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

Contents

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.

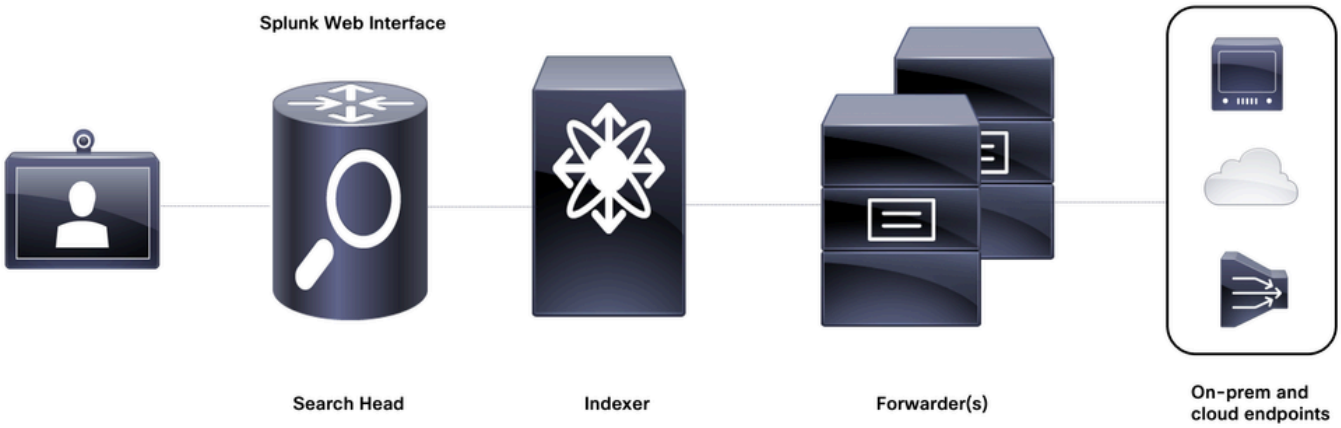
O Splunk é uma plataforma de análise de dados em tempo real projetada para incluir, indexar, pesquisar e visualizar dados gerados por máquina. O Splunk é especialmente eficaz em ambientes de segurança cibernética como uma ferramenta de Gerenciamento de Informações e Eventos de Segurança (SIEM) devido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

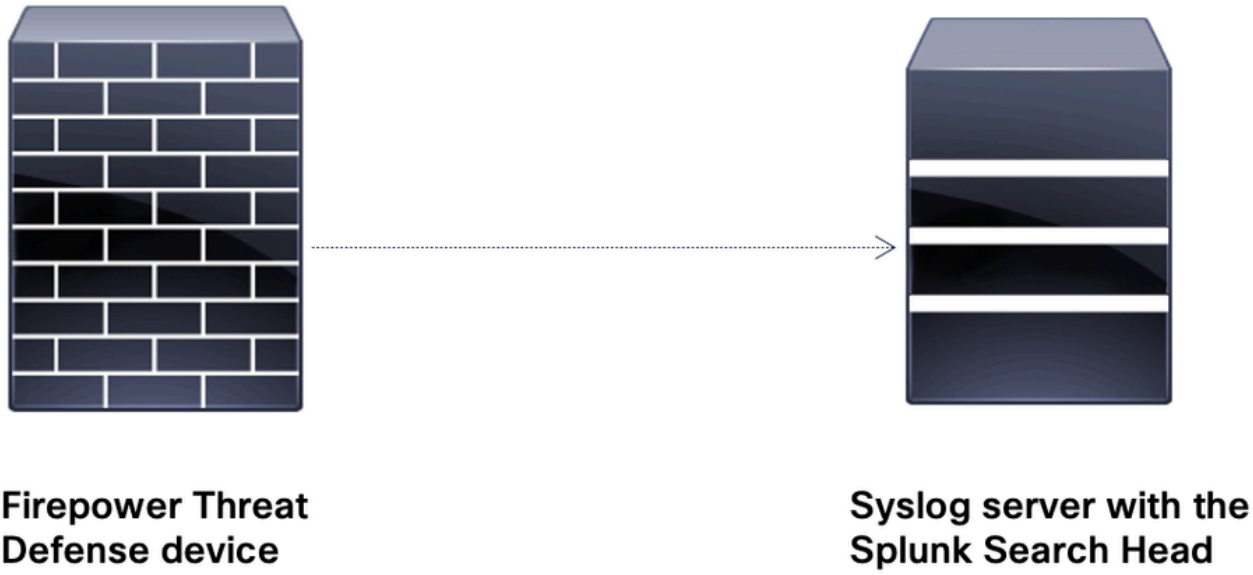
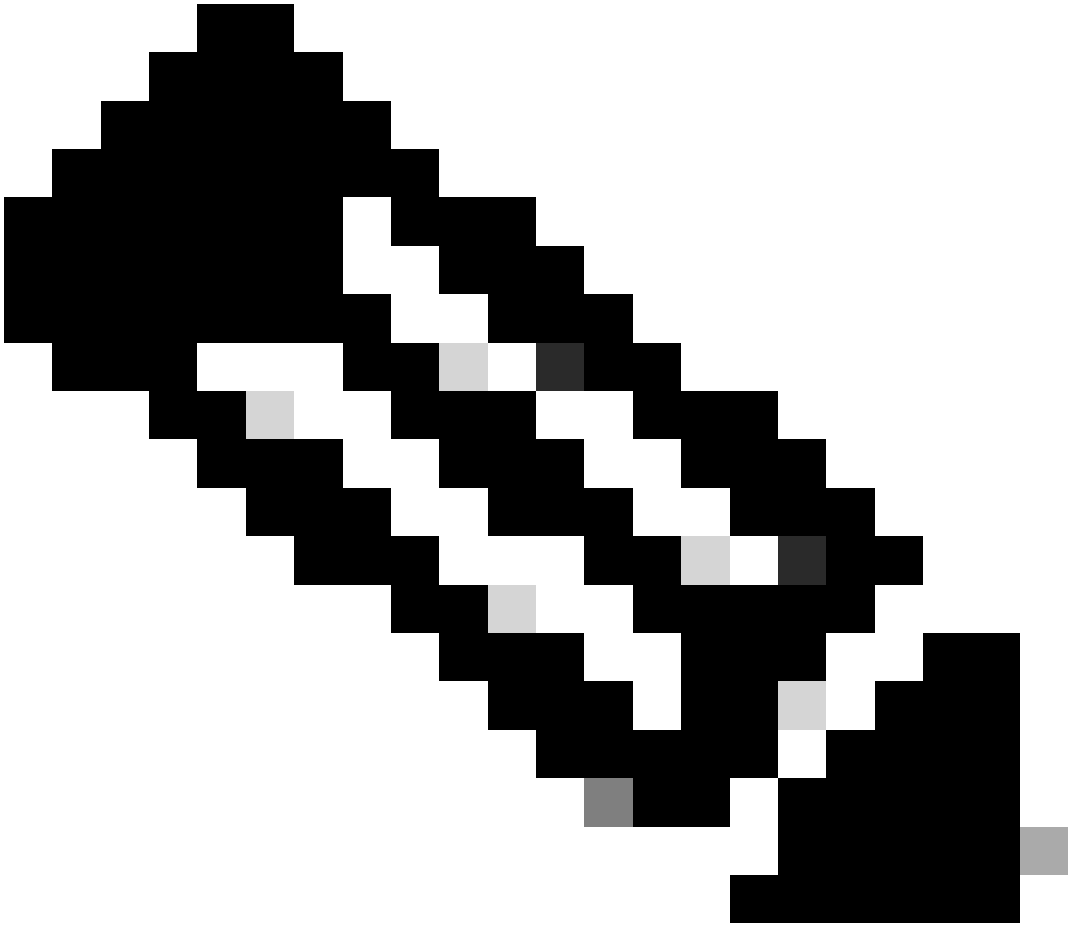


Diagrama de Rede

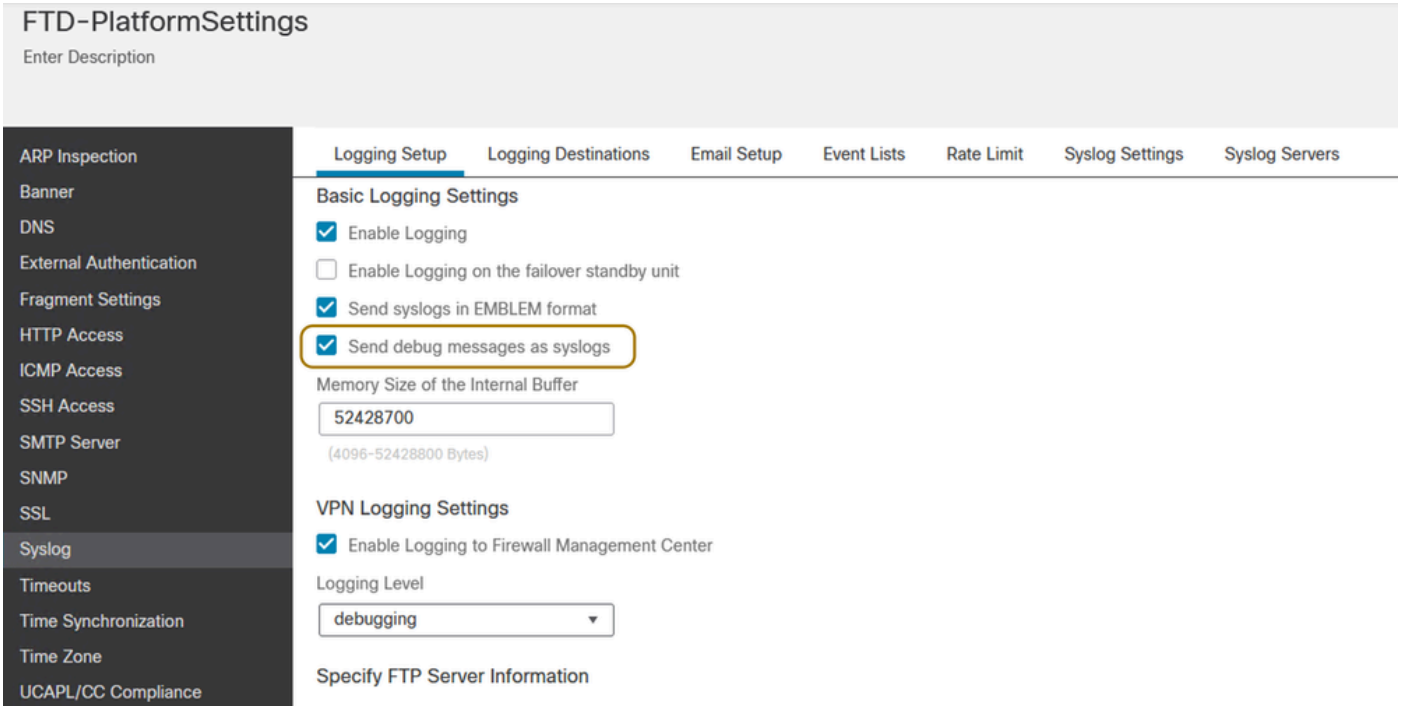


Note: O ambiente de laboratório para este documento não requer instâncias separadas de encaminhador e indexador. A máquina do Windows, ou seja, o Servidor syslog no qual a instância do Splunk Enterprise está instalada, está atuando como o indexador e o cabeçalho de pesquisa.

Configurações

Definir as configurações de Syslog para o FTD

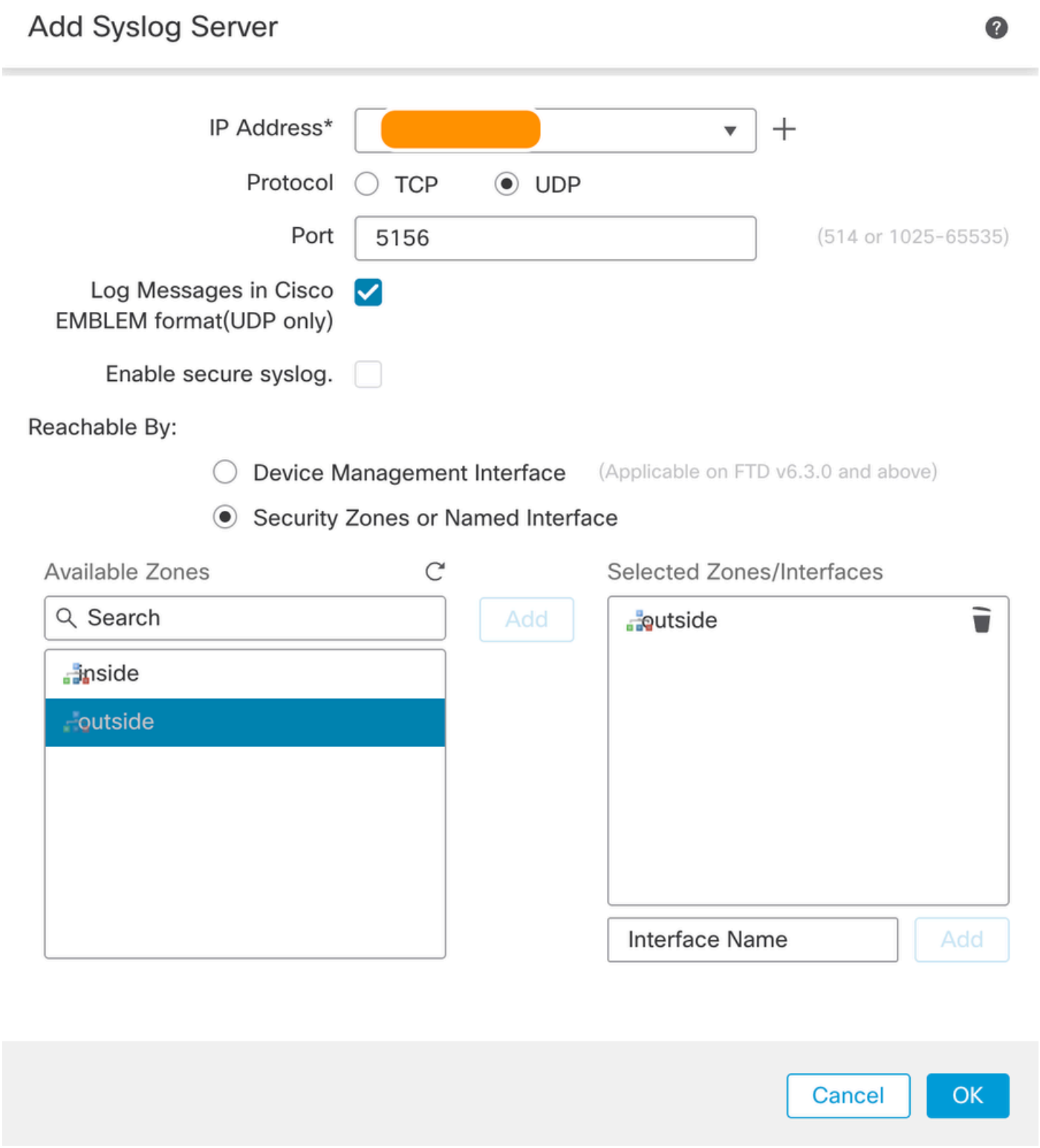
Etapa 1. Configure as definições preliminares do syslog no FMC para o FTD em Devices > Platform Settings para enviar os logs ao servidor syslog no qual a instância Splunk está sendo executada.



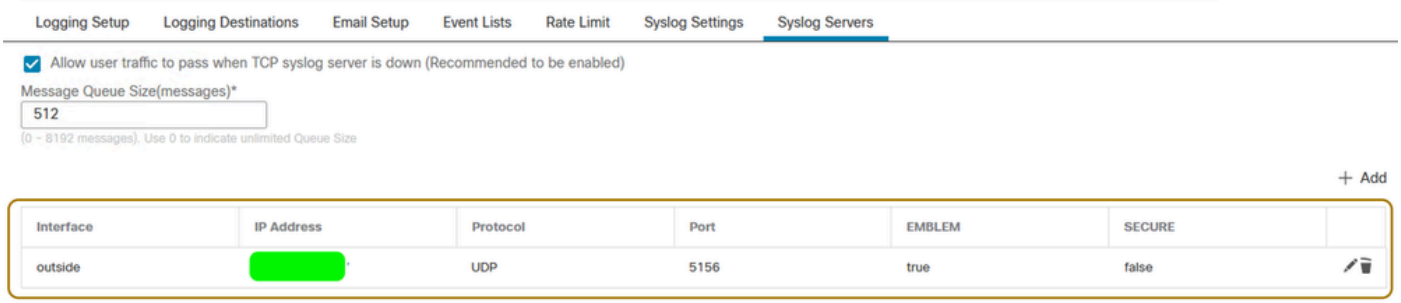
Configurações da plataforma no FTD - Syslog

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
```

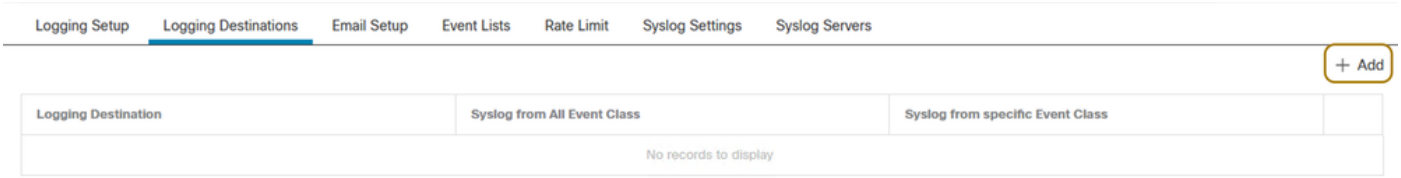


Configurações da plataforma em FTD - Adicionar servidor de syslog

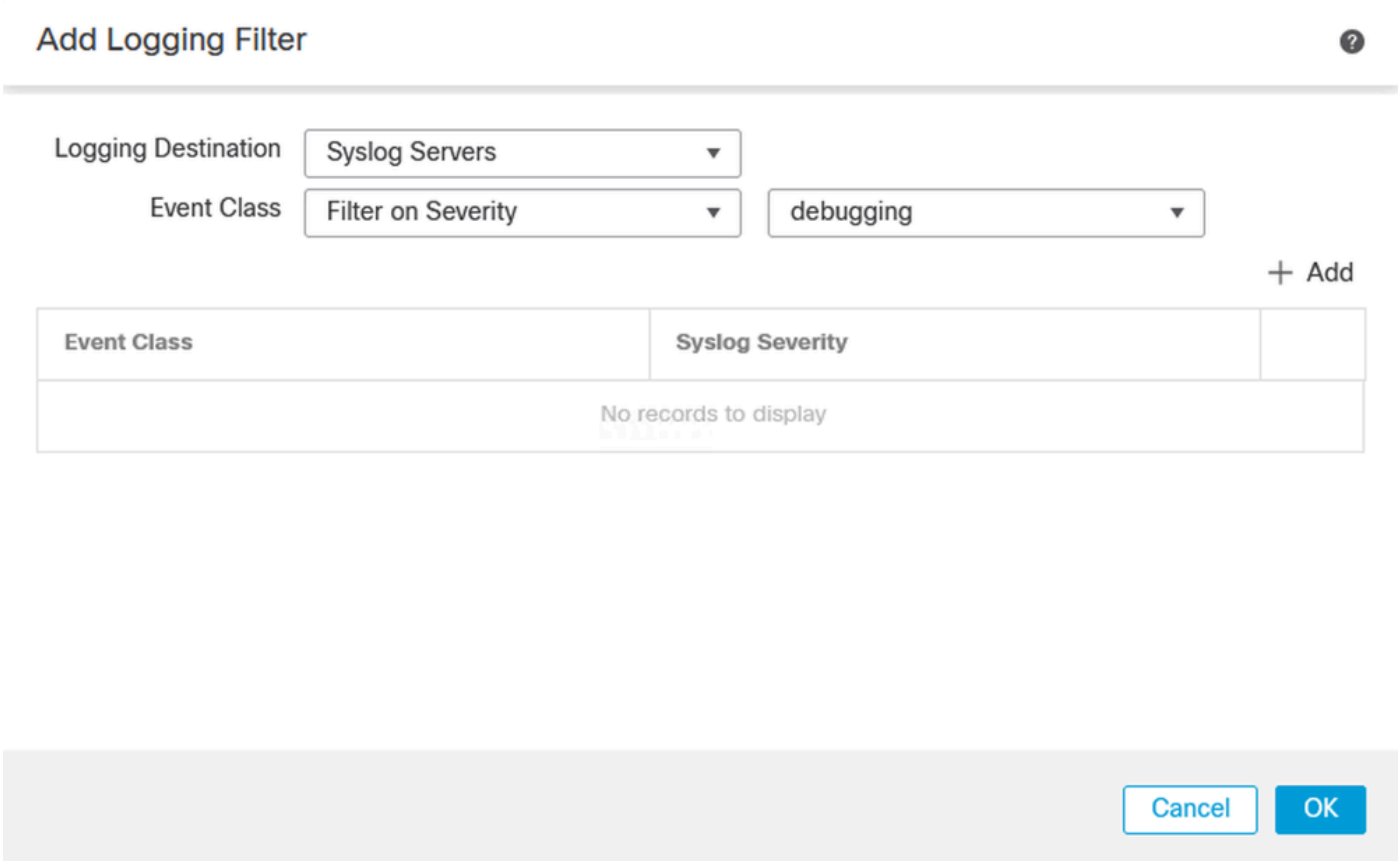


Configurações de plataforma no FTD - Servidor Syslog adicionado

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.



Configurações da plataforma em FTD - Adicionar destino de registro



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

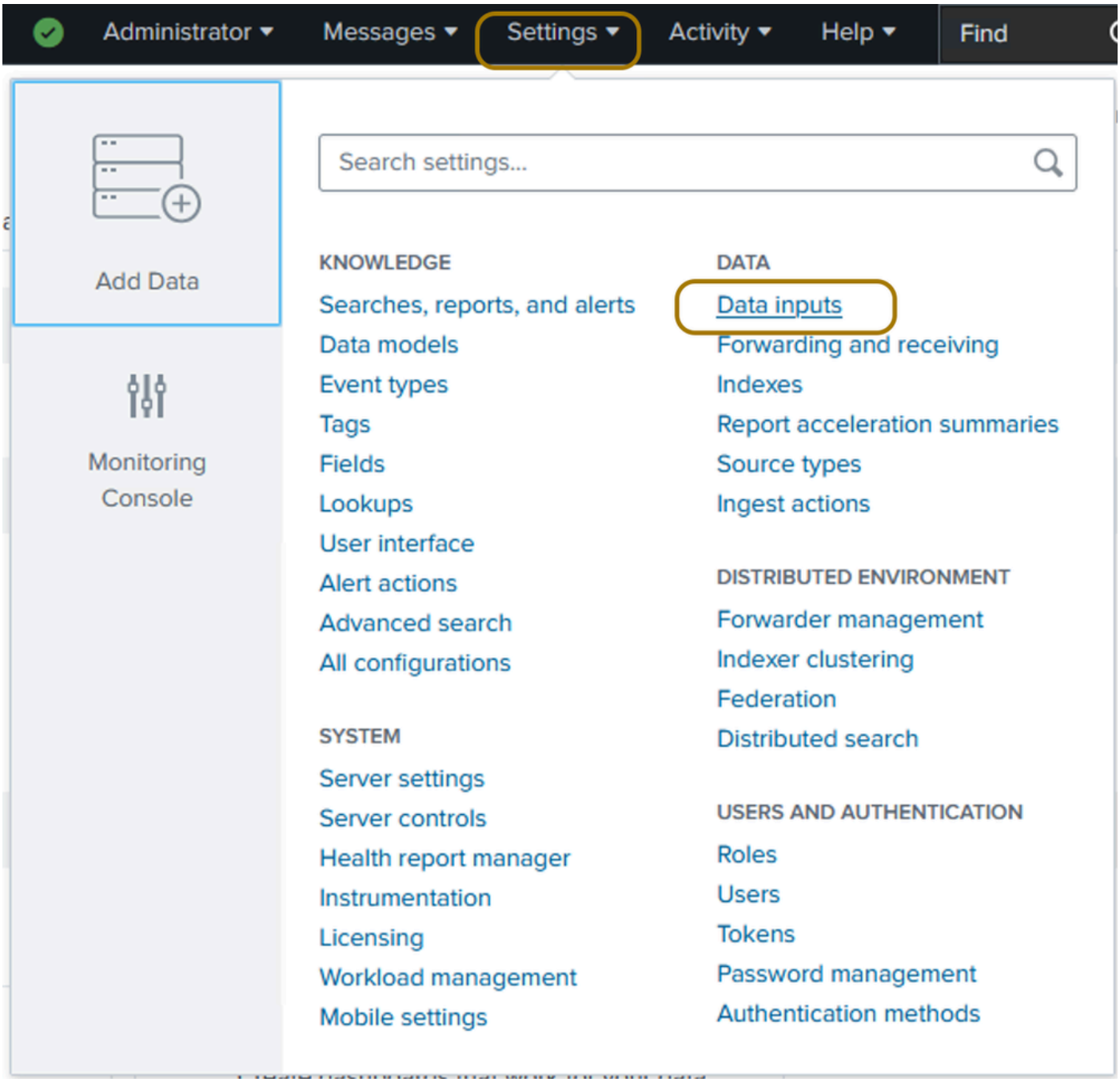
Implante as alterações de configuração da plataforma no FTD após concluir estas etapas.

Configurar uma Entrada de Dados na Instância do Splunk Enterprise

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

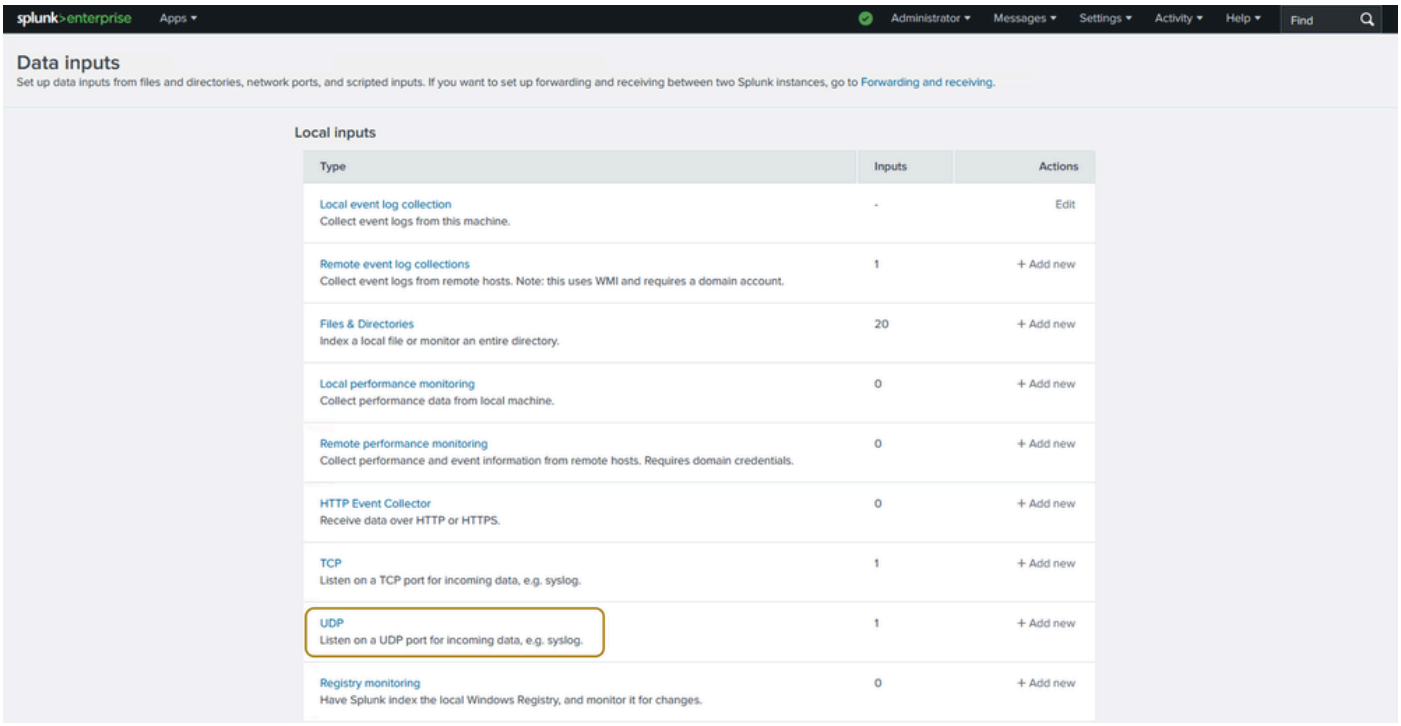
Página de Login da Interface da Web do Splunk

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.

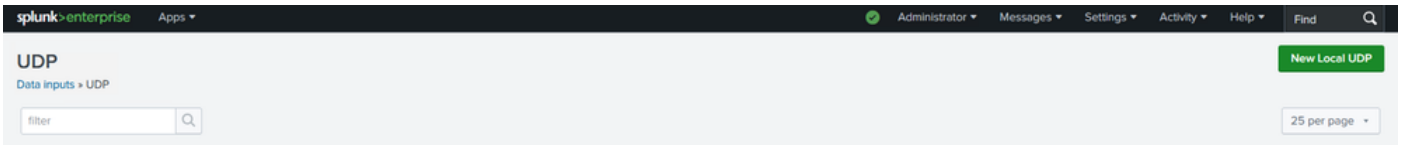


Navegar para Entradas de Dados no Splunk

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

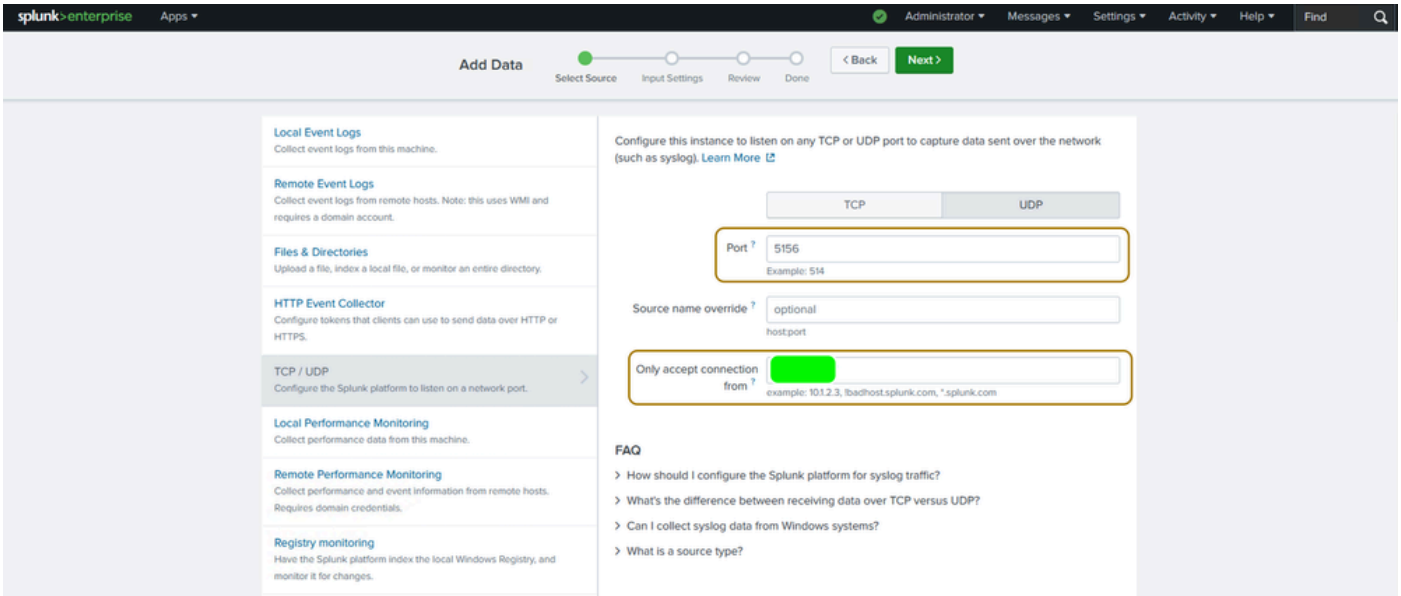


Clique em 'UDP' para uma Entrada de Dados UDP



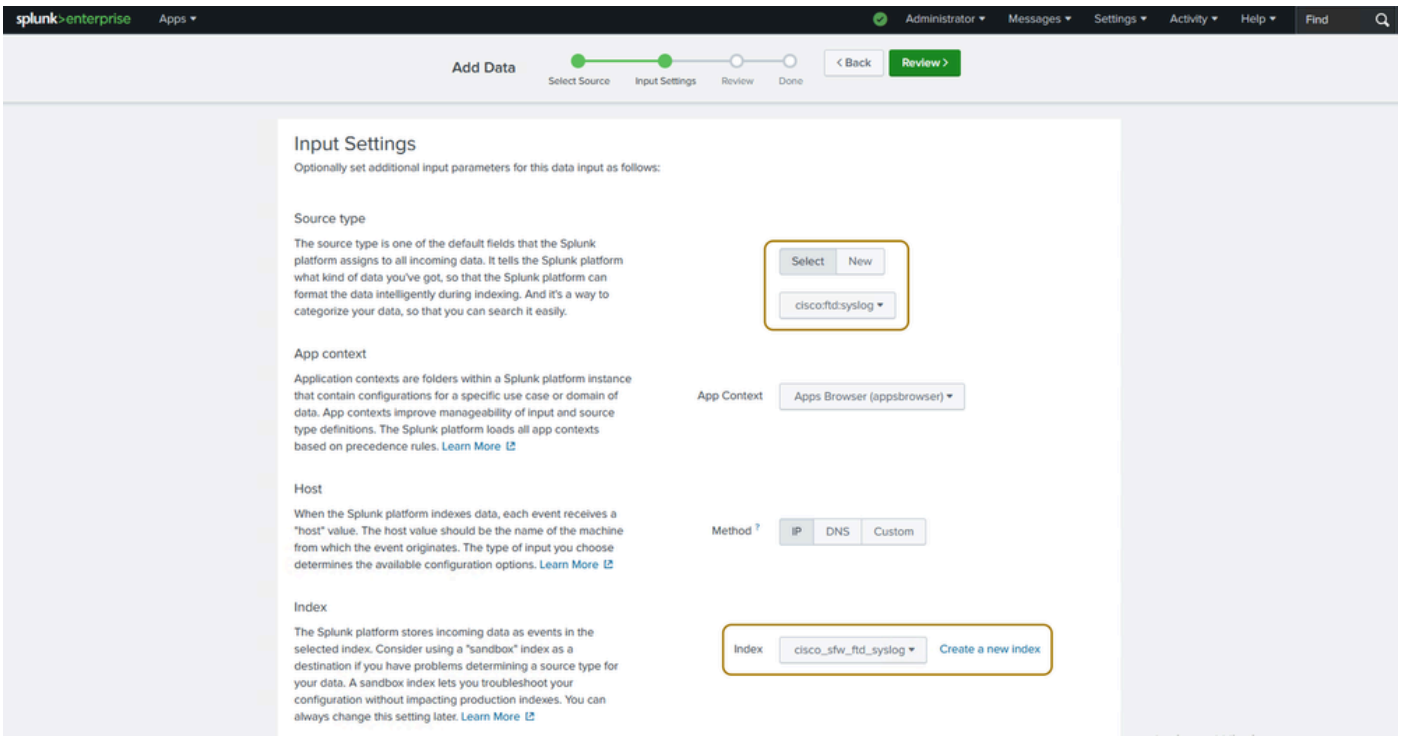
Criar uma Entrada 'Novo UDP Local'

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.



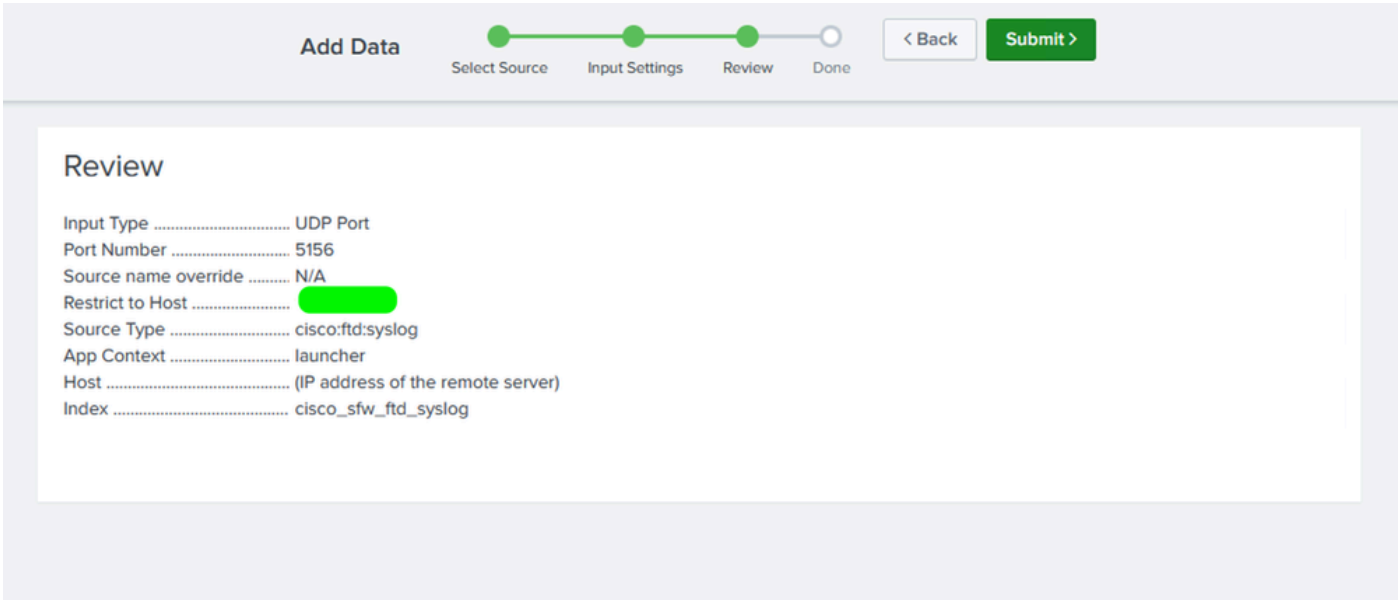
Especificar o endereço IP da Porta e do FTD

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.



Definir Configurações de Entrada de Dados

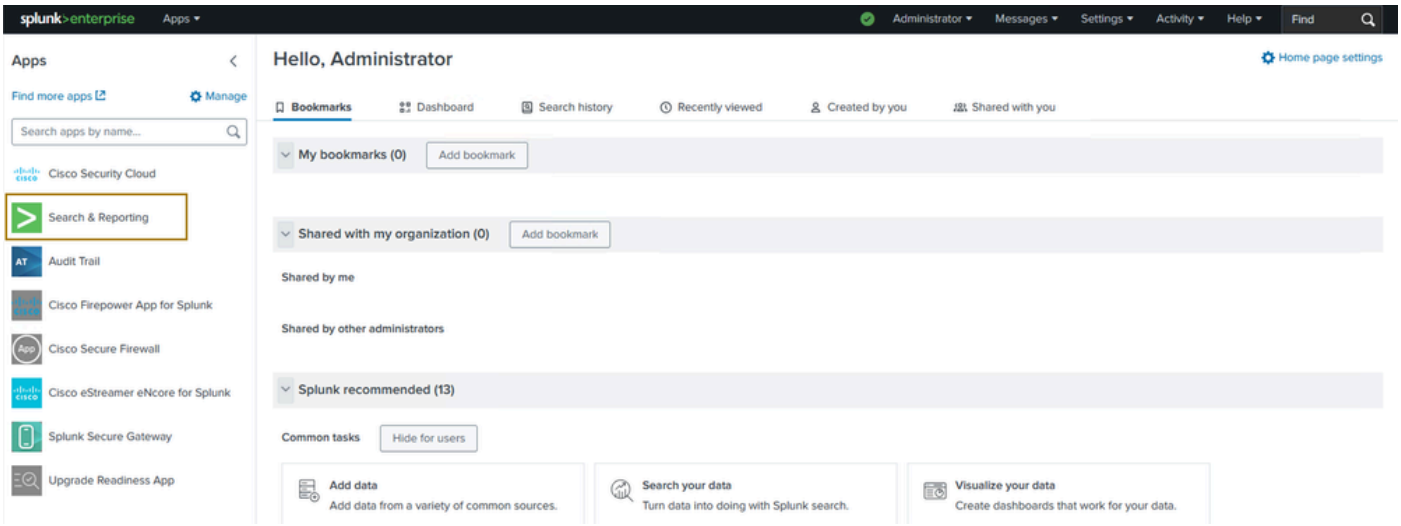
Etapa 6. Revise as configurações e clique em Enviar.



Revisar Configurações de Entrada de Dados

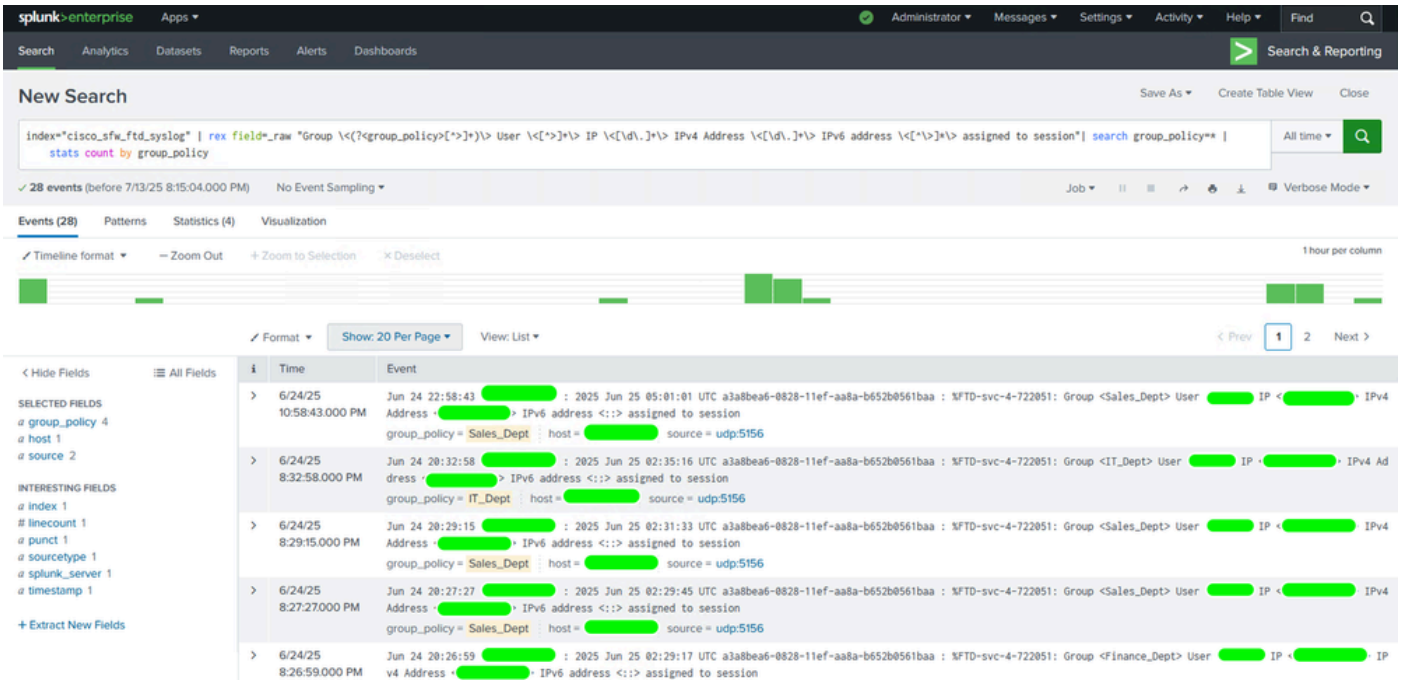
Executar consultas SPL e criar painéis

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

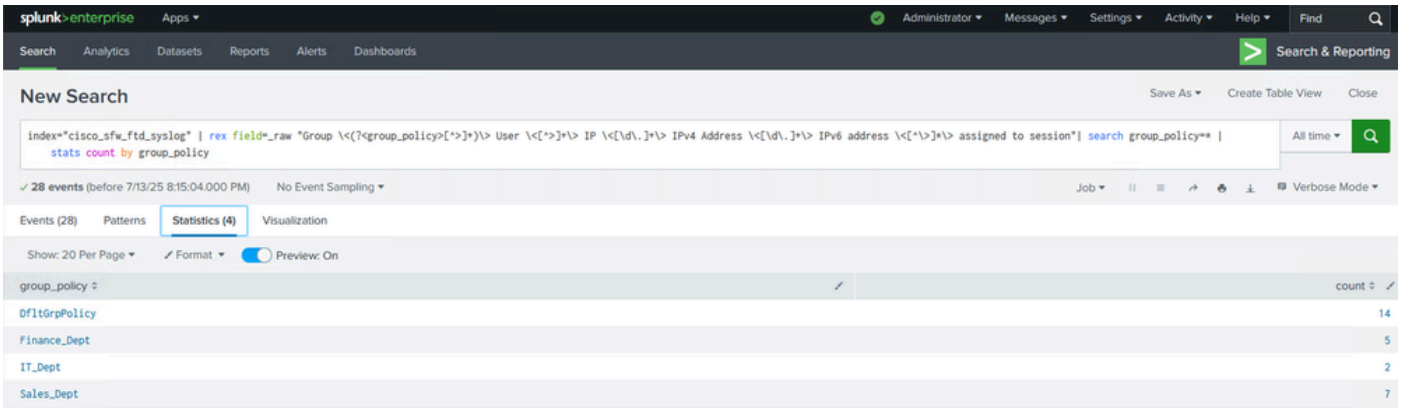


Navegue até o aplicativo Pesquisa e relatório

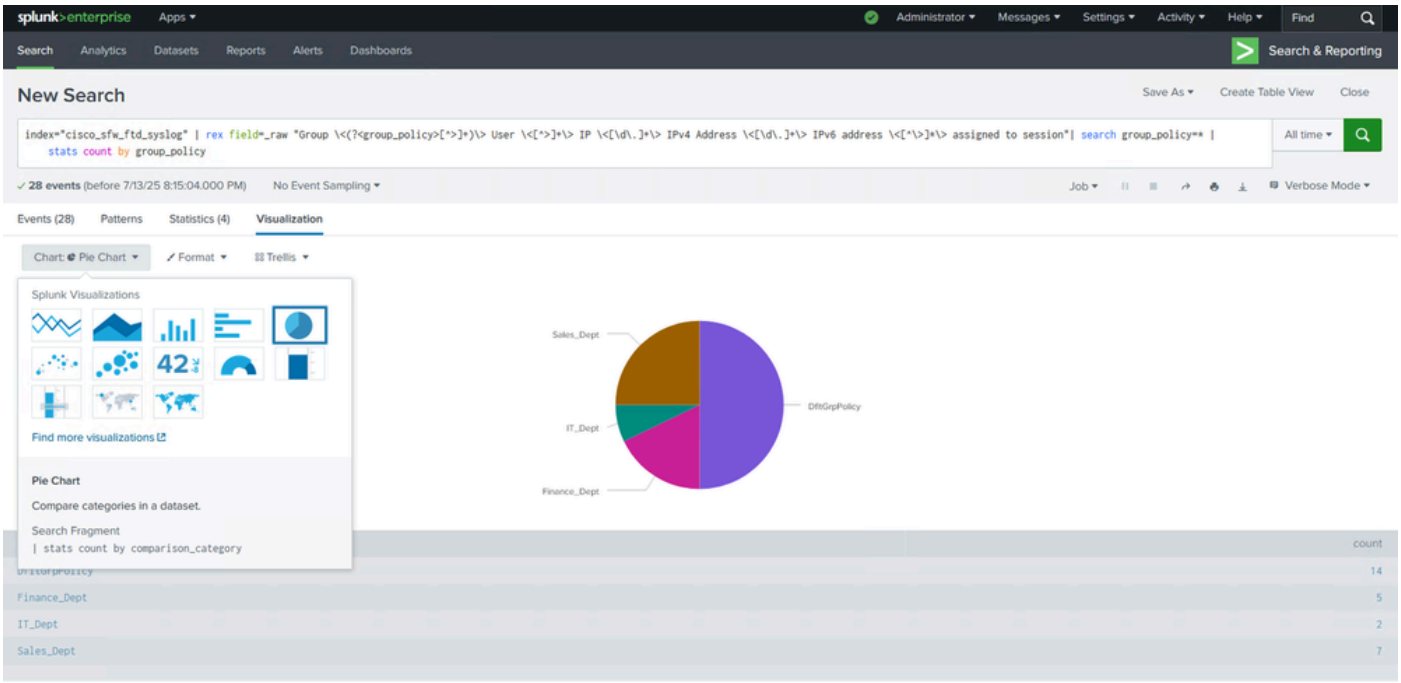
Etapa 2. Formule e execute uma consulta SPL de acordo com os dados que você deseja visualizar. Você poderá ver completamente cada log (no modo verboso) sob a guia Eventos, a contagem de conexões por política de grupo na guia Estatísticas e visualizar esses dados usando essas estatísticas sob a guia Visualização.



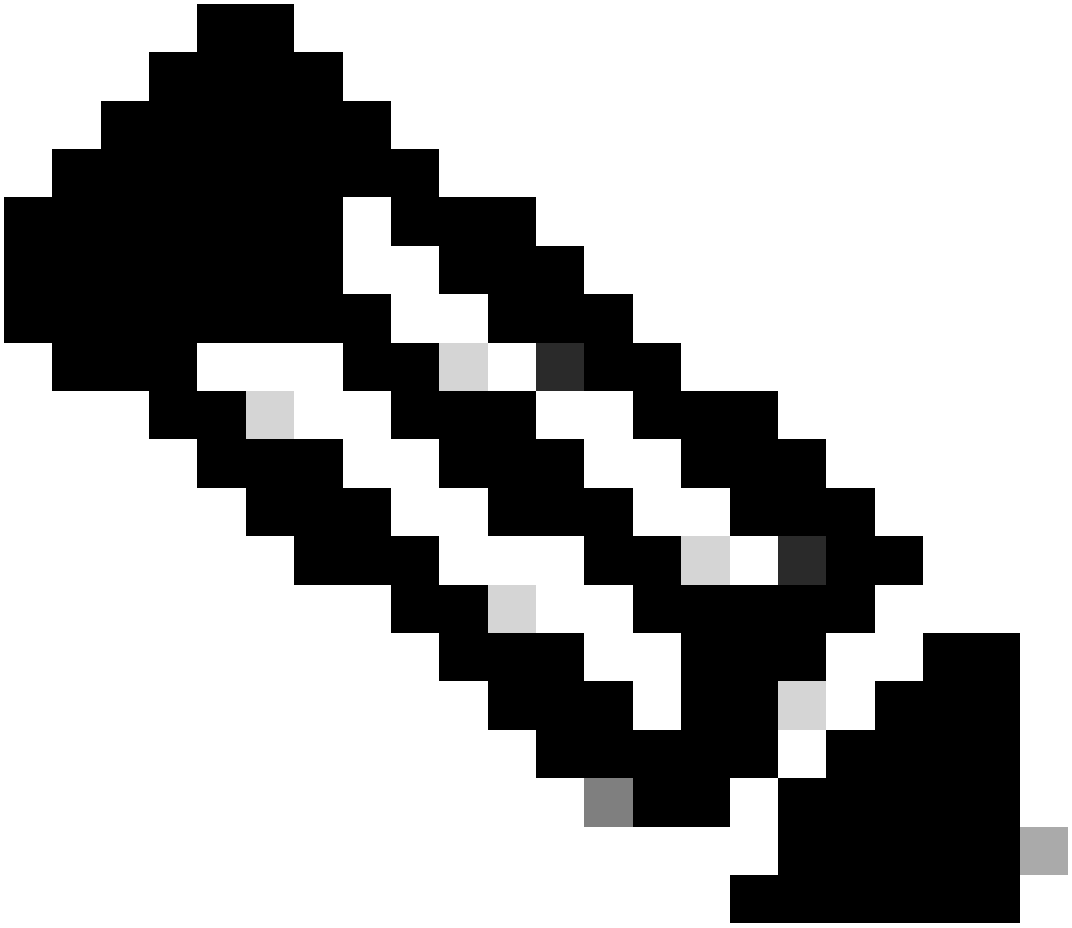
Procurar eventos usando consultas SPL



Verifique a guia Estatísticas

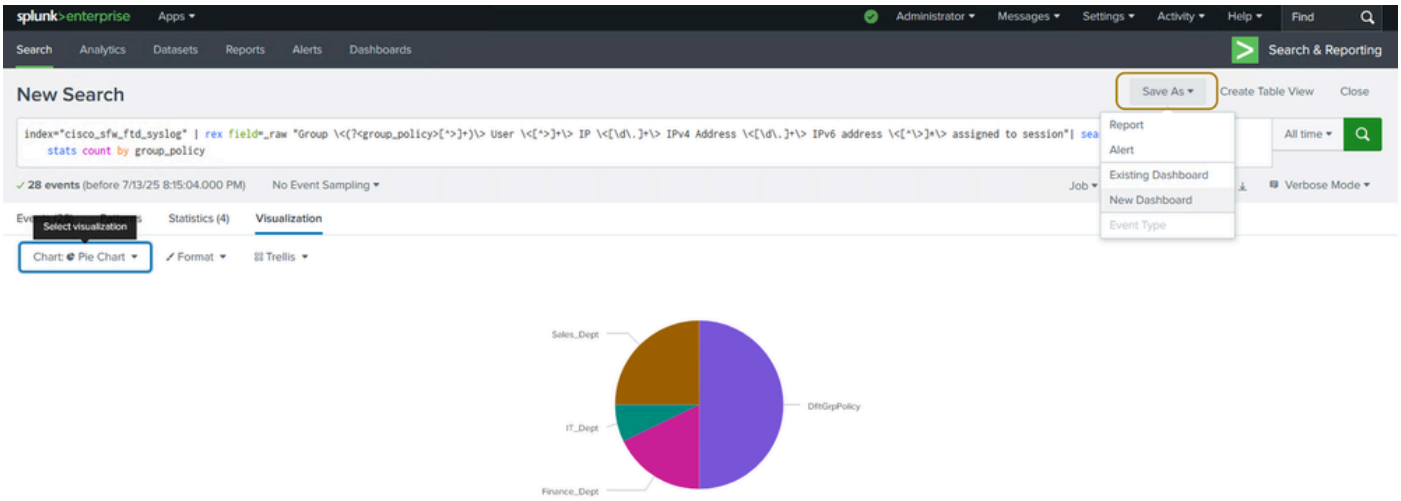


A guia Visualization (Visualização) mostrará o gráfico/gráfico



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

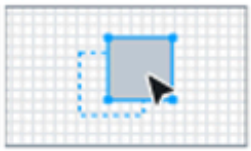
How do you want to build your dashboard? What's this?

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

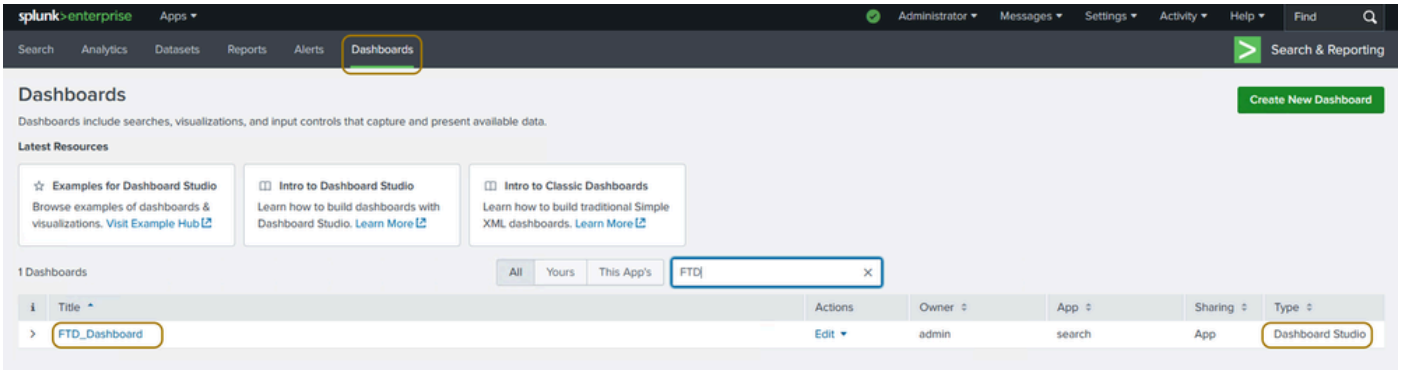
Cancel | Save to Dashboard

Configurações para o novo painel

: 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.

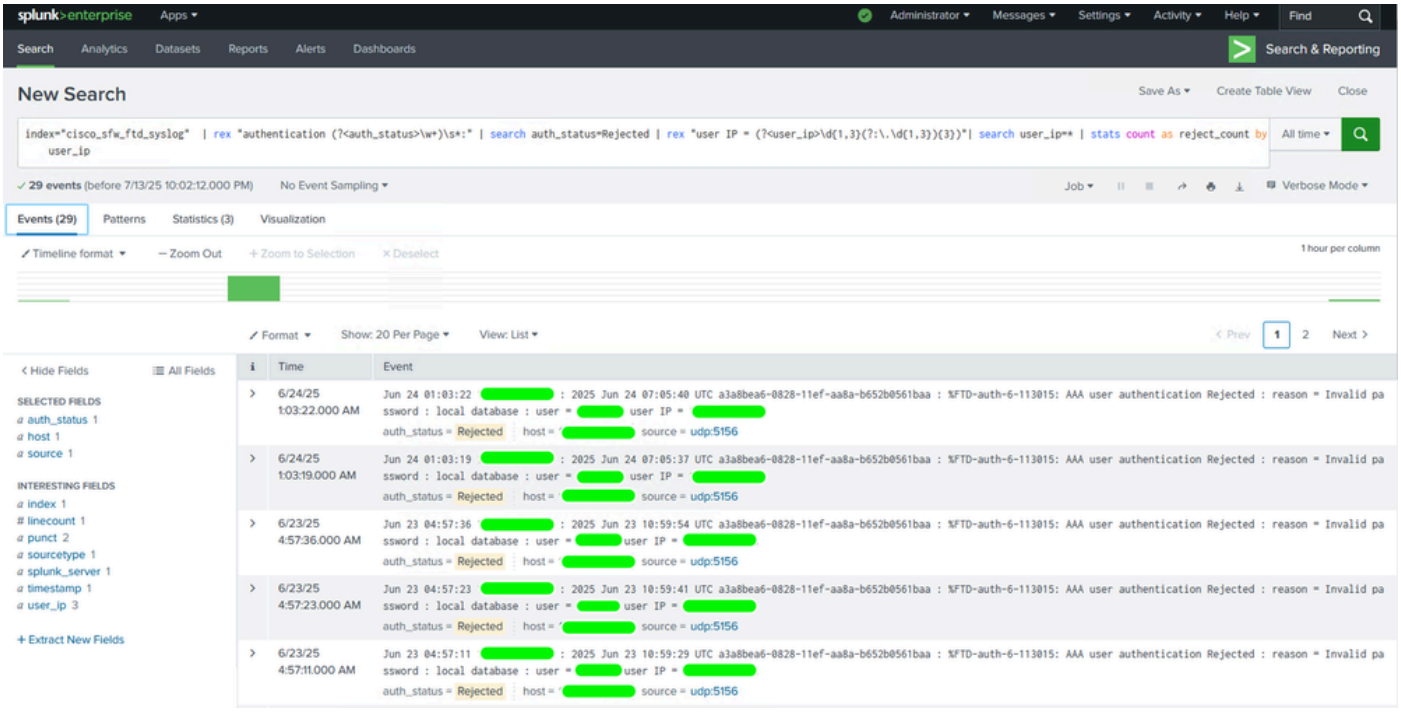
Etapa 6. Navegue até a guia Painel para pesquisar e escolher o painel que você criou. Clique nele para exibir, editar ou reorganizar seus painéis.



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 continu
Trigger Conditions: A

custom

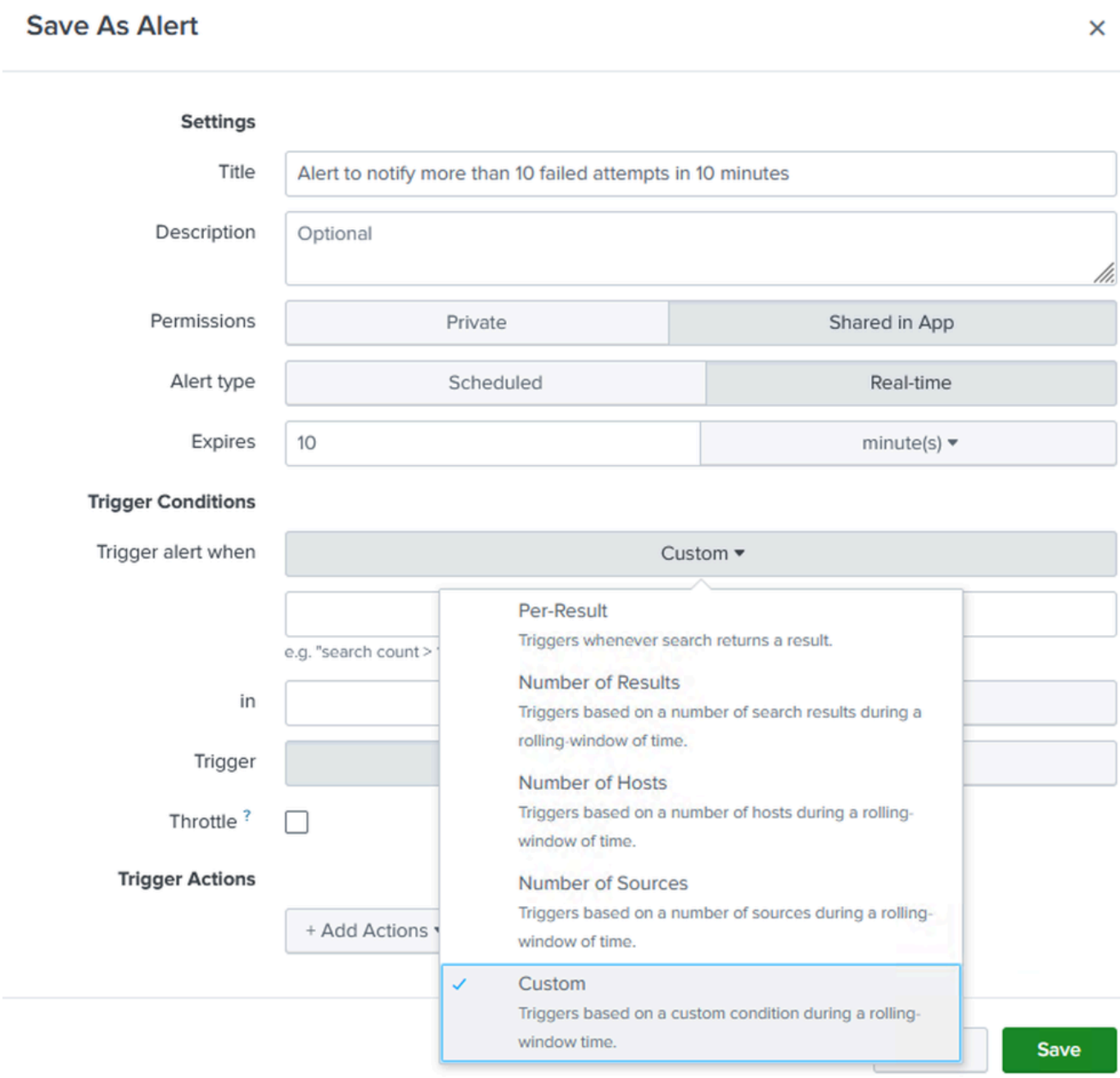
condition is used to search if the

reject_count

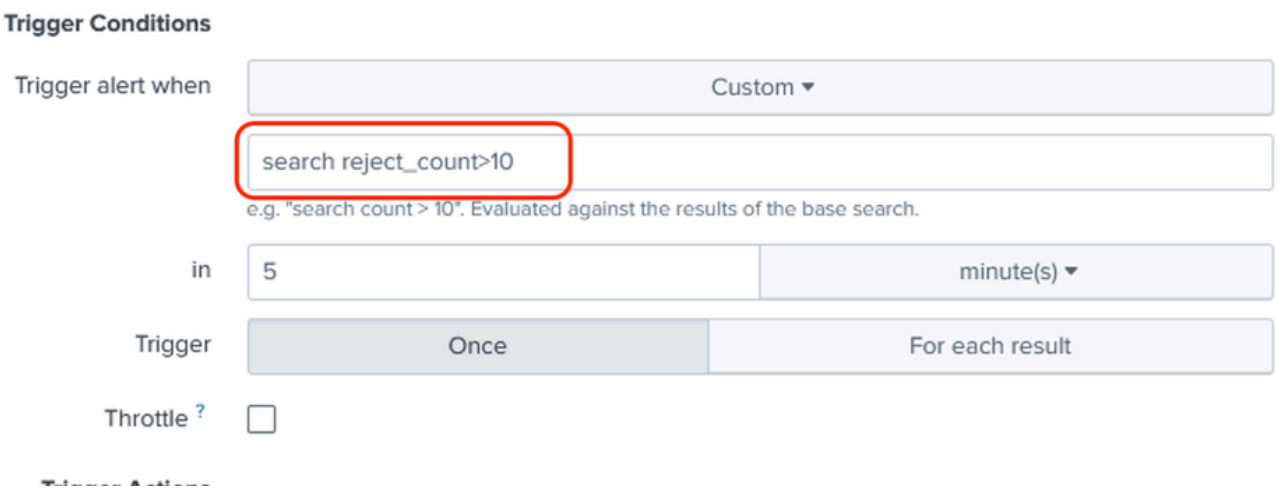
counter from the SPL query has exceeded 10 in the last 5 minutes for any IP address.
Trigger Actions: Set a trigger action such as

Add to Triggered Alerts, Send email, etc.

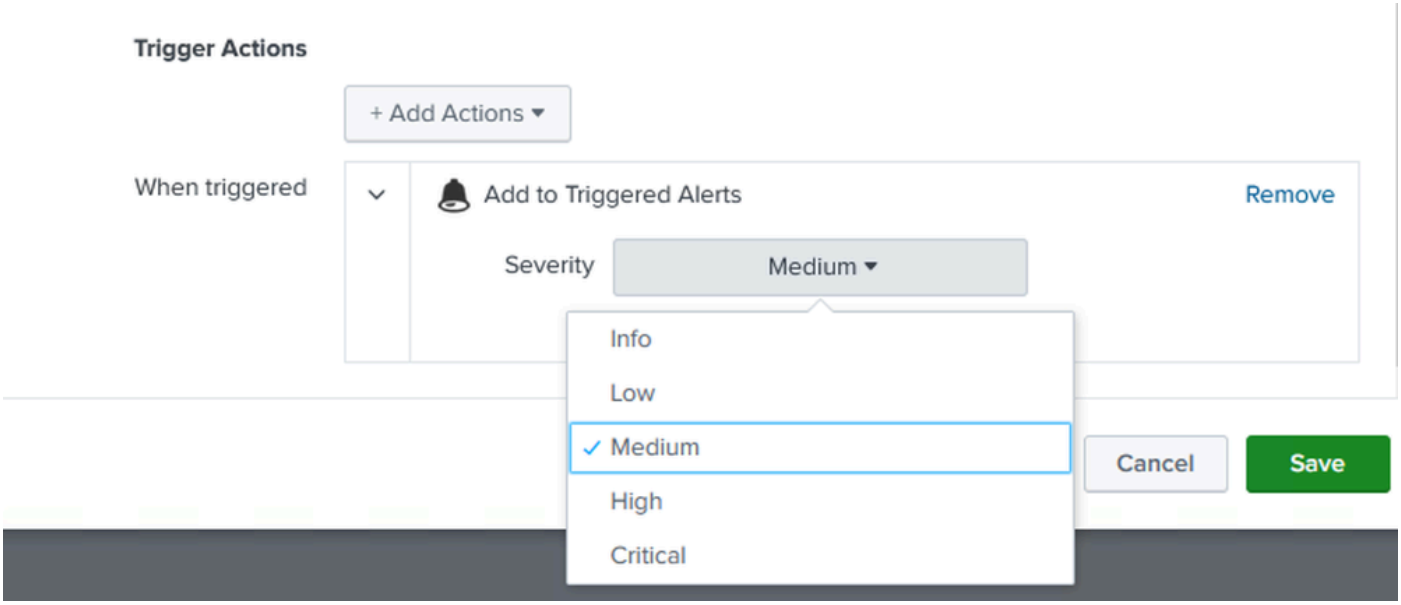
and set the alert severity as per your requirement.



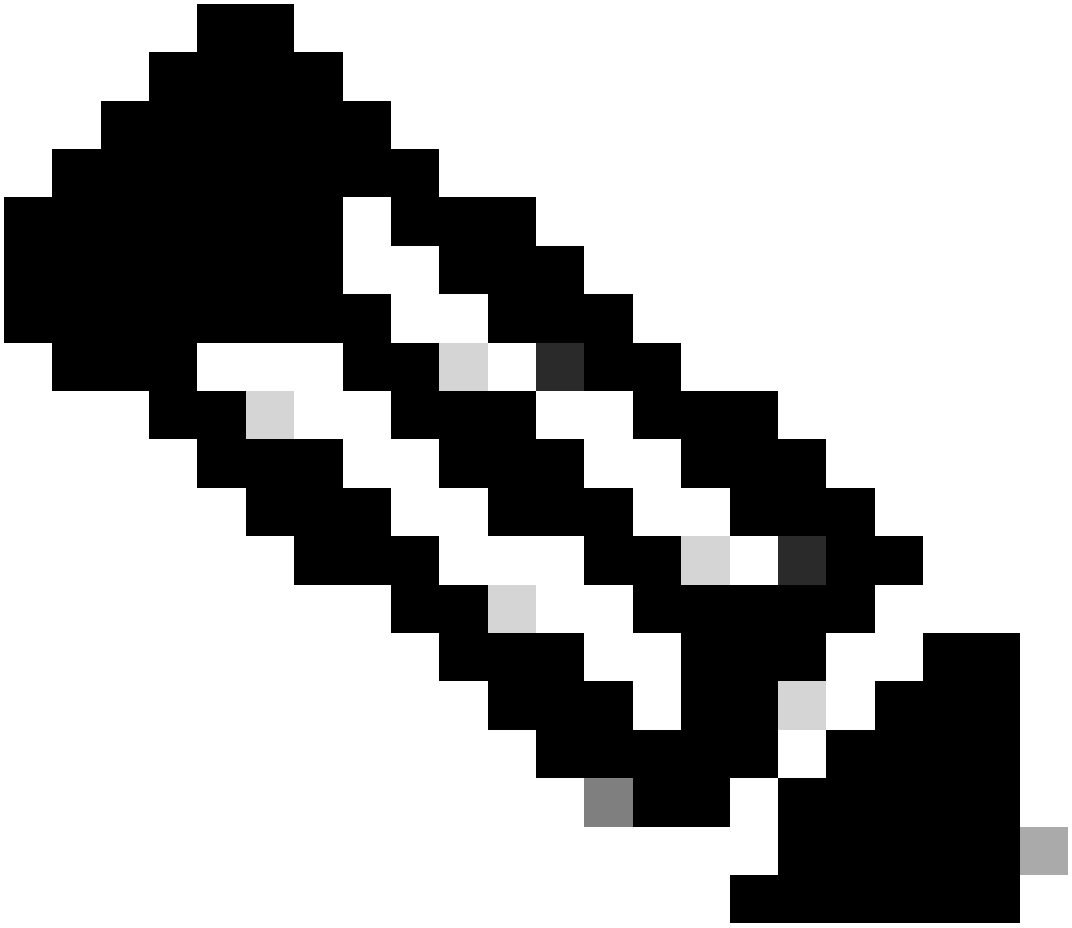
Configurações adicionais para a criação de alertas



Configurações adicionais para a criação de alertas



Configurações adicionais para a criação de alertas



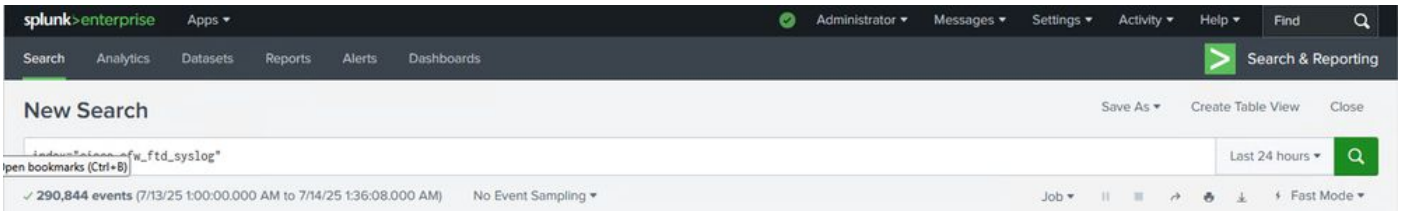
Note: Se você quiser disparar os alertas para cada resultado, terá que definir as configurações de limitação de acordo também.

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.

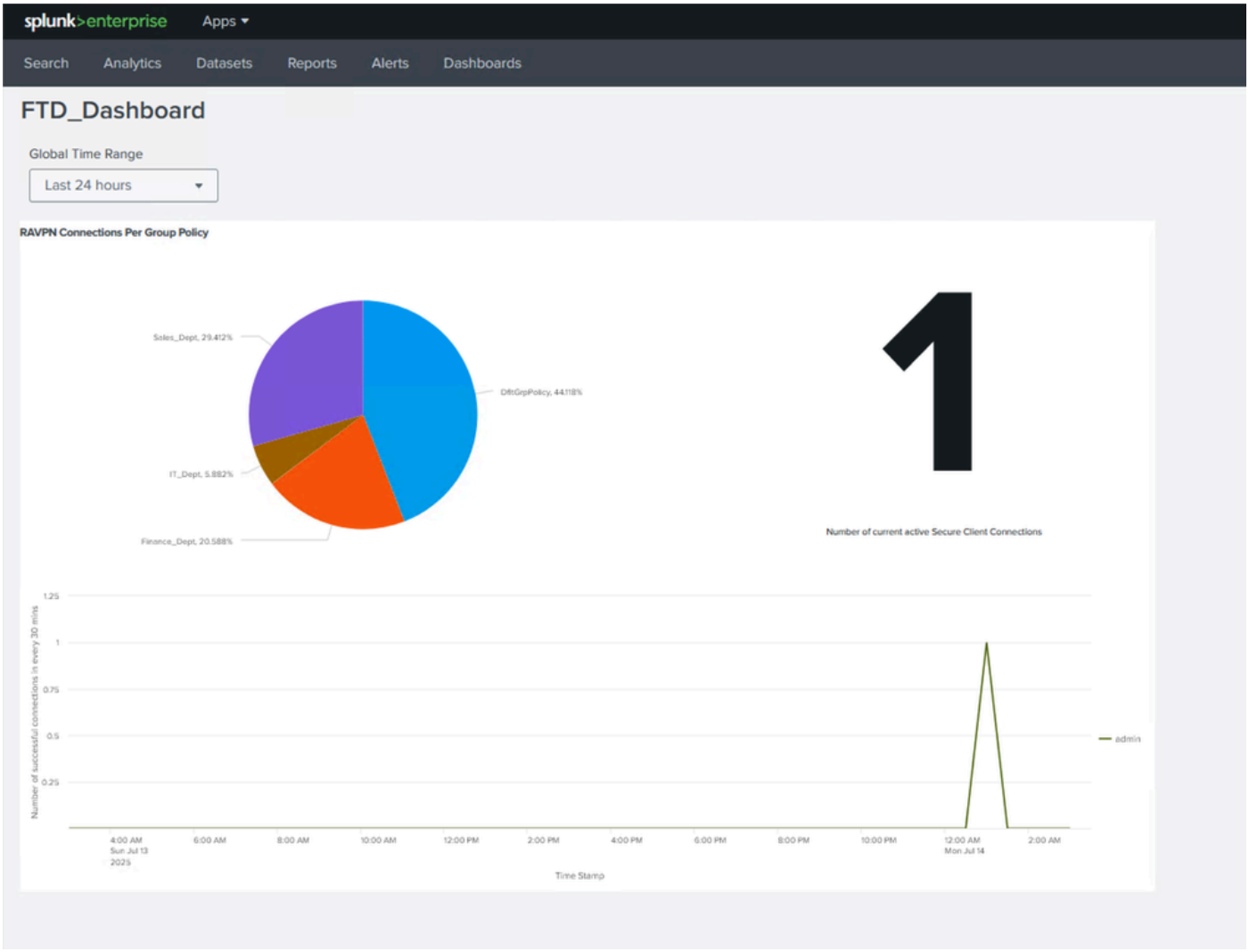


Verificar e exibir logs

Verificar e exibir logs

Exibir os painéis em tempo real

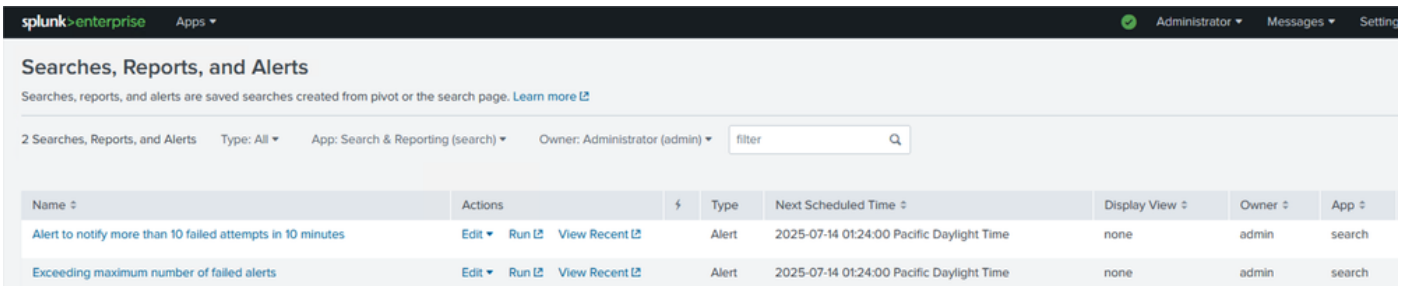
Você pode navegar até o painel personalizado que criou e ver a alteração em cada um dos painéis à medida que novos dados e logs são gerados a partir do FTD.



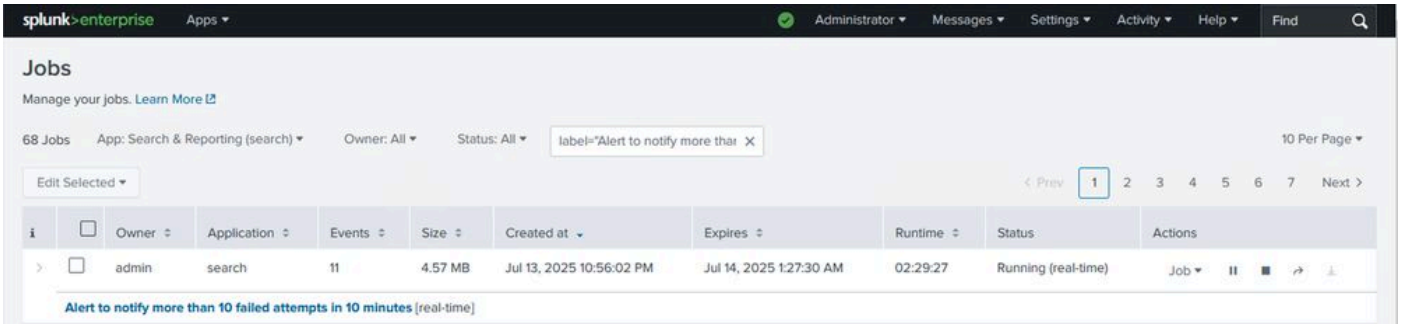
Exibir painéis

Verifique se algum alerta foi disparado

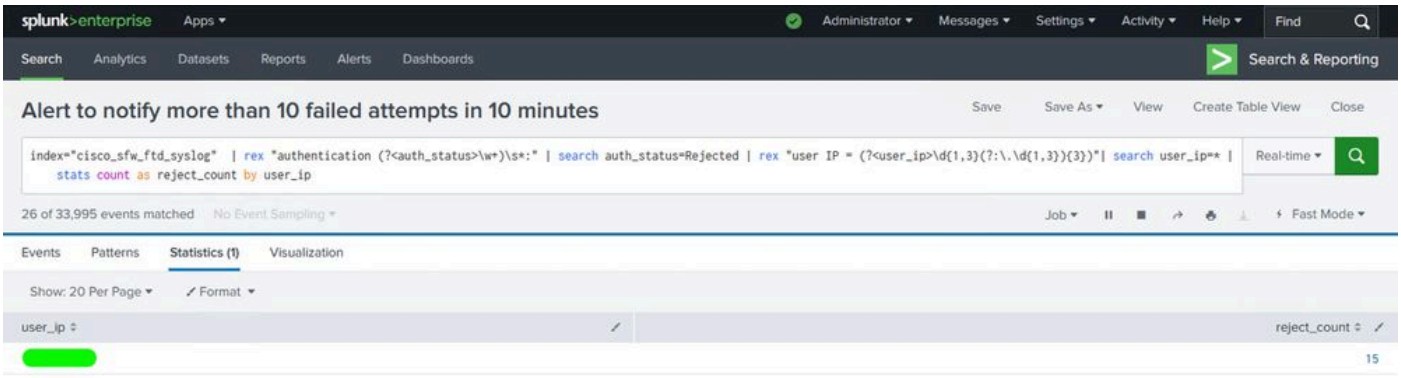
Para verificar as informações sobre os alertas, você pode navegar para as pesquisas de seção, relatórios e alertas para ver as informações de alerta recentes. Clique em View Recent para verificar mais sobre os trabalhos e pesquisas.



Verificar e exibir alertas



Verificar e exibir alertas



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.