# Creazione di dashboard e avvisi personalizzati su Splunk mediante syslog da FTD

## Sommario



## Introduzione

In questo documento viene descritta una procedura dettagliata per la configurazione di FTD per l'invio di syslog a Splunk e per l'utilizzo di tali log per la creazione di dashboard e avvisi personalizzati.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti prima di esaminare questa guida alla configurazione:

- Syslog
- Conoscenze base di SPL (Search Processing Language) di Splunk

In questo documento si presume inoltre che l'istanza di Splunk Enterprise sia già installata in un server e che si disponga dell'accesso all'interfaccia Web.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Firepower Threat Defense (FTD) in esecuzione sulla versione 7.2.4
- Cisco Firepower Management Center (FMC) in esecuzione sulla versione 7.2.4
- Istanza di Splunk Enterprise (versione 9.4.3) in esecuzione su un computer Windows

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti.

# Premesse

I dispositivi Cisco FTD generano syslog dettagliati relativi a eventi di intrusione, policy di controllo dell'accesso, eventi di connessione e altro ancora. L'integrazione di questi registri con Splunk consente un'analisi efficace e l'invio di avvisi in tempo reale per le operazioni di sicurezza della rete.

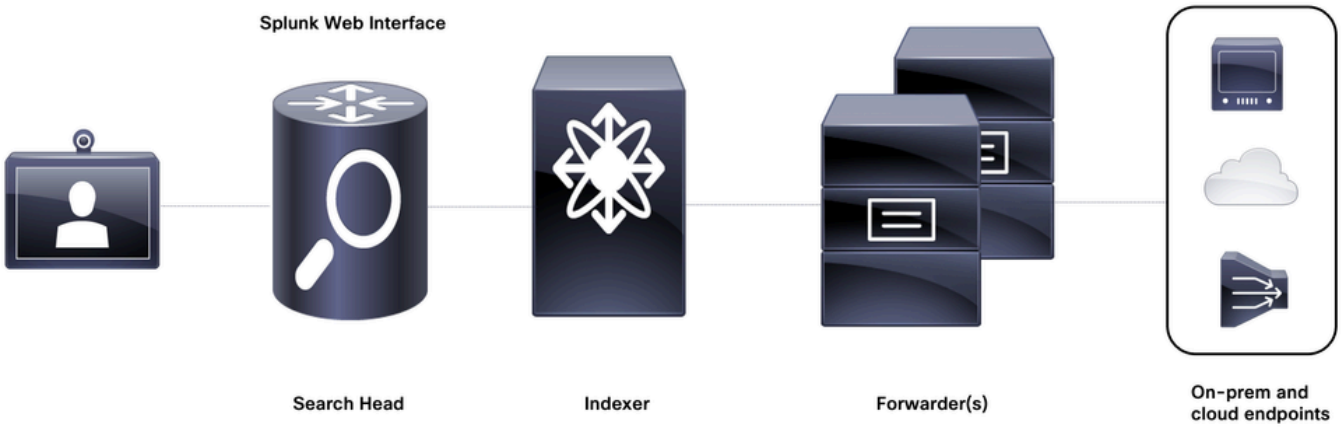
Splunk è una piattaforma di analisi dei dati in tempo reale progettata per acquisire, indicizzare, ricercare e visualizzare i dati generati dalla macchina. Splunk è particolarmente efficace negli ambienti di cibersicurezza come strumento SIEM (Security Information and Event Management) grazie alla sua capacità di:

- Caricamento dei dati di log in scala
- Esecuzione di ricerche complesse con SPL
- Creare dashboard e avvisi
- Integrazione con i sistemi di gestione della sicurezza e di risposta agli incidenti

Splunk elabora i dati attraverso una pipeline strutturata in modo da rendere i dati di macchine non strutturate o semistrutturate utili e utilizzabili. Le fasi principali di questa conduttura sono spesso denominate IPIS, che rappresentano:

- Ingresso
- Analisi
- Indicizzazione
- Ricerca

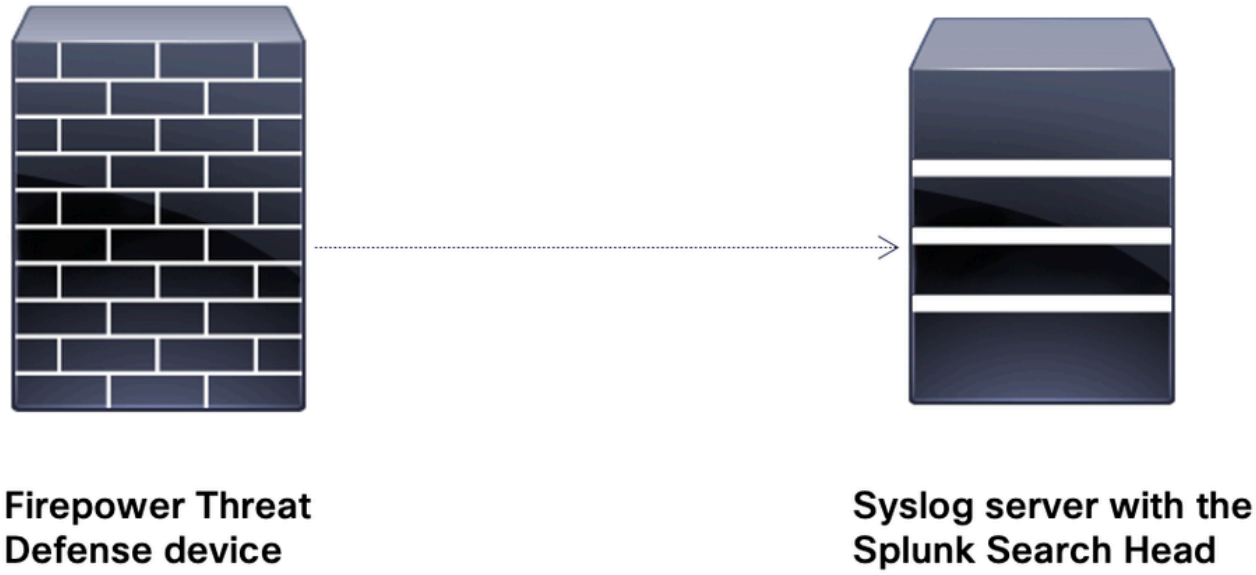
I principali componenti generali dell'architettura sottostante utilizzati per realizzare la pipeline IPIS sono illustrati nel seguente diagramma:



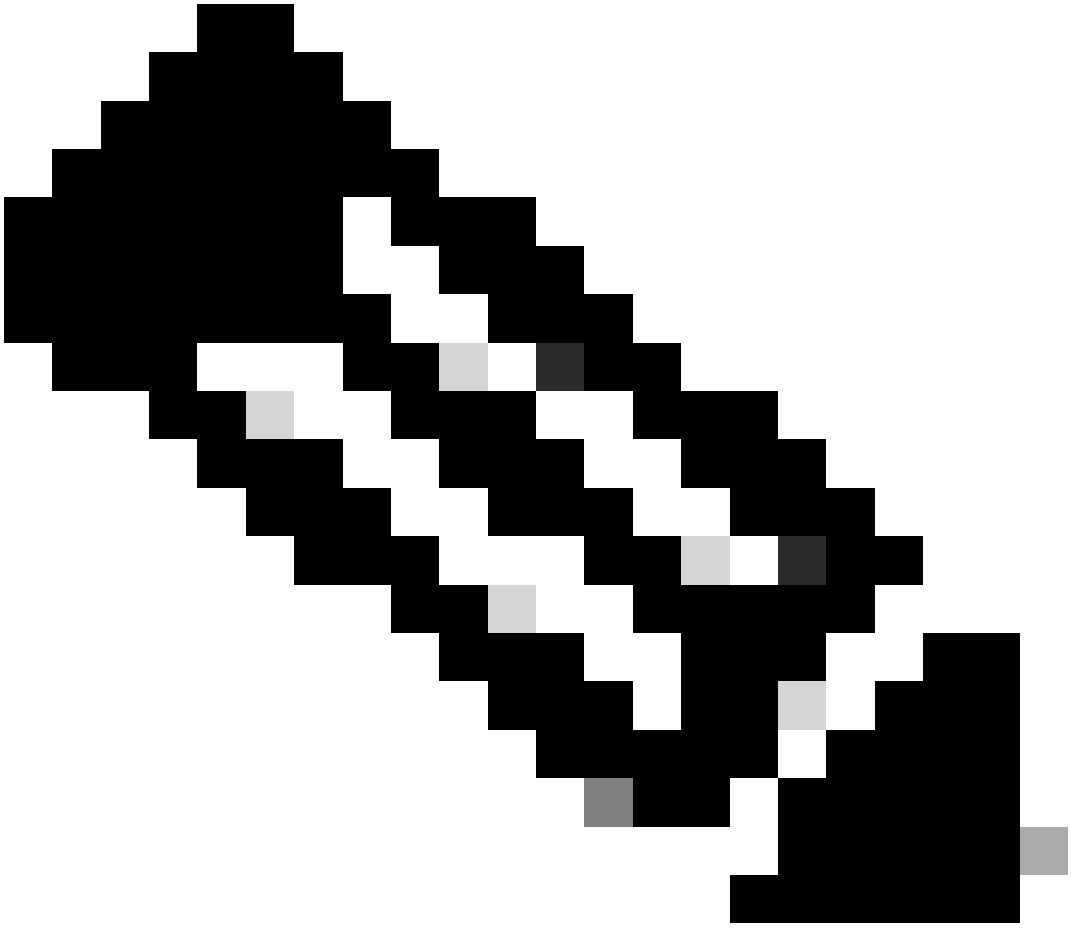

Architettura di base di Splunk

# Configurazione

## Esempio di rete




Esempio di rete

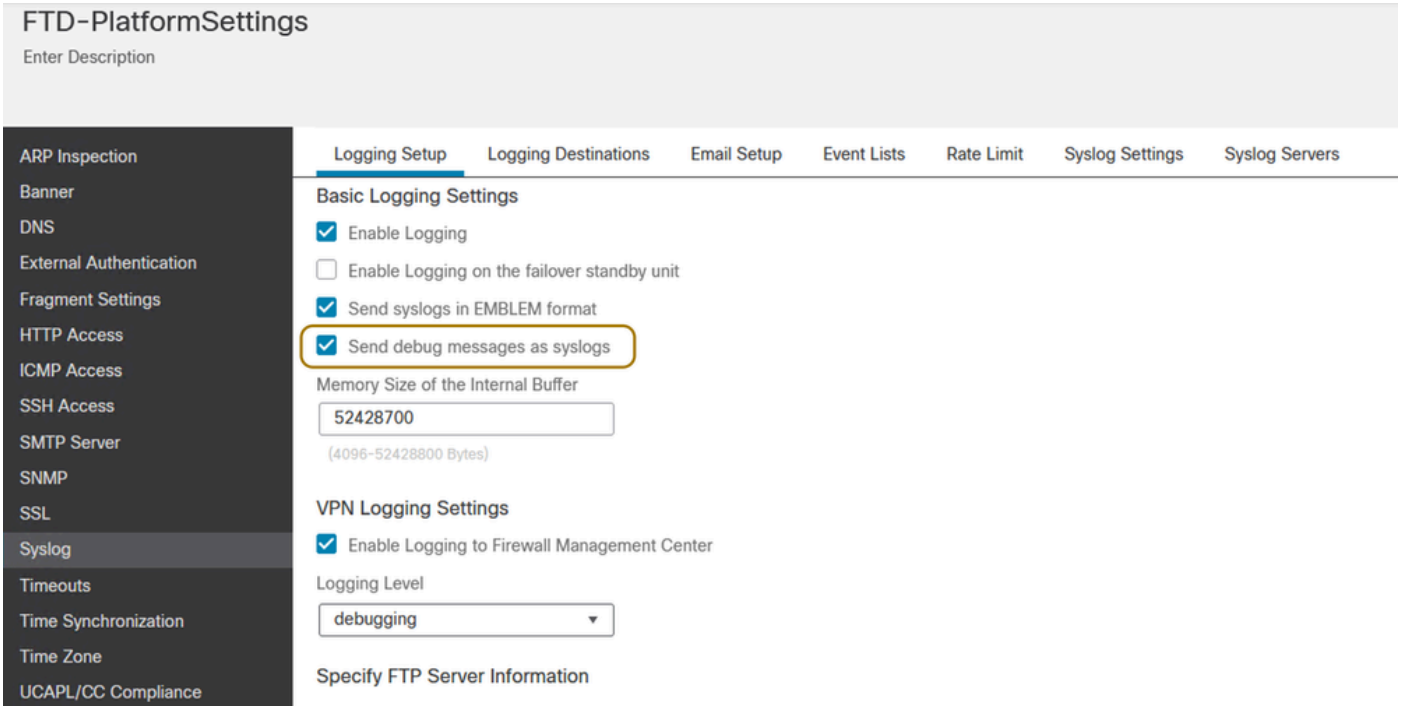


Nota: L'ambiente lab per questo documento non richiede istanze separate del server di inoltro e dell'indicizzatore. Il computer Windows, ovvero il server syslog in cui è installata l'istanza Splunk Enterprise, funge da indicizzatore e da testa di ricerca.

## Configurazioni

### Configurazione delle impostazioni syslog per FTD

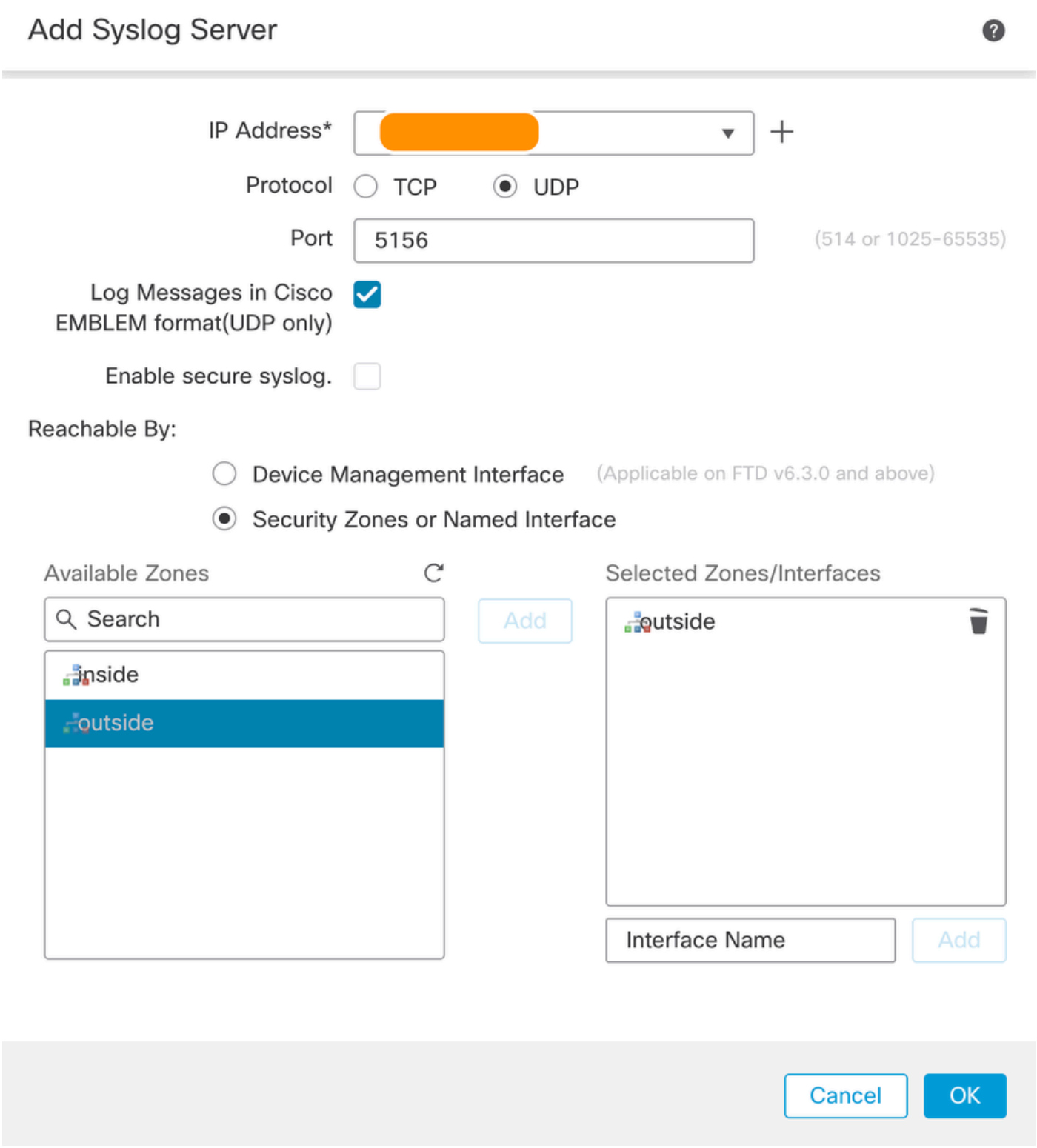
Passaggio 1. Configurare le impostazioni preliminari del syslog su FMC per FTD in Dispositivi > Impostazioni piattaforma per inviare i log al server syslog su cui è in esecuzione l'istanza Splunk.



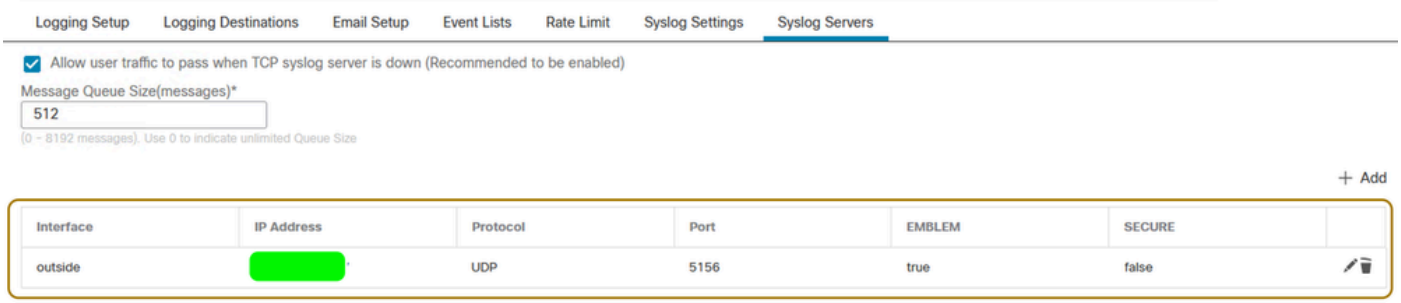

Impostazioni piattaforma su FTD - Syslog

Passaggio 2. Configurare l'indirizzo IP del computer in cui è installata l'istanza di Splunk Enterprise ed eseguirla come server Syslog. Definire i campi come indicato.

```
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
```

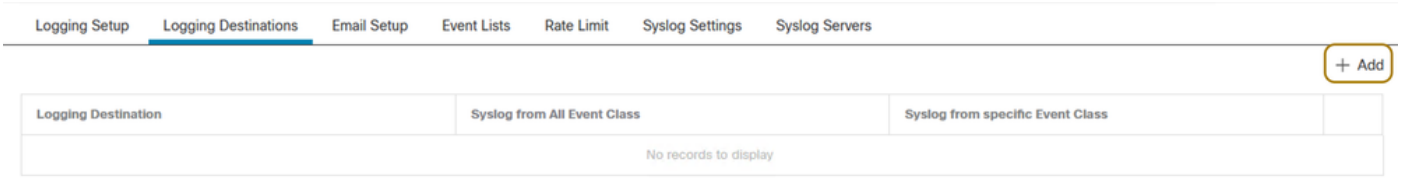



Impostazioni piattaforma su FTD - Aggiungi server syslog

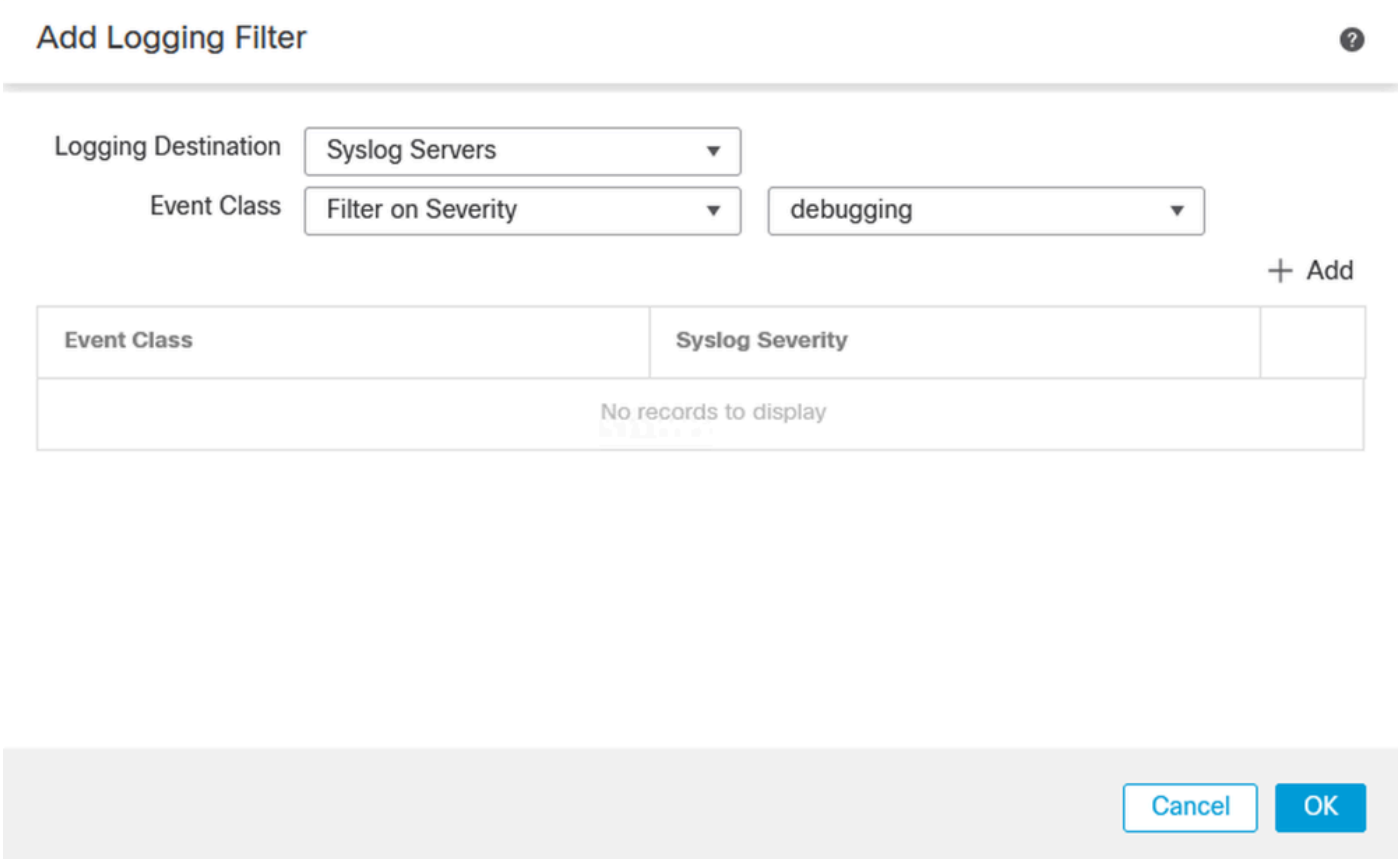



Impostazioni piattaforma su FTD - server syslog aggiunto

Passaggio 3. Aggiungere una destinazione di registrazione per i server Syslog. Il livello di log può essere impostato in base alla propria scelta o allo Use Case.




Impostazioni piattaforma su FTD - Aggiungi destinazione di registrazione




Impostazioni piattaforma su FTD - Impostazione del livello di gravità per la destinazione di registrazione

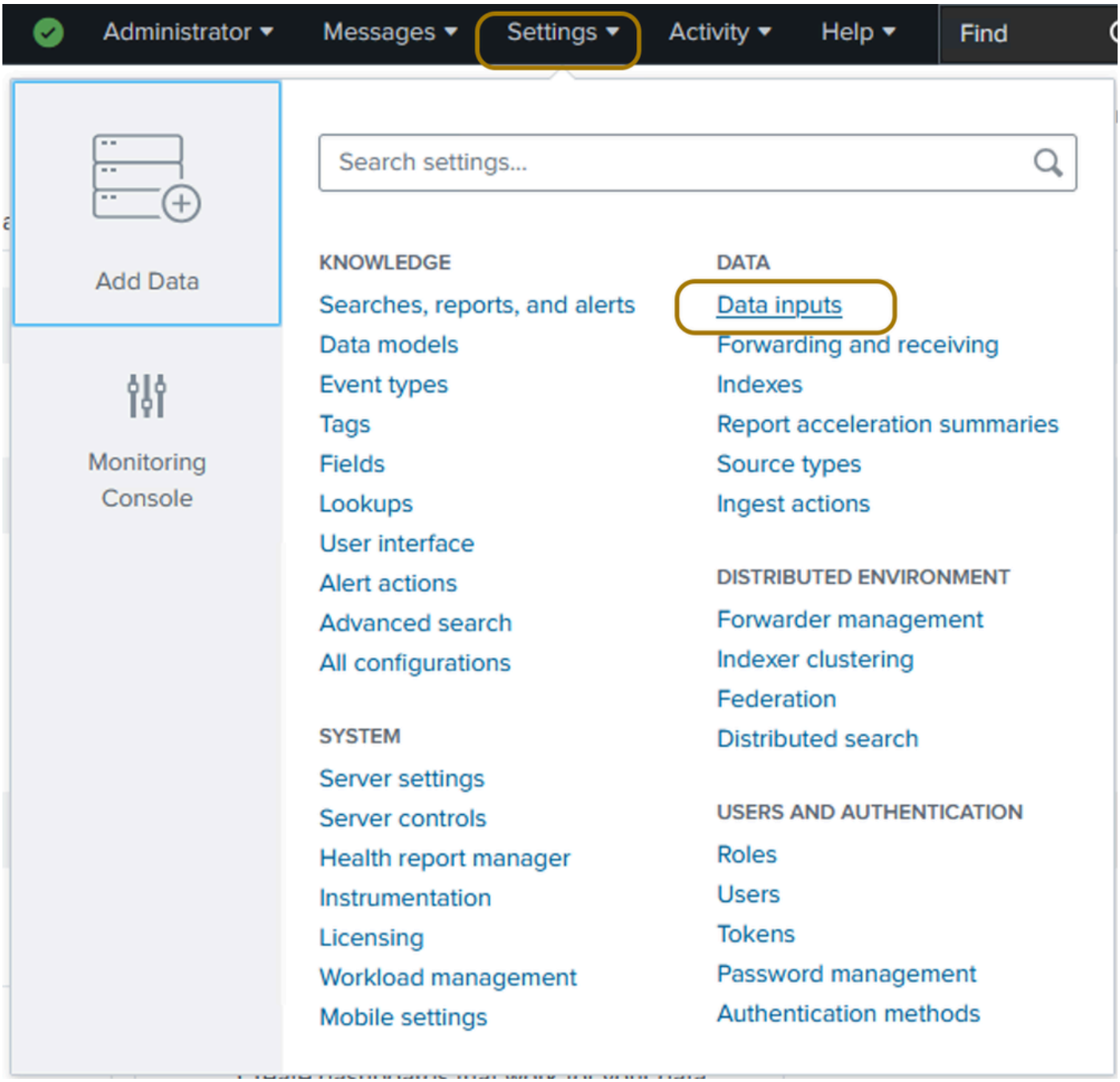
Dopo aver completato questi passaggi, distribuire le modifiche alle impostazioni della piattaforma nell'FTD.

Configurare un input di dati nell'istanza di Splunk Enterprise

Passaggio 1. Accedere all'interfaccia Web dell'istanza di Splunk Enterprise.

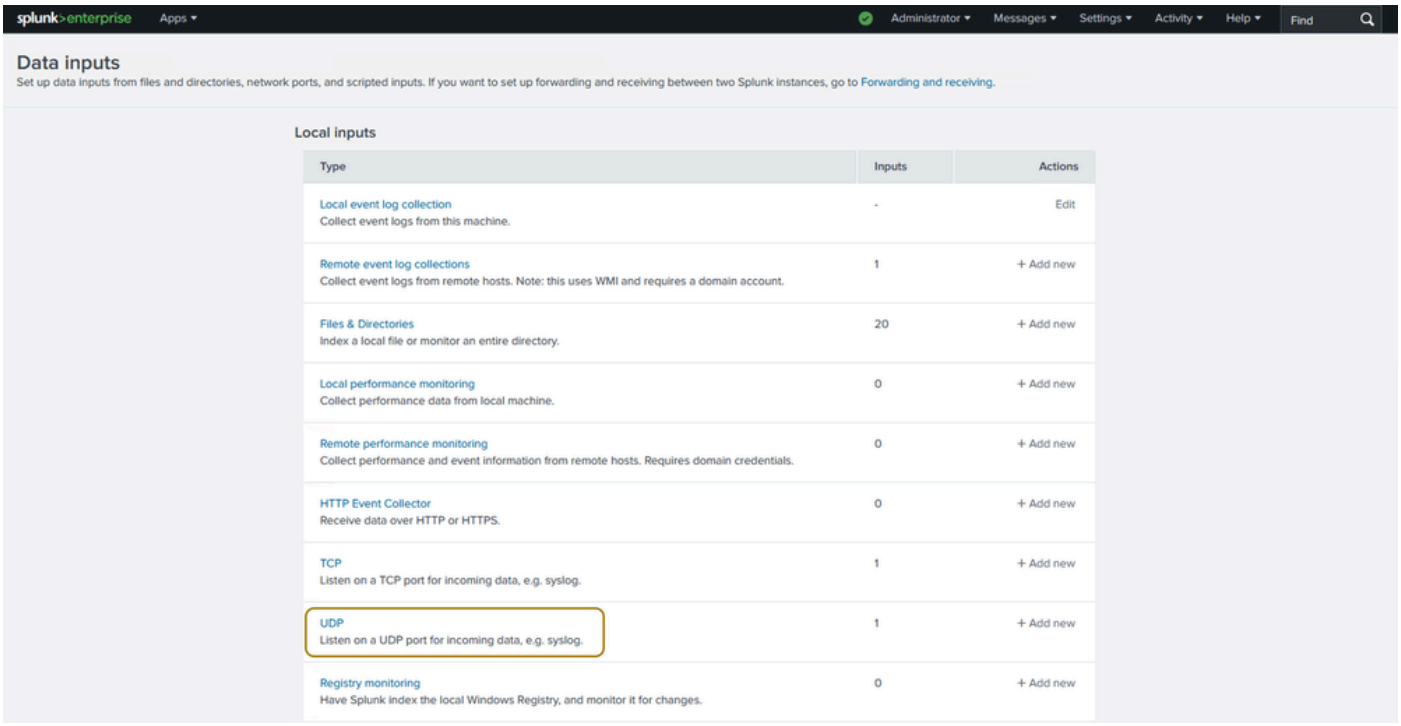

Pagina di accesso all'interfaccia Web Splunk

Passaggio 2. È necessario definire un input di dati in modo da poter archiviare e indicizzare i syslog in Splunk. Passare a Impostazioni > Dati > Input dati dopo l'accesso.

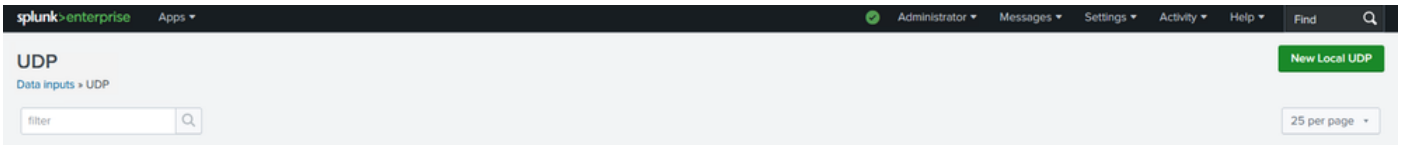



Passa agli input di dati sullo splunk

Passaggio 3. Scegliere UDP e fare clic su Nuovo UDP locale nella pagina successiva che viene visualizzata.

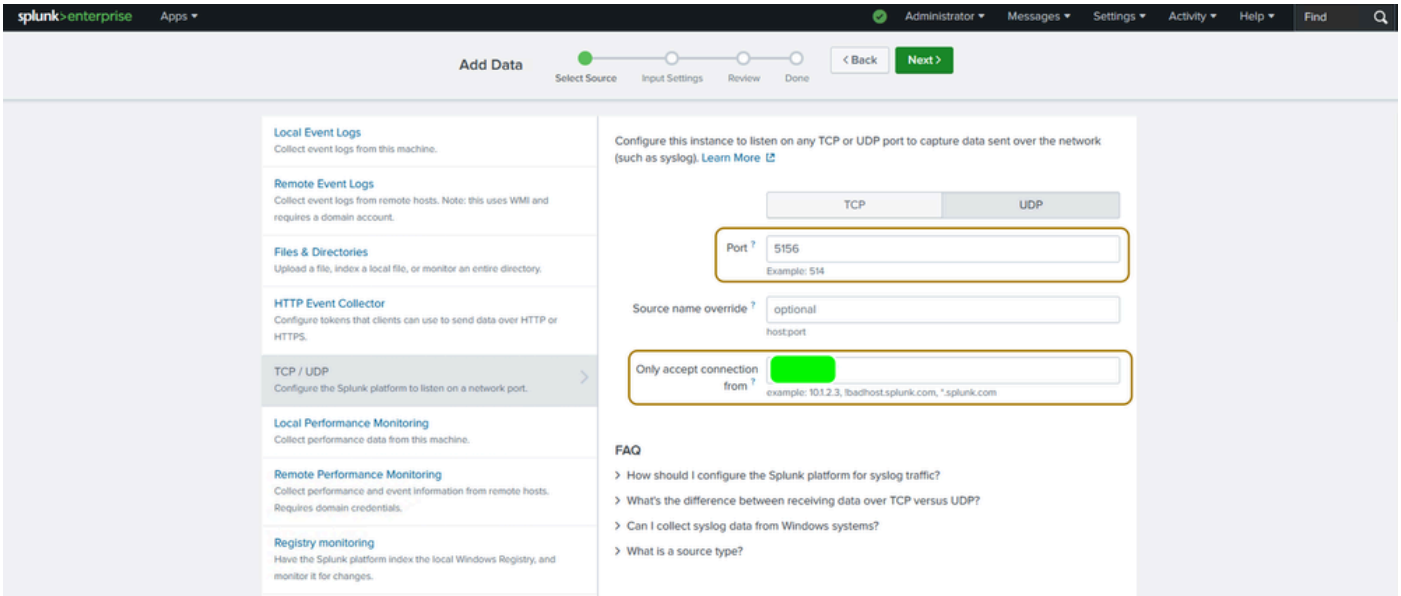



Fare clic su 'UDP' per immettere dati UDP



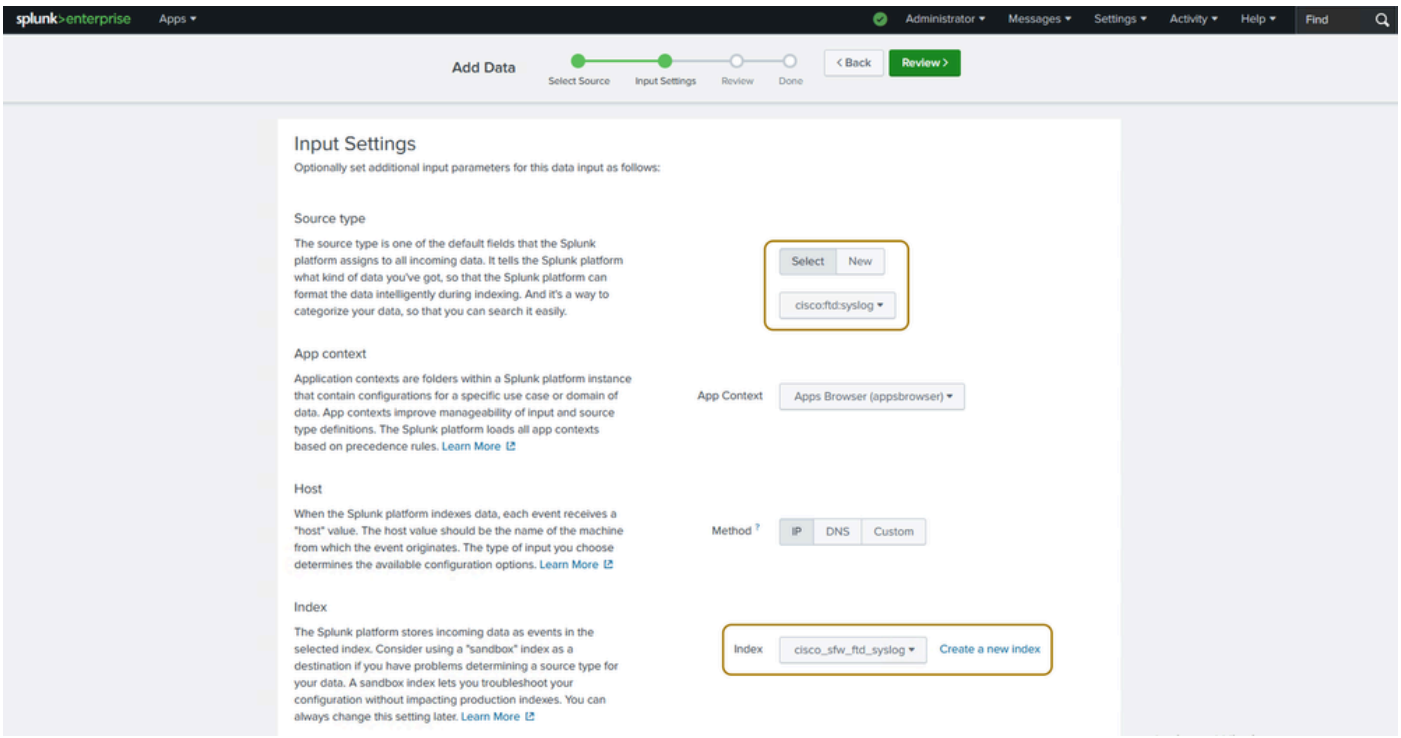

Crea un input 'Nuovo UDP locale'

Passaggio 4. Immettere la porta su cui vengono inviati i syslog. Deve essere la stessa porta configurata sulle impostazioni del syslog FTD, in questo caso 5156. Per accettare i syslog solo da un'origine (FTD), impostare il campo Accetta solo connessione da sull'indirizzo IP dell'interfaccia sull'FTD che comunica con il server Splunk. Fare clic su Next (Avanti).



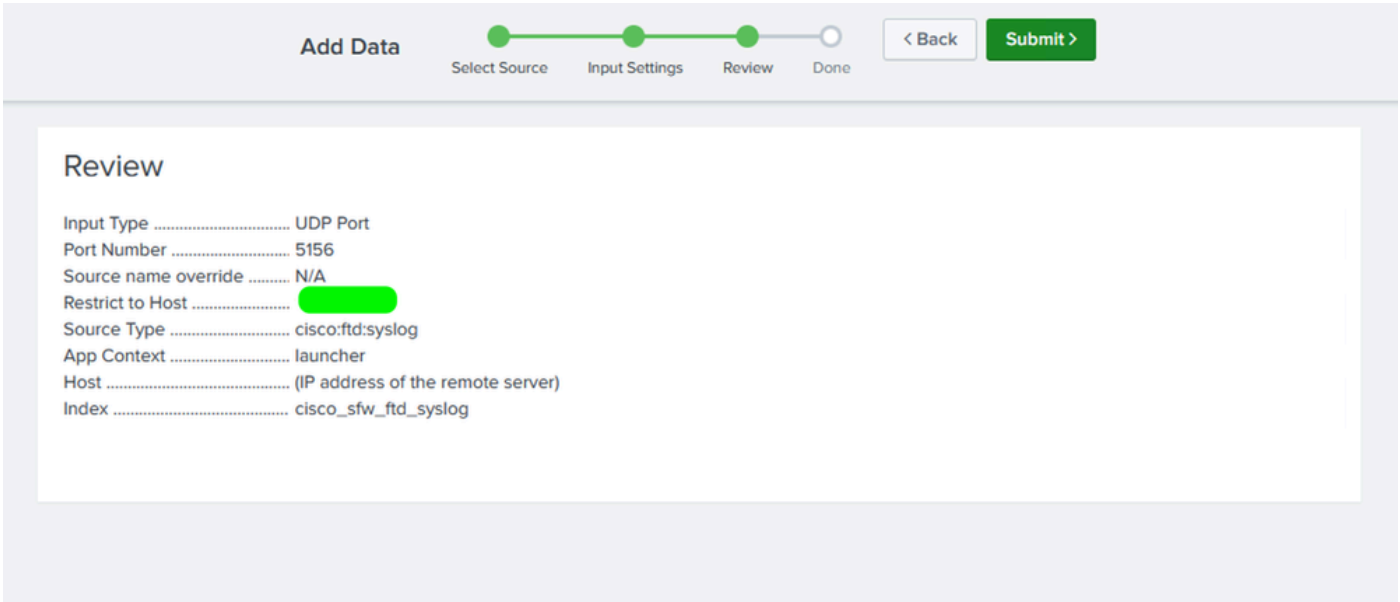

Specificare la porta e l'indirizzo IP FTD

Passaggio 5. È possibile cercare e scegliere il tipo di origine e i valori dei campi di indice tra quelli predefiniti in Splunk, come evidenziato nell'immagine successiva. È possibile utilizzare le impostazioni predefinite per i campi rimanenti.




Configura impostazioni di input dati

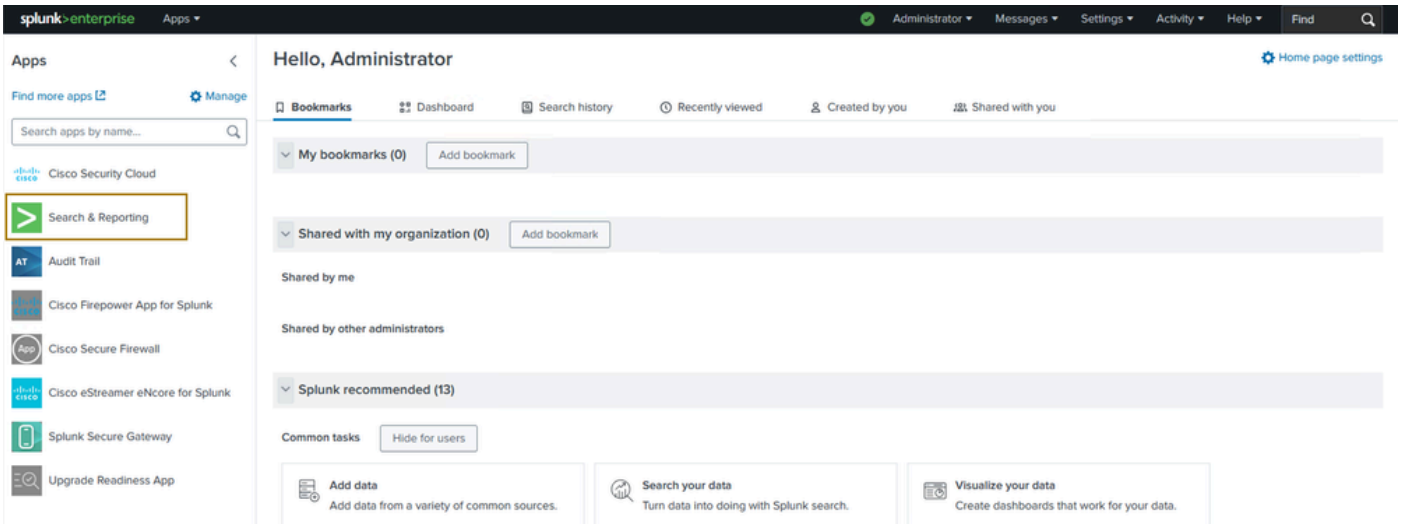
Passaggio 6. Verificare le impostazioni e fare clic su Invia.




Verifica impostazioni di input dati

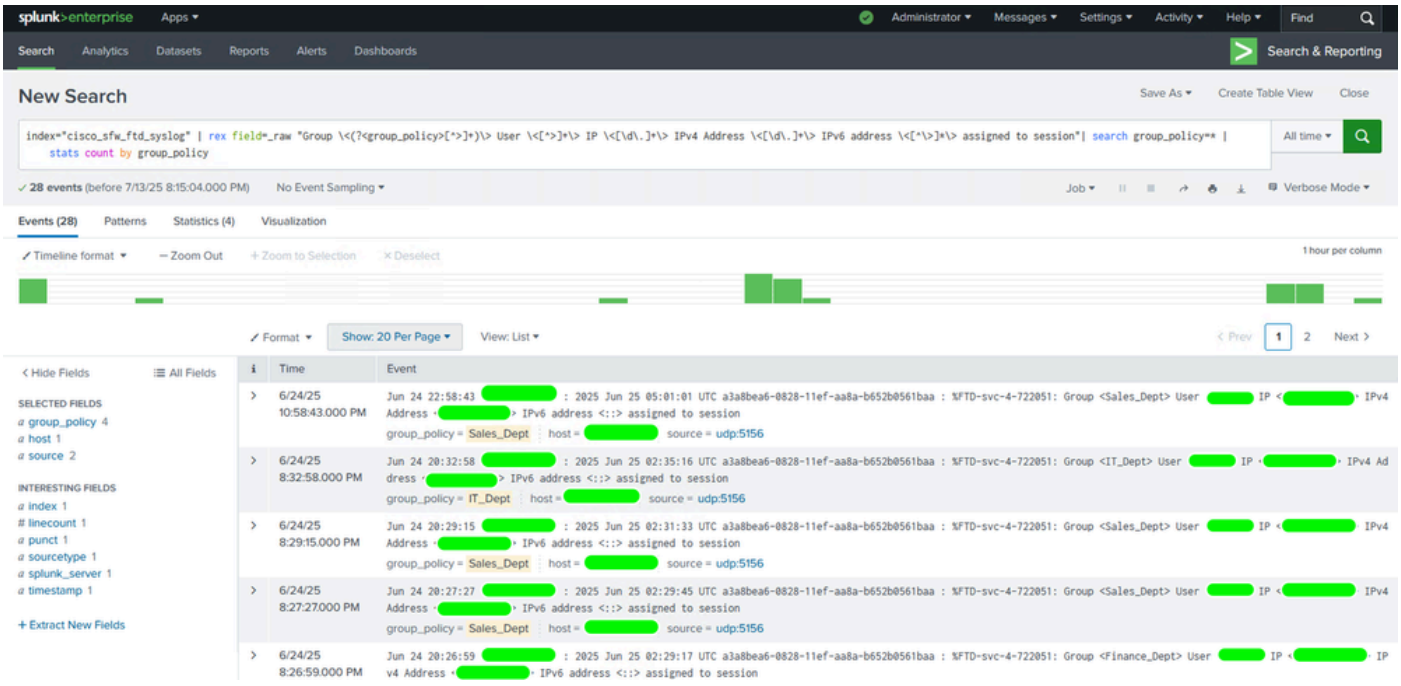
Esecuzione di query SPL e creazione di dashboard

Passaggio 1. Passare all'app Ricerca e report in Splunk.

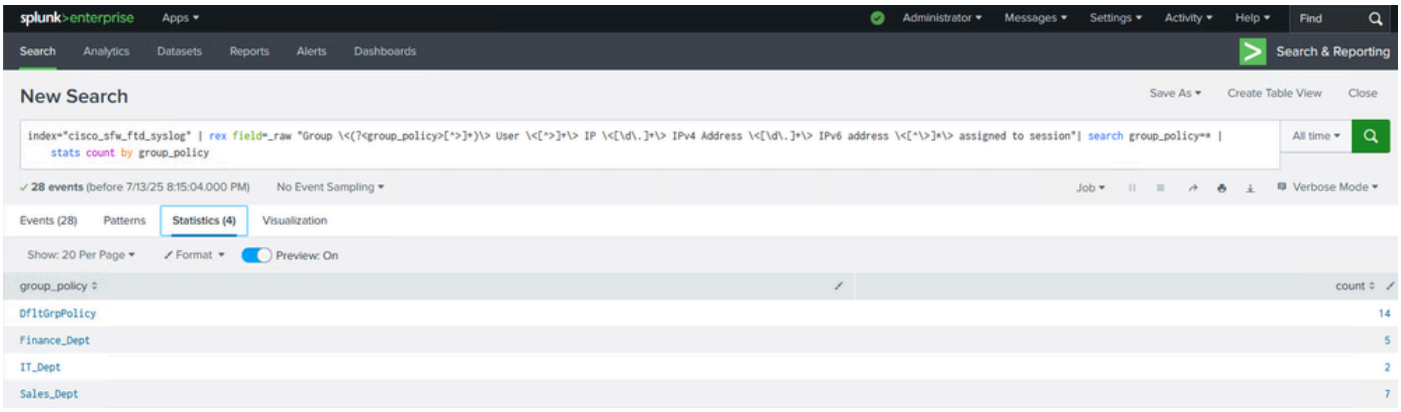



Passare all'app Ricerca e report

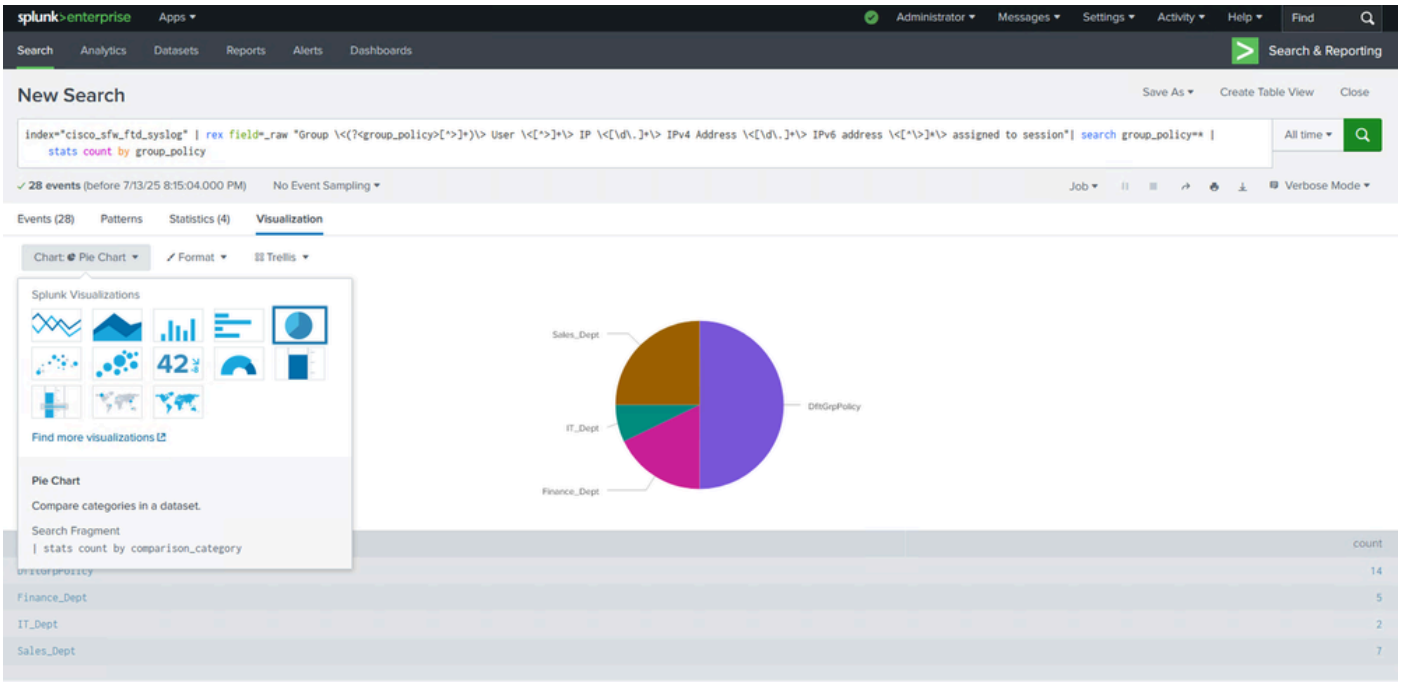
Passaggio 2. Formulare ed eseguire una query SPL in base ai dati da visualizzare. In modalità dettagliata, sarà possibile visualizzare completamente ogni registro nella scheda Eventi, il conteggio delle connessioni per criterio di gruppo nella scheda Statistiche e visualizzare questi dati utilizzando le statistiche disponibili nella scheda Visualizzazione.



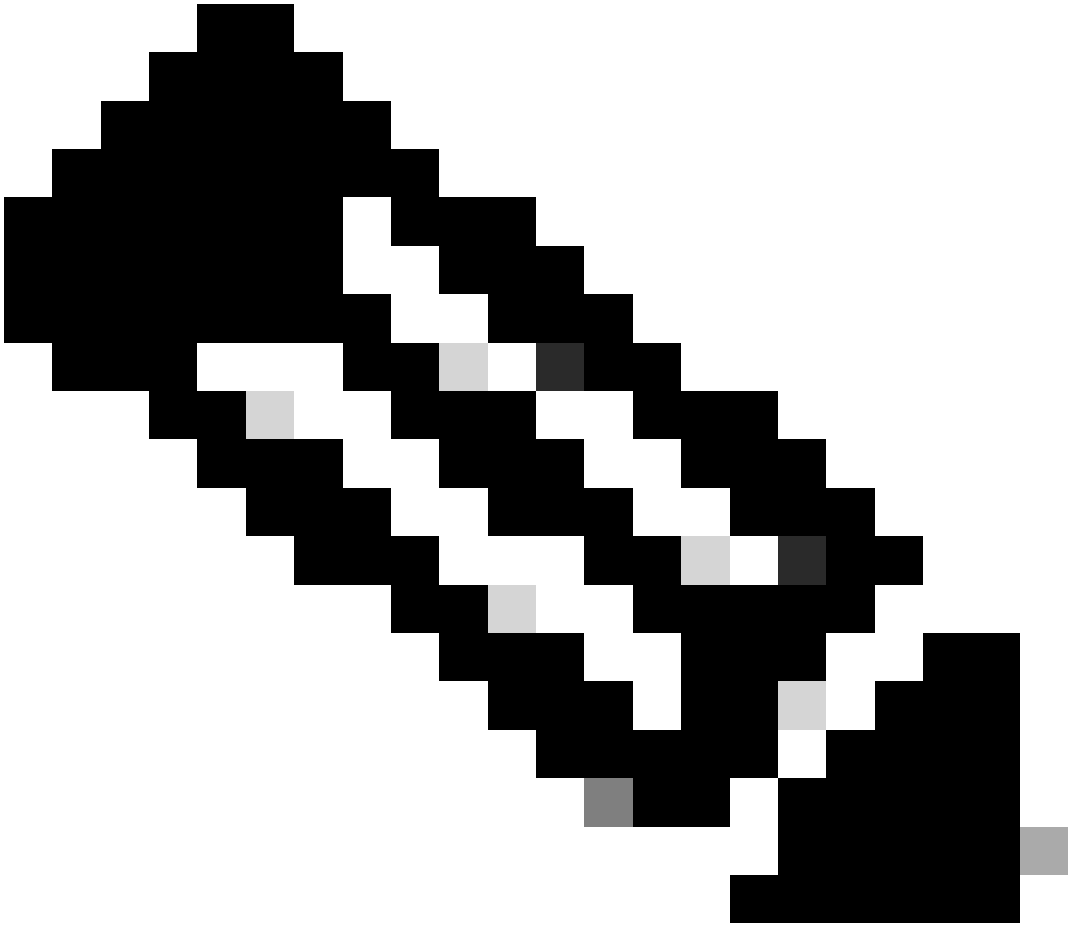

Ricerca di eventi tramite query SPL




Selezionare la scheda Statistiche

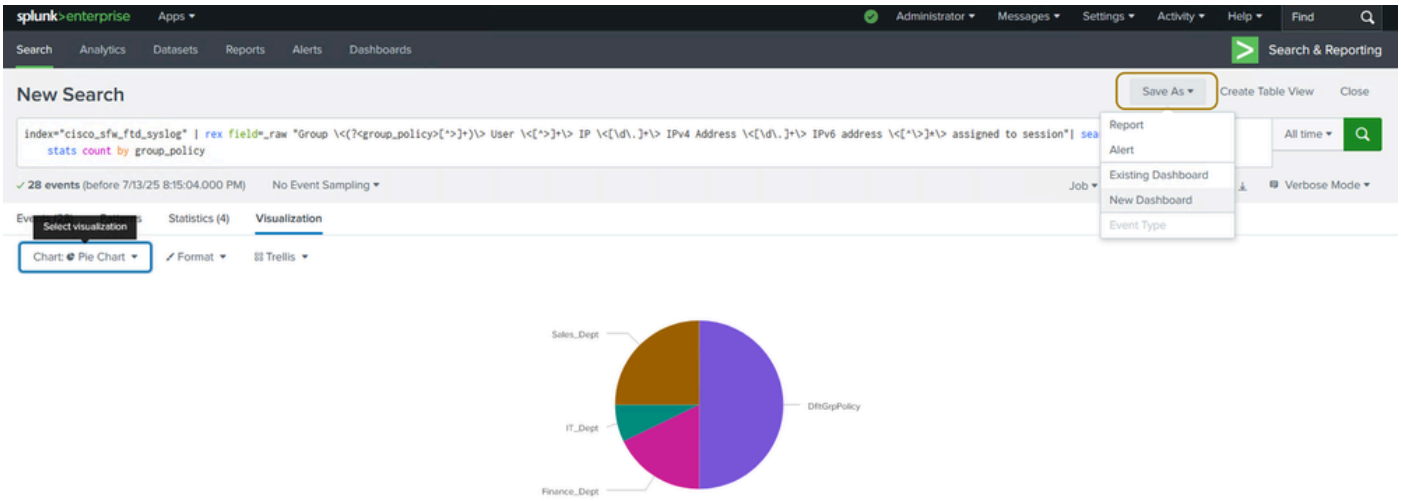



Nella scheda Visualizzazione verrà visualizzato il grafico



Nota: In questo esempio la query recupera i registri per le connessioni VPN ad accesso remoto riuscite tra criteri di gruppo diversi. È stato utilizzato un grafico a torta per visualizzare il numero e la percentuale di connessioni riuscite per criterio di gruppo. In base ai requisiti e alle preferenze, è possibile scegliere di utilizzare un tipo diverso di visualizzazione, ad esempio un grafico a barre.

Passaggio 3. Fare clic su Salva con nome e scegliere Dashboard nuovo o esistente a seconda che si disponga già di un dashboard a cui si desidera aggiungere questo pannello o crearne uno nuovo. In questo esempio viene illustrato il secondo.




Salvare il pannello in un dashboard

Passaggio 4. Assegnare un titolo al dashboard che si sta creando e specificare un titolo per il pannello che conterrà il grafico a torta.

Save Panel to New Dashboard

Dashboard Title: FTD_Dashboard

ftd_dashboard — Edit ID

Description: Optional

Permissions: Private

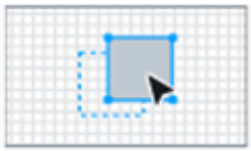
How do you want to build your dashboard? What's this?

**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

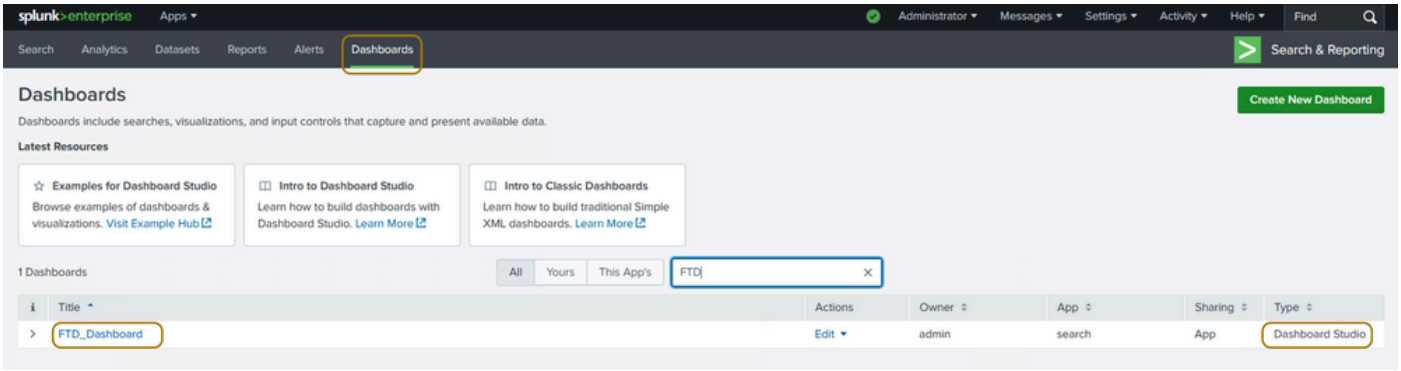
Cancel | Save to Dashboard

Impostazioni per il nuovo dashboard

È possibile impostare le autorizzazioni su Privato o Condiviso in App a seconda che sia consentito solo all'utente corrente visualizzare il dashboard o ad altri utenti con accesso all'istanza di Splunk. Inoltre, a seconda che si desideri o meno il controllo granulare sulle impostazioni del pannello e sul layout del dashboard, scegliere la modalità Classica o Dashboard Studio per creare il dashboard.

Passaggio 5 (facoltativo). Eseguite e salvate altre query SPL come pannelli in questo pannello di controllo in base alle vostre esigenze utilizzando i passi precedenti.

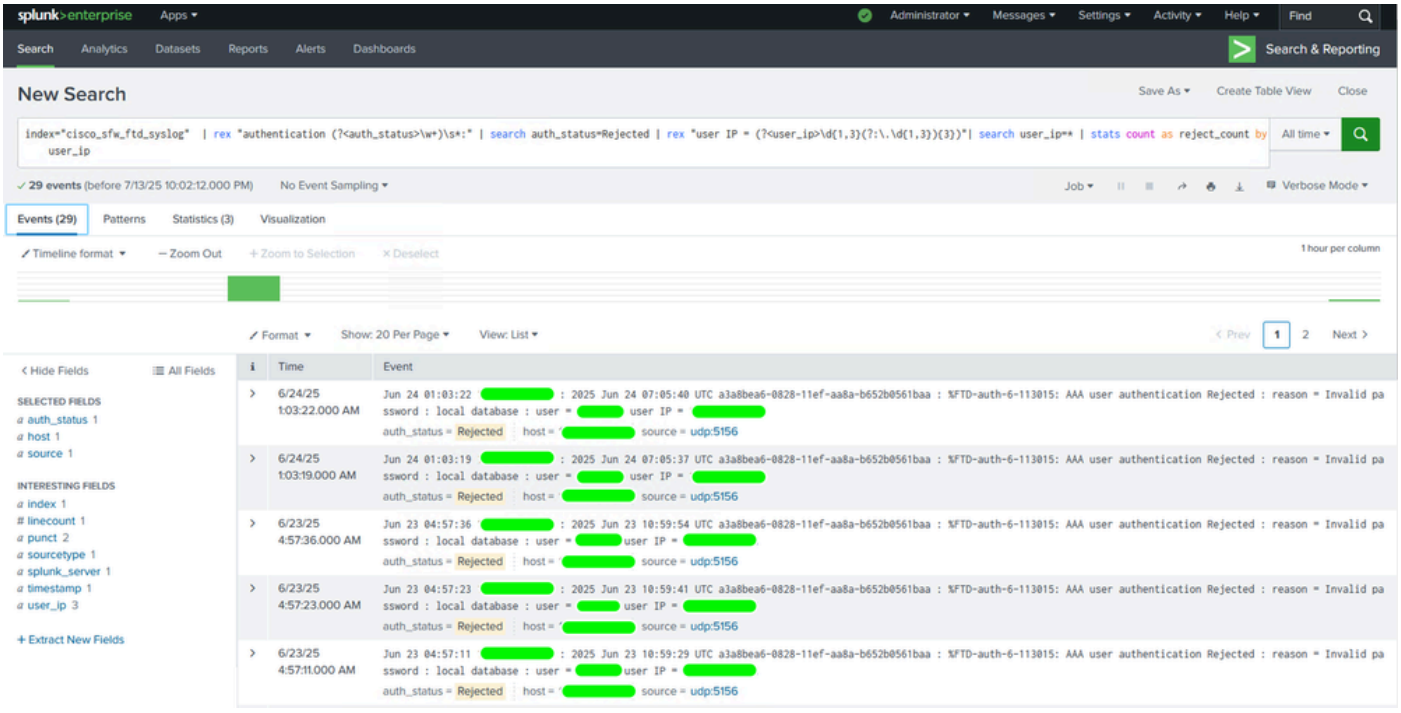
Passaggio 6. Passare alla scheda Dashboard per cercare e scegliere il dashboard creato. Fate clic su di esso per visualizzare, modificare o ridisporre i relativi pannelli.




Come visualizzare il dashboard

Configurazione degli avvisi in base alle query SPL

Passaggio 1. Passare all'app Ricerca e report per creare ed eseguire la query SPL per verificare che stia recuperando i log corretti che verranno utilizzati per attivare l'avviso.




Esegui query SPL per la creazione dei rispettivi avvisi

Nota: In questo esempio, la query viene utilizzata per recuperare i log di autenticazione non riusciti per la VPN ad accesso remoto per attivare avvisi quando il numero di tentativi non riusciti supera una determinata soglia entro un determinato periodo di tempo.

Passaggio 3. Fare clic su Salva con nome e scegliere Avviso.


Salva l'avviso

Passaggio 4. Assegnare un titolo all'avviso. Immettere tutti gli altri dettagli e parametri necessari per configurare l'avviso e fare clic su Salva. Le impostazioni utilizzate per questo avviso sono descritte qui.

<#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**

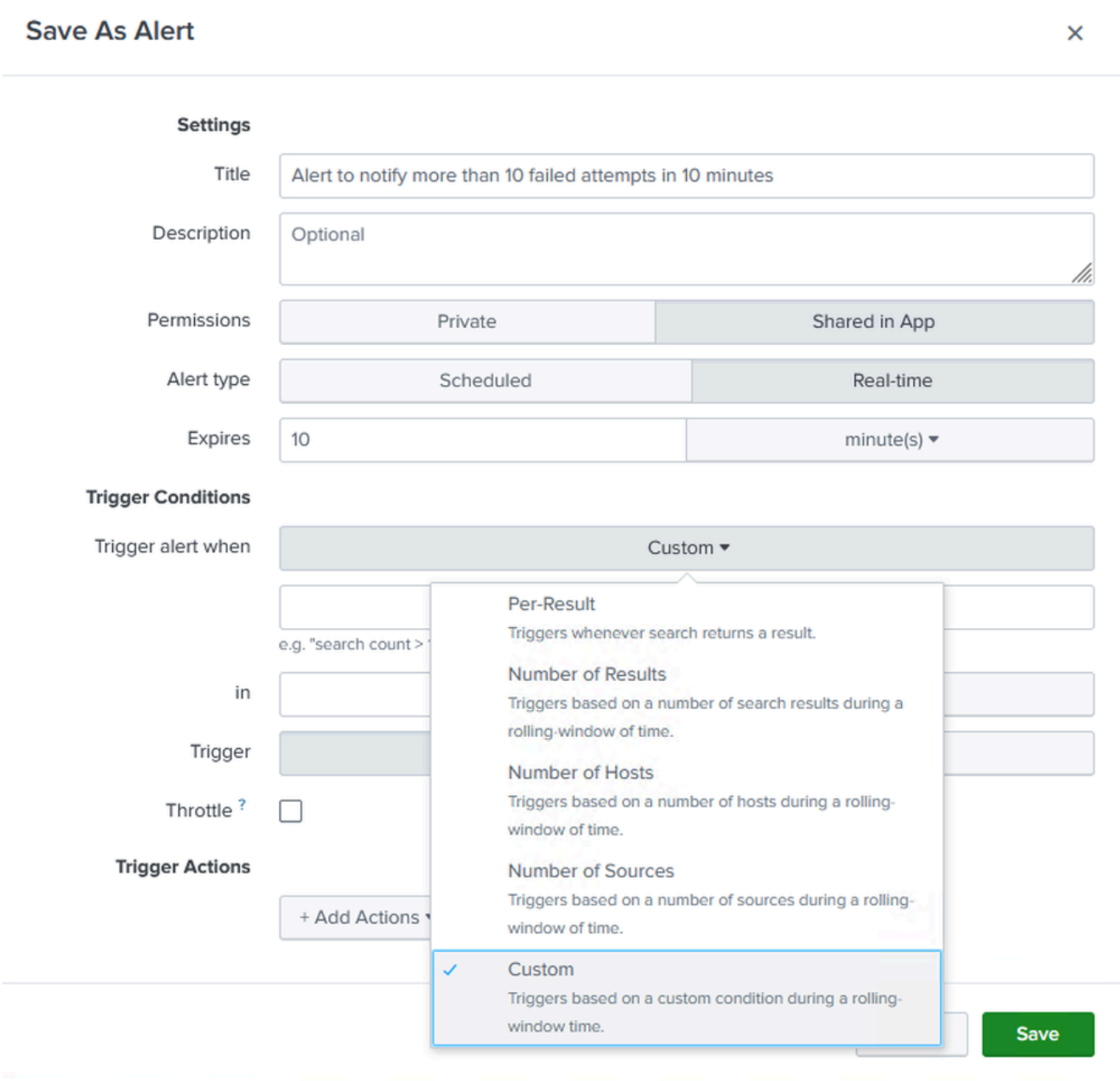
condition is used to search if the

**reject_count**

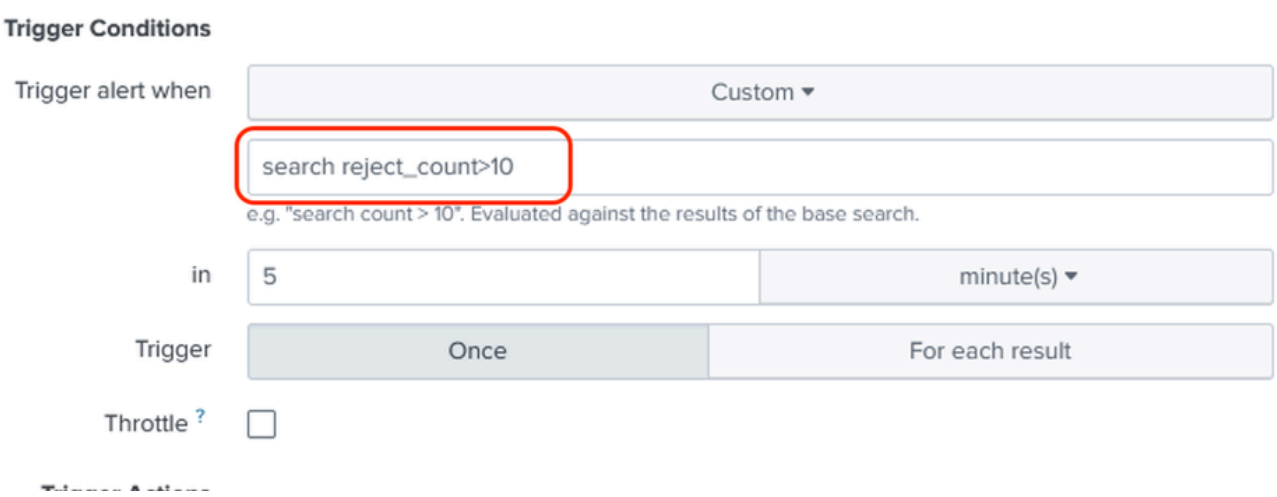
counter from the SPL query has exceeded 10 in the last 5 minutes for any IP address.
Trigger Actions: Set a trigger action such as

**Add to Triggered Alerts, Send email, etc.**

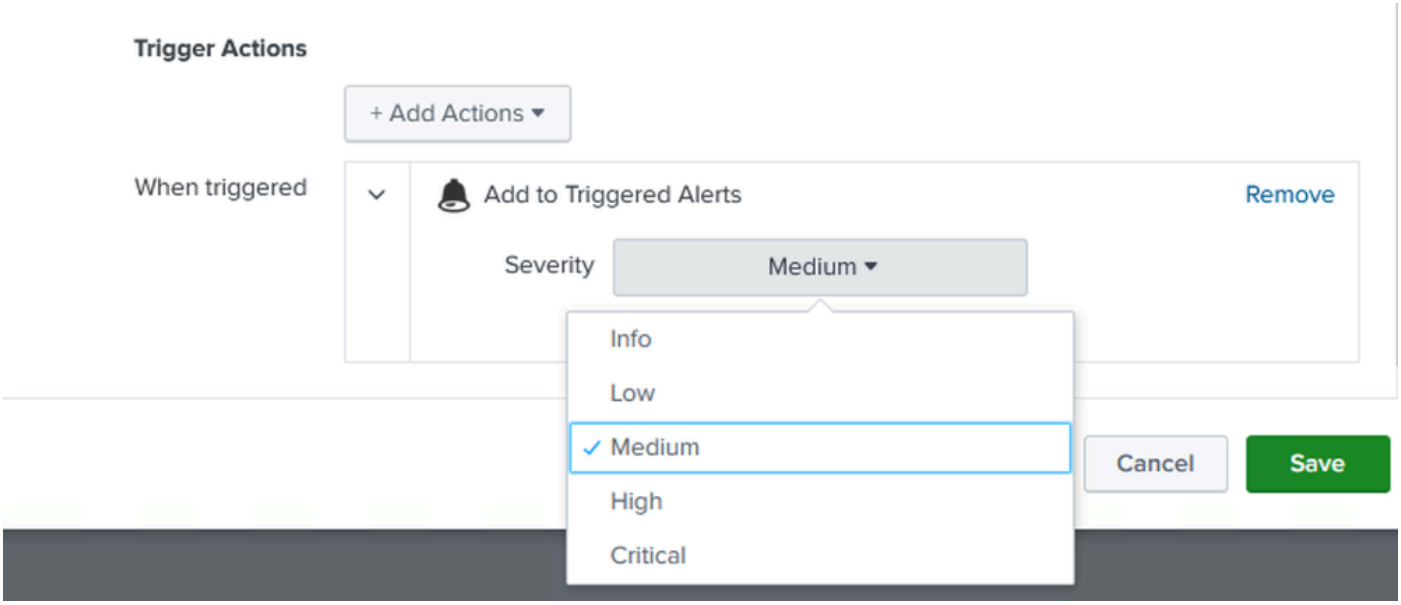
and set the alert severity as per your requirement.



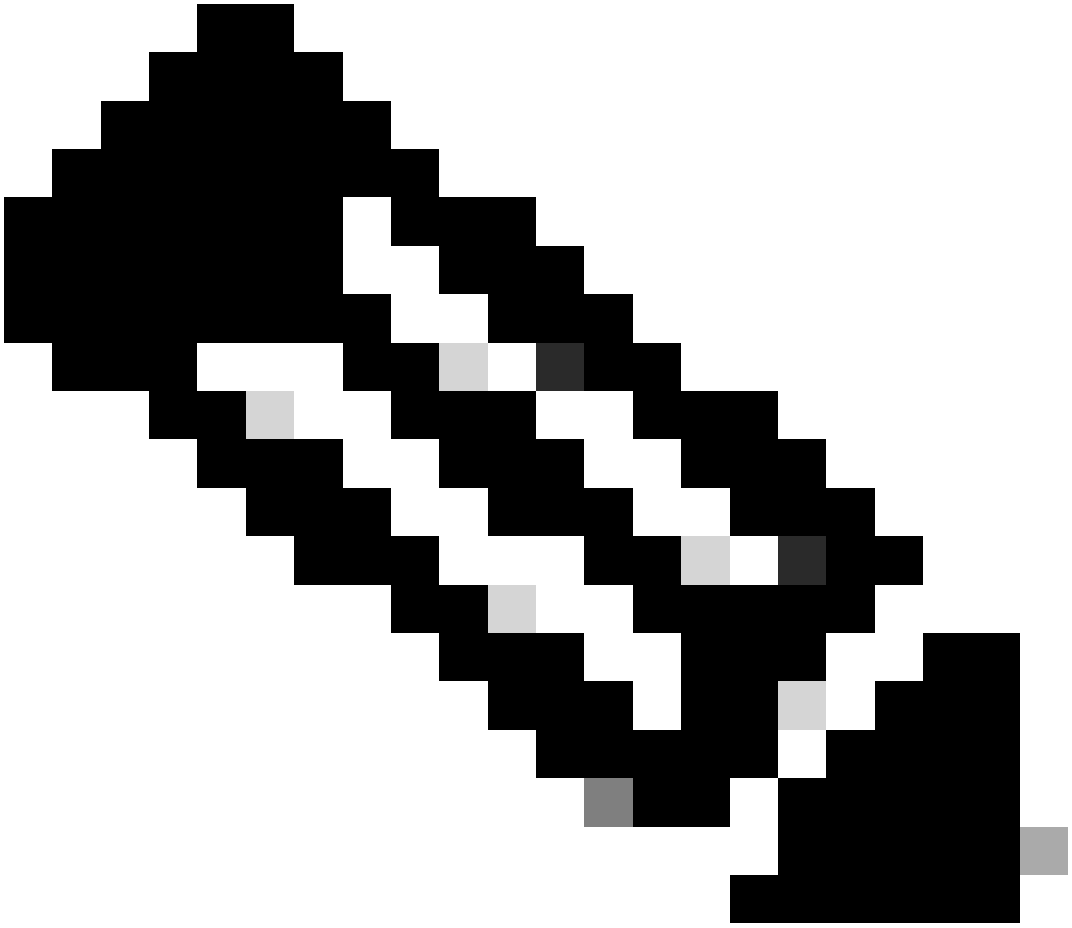

Impostazioni aggiuntive per la creazione di avvisi



Impostazioni aggiuntive per la creazione di avvisi




Impostazioni aggiuntive per la creazione di avvisi



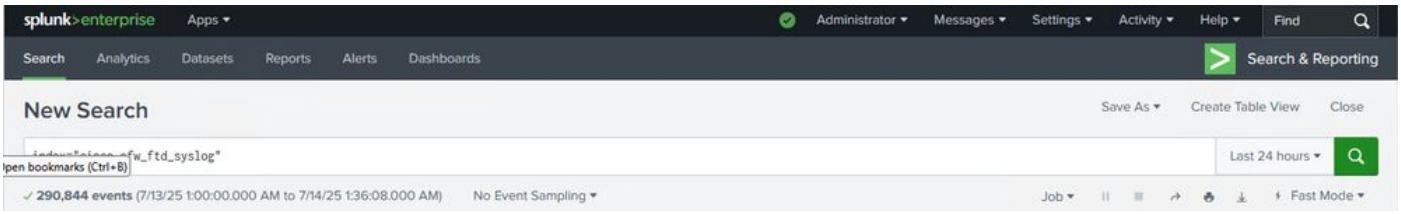
Nota: Se si desidera attivare gli avvisi per ogni risultato, è necessario definire anche le impostazioni di limitazione di conseguenza.

## Verifica

Una volta creati i dashboard e gli avvisi, è possibile verificare le configurazioni, il flusso di dati, i dashboard e gli avvisi in tempo reale utilizzando le istruzioni fornite in questa sezione.

### Visualizza registri

È possibile usare l'app di ricerca per verificare se i log inviati dal firewall vengono ricevuti e visibili all'intestazione di ricerca dello splunk. È possibile verificare questa condizione controllando i log più recenti indicizzati (indice di ricerca = "cisco_sfw_ftd_syslog") e l'indicatore orario associato.

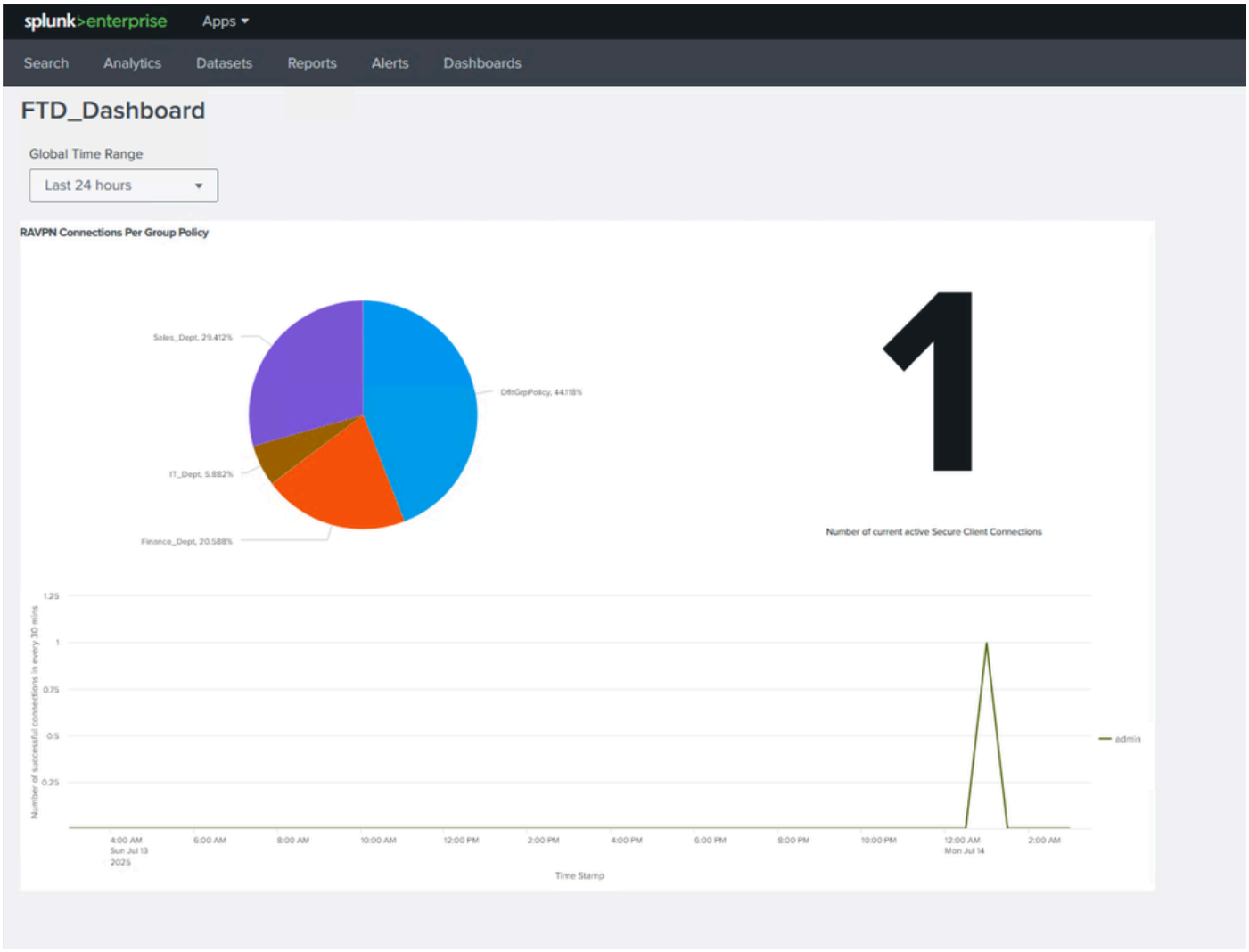



Controllo e visualizzazione dei registri


Controllo e visualizzazione dei registri

## Visualizzare i dashboard in tempo reale

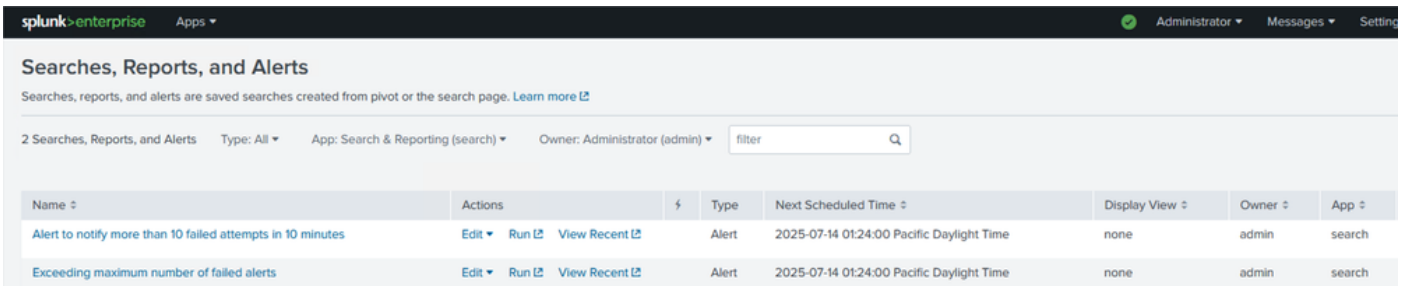
Potete passare al dashboard personalizzato che avete creato e visualizzare le modifiche su ciascuno dei pannelli quando vengono generati nuovi dati e log dall'FTD.



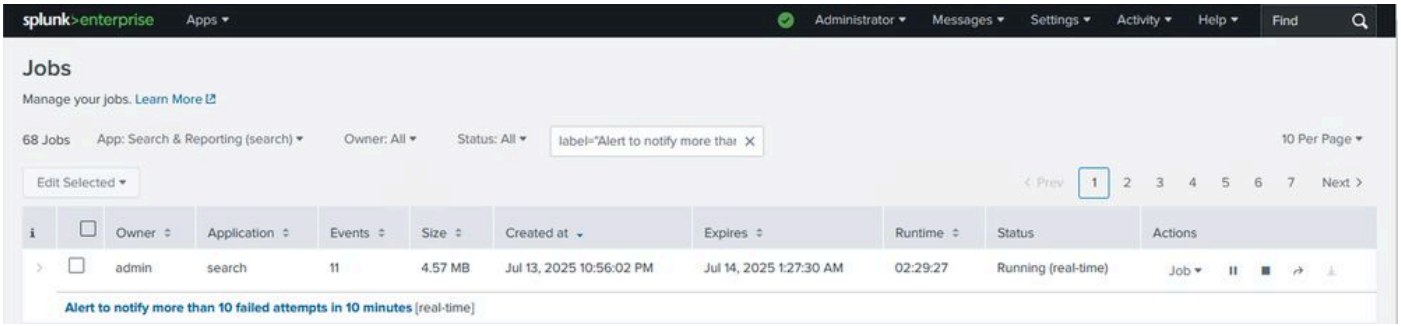

Visualizza dashboard

## Controlla se sono stati attivati avvisi

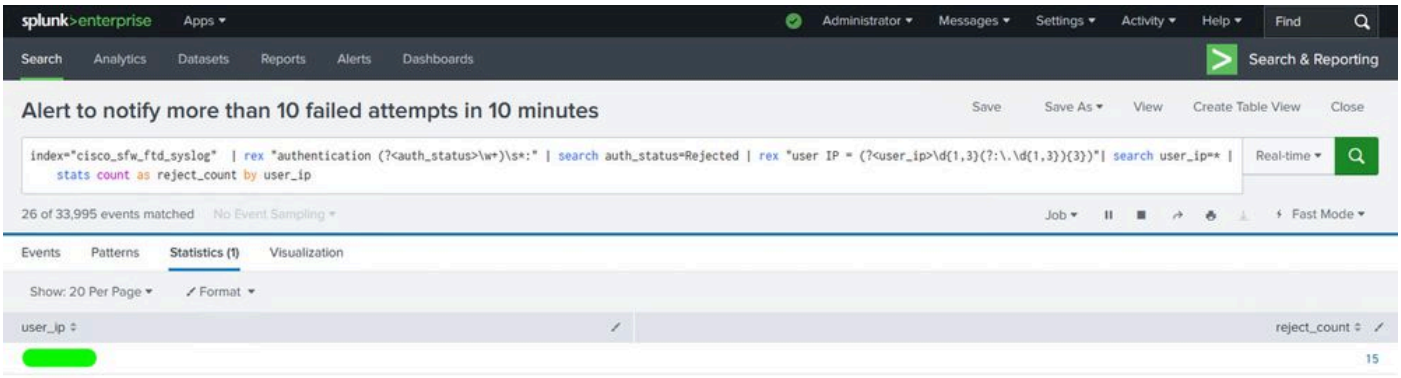
Per verificare le informazioni relative agli avvisi, è possibile passare alla sezione ricerche, report e avvisi per visualizzare le informazioni relative agli avvisi recenti. Fare clic su View Recent (Visualizza recenti) per ulteriori informazioni sui job e le ricerche.




Controlla e visualizza avvisi




Controlla e visualizza avvisi




Verifica statistiche per avvisi attivati

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).