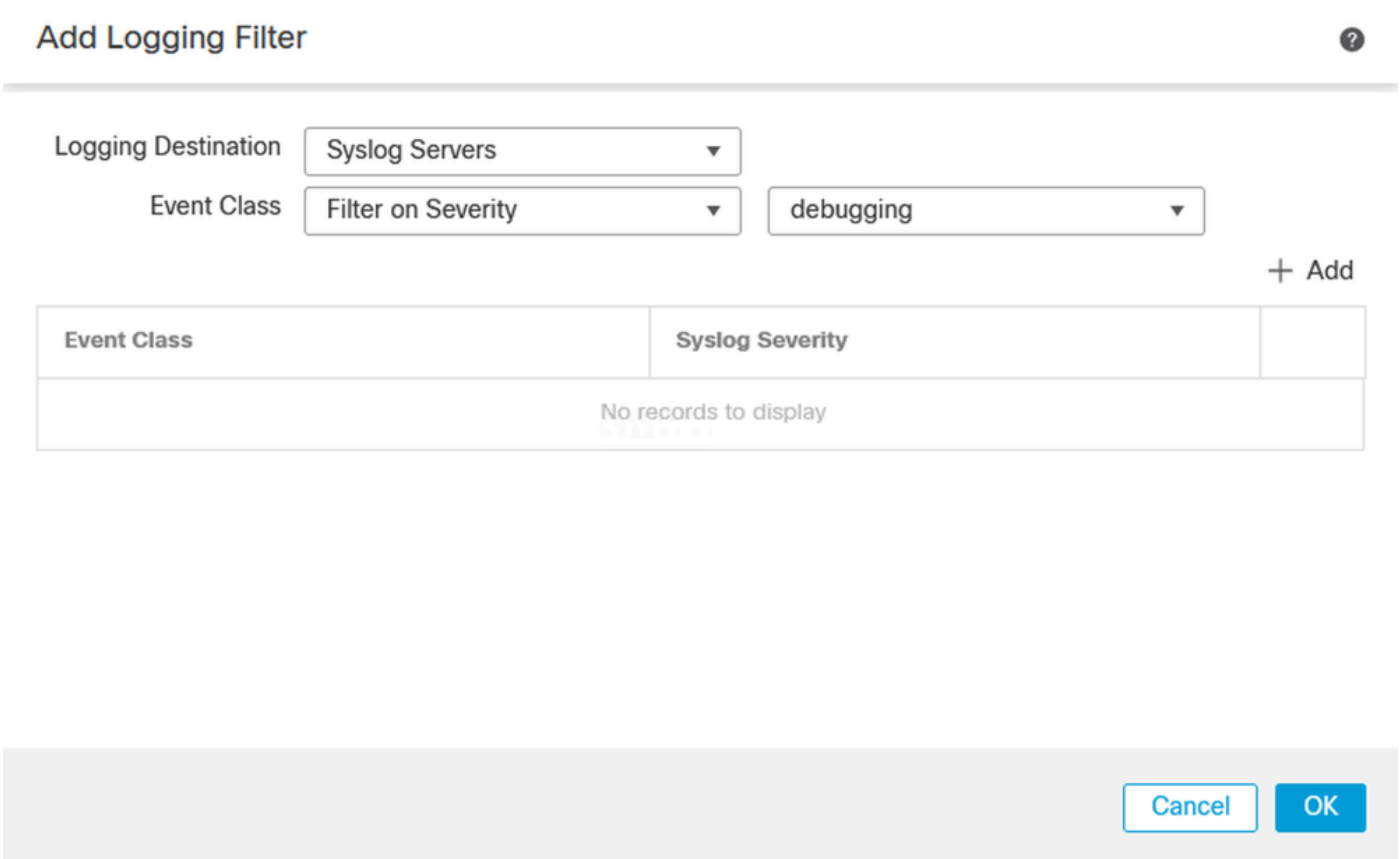


Configuración de la plataforma en FTD - Servidor Syslog agregado

Paso 3. Agregue un destino de registro para los servidores Syslog. El nivel de registro se puede establecer según su elección o caso de uso.



Configuración de la plataforma en FTD - Agregar destino de registro



Configuración de la plataforma en FTD - Establecer el nivel de gravedad para el destino de registro

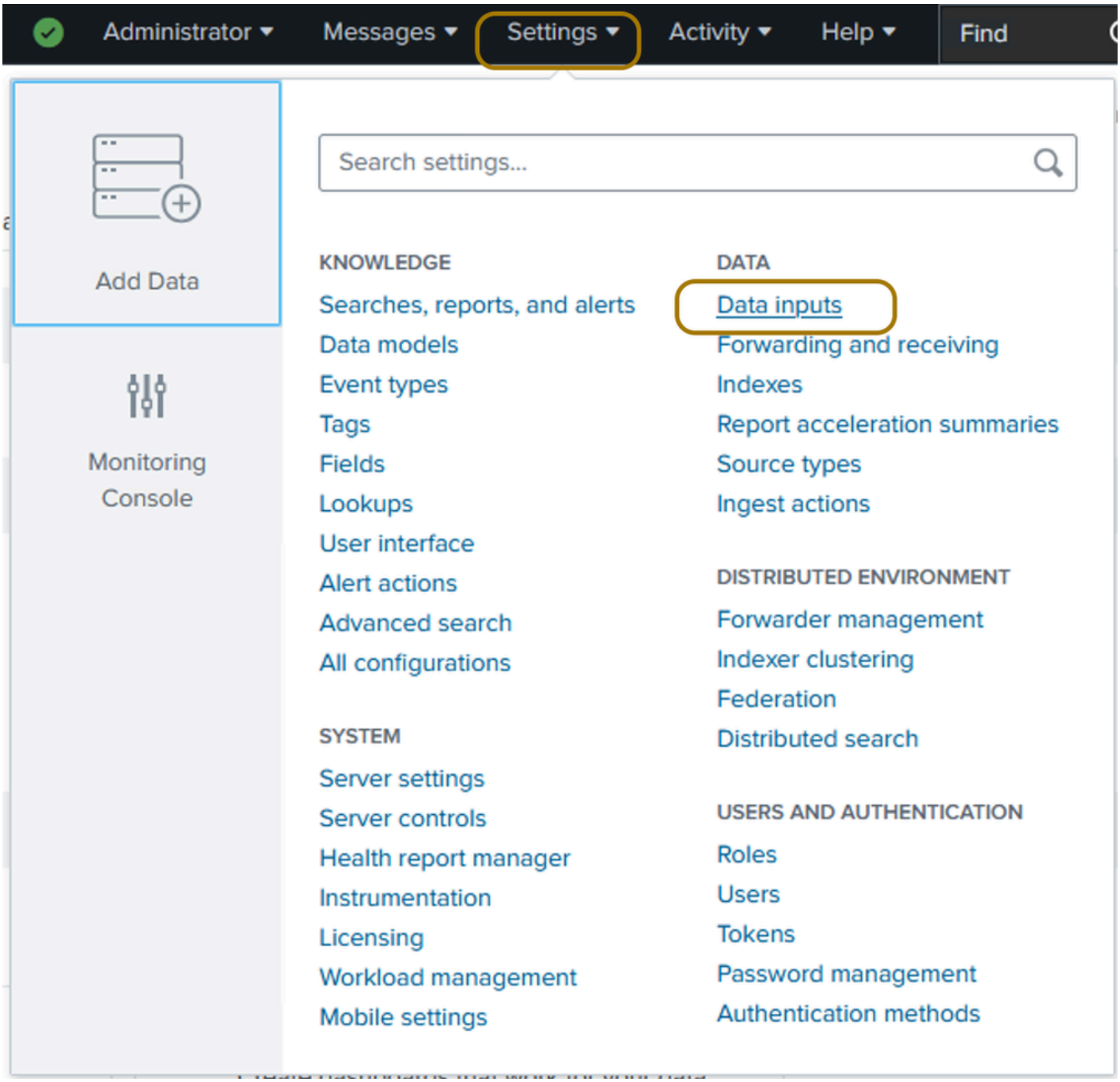
Implemente los cambios de configuración de la plataforma en el FTD después de completar estos pasos.

Configuración de una entrada de datos en la instancia empresarial de Splunk

Paso 1. Inicie sesión en la interfaz web de la instancia de Splunk Enterprise.

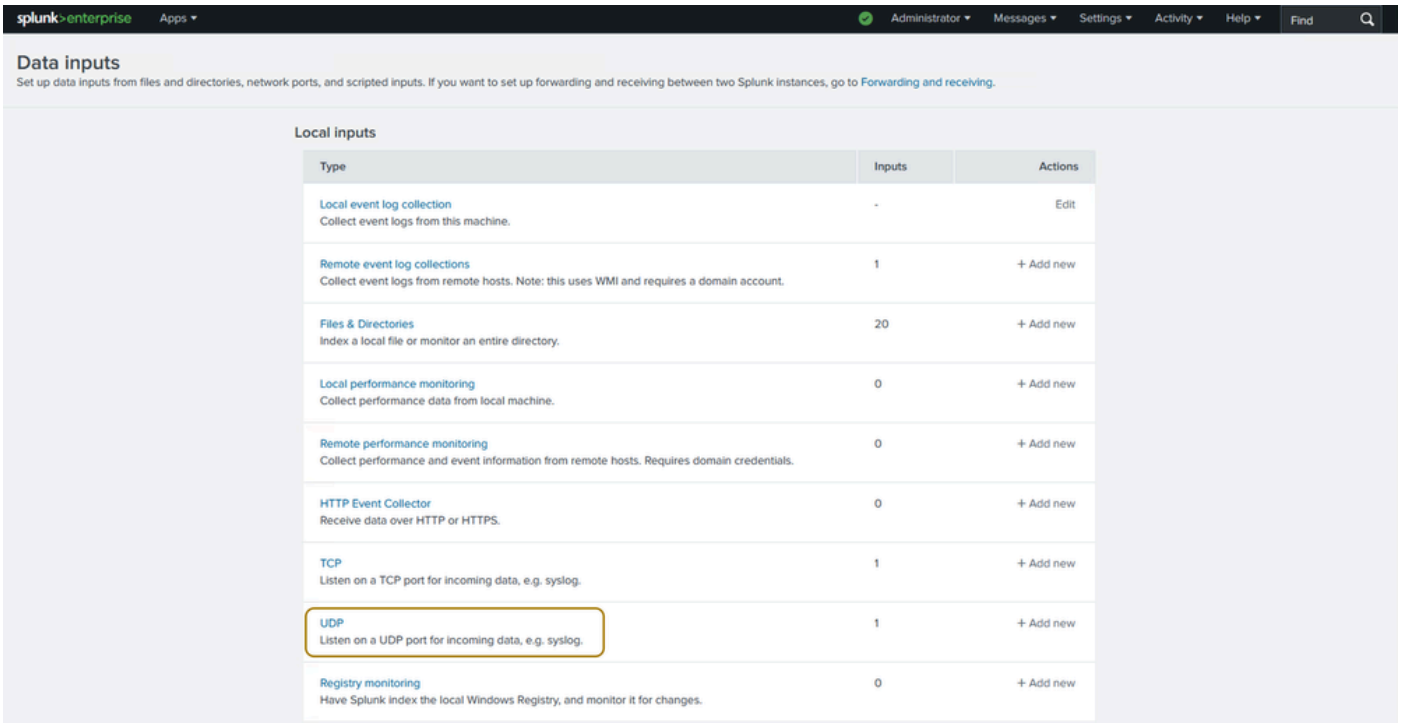
Página de inicio de sesión de Splunk Web Interface

Paso 2. Debe definir una entrada de datos para poder almacenar e indexar los registros del sistema en Splunk. Navegue hasta Configuraciones > Datos > Entradas de datos después de iniciar sesión.

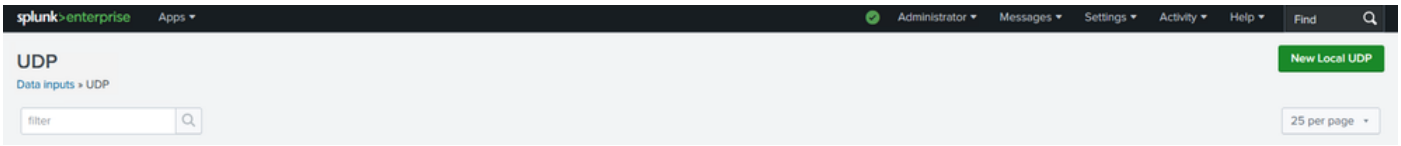


Navegar hasta Entradas de datos en Splunk

Paso 3. Elija UDP y luego haga clic en New Local UDP en la siguiente página que aparece.

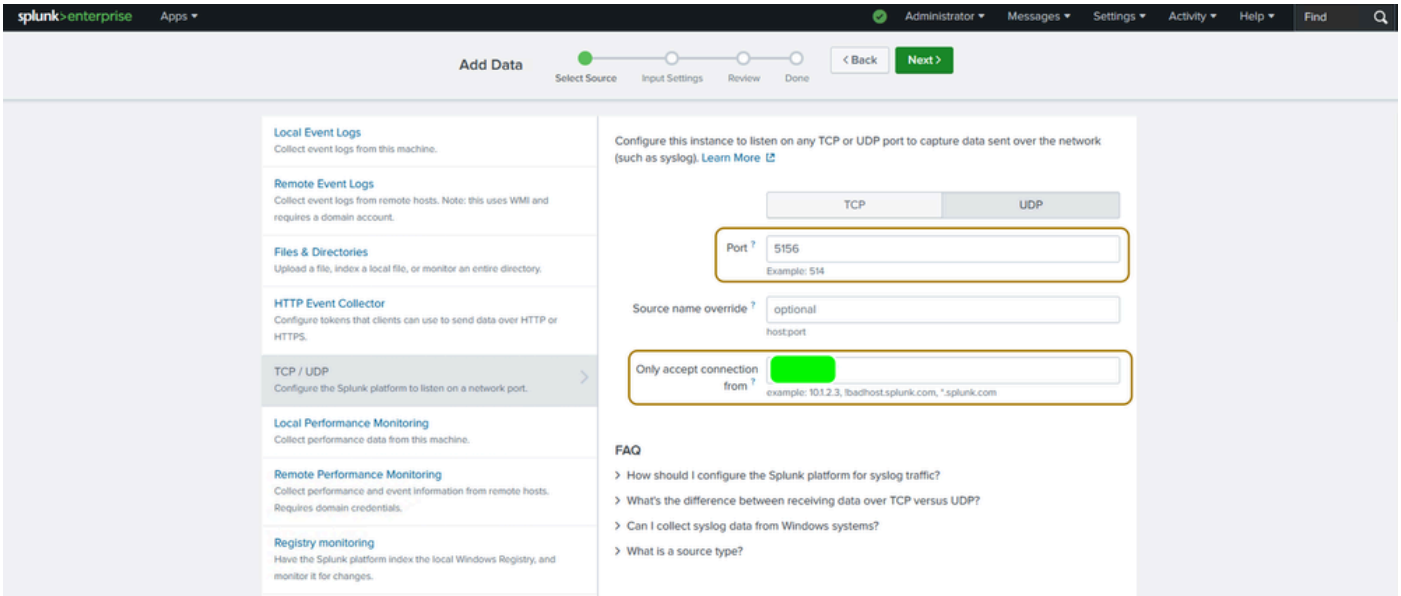


Haga clic en 'UDP' para una entrada de datos UDP



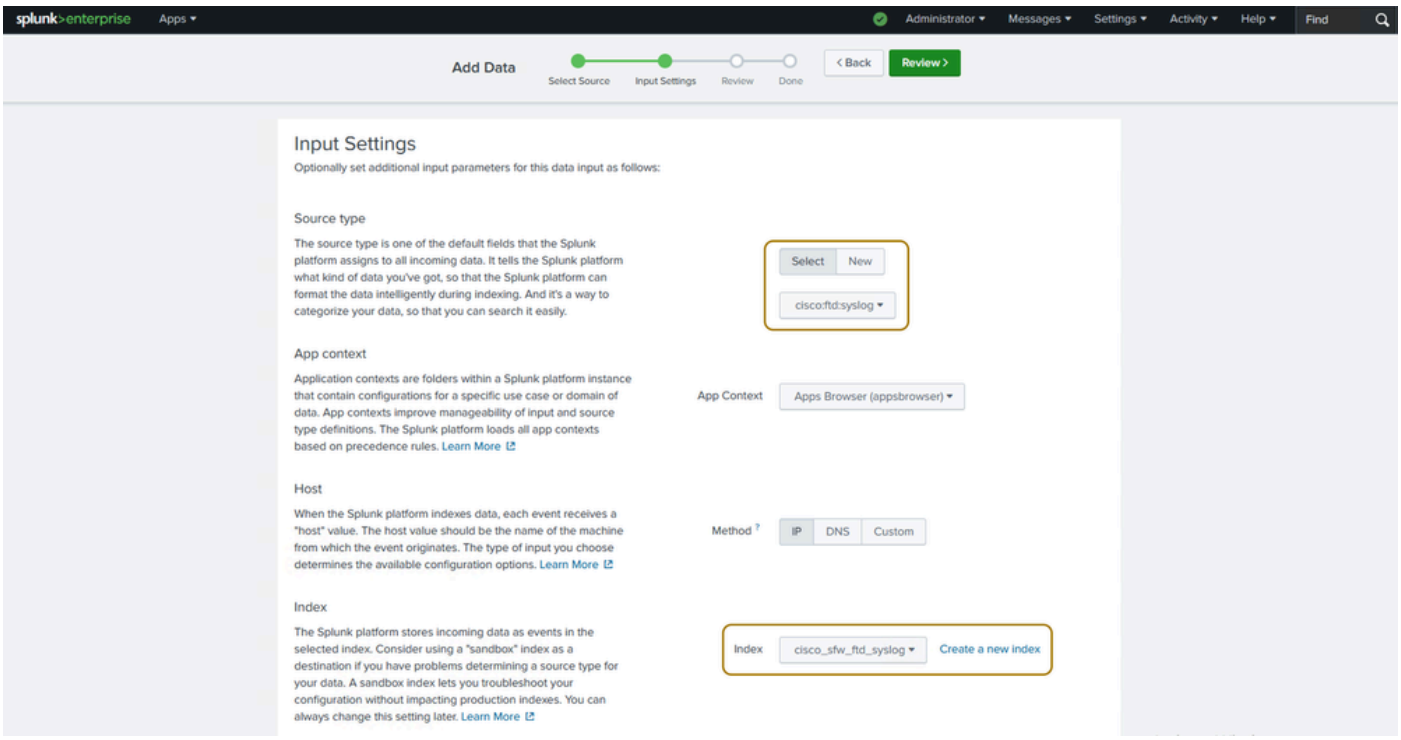
Crear una entrada 'New Local UDP'

Paso 4. Introduzca el puerto en el que se envían los registros del sistema. Debe ser el mismo que el puerto configurado en la configuración de FTD syslog, en este caso 5156. Para aceptar los syslogs solamente de un origen (el FTD), establezca el campo Only Accept Connection From en la IP de la interfaz en el FTD que se comunica con el servidor Splunk. Haga clic en Next (Siguiente).



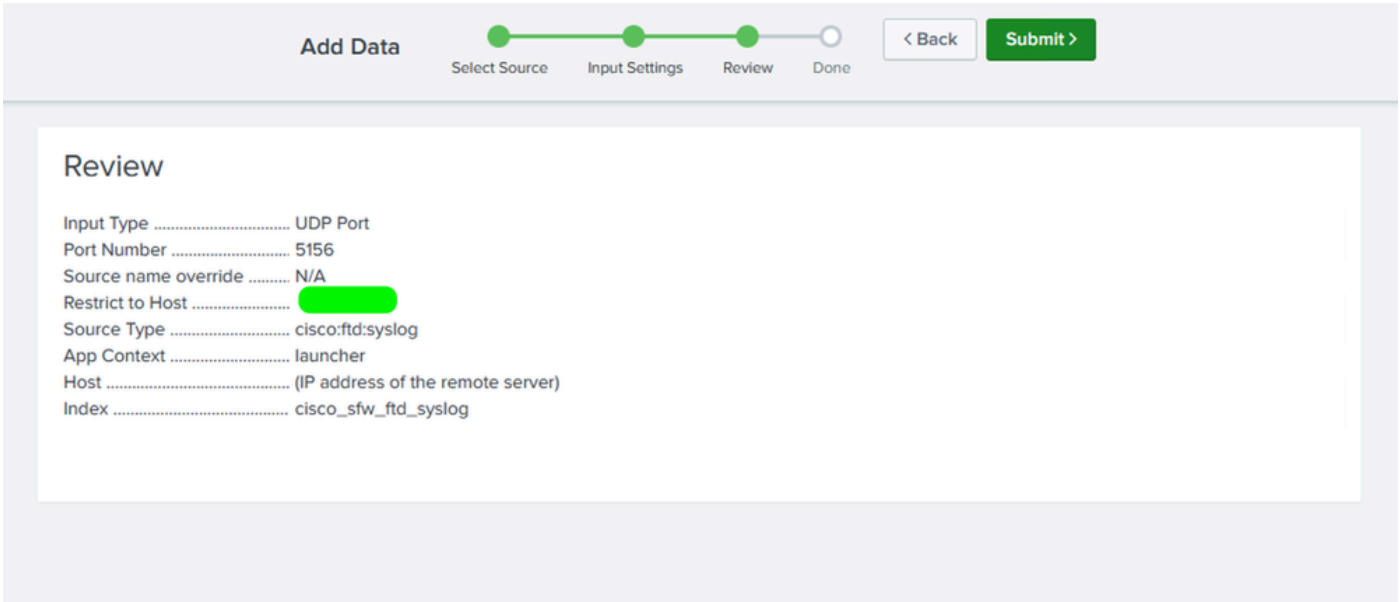
Especificar puerto y dirección IP de FTD

Paso 5. Puede buscar y elegir los valores de los campos tipo de origen e índice de los valores predefinidos en Splunk, como se resalta en la siguiente imagen. La configuración predeterminada se puede utilizar para los campos restantes.



Configurar los parámetros de entrada de datos

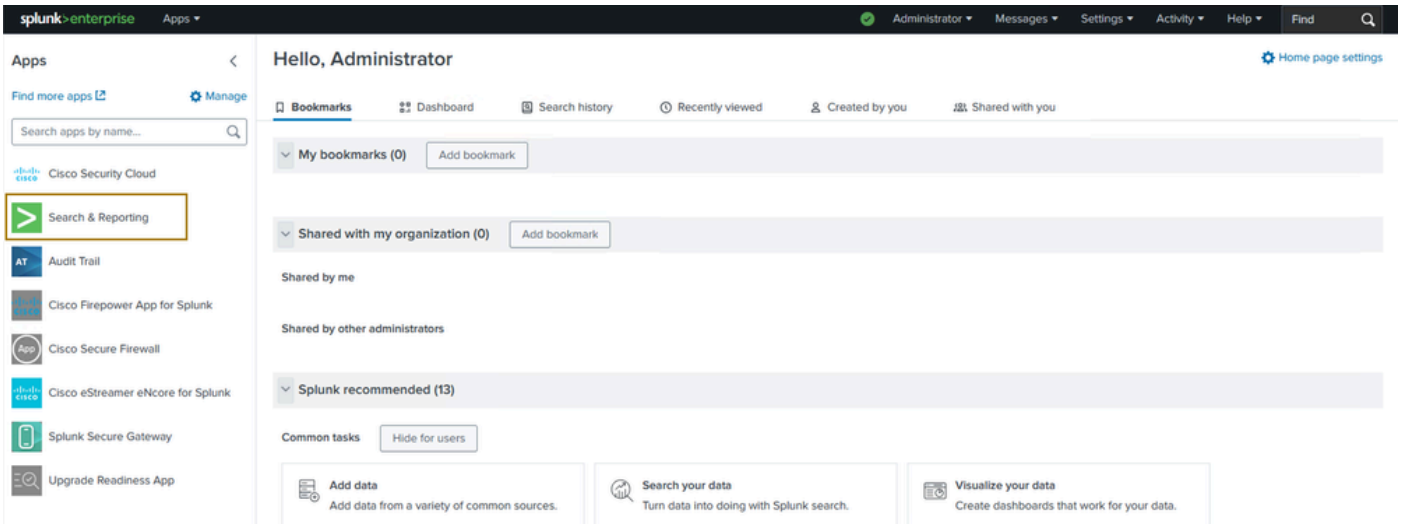
Paso 6. Revise la configuración y haga clic en Enviar.



Revisar configuración de entrada de datos

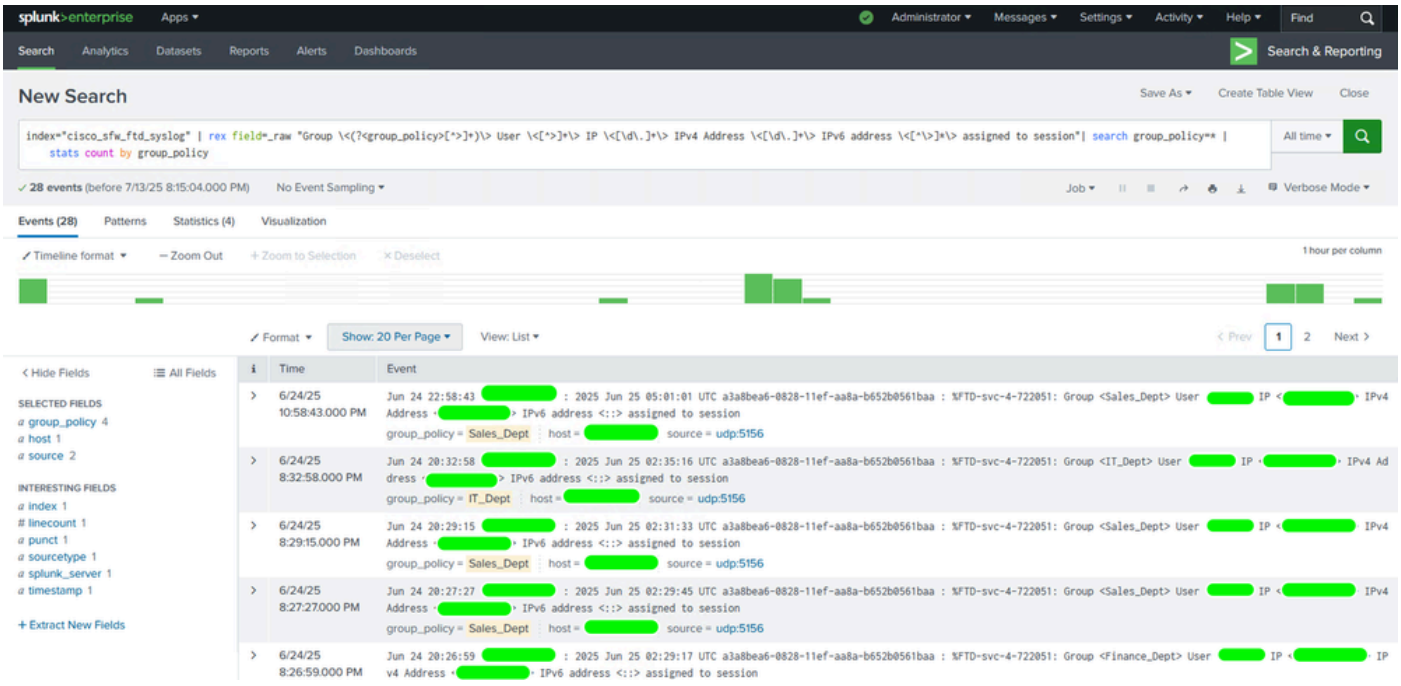
Ejecutar consultas SPL y crear paneles

Paso 1. Navegue hasta la aplicación de búsqueda e informes en Splunk.

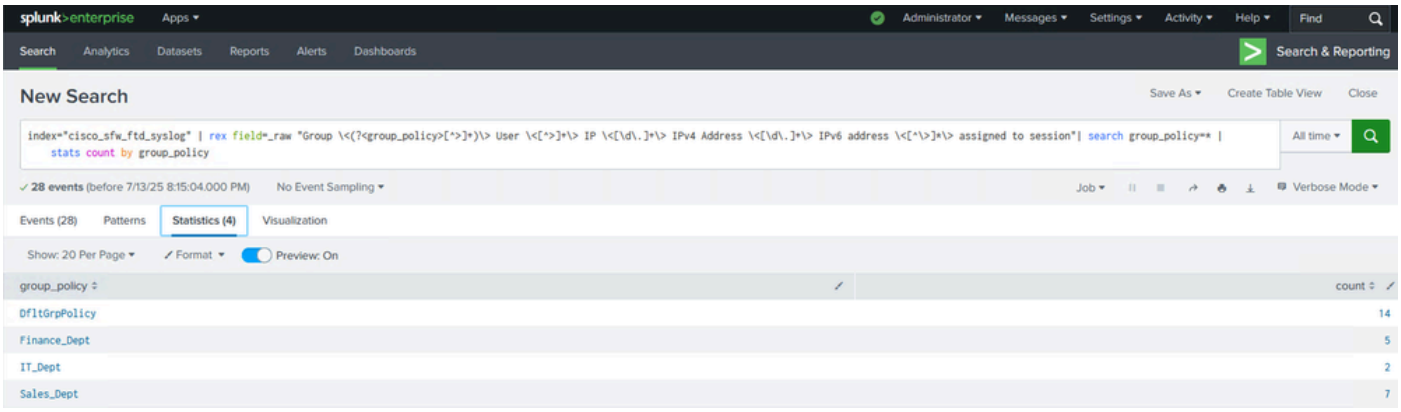


Vaya a la aplicación Buscar y generar informes

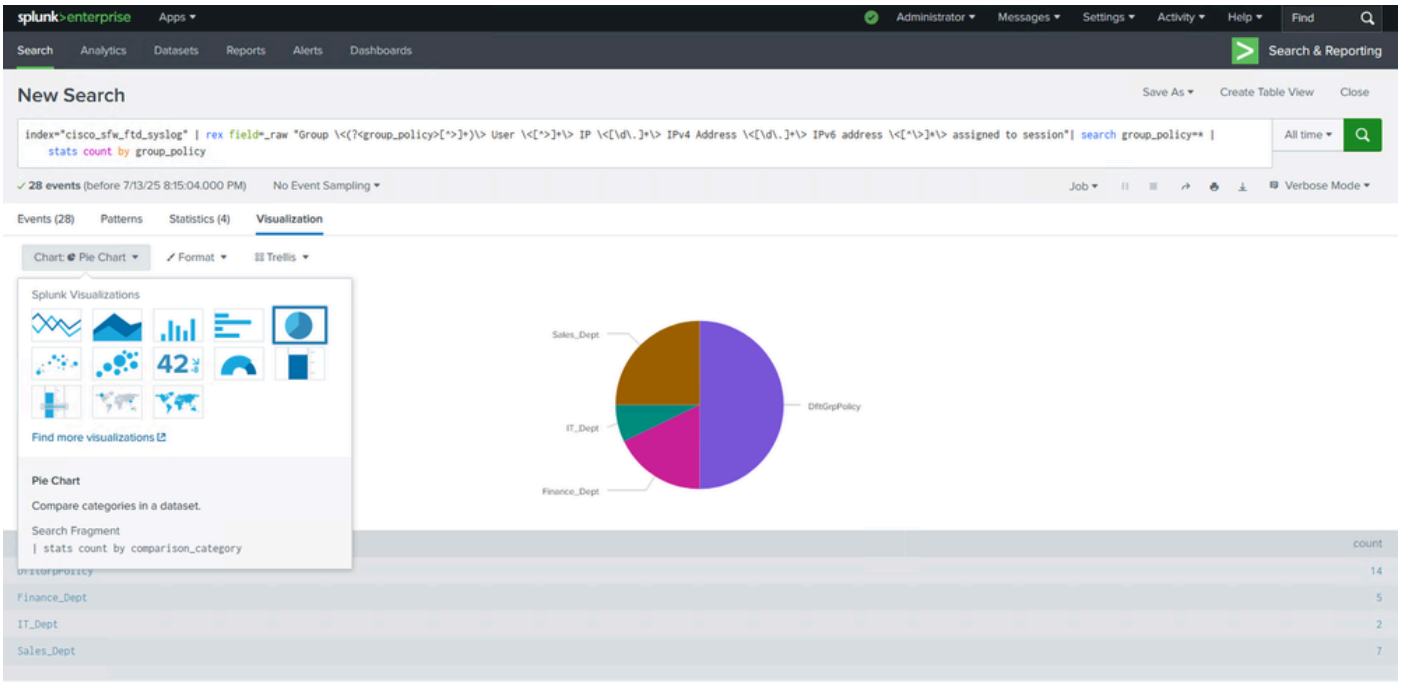
Paso 2. Formular y ejecutar una consulta SPL según los datos que desee visualizar. Podrá ver cada registro por completo (en el modo detallado) en la pestaña Eventos, el recuento de conexiones por política de grupo en la pestaña Estadísticas y visualizar estos datos usando estas estadísticas en la pestaña Visualización.



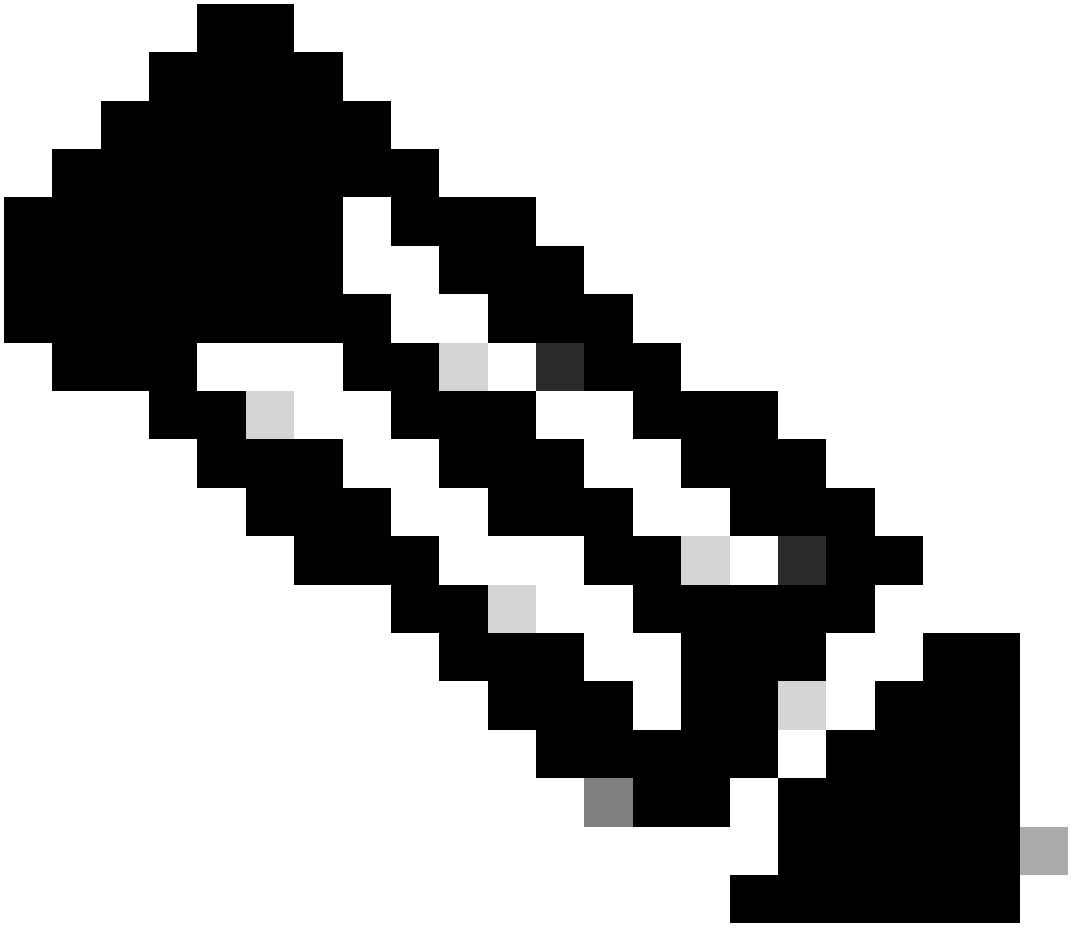
Buscar eventos mediante consultas SPL



Seleccione la ficha Estadísticas.

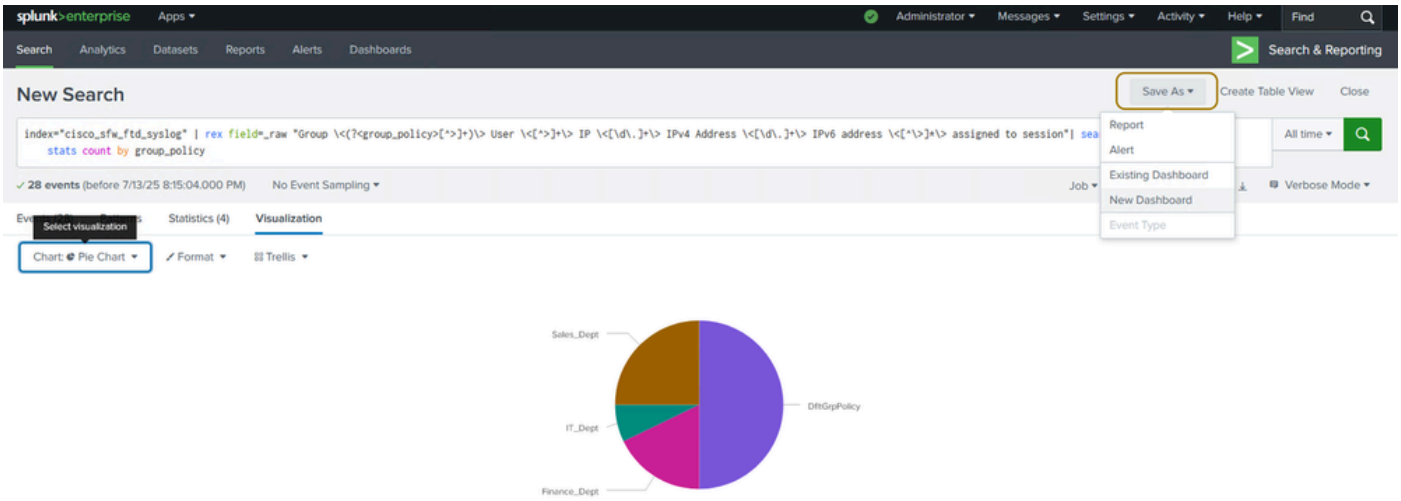


La ficha Visualización mostrará el gráfico/gráfico



Nota: En este ejemplo, la consulta está obteniendo registros de conexiones VPN de acceso remoto correctas entre diferentes políticas de grupo. Se ha utilizado un gráfico circular para visualizar el número y porcentaje de conexiones exitosas por política de grupo. En función de sus requisitos y preferencias, puede optar por utilizar un tipo de visualización diferente, como un gráfico de barras.

Paso 3. Haga clic en Guardar como y elija Nuevo o existente panel dependiendo de si ya tiene un panel al que desea agregar este panel o desea crear uno nuevo. En este ejemplo se muestra el último.



Guardar el panel en un panel

Paso 4. Asigne un título al panel que está creando y proporcione un título para el panel que contendrá el gráfico circular.

Save Panel to New Dashboard

Dashboard Title: FTD_Dashboard

ftd_dashboard — Edit ID

Description: Optional

Permissions: Private

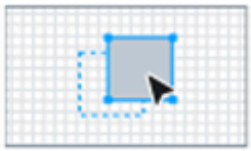
How do you want to build your dashboard? What's this?

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

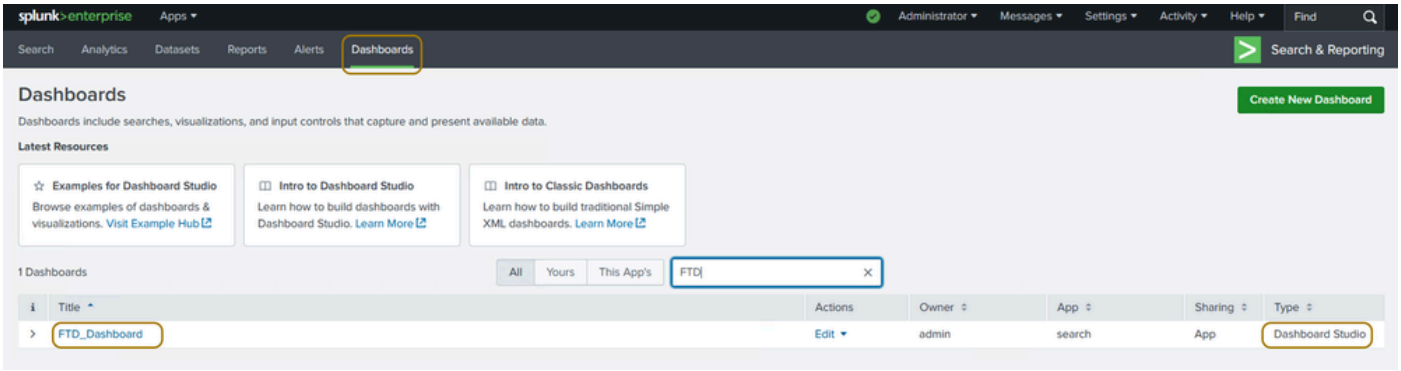
Cancel | Save to Dashboard

Configuración del nuevo panel

Puede establecer los permisos en Privado o Compartido en la aplicación en función de si solo se supone que debe ver el panel o si también están permitidos otros usuarios con acceso a la instancia de Splunk. Además, dependiendo de si desea o no un control granular sobre la configuración del panel y el diseño del panel, elija el modo Classic o Dashboard Studio para crear el panel.

Paso 5 (opcional). Ejecute y guarde más consultas SPL como paneles en este panel según sus requisitos utilizando los pasos mencionados anteriormente.

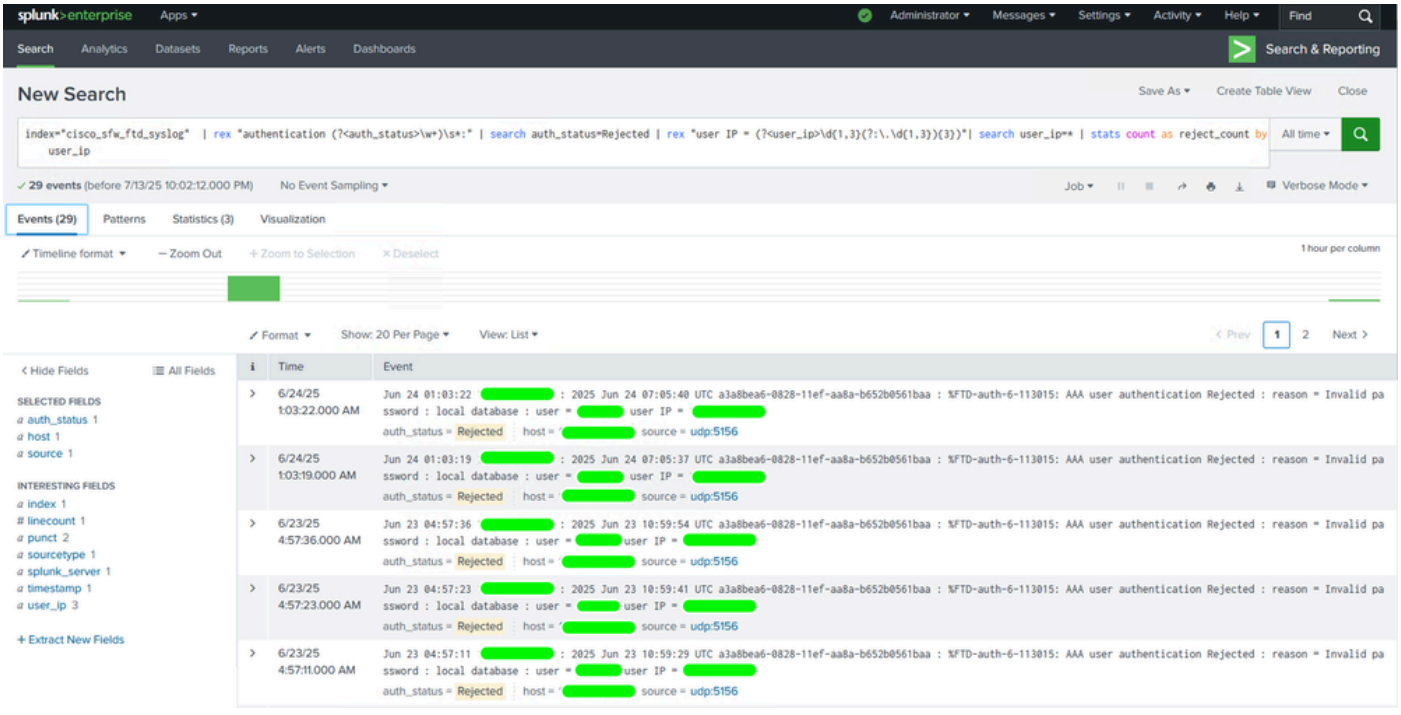
Paso 6. Navegue hasta la pestaña Panel para buscar y elegir el panel que ha creado. Haga clic en él para ver, editar o reorganizar sus paneles.

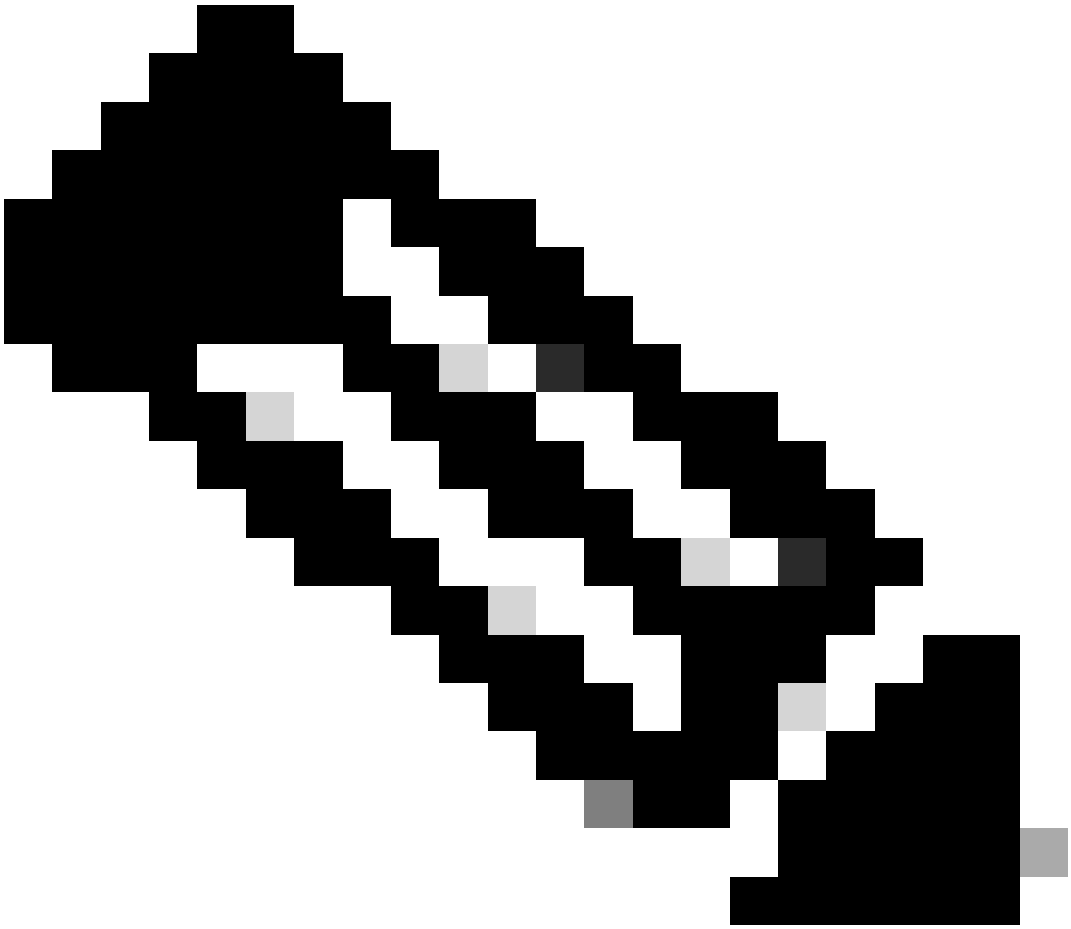


Visualización del panel

Configurar alertas basadas en consultas SPL

Paso 1. Navegue hasta la aplicación de búsqueda e informes para construir y ejecutar su consulta SPL para verificar que está obteniendo los registros correctos que se utilizarán para activar la alerta.





Nota: En este ejemplo, la consulta se utiliza para obtener registros de autenticación erróneos para VPN de acceso remoto para activar alertas cuando el número de intentos fallidos excede un determinado umbral en una determinada cantidad de tiempo.

Paso 3. Haga clic en Guardar como y elija Alerta.

Guardar la alerta

Paso 4. Dé un título para nombrar la alerta. Rellene todos los demás detalles y parámetros

necesarios para configurar la alerta y haga clic en Guardar. La configuración utilizada para esta alerta se ha mencionado aquí.

<#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

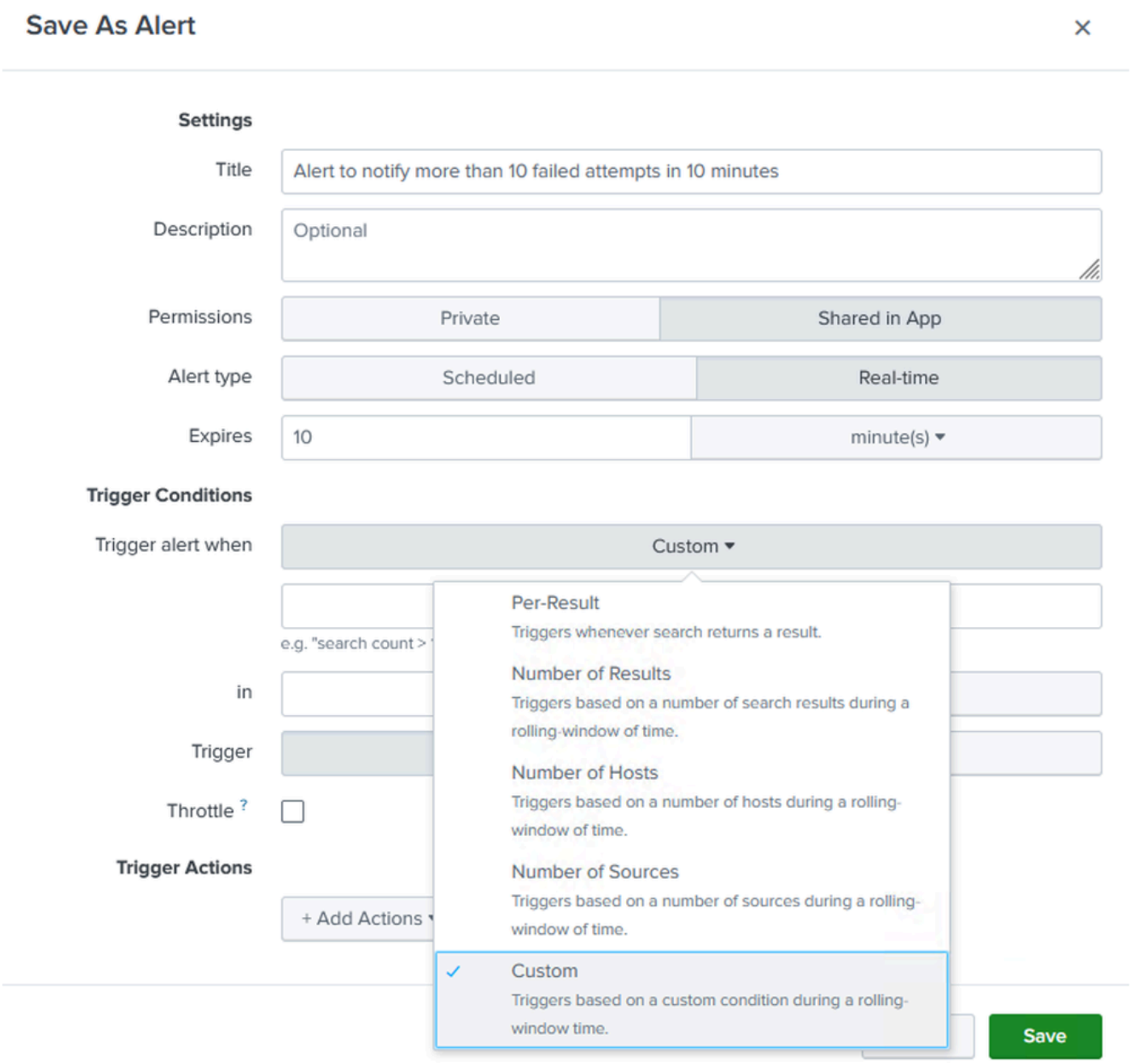
condition is used to search if the

reject_count

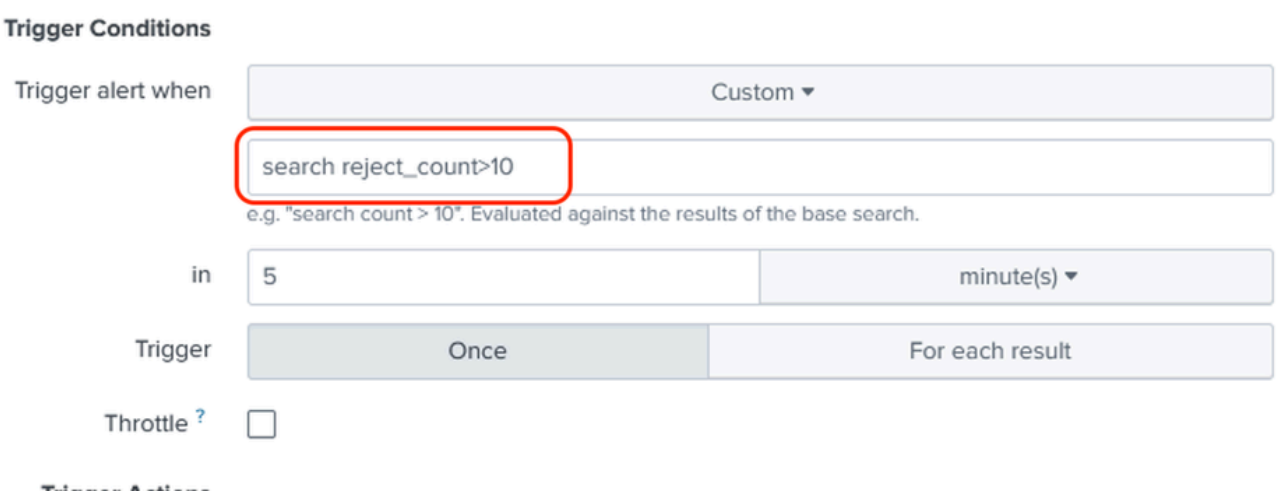
counter from the SPL query has exceeded 10 in the last 5 minutes for any IP address.
Trigger Actions: Set a trigger action such as

Add to Triggered Alerts, Send email, etc.

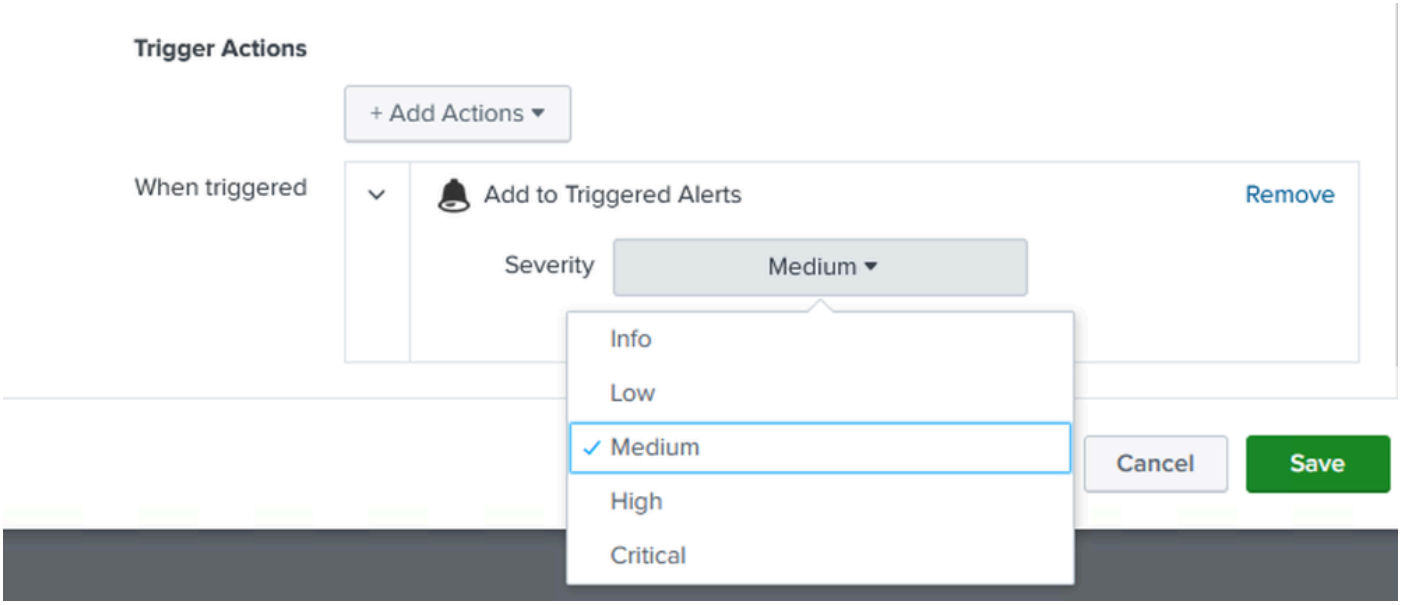
and set the alert severity as per your requirement.



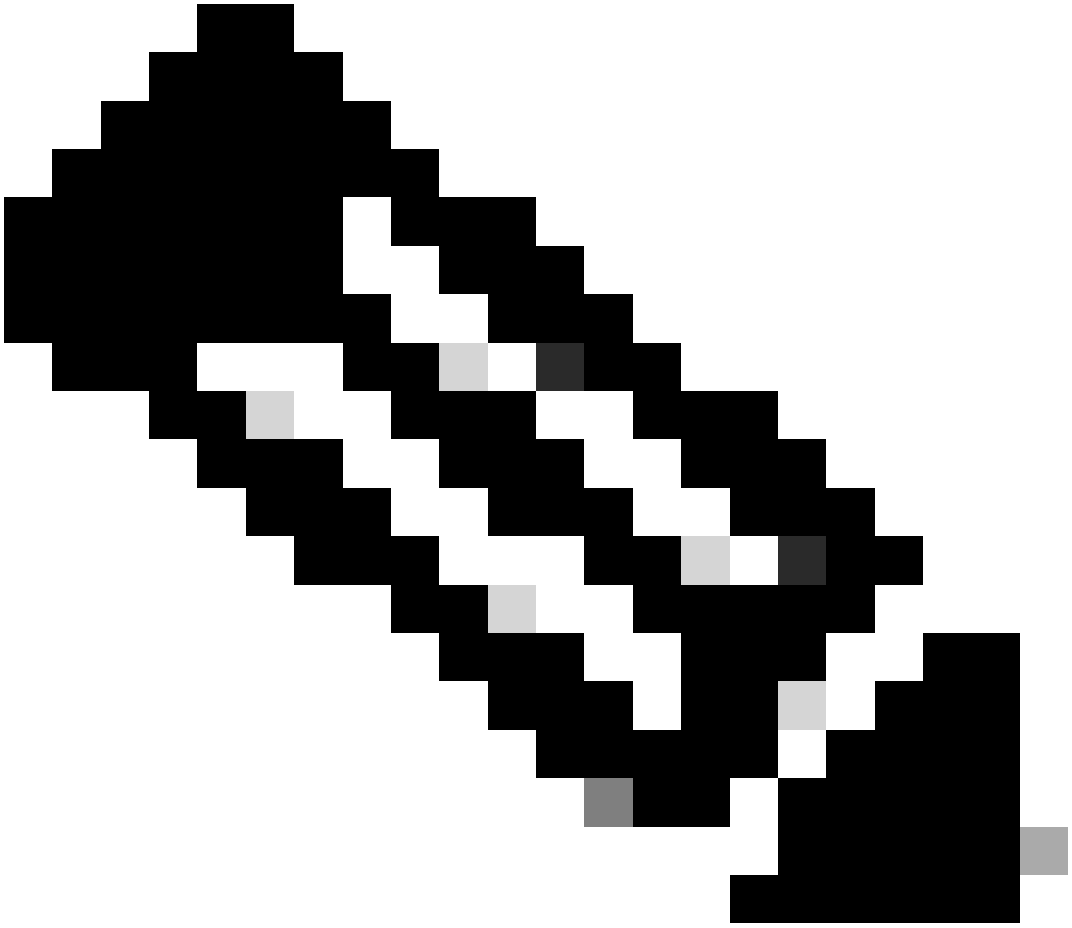
Configuración adicional para la creación de alertas



Configuración adicional para la creación de alertas



Configuración adicional para la creación de alertas



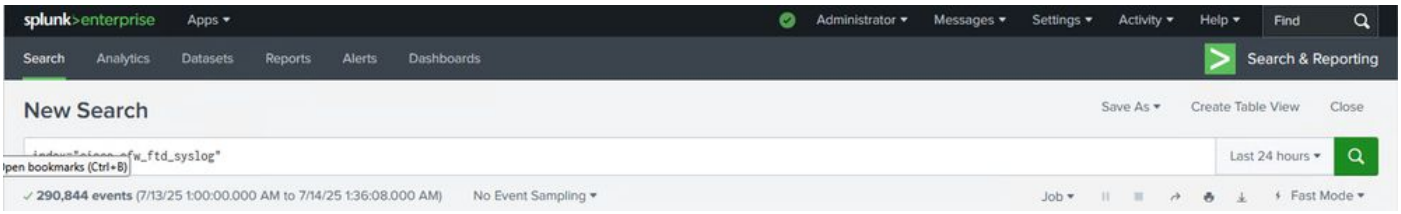
Nota: Si desea activar las alertas para cada resultado, también tendrá que definir la configuración de aceleración en consecuencia.

Verificación

Una vez creados los paneles y las alertas, puede verificar las configuraciones, el flujo de datos, los paneles y las alertas en tiempo real mediante las instrucciones proporcionadas en esta sección.

Ver registros

Puede utilizar la aplicación de búsqueda para confirmar si los registros enviados por el firewall son recibidos y visibles para el encabezado de búsqueda splunk. Esto se puede verificar comprobando los registros más recientes indizados (índice de búsqueda = "cisco_sfw_ftd_syslog") y la marca de tiempo asociada a él.

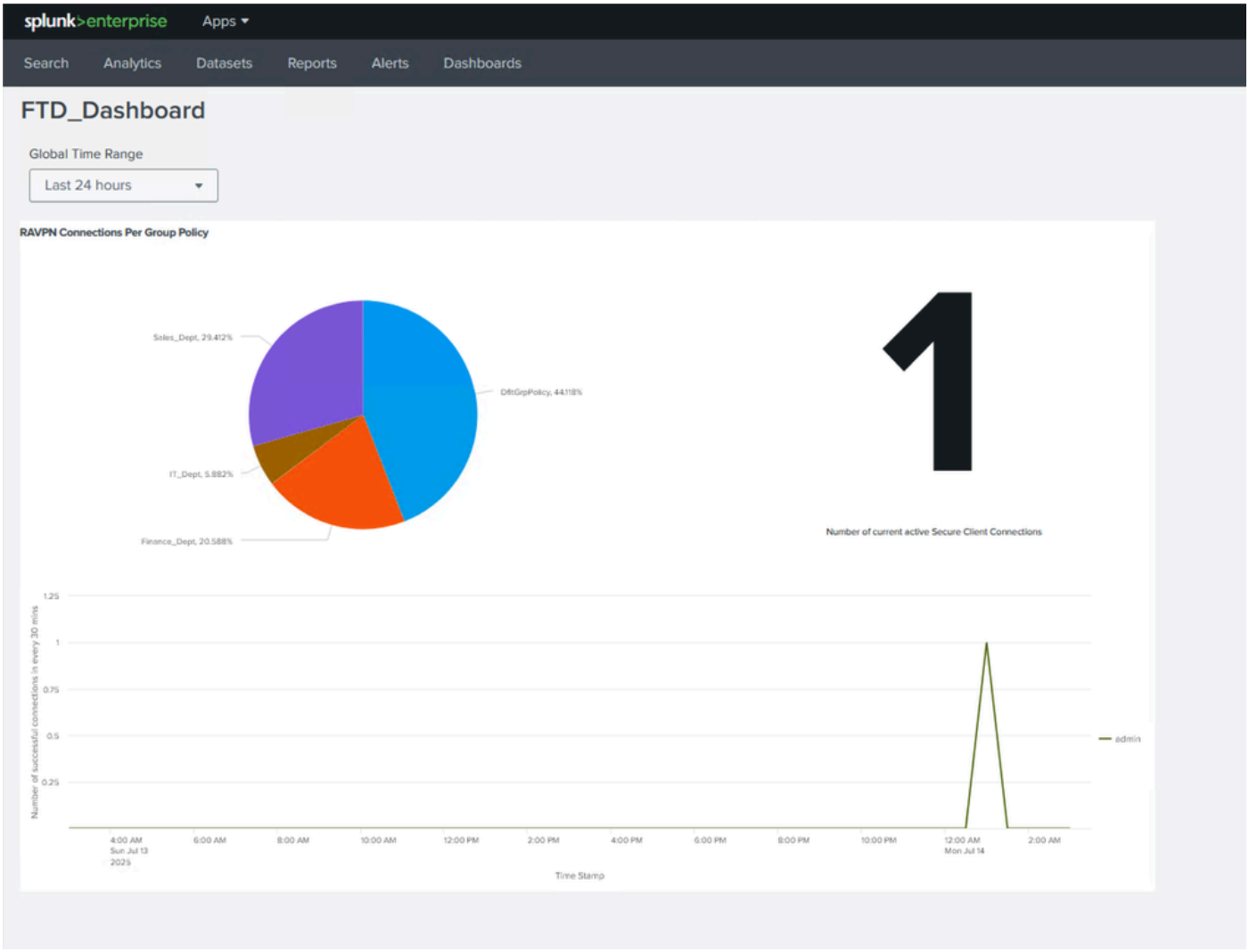


Comprobar y ver registros

Comprobar y ver registros

Ver los paneles en tiempo real

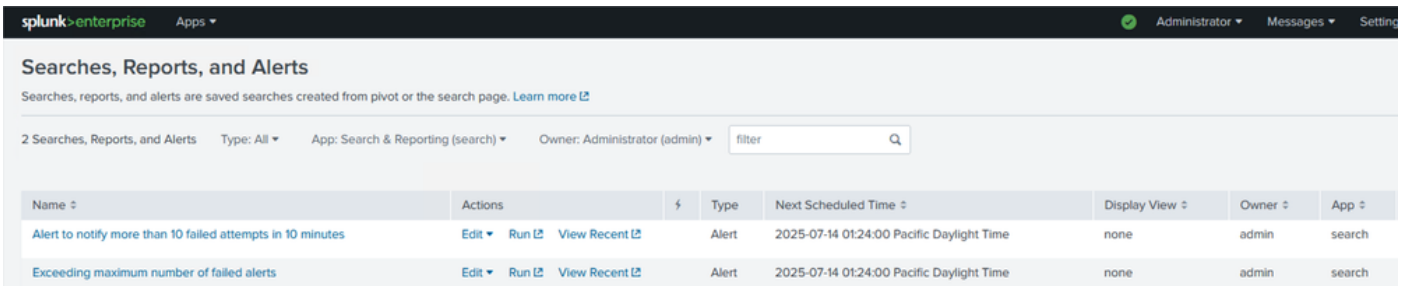
Puede desplazarse al panel personalizado que ha creado y ver el cambio en cada uno de los paneles a medida que se generan nuevos datos y registros a partir del FTD.



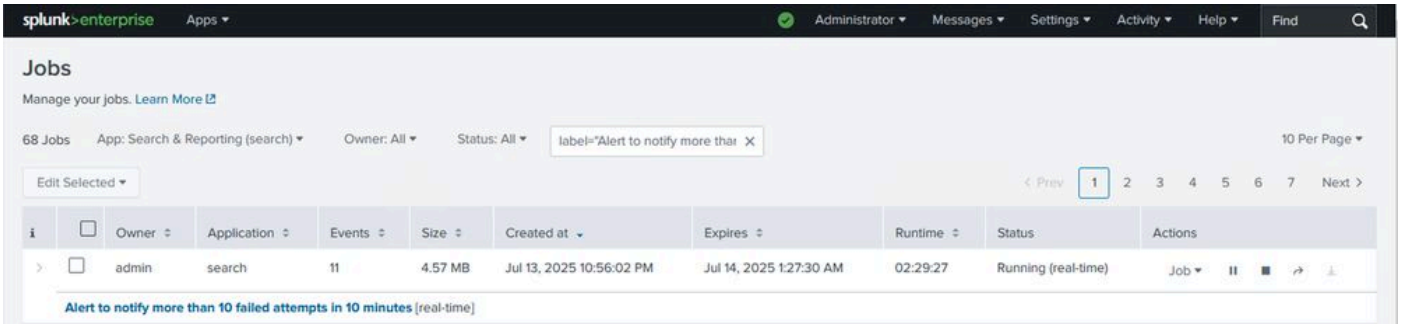
Ver paneles

Comprobar si se ha desencadenado alguna alerta

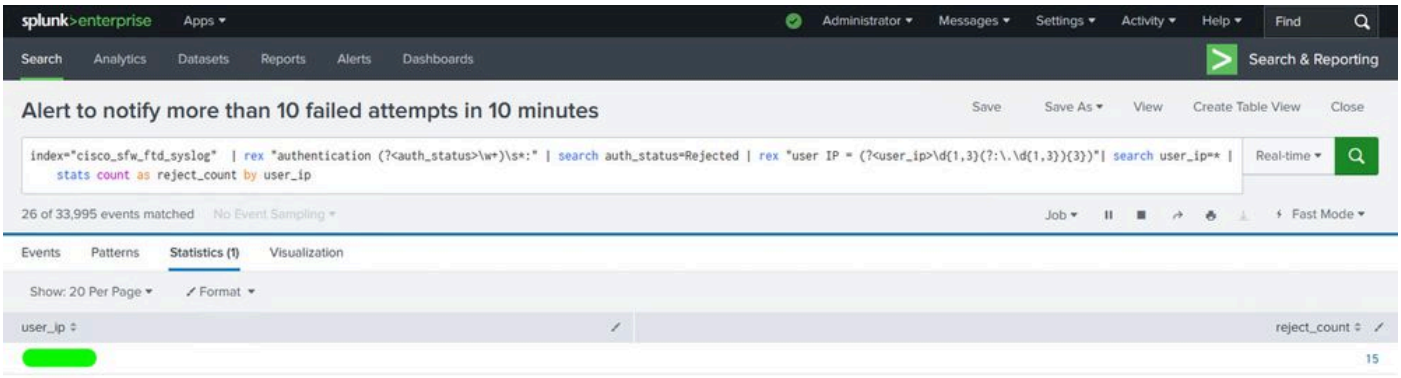
Para verificar la información sobre las alertas, puede navegar a la sección búsquedas, informes y alertas para ver la información de alertas recientes. Haga clic en Ver Reciente para verificar más sobre los trabajos y las búsquedas.



Comprobar y ver alertas



Comprobar y ver alertas



Comprobar estadísticas para alertas desencadenadas

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).