

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](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[組態](#)

[設定FTD的系統日誌設定](#)

[在Splunk Enterprise例項上配置資料輸入](#)

[執行SPL查詢和建立儀表板](#)

[根據SPL查詢配置警報](#)

[驗證](#)

[檢視日誌](#)

[檢視即時儀表板](#)

[檢查是否已觸發任何警報](#)

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面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。

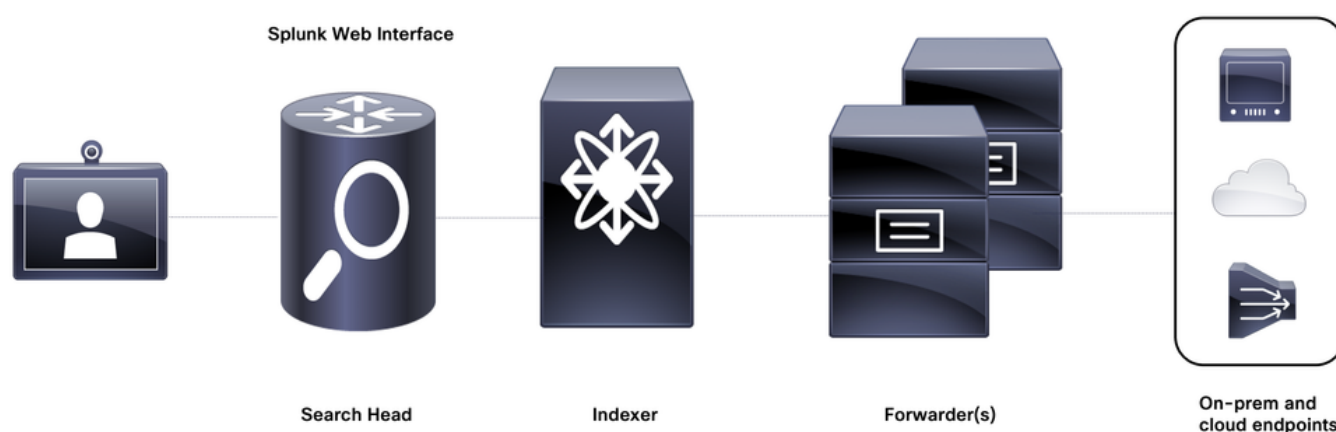
Splunk是一個即時資料分析平台，旨在攝取、索引、搜尋和視覺化電腦生成的資料。Splunk作為安全資訊和事件管理(SIEM)工具在網路安全環境中尤為有效，因為它能夠：

- 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：

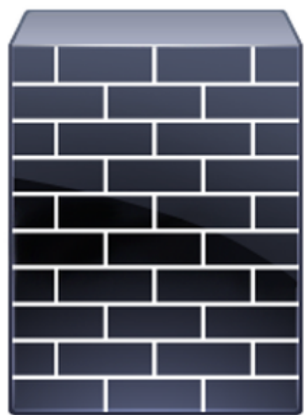
- 輸入
- 正在分析
- 索引
- 正在搜尋

用於實現IPIS管道的底層架構的主要元件如下圖所示：



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-PlatformSettings

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Logging Setup

Logging Destinations

Email Setup

Event Lists

Rate Limit

Syslog Settings

Syslog Servers

Basic Logging Settings

☒ Enable Logging

☐ Enable Logging on the failover standby unit

☒ Send syslogs in EMBLEM format

☒ Send debug messages as syslogs

Memory Size of the Internal Buffer

52428700

(4096-52428800 Bytes)

VPN Logging Settings

☒ Enable Logging to Firewall Management Center

Logging Level

debugging

Specify FTP Server Information

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

Add Syslog Server



IP Address* +

Protocol ☐ TCP ☒ UDP

Port (514 or 1025-65535)

Log Messages in Cisco EMBLEM format(UDP only) ☒

Enable secure syslog. ☐

Reachable By:

- ☐ Device Management Interface (Applicable on FTD v6.3.0 and above)
- ☒ Security Zones or Named Interface

Available Zones



inside
outside

Add

Selected Zones/Interfaces

outside



Interface Name

Add

Cancel

OK

Logging Setup

Logging Destinations

Email Setup

Event Lists

Rate Limit

Syslog Settings

Syslog Servers

☒ Allow user traffic to pass when TCP syslog server is down (Recommended to be enabled)

Message Queue Size(messages)*

512

(0 - 8192 messages). Use 0 to indicate unlimited Queue Size

+ Add

Interface	IP Address	Protocol	Port	EMBLEM	SECURE	
outside		UDP	5156	true	false	

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。

Logging Setup

Logging Destinations

Email Setup

Event Lists

Rate Limit

Syslog Settings

Syslog Servers

+ Add

Logging Destination	Syslog from All Event Class	Syslog from specific Event Class	
No records to display			

FTD上的平台設定 — 新增記錄目的地

Add Logging Filter

?

Logging Destination

Syslog Servers

Event Class

Filter on Severity

debugging

+ Add

Event Class	Syslog Severity	
No records to display		

Cancel

OK

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。

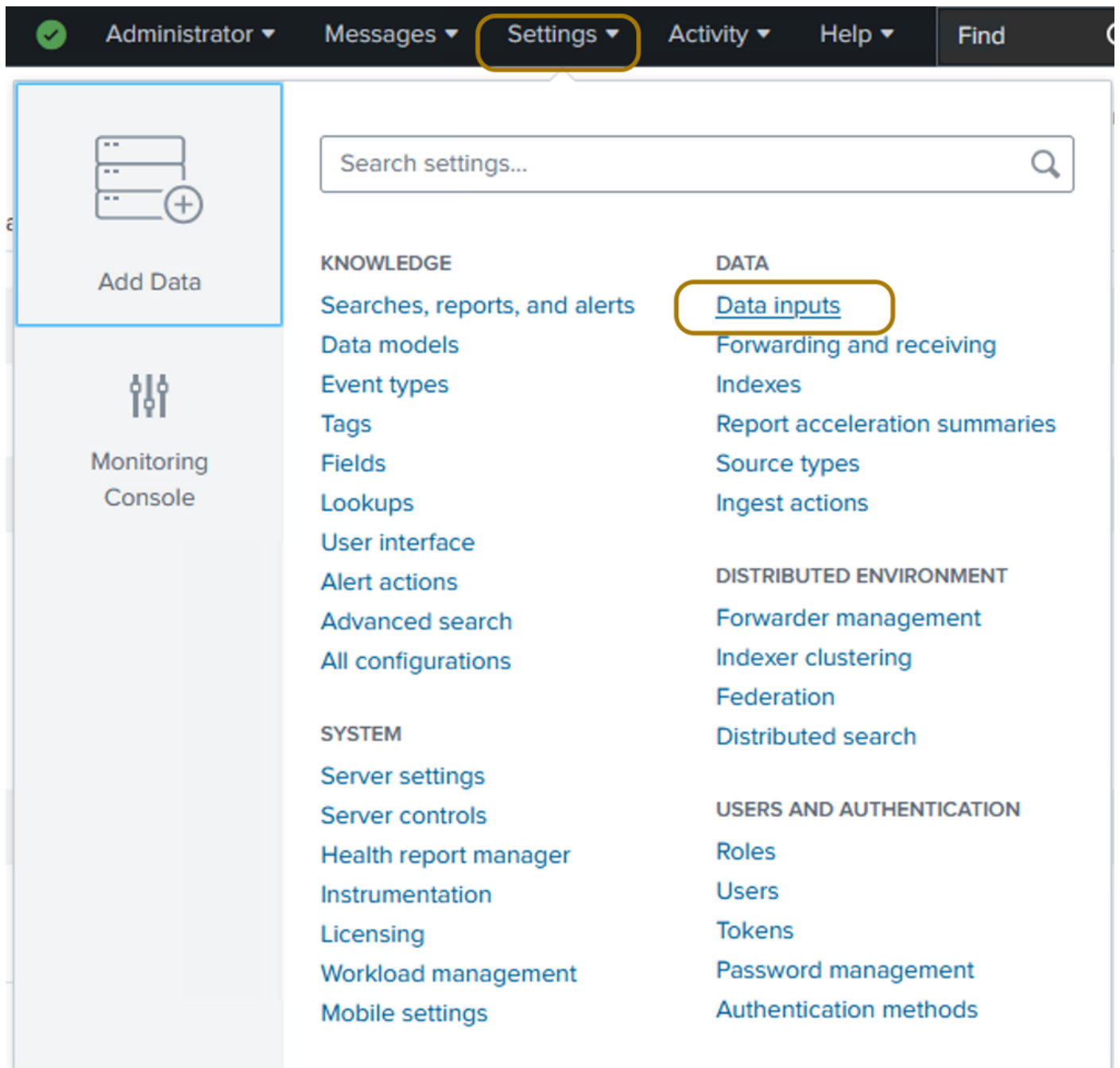
在Splunk Enterprise例項上配置資料輸入

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。

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Data inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to [Forwarding and receiving](#).

Local inputs

Type	Inputs	Actions
Local event log collection Collect event logs from this machine.	-	Edit
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	+ Add new
Files & Directories Index a local file or monitor an entire directory.	20	+ Add new
Local performance monitoring Collect performance data from local machine.	0	+ Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	1	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	1	+ Add new
Registry monitoring Have Splunk index the local Windows Registry, and monitor it for changes.	0	+ Add new

按一下「UDP」進行UDP資料輸入

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

UDP

Data inputs > UDP

filter

25 per page

New Local UDP

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）。

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Add Data

Select Source Input Settings Review Done

< Back Next >

[Local Event Logs](#)
Collect event logs from this machine.

[Remote Event Logs](#)
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

[Files & Directories](#)
Upload a file, index a local file, or monitor an entire directory.

[HTTP Event Collector](#)
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

[Local Performance Monitoring](#)
Collect performance data from this machine.

[Remote Performance Monitoring](#)
Collect performance and event information from remote hosts. Requires domain credentials.

[Registry monitoring](#)
Have the Splunk platform index the local Windows Registry, and monitor it for changes.

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). [Learn More](#)

TCP UDP

Port ? 5156
Example: 514

Source name override ? optional
host:port

Only accept connection from ?
example: 10.1.2.3, !badhost.splunk.com, *splunk.com

FAQ

- > How should I configure the Splunk platform for syslog traffic?
- > What's the difference between receiving data over TCP versus UDP?
- > Can I collect syslog data from Windows systems?
- > What is a source type?

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。

splunkenterpriseApps

AdministratorMessagesSettingsActivityHelpFind

Add Data

Select SourceInput SettingsReviewDone

< BackReview >

Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

SelectNew

cisco:ftd:syslog

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. [Learn More](#)

App Context

Apps Browser (appsbrowser)

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Method ?

IPDNSCustom

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index

cisco_sfw_ftd_syslogCreate a new index

配置資料輸入設定

步驟6.檢查設定，然後按一下「Submit」。

Add Data

Select SourceInput SettingsReviewDone

< BackSubmit >

Review

Input Type UDP Port

Port Number 5156

Source name override N/A

Restrict to Host

Source Type cisco:ftd:syslog

App Context launcher

Host (IP address of the remote server)

Index cisco_sfw_ftd_syslog

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。

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Apps < Manage

Find more apps 🔍 Search apps by name...

- Cisco Security Cloud
- Search & Reporting**
- Audit Trail
- Cisco Firepower App for Splunk
- Cisco Secure Firewall
- Cisco eStreamer eNcore for Splunk
- Splunk Secure Gateway
- Upgrade Readiness App

Hello, Administrator

Bookmarks Dashboard Search history Recently viewed Created by you Shared with you

My bookmarks (0) Add bookmark

Shared with my organization (0) Add bookmark

Shared by me

Shared by other administrators

Splunk recommended (13)

Common tasks Hide for users

- Add data Add data from a variety of common sources.
- Search your data Turn data into doing with Splunk search.
- Visualize your data Create dashboards that work for your data.

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。

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search Save As Create Table View Close

index="cisco_sfwd_syslog" | rex field=_raw "Group \(<?group_policy>[^\)]*\) User \(<?>[^\)]*\) IP \(<?>[^\)]*\) IPv4 Address \(<?>[^\)]*\) IPv6 address \(<?>[^\)]*\) assigned to session" | search group_policy=* | stats count by group_policy

28 events (before 7/13/25 8:15:04.000 PM) No Event Sampling

Events (28) Patterns Statistics (4) Visualization

Timeline format Zoom Out Zoom to Selection Deselect 1 hour per column

Format Show: 20 Per Page View: List

Hide Fields	All Fields	Time	Event
SELECTED FIELDS # group_policy 4 # host 1 # source 2	INTERESTING FIELDS # index 1 # linecount 1 # punct 1 # sourcetype 1 # splunk_server 1 # timestamp 1	6/24/25 10:58:43.000 PM	Jun 24 22:58:43 [REDACTED] : 2025 Jun 25 05:01:01 UTC a3a8bea6-0828-11ef-aa8a-b652b0561baa : XFTD-svc-4-722051: Group <Sales_Dept> User [REDACTED] IP <[REDACTED]> IPv4 Address [REDACTED] IPv6 address <[:> assigned to session group_policy = Sales_Dept host = [REDACTED] source = udp:5156
		6/24/25 8:32:58.000 PM	Jun 24 20:32:58 [REDACTED] : 2025 Jun 25 02:35:16 UTC a3a8bea6-0828-11ef-aa8a-b652b0561baa : XFTD-svc-4-722051: Group <IT_Dept> User [REDACTED] IP <[REDACTED]> IPv4 Address [REDACTED] IPv6 address <[:> assigned to session group_policy = IT_Dept host = [REDACTED] source = udp:5156
		6/24/25 8:29:15.000 PM	Jun 24 20:29:15 [REDACTED] : 2025 Jun 25 02:31:33 UTC a3a8bea6-0828-11ef-aa8a-b652b0561baa : XFTD-svc-4-722051: Group <Sales_Dept> User [REDACTED] IP <[REDACTED]> IPv4 Address [REDACTED] IPv6 address <[:> assigned to session group_policy = Sales_Dept host = [REDACTED] source = udp:5156
		6/24/25 8:27:27.000 PM	Jun 24 20:27:27 [REDACTED] : 2025 Jun 25 02:29:45 UTC a3a8bea6-0828-11ef-aa8a-b652b0561baa : XFTD-svc-4-722051: Group <Sales_Dept> User [REDACTED] IP <[REDACTED]> IPv4 Address [REDACTED] IPv6 address <[:> assigned to session group_policy = Sales_Dept host = [REDACTED] source = udp:5156
		6/24/25 8:26:59.000 PM	Jun 24 20:26:59 [REDACTED] : 2025 Jun 25 02:29:17 UTC a3a8bea6-0828-11ef-aa8a-b652b0561baa : XFTD-svc-4-722051: Group <Finance_Dept> User [REDACTED] IP <[REDACTED]> IPv4 Address [REDACTED] IPv6 address <[:> assigned to session

使用SPL查詢搜尋事件

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search Save As Create Table View Close

index="cisco_sfwd_syslog" | rex field=_raw "Group \(<?group_policy>[^\)]*\) User \(<?>[^\)]*\) IP \(<?>[^\)]*\) IPv4 Address \(<?>[^\)]*\) IPv6 address \(<?>[^\)]*\) assigned to session" | search group_policy=* | stats count by group_policy

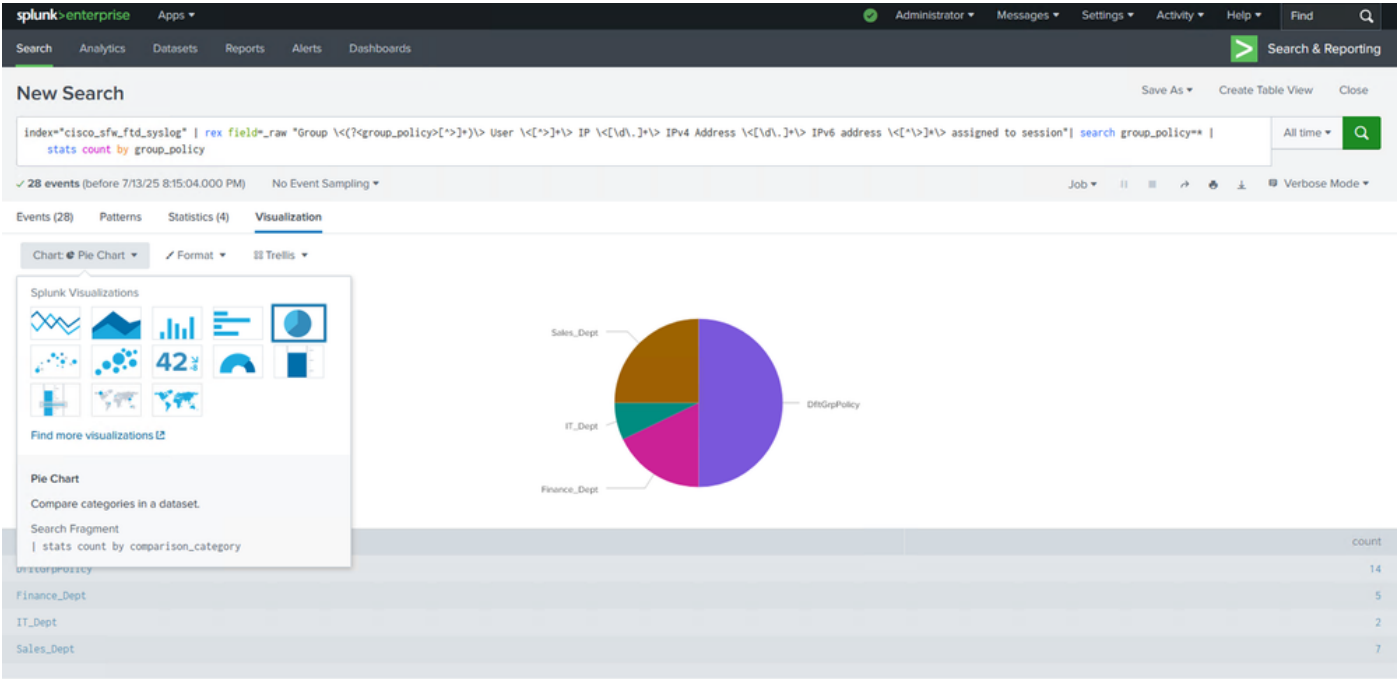
28 events (before 7/13/25 8:15:04.000 PM) No Event Sampling

Events (28) Patterns Statistics (4) Visualization

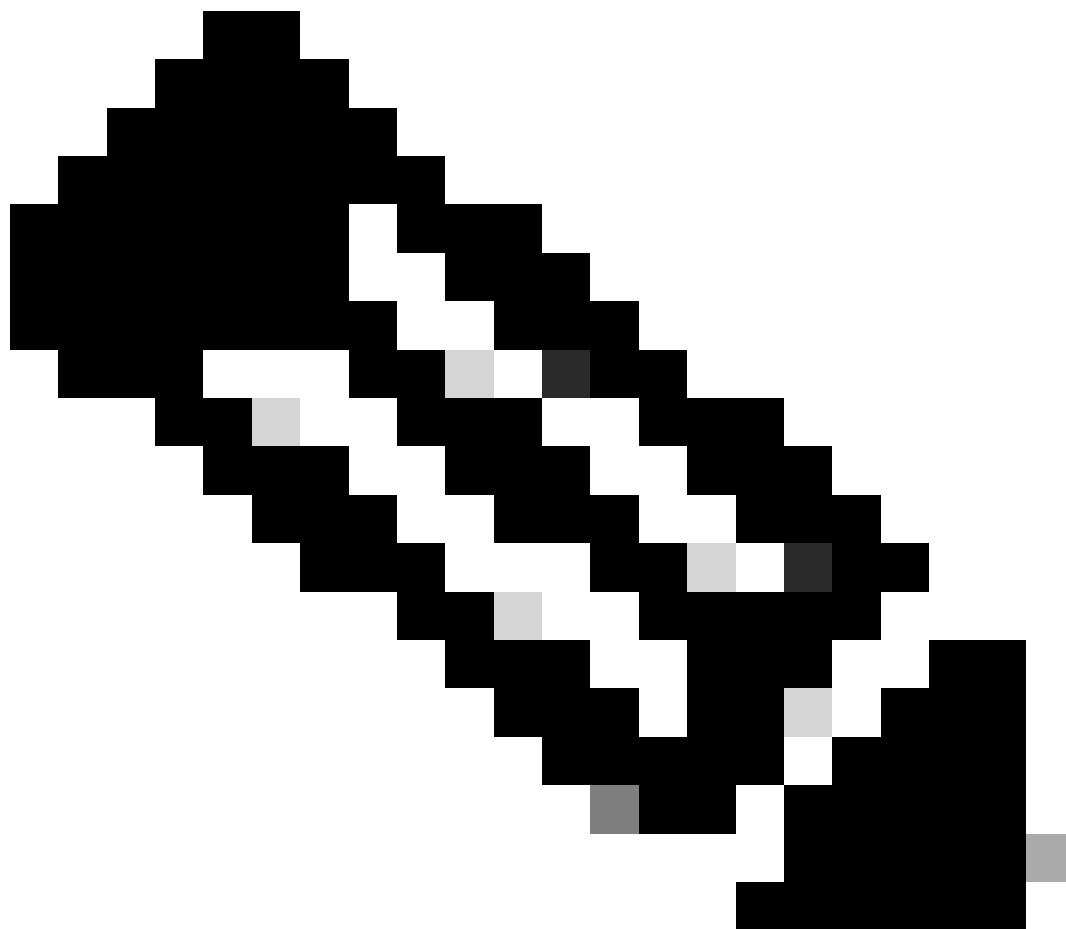
Show: 20 Per Page Format Preview: On

group_policy	count
OffitGrpPolicy	14
Finance_Dept	5
IT_Dept	2
Sales_Dept	7

檢查統計資訊頁籤

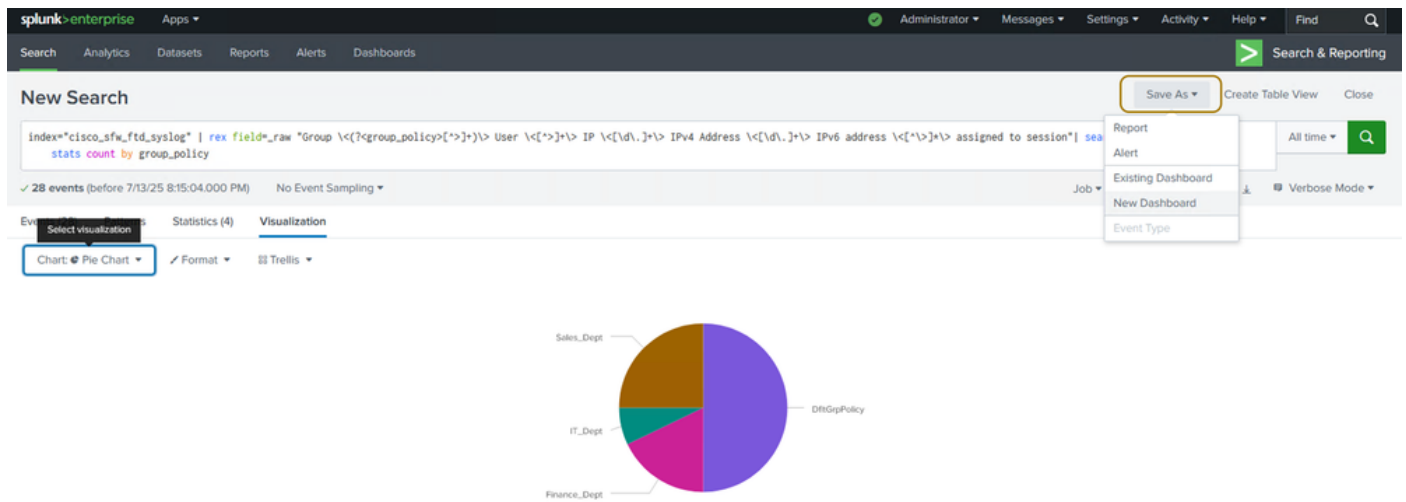


視覺化頁籤將顯示圖形/圖表



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

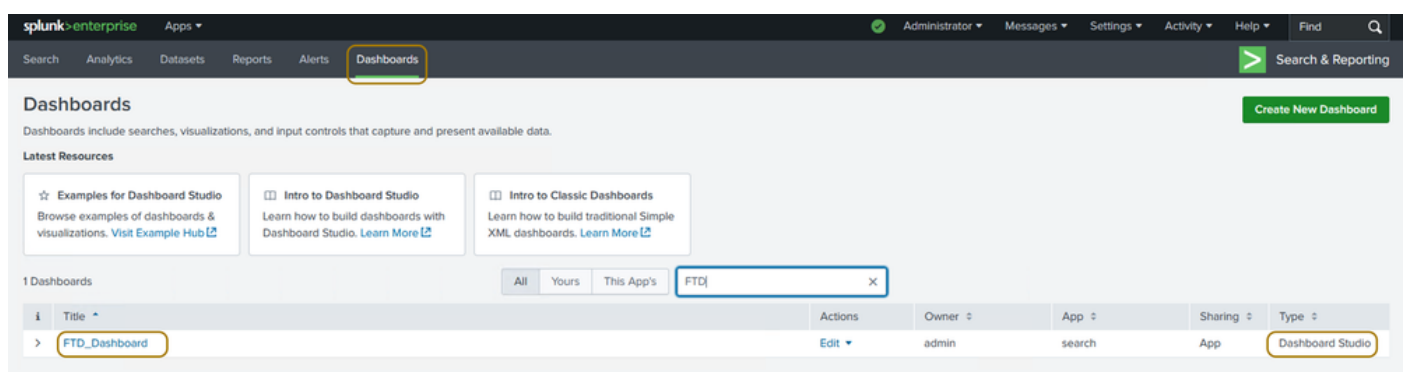
Cancel

Save to Dashboard

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。

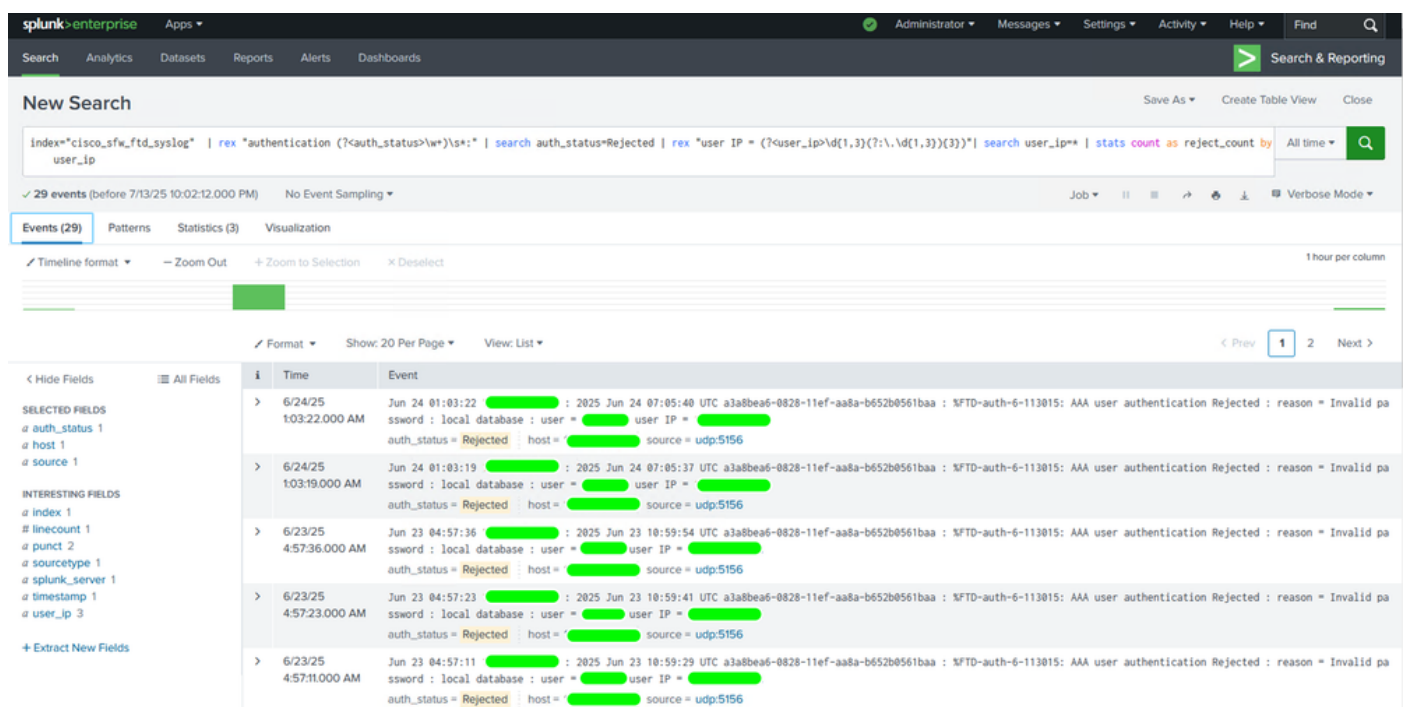
步驟6.定位至控制面板標籤，以搜尋並選擇您建立的控制面板。按一下它可檢視、編輯或重新排列其面板。



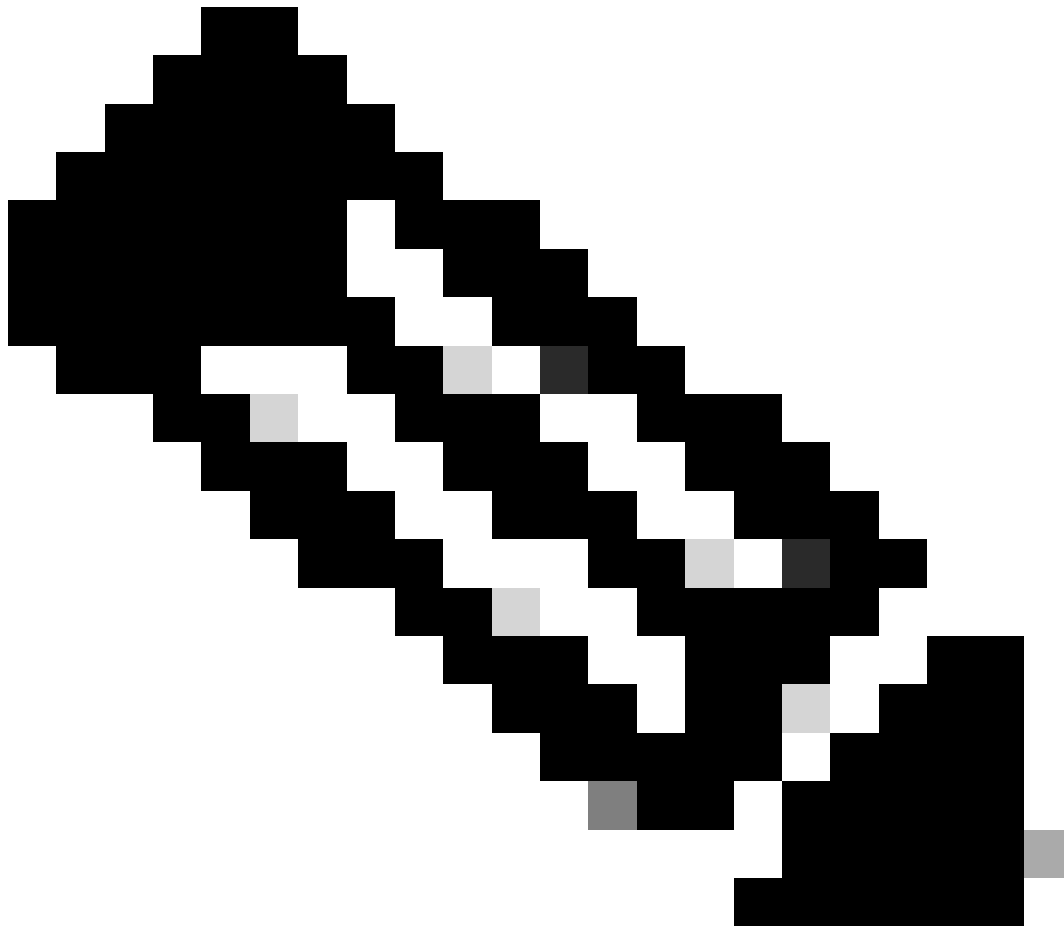
如何檢視儀表板

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 continuously)

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.

Save As Alert



Settings

Title

Alert to notify more than 10 failed attempts in 10 minutes

Description

Optional

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Expires

10

minute(s) ▼

Trigger Conditions

Trigger alert when

Custom ▼

e.g. "search count > 10"

in

Trigger

Throttle ?

☐

Trigger Actions

+ Add Actions ▼

Per-Result

Triggers whenever search returns a result.

Number of Results

Triggers based on a number of search results during a rolling-window of time.

Number of Hosts

Triggers based on a number of hosts during a rolling-window of time.

Number of Sources

Triggers based on a number of sources during a rolling-window of time.



Custom

Triggers based on a custom condition during a rolling-window time.

Save

Trigger Conditions

Trigger alert when

Custom ▼

search reject_count>10

e.g. "search count > 10". Evaluated against the results of the base search.

in

5

minute(s) ▼

Trigger

Once

For each result

Throttle ?

☐

建立警報的其他設定

Trigger Actions

+ Add Actions ▼

When triggered



Add to Triggered Alerts

Remove

Severity

Medium ▼

Info

Low

✓ Medium

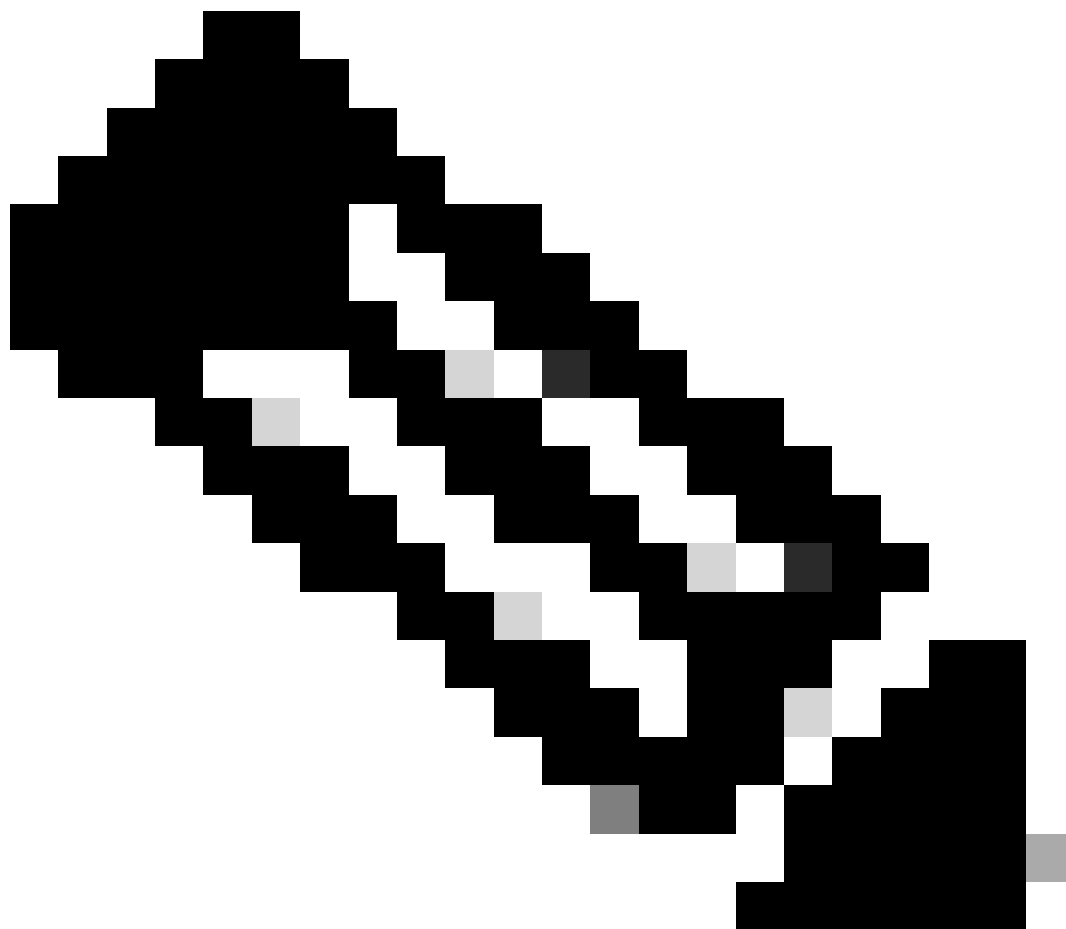
High

Critical

Cancel

Save

建立警報的其他設定



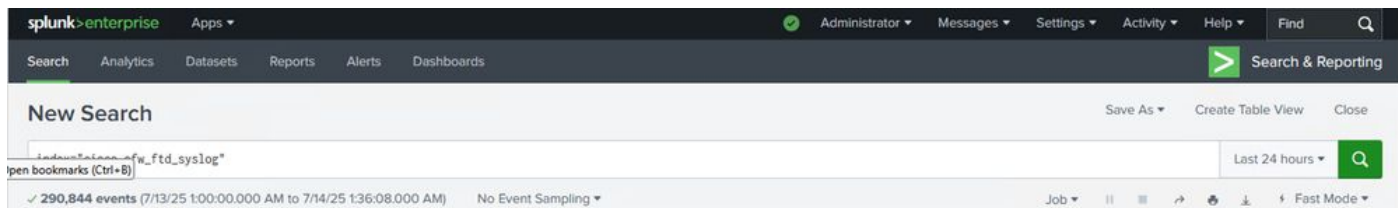
附註：如果要觸發每個結果的警報，也必須相應地定義限制設定。

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。



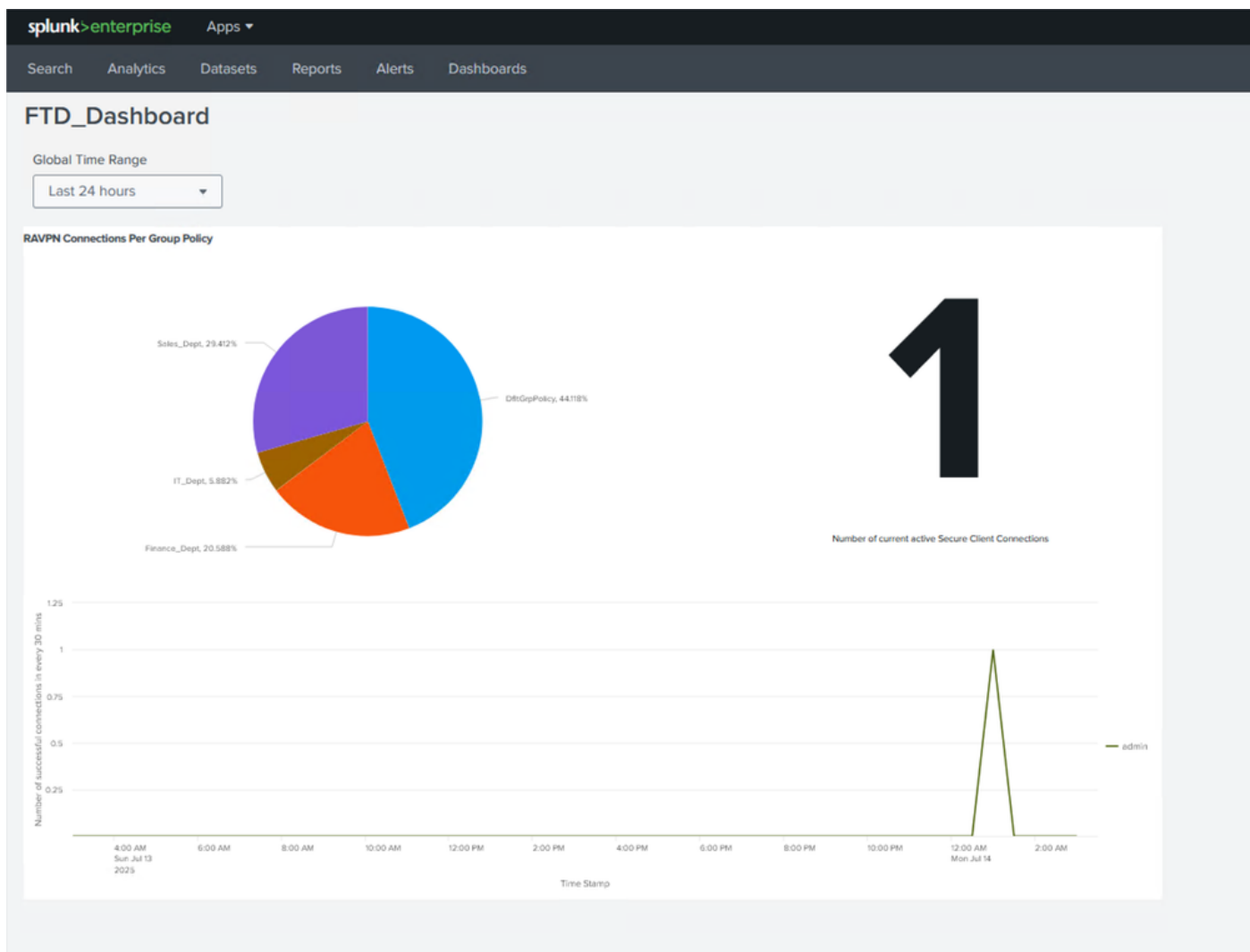
檢查和檢視日誌

i	Time	Event
>	7/14/25 1:36:00.000 AM	Jul 14 01:36:00 [REDACTED] :Jul 14 07:36:09 UTC: %FTD-config-7-111009: User 'enable_1' executed cmd: show resource usage resource Routes host = [REDACTED] ; source = udp:5156

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。

splunk>enterpriseApps

AdministratorMessagesSettings

Searches, Reports, and Alerts

Searches, reports, and alerts are saved searches created from pivot or the search page. [Learn more](#)

2 Searches, Reports, and AlertsType: AllApp: Search & Reporting (search)Owner: Administrator (admin)filter

Name	Actions	Type	Next Scheduled Time	Display View	Owner	App
Alert to notify more than 10 failed attempts in 10 minutes	Edit Run View Recent	Alert	2025-07-14 01:24:00 Pacific Daylight Time	none	admin	search
Exceeding maximum number of failed alerts	Edit Run View Recent	Alert	2025-07-14 01:24:00 Pacific Daylight Time	none	admin	search

檢查並檢視警報

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

Jobs

Manage your jobs. [Learn More](#)

68 JobsApp: Search & Reporting (search)Owner: AllStatus: Alllabel="Alert to notify more than 10 failed attempts in 10 minutes"10 Per Page

Edit Selected

i	Owner	Application	Events	Size	Created at	Expires	Runtime	Status	Actions
>	admin	search	11	4.57 MB	Jul 13, 2025 10:56:02 PM	Jul 14, 2025 1:27:30 AM	02:29:27	Running (real-time)	Job Pause Stop Refresh Download

Alert to notify more than 10 failed attempts in 10 minutes [real-time]

檢查並檢視警報

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

Alert to notify more than 10 failed attempts in 10 minutes

SaveSave AsViewCreate Table ViewClose

index="cisco_sfwd_syslog" | rex "authentication (?<auth_status>\w*)s*:" | search auth_status=Rejected | rex "user IP = (?<user_ip>\d{1,3}(?:\.\d{1,3}){3})" | search user_ip=* | stats count as reject_count by user_ip

26 of 33,995 events matchedNo Event Sampling

JobPauseStopRefreshDownloadFast Mode

EventsPatternsStatistics (1)Visualization

Show: 20 Per PageFormat

user_ip	reject_count
	15

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）。