Créer des tableaux de bord et des alertes personnalisés sur le Splunk à l'aide des Syslogs de FTD

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Diagramme du réseau
  - Configurations
    - Configuration des paramètres Syslog pour le FTD
    - Configurer une entrée de données sur l'instance Splunk Enterprise
    - Exécuter des requêtes SPL et créer des tableaux de bord
    - Configuration des alertes en fonction des requêtes SPL
- Vérifier
  - Afficher les journaux
  - Afficher les tableaux de bord en temps réel
  - Vérifier si des alertes ont été déclenchées

Introduction

Ce document décrit une procédure pas à pas pour configurer FTD pour envoyer des syslogs à Splunk et utiliser ces logs pour créer des tableaux de bord et des alertes personnalisés.

Conditions préalables

Exigences

Cisco vous recommande d'avoir connaissance de ces sujets avant de passer en revue ce guide de configuration :

- Syslog
- Connaissances de base de Splunk's Search Processing Language (SPL)

Ce document suppose également que vous disposez déjà d'une instance Splunk Enterprise installée sur un serveur et que vous avez accès à l'interface Web.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Firepower Threat Defense (FTD) exécuté sur la version 7.2.4
- Cisco Firepower Management Center (FMC) exécuté sur la version 7.2.4
- Instance Splunk Enterprise (version 9.4.3) exécutée sur un ordinateur Windows

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration.

Informations générales

Les périphériques Cisco FTD génèrent des syslogs détaillés couvrant les événements d'intrusion, les politiques de contrôle d'accès, les événements de connexion, etc. L'intégration de ces journaux avec Splunk permet une analyse puissante et des alertes en temps réel pour les opérations de sécurité du réseau.

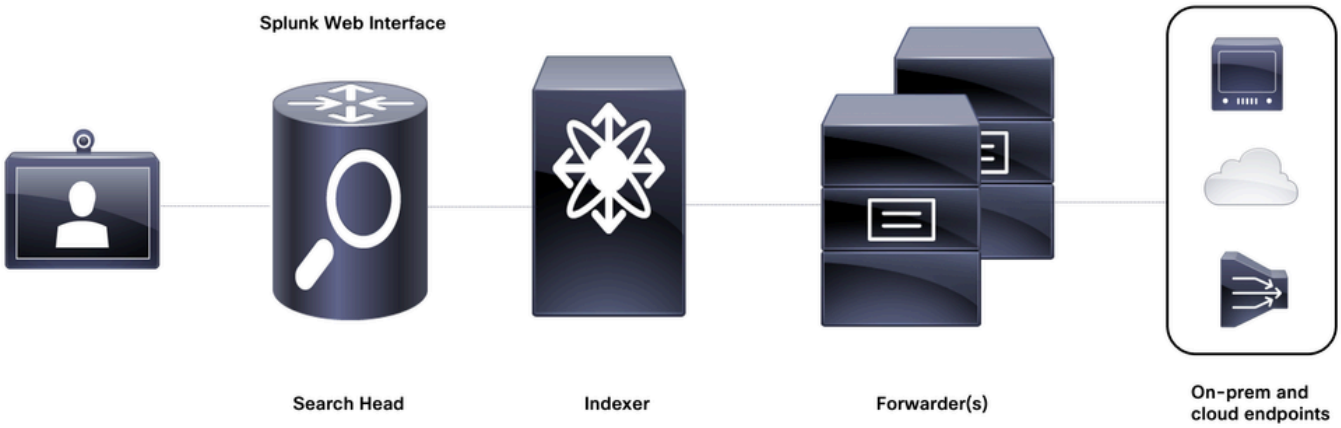
Splunk est une plate-forme d'analyse de données en temps réel conçue pour ingérer, indexer, rechercher et visualiser des données générées par des machines. Splunk est particulièrement efficace dans les environnements de cybersécurité en tant qu'outil SIEM (Security Information and Event Management) en raison de sa capacité à :

- Ingérer les données de journal à grande échelle
- Effectuer des recherches complexes avec SPL
- Créer des tableaux de bord et des alertes
- Intégration aux systèmes d'orchestration de la sécurité et de réponse aux incidents

Splunk traite les données via un pipeline structuré afin de rendre les données non structurées ou semi-structurées de la machine utiles et exploitables. Les étapes clés de ce pipeline sont souvent appelées IPIS qui signifie :

- Entrée
- Analyse
- Indexation
- Recherche

Les principaux composants généraux de l'architecture sous-jacente qui sont utilisés pour réaliser le pipeline IPIS sont représentés dans ce schéma :



Architecture sous-jacente Splunk

Configurer

Diagramme du réseau

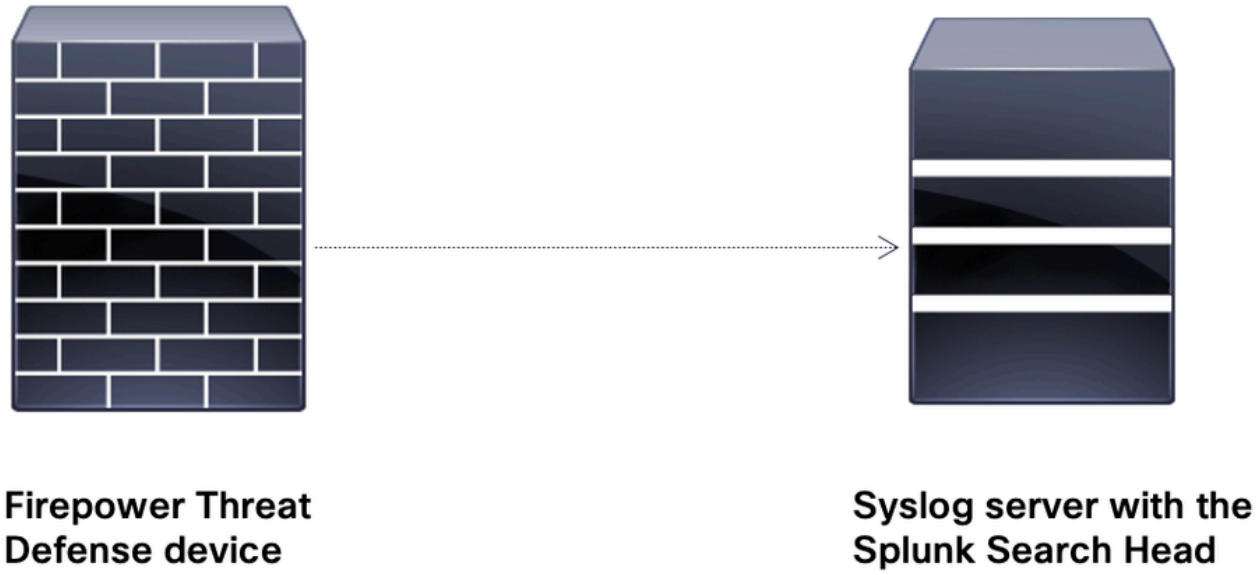
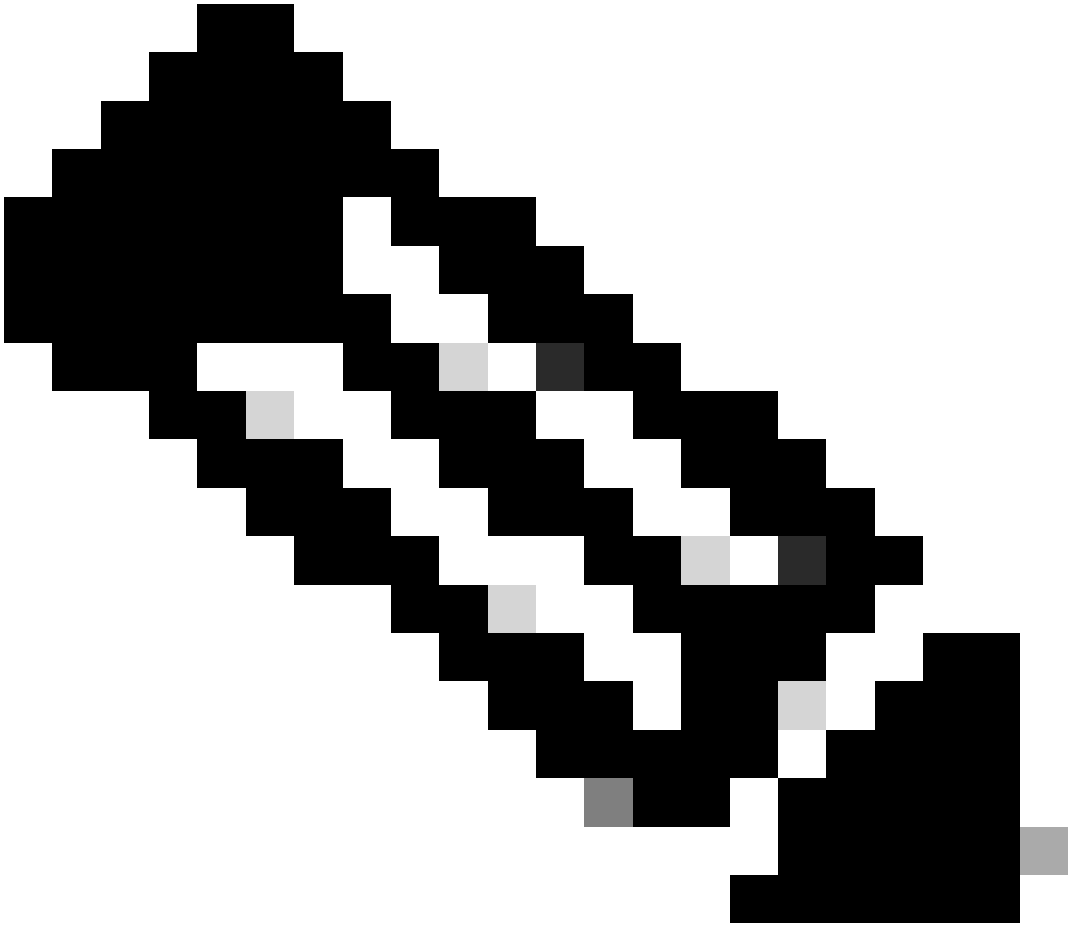


Diagramme du réseau

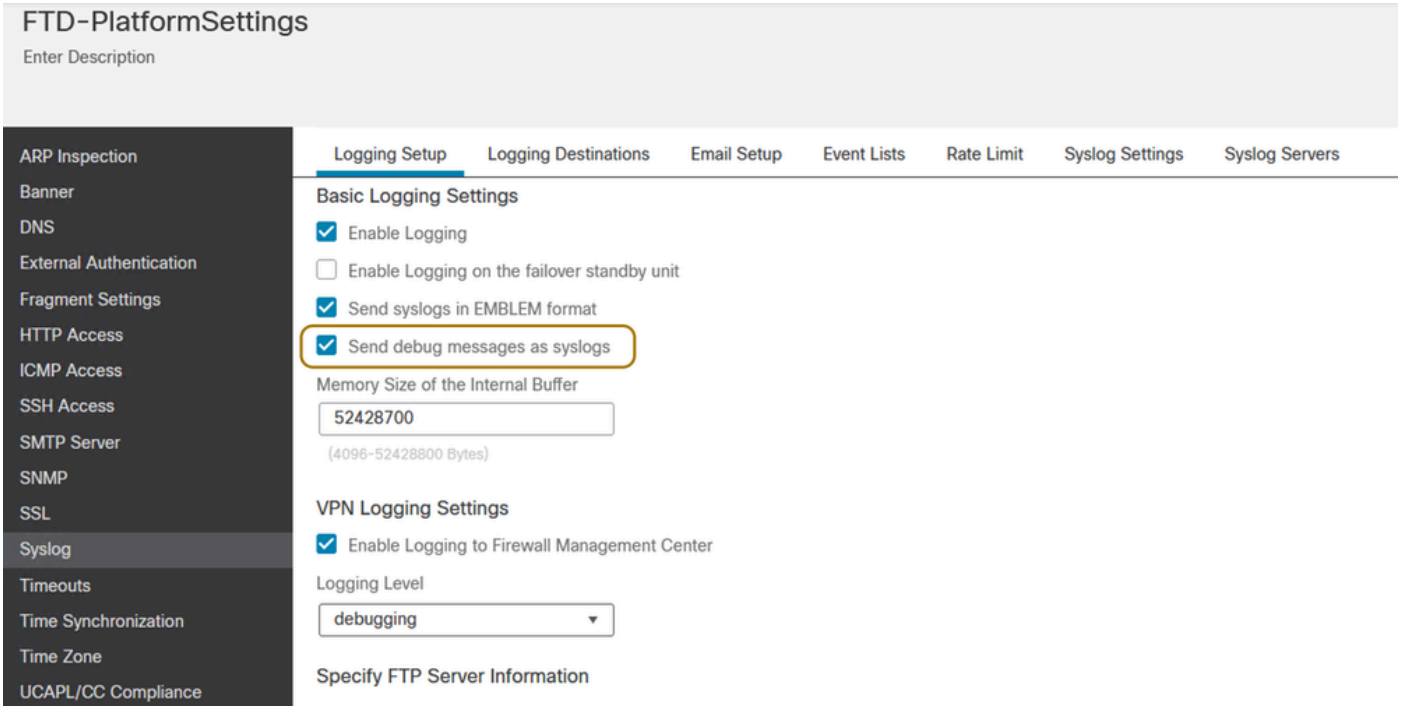


Remarque : L'environnement de travaux pratiques de ce document ne nécessite pas d'instances de redirecteur et d'indexeur séparées. L'ordinateur Windows, c'est-à-dire le serveur Syslog sur lequel l'instance Splunk Enterprise est installée, agit en tant qu'indexeur et en tant que tête de recherche.

Configurations

Configuration des paramètres Syslog pour le FTD

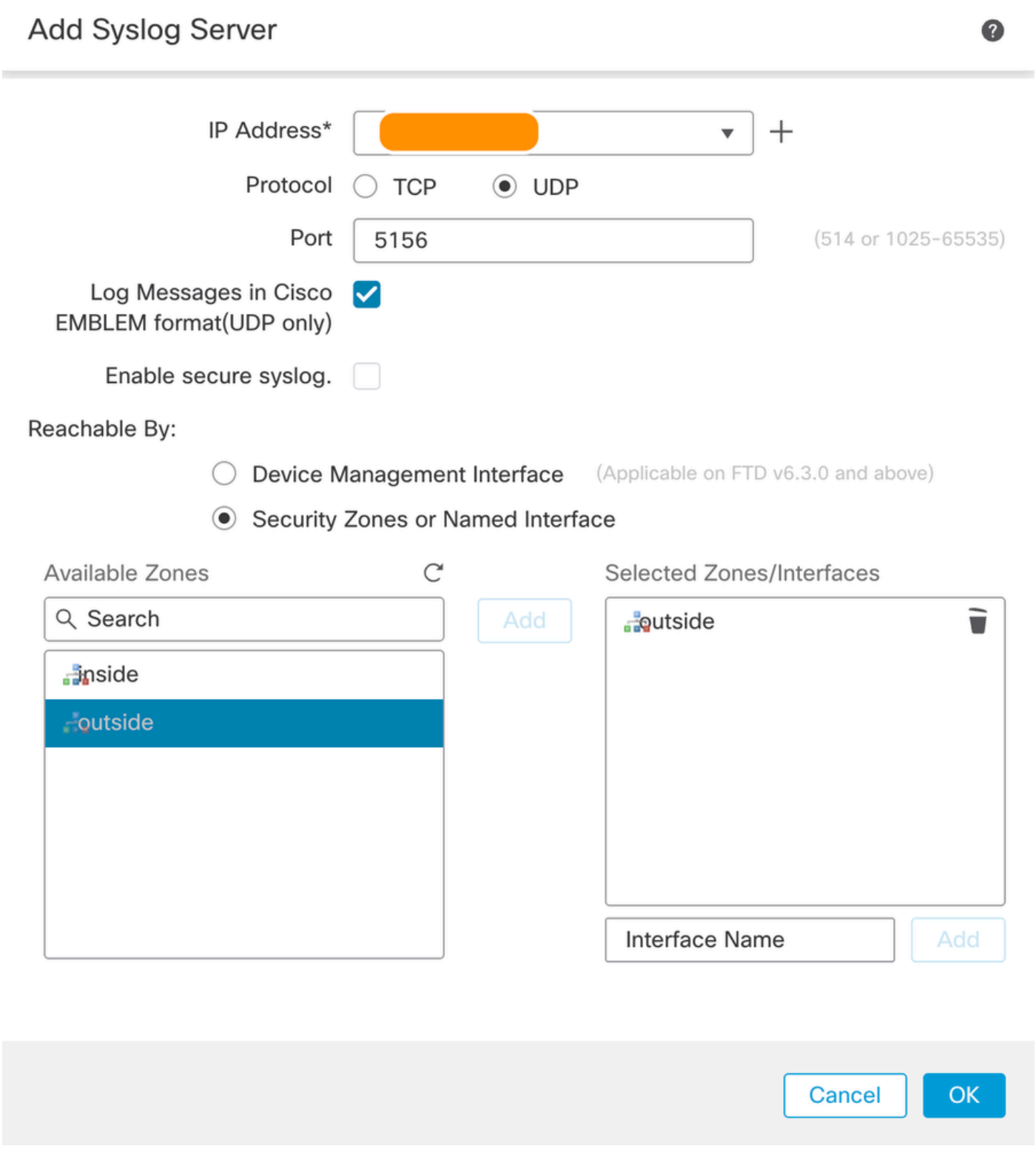
Étape 1. Configurez les paramètres syslog préliminaires sur FMC pour le FTD sous Devices > Platform Settings afin d'envoyer les journaux au serveur syslog sur lequel l'instance Splunk est exécutée.



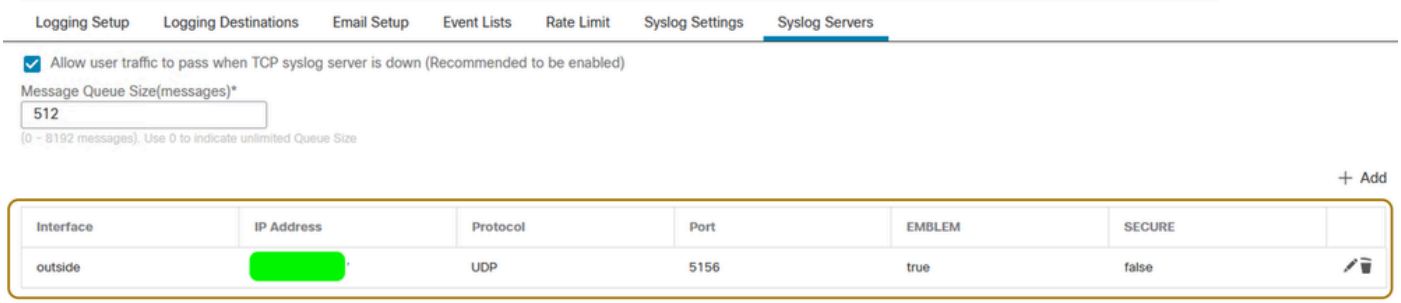
Paramètres de plateforme sur FTD - Syslog

Étape 2 : configuration de l'adresse IP de l'ordinateur sur lequel l'instance Splunk Enterprise est installée et s'exécute en tant que serveur Syslog. Définissez les champs comme indiqué.

```
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
```

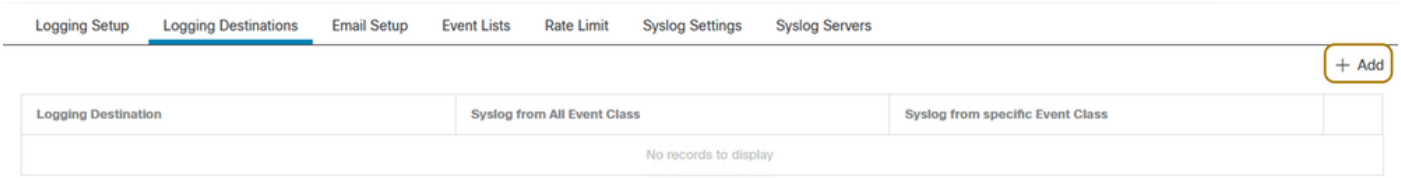


Paramètres de plateforme sur FTD - Ajouter un serveur Syslog

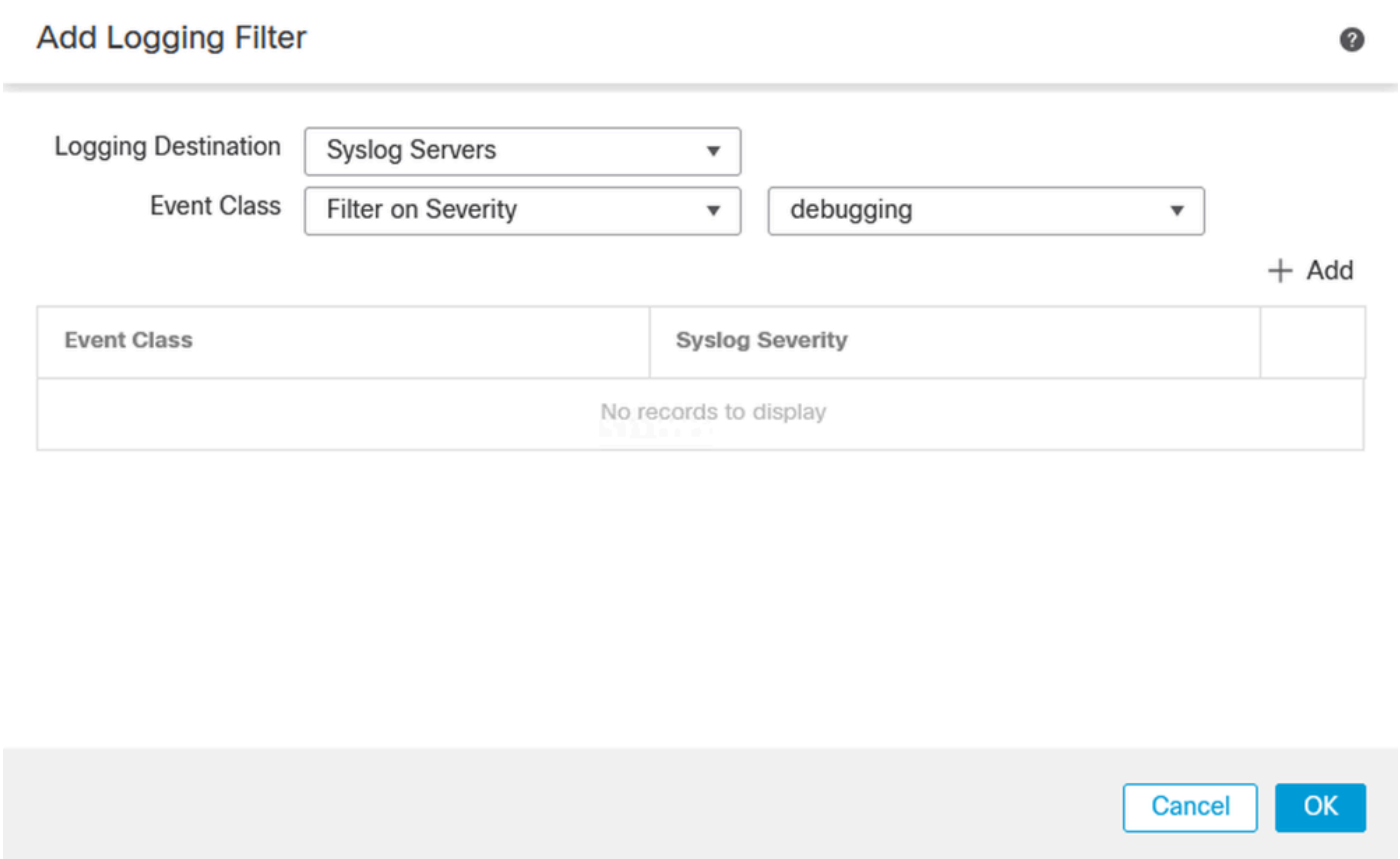


Paramètres de plateforme sur FTD - serveur Syslog ajouté

Étape 3. Ajout d'une destination de journalisation pour les serveurs Syslog. Le niveau de journalisation peut être défini en fonction de votre choix ou du cas d'utilisation.



Paramètres de plateforme sur FTD - Ajouter une destination de journalisation



Paramètres de plate-forme sur FTD - Définir le niveau de gravité pour la destination de journalisation

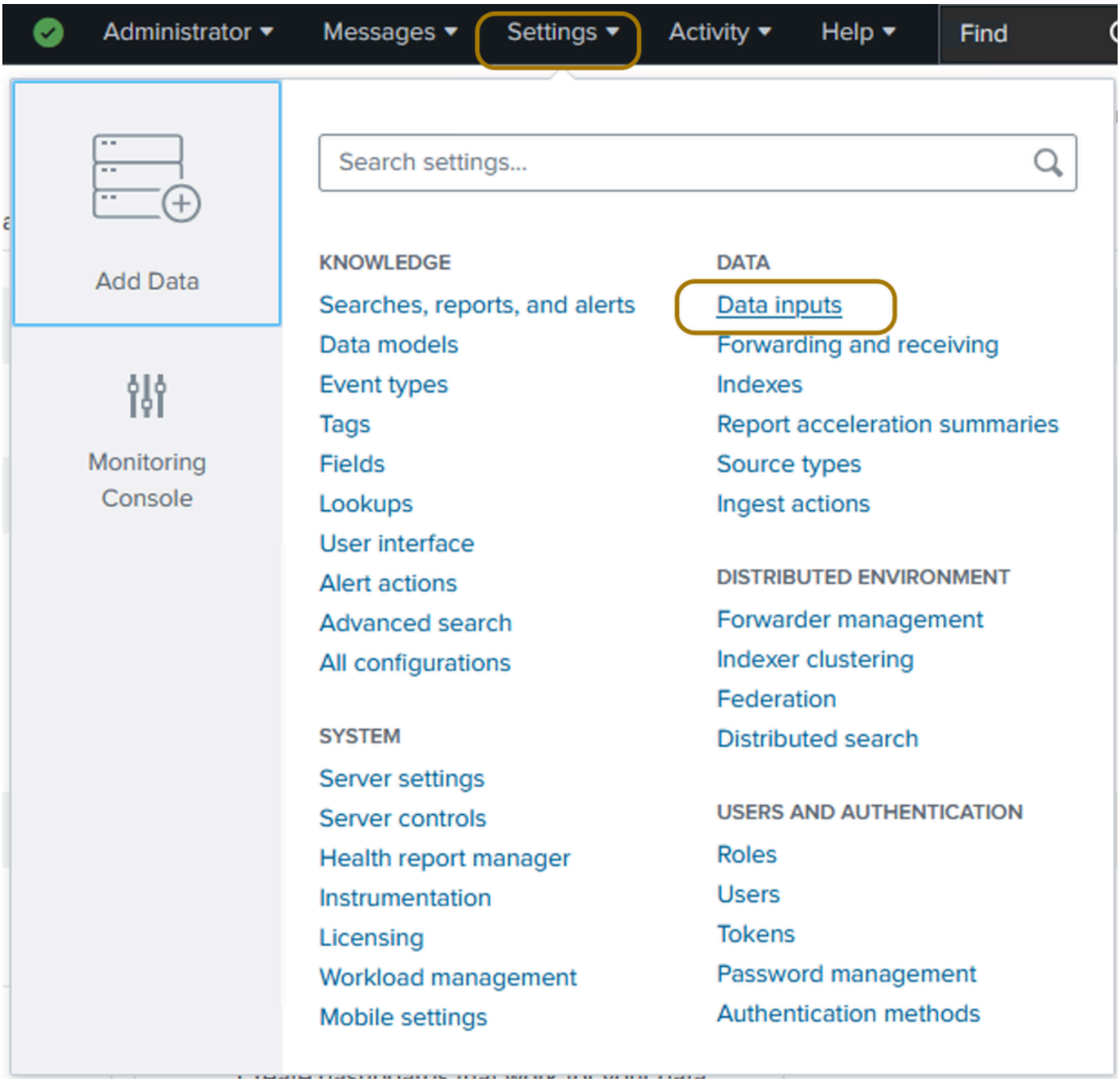
Déployez les modifications des paramètres de la plate-forme sur le FTD après avoir effectué ces étapes.

Configurer une entrée de données sur l'instance Splunk Enterprise

Étape 1. Connexion à l’interface Web de l’instance de Splunk Enterprise

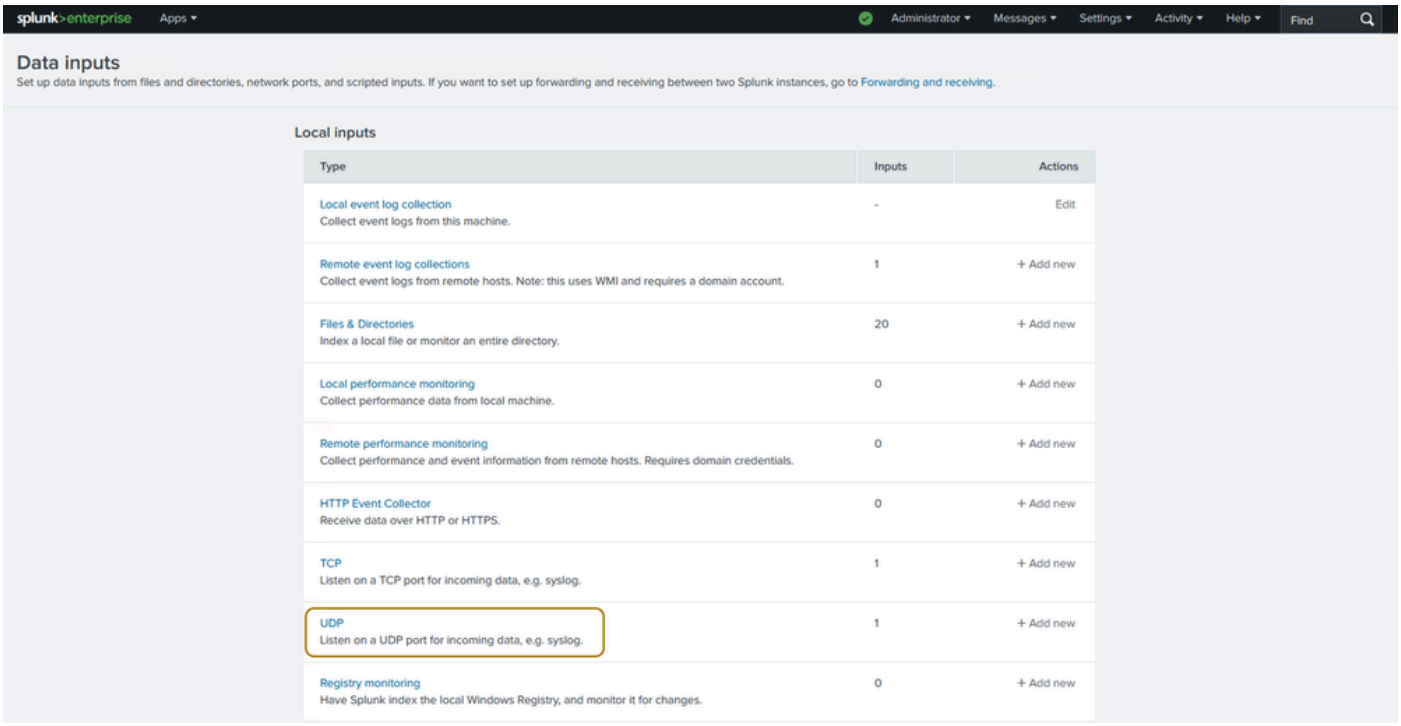
Page de connexion de l'interface Web Splunk

Étape 2. Vous devez définir une entrée de données afin de pouvoir stocker et indexer les syslogs sur Splunk. Accédez à Paramètres > Données > Entrées de données après vous être connecté.

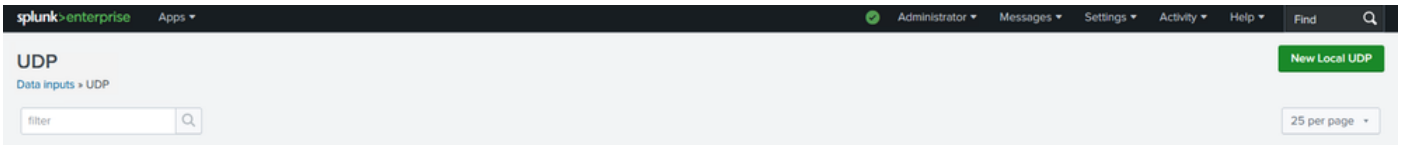


Accédez à Entrées de données sur le Splunk

Étape 3. Choisissez UDP, puis cliquez sur New Local UDP sur la page suivante qui apparaît.

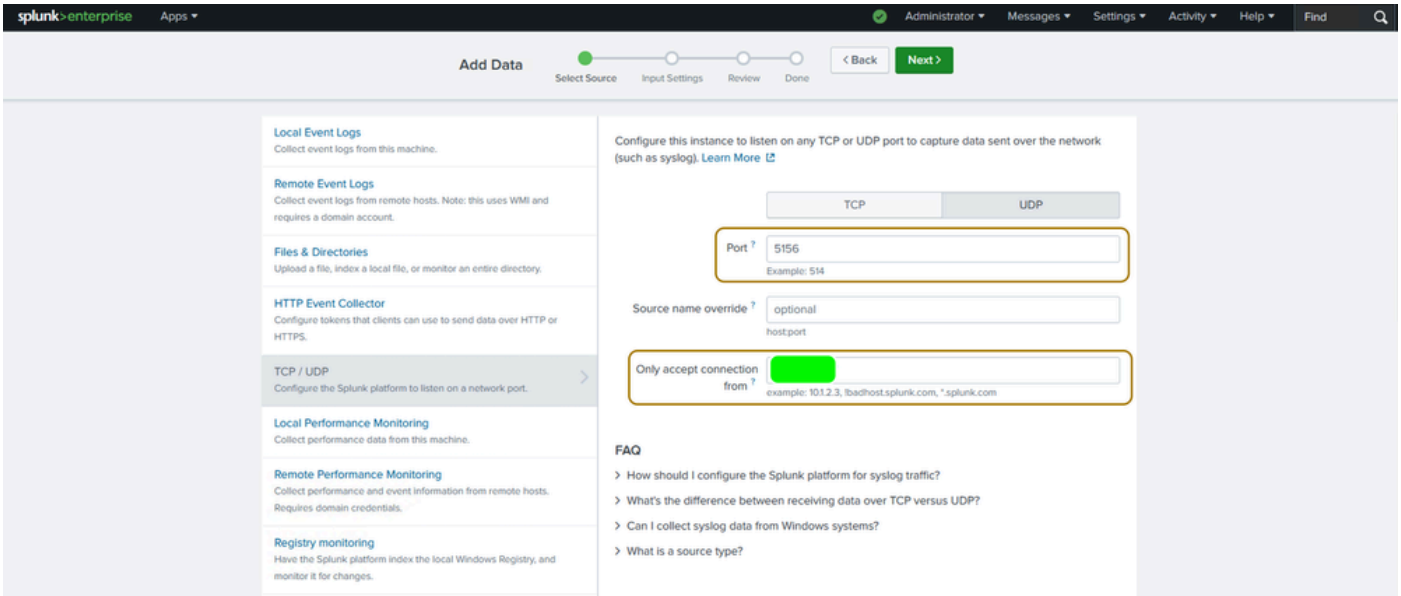


Cliquez sur « UDP » pour une entrée de données UDP



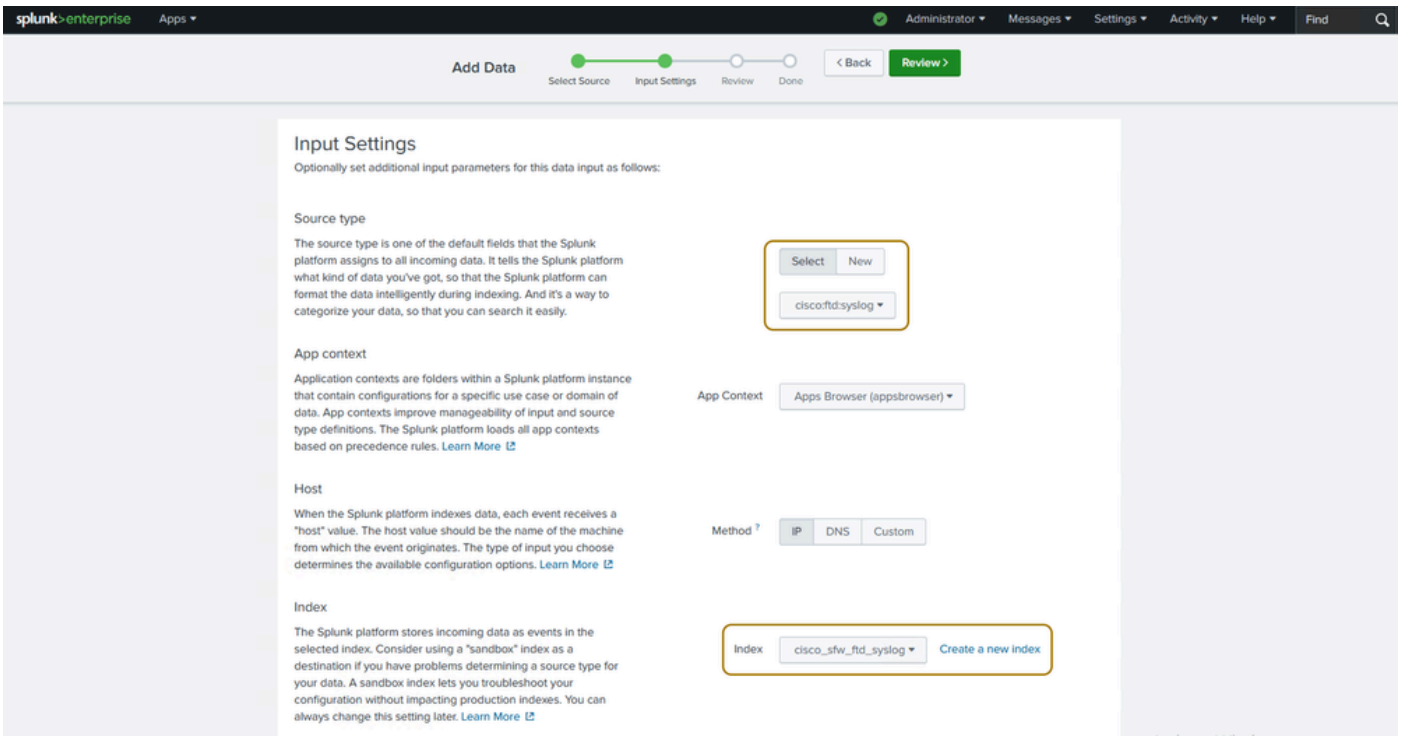
Créer une entrée « Nouveau protocole UDP local »

Étape 4. Entrez le port sur lequel les syslogs sont envoyés. Il doit être identique au port configuré sur les paramètres syslog FTD, dans ce cas 5156. Afin d'accepter les syslogs d'une seule source (le FTD), définissez le champ Only Accept Connection From sur l'IP de l'interface sur le FTD qui communique avec le serveur Splunk. Cliquez sur Next (Suivant).



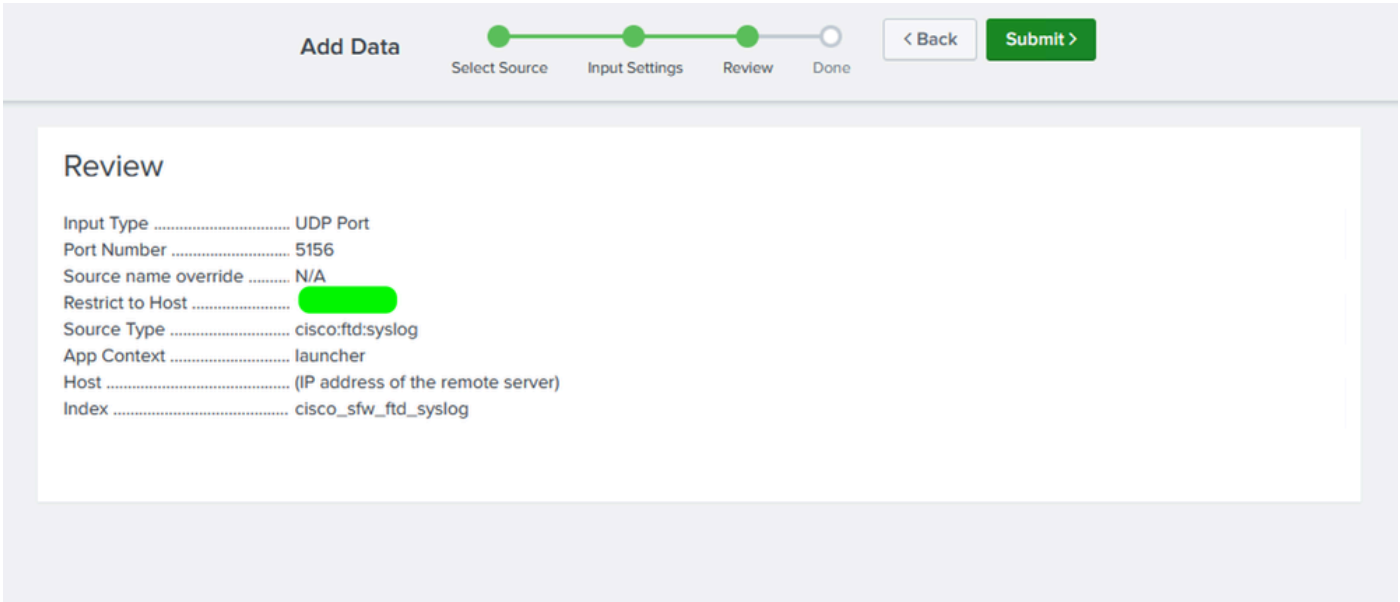
Spécifier le port et l'adresse IP FTD

Étape 5. Vous pouvez rechercher et choisir le type de source et les valeurs de champ d'index à partir des valeurs prédéfinies sur Splunk comme mis en surbrillance dans l'image suivante. Les paramètres par défaut peuvent être utilisés pour les champs restants.



Configurer les paramètres d'entrée de données

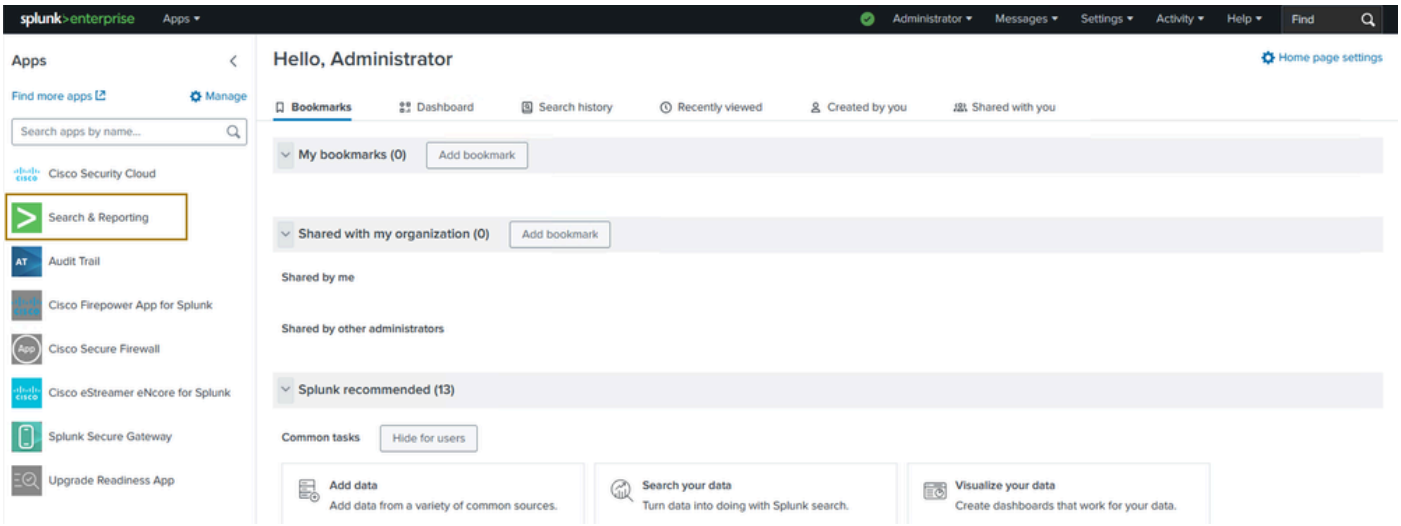
Étape 6. Vérifiez les paramètres et cliquez sur Submit.



Vérifier les paramètres d'entrée de données

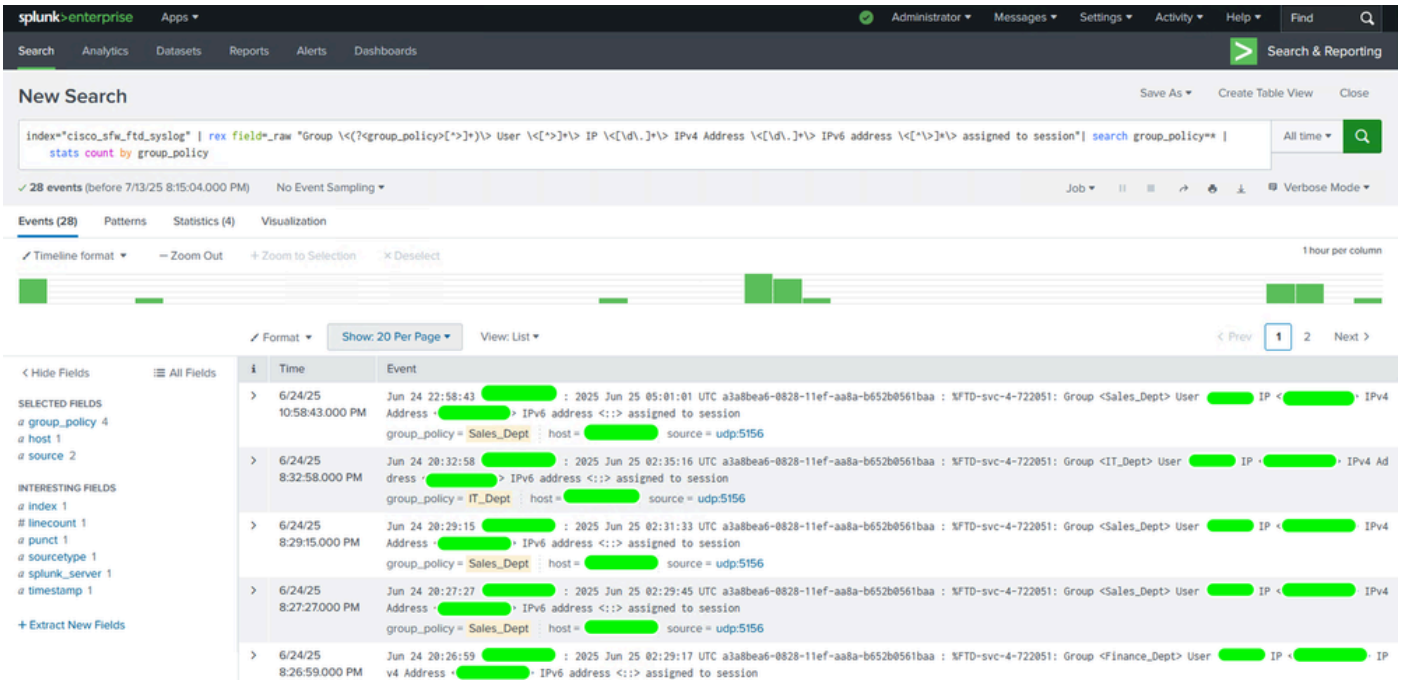
Exécuter des requêtes SPL et créer des tableaux de bord

Étape 1. Accédez à l'application Recherche et création de rapports sur Splunk.

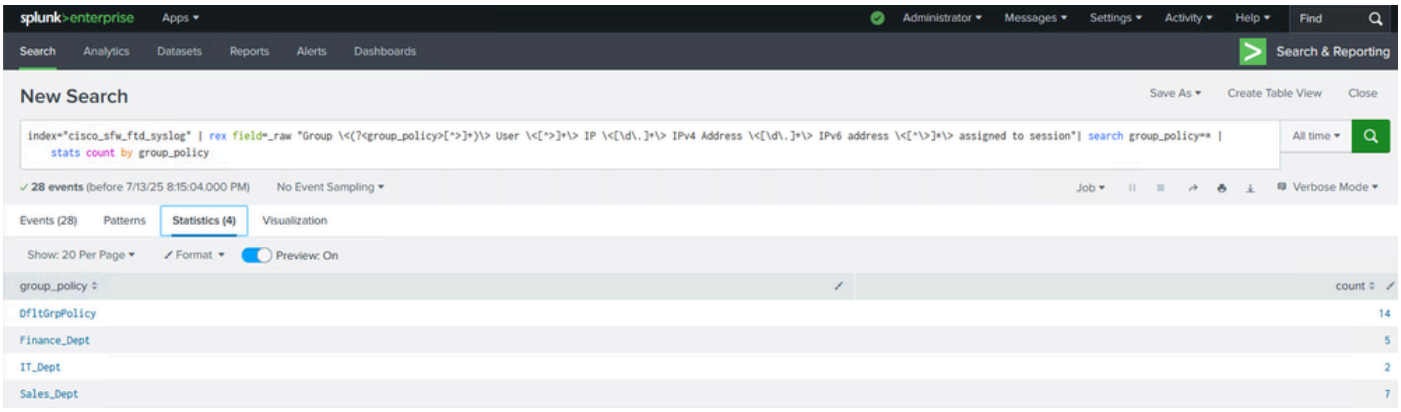


Accédez à l'application Recherche et création de rapports

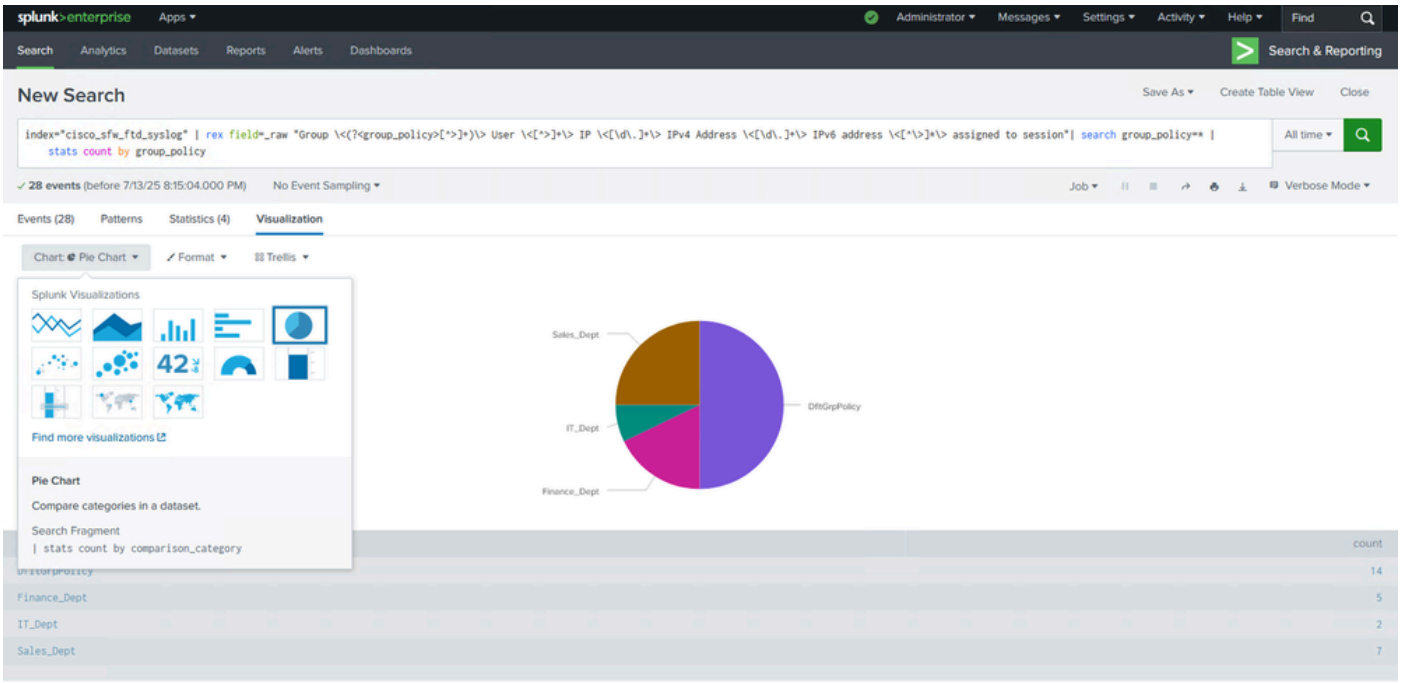
Étape 2. Formuler et exécuter une requête SPL en fonction des données que vous souhaitez visualiser. Vous pourrez voir chaque journal complètement (en mode détaillé) sous l'onglet Événements, le nombre de connexions par stratégie de groupe dans l'onglet Statistiques et visualiser ces données en utilisant ces statistiques sous l'onglet Visualisation.



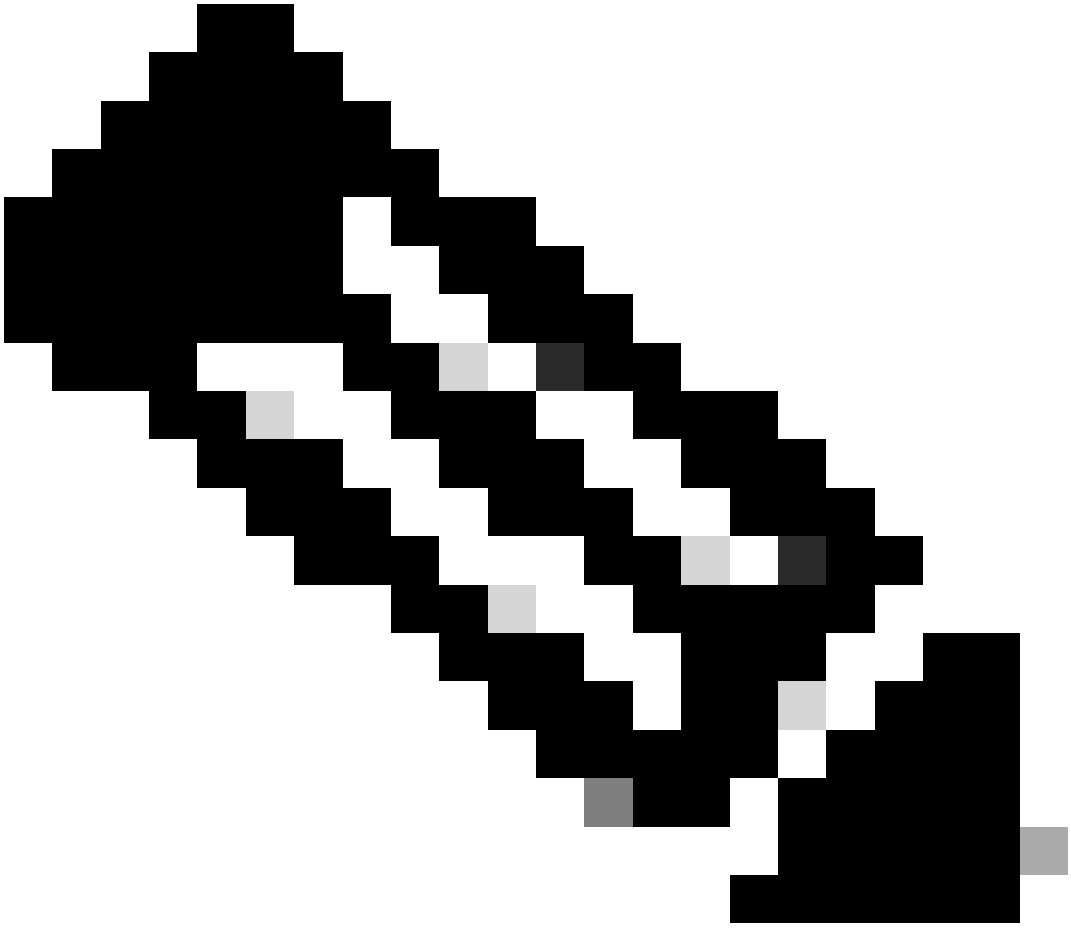
Rechercher des événements à l'aide de requêtes SPL



Vérifiez l'onglet Statistiques

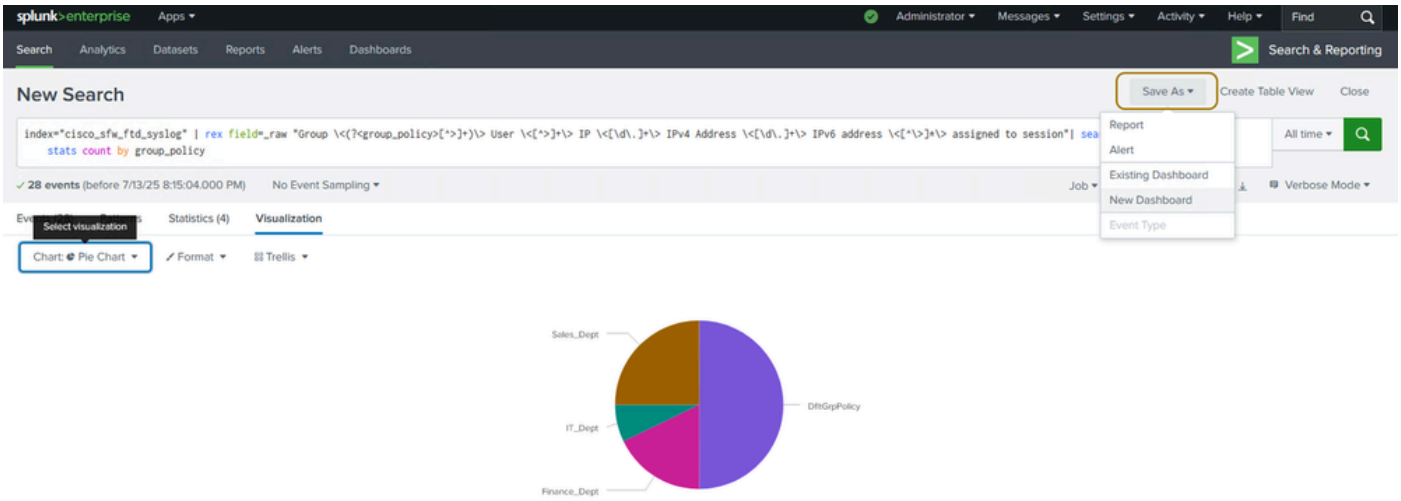


L'onglet Visualisation affiche le graphique/graphique



Remarque : Dans cet exemple, la requête recherche des journaux pour les connexions VPN d'accès à distance réussies à travers différentes stratégies de groupe. Un graphique à secteurs a été utilisé afin de visualiser le nombre et le pourcentage de connexions réussies par stratégie de groupe. En fonction de vos besoins et préférences, vous pouvez choisir d'utiliser un autre type de visualisation, tel qu'un graphique à barres.

Étape 3. Cliquez sur Enregistrer sous et choisissez Nouveau tableau de bord ou Tableau de bord existant selon que vous disposez déjà d'un tableau de bord auquel vous voulez ajouter ce panneau ou que vous voulez en créer un nouveau. Cet exemple illustre ce dernier.



Enregistrer le panneau dans un tableau de bord

Étape 4. Attribuez un titre au tableau de bord que vous créez et fournissez un titre au panneau qui contiendra le graphique à secteurs.

Save Panel to New Dashboard

Dashboard Title: FTD_Dashboard

ftd_dashboard — Edit ID

Description: Optional

Permissions: Private

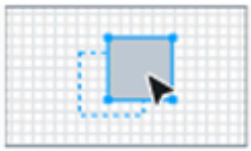
How do you want to build your dashboard? What's this?

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

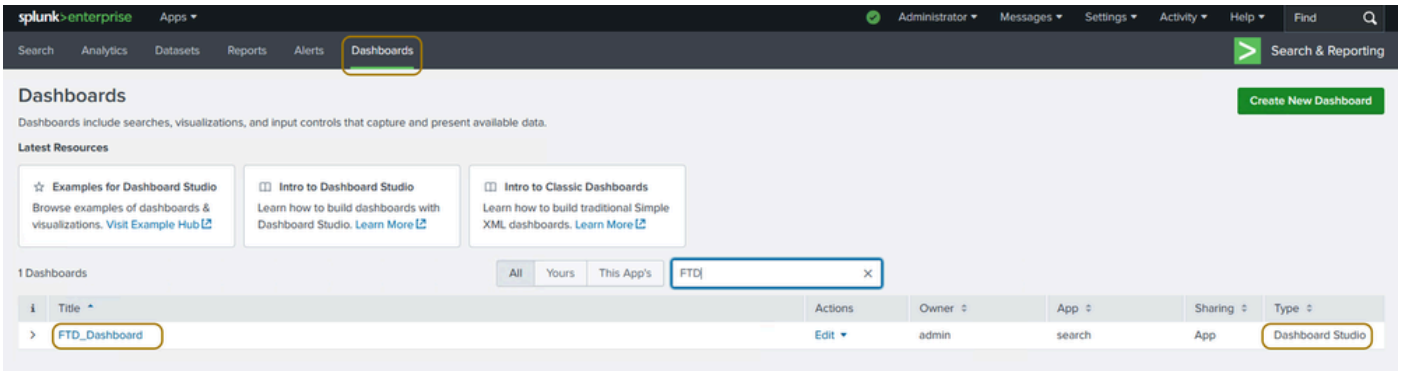
Cancel | Save to Dashboard

Paramètres du nouveau tableau de bord

Vous pouvez définir les autorisations sur Privé ou Partagé dans l'application selon que vous êtes seul autorisé à afficher le tableau de bord ou que d'autres utilisateurs ayant accès à l'instance Splunk sont également autorisés. En outre, selon que vous souhaitez ou non un contrôle granulaire des paramètres du panneau et de la disposition du tableau de bord, choisissez le mode Studio classique ou Tableau de bord pour créer votre tableau de bord.

Étape 5 (facultatif). Exécutez et enregistrez d'autres requêtes SPL sous forme de panneaux dans ce tableau de bord, conformément à vos besoins, en suivant les étapes mentionnées précédemment.

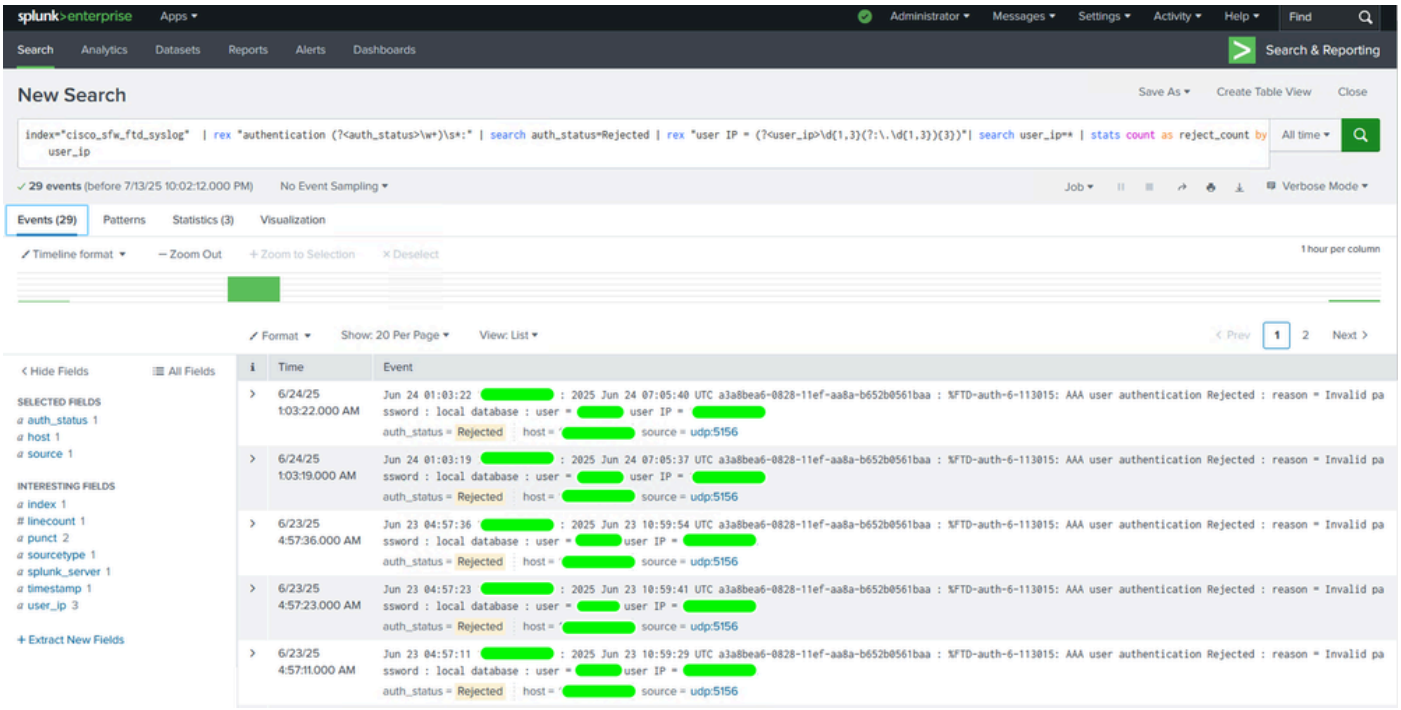
Étape 6. Accédez à l'onglet Tableau de bord afin de rechercher et de choisir le tableau de bord que vous avez créé. Cliquez dessus pour afficher, modifier ou réorganiser ses panneaux.



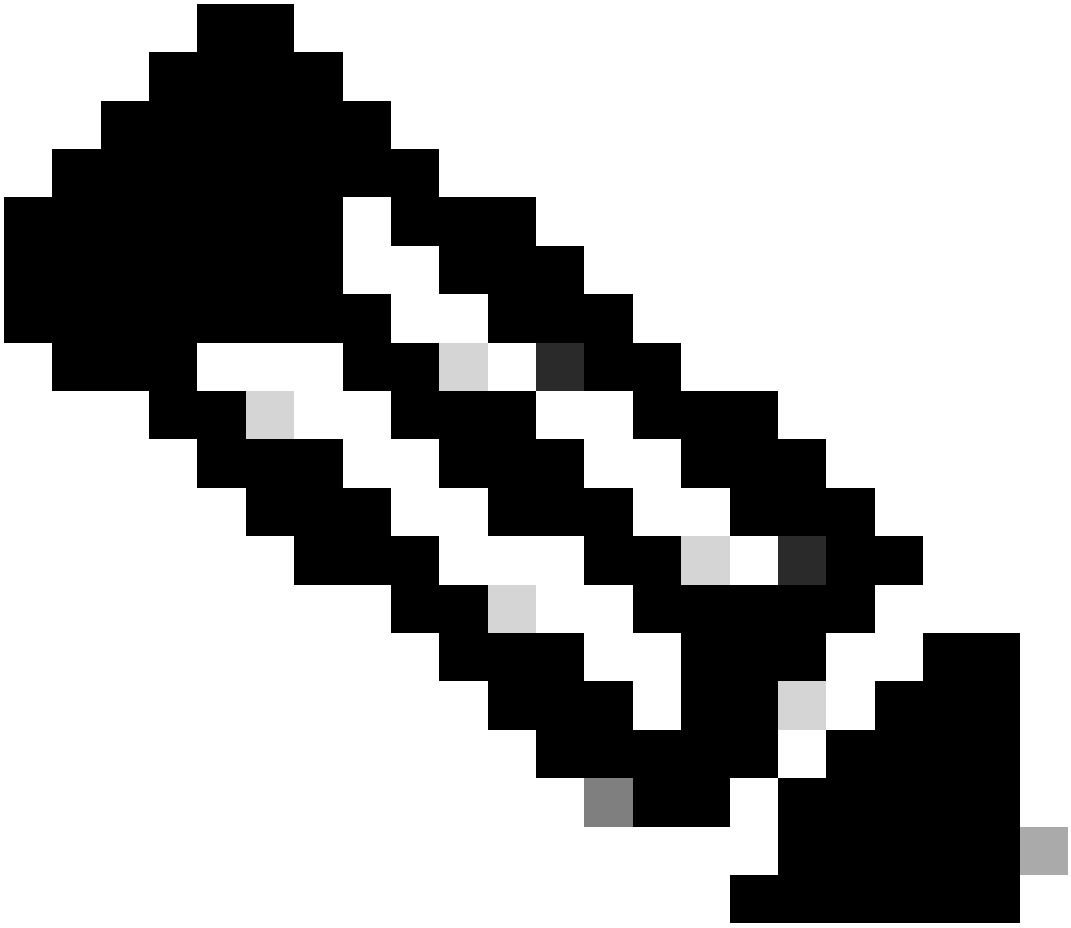
Affichage du tableau de bord

Configuration des alertes en fonction des requêtes SPL

Étape 1. Accédez à l'application de recherche et de création de rapports pour créer et exécuter votre requête SPL afin de vérifier qu'elle extrait les journaux corrects qui seront utilisés pour déclencher l'alerte.



Exécuter des requêtes SPL pour créer des alertes respectives



Remarque : Dans cet exemple, la requête est utilisée pour rechercher les journaux d'authentification en échec pour le VPN d'accès à distance afin de déclencher des alertes lorsque le nombre de tentatives infructueuses dépasse un certain seuil dans un certain laps de temps.

Étape 3. Cliquez sur Enregistrer sous et sélectionnez Alerte.

Enregistrer l'alerte

Étape 4. Attribuez un nom à l’alerte. Renseignez tous les autres détails et paramètres requis pour configurer l'alerte, puis cliquez sur Enregistrer. Les paramètres utilisés pour cette alerte ont été

mentionnés ici.

<#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

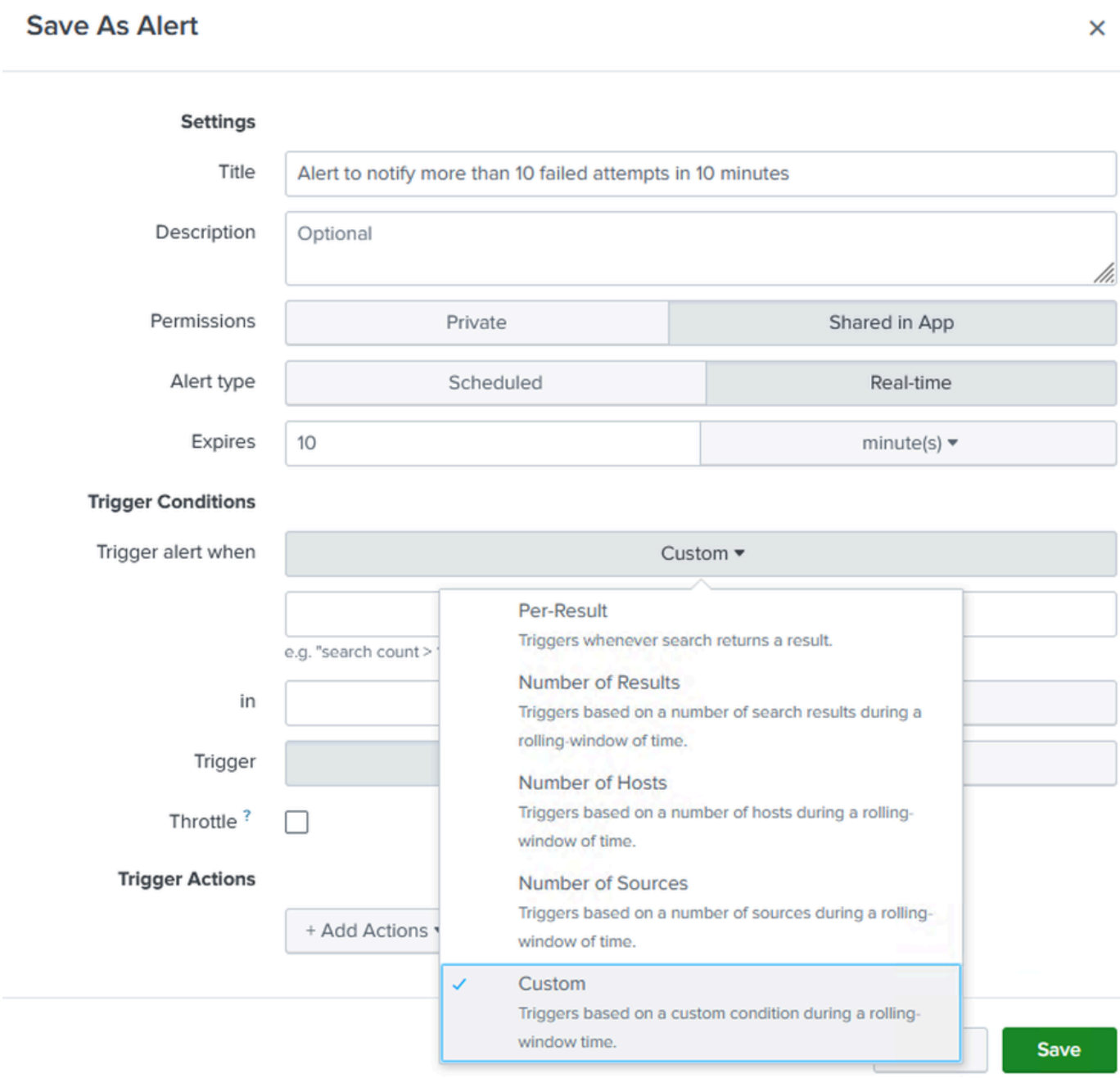
condition is used to search if the

reject_count

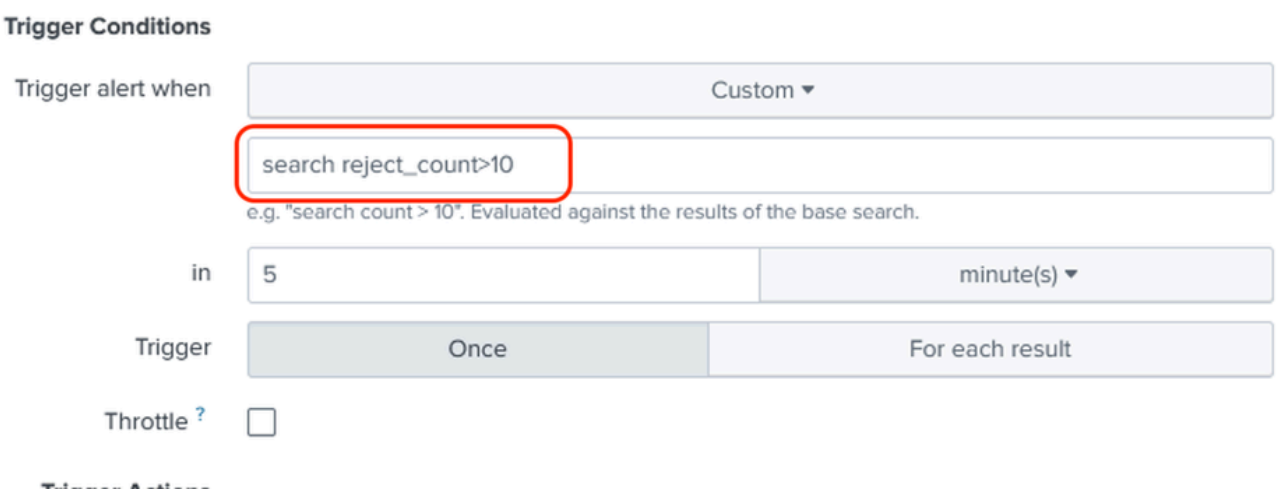
counter from the SPL query has exceeded 10 in the last 5 minutes for any IP address.
Trigger Actions: Set a trigger action such as

Add to Triggered Alerts, Send email, etc.

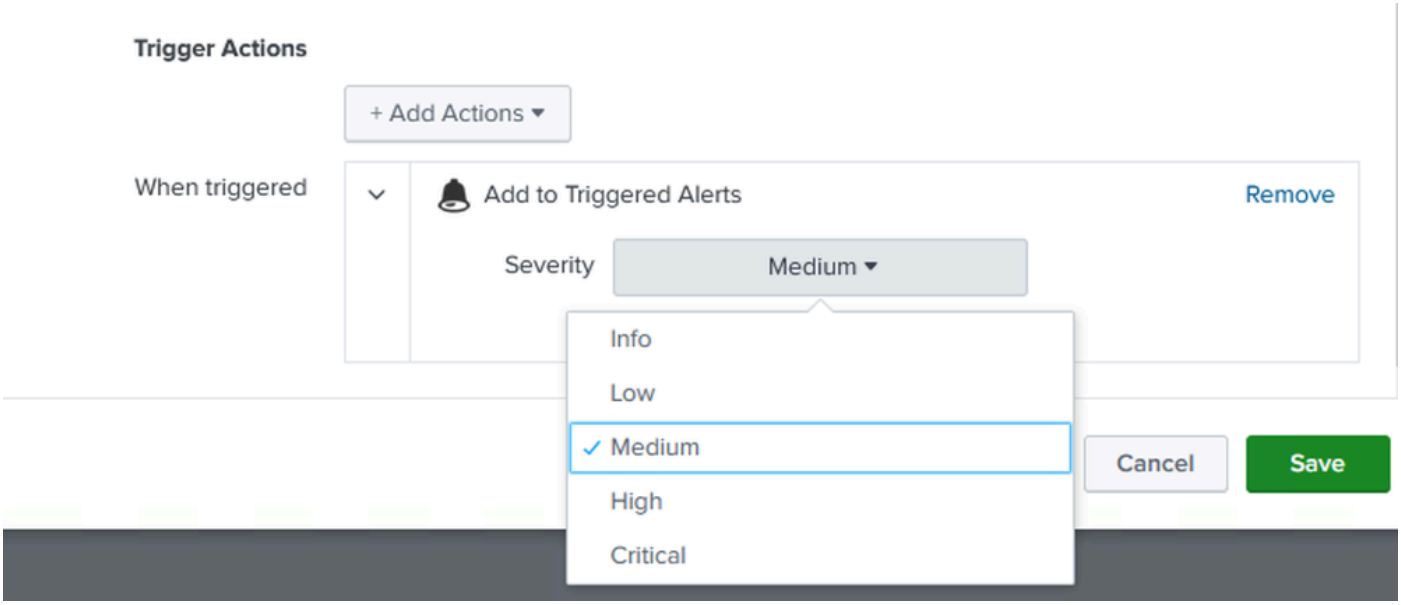
and set the alert severity as per your requirement.



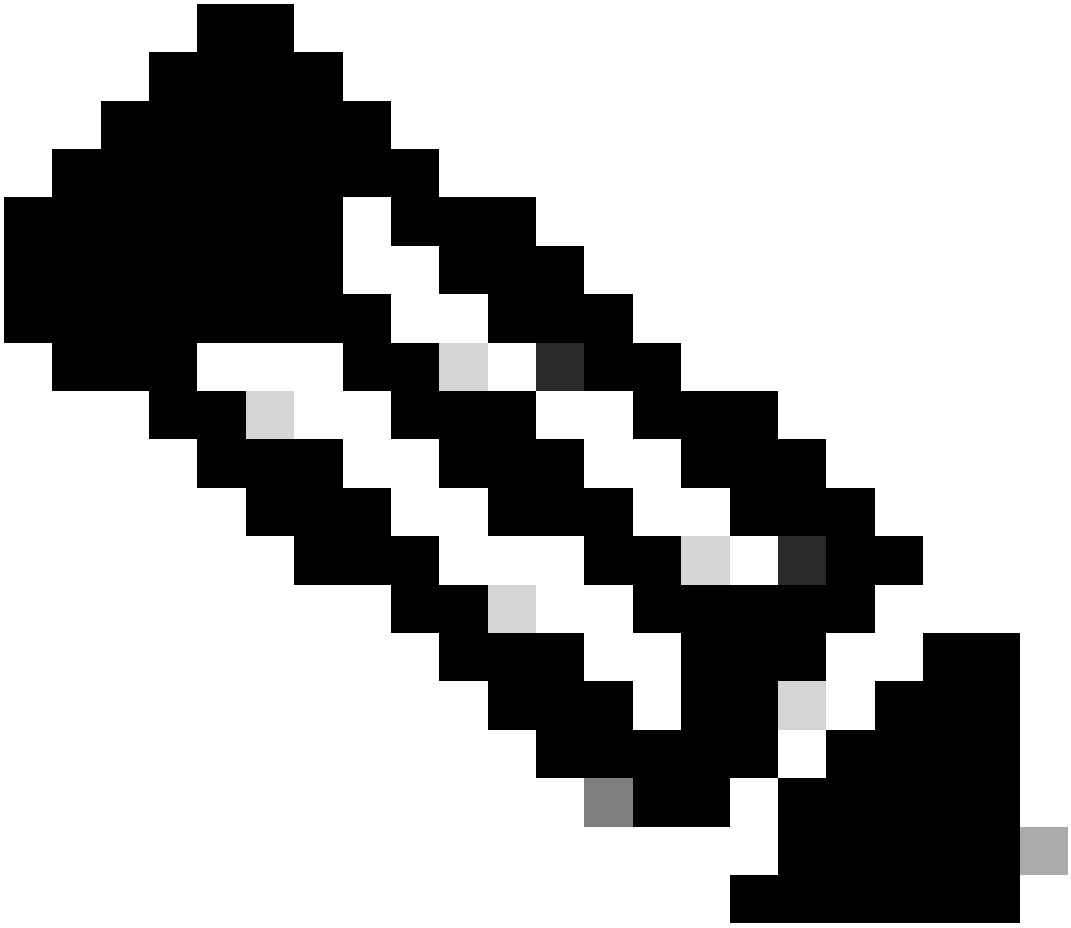
Paramètres supplémentaires pour la création d'alertes



Paramètres supplémentaires pour la création d'alertes



Paramètres supplémentaires pour la création d'alertes



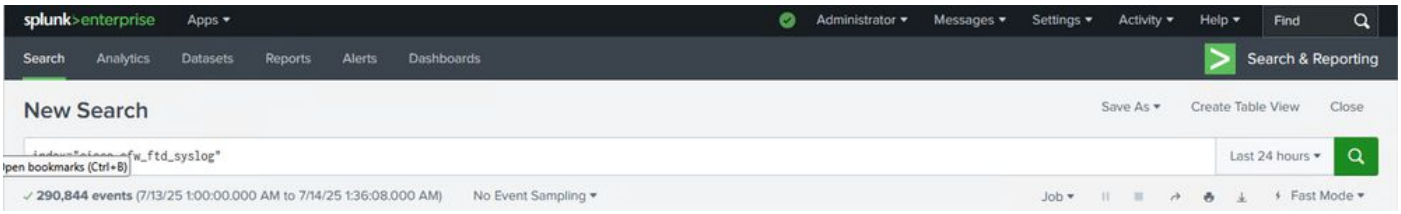
Remarque : Si vous voulez déclencher les alertes pour chaque résultat, vous devrez également définir les paramètres d'étranglement en conséquence.

Vérifier

Une fois que vous avez créé les tableaux de bord et les alertes, vous pouvez vérifier les configurations, le flux de données, les tableaux de bord et les alertes en temps réel en suivant les instructions fournies dans cette section.

Afficher les journaux

Vous pouvez utiliser l'application de recherche afin de confirmer si les journaux envoyés par le pare-feu sont reçus et visibles par la tête de recherche de splunk. Vous pouvez le vérifier en vérifiant les derniers journaux indexés (index de recherche = "cisco_sfw_ftd_syslog") et l'horodatage qui leur est associé.

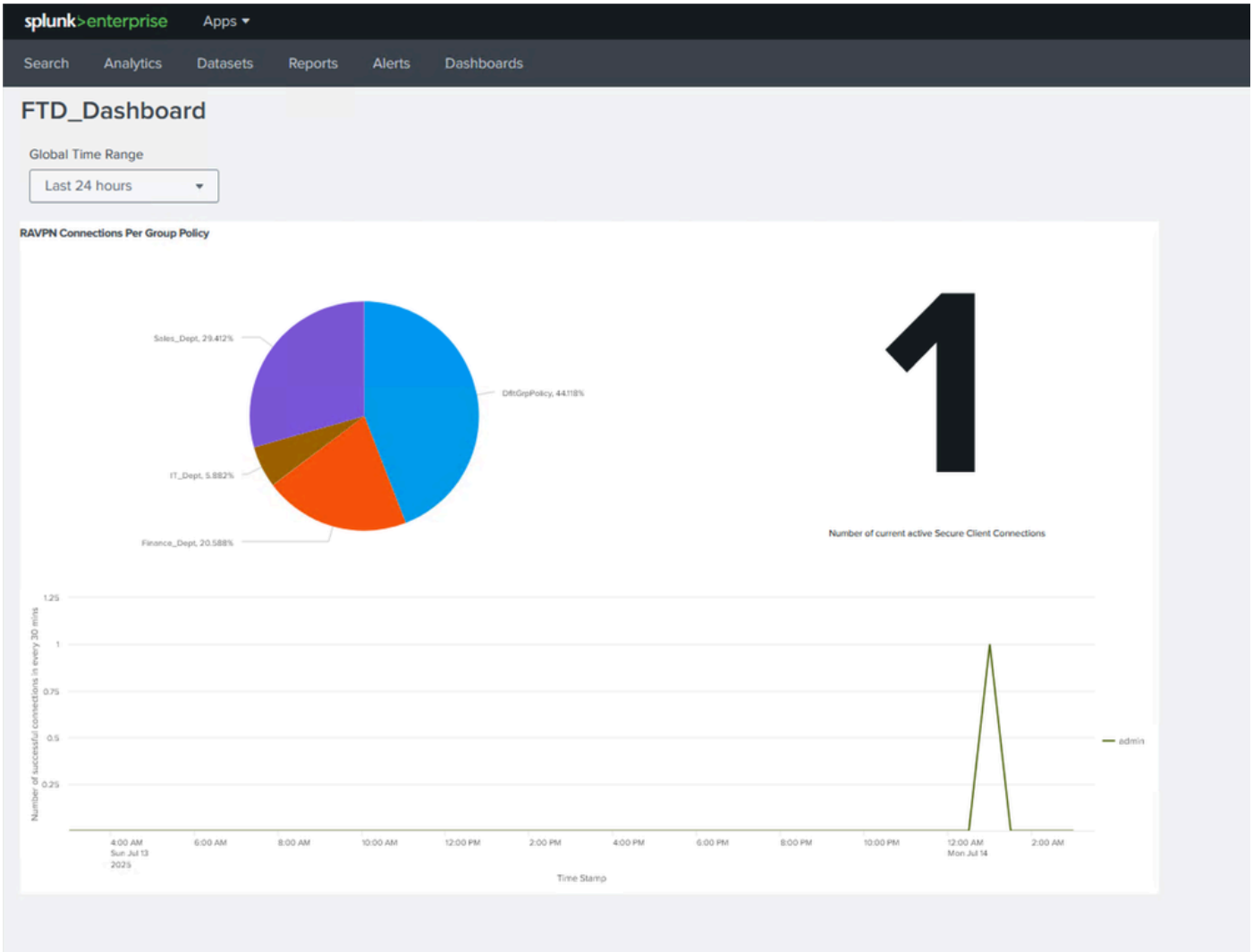


Vérifier et afficher les journaux

Vérifier et afficher les journaux

Afficher les tableaux de bord en temps réel

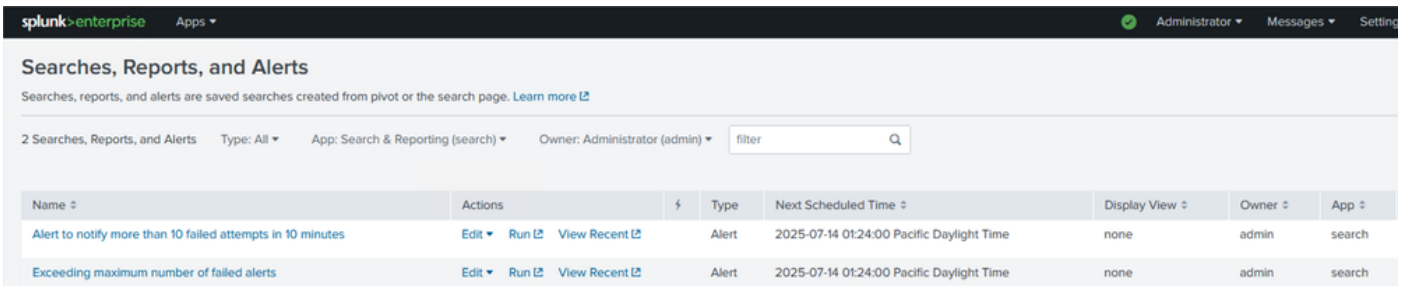
Vous pouvez naviguer jusqu'au tableau de bord personnalisé que vous avez créé et voir les modifications sur chacun des panneaux lorsque de nouvelles données et de nouveaux journaux sont générés à partir du FTD.



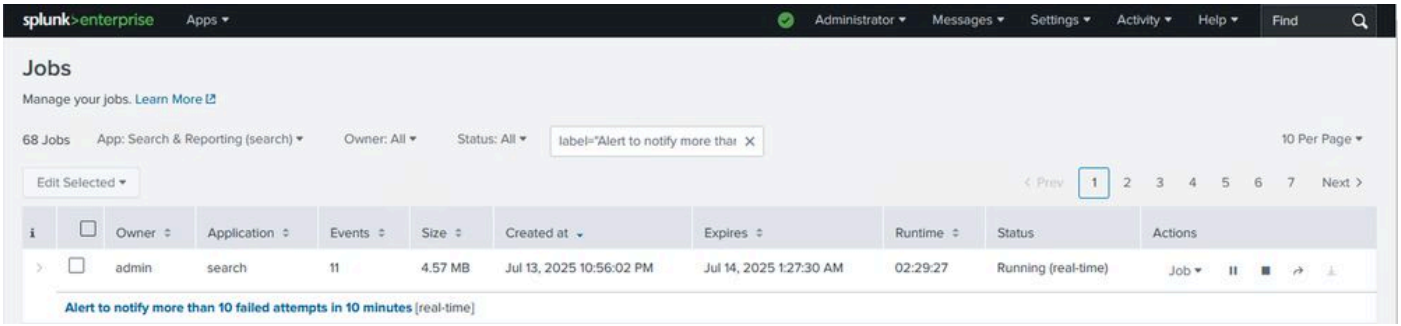
Afficher les tableaux de bord

Vérifier si des alertes ont été déclenchées

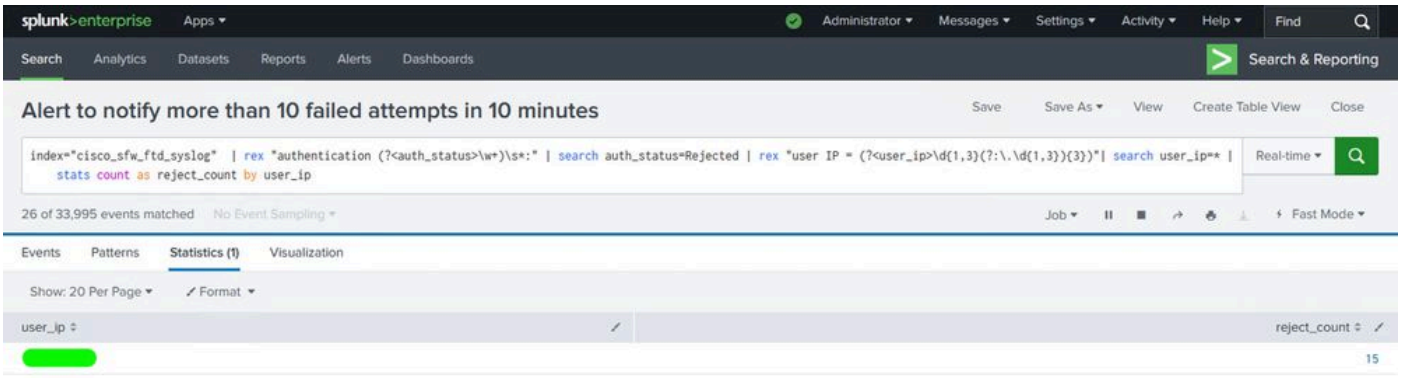
Afin de vérifier les informations sur les alertes, vous pouvez naviguer jusqu'à la section recherches, rapports et alertes pour voir les informations d'alerte récentes. Cliquez sur View Recent afin de vérifier plus en détail les travaux et les recherches.



Vérifier et afficher les alertes



Vérifier et afficher les alertes



Vérifier les statistiques pour les alertes déclenchées

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.