在Splunk上使用FTD中的Syslogs建立自定義控制面板和警報

目錄

簡介

本檔案介紹設定FTD以向Splunk傳送系統日誌以及使用那些日誌建立自訂控制板和警報的逐步演練。

必要條件

需求

思科建議您在閱讀本配置指南之前瞭解以下主題：

- 系統日誌
- Splunk搜尋處理語言(SPL)的基本知識

本檔案還假設您已經在伺服器上安裝Splunk Enterprise執行個體且可以存取Web介面。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 在7.2.4版上運行的Cisco Firepower威脅防禦(FTD)

- 運行在7.2.4版上的Cisco Firepower管理中心(FMC)
- 在Windows電腦上運行的Splunk Enterprise例項（版本9.4.3）

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。

背景資訊

思科FTD裝置生成涵蓋入侵事件、訪問控制策略、連線事件等內容的詳細系統日誌。將這些日誌與Splunk整合，可為網路安全操作提供強大的分析和即時警報。

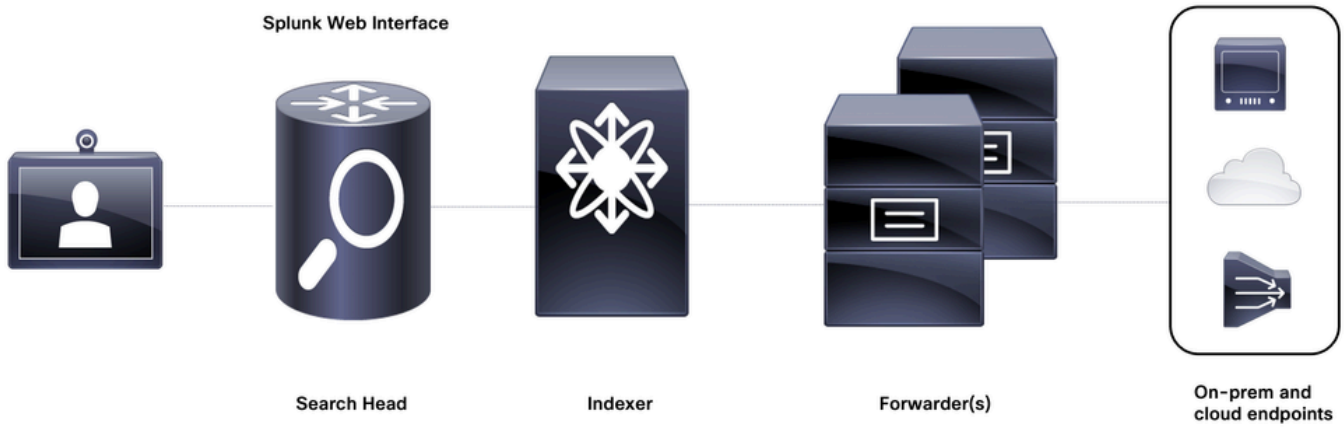
Splunk是一個即時資料分析平台，旨在攝取、索引、搜尋和視覺化電腦生成的資料。Splunk作為安全資訊和事件管理(SIEM)工具在網路安全環境中尤為有效，因為它能夠：

- 大規模接收日誌資料
- 使用SPL執行複雜搜尋
- 建立控制面板和警報
- 與安全協調和事件響應系統整合

Splunk通過結構化管道處理資料，以使非結構化或半結構化的機器資料變得有用並可操作。該管線的關鍵階段通常稱為IPIS，代表：

- 輸入
- 正在分析
- 索引
- 正在搜尋

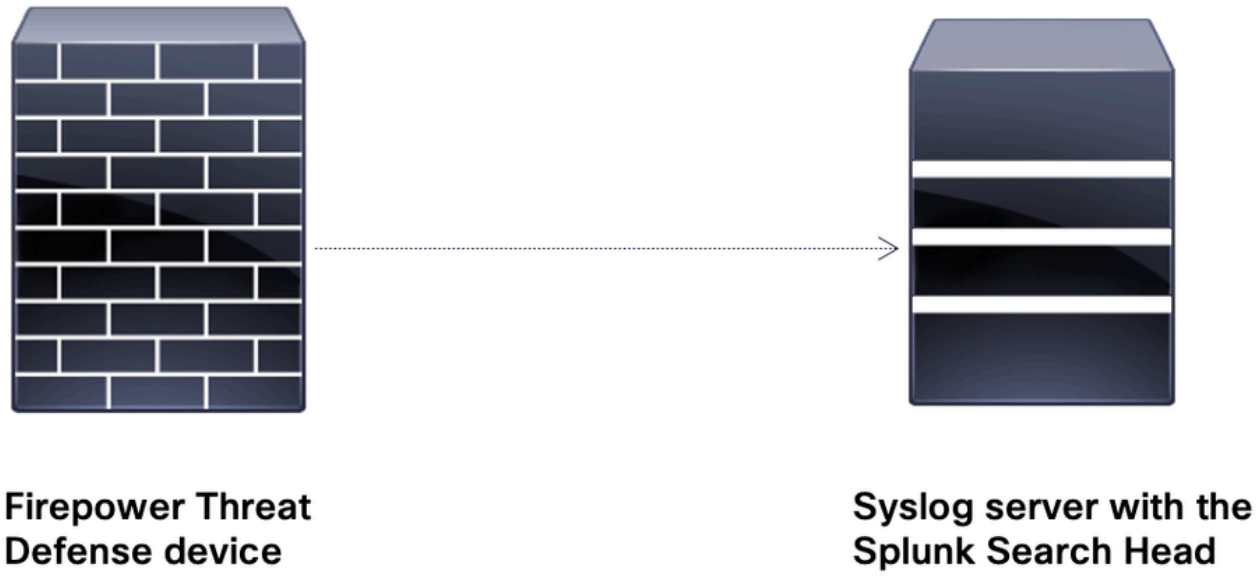
用於實現IPIS管道的底層架構的主要元件如下圖所示：



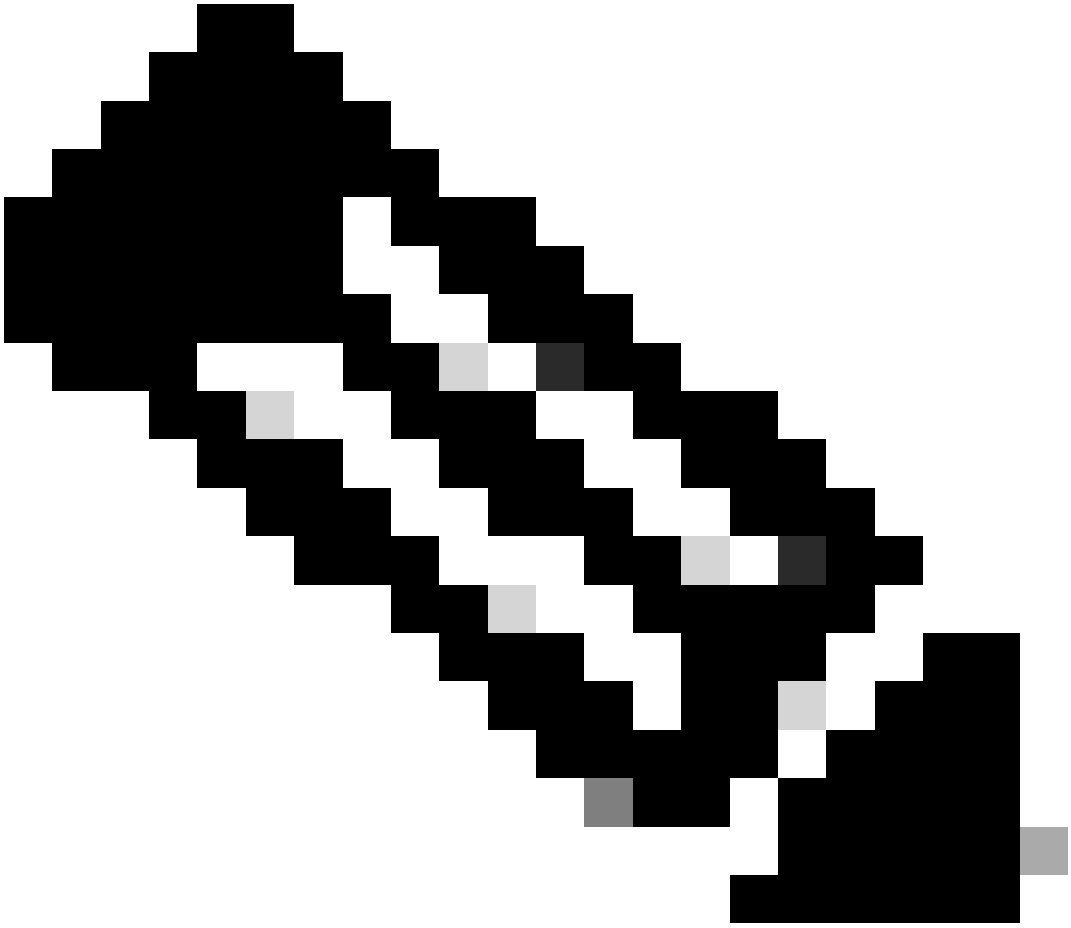
Splunk基礎體系結構

設定

網路圖表


Firepower Threat Defense device
Syslog server with the Splunk Search Head

網路圖表

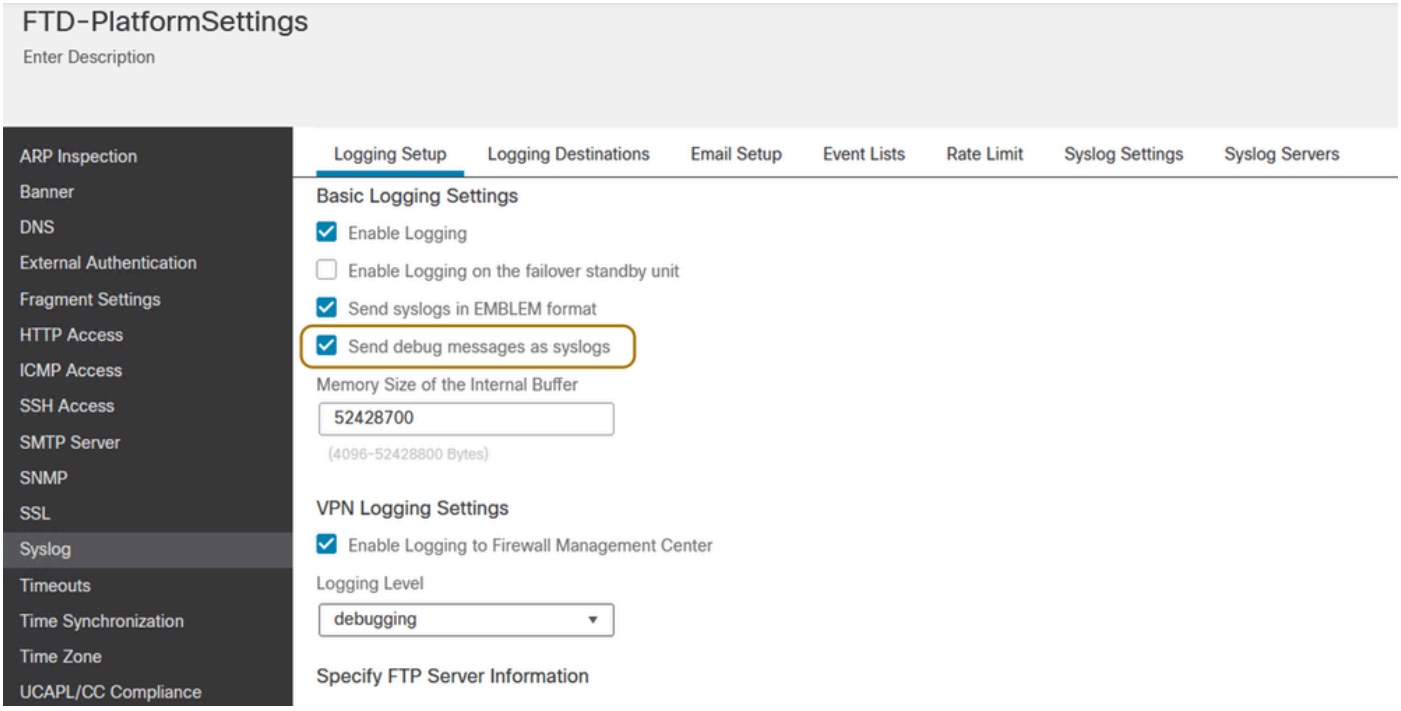


附註：本文檔的實驗環境不需要單獨的轉發器和索引器例項。安裝Splunk Enterprise例項的Windows電腦（即Syslog伺服器）充當索引器和搜尋頭。

組態

設定FTD的系統日誌設定

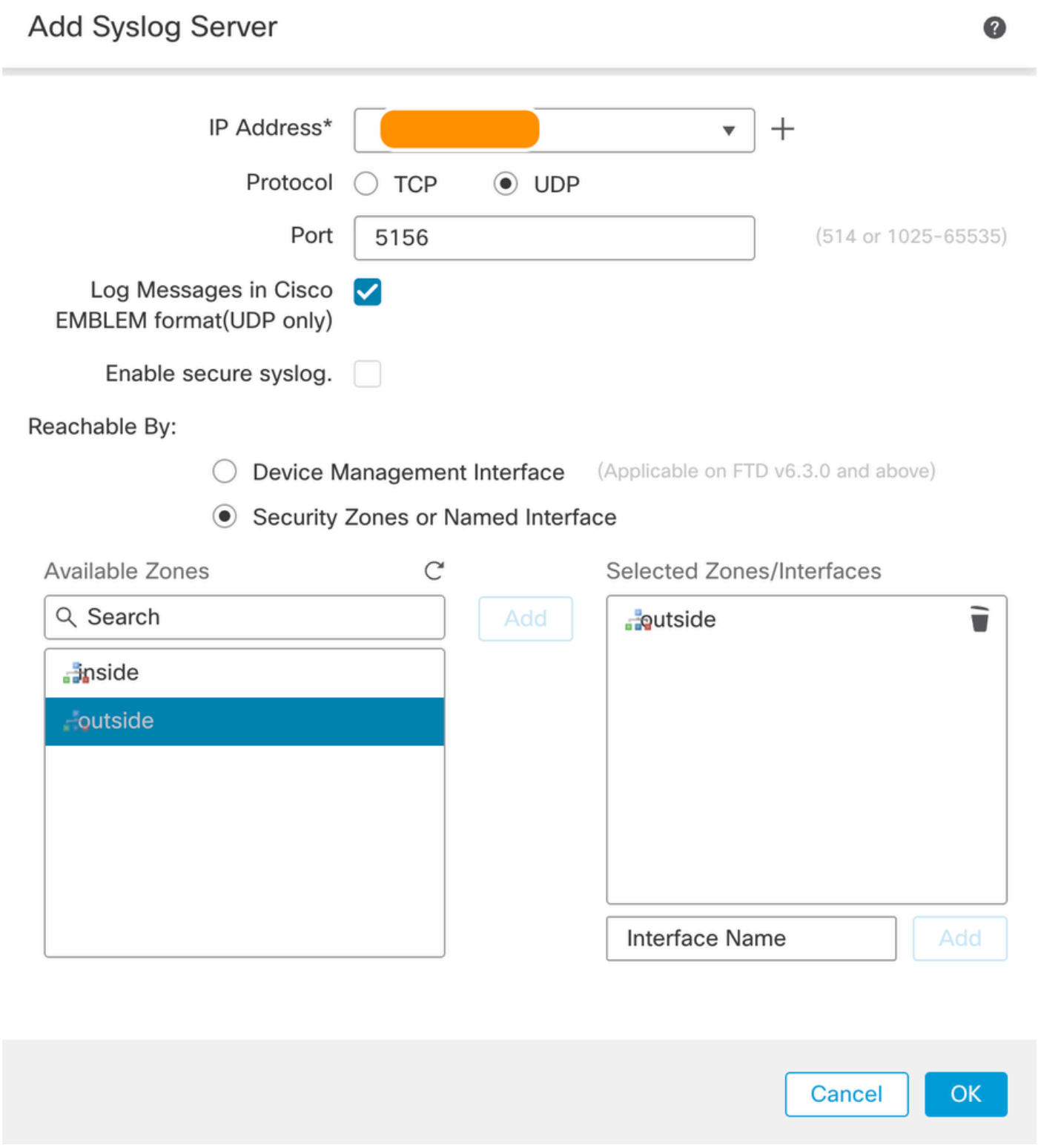
步驟1.在Devices > Platform Settings下為FTD在FMC上配置初步系統日誌設定，以便將日誌傳送到正在運行Splunk例項的系統日誌伺服器。



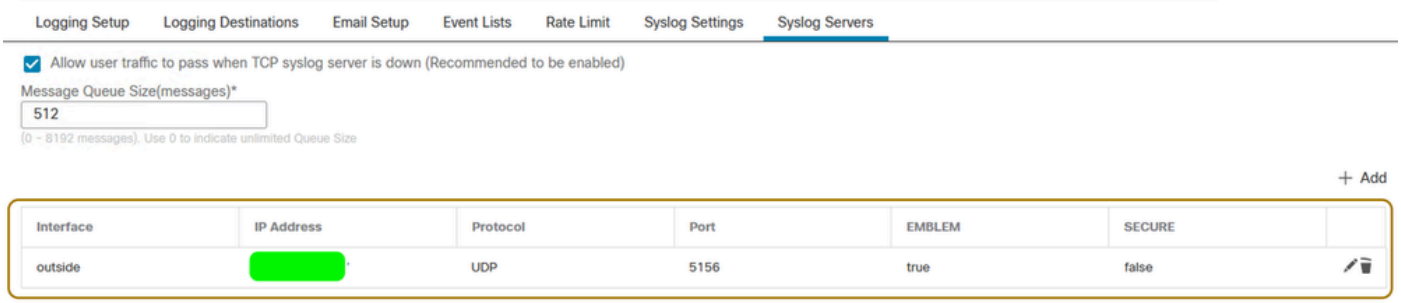
FTD上的平台設定 — 系統日誌

步驟2.配置安裝Splunk Enterprise例項並作為Syslog Server運行的電腦的IP地址。定義上述欄位。

```
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
```

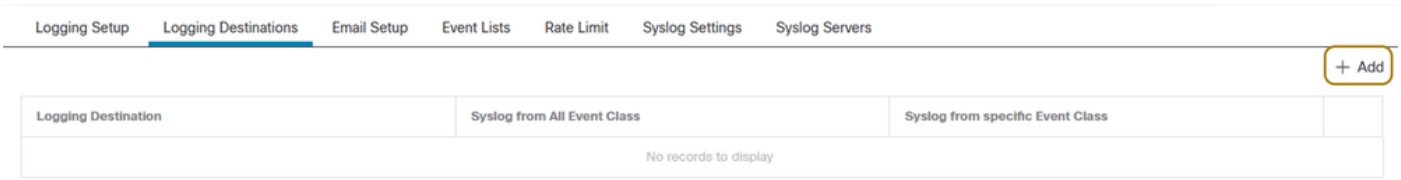


FTD上的平台設定 — 新增系統日誌伺服器

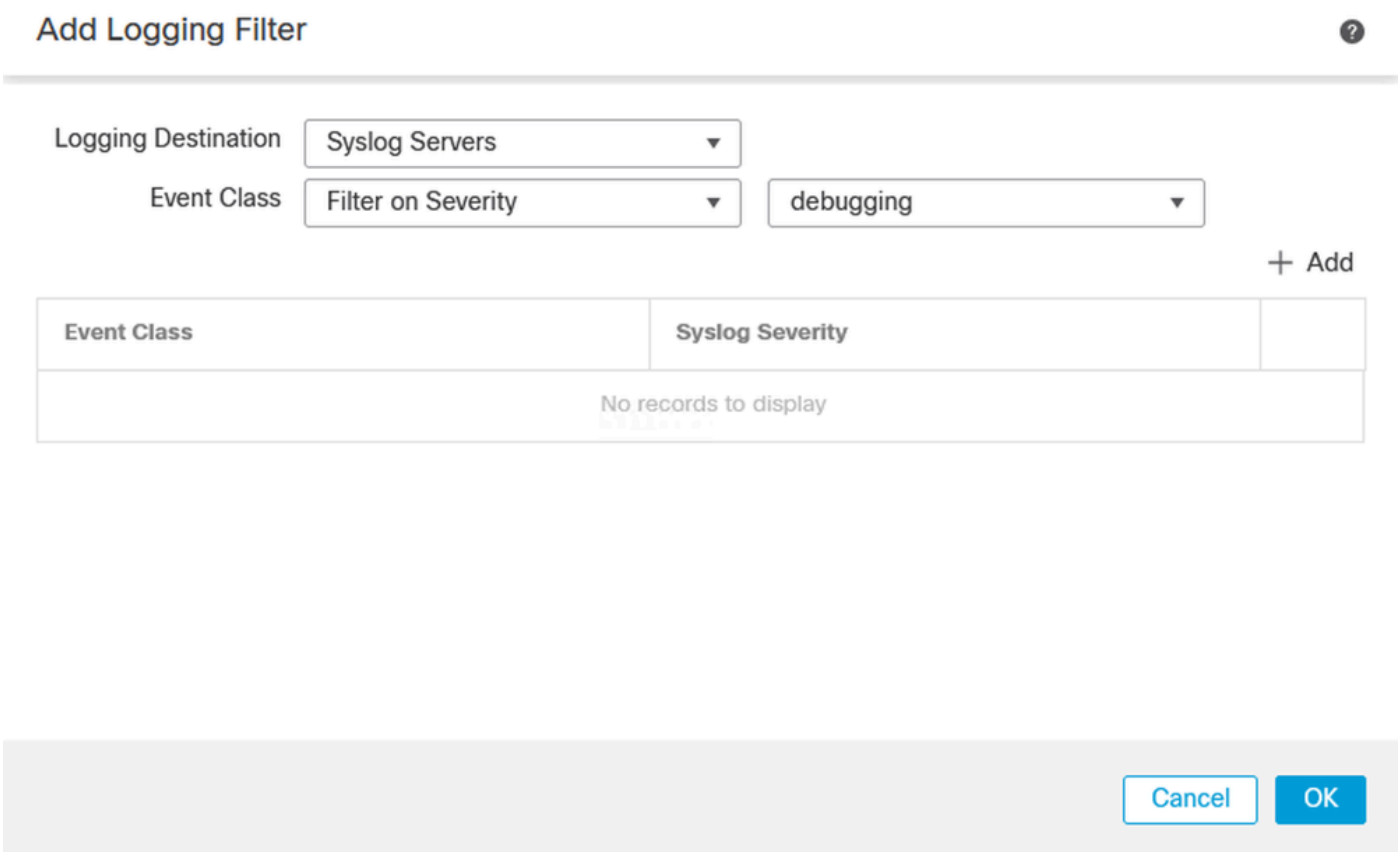


FTD上的平台設定 — 已新增系統日誌伺服器

步驟3.為Syslog伺服器新增日誌記錄目標。可根據您的選擇或使用案例設定日誌級別。



FTD上的平台設定 — 新增記錄目的地



FTD上的平台設定 — 設定記錄目的地的嚴重性等級

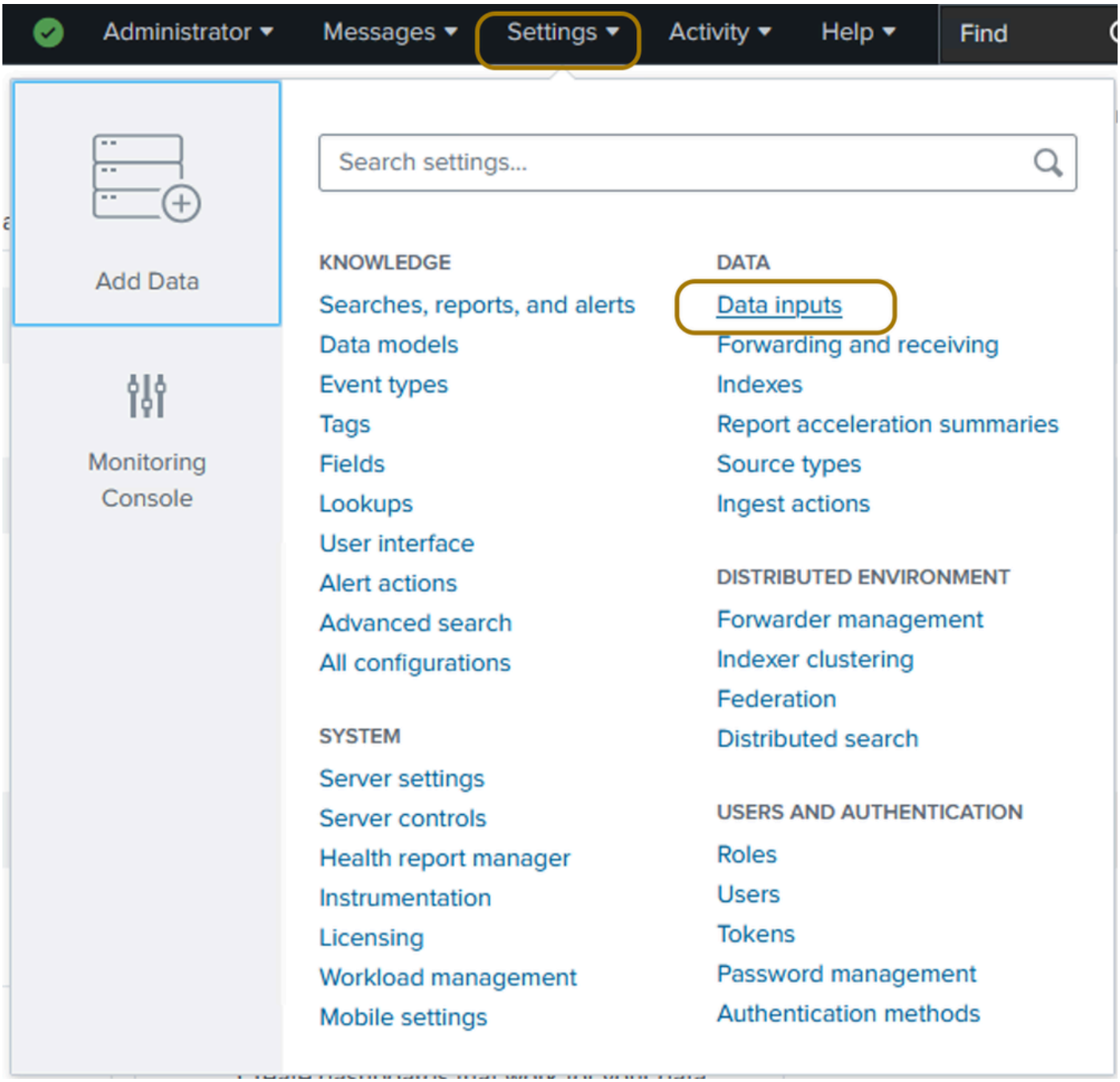
完成這些步驟後，將平台設定更改部署到FTD。

在Splunk Enterprise例項上配置資料輸入

步驟1.登入到Splunk Enterprise例項Web介面。

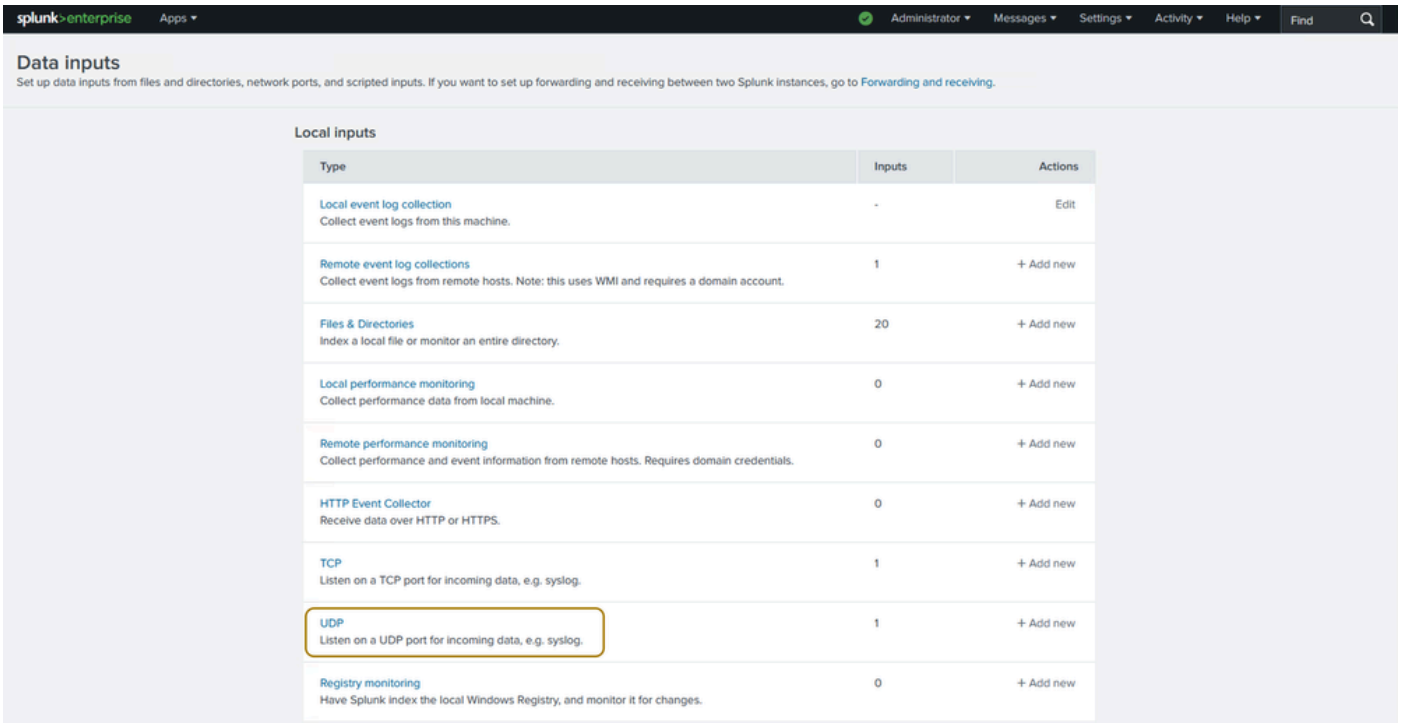
Splunk Web介面登入頁

步驟2.必須定義資料輸入，以便在Splunk上儲存和索引系統日誌。登入後導航到設定>資料>資料輸入。

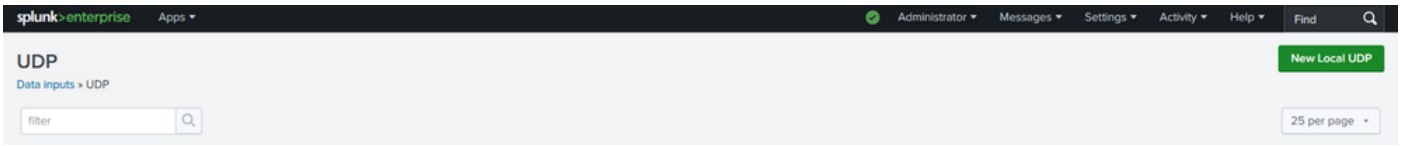


導航到Splunk上的資料輸入

步驟3.選擇UDP，然後在出現的下一頁上按一下New Local UDP。

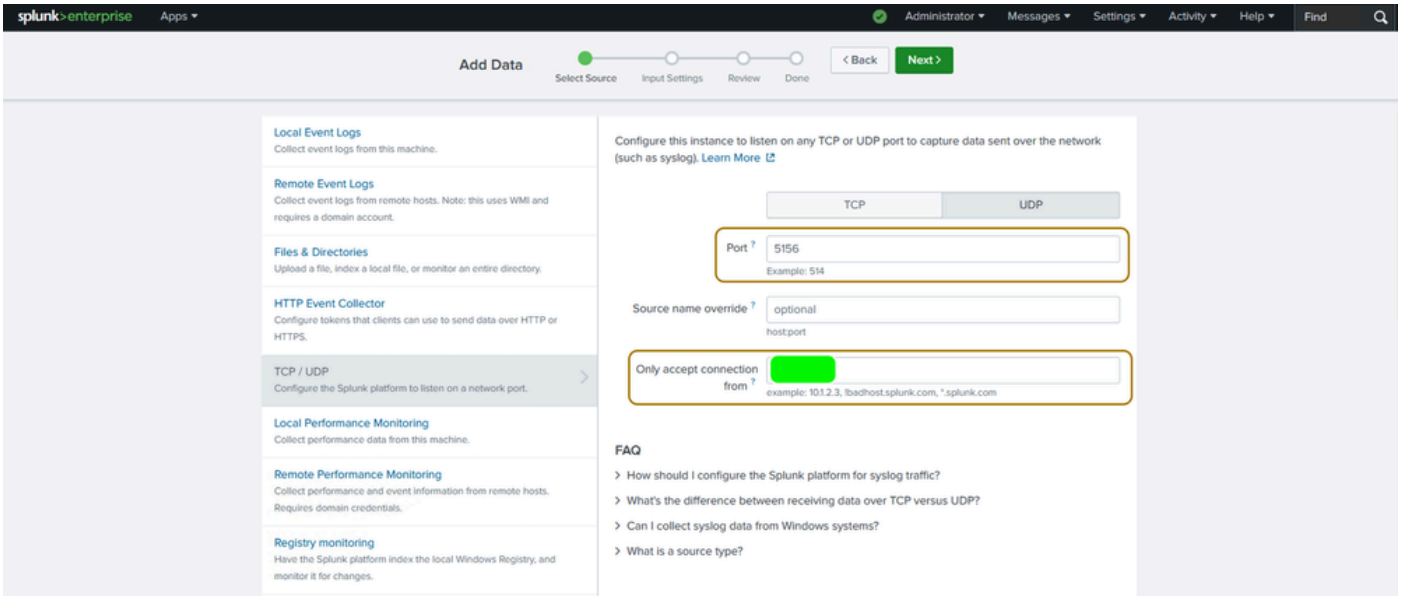


按一下「UDP」進行UDP資料輸入



建立「新本地UDP」輸入

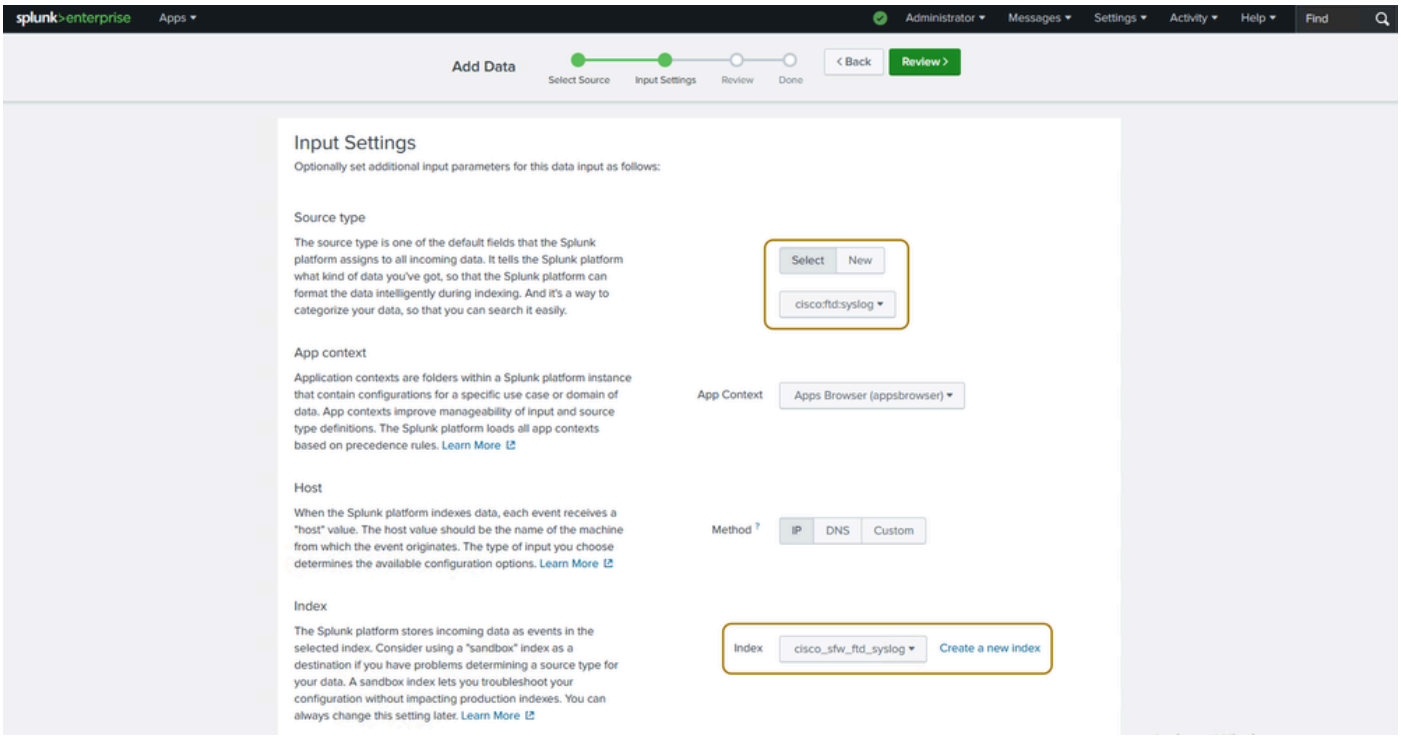
步驟4.輸入傳送系統日誌的埠。它必須與FTD系統日誌設定上配置的埠相同，本例中為5156。若要僅接受來自一個來源(FTD)的系統日誌，請將Only Accept Connection From欄位設定為與Splunk伺服器通訊的FTD上介面的IP。按「Next」（下一步）。



指定埠和FTD IP地址

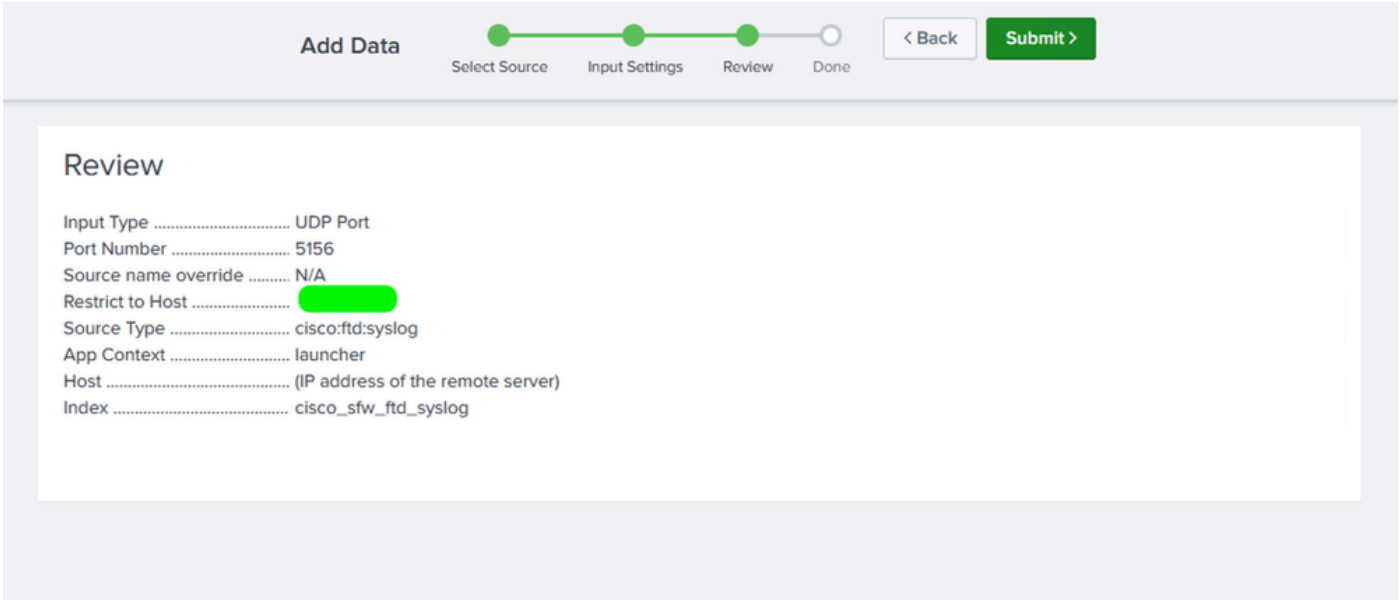
步驟5.您可以搜尋並選擇Splunk上預定義欄位值中的源型別和索引欄位值，如下圖所示。預設設定

可用於其餘欄位。



配置資料輸入設定

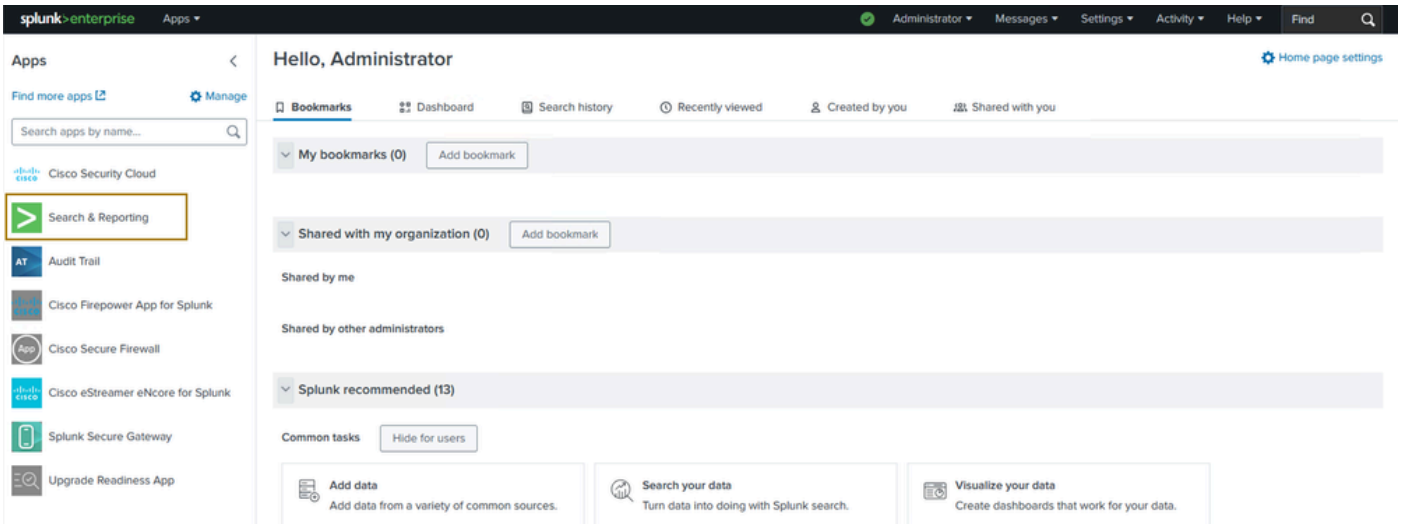
步驟6.檢查設定，然後按一下「Submit」。



檢視資料輸入設定

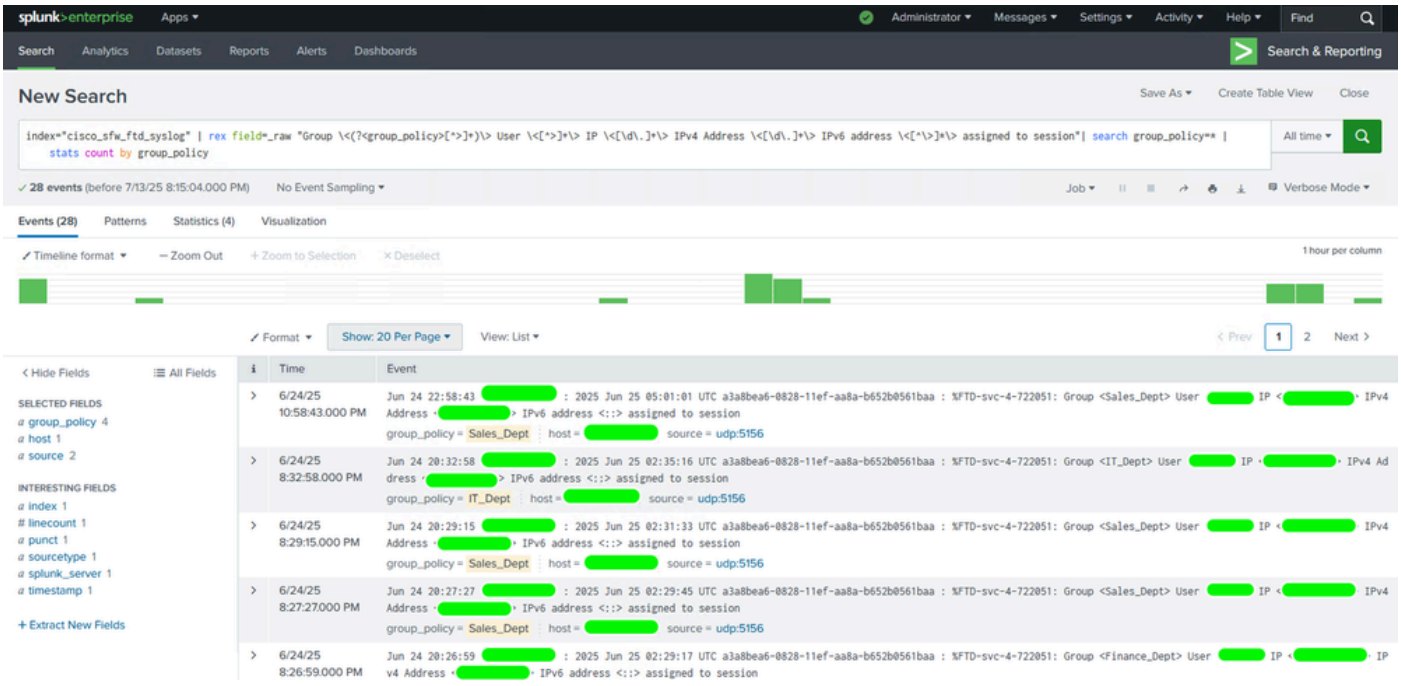
執行SPL查詢和建立儀表板

步驟1.在Splunk上導航到Search and Reporting App。

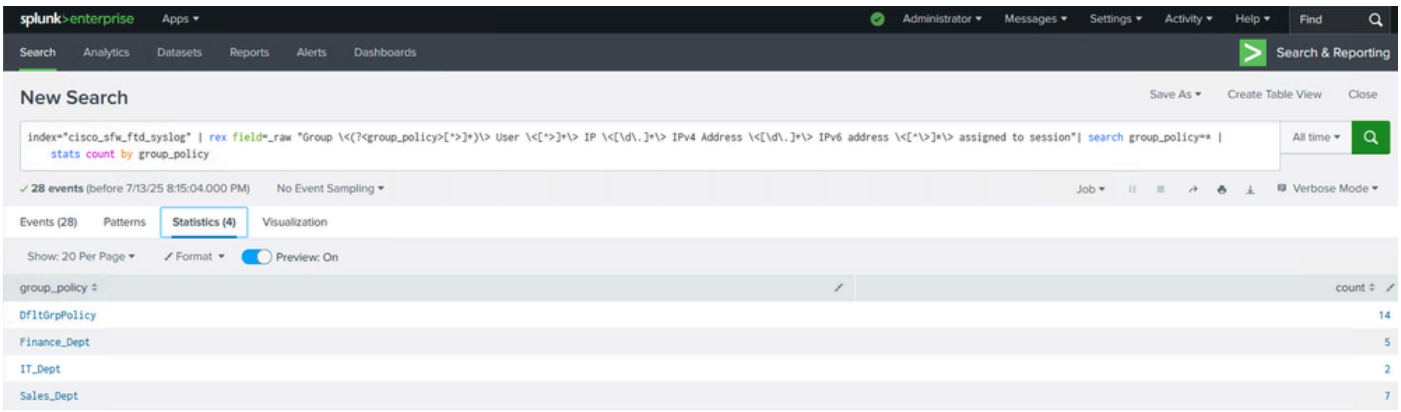


導航到「搜尋和報告」應用程式

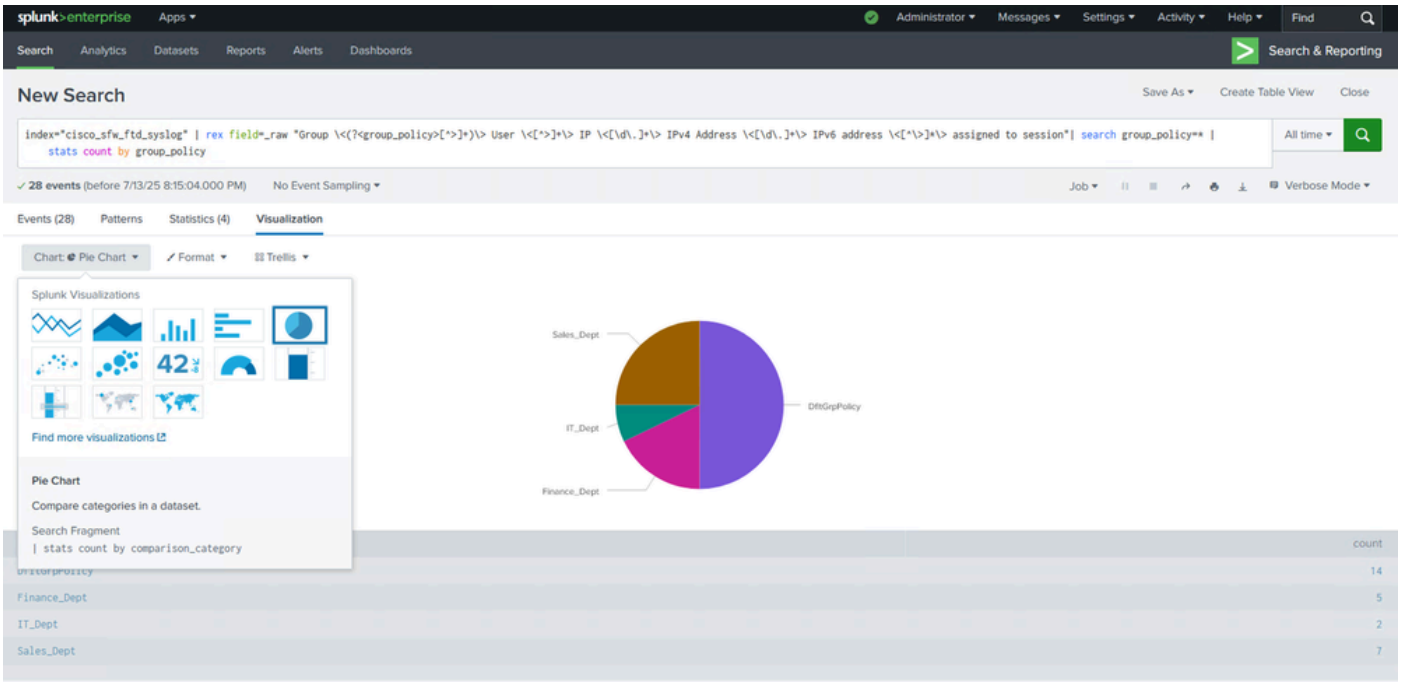
步驟2.根據要視覺化的資料制定並執行SPL查詢。您將能夠在Events 頁籤下完整檢視每個日誌(在詳細模式下)，在Statistics 頁籤下檢視每個組策略的連線計數，並在Visualization頁籤下使用這些統計資訊來視覺化此資料。



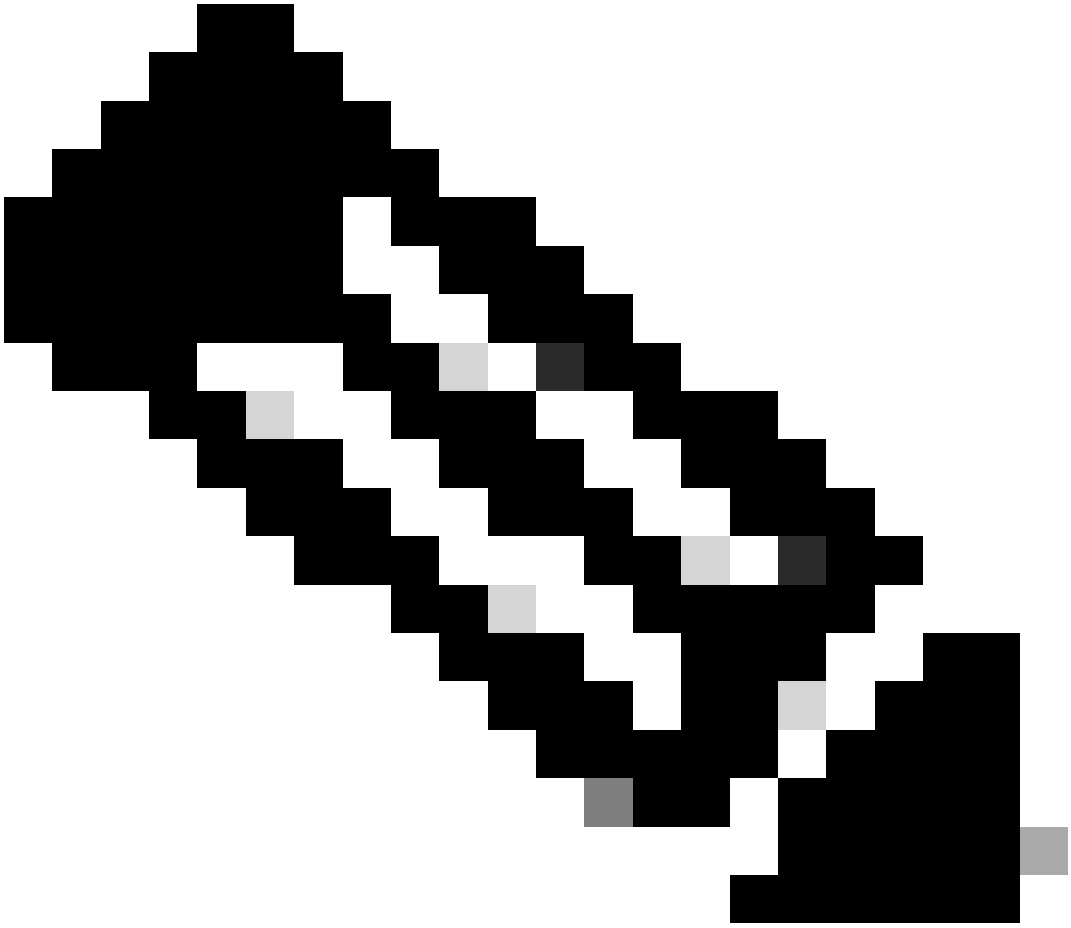
使用SPL查詢搜尋事件



檢查統計資訊頁籤

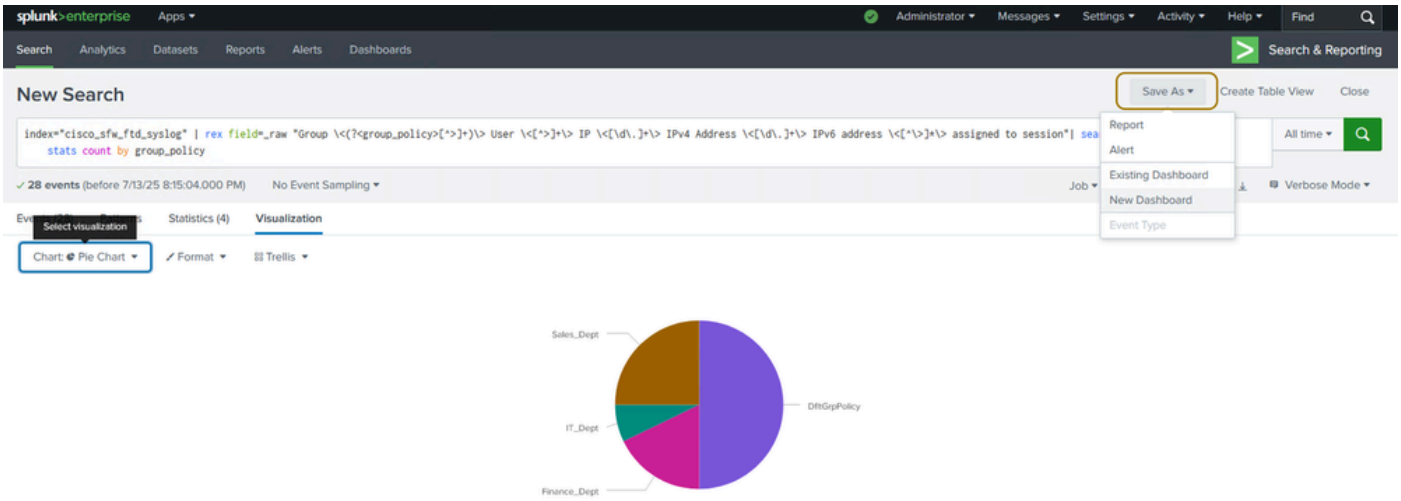


視覺化頁籤將顯示圖形/圖表



附註：在本示例中，查詢獲取不同組策略之間遠端訪問VPN連線成功的日誌。已使用餅圖來顯示每個組策略成功連線的數量和百分比。根據您的要求和首選項，您可以選擇使用其他型別的視覺化，如條形圖。

步驟3.按一下另存為，然後選擇新建或現有儀表板，具體取決於您是否已擁有要向其中新增此面板的儀表板或要建立新面板。以下示例顯示了後者。



將面板儲存到儀表板

步驟4.為正在建立的儀表板指定標題，並為將包含餅圖的面板提供標題。

Save Panel to New Dashboard

Dashboard Title: FTD_Dashboard

ftd_dashboard Edit ID

Description: Optional

Permissions: Private

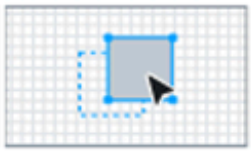
How do you want to build your dashboard? What's this?

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

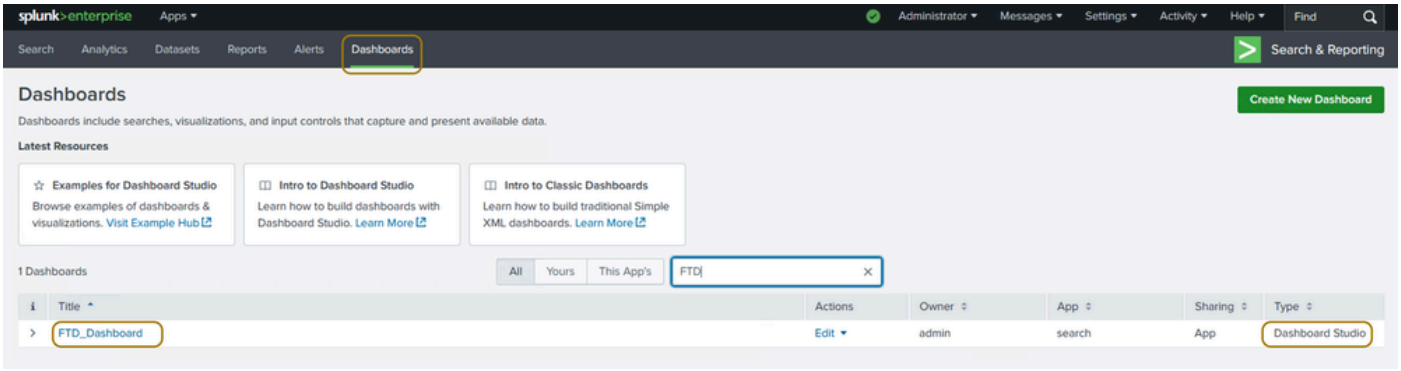
Cancel Save to Dashboard

新儀表板的設定

許可權設定為。此外，根據您是否要對儀表板的面板設定和佈局進行精細控制，選擇經典模式或儀表板工作室模式來構建儀表板。

第5步（可選）。 按照您的要求，使用前面提到的步驟，執行更多的SPL查詢並將其儲存為此控制面板的面板。

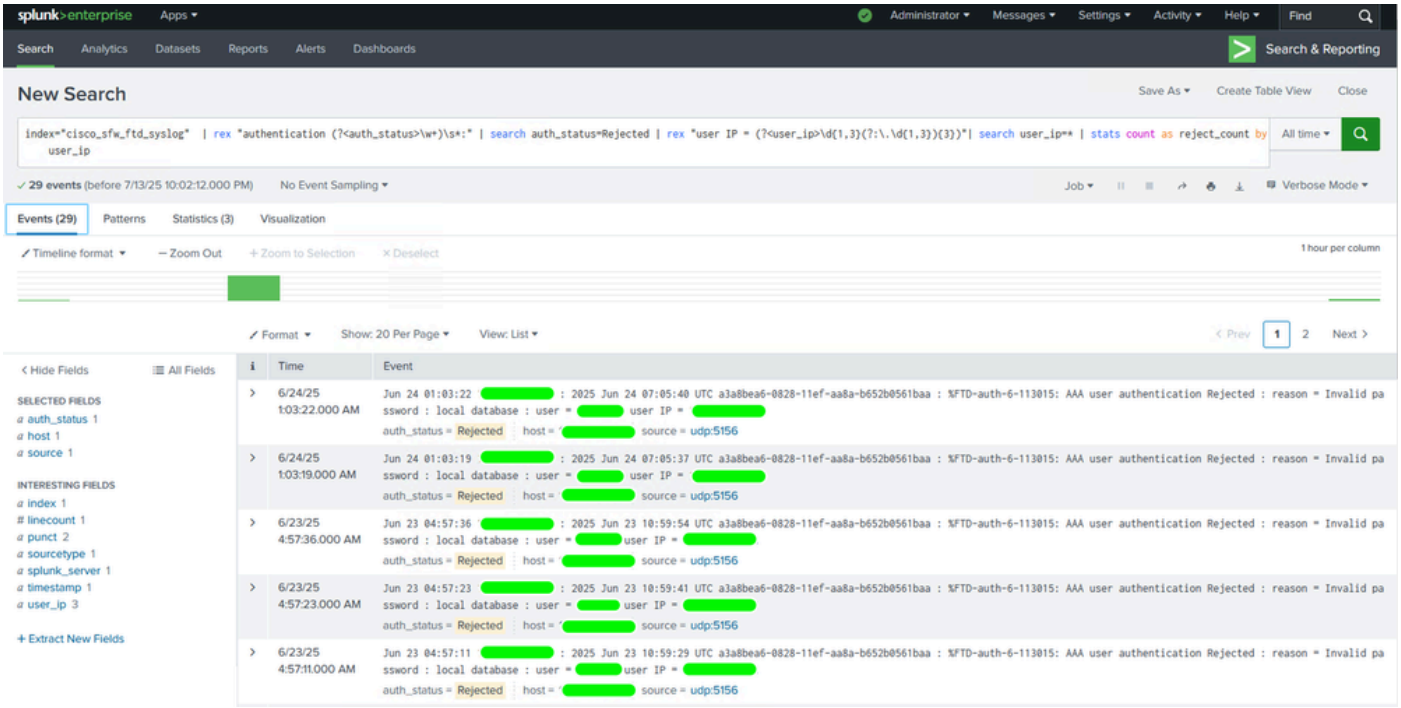
步驟6.定位至控制面板標籤，以搜尋並選擇您建立的控制面板。按一下它可檢視、編輯或重新排列其面板。



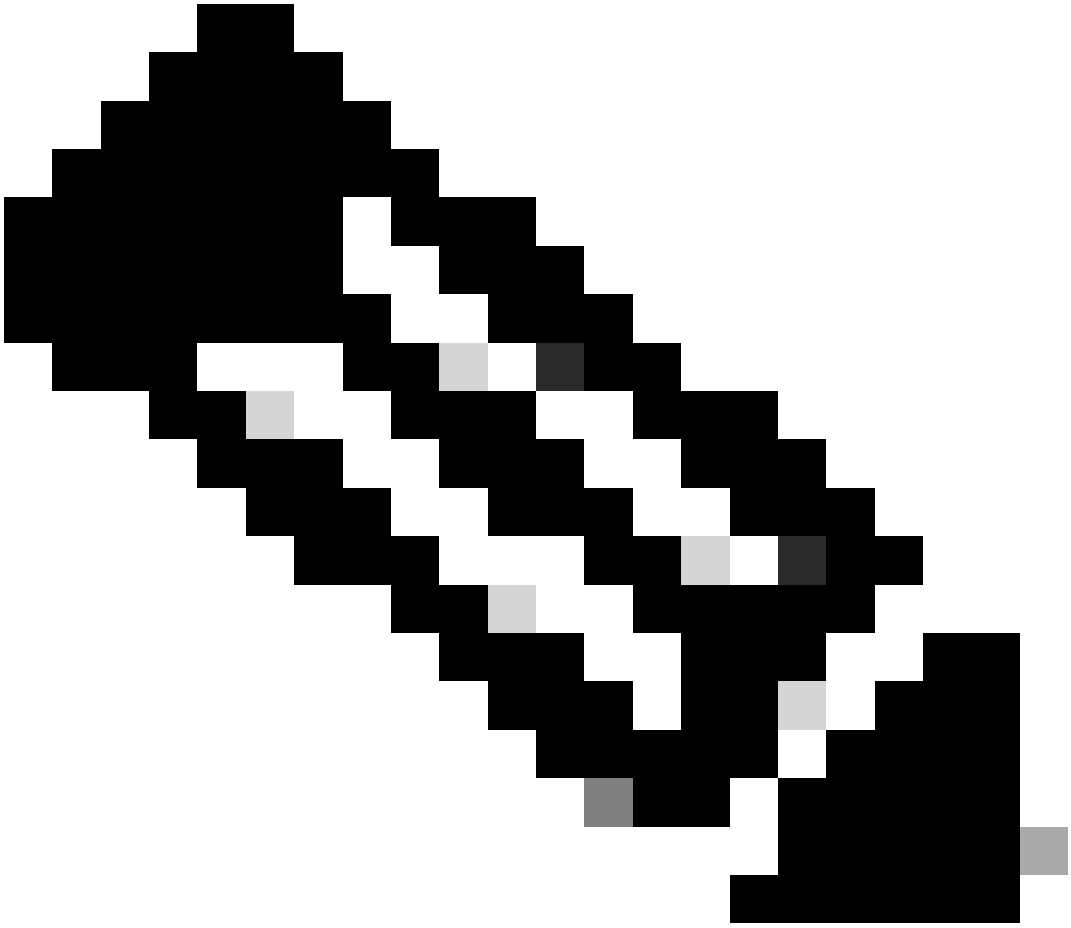
如何檢視儀表板

根據SPL查詢配置警報

步驟1.導航到Search and Reporting App以構造並運行SPL查詢，以驗證其正在獲取用於觸發警報的正確日誌。



運行SPL查詢以建立各自的警報



附註：在本示例中，查詢用於獲取遠端訪問VPN的失敗身份驗證日誌，以便在在一定時間內失敗嘗試次數超過特定閾值時觸發警報。

步驟3.按一下Save As ，然後選擇Alert。

儲存警報

步驟4.為警報命名。填寫配置警報所需的所有其他詳細資訊和引數，然後按一下「儲存」。此處已提到用於此警報的設定。

<#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

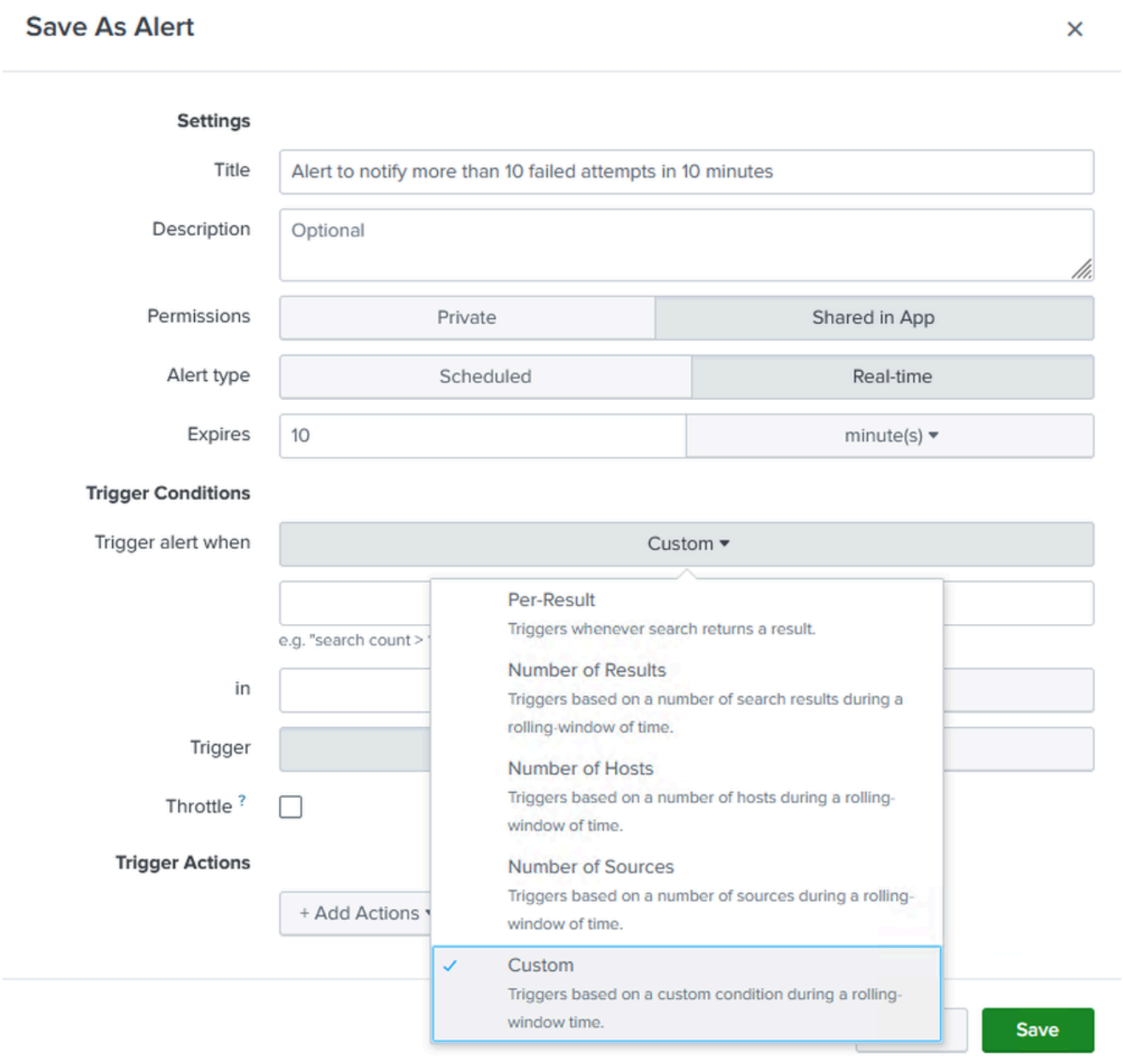
condition is used to search if the

reject_count

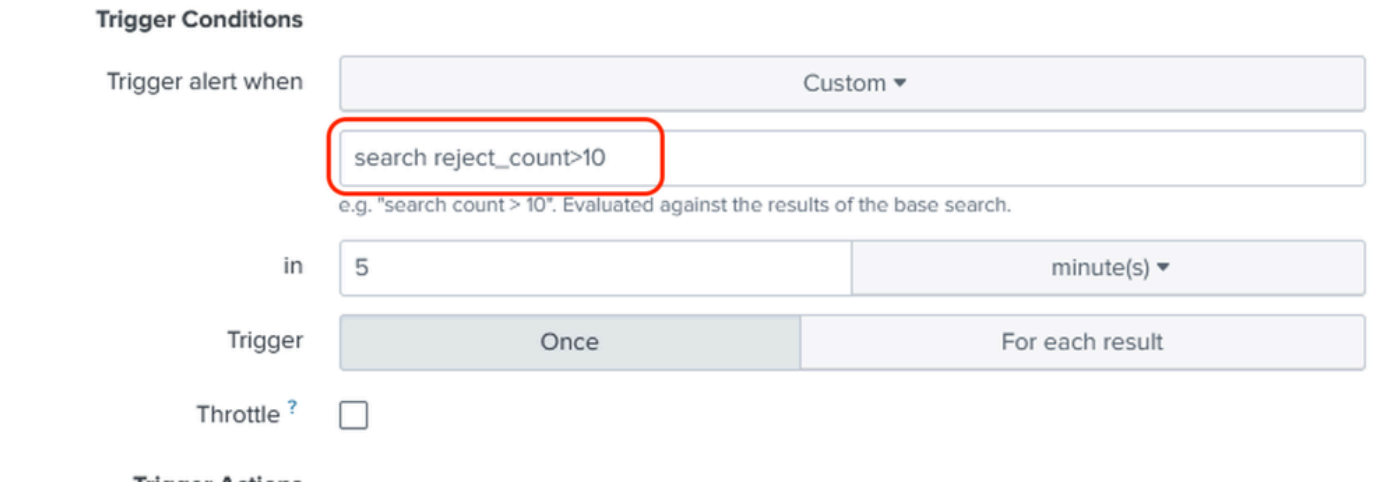
counter from the SPL query has exceeded 10 in the last 5 minutes for any IP address.
Trigger Actions: Set a trigger action such as

Add to Triggered Alerts, Send email, etc.

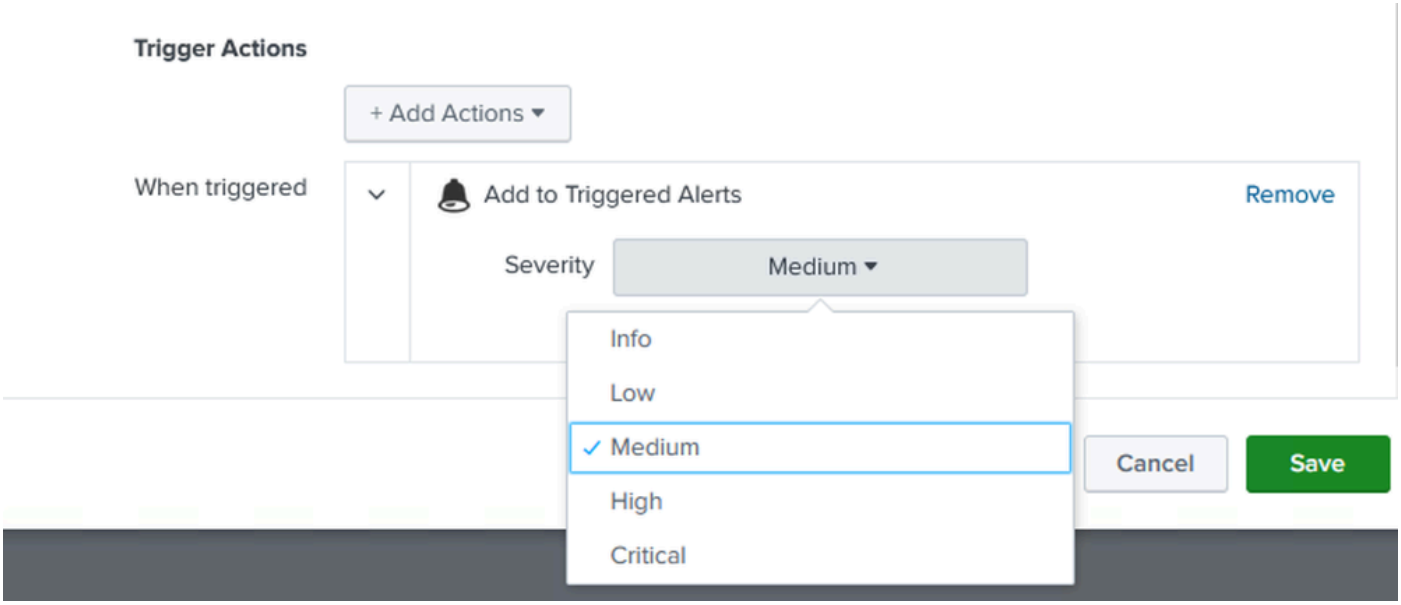
and set the alert severity as per your requirement.



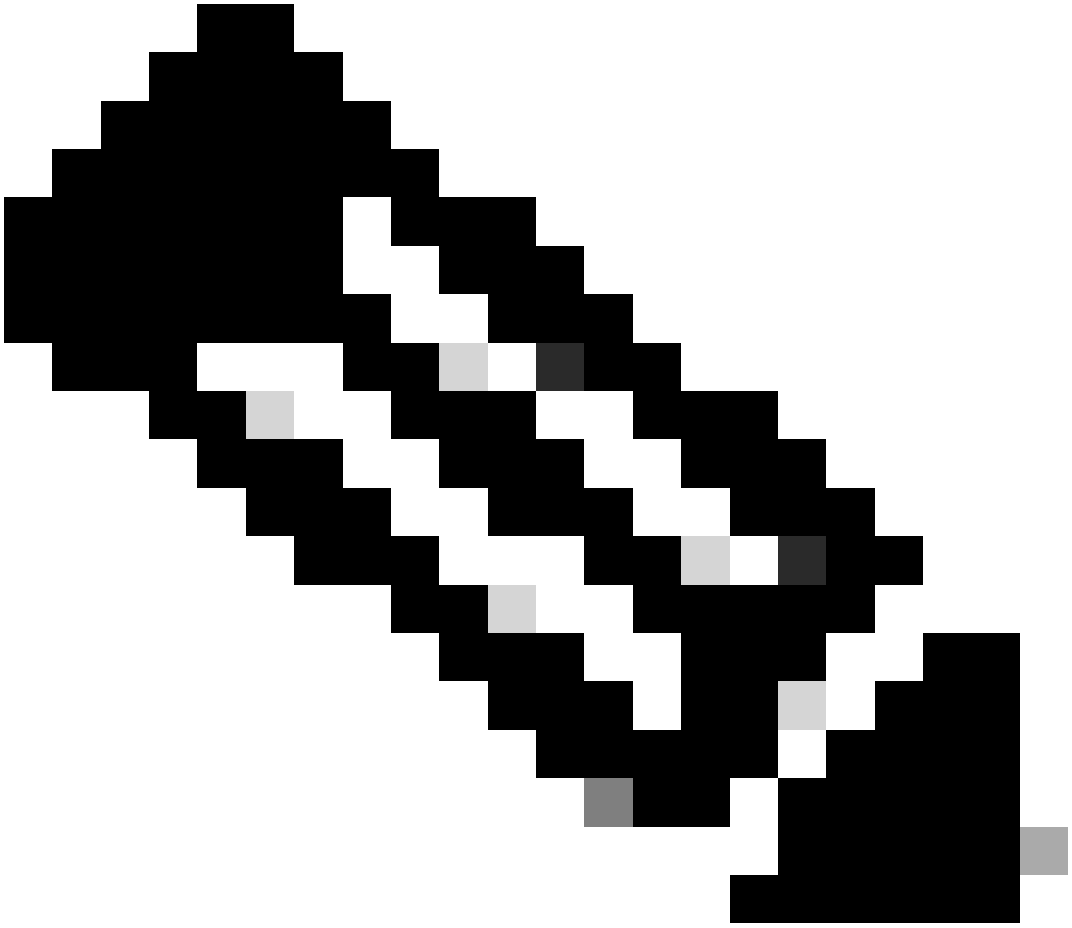
建立警報的其他設定



建立警報的其他設定



建立警報的其他設定



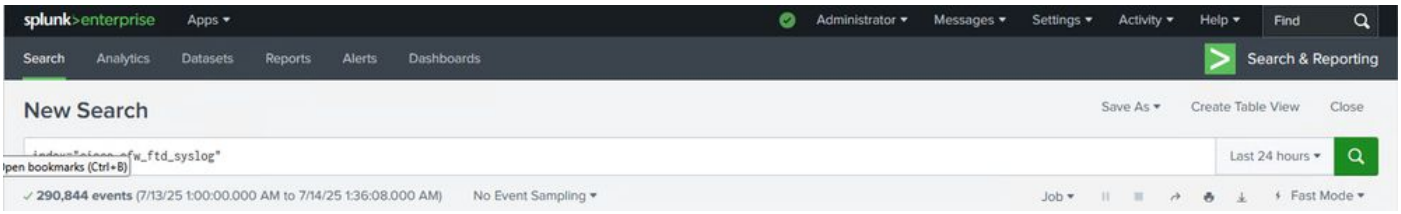
附註：如果要觸發每個結果的警報，也必須相應地定義限制設定。

驗證

建立控制面板和警報後，您可以使用本節中提供的說明來驗證配置、資料流、控制面板和即時警報。

檢視日誌

您可以使用搜尋應用來確認是否收到防火牆傳送的日誌，並且這些日誌是否可以顯示在splunk搜尋頭中。這可以通過檢查已編制索引的最新日誌(搜尋索引= "cisco_sfw_ftd_syslog")以及與其關聯的時間戳來驗證。

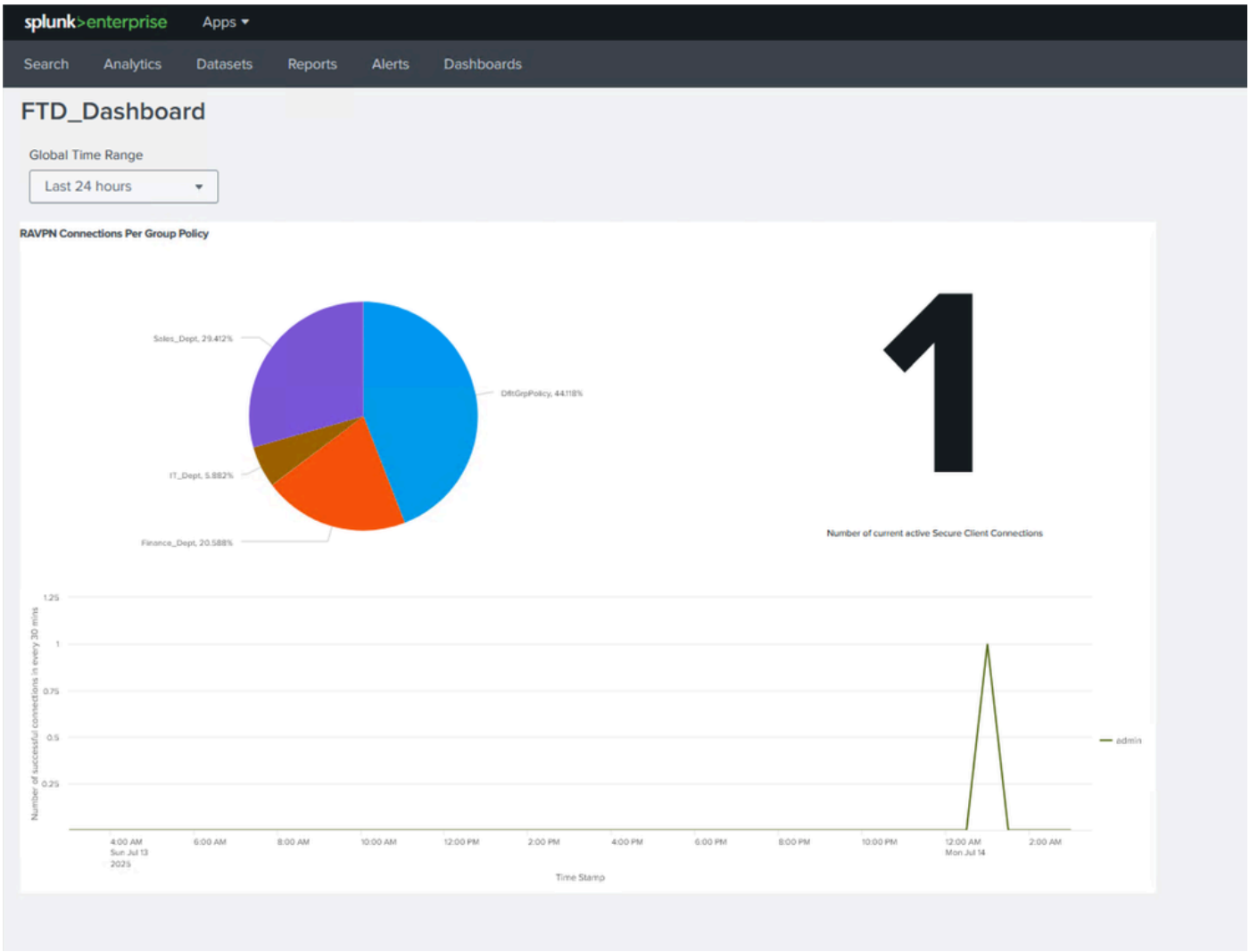


檢查和檢視日誌

檢查和檢視日誌

檢視即時儀表板

您可以導航到已建立的自定義儀表板，並在從FTD生成新資料和日誌時，檢視每個面板上的更改。

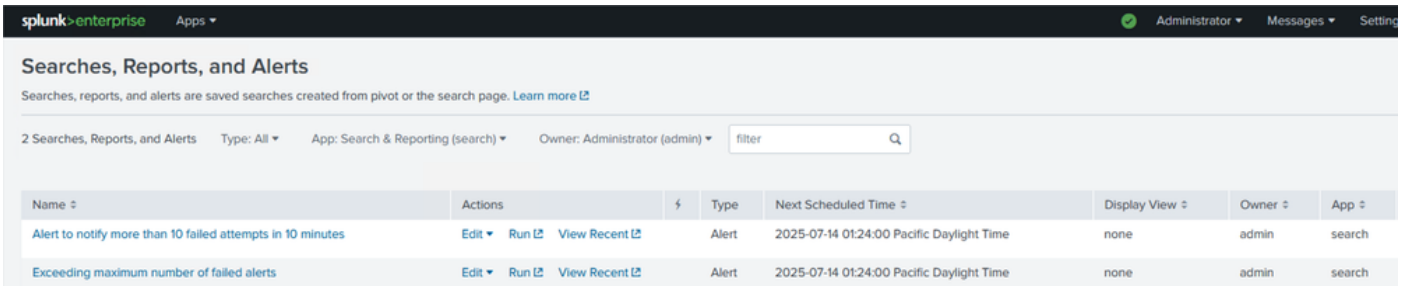


檢視儀表板

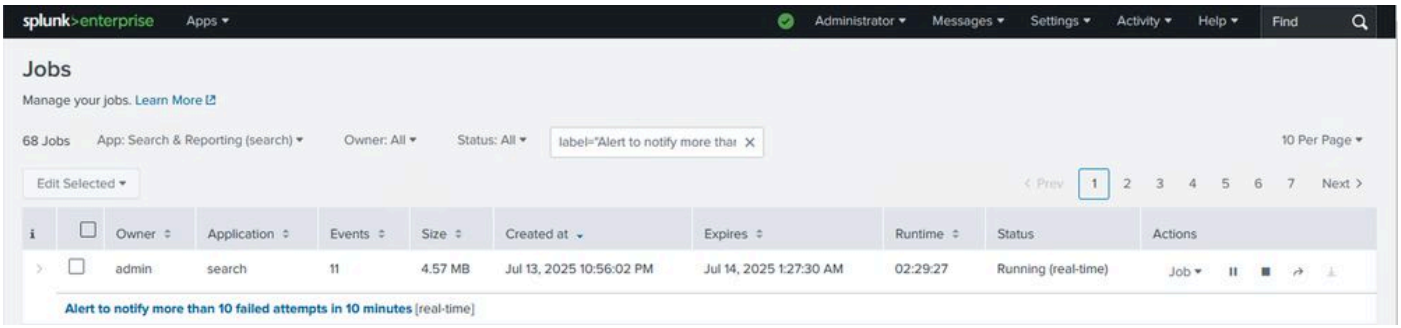
檢查是否已觸發任何警報

要驗證有關警報的資訊，可以導航到搜尋、報告和警報部分，以檢視最近的警報資訊。按一下View

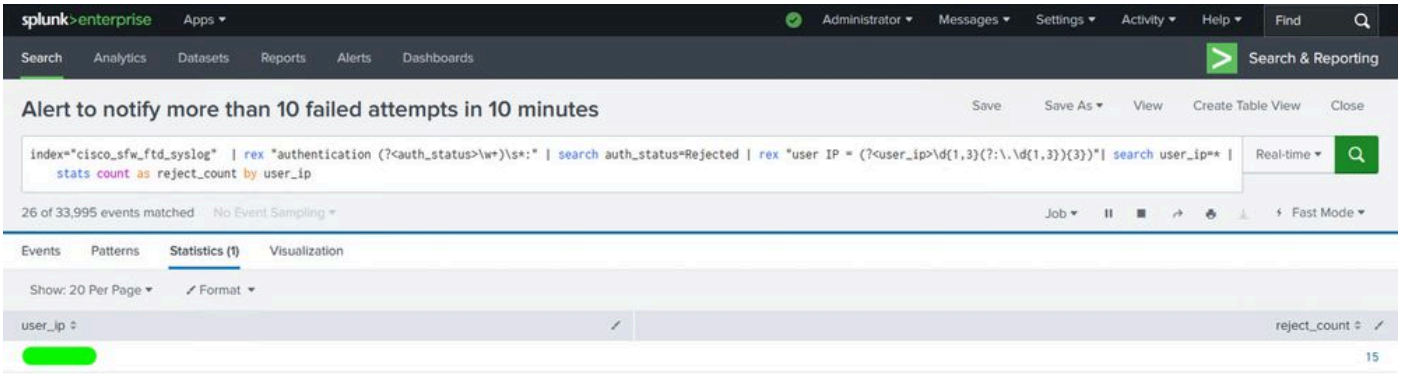
Recent以進一步檢查有關作業和搜尋的資訊。



檢查並檢視警報



檢查並檢視警報



檢查觸發警報的統計資訊

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。