

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

## Contenido

---

### [Introducción](#)

### [Prerequisites](#)

#### [Requirements](#)

#### [Componentes Utilizados](#)

### [Antecedentes](#)

### [Configurar](#)

#### [Diagrama de la red](#)

#### [Configuraciones](#)

##### [Configuración de Syslog para el FTD](#)

##### [Configuración de una entrada de datos en la instancia empresarial de Splunk](#)

##### [Ejecutar consultas SPL y crear paneles](#)

##### [Configurar alertas basadas en consultas SPL](#)

### [Verificación](#)

#### [Ver registros](#)

#### [Ver los paneles en tiempo real](#)

#### [Comprobar si se ha desencadenado alguna alerta](#)

---

## 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.

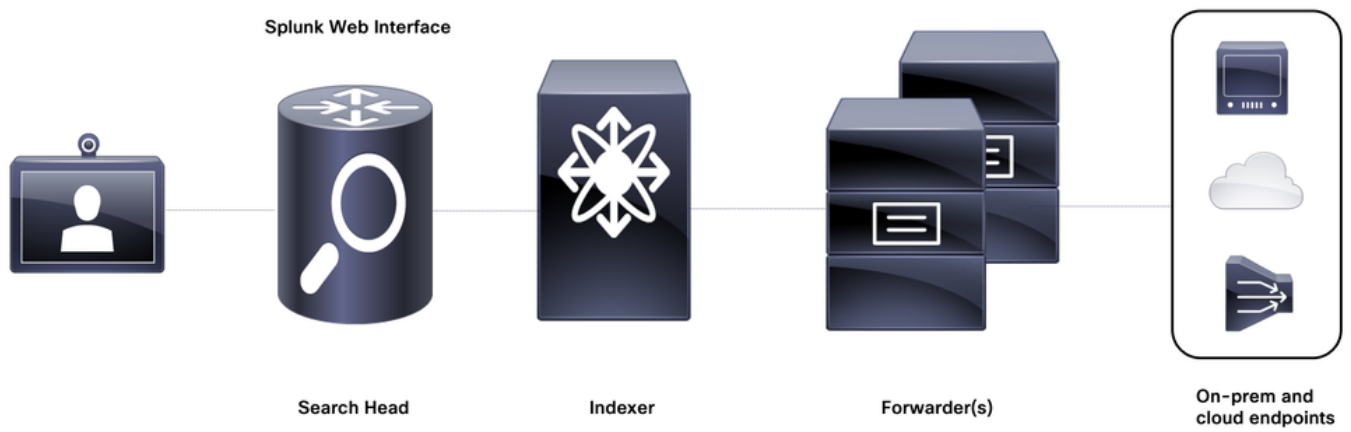
Splunk es una plataforma de análisis de datos en tiempo real diseñada para ingerir, indexar, buscar y visualizar datos generados por máquinas. Splunk es especialmente eficaz en entornos de ciberseguridad como una herramienta de gestión de eventos de seguridad (SIEM) gracias a su capacidad para:

- 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

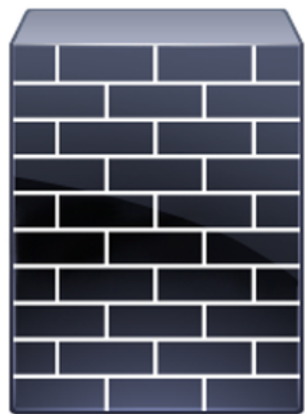
Los principales componentes generales de la arquitectura subyacente que se utilizan para realizar la canalización IPIS se muestran en este diagrama:



Disminuir la arquitectura subyacente

## Configurar

Diagrama de la red

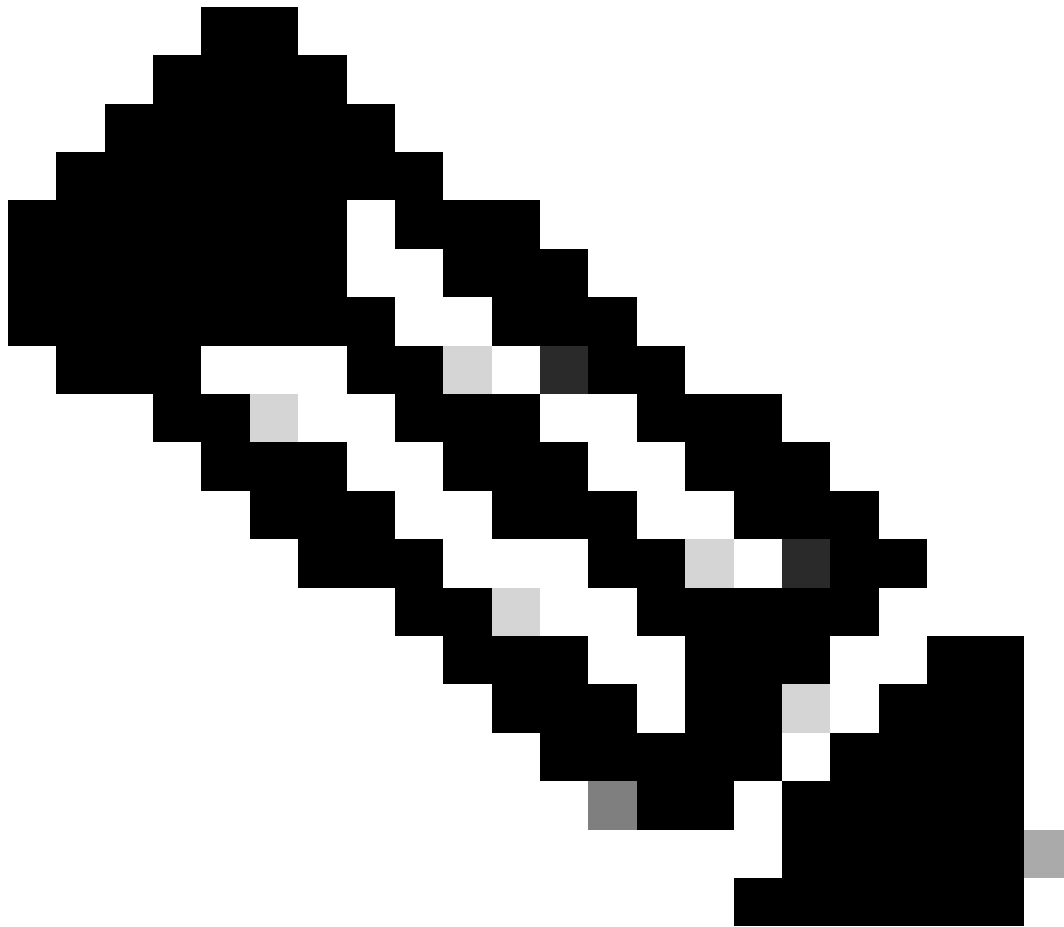


**Firepower Threat  
Defense device**



**Syslog server with the  
Splunk Search Head**

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.

FTD-PlatformSettings

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Logging Setup

Logging Destinations

Email Setup

Event Lists

Rate Limit

Syslog Settings

Syslog Servers

Basic Logging Settings

☒ Enable Logging

☐ Enable Logging on the failover standby unit

☒ Send syslogs in EMBLEM format

☒ Send debug messages as syslogs

Memory Size of the Internal Buffer

52428700

(4096-52428800 Bytes)

VPN Logging Settings

☒ Enable Logging to Firewall Management Center

Logging Level

debugging

Specify FTP Server Information

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

## Add Syslog Server



IP Address\*

Protocol

☐

TCP

☒

UDP

Port

5156

(514 or 1025-65535)

Log Messages in Cisco  
EMBLEM format(UDP only)

☒

Enable secure syslog.

☐

Reachable By:

☐

Device Management Interface

(Applicable on FTD v6.3.0 and above)

☒

Security Zones or Named Interface

Available Zones



Search

inside

outside

Add

Selected Zones/Interfaces

outside

Interface Name

Add

Cancel

OK

Logging Setup
Logging Destinations
Email Setup
Event Lists
Rate Limit
Syslog Settings
Syslog Servers

☒ Allow user traffic to pass when TCP syslog server is down (Recommended to be enabled)

Message Queue Size(messages)\*

512

(0 - 8192 messages). Use 0 to indicate unlimited Queue Size

+ Add

| Interface | IP Address | Protocol | Port | EMBLEM | SECURE |  |
|-----------|------------|----------|------|--------|--------|--|
| outside   |            | UDP      | 5156 | true   | false  |  |

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.

Logging Setup
Logging Destinations
Email Setup
Event Lists
Rate Limit
Syslog Settings
Syslog Servers

+ Add

| Logging Destination   | Syslog from All Event Class | Syslog from specific Event Class |  |
|-----------------------|-----------------------------|----------------------------------|--|
| No records to display |                             |                                  |  |

Configuración de la plataforma en FTD - Agregar destino de registro

Add Logging Filter
?

Logging Destination

Syslog Servers

Event Class

Filter on Severity

debugging

+ Add

| Event Class           | Syslog Severity |  |
|-----------------------|-----------------|--|
| No records to display |                 |  |

Cancel

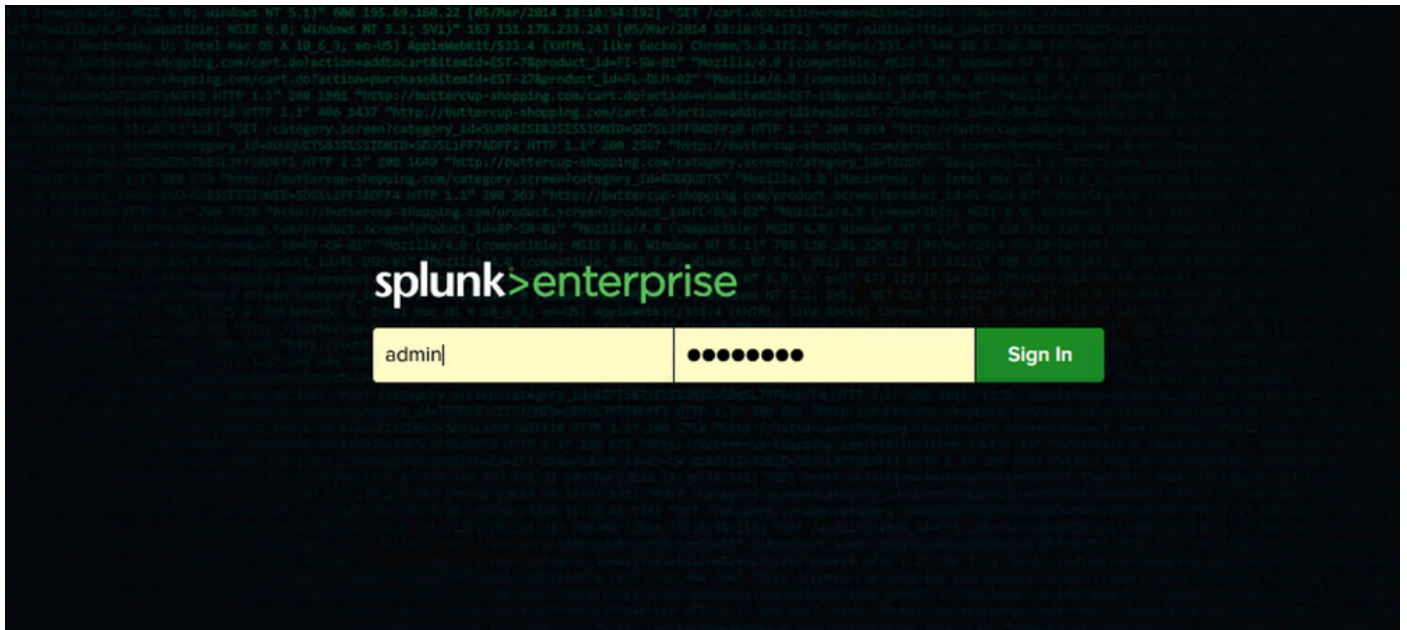
OK

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.

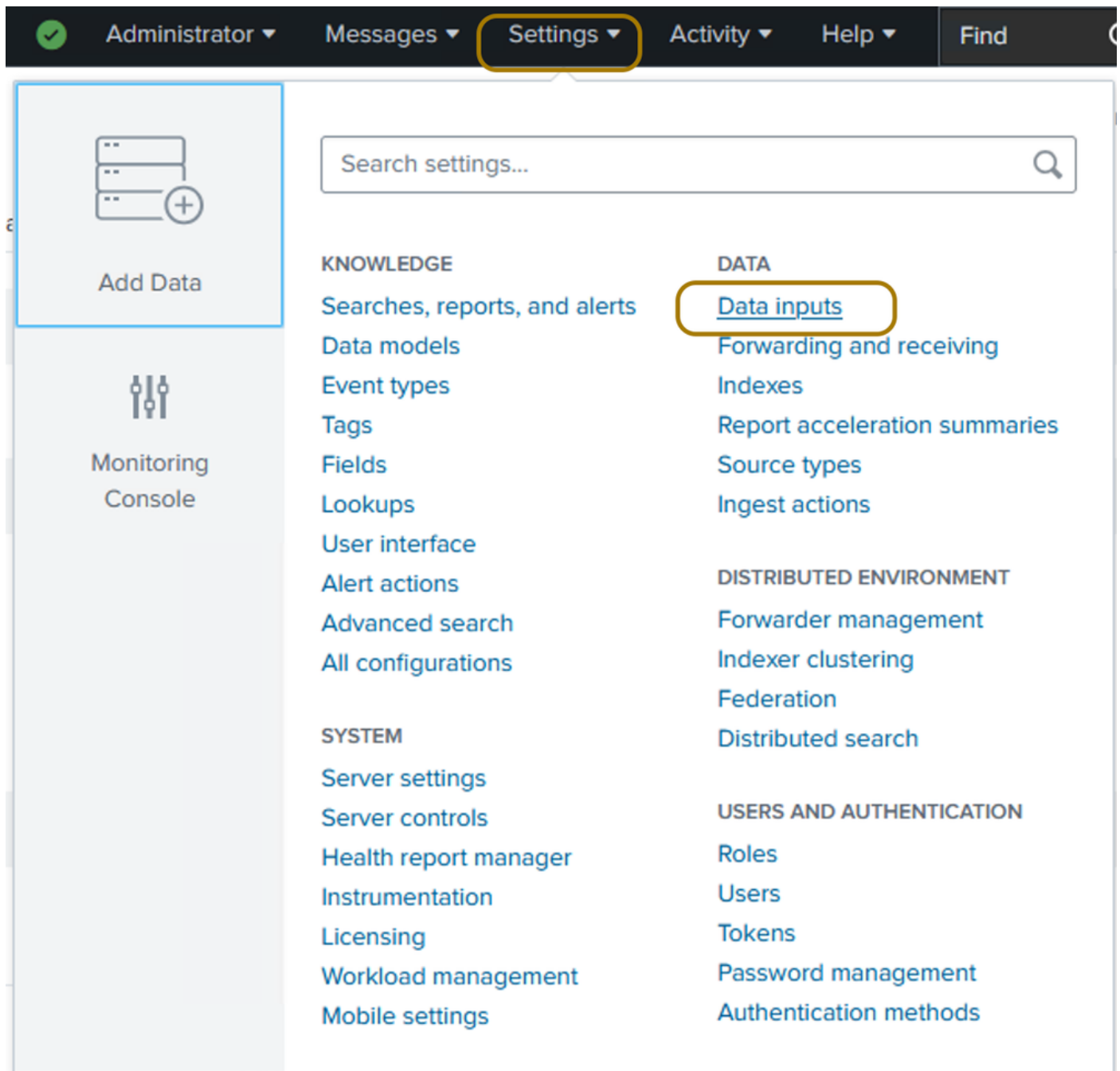
## Configuración de una entrada de datos en la instancia empresarial de Splunk

### 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.

| Local inputs                                                                                                               |        |           |
|----------------------------------------------------------------------------------------------------------------------------|--------|-----------|
| Type                                                                                                                       | Inputs | Actions   |
| Local event log collection<br>Collect event logs from this machine.                                                        | -      | Edit      |
| Remote event log collections<br>Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.   | 1      | + Add new |
| Files & Directories<br>Index a local file or monitor an entire directory.                                                  | 20     | + Add new |
| Local performance monitoring<br>Collect performance data from local machine.                                               | 0      | + Add new |
| Remote performance monitoring<br>Collect performance and event information from remote hosts. Requires domain credentials. | 0      | + Add new |
| HTTP Event Collector<br>Receive data over HTTP or HTTPS.                                                                   | 0      | + Add new |
| TCP<br>Listen on a TCP port for incoming data, e.g. syslog.                                                                | 1      | + Add new |
| UDP<br>Listen on a UDP port for incoming data, e.g. syslog.                                                                | 1      | + Add new |
| Registry monitoring<br>Have Splunk index the local Windows Registry, and monitor it for changes.                           | 0      | + Add new |

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

splunkenterprise

Apps

Administrator

Messages

Settings

Activity

Help

Find

UDP

Data inputs > UDP

filter

25 per page

New Local 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).

splunkenterprise

Apps

Administrator

Messages

Settings

Activity

Help

Find

Add Data

Select Source

Input Settings

Review

Done

< Back

Next >

Local Event Logs

Collect event logs from this machine.

Remote Event Logs

Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories

Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector

Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP

Configure the Splunk platform to listen on a network port.

Local Performance Monitoring

Collect performance data from this machine.

Remote Performance Monitoring

Collect performance and event information from remote hosts. Requires domain credentials.

Registry monitoring

Have the Splunk platform index the local Windows Registry, and monitor it for changes.

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). [Learn More](#)

TCP

UDP

Port ?

5156

Example: 514

Source name override ?

optional

host:port

Only accept connection from ?

example: 10.1.2.3, !badhost.splunk.com, \*.splunk.com

FAQ

> How should I configure the Splunk platform for syslog traffic?

> What's the difference between receiving data over TCP versus UDP?

> Can I collect syslog data from Windows systems?

> What is a source type?

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.

**Input Settings**

Optionally set additional input parameters for this data input as follows:

**Source type**

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

**App context**

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. [Learn More](#)

**Host**

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

**Index**

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Configurar los parámetros de entrada de datos

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

**Review**

Input Type ..... UDP Port

Port Number ..... 5156

Source name override ..... N/A

Restrict to Host .....

Source Type ..... cisco:ftd:syslog

App Context ..... launcher

Host ..... (IP address of the remote server)

Index ..... cisco\_sfw\_ftd\_syslog

Revisar configuración de entrada de datos

Ejecutar consultas SPL y crear paneles

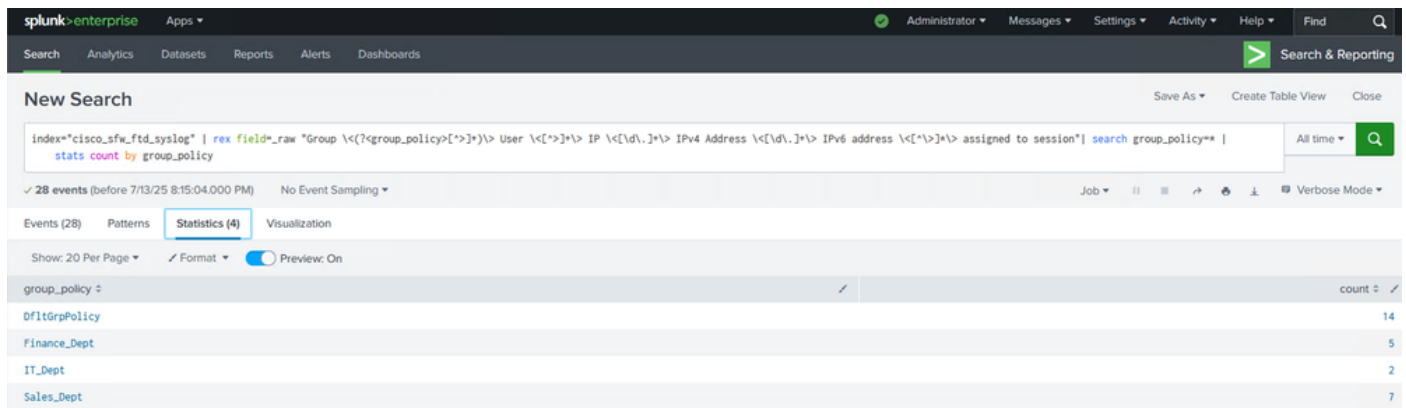
Paso 1. Navegue hasta la aplicación de búsqueda e informes en Splunk.

Vaya a la aplicación Buscar y generar informes

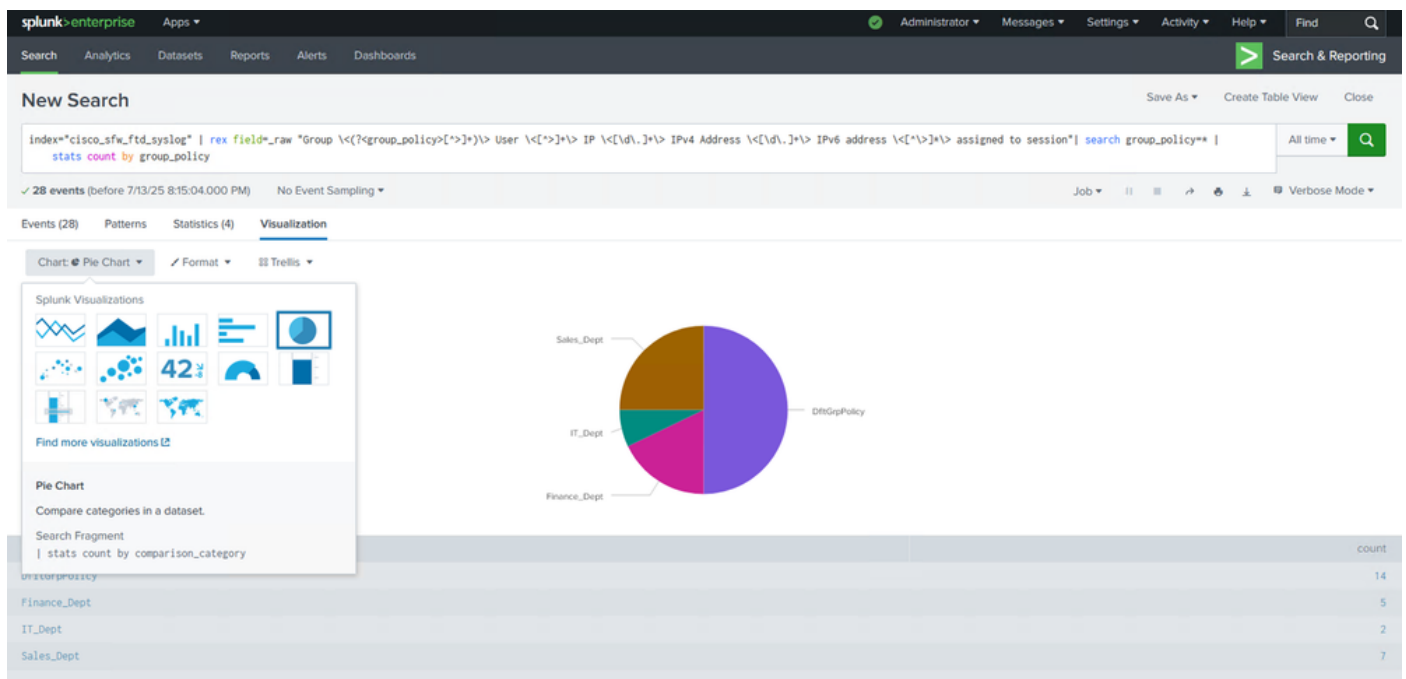
Paso 2. Formular y ejecutar una consulta SPL según los datos que desee visualizar. Podrá ver cada registro por completo (en el modo detallado) en la pestaña Eventos, el recuento de conexiones por política de grupo en la pestaña Estadísticas y visualizar estos datos usando estas estadísticas en la pestaña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

| i | Time                       | Event                                                                                                                                                                                                                                                                                                  |
|---|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| > | 6/24/25<br>10:58:43.000 PM | Jun 24 22:58:43 [REDACTED] : 2025 Jun 25 05:01:01 UTC a3a8bea6-0828-11ef-aa8a-b652b0561baa : %FTD-svc-4-722051: Group <Sales_Dept> User [REDACTED] IP <[REDACTED]> IPv4 Address <[REDACTED]> IPv6 address <[:]> assigned to session<br>group_policy = Sales_Dept   host = [REDACTED] source = udp:5156 |
| > | 6/24/25<br>8:32:58.000 PM  | Jun 24 20:32:58 [REDACTED] : 2025 Jun 25 02:35:16 UTC a3a8bea6-0828-11ef-aa8a-b652b0561baa : %FTD-svc-4-722051: Group <IT_Dept> User [REDACTED] IP <[REDACTED]> IPv4 Address <[REDACTED]> IPv6 address <[:]> assigned to session<br>group_policy = IT_Dept   host = [REDACTED] source = udp:5156       |
| > | 6/24/25<br>8:29:15.000 PM  | Jun 24 20:29:15 [REDACTED] : 2025 Jun 25 02:31:33 UTC a3a8bea6-0828-11ef-aa8a-b652b0561baa : %FTD-svc-4-722051: Group <Sales_Dept> User [REDACTED] IP <[REDACTED]> IPv4 Address <[REDACTED]> IPv6 address <[:]> assigned to session<br>group_policy = Sales_Dept   host = [REDACTED] source = udp:5156 |
| > | 6/24/25<br>8:27:27.000 PM  | Jun 24 20:27:27 [REDACTED] : 2025 Jun 25 02:29:45 UTC a3a8bea6-0828-11ef-aa8a-b652b0561baa : %FTD-svc-4-722051: Group <Sales_Dept> User [REDACTED] IP <[REDACTED]> IPv4 Address <[REDACTED]> IPv6 address <[:]> assigned to session<br>group_policy = Sales_Dept   host = [REDACTED] source = udp:5156 |
| > | 6/24/25<br>8:26:59.000 PM  | Jun 24 20:26:59 [REDACTED] : 2025 Jun 25 02:29:17 UTC a3a8bea6-0828-11ef-aa8a-b652b0561baa : %FTD-svc-4-722051: Group <Finance_Dept> User [REDACTED] IP <[REDACTED]> IPv4 Address <[REDACTED]> IPv6 address <[:]> assigned to session                                                                  |

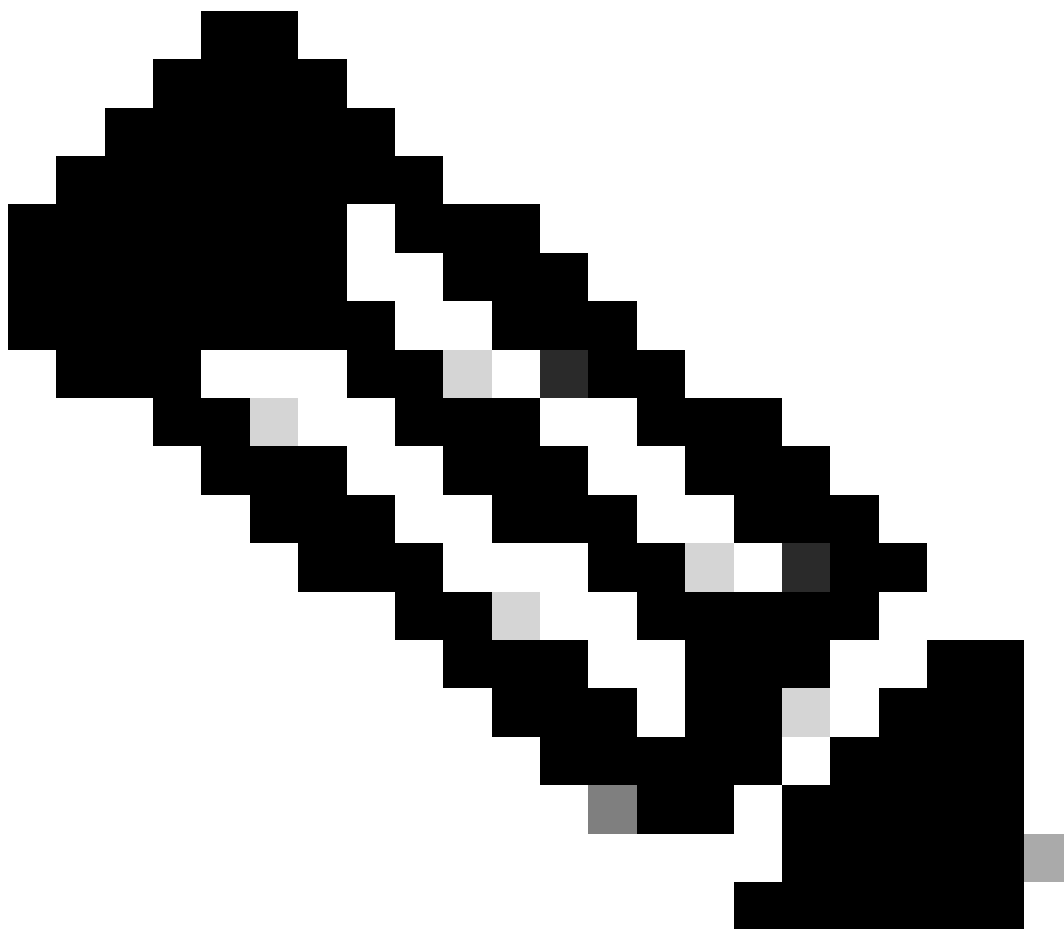
Buscar eventos mediante consultas SPL



Selecione la ficha Estadísticas.



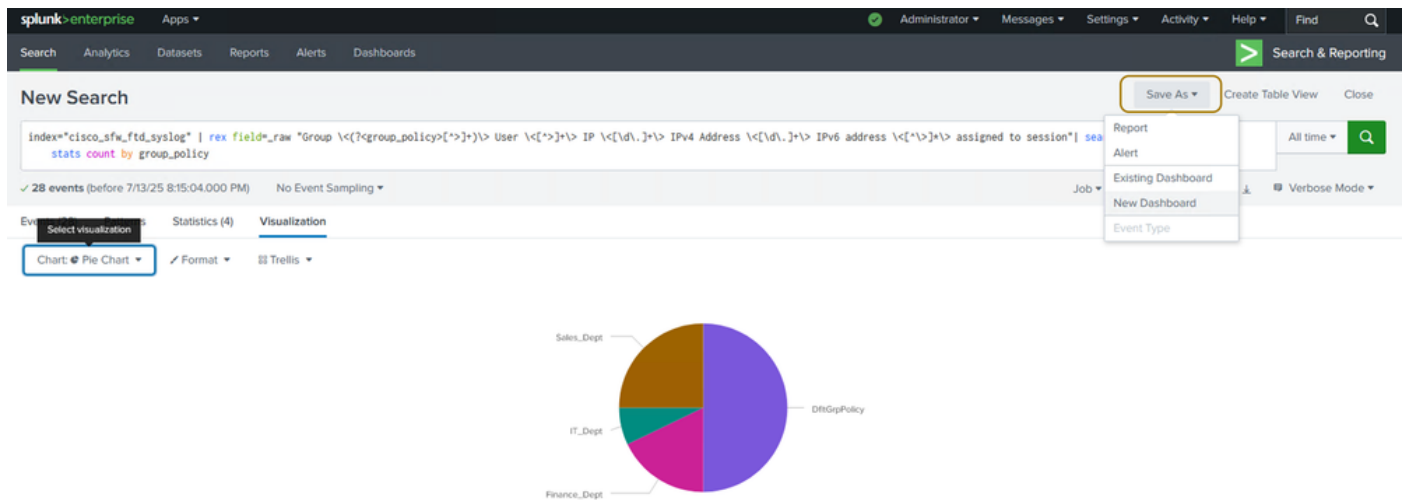
La ficha Visualización mostrará el gráfico/gráfico



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

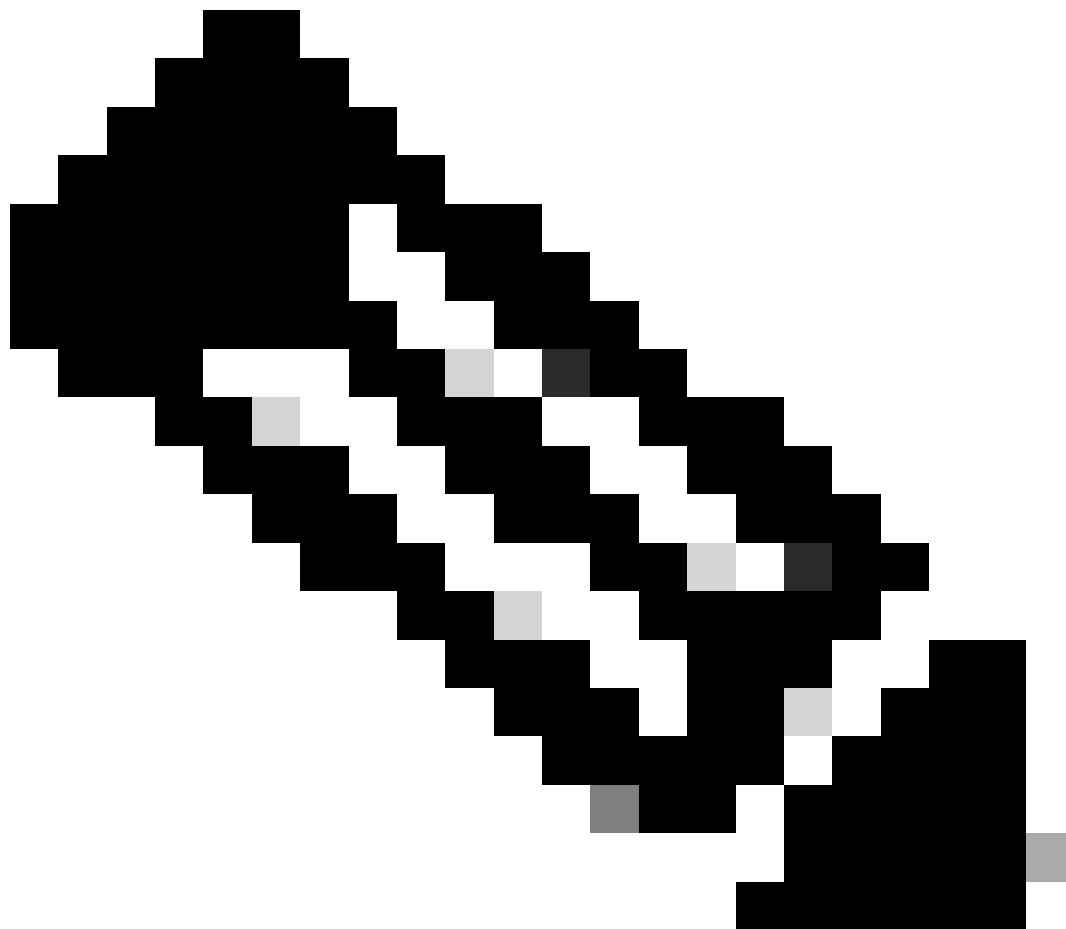
Statistics Table

> Advanced Panel Settings

Cancel

Save to Dashboard





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 continuously)

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.

## Save As Alert



### Settings

|             |                                                            |               |
|-------------|------------------------------------------------------------|---------------|
| Title       | Alert to notify more than 10 failed attempts in 10 minutes |               |
| Description | Optional                                                   |               |
| Permissions | Private                                                    | Shared in App |
| Alert type  | Scheduled                                                  | Real-time     |
| Expires     | 10                                                         | minute(s) ▼   |

### Trigger Conditions

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Trigger alert when | Custom ▼                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |  |
|                    | <div><div>Per-Result<br/>Triggers whenever search returns a result.</div><div>Number of Results<br/>Triggers based on a number of search results during a rolling-window of time.</div><div>Number of Hosts<br/>Triggers based on a number of hosts during a rolling-window of time.</div><div>Number of Sources<br/>Triggers based on a number of sources during a rolling-window of time.</div><div><input checked="" type="checkbox"/> Custom<br/>Triggers based on a custom condition during a rolling-window time.</div></div> |  |
|                    | <div><div></div><div>e.g. "search count &gt; 10"</div></div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |  |
| in                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |
| Trigger            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |
| Throttle ?         | <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |  |
| Trigger Actions    | <div>+ Add Actions ▼</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |  |

Save

Configuración adicional para la creación de alertas

### Trigger Conditions

|                    |                                                                                                                                |                 |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Trigger alert when | Custom ▼                                                                                                                       |                 |
|                    | <div>search reject_count&gt;10</div> <div>e.g. "search count &gt; 10". Evaluated against the results of the base search.</div> |                 |
| in                 | 5                                                                                                                              | minute(s) ▼     |
| Trigger            | Once                                                                                                                           | For each result |
| Throttle ?         | <input type="checkbox"/>                                                                                                       |                 |

Trigger Actions

+ Add Actions ▾

When triggered

▼

 Add to Triggered Alerts

Remove

Severity

Medium ▾

Info

Low

✓ Medium

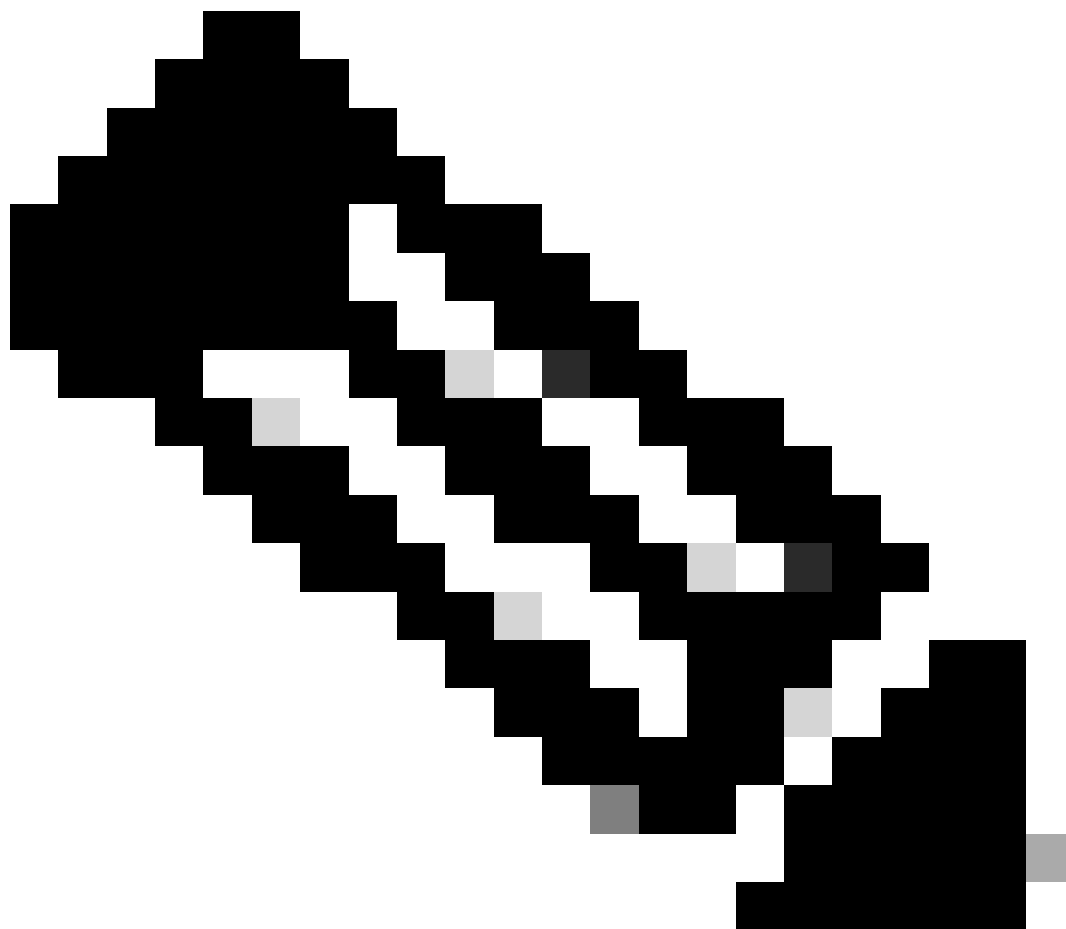
High

Critical

Cancel

Save

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.

splunk>enterprise Apps

Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

### New Search

Save As Create Table View Close

Search: `index=main w_ftd_syslog` Last 24 hours

290,844 events (7/13/25 1:00:00.000 AM to 7/14/25 1:36:08.000 AM) No Event Sampling

Job Fast Mode

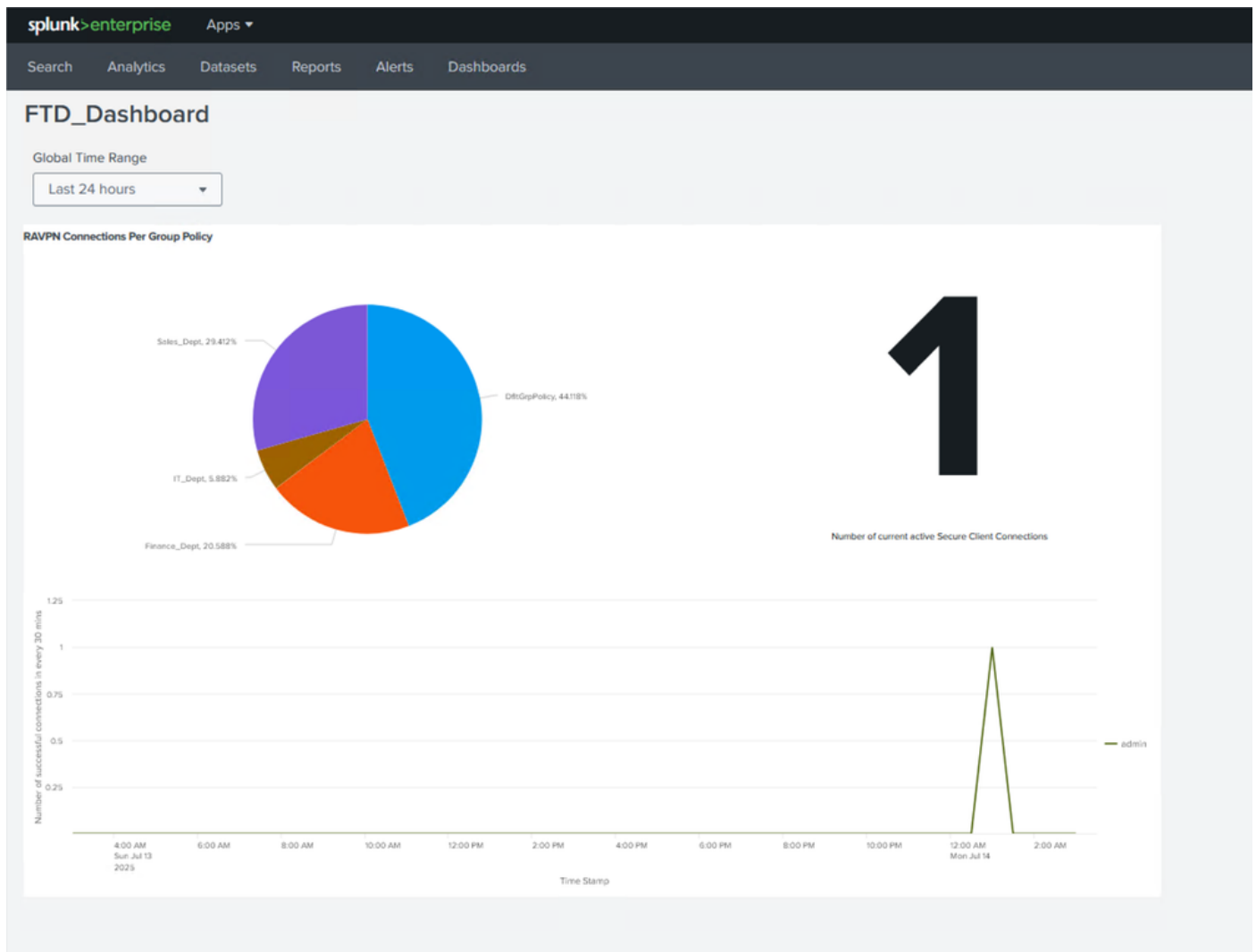
Comprobar y ver registros

| i | Time                   | Event                                                                                                                                                                        |
|---|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| > | 7/14/25 1:36:00.000 AM | Jul 14 01:36:00 [REDACTED] :Jul 14 07:36:09 UTC: %FTD-config-7-111009: User 'enable_1' executed cmd: show resource usage resource Routes host = [REDACTED] source = udp:5156 |

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.

splunk>enterpriseApps

AdministratorMessagesSettings

Searches, Reports, and Alerts

Searches, reports, and alerts are saved searches created from pivot or the search page. [Learn more](#)

2 Searches, Reports, and AlertsType: AllApp: Search & Reporting (search)Owner: Administrator (admin)filter

| Name                                                       | Actions            | Type  | Next Scheduled Time                       | Display View | Owner | App    |
|------------------------------------------------------------|--------------------|-------|-------------------------------------------|--------------|-------|--------|
| Alert to notify more than 10 failed attempts in 10 minutes | EditRunView Recent | Alert | 2025-07-14 01:24:00 Pacific Daylight Time | none         | admin | search |
| Exceeding maximum number of failed alerts                  | EditRunView Recent | Alert | 2025-07-14 01:24:00 Pacific Daylight Time | none         | admin | search |

Comprobar y ver alertas

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

Jobs

Manage your jobs. [Learn More](#)

68 JobsApp: Search & Reporting (search)Owner: AllStatus: Alllabel="Alert to notify more than 10 failed attempts in 10 minutes"10 Per Page

Edit Selected

< Prev1234567Next >

| i | Owner | Application | Events | Size    | Created at               | Expires                 | Runtime  | Status              | Actions        |
|---|-------|-------------|--------|---------|--------------------------|-------------------------|----------|---------------------|----------------|
| > | admin | search      | 11     | 4.57 MB | Jul 13, 2025 10:56:02 PM | Jul 14, 2025 1:27:30 AM | 02:29:27 | Running (real-time) | JobJob Actions |

Alert to notify more than 10 failed attempts in 10 minutes [real-time]

Comprobar y ver alertas

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

Alert to notify more than 10 failed attempts in 10 minutes

SaveSave AsViewCreate Table ViewClose

index="cisco\_sfwd\_syslog" | rex "authentication (?<auth\_status>\w\*)s\*:" | search auth\_status=Rejected | rex "user IP = (?<user\_ip>\d{1,3}(?:\.\d{1,3}){3})" | search user\_ip\*\* | stats count as reject\_count by user\_ip

26 of 33,995 events matchedNo Event Sampling

JobJob ActionsFast Mode

EventsPatternsStatistics (1)Visualization

Show: 20 Per PageFormat

| user_ip | reject_count |
|---------|--------------|
|         |              |

15

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).