

Criar painéis e alertas personalizados sobre o Splunk usando Syslogs do FTD

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Definir as configurações de Syslog para o FTD](#)

[Configurar uma Entrada de Dados na Instância do Splunk Enterprise](#)

[Executar consultas SPL e criar painéis](#)

[Configurar alertas com base em consultas SPL](#)

[Verificar](#)

[Exibir logs](#)

[Exibir os painéis em tempo real](#)

[Verifique se algum alerta foi disparado](#)

Introdução

Este documento descreve um passo a passo para configurar o FTD para enviar syslogs ao Splunk e usar esses logs para criar painéis e alertas personalizados.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos antes de passar por este guia de configuração:

- Syslog
- Conhecimento básico da Linguagem de Processamento de Pesquisa (SPL - Search Processing Language) do Splunk

Este documento também pressupõe que você já tenha a instância do Splunk Enterprise instalada em um servidor e tenha acesso à interface da Web.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- O Cisco Firepower Threat Defense (FTD) é executado na versão 7.2.4
- Cisco Firepower Management Center (FMC) em execução na versão 7.2.4
- Instância do Splunk Enterprise (versão 9.4.3) em execução em uma máquina com Windows

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial.

Informações de Apoio

Os dispositivos Cisco FTD geram syslogs detalhados que cobrem eventos de intrusão, políticas de controle de acesso, eventos de conexão e muito mais. A integração desses registros com o Splunk permite uma análise eficiente e alertas em tempo real para operações de segurança de rede.

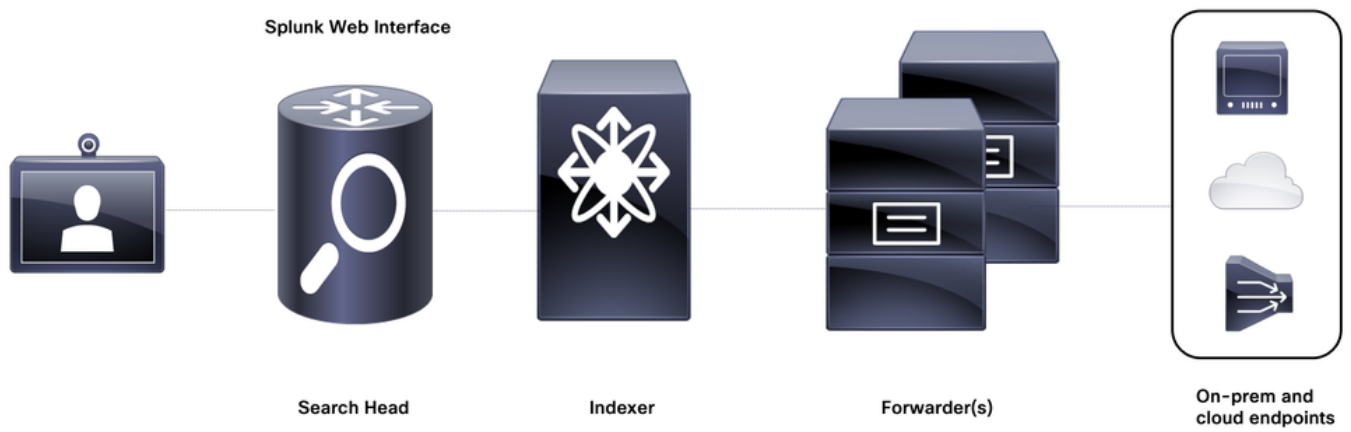
O Splunk é uma plataforma de análise de dados em tempo real projetada para incluir, indexar, pesquisar e visualizar dados gerados por máquina. O Splunk é especialmente eficaz em ambientes de segurança cibernética como uma ferramenta de Gerenciamento de Informações e Eventos de Segurança (SIEM) devido à sua capacidade de:

- Incluir dados de log em escala
- Executar pesquisas complexas com SPL
- Criar painéis e alertas
- Integrar-se com sistemas de orquestração de segurança e resposta a incidentes

O Splunk processa dados por meio de um pipeline estruturado para tornar úteis e acionáveis os dados da máquina não estruturados ou semiestruturados. As principais etapas desse pipeline são frequentemente chamadas de IPIS que significa:

- Entrada
- Análise
- Indexação
- Pesquisa

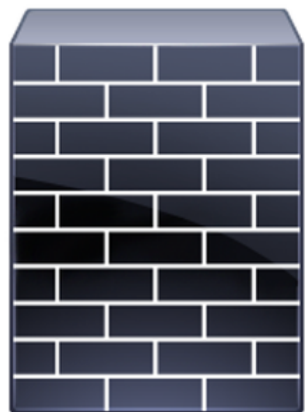
Os principais componentes amplos da arquitetura subjacente que são usados para realizar o pipeline do IPIS são mostrados neste diagrama:



Arquitetura subjacente de Splunk

Configurar

Diagrama de Rede



**Firepower Threat
Defense device**



**Syslog server with the
Splunk Search Head**

Diagrama de Rede



Note: O ambiente de laboratório para este documento não requer instâncias separadas de encaminhador e indexador. A máquina do Windows, ou seja, o Servidor syslog no qual a instância do Splunk Enterprise está instalada, está atuando como o indexador e o cabeçalho de pesquisa.

Configurações

Definir as configurações de Syslog para o FTD

Etapa 1. Configure as definições preliminares do syslog no FMC para o FTD em Devices > Platform Settings para enviar os logs ao servidor syslog no qual a instância Splunk está sendo executada.

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

Configurações da plataforma no FTD - Syslog

Etapa 2. Configure o endereço IP da máquina em que a instância do Splunk Enterprise está instalada e em execução como um Servidor Syslog. Defina os campos conforme 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 (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



Add

inside
outside

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	

Configurações de plataforma no FTD - Servidor Syslog adicionado

Etapa 3. Adicione um destino de registro para servidores Syslog. O nível de registro pode ser definido de acordo com sua escolha ou 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			

Configurações da plataforma em FTD - Adicionar 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

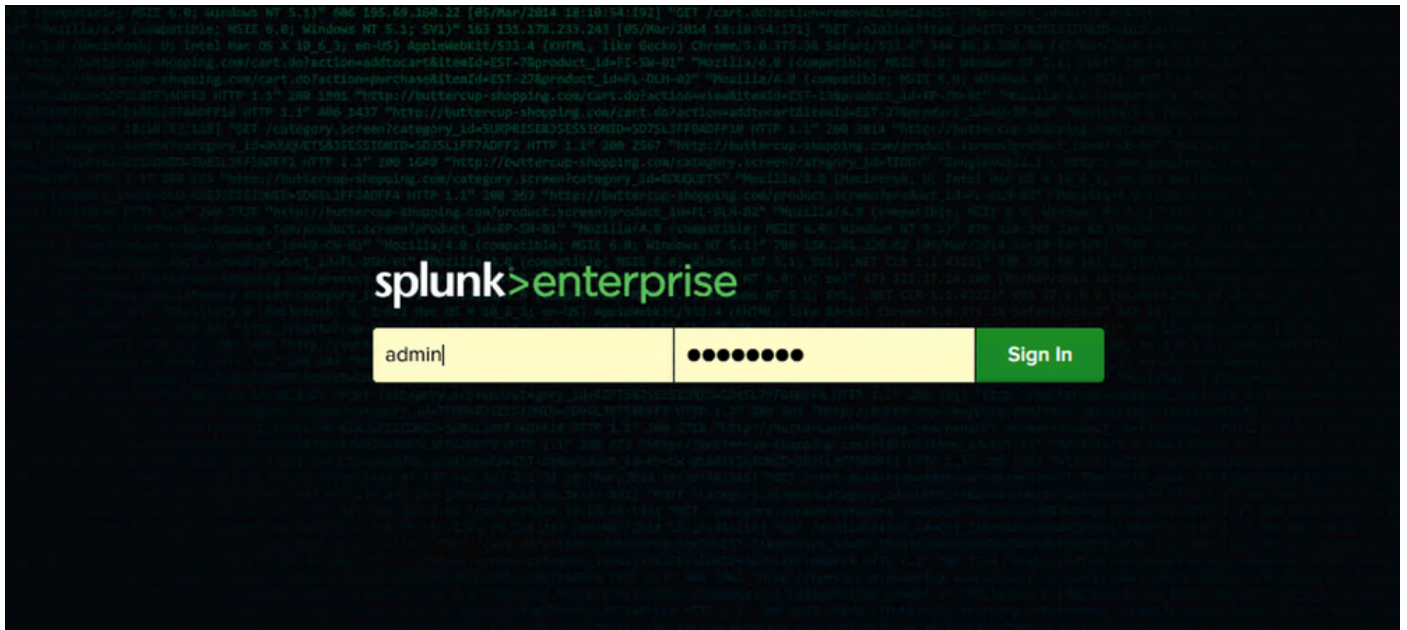
OK

Configurações da plataforma em FTD - Definir nível de severidade para destino de registro

Implante as alterações de configuração da plataforma no FTD após concluir estas etapas.

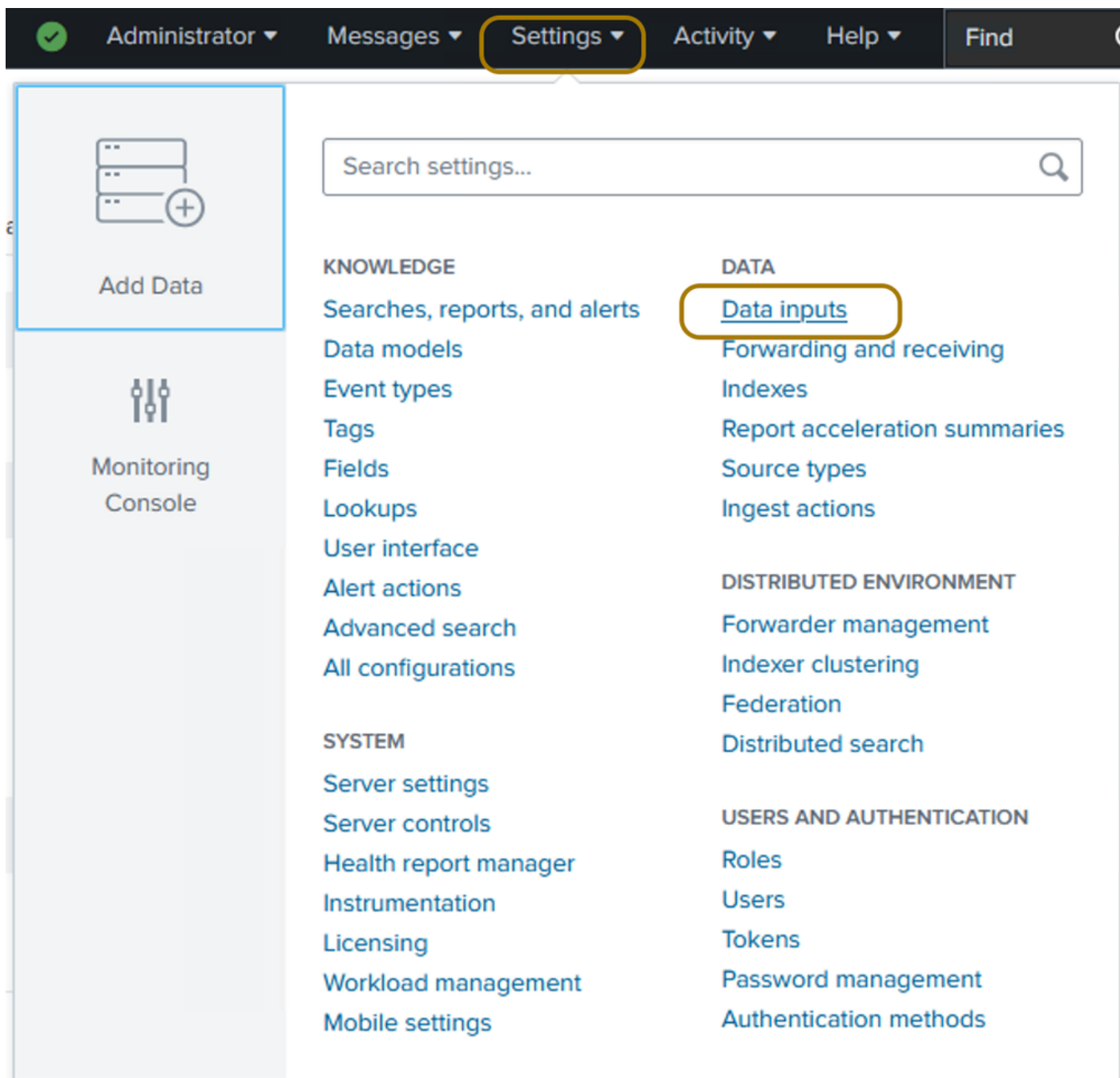
Configurar uma Entrada de Dados na Instância do Splunk Enterprise

Etapa 1. Efetue login na interface da Web da instância do Splunk Enterprise.



Página de Login da Interface da Web do Splunk

Etapa 2. Você deve definir uma Entrada de Dados para que possa armazenar e indexar os syslogs no Splunk. Navegue para Configurações > Dados > Entradas de dados depois de fazer login.



Navegar para Entradas de Dados no Splunk

Etapa 3. Escolha UDP e clique em New Local UDP na próxima página que aparece.

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

Clique em 'UDP' para uma Entrada de Dados UDP

splunk>enterprise

Apps

Administrator

Messages

Settings

Activity

Help

Find

UDP

Data inputs > UDP

filter

25 per page

New Local UDP

Criar uma Entrada 'Novo UDP Local'

Etapa 4. Digite a porta para onde os syslogs estão sendo enviados. Ele deve ser o mesmo que a porta configurada nas configurações de syslog do FTD, nesse caso 5156. Para aceitar os syslogs somente de uma origem (o FTD), defina o campo Only Accept Connection From para o IP da interface no FTD que está se comunicando com o servidor Splunk. Clique em Next.

splunk>enterprise

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 o endereço IP da Porta e do FTD

Etapa 5. Você pode pesquisar e escolher o tipo de origem e os valores dos campos de índice dos predefinidos no Splunk, como destacado na próxima imagem. As configurações padrão podem ser usadas para os campos restantes.

The screenshot shows the 'Add Data' wizard in Splunk, specifically the 'Input Settings' step. The progress bar at the top indicates the current step is 'Input Settings', with 'Select Source' completed and 'Review' and 'Done' pending. The 'Review' button is highlighted in green. The main content area is titled 'Input Settings' and includes a sub-header 'Optionally set additional input parameters for this data input as follows:'. Below this, there are four sections: 'Source type', 'App context', 'Host', and 'Index'. Each section has a descriptive paragraph and a corresponding input field. The 'Source type' field is a dropdown menu with 'cisco:ftd:syslog' selected. The 'App context' field is a dropdown menu with 'Apps Browser (appsbrowser)' selected. The 'Host' field is a text input with 'IP' selected. The 'Index' field is a dropdown menu with 'cisco_sfw_ftd_syslog' selected, and a 'Create a new index' link is visible next to it. The 'Review' button is highlighted in green.

Definir Configurações de Entrada de Dados

Etapa 6. Revise as configurações e clique em Enviar.

The screenshot shows the 'Add Data' wizard in Splunk, specifically the 'Review' step. The progress bar at the top indicates the current step is 'Review', with 'Select Source' and 'Input Settings' completed and 'Done' pending. The 'Submit' button is highlighted in green. The main content area is titled 'Review' and displays a list of configuration parameters and their values. The parameters are: 'Input Type' (UDP Port), 'Port Number' (5156), 'Source name override' (N/A), 'Restrict to Host' (a redacted value), 'Source Type' (cisco:ftd:syslog), 'App Context' (launcher), 'Host' ((IP address of the remote server)), and 'Index' (cisco_sfw_ftd_syslog). The 'Review' button is highlighted in green.

Revisar Configurações de Entrada de Dados

Executar consultas SPL e criar painéis

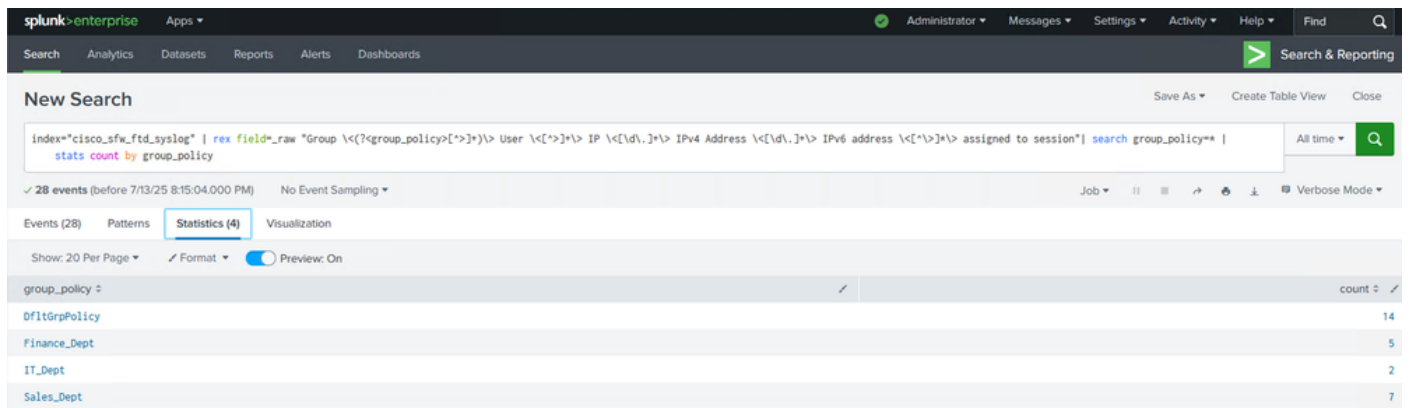
Etapa 1. Navegue até o Aplicativo de Pesquisa e Relatório no Splunk.

Navegue até o aplicativo Pesquisa e relatório

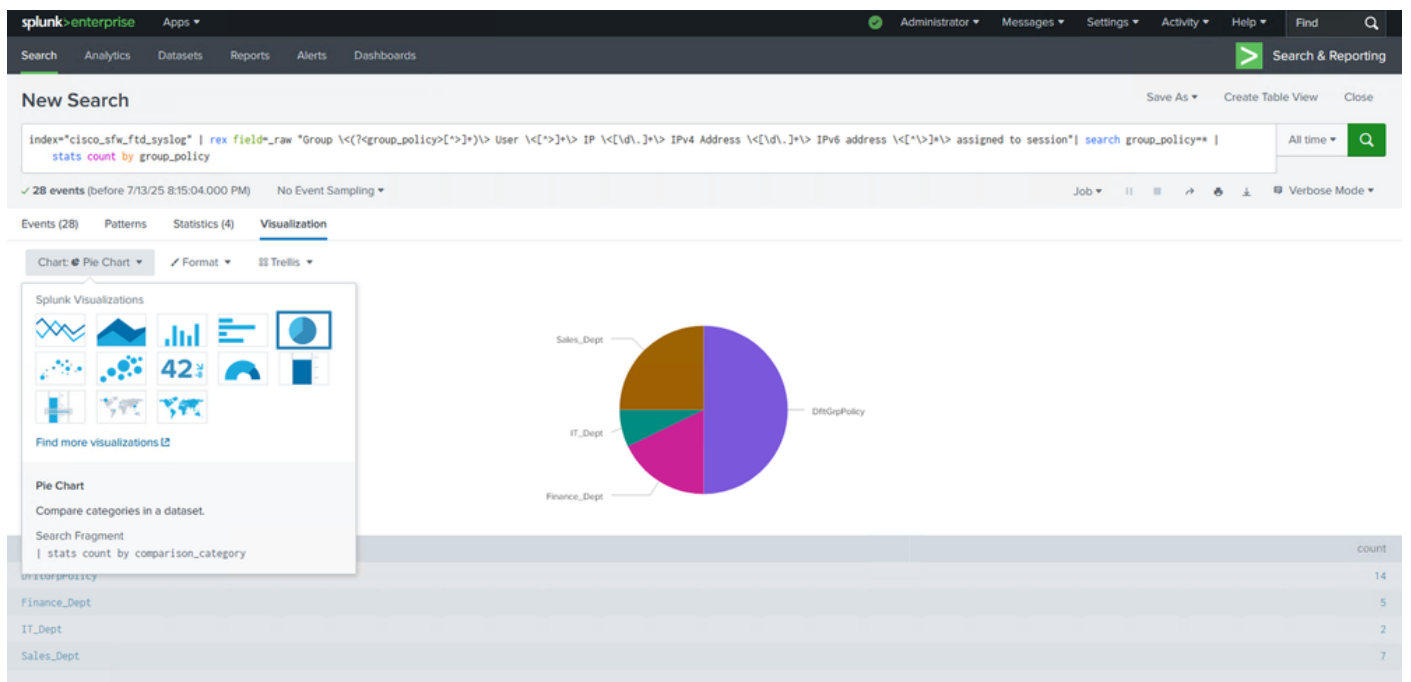
Etapa 2. Formule e execute uma consulta SPL de acordo com os dados que você deseja visualizar. Você poderá ver completamente cada log (no modo verboso) sob a guia Eventos, a contagem de conexões por política de grupo na guia Estatísticas e visualizar esses dados usando essas estatísticas sob a guia Visualização.

i	Time	Event
>	6/24/25 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 group_policy = Sales_Dept host = [redacted] source = udp:5156
>	6/24/25 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 group_policy = IT_Dept host = [redacted] source = udp:5156
>	6/24/25 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 group_policy = Sales_Dept host = [redacted] source = udp:5156
>	6/24/25 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 group_policy = Sales_Dept host = [redacted] source = udp:5156
>	6/24/25 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

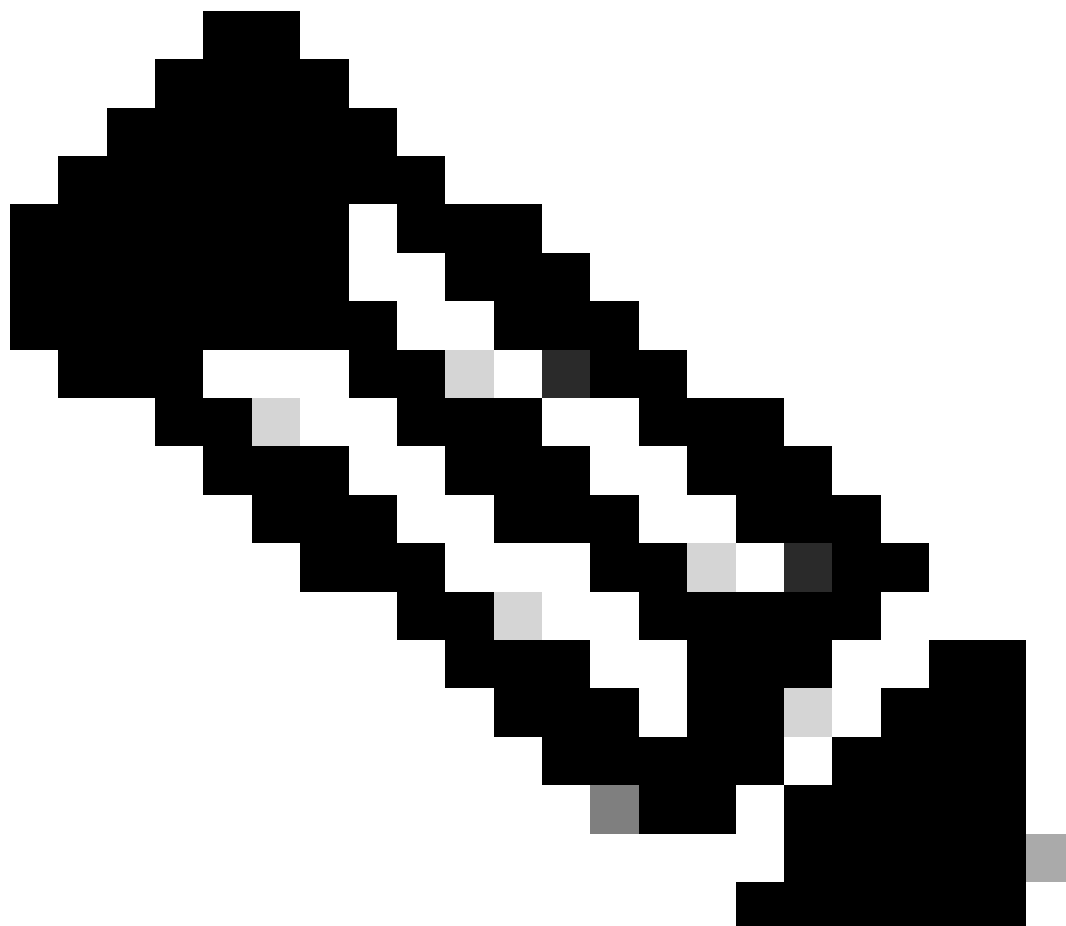
Procurar eventos usando consultas SPL



Verifique a guia Estatísticas

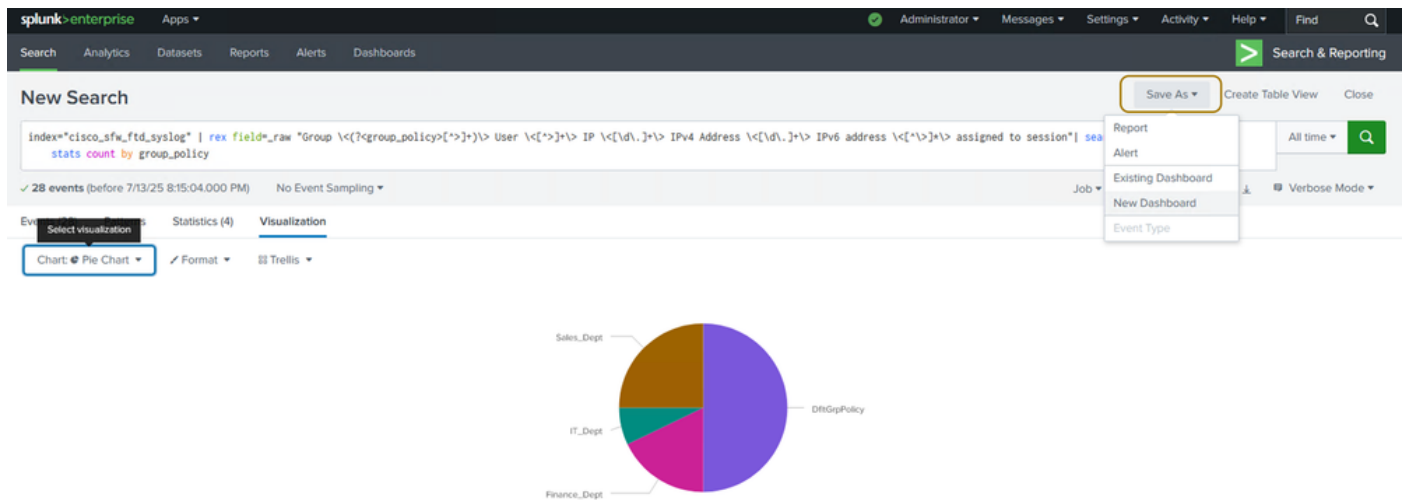


A guia Visualization (Visualização) mostrará o gráfico/gráfico



Note: Neste exemplo, a consulta está buscando logs para conexões VPN de acesso remoto bem-sucedidas em diferentes políticas de grupo. Um gráfico de pizza foi usado para visualizar o número e a porcentagem de conexões bem-sucedidas por política de grupo. Com base em seus requisitos e preferências, você pode optar por usar um tipo diferente de visualização, como um gráfico de barras também.

Etapa 3. Clique em Salvar Como e escolha Painel Novo ou Existente, dependendo se você já tem um painel ao qual deseja adicionar esse painel ou se deseja criar um novo. Este exemplo mostra o último.



Salvar o painel em um painel

Etapa 4. Dê um título ao painel que você está criando e forneça um título para o painel que conterá o gráfico de pizza.

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

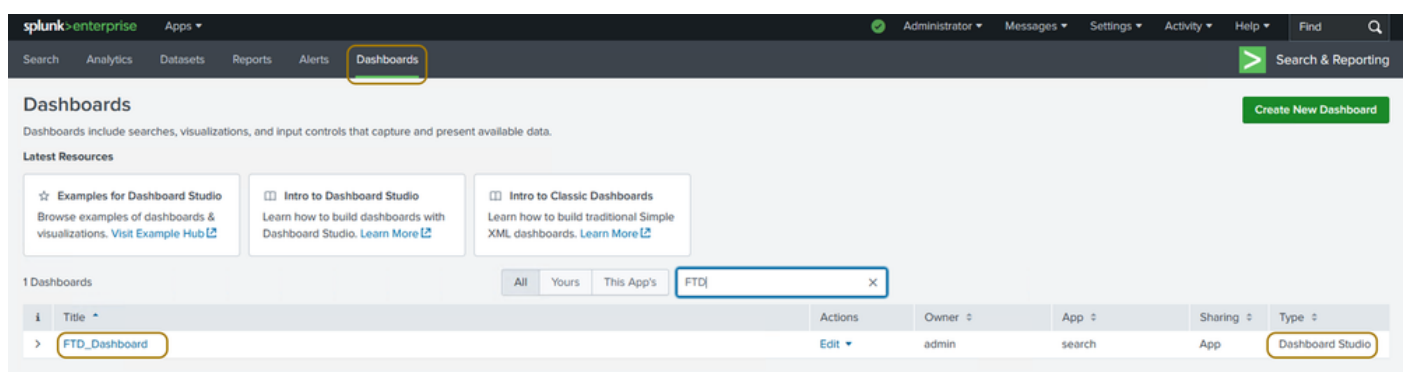
Cancel

Save to Dashboard

: Você pode definir as permissões como Particular ou Compartilhado no Aplicativo com base no fato de apenas você ter que exibir o painel ou de outros usuários com acesso à instância do Splunk também terem permissão. Além disso, dependendo se você deseja ou não controle granular sobre as configurações e o layout do painel, escolha o modo Clássico ou Dashboard Studio para criar seu painel.

Etapa 5 (opcional). Execute e salve mais consultas SPL como painéis para este painel, de acordo com suas necessidades, usando as etapas mencionadas anteriormente.

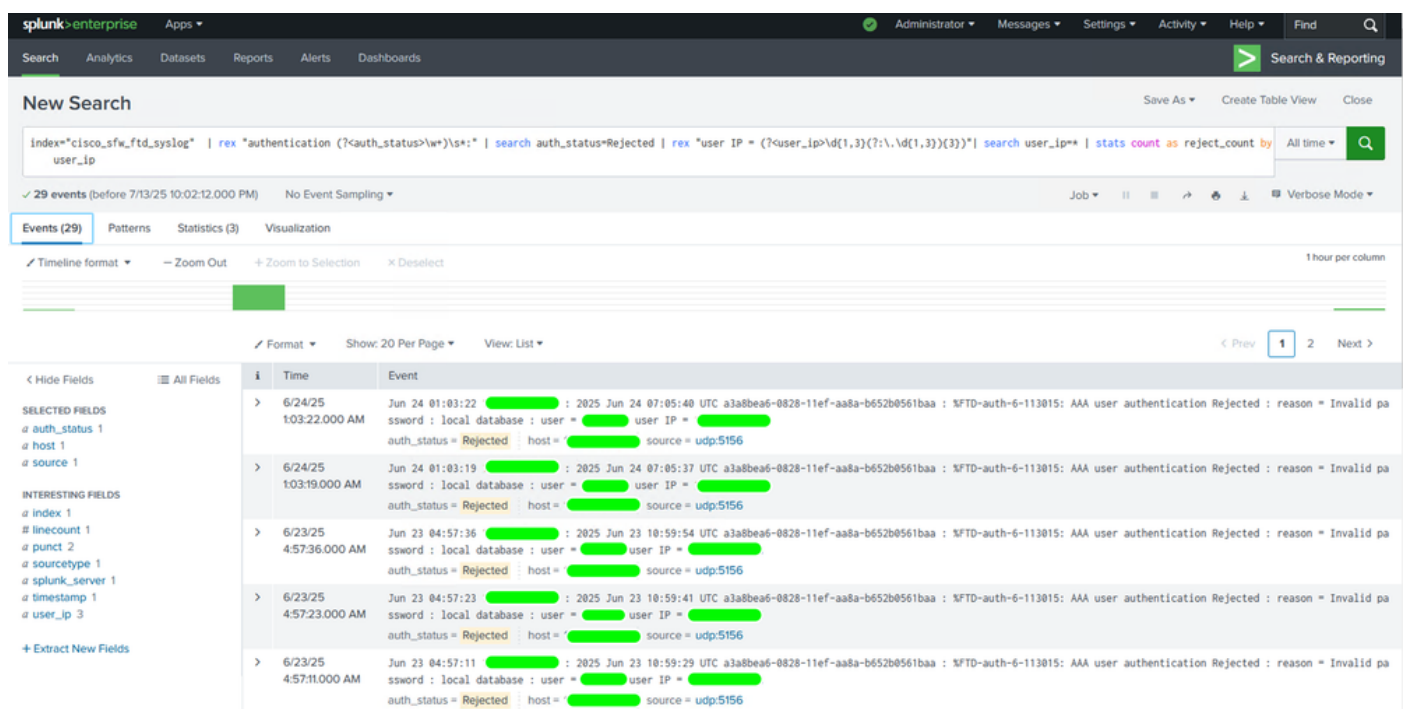
Etapa 6. Navegue até a guia Painel para pesquisar e escolher o painel que você criou. Clique nele para exibir, editar ou reorganizar seus painéis.



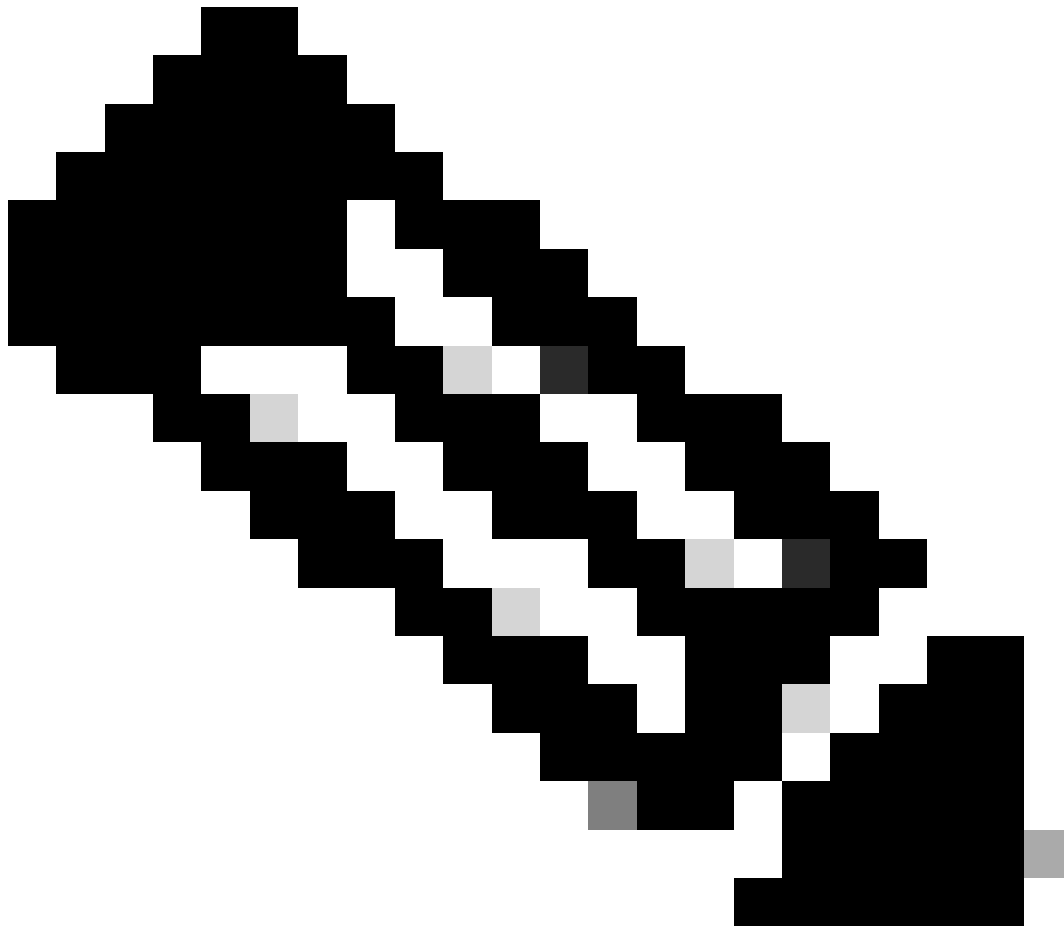
Como visualizar o painel

Configurar alertas com base em consultas SPL

Etapa 1. Navegue até o Aplicativo de Pesquisa e Relatório para construir e executar sua consulta SPL para verificar se está buscando os logs corretos que serão usados para disparar o alerta.



Executar consultas SPL para criar alertas respectivos



Note: Neste exemplo, a consulta é usada para buscar logs de autenticação com falha para VPN de acesso remoto para disparar alertas quando o número de tentativas com falha exceder um determinado limite dentro de um determinado período de tempo.

Etapa 3. Clique em Salvar como e escolha Alerta.



Salvar o alerta

Etapa 4. Dê um Título para nomear o Alerta. Preencha todos os outros detalhes e parâmetros necessários para configurar o alerta e clique em Salvar. As configurações usadas para este alerta foram mencionadas aqui.

<#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 ▼	
	Per-Result Triggers whenever search returns a result. Number of Results Triggers based on a number of search results during a rolling-window of time. Number of Hosts Triggers based on a number of hosts during a rolling-window of time. Number of Sources Triggers based on a number of sources during a rolling-window of time. ☒ Custom Triggers based on a custom condition during a rolling-window time.	
	e.g. "search count > 10"	
in		
Trigger		
Throttle ?	☐	
Trigger Actions	+ Add Actions ▼	

Save

Configurações adicionais para a criação de alertas

Trigger Conditions

Trigger alert when	Custom ▼	
	search reject_count>10 e.g. "search count > 10". Evaluated against the results of the base search.	
in	5	minute(s) ▼
Trigger	Once	For each result
Throttle ?	☐	

Trigger Actions

+ Add Actions ▾

When triggered

▼

 Add to Triggered Alerts

Remove

Severity

Medium ▾

Info

Low

✓ Medium

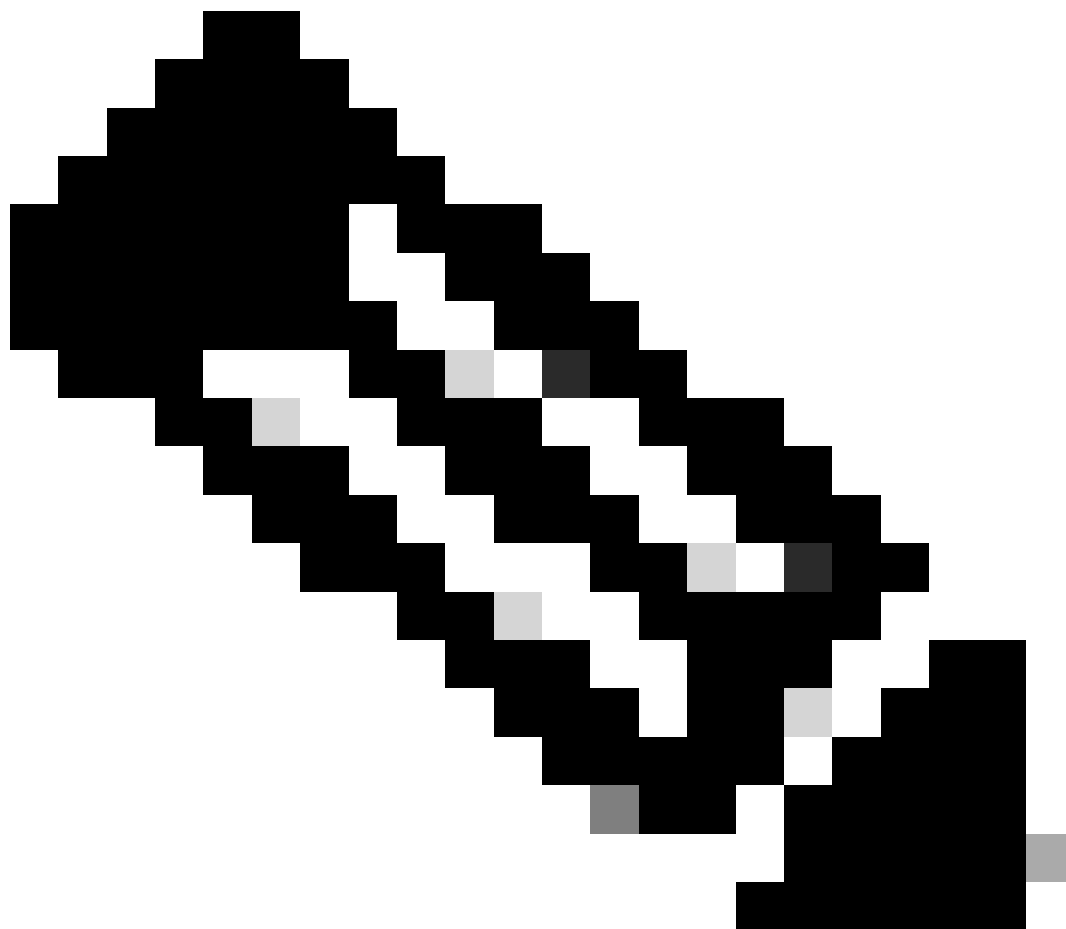
High

Critical

Cancel

Save

Configurações adicionais para a criação de alertas



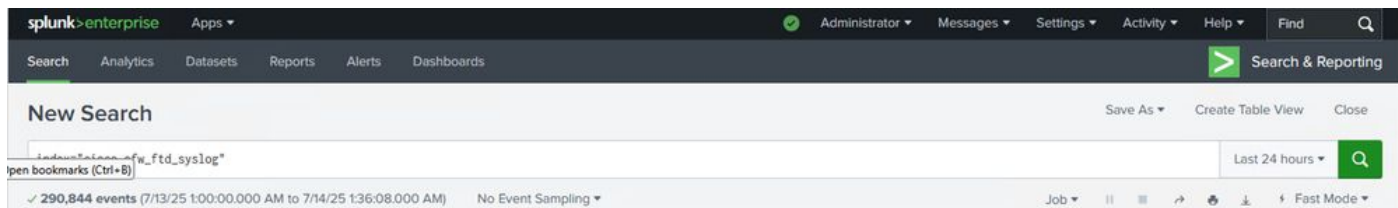
Note: Se você quiser disparar os alertas para cada resultado, terá que definir as configurações de limitação de acordo também.

Verificar

Depois de criar os painéis e alertas, você pode verificar as configurações, o fluxo de dados, os painéis e os alertas em tempo real usando as instruções fornecidas nesta seção.

Exibir logs

Você pode usar o aplicativo de pesquisa para confirmar se os logs enviados pelo firewall são recebidos e visíveis para o cabeçalho de pesquisa de fragmento. Isso pode ser verificado verificando os logs indexados mais recentes (índice de pesquisa = "cisco_sfw_ftd_syslog") e o carimbo de data/hora associado a ele.



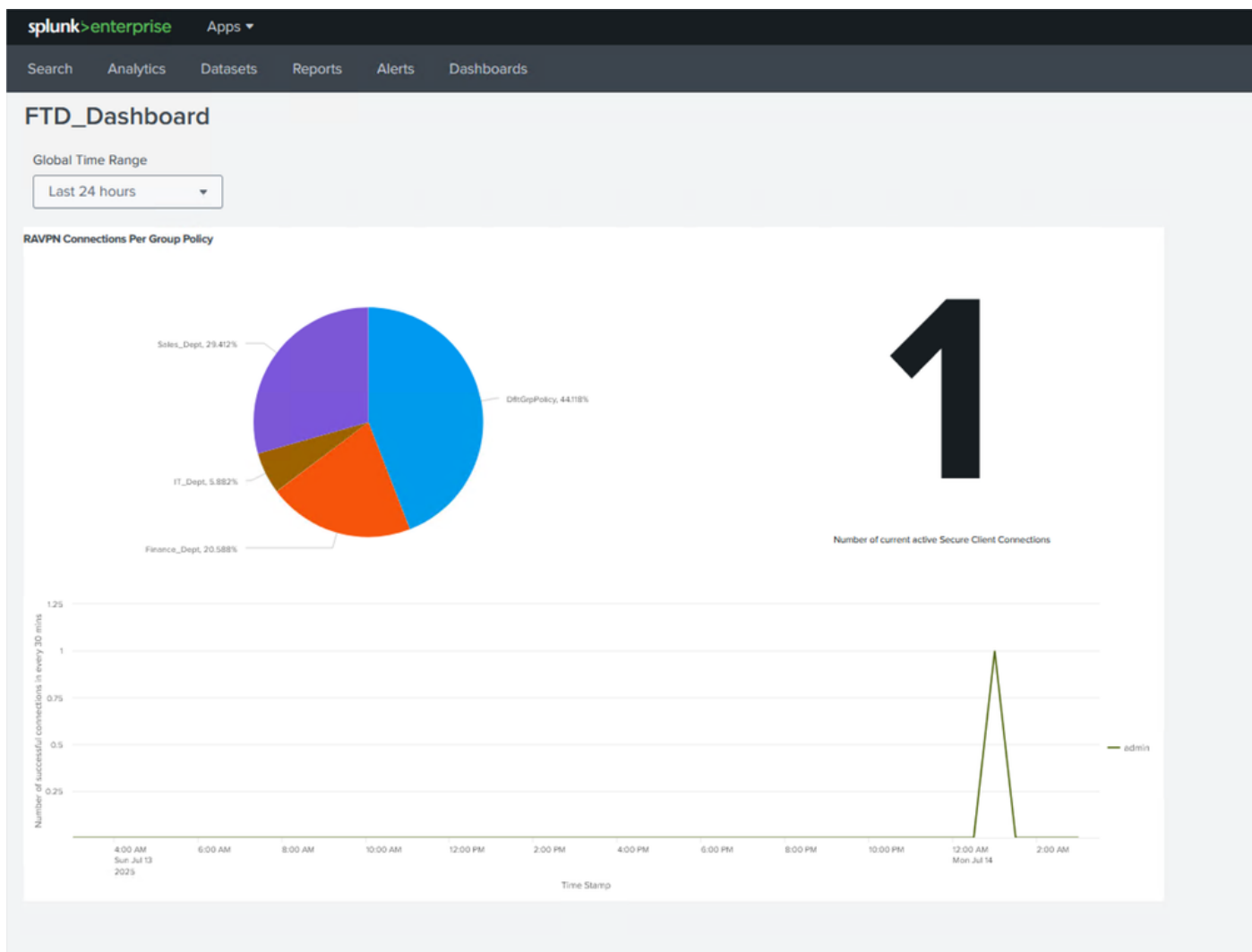
Verificar e exibir logs

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

Verificar e exibir logs

Exibir os painéis em tempo real

Você pode navegar até o painel personalizado que criou e ver a alteração em cada um dos painéis à medida que novos dados e logs são gerados a partir do FTD.



Exibir painéis

Verifique se algum alerta foi disparado

Para verificar as informações sobre os alertas, você pode navegar para as pesquisas de seção, relatórios e alertas para ver as informações de alerta recentes. Clique em View Recent para verificar mais sobre os trabalhos e pesquisas.

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

Verificar e exibir 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 >

	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 ControlJob Actions

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

Verificar e exibir 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

Real-time

26 of 33,995 events matchedNo Event Sampling

JobJob ControlJob ActionsFast Mode

EventsPatternsStatistics (1)Visualization

Show: 20 Per PageFormat

user_ip	reject_count
---------	--------------

15

Verificar Estatísticas para Alerta Disparado

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.