FTDからのsyslogを使用したSplunkでのカスタムダッシュボードとアラートの作成

内容

はじめに

このドキュメントでは、FTDを設定してSplunkにsyslogを送信し、それらの口グを使用してカスタムダッシュボードとアラートを構築する手順を段階的に説明します。

前提条件

要件

この設定ガイドを読む前に、次の項目に関する知識があることが推奨されます。

- Syslog
- Splunkの検索処理言語(SPL)に関する基礎知識

また、このドキュメントでは、サーバにSplunk Enterpriseインスタンスがすでにインストールされており、Webインターフェイスにアクセスできることを前提としています。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- バージョン7.2.4上で動作するCisco Firepower Threat Defense(FTD)
- バージョン7.2.4で稼働するCisco Firepower Management Center(FMC)
- Windowsマシン上で動作するSplunk Enterpriseインスタンス（バージョン9.4.3）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。

背景説明

Cisco FTDデバイスは、侵入イベント、アクセスコントロールポリシー、接続イベントなどを対象とした詳細なsyslogを生成します。これらのログをSplunkと統合することで、ネットワークセキュリティ運用に関する強力な分析とリアルタイムのアラートが可能になります。

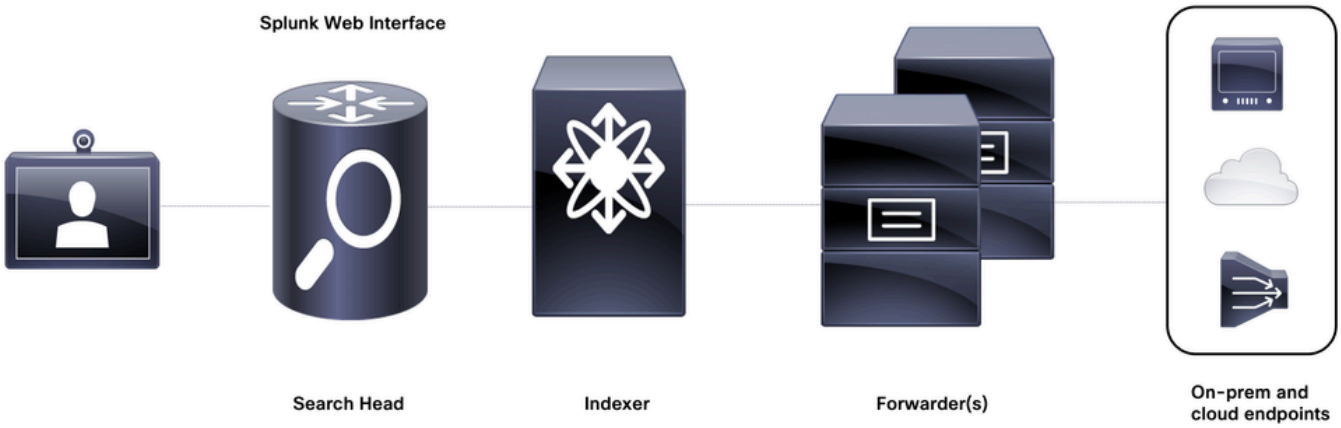
Splunkは、マシン生成データの取り込み、インデックス作成、検索、可視化を目的としたリアルタイムデータ分析プラットフォームです。 Splunkは、セキュリティ情報およびイベント管理(SIEM)ツールとしてサイバーセキュリティ環境に特に効果的です。その理由は次のとおりです。

- 規模に応じたログデータの取り込み
- SPLを使用した複雑な検索の実行
- ダッシュボードとアラートの作成
- セキュリティオーケストレーションおよびインシデント対応システムとの統合

Splunkは、構造化されたパイプラインを通じてデータを処理し、非構造化または半構造化されたマシンデータを有用で実用的なものにします。このパイプラインの主なステージは、一般にIPISと呼ばれます。これは、次を表します。

- 入力
- 解析
- インデックス
- 検索

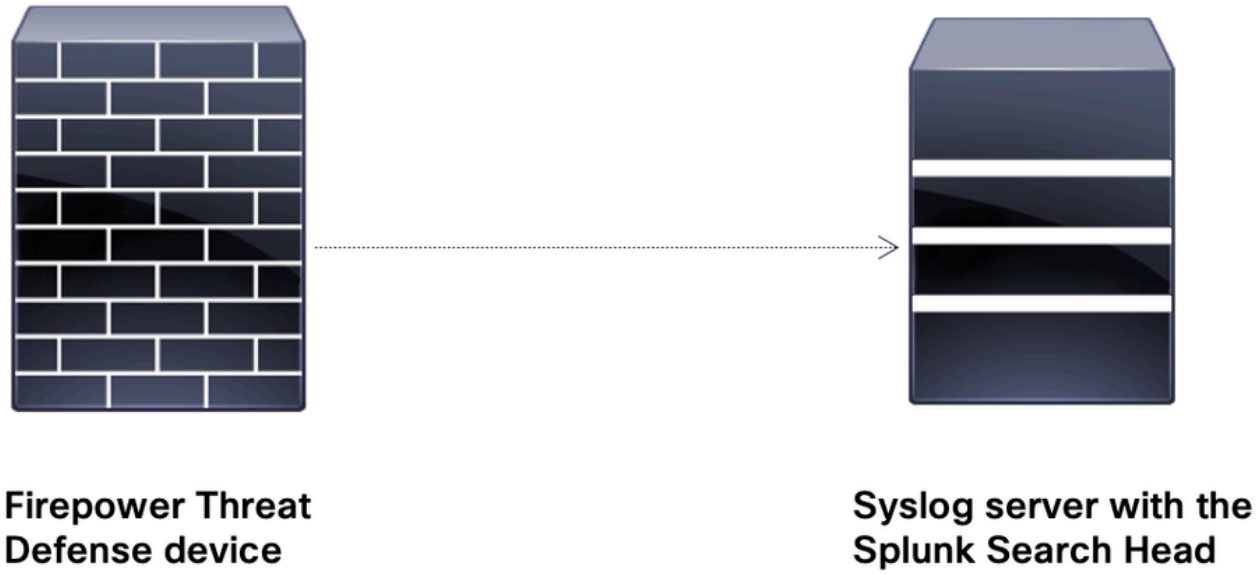
次の図は、IPISパイプラインの実現に使用される基盤となるアーキテクチャの主要なコンポーネントを示しています。



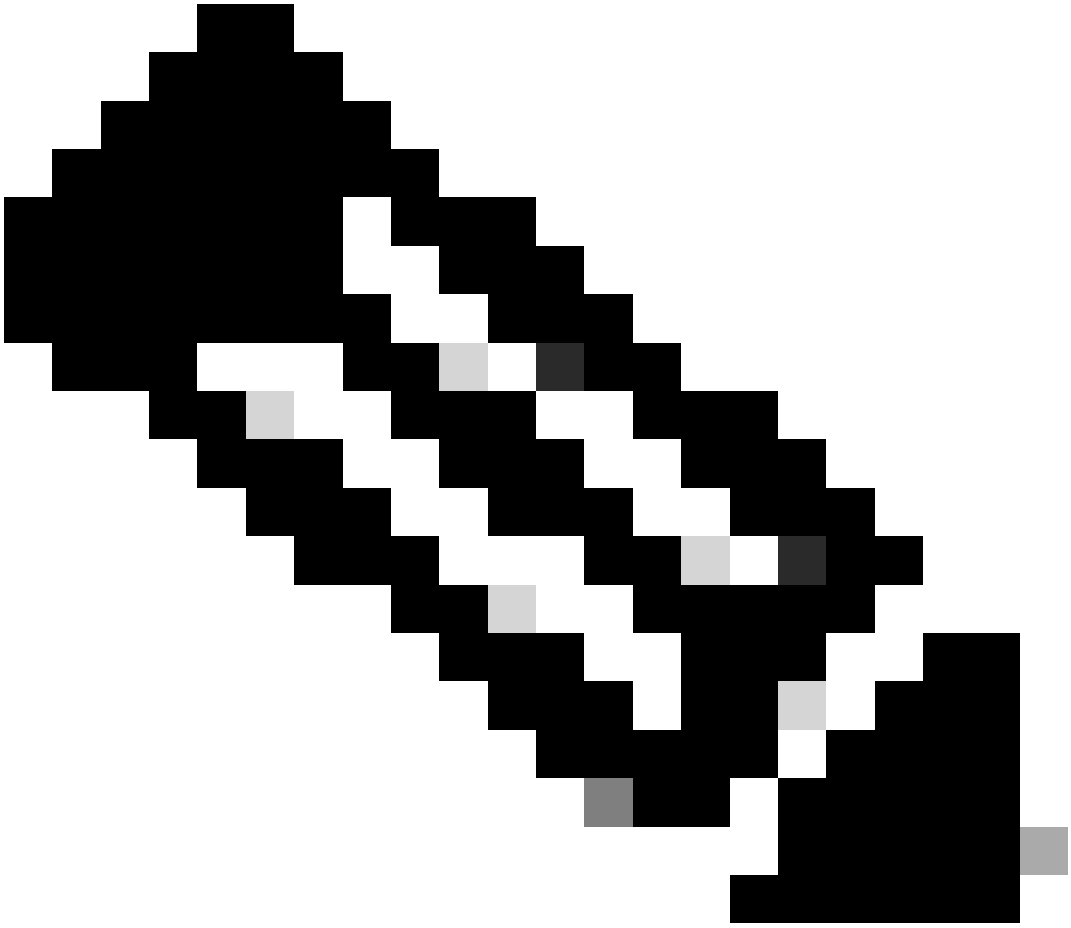
Splunkの基盤アーキテクチャ

設定

ネットワーク図



ネットワーク図

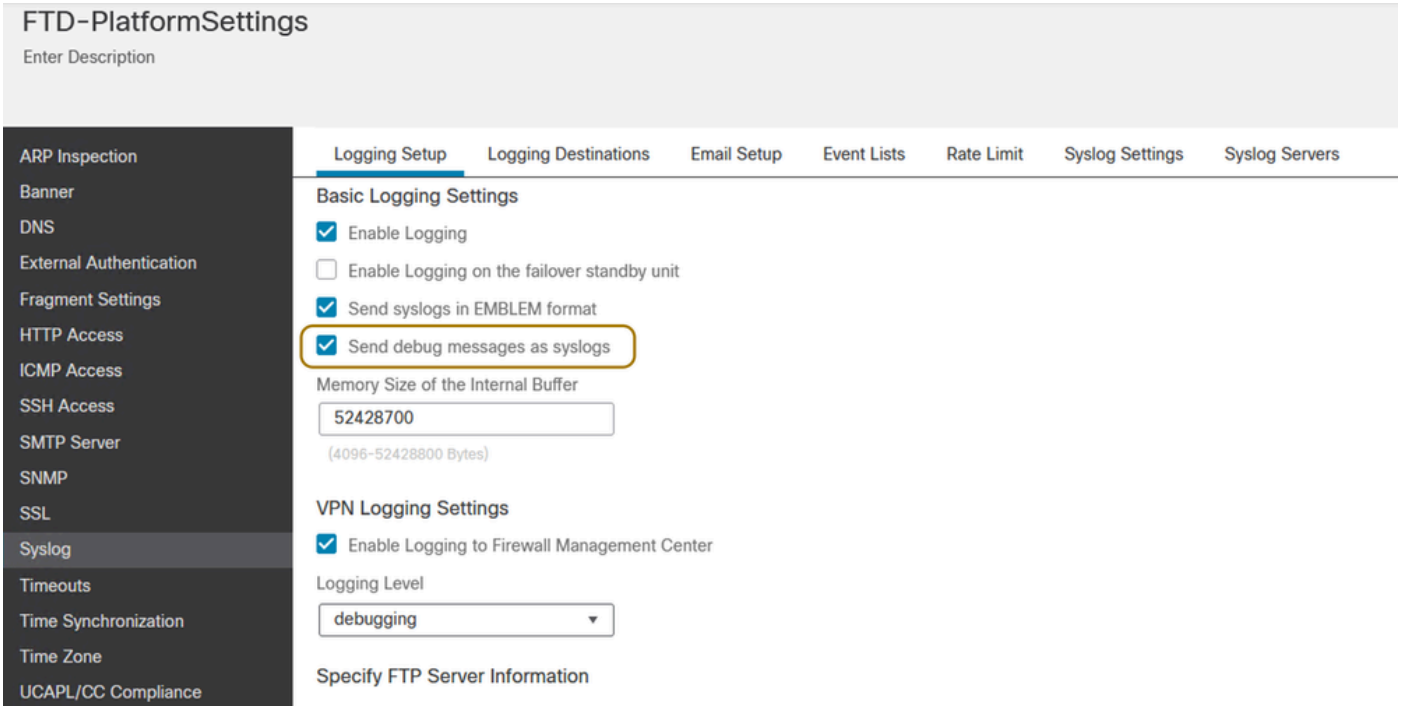


注：このドキュメントのラボ環境では、フォワーダとインデクサの個別のインスタンスは必要ありません。Splunk Enterpriseインスタンスがインストールされ ているWindowsマシン（つまりsyslogサーバ）が、インデクサおよび検索ヘッドとして機能します。

コンフィギュレーション

FTDのsyslog設定の設定

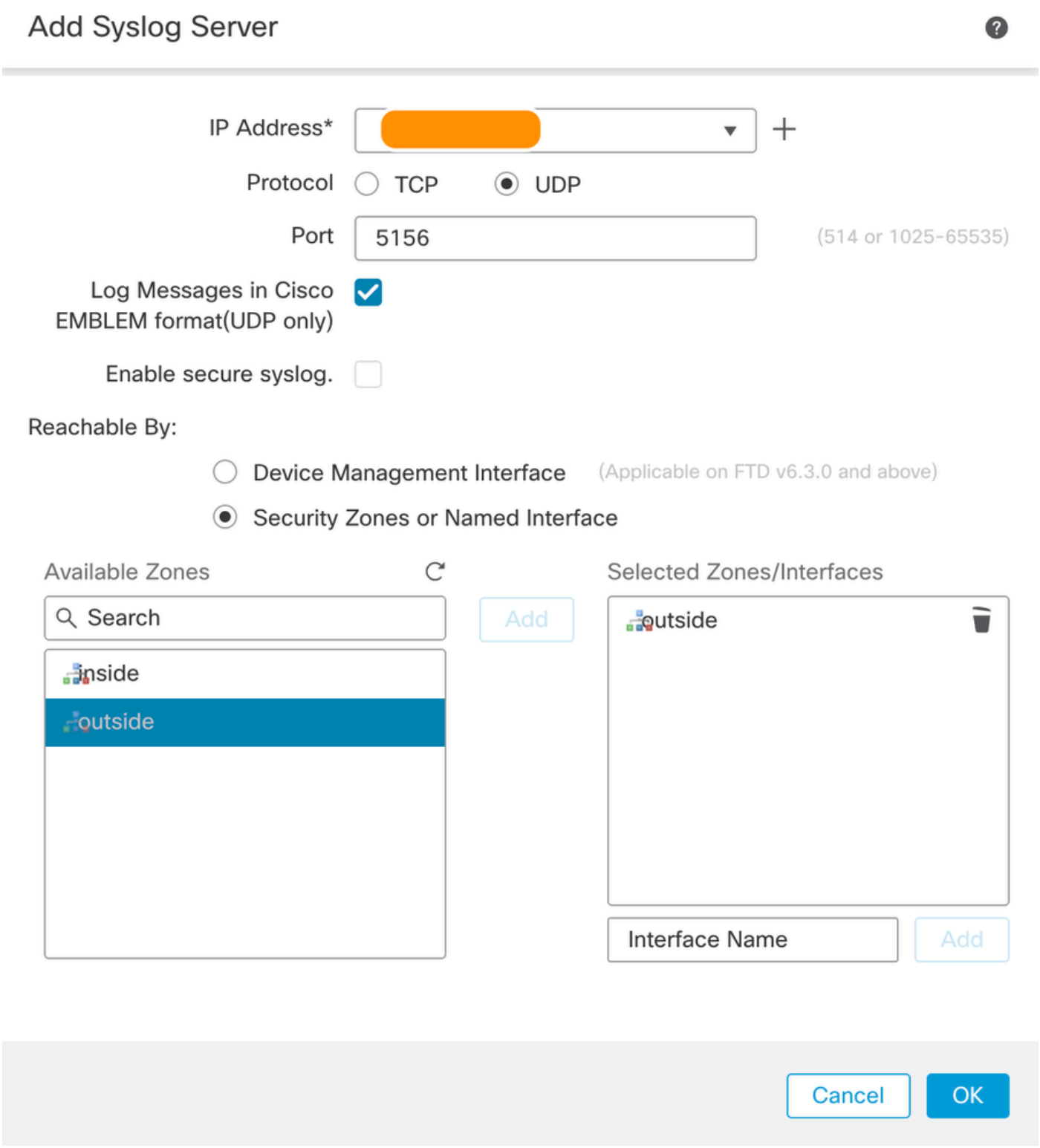
ステップ 1：Splunkインスタンスが実行されているsyslogサーバにログを送信するため、FTDのFMCでDevices > Platform Settingsの下に予備syslog設定を設定します。



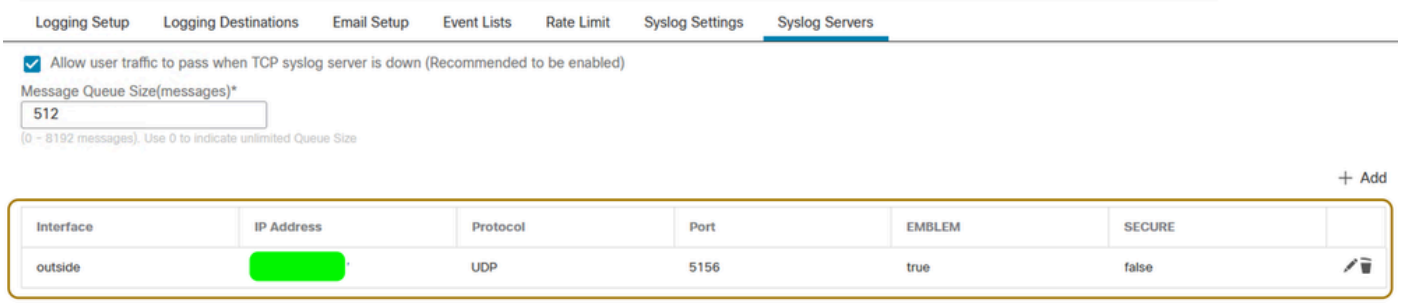
FTDのプラットフォーム設定：syslog

ステップ 2：Splunk Enterpriseインスタンスがインストールされ、Syslogサーバとして実行されているマシンのIPアドレスを設定します。前述のようにフィールドを定義します。

```
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
```

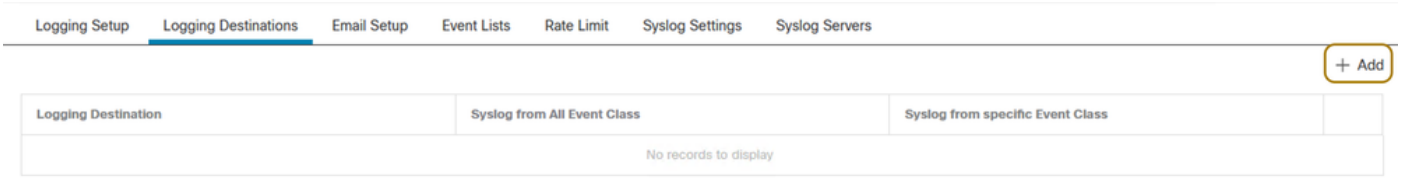


FTDのプラットフォーム設定 – syslogサーバの追加

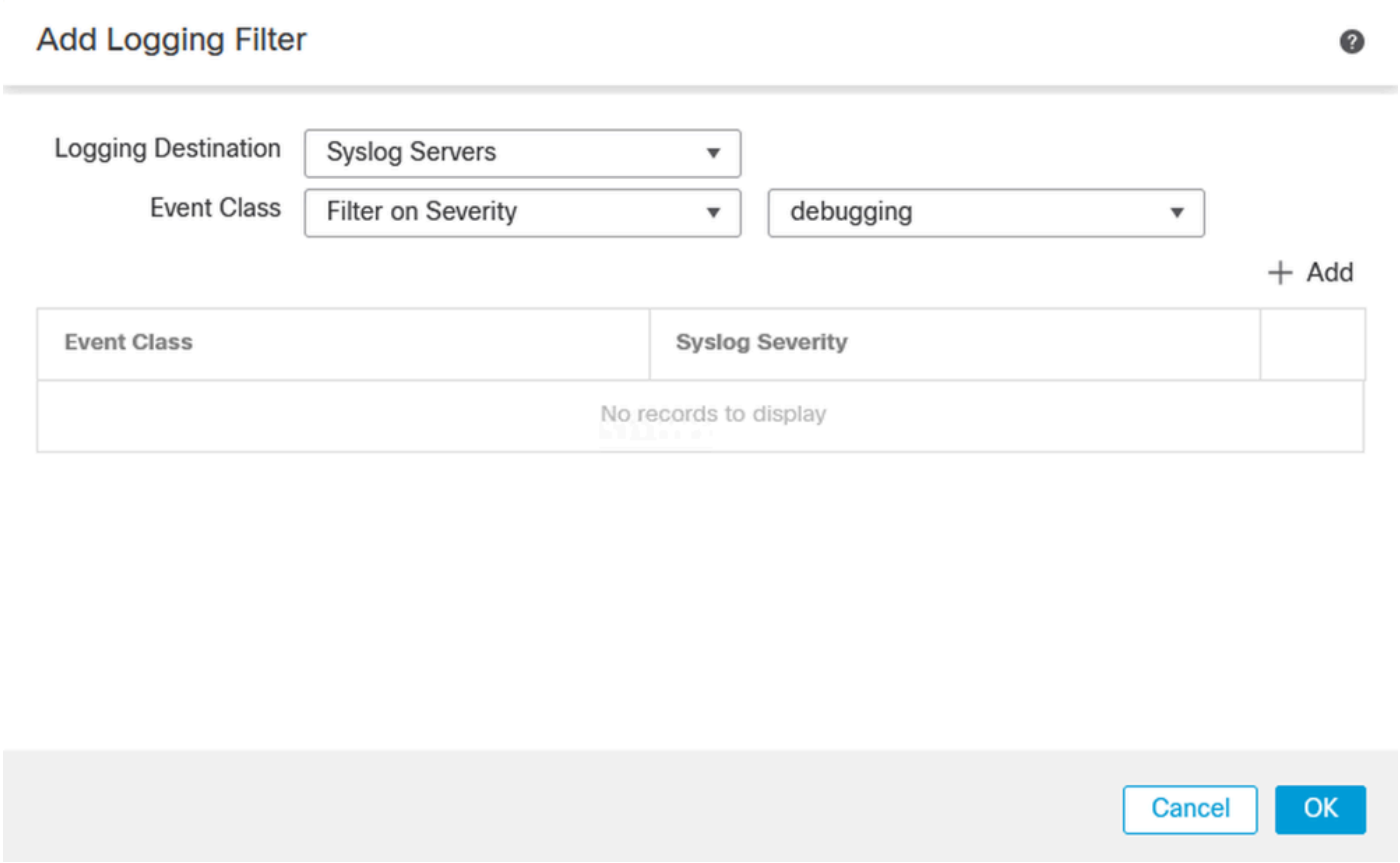


FTDのプラットフォーム設定：syslogサーバが追加されました

ステップ 3：Syslogサーバのロギング宛先を追加します。ログレベルは、選択または使用例に応じて設定できます。



FTDのプラットフォーム設定：ロギング宛先の追加



FTDのプラットフォーム設定：ロギング宛先の重大度レベルの設定

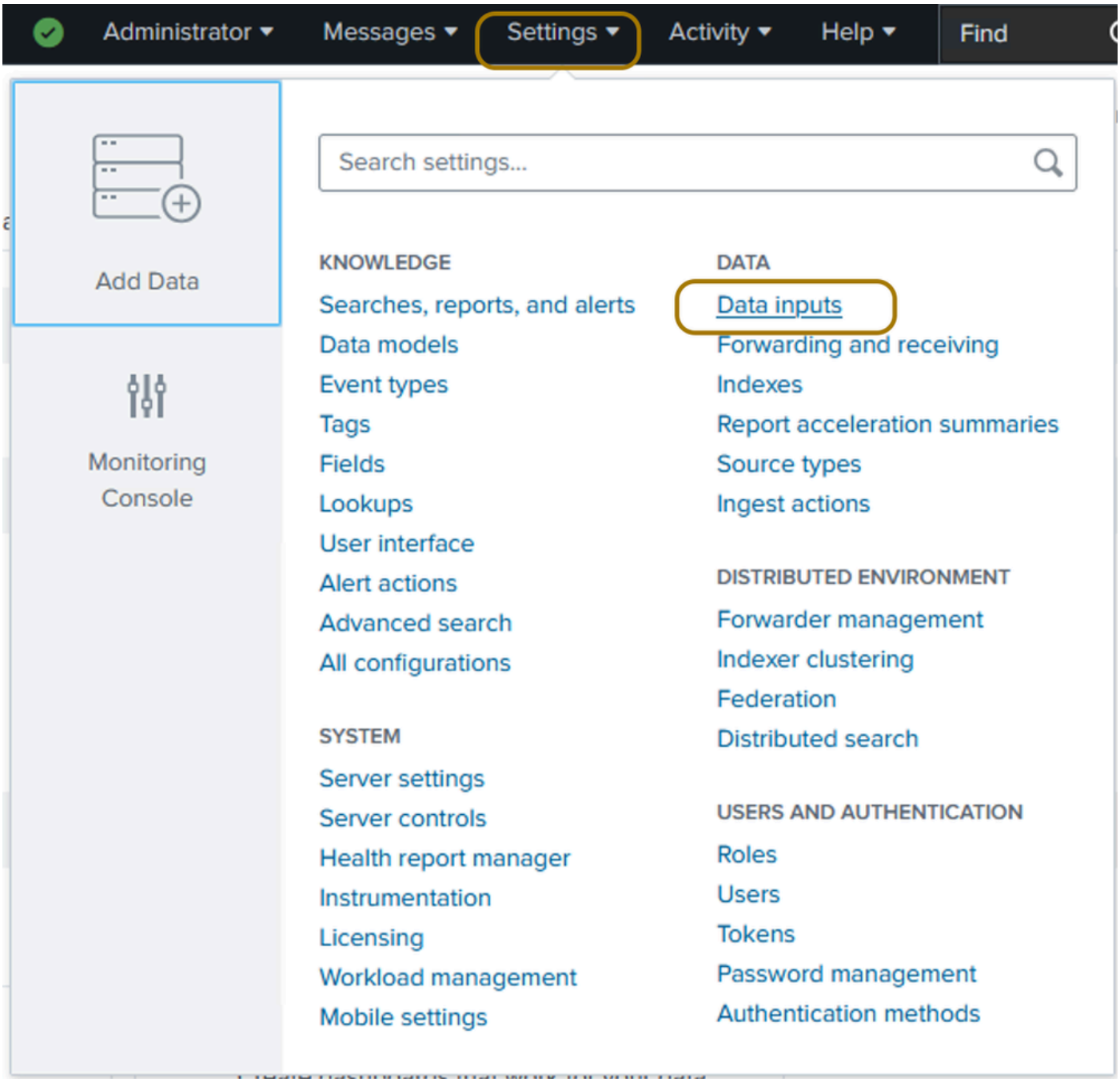
次の手順を実行した後、プラットフォーム設定の変更をFTDに展開します。

Splunk Enterpriseインスタンスでのデータ入力の設定

ステップ 1：Splunk EnterpriseインスタンスのWebインターフェイスにログインします。

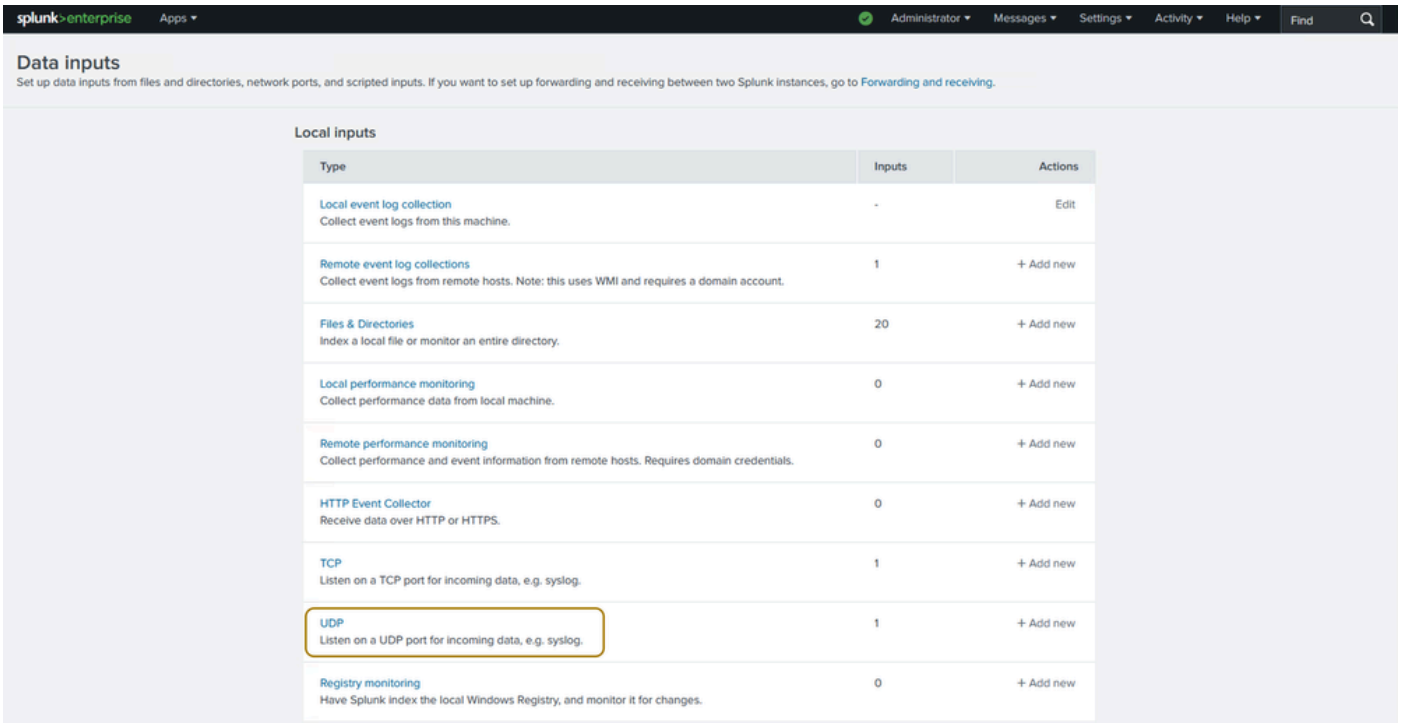
Splunk Webインターフェイスログインページ

ステップ 2：Splunkにsyslogを保存し、インデックスを作成できるように、データ入力を定義する必要があります。ログイン後、Settings > Data > Data Inputsの順に選択します。

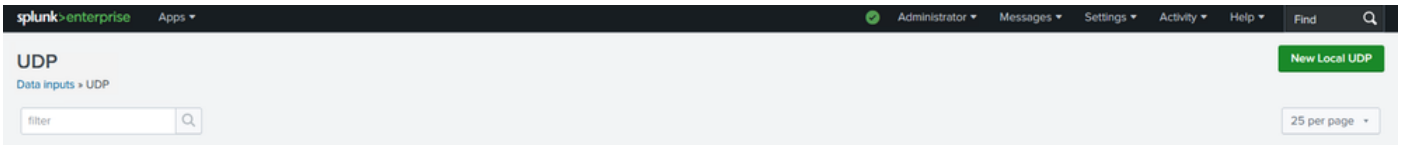


Splunkのデータ入力へ移動

ステップ 3：UDPを選択し、表示される次のページでNew Local UDPをクリックします。

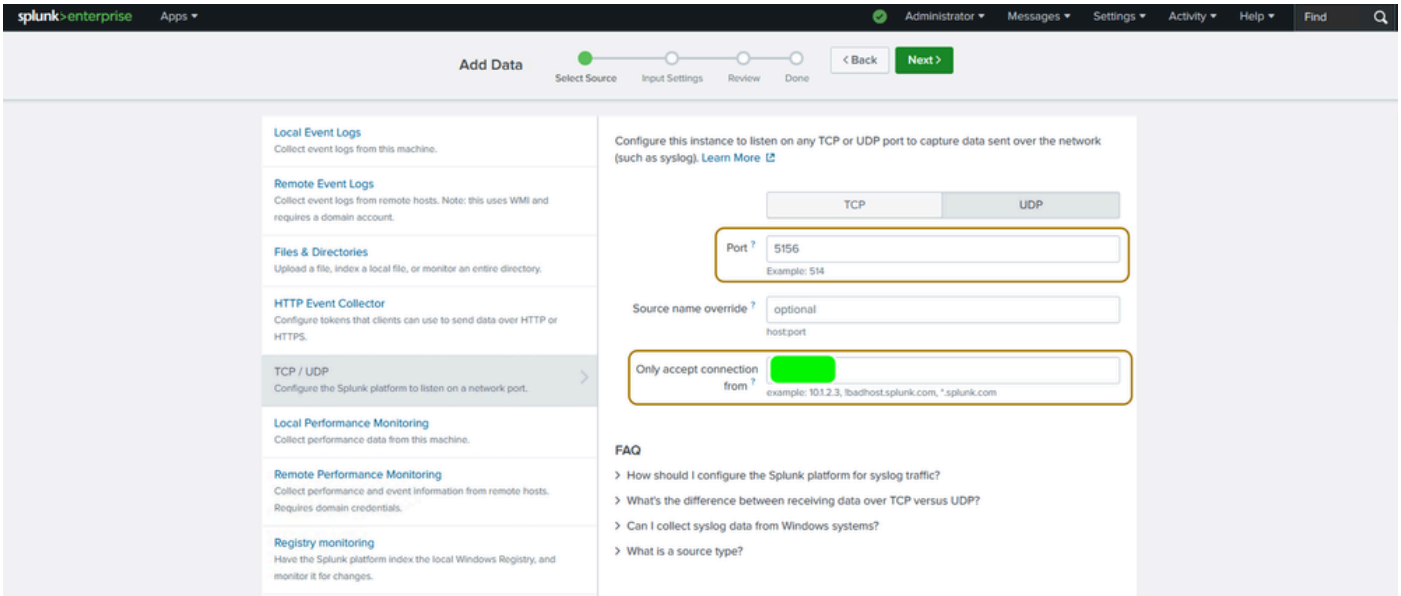


UDPデータ入力の「UDP」をクリックします。



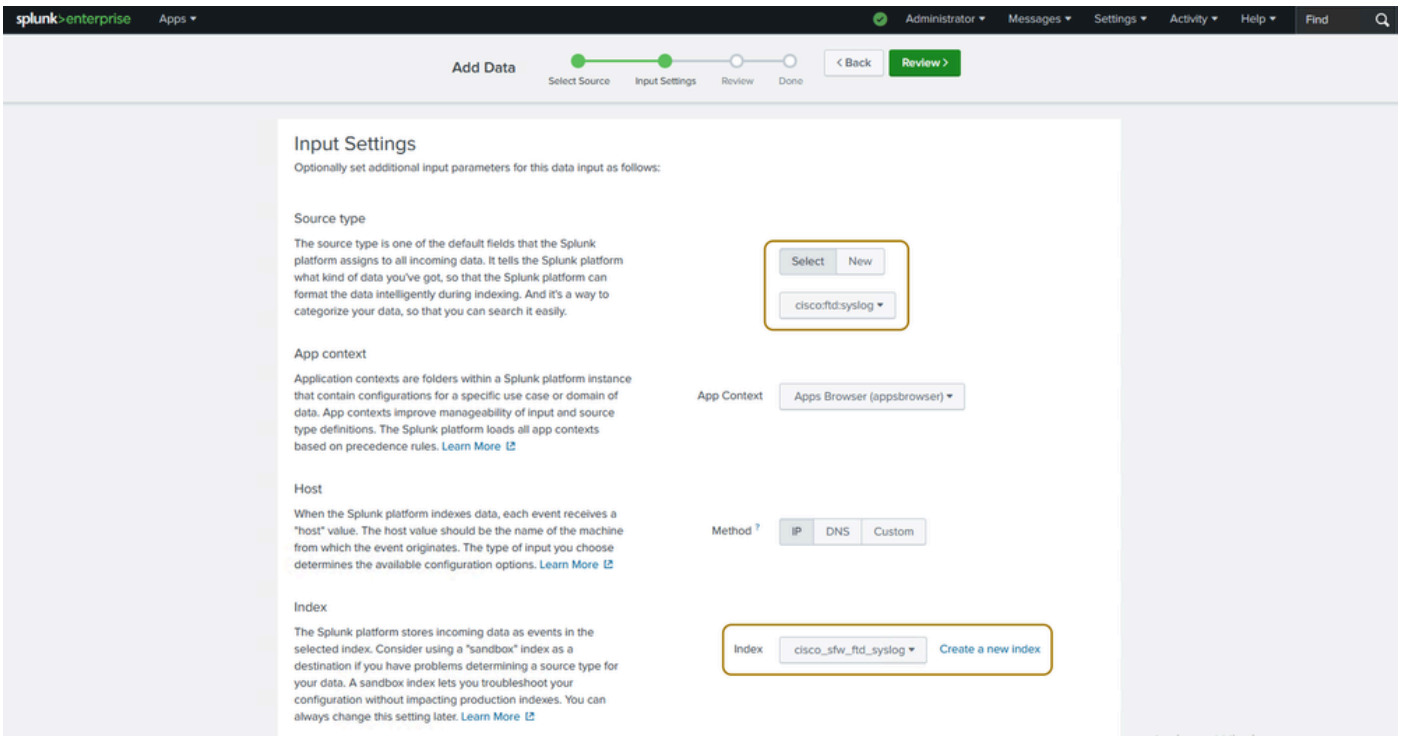
「新しいローカルUDP」入力の作成

ステップ 4：syslogが送信されるポートを入力します。これは、FTD syslog設定で設定されているポート（この場合は5156）と同じである必要があります。1つのソース(FTD)からのみsyslogを受け入れるようにするには、Only Accept Connection Fromフィールドを、Splunkサーバと通信するFTDのインターフェイスのIPに設定します。[Next] をクリックします。



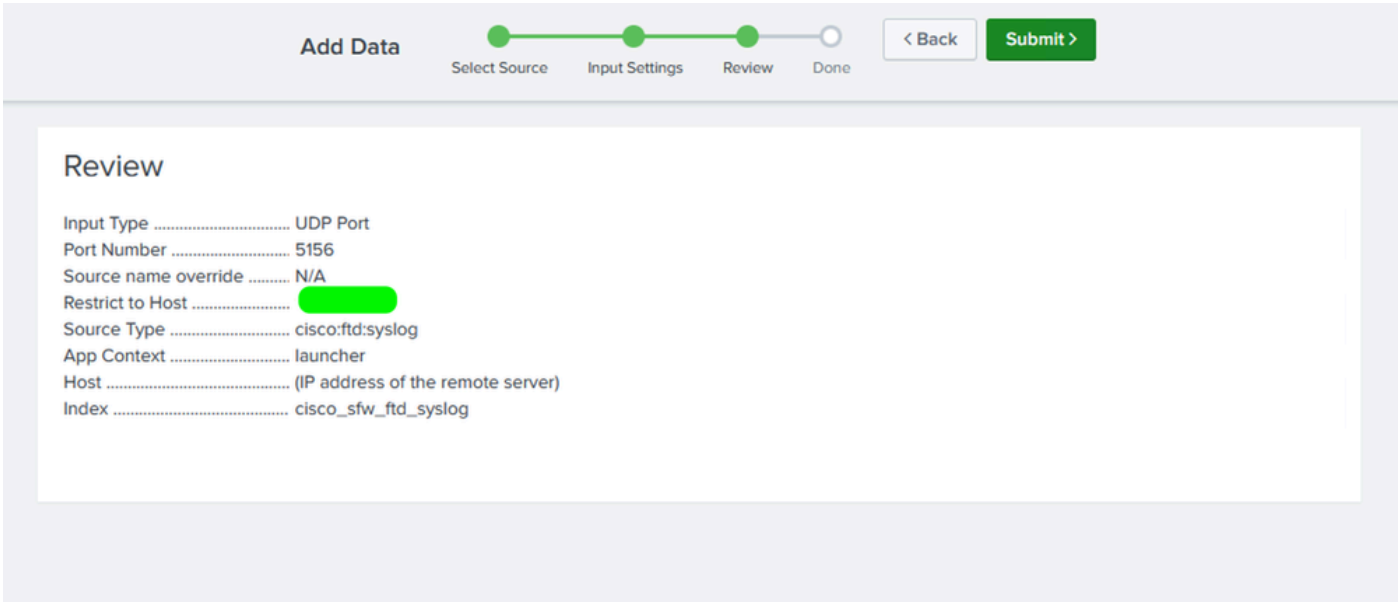
ポートとFTD IPアドレスを指定します。

ステップ 5：次の図で強調表示されているように、Splunkで事前定義されているフィールド値から、ソースタイプとインデックスフィールドの値を検索して選択できます。残りのフィールドにはデフォルト設定を使用できます。



データ入力設定の構成

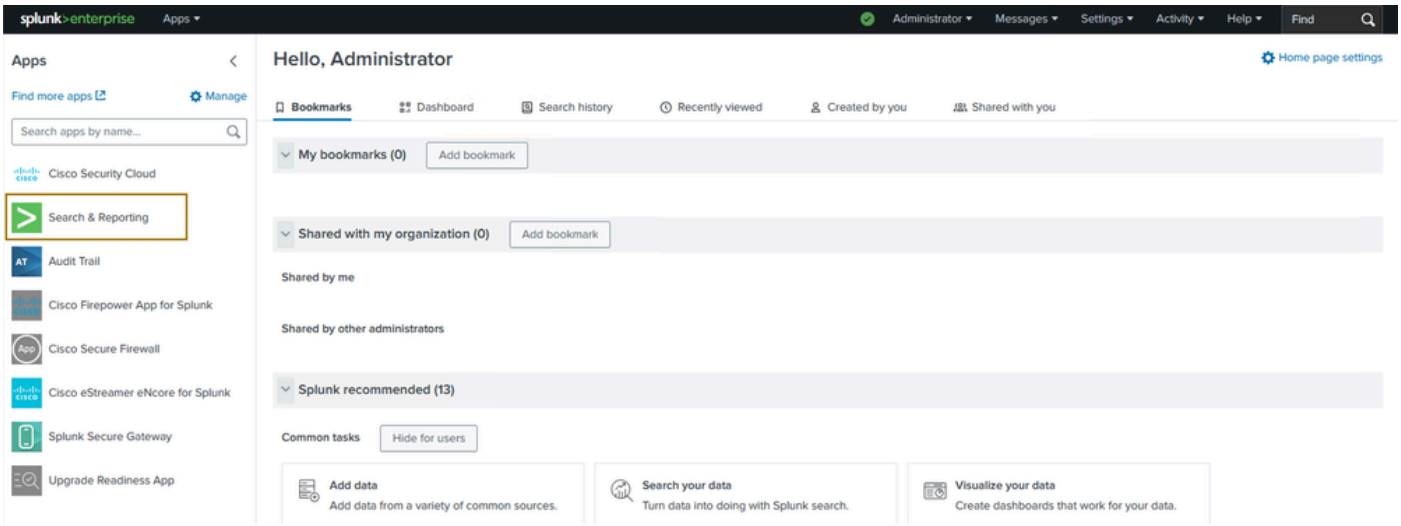
手順 6：設定を確認し、Submitをクリックします。



データ入力設定の確認

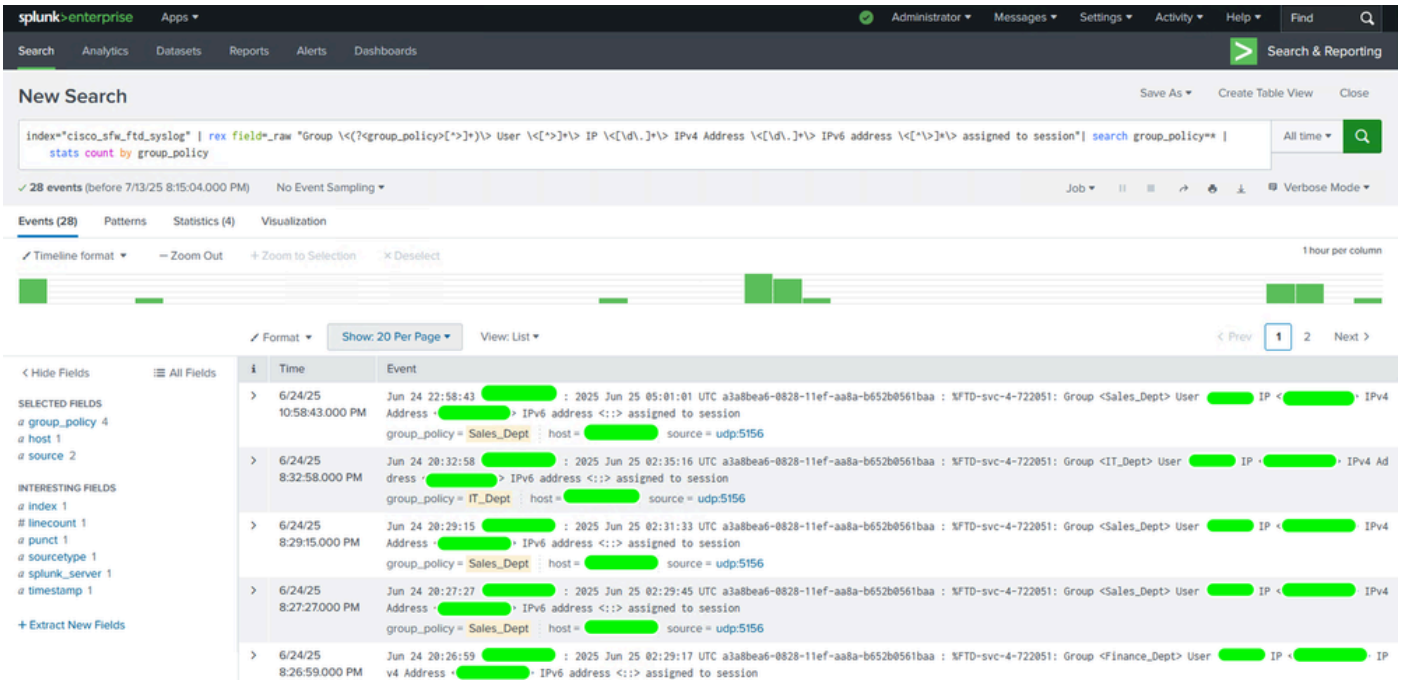
SPLクエリの実行とダッシュボードの作成

ステップ 1：SplunkのSearch and Reporting Appに移動します。

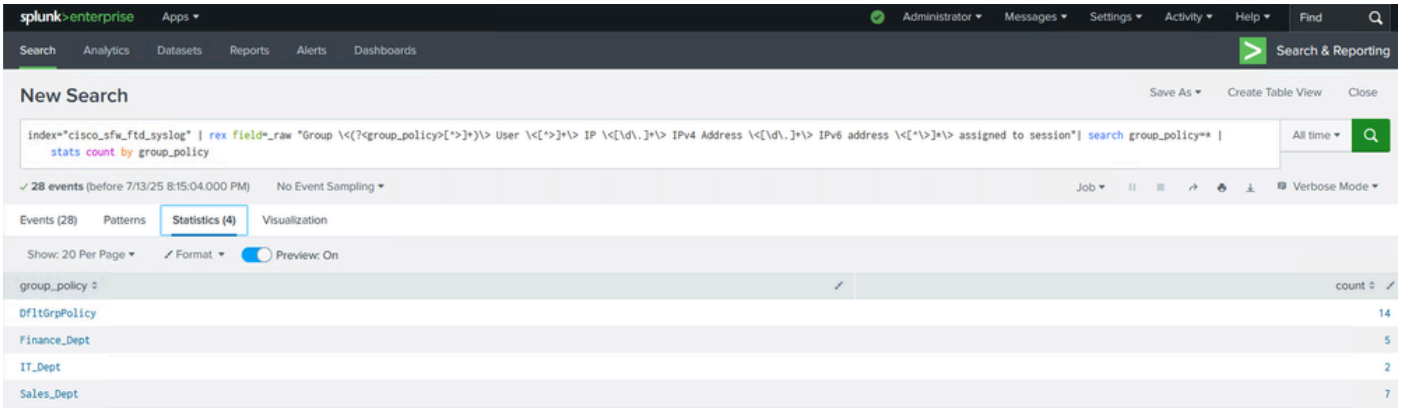


Search and Reportingアプリケーションに移動します

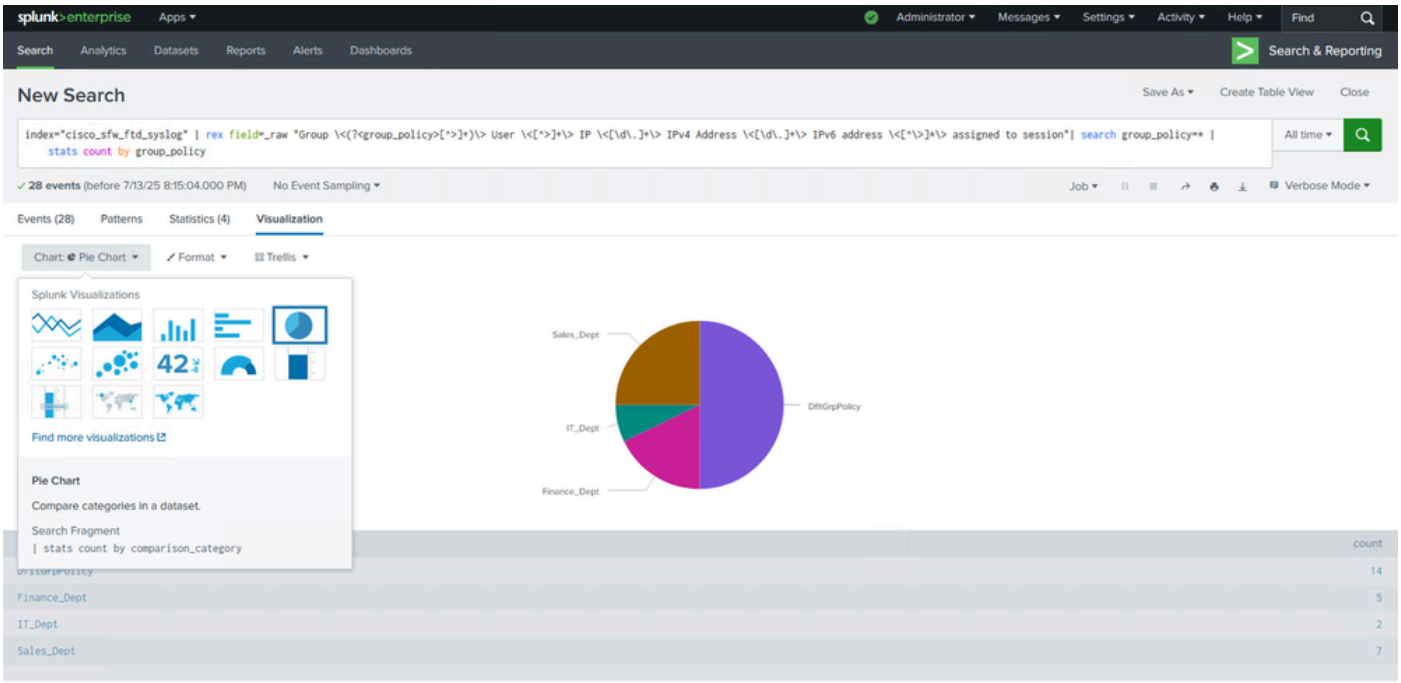
ステップ 2：可視化したいデータに基づいてSPLクエリを作成し、実行します。各ログは(冗長モードで)Eventsタブで完全に確認でき、Statisticsタブでグループポリシーごとの接続数を確認して、これらの統計情報をVisualizationタブで使用してこのデータを視覚化できます。



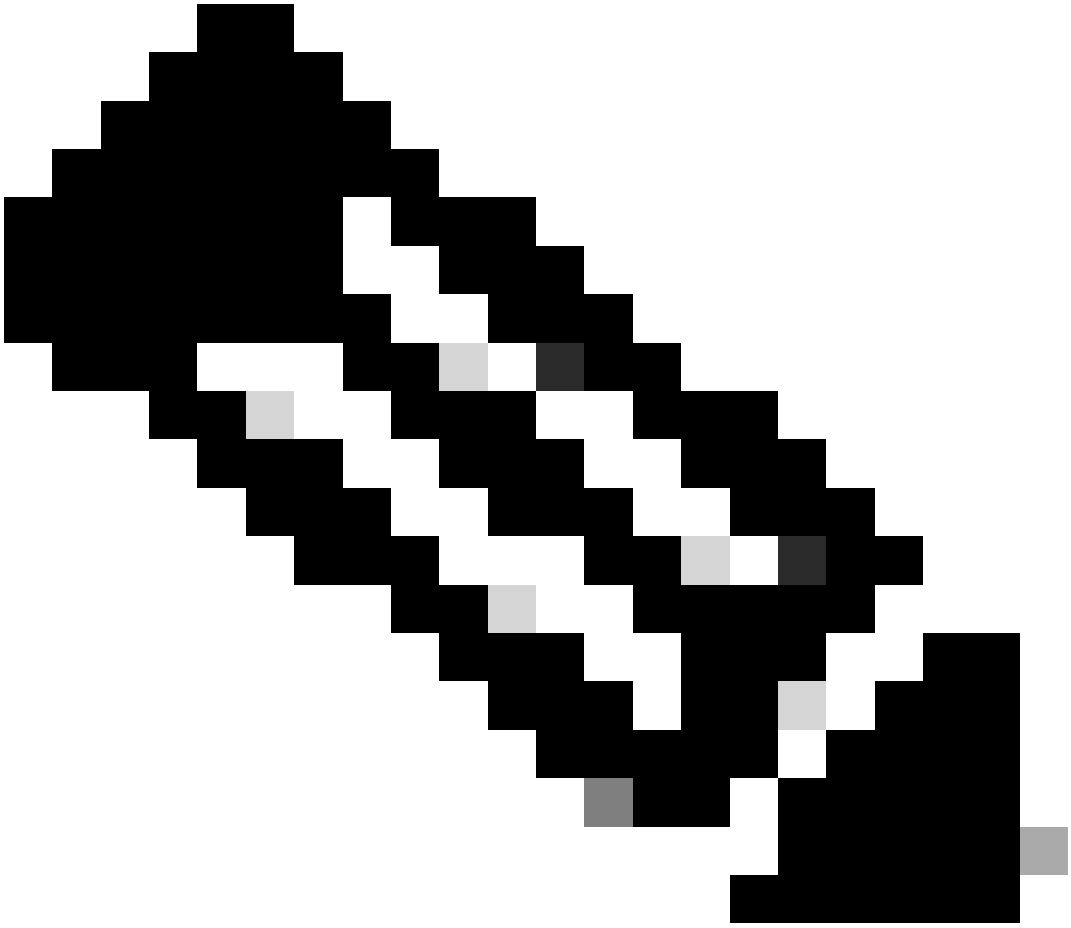
SPLクエリを使用したイベントの検索



Statisticsタブのチェック

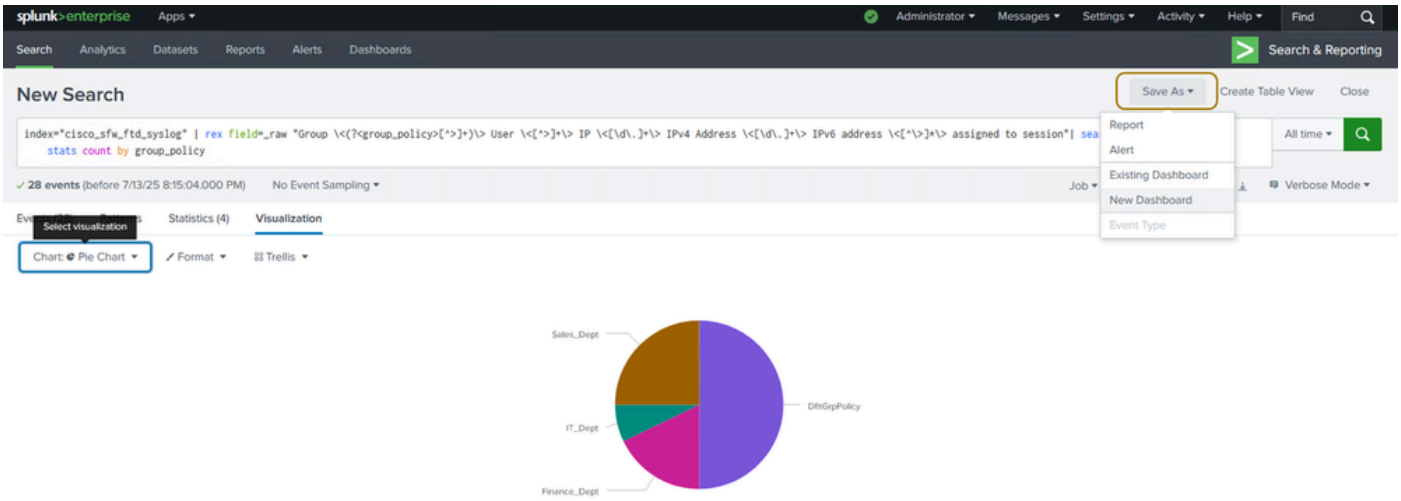


[ビジュアル化]タブにグラフ/グラフが表示されます



注：この例では、クエリは異なるグループポリシー間でリモートアクセスVPN接続が成功した場合の口グを取得しています。グループポリシーごとの成功した接続の数と割合を視覚化するために、円グラフが使用されています。要件と環境設定に基づいて、棒グラフなどの別のタイプのビジュアライゼーションを使用することもできます。

ステップ 3：Save Asをクリックし、このパネルを追加するダッシュボードが既にあるのか、新しく作成するのかに応じて、NewまたはExisting dashboardを選択します。 次の例は、後者の場合を示しています。



パネルをダッシュボードに保存する

ステップ 4：作成するダッシュボードにタイトルを付け、円グラフを含むパネルのタイトルを指定します。

Save Panel to New Dashboard

Dashboard Title: FTD_Dashboard

ftd_dashboard — Edit ID

Description: Optional

Permissions: Private

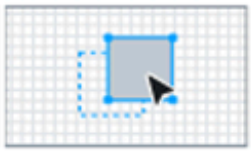
How do you want to build your dashboard? What's this?

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

新しいダッシュボードの設定

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

custom

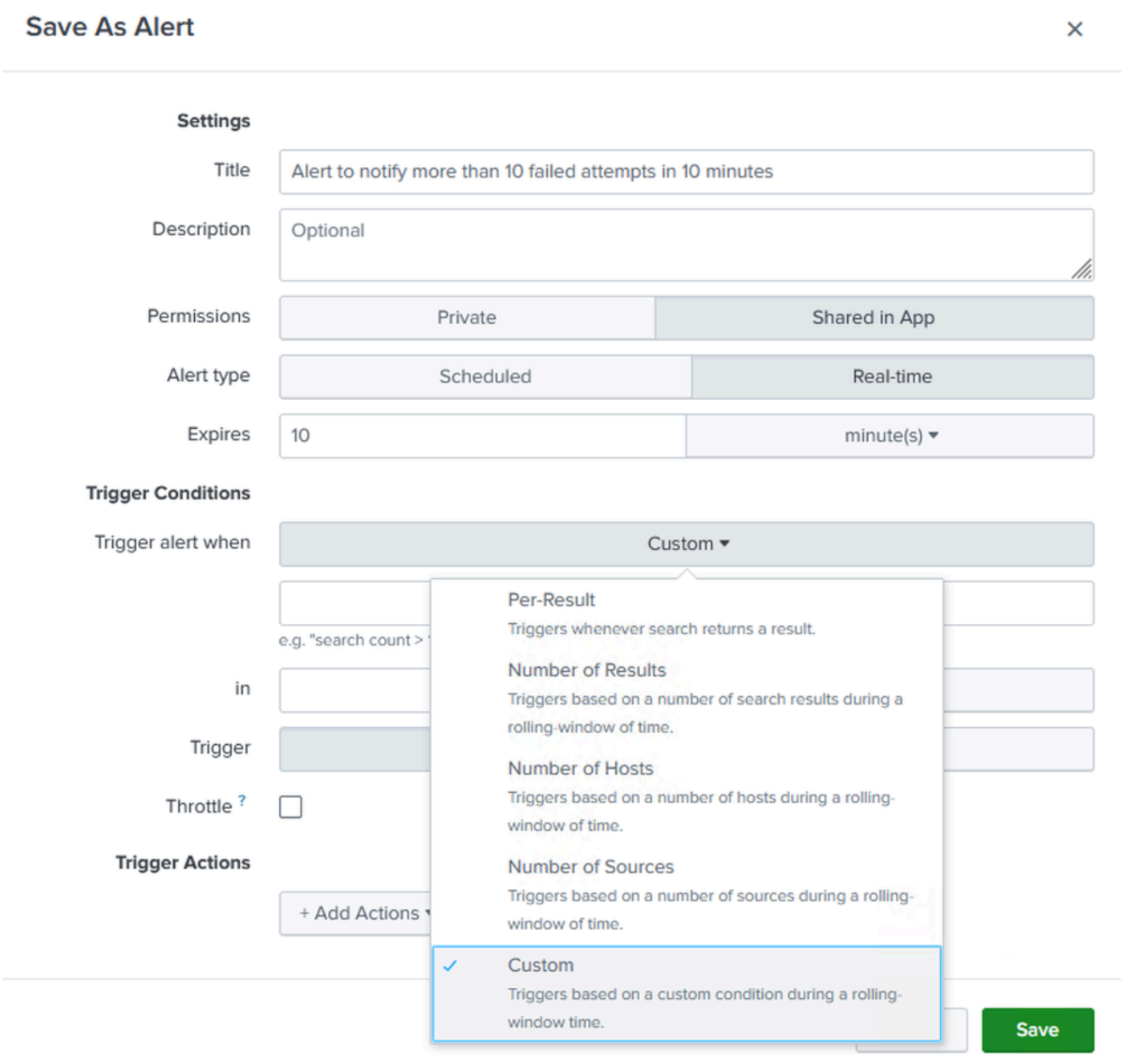
condition is used to search if the

reject_count

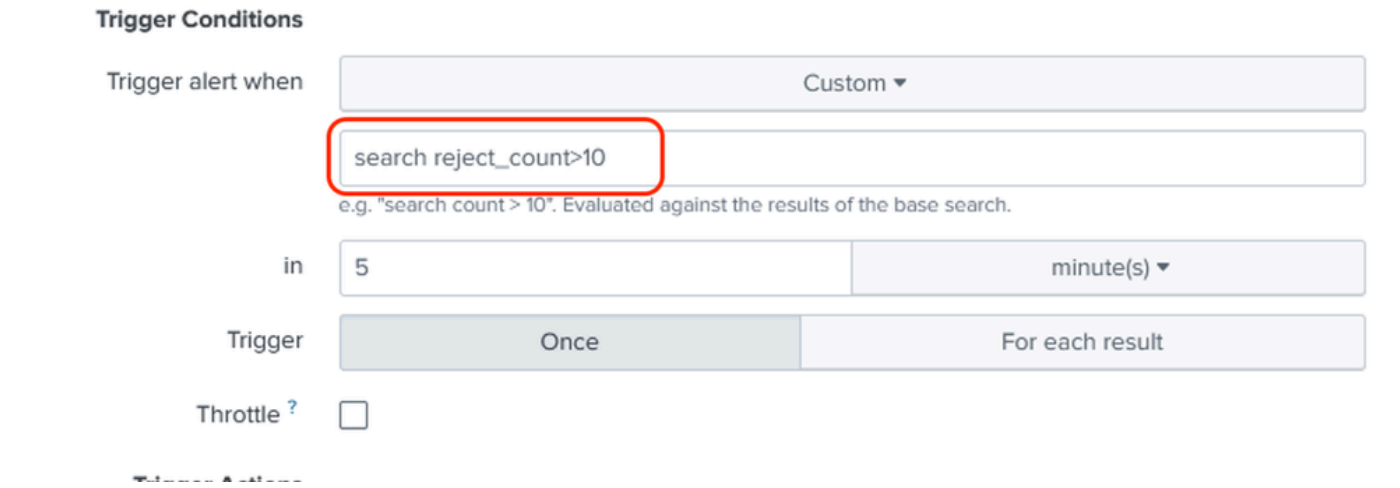
counter from the SPL query has exceeded 10 in the last 5 minutes for any IP address.
Trigger Actions: Set a trigger action such as

Add to Triggered Alerts, Send email, etc.

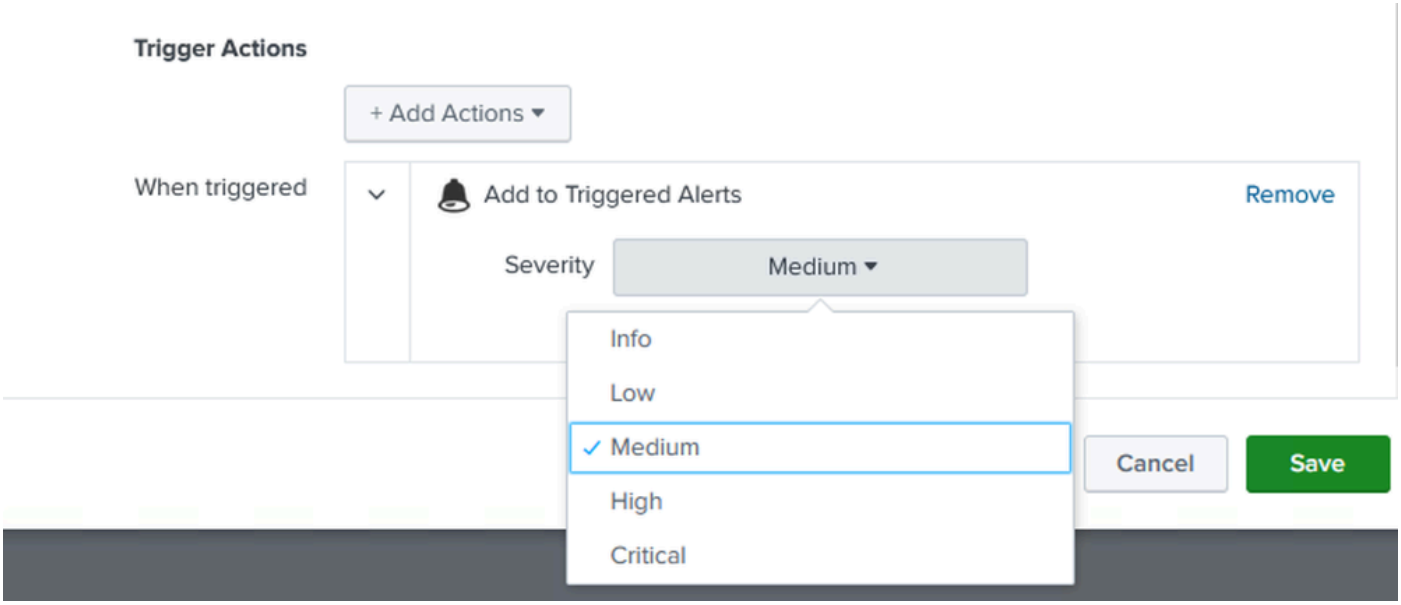
and set the alert severity as per your requirement.



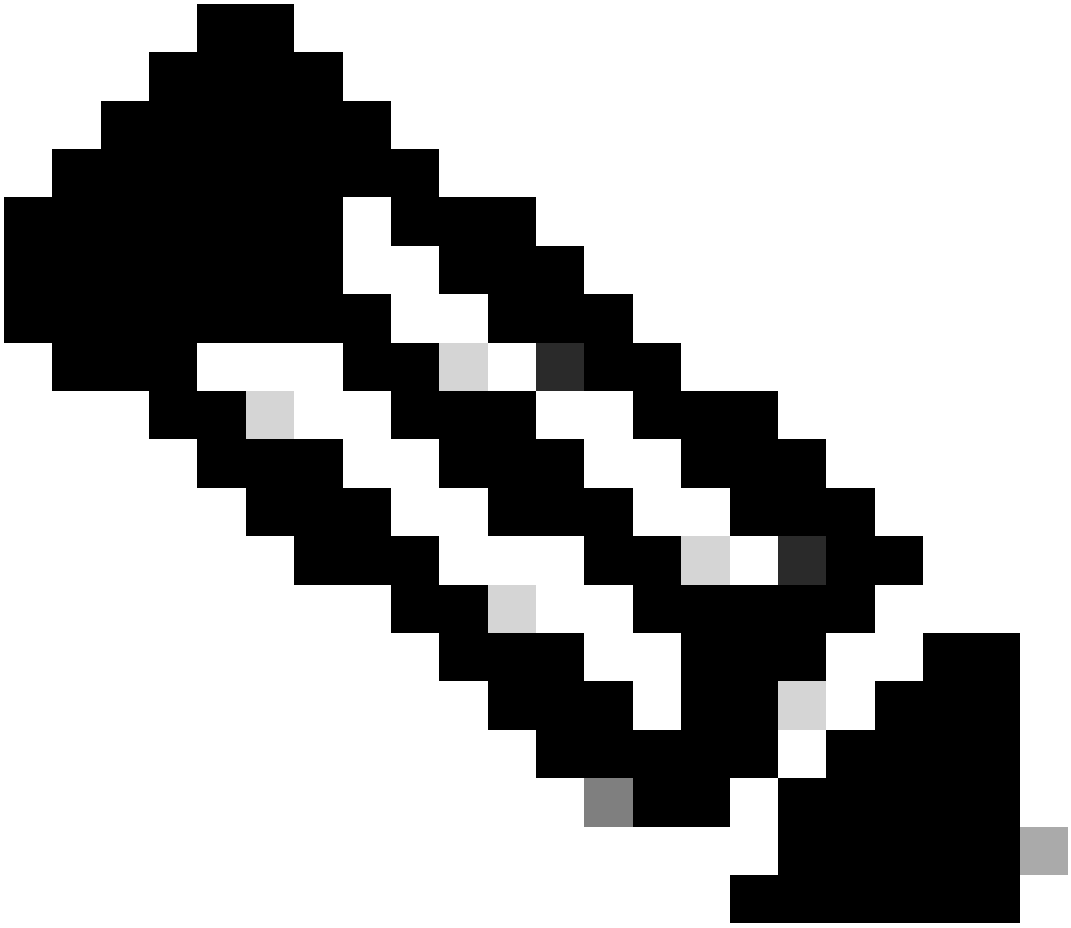
アラート作成の追加設定



アラート作成の追加設定



アラート作成の追加設定



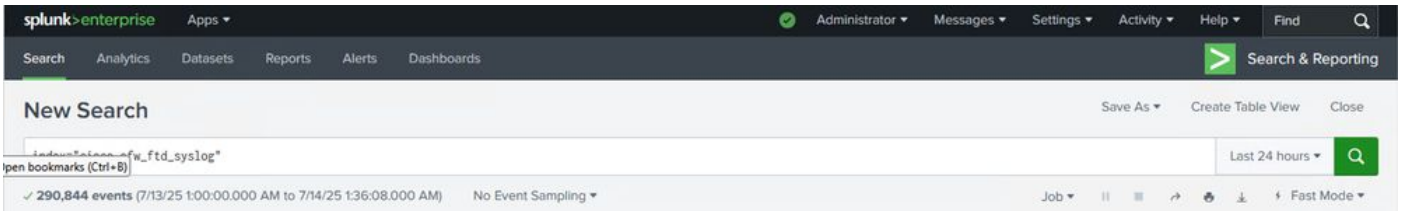
注：結果ごとにアラートをトリガーする場合は、それに応じてスロットリング設定も定義する必要があります。

確認

ダッシュボードとアラートを作成したら、このセクションで説明されている手順を使用して、設定、データフロー、ダッシュボード、およびリアルタイムアラートを確認できます。

View Logs

検索アプリケーションを使用して、ファイアウォールから送信されたログが受信され、Splunk検索ヘッドに表示されるかどうかを確認できます。これは、インデックスで指定された最新の口グ(検索インデックス= "cisco_sfw_ftd_syslog")とそれに関連付けられたタイムスタンプを確認することで確認できます。

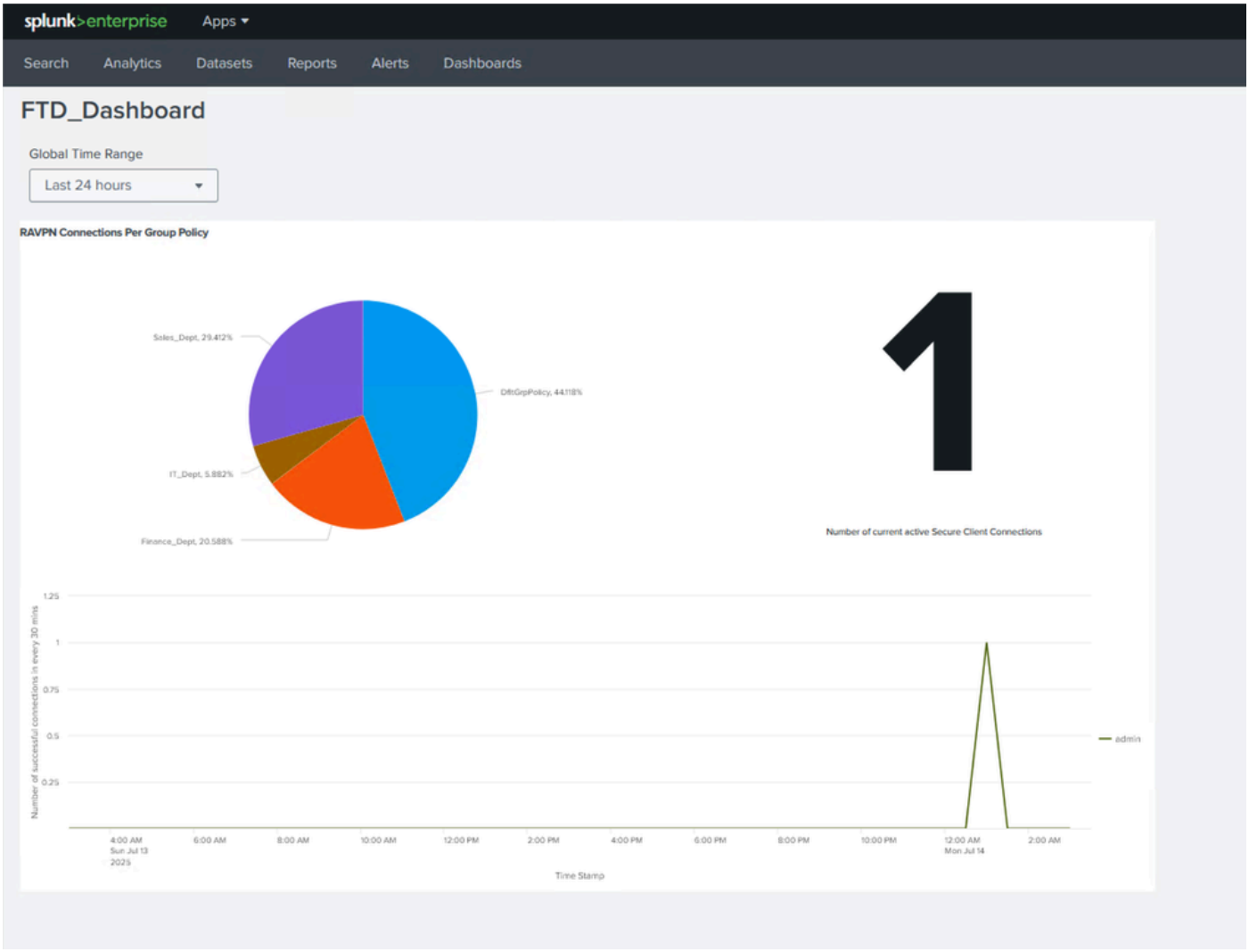


ログの確認と表示

ログの確認と表示

リアルタイムダッシュボードの表示

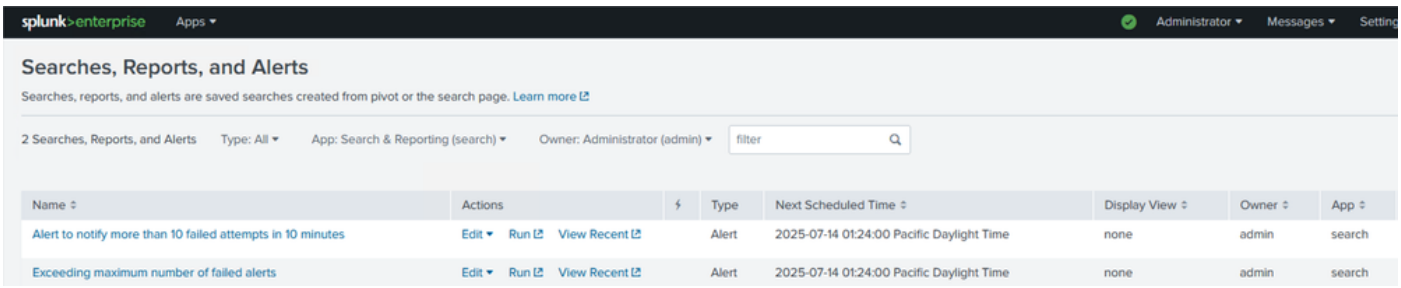
作成したカスタムダッシュボードに移動し、FTDから新しいデータとログが生成されると、各パネルに変更が表示されます。



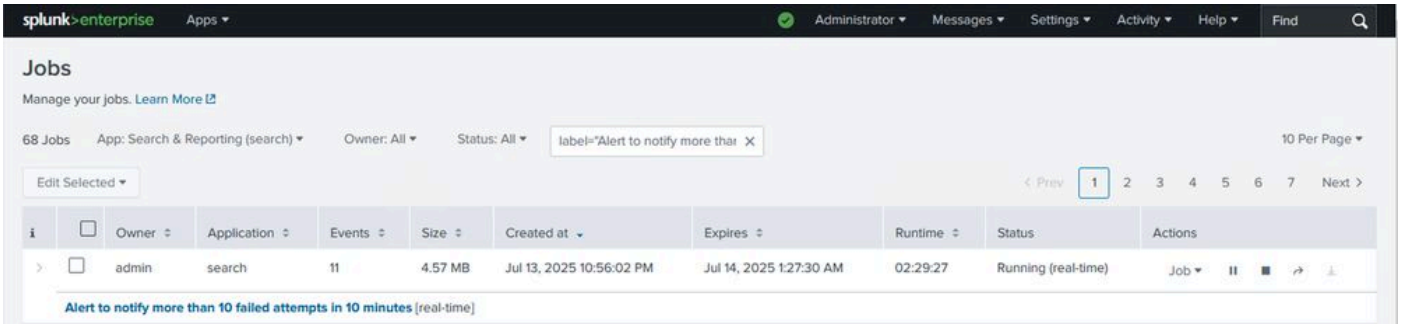
ダッシュボードの表示

アラートがトリガーされたかどうかを確認します

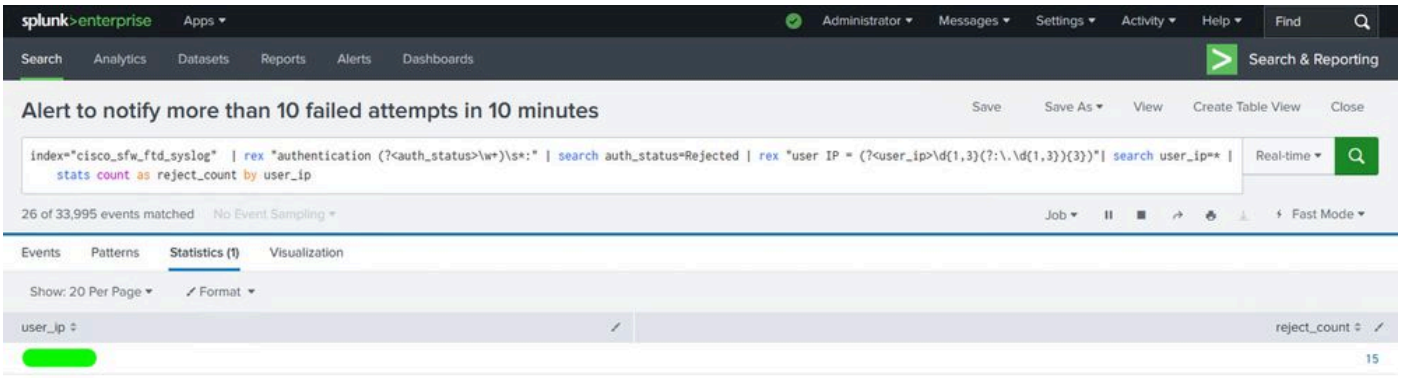
アラートに関する情報を確認するには、検索、レポート、およびアラートのセクションに移動して、最新のアラート情報を表示します。ジョブと検索の詳細を確認するには、View Recentをクリックします。



アラートの確認と表示



アラートの確認と表示



トリガーされたアラートの統計情報の確認

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。