

ةصصخم تاهيبننتو تامولعم تاحول عاشنإ FTD نم Syslogs مادختساب Splunk ىلع

تايوتحملإ

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتلإ](#)

[ةكبشلل ليطي طختلا مسرلا](#)

[تانوكتلإ](#)

[FTD ل Syslog تادادعل نيوكت](#)

[Splunk Enterprise ليثم ىلع تانايبل لغلل نيوكت](#)

[تامولعملإ تاحول عاشنإو SPL تامالعتسا ذي فنن](#)

[SPL تامالعتسا ىلإ اذانتسا تاهيبننتلا نيوكت](#)

[ةحصلا نم ققختلا](#)

[تالجسلا ضرع](#)

[ىلعفلإ تقولا ي ف تامولعملإ تاحول ضرع](#)

[تاهيبننت ةيأ لي غشت نم ققختلا](#)

ةمدقملا

ميسقتلا ىلإ syslogs لاسرلإ FTD نيوكتل ةوطخب ةوطخي شملل دنتسملل اذه فصبي
ةصصخم تاهيبننتو تامولعم تاحول عاشنإل تالجسلل هذه مادختساو.

ةيساسألا تابلطتملا

تابلطتملا

دشرم ليكشت اذه لالخن نم رمي نأ لبق عوضوم اذه نم ةفرعم تنأ ىقلتني نأ يصوي cisco:

- Syslog
- Splunk (SPL) ي ف ثحبلل ةجلعم ةغلب ةيساسأ ةفرعم

لكي دلوم داخ ىلع تبثم Splunk Enterprise ليثم لعفلاب لكي دل نأ اضيأ دنتسملل اذه ضررت في
بيلولا ةهجاو ىلإ لوصولل قح.

ةمدختسملا تانوكملا

ةيلاتلا ةيداملل تانوكملل او جماربلا تارادصلإ ىلإ دنتسملل اذه ي ف ةدراولل تامولعملل دنتست

- Cisco Firepower Threat Defense (FTD) ديق رادصلال ىلع ليغشتال ديق 7.2.4
- Cisco Firepower (FMC) رادصلال ىلع لمعي 7.2.4 رادإ زكرم
- Windows زاهج ىلع ليغشتال ديق (9.4.3 رادصلال) Splunk Enterprise لىثم

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دنتسمل اذه يف ةدراول تامولعمل عاشنإ مت (يضايرتفا) حوسمم نيوكتب دنتسمل اذه يف ةمدختسمل ةزهجال عيمج تأدب.

ةيساسأ تامولعم

للسلثال ثادحأ يظغت ةيليصفت syslogs عاشنإب Cisco نم FTD لوكوتورب ةزهجأ موقت عم تالچسل هذه جمدهي تي. ريثكل كذا ريغو لاصلتال ثادحأو لوصول يف مكحتال تاسايسو ةكبشل نامأ تايلمعمل يلعفل تقولا يف هيبنتلال واعف ليحلت عارجا ةينام Splunk.

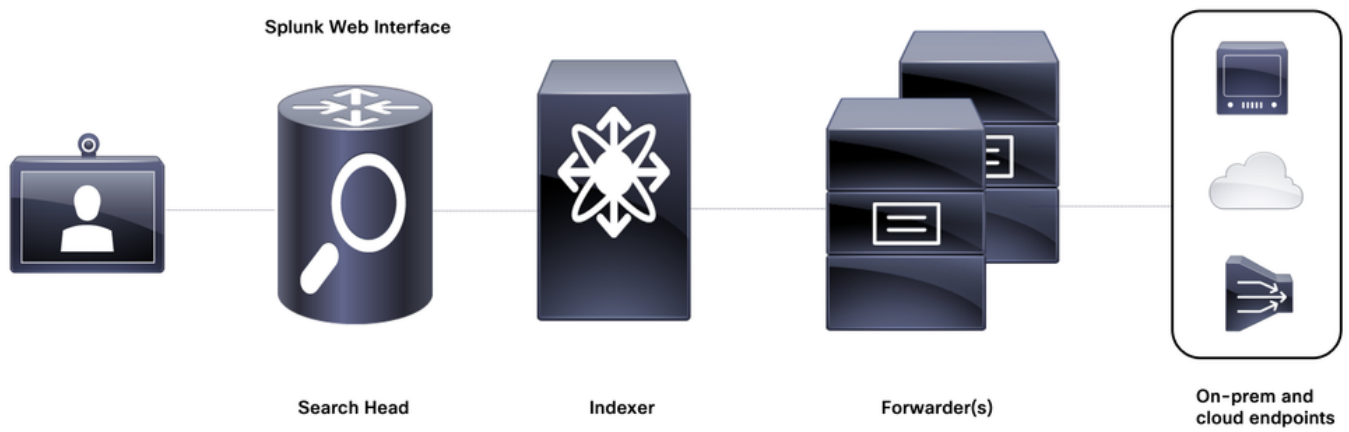
متي تال تانايبل جارختسال ممصم يلعفل تقولا يف تانايبل تاليلحت ماظن وه SPLUNK صاخ لكشب الاعف SPLUNK ربتعي. اهضرعو اهنع ثحبلاو اهتسرهفو زاهجال ةطساوب اهؤاشنإ ىلع هتردقل ارظن (SIEM) نامأ تامولعمو ثادحأ ةرادإ ةادأك يناربيلسل نامأ تائيب يف:

- سايقلا دنع لچسل تانايبل لاخدا
- SPL مادختساب ةدقعم ثحب تايلمع عارجا
- تاهيبننو تامولعم تاحول عاشنإ
- ثداوحال عم قفاوتلالو نمألا ةمظنا عم جمدل

ةزهجال تانايبل لعج لجأ نم ةلكيهم تاقفدت لالخن نم تانايبل ةجلاعمب Splunk ةيلمع موقت ةيساسألا لحارملال ىلإ راشي ام ةداع. ذيفنتلل ةلباقو ةديفم ةلكيهم هبش وأ ةلكيهم ريغ لثمت يتلالو IPIS مساب اذه بيبانألا طخل:

- لاخدا
- ليحلت
- ةسرهف
- ثحب

تاقفدت قيقحت يف ةمدختسمل ةيساسألا ةينبلل ةيسيئرلا ةماعلا تانوكمل ضرع متي يطيختل مسرلا اذه يف IPIS:



ةمخض ةيساسأ ةينب

نيوكتلا

ةكبشلل يطي طختلا مسرلا

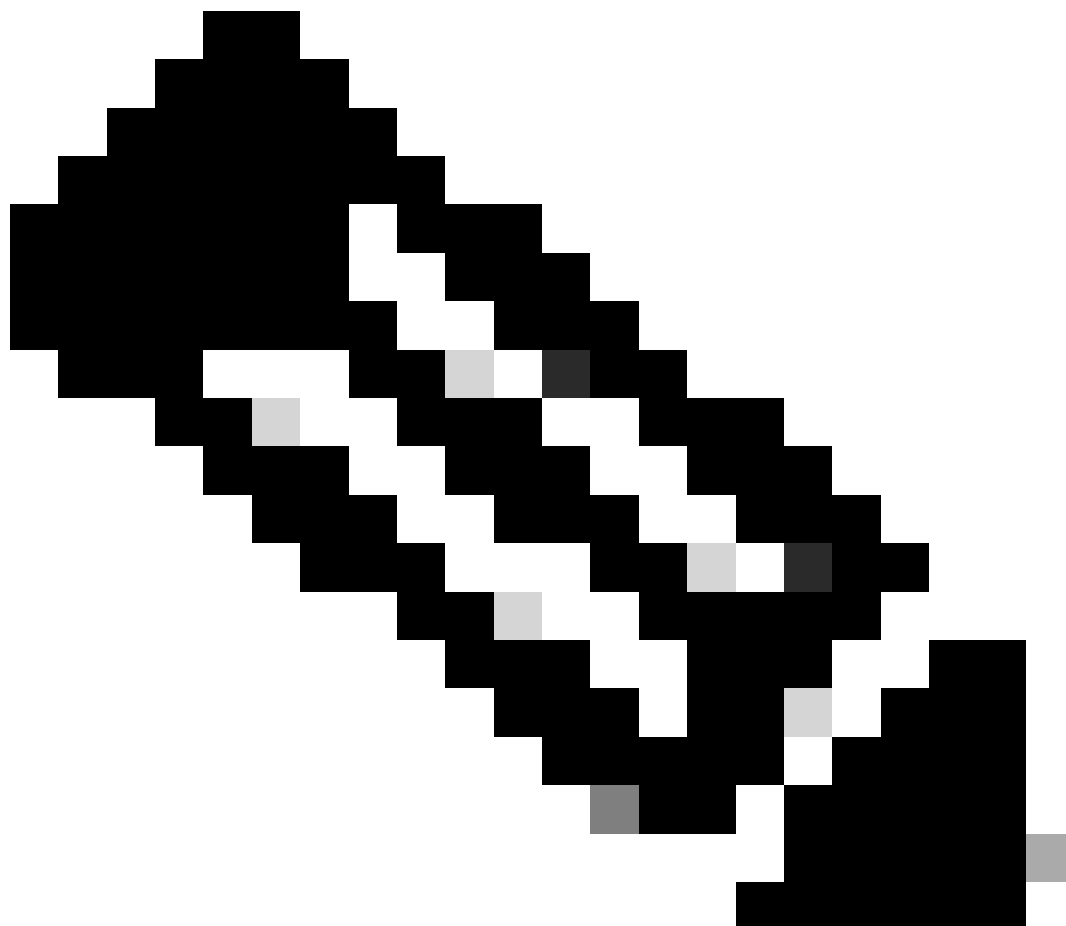


**Firepower Threat
Defense device**



**Syslog server with the
Splunk Search Head**

ةكبشلل يطي طختلا مسرلا



ردصم لل ةلصفنم تاليثم دنتسم الاذهب ةصاخلا لمعملا ةئيب بلطت ال :ةظحال م
Splunk ليثم تئبثت مت يذال syslog م داخ ي Windows زاهج لمعي .ةسرهفملاو
ثحب س أرو سرهفمك هيلع Enterprise

تانيوكتال

FTD ل syslog تادادعإ نيوكت

ماظنل تادادعإ > ةزهجألا نمض FTD ل FMC ىلع ةلؤلأال syslog تادادعإ نيوكتب مق 1. ةوطخال
هيلع Splunk ليثم ليغشت متي يذال syslog م داخ ىلإ تالجسلا لاسرل يساسألا

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 - Syslog يلع يساسألماظنللا تادادع

Splunk Enterprise ليثم تيبتت هي فمتي يذلا زاهلل IP ناووع نيوكتب مق 2. ةوطخلال
روكذم وه امك لوقحل ديحتب مق syslog. مداخلك هليغشتو

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



Add

inside
outside

Selected Zones/Interfaces

outside



Interface Name

Add

Cancel

OK

syslog مداخل ةفاضل - FTD لى لى ساسألل ماطنلل تادادعل

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	

فامض Syslog مءاخ - FTD ىلع يساسألا ماطنلا تاءاعإ

قلاحل اقفلولسلسلال ىوسم نلعل نكمى Syslog. مءاؤل لسللسل ةهؤو فضا. 3 ةوطلؤل لكب ةصاؤل مءاؤلسالا وأ رائلؤل

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			

لسلسل ةهؤو فاضا - FTD ىلع يساسألا ماطنلا تاءاعإ

Add Logging Filter

Logging Destination
Syslog Servers

Event Class
Filter on Severity
debugging

+ Add

Event Class	Syslog Severity	
No records to display		

Cancel

OK

لسلسل ةهؤول ةروطؤل ىوسم نلعلل - FTD ىلع يساسألا ماطنلا تاءاعإ

ئاوطلؤل هؤه لاملكإ ءعب FTD ىلع يساسألا ماطنلا ءاعإ ئارلللؤل رشنل مقل

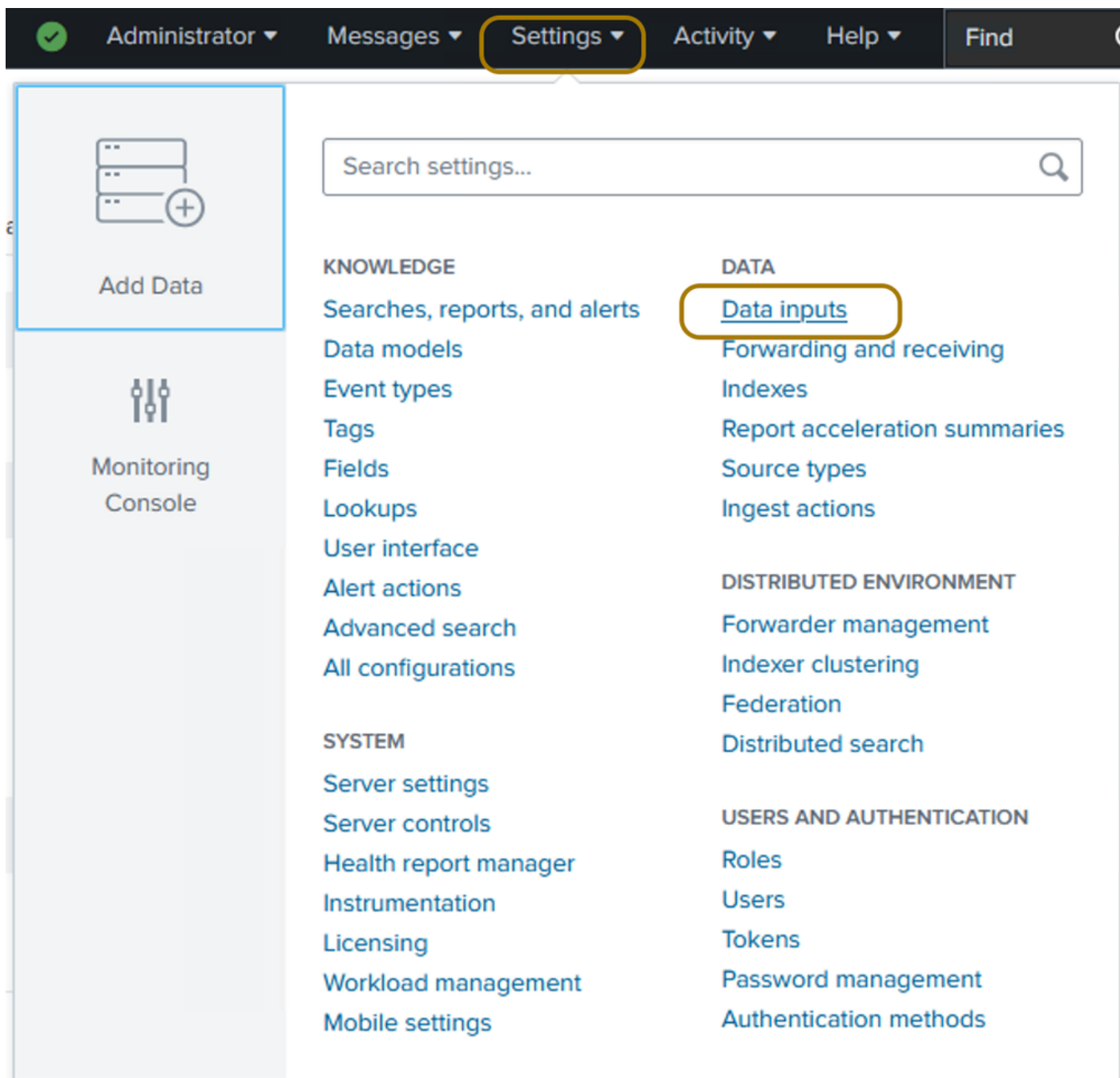
Splunk Enterprise لسلل ىلع ئانايلل لءاؤل ئلؤل

Splunk Enterprise لي م بيو هجاو ىل ل وخذل ليجست 1. ةوطخل



SPLUNK بيو هجاو ىل ل وخذل ليجست ةحفص

لقتنا Splunk.ىل syslogs ةسرهفو نيزخت كنكمي ىتح تانايب لاخدا ديدحت بجي 2. ةوطخل
ل وخذل ليجست دعب تانايب لالاخدا > تانايب ل > تادادعلا ىل



Splunk في تانايابل تالخدم إلى لقتنا

رهظت التلية لصل في ديدجالي ل UDP إلى عرقنا م UDP رتخأ 3. ةوطخل

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

UDP تانايې لځدال 'UDP' ىل ع رقن

splunk>enterprise

Apps

Administrator

Messages

Settings

Activity

Help

Find

UDP

Data inputs > UDP

filter

Q

New Local UDP

25 per page

'دي دج ي ل حم UDP' لځد اءاشن

نأ ام ب سفن ل ا تن ك يغبني وه .تلسراً نو كي syslogs ل ا يأ ىل ع ءاني م ل ا 4 ةوطخ ل خدي ل ا تلبق in order to 5156 ةل ا ح ل ا هذ ه ي ف ،د ا د ع ا ةي ل م ع FTD syslog ل ا ىل ع ل ك شي ءاني م ل ا نم IP ل ا ىل ل ا ل ا ح نم ل ي ص و ت ل و ب ق ط ق ف ل ا ت ت ب ث ، (ل ا FTD) ر د ص م د ح ا و نم ط ق ف syslogs (ي ل ا ت ل ا) Next ق و ف ر ق ن ا . ل د ا ن splunk ل ا ع م ل ص ت ي نو كي نأ FTD ل ا ىل ع ن ر ا ق ل ا

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?

FTD و ذفنم لل IP ناو نع دي دحت

اقبس م ةددم ال ك لت نم ل قحل م ق ةسره فو ردم ال عون رايتخاو شحب ال كن كم ي 5. ةوطخل لوقحل ل ةيضا رتفال ا تاداع ال م ادختس كن م ي . ةيالات ال ةروصل ال ي ف زرم وه امك Splunk لى ل ةي ق ب م ال .

Add Data Select Source Input Settings Review Done < Back Review >

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.

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](#)

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](#)

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](#)

Select **New**
cisco:ftd:syslog

App Context
Apps Browser (appsbrowser)

Method
IP DNS Custom

Index
cisco_sfw_ftd_syslog [Create a new index](#)

تاناي ب ال ل ادخ ا تاداع ل ني وكت

ل اسر ا قوف ر قن او تاداع ال عجار 6. ةوطخل

Add Data Select Source Input Settings Review Done < Back Submit >

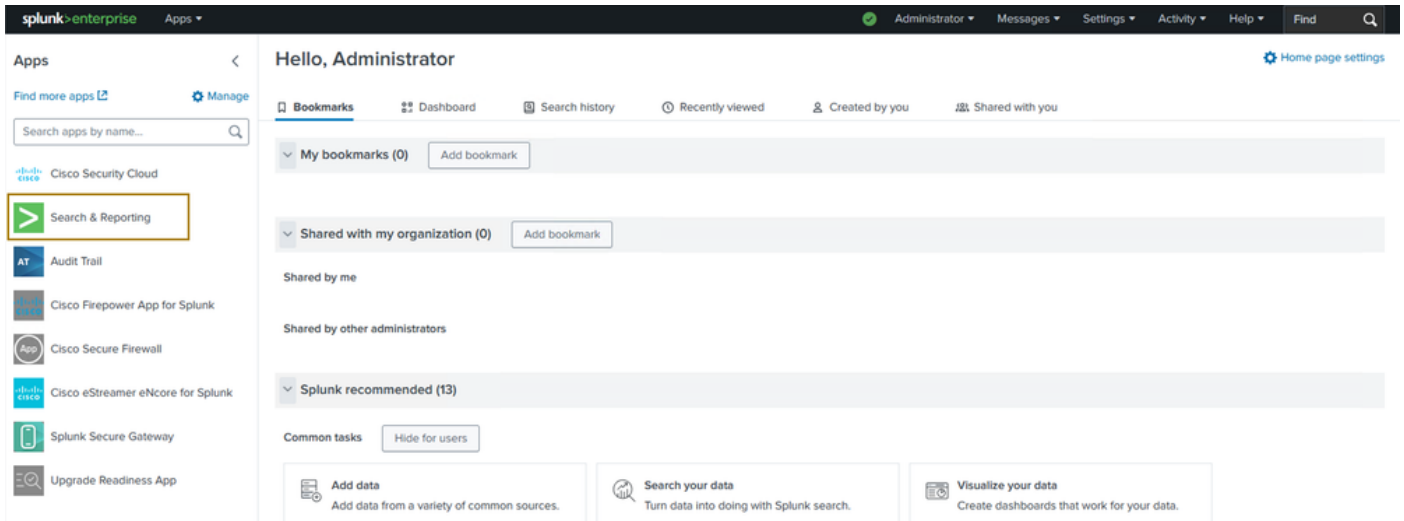
Review

Input Type UDP Port
Port Number 5156
Source name override N/A
Restrict to Host IP address of the remote server
Source Type cisco:ftd:syslog
App Context launcher
Host IP address of the remote server
Index cisco_sfw_ftd_syslog

تاناي ب ال ل ادخ ا تاداع ل عجار م

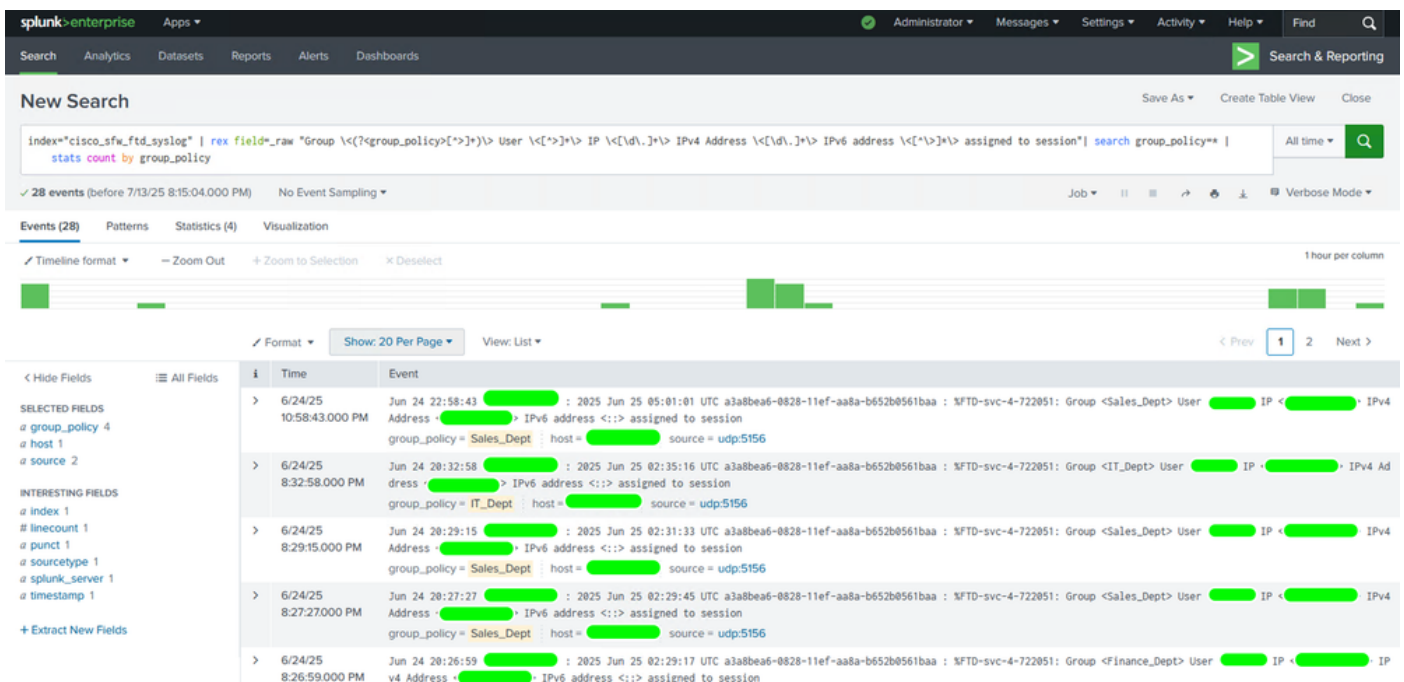
تامول عمل ااحول عاشن او SPL تامال عتسا ذي فنت

Splunk لى ل ريراقت ال دادع او شحب ال ق ي ب طت لى ل قنتا 1. ةوطخل

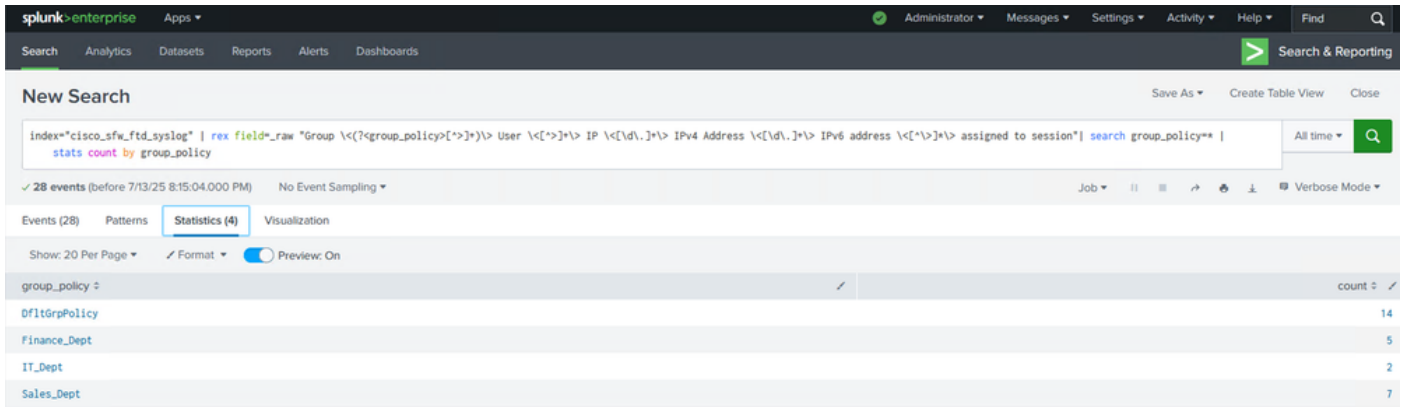


ري راق الت دادع او شح بل ق ي ب ط ت يل ل ق ت نا

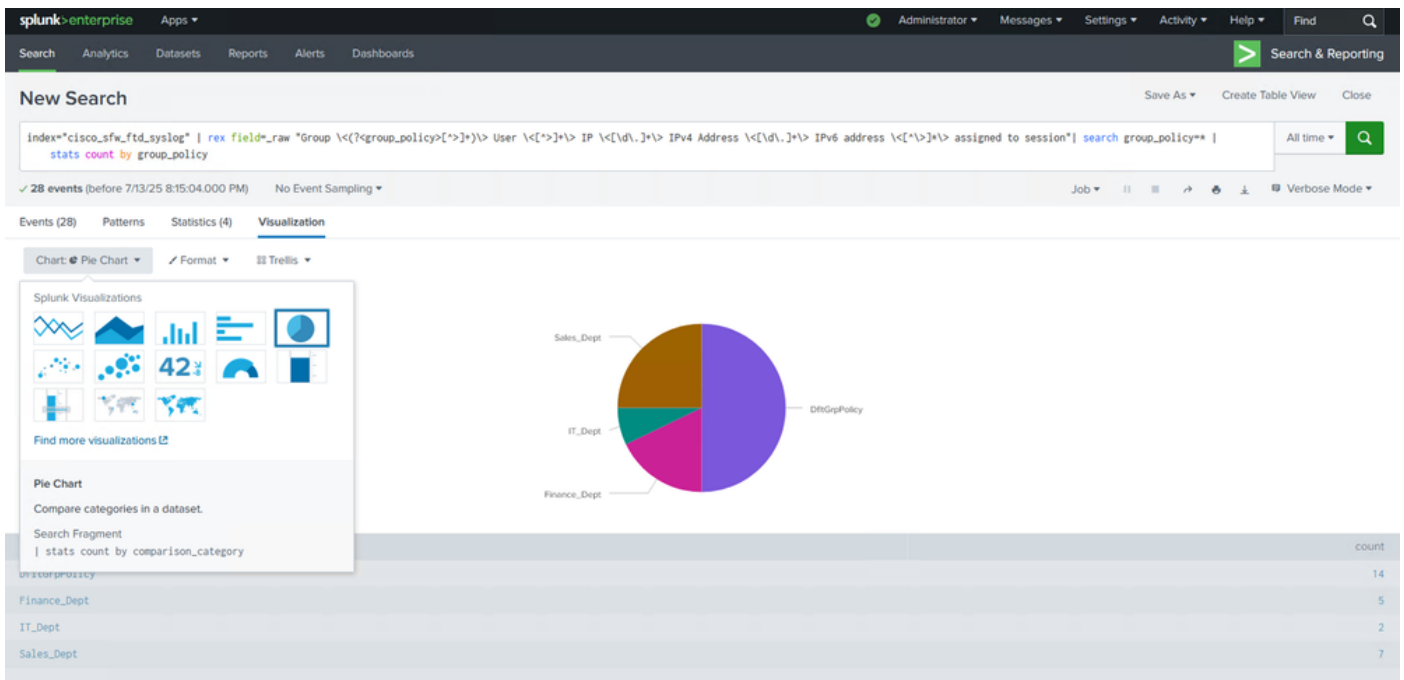
اهروصت ديرت ي ت ل ا ت ا ن ا ي ب ل ل ا ق ف و ه ذ ي ف ن ت و S P L م ا ل ع ت س ا ع غ ا ي ص ب م ق 2 . ق و ط خ ل ، ث ا د ح ا ل ا ب ي و ب ت ل ا م ا ل ع ن م ض (ل و ط م ل ا ع ض و ل ا ي ف) ل م ا ك ل ك ش ب ل ج س ل ك ا ي و ر ن م ن ك م ت ت س ا ي ئ ر م ت ا ن ا ي ب ل ا ه ذ ه ض ر ع و ت ا ي ا ص ا ح ا ب ي و ب ت ل ا م ا ل ع ي ف ع و م ج م ج ه ن ل ك ل ت ا ل ا ص ت ا ل ا د د ع و . ت ا ي ا ر م ل ا ب ي و ب ت ل ا م ا ل ع ن م ض ت ا ي ا ص ا ح ا ل ا ه ذ ه م ا د خ ت س ا ب .



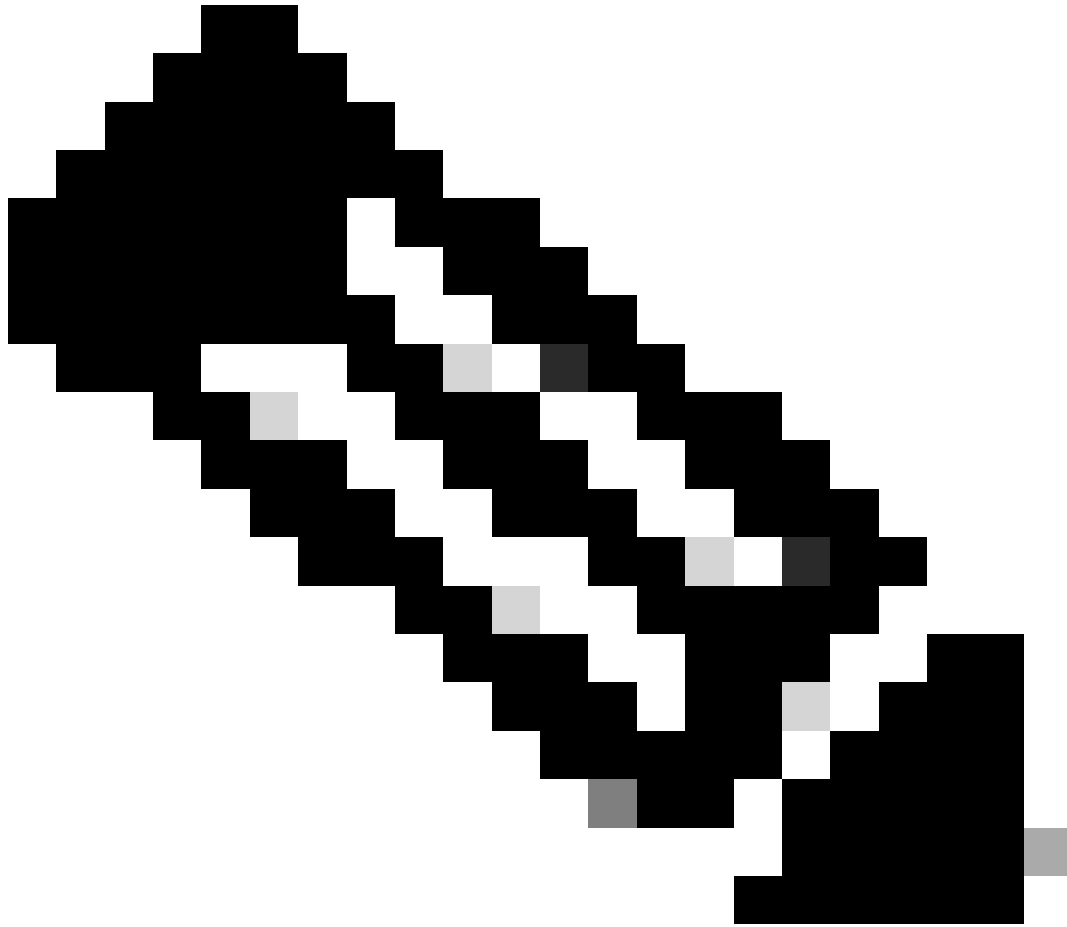
S P L م ا ل ع ت س ا م ا د خ ت س ا ب ث ا د ح ا ن ع ش ح ب ل ا



تايئاصخ ال بيوبتل ةمالع نم ققحت

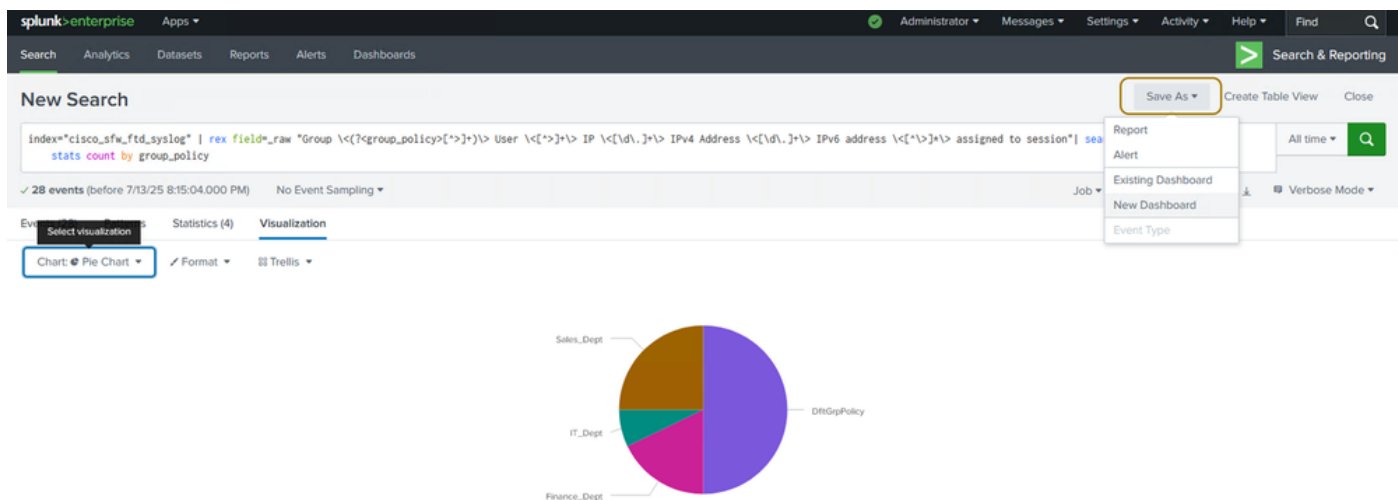


ططخمل/ينايبل مسرل تايئرمل بيوبتل ةمالع ضرعت فوس



نَع لوصول VPN تالاصتال تالجس بلجب مالعستالال موقى، لاثملا اذه يف: عطحالم
ددع ضرعل يرئاد ططخم مادختسا مت. عفلتخم عومجم جهن ربع عجانلا دعب
كتاداريتسا ىلع اءانب. عومجم جهن لكل عيؤئملا اهتبسنو عجانلا تالاصتال
مسرلا لثم تايرملا نم فلتخم عون مادختسا رايتخا كنكمي، كتاليفضتو
كلذك يطيرشلل ينابل.

كيدل تناك اذا امل اقفو دوجوم وأ عديج تامولعم عحول رتخاو مساب ظفح قوف رقنا 3. عوطخلا
هذه ضرعت. عديج تامولعم عحول عاشنا ديرت وأ اهلا عحولل هذه عفاضلا ديرت تامولعم عحول
عريخالا علثملا.



تامولعم ةحول في ةحولل ظفح

يتل ةحولل اناونع لخدأوا هئاشنإب موقت يتل تامولعم ةحولل اناونع ددح. 4 ةوطخل
يرئادل ططخم الما لعل يوتحتس.

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

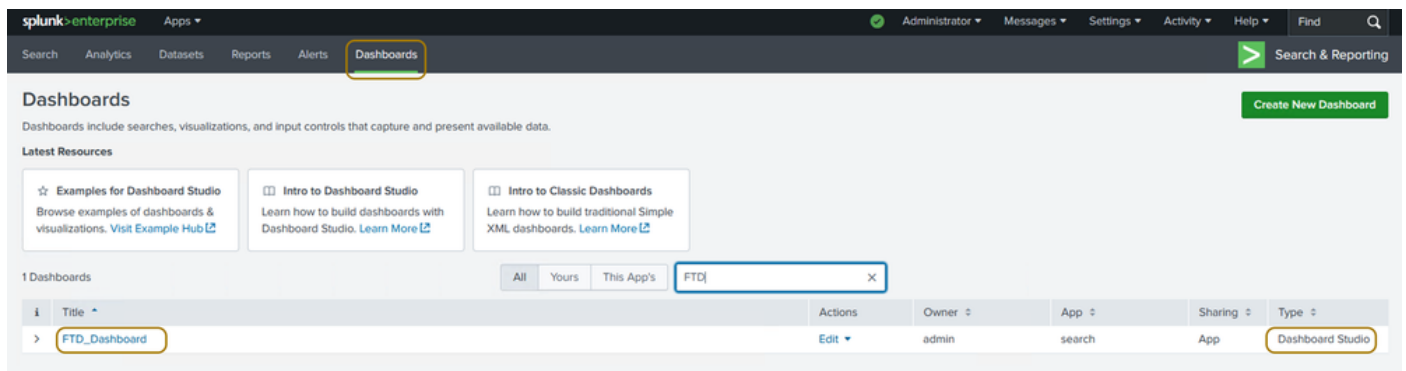
Cancel

Save to Dashboard

حامسلا مأ طقف تامولعمل ةحول ضرع ضرتمفملا نم ناك اذا ام ىلع ءانب ىلع ةوالع .اضىأ Splunk لىثم ىلإ لوصول قح مهيدل نيذل نيخآلا ني مدختسملل ةحولل تادادعإ يف تايوتسملا ددعتم مكحتل ديرت تنك اذا ام ىلع ءانب ،كلذل ةحول عاشنإل Dashboard Studio وأ Classic عضول رتخأ ،ال مأ تامولعمل ةحول طيختو كـب ةصاخلا تامولعمل

ةحول ىلإ تاحولك اهظفحو SPL تامالعتسا نم ديزملا ذيفنتب مق .(ةيرايخا) 5 ةوطخل ةروكذمل ةقباسلا تاوطخل مادختساب كاتابلطتملاقفو هذه تامولعمل

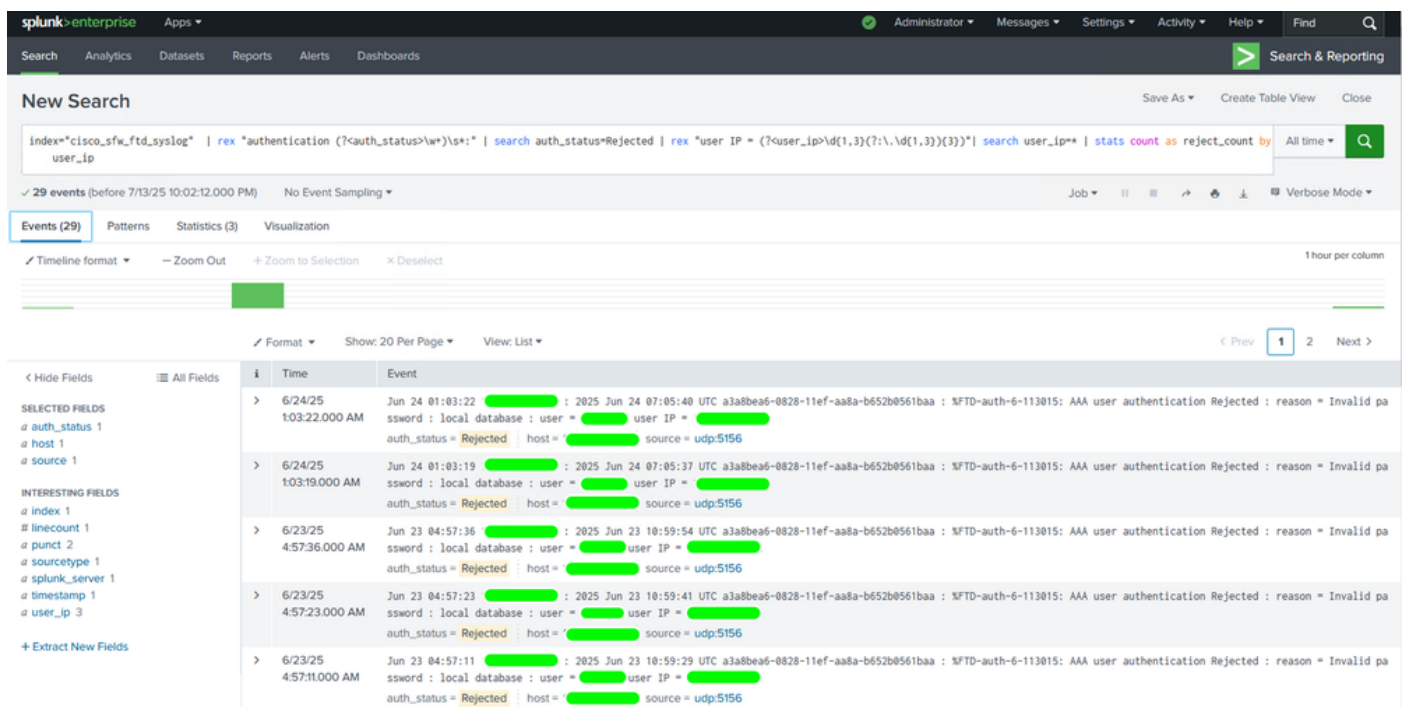
تمق يتلا تامولعمل ةحول يف شحبلل تامولعمل ةحول بيوبتلل ةمالع ىلإ لقتنا . 6 ةوطخل هتاحول بيترت ةداعإ وأ ،ريرت ،ضرعل هرقنا .ةحولل هذه رايخاو اهئاشنإب



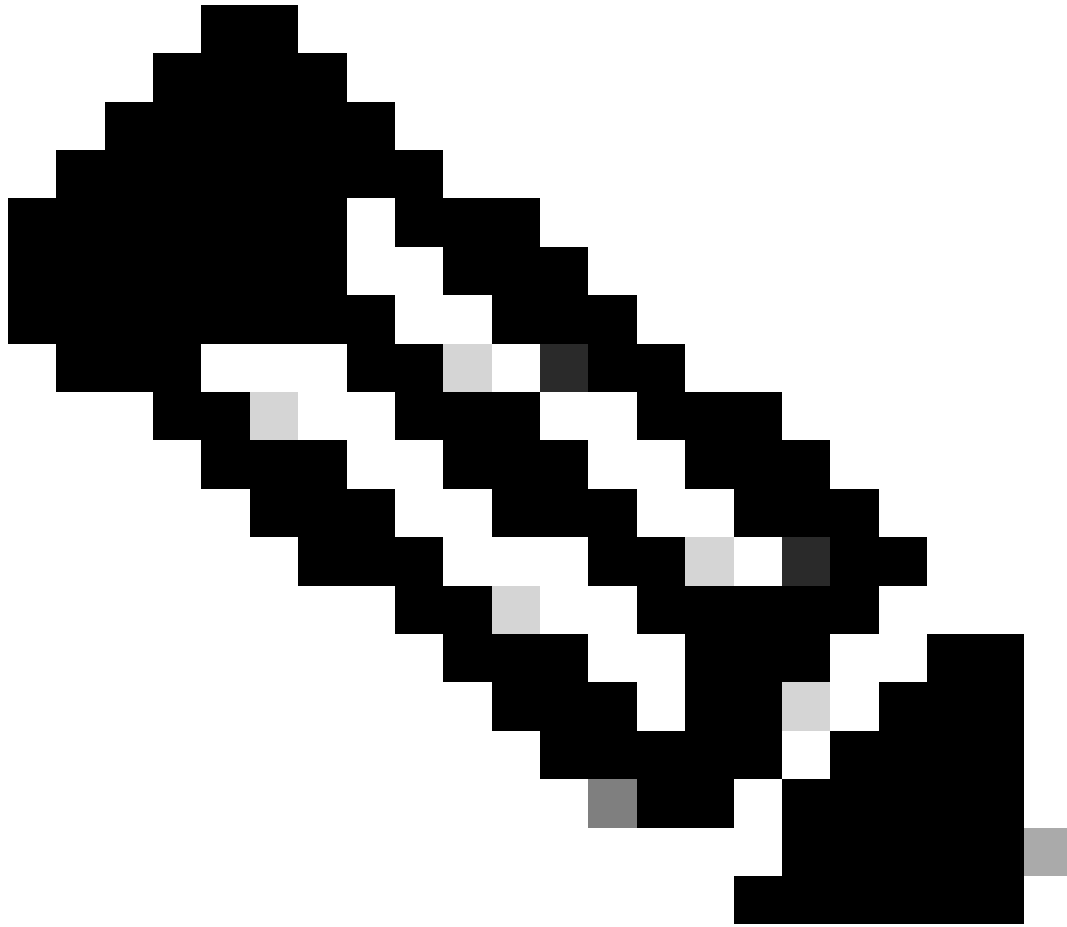
تامولعمل ةحول ضرع ةيفيك

SPL تامالعتسا ىلإ ادانتسا تاهيبنتل نيوكت

هليغشتو SPL مالعستسا عاشنإل ريراقتل دادعإو شحبلل قيبطت ىلإ لقتنا . 1 ةوطخل هـيبنتل ليغشتل اهمادختسا متيس يتلا ةحيحصلا تالجسل بلجي هنأ نم ققحتلل



ةصاخ تاهيبنتل عاشنإل SPL تامالعتسا ليغشت



ةلشافلا ةقداصملا تالچس بلجل مالعتسالا مادختسا متي، لاثملا اذه يف :ةظحالم
ددع زواجتي ام دنع تاهي بننتلا ليغشتل دعب نع لوصولاب ةصاخلا VPN ةكبشل
ةنعم ةينمز ةرتف لالخال اني عم ادح ةلشافلا تالواحملا

هيبنت رتخاو مساب ظفح قوف رقنا 3. ةوطخل



هيبنتلا ظفح

رخأل تادشرملاو ليصافتلا ةفاك ةئبعتب مق .هيبنتلا ةيمستل اناونع ددح 4. ةوطخل
هيبنتلا اذهل ةمدختسملا تادادعالا ركذ مت .ظفح قوف رقناو هيبنتلا نيوكتل ةبولطملا
انه

<#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 ▼	
	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.	
	e.g. "search count > 10"	
in		
Trigger		
Throttle ?	☐	
Trigger Actions	+ Add Actions ▼	

Save

هېښننه لاس ته راځي کله چې د تاداد د

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 ?	☐	

Trigger Actions

+ Add Actions ▾

When triggered

▼

 Add to Triggered Alerts

Remove

Severity

Medium ▾

Info

Low

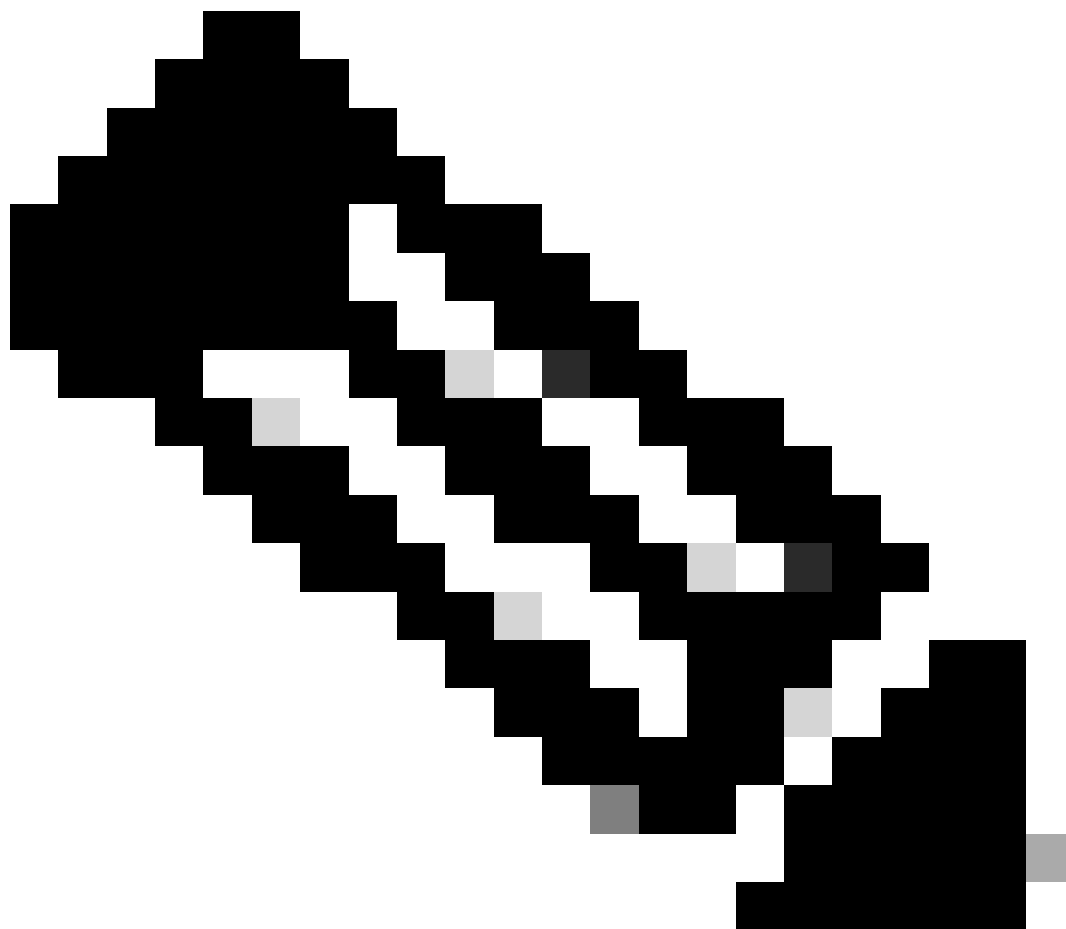
✓ Medium

High

Critical

Cancel

Save



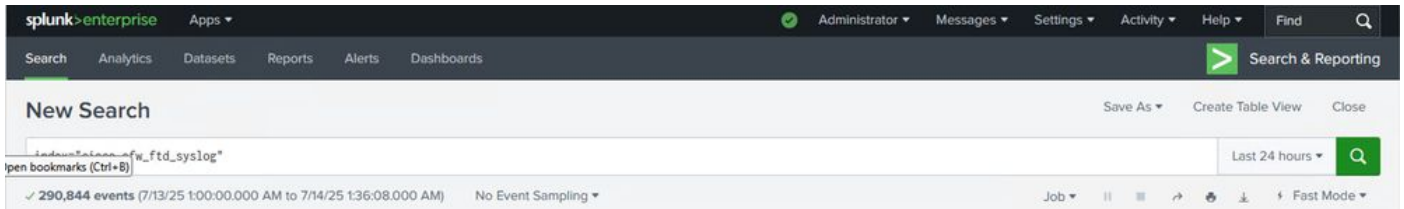
تادادع| ديدحت كئيلع بجي ف ،ةجيتن ن لك ل تاهيبننتل لايغشت ديرت تنك اذا :ةطحال ماضيأ كلذل اق فو مكحتل

ةحصلال نم ققحتل

تانايبال قفدتو تانايبوكتل نم ققحتل كنكمي ،تاهيبننتل او تانايبال تاحول عاشن| درجمب اذه ي ف دراول تاميلعتل مادختساب يلعلقو لاقول ي ف تاهيبننتل او تامولعمل تاحولو م سقل

تالچسل ضرع

رادج ةطساوب اهل اسرا مت ي تال تالچسل تناك اذا ام ديكأتل ثحبال قيبطت مادختسا كنكمي نكمي .ةلتكل نم ري بك عج ثحب سار يلع ةيؤرلل اهتيلباقو اهيقلت مت دق ةيامحال = ثحبال سرهف) ةسرهفم تالچسل ثدحأ نم ققحتل لال خ نم عارجال اذه نم ققحتل هب طبترم لاقول عباطو ("cisco_sfw_ftd_syslog")



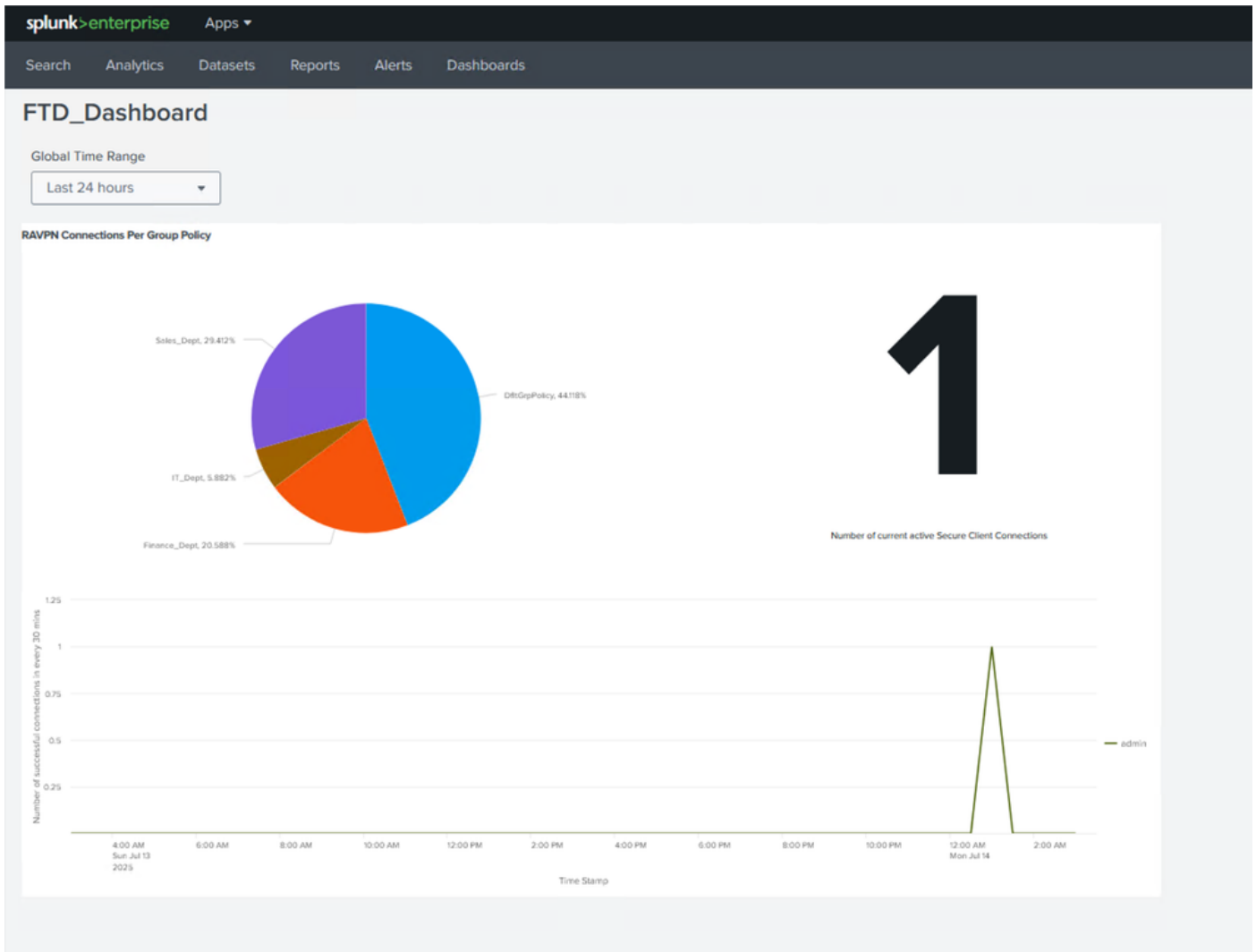
اهضرعو تالچسلا صحف

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

اهضرعو تالچسلا صحف

يلعفل تقولا في تامولعمل تاحول ضرع

يلع ريغتلا ةيؤرو اهئاشناب تمق ي لتلا ةصصخملا تامولعمل ةحول ىلا ل لاق تنالا كنكمي FTD. نم اهؤاشن م تي ةديج تالچسو تانايبك تاحوللا نم لك



تامولعمل تاحول ضرع

تاهايبن ت ةيأ ليغشت نم ققحتلا

ع طقم ال شح ب تاي لمع ى ل لاق تنال ك نكمي ، تاهي بنتل لوح تامول عم لم نم ق قحتل
ثح أال ضرع قوف رقا . ةري أال هيبنتل تامول عم ىل ع ال طالل تاهي بنتل وري راق تل و
شحب ال تاي لمعو ماهم لم نم رثك أ قحتل

splunk>enterprise Apps								
Searches, Reports, and Alerts								
Searches, reports, and alerts are saved searches created from pivot or the search page. Learn more								
2 Searches, Reports, and Alerts Type: All App: 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		

اهضرعو تاهي بنتل نم ق قحتل

splunk>enterprise

Apps

Administrator

Messages

Settings

Activity

Help

Find

Jobs

Manage your jobs. [Learn More](#)

68 Jobs

App: Search & Reporting (search)

Owner: All

Status: All

label="Alert to notify more than 10 failed attempts in 10 minutes" X

10 Per Page

Edit Selected

< Prev

1

2

3

4

5

6

7

Next >

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

Alert to notify more than 10 failed attempts in 10 minutes

[real-time]

اهضرعو تاهي بنتل نم ق قحتل

splunk>enterprise Apps										
Search Analytics Datasets Reports Alerts Dashboards										
Search > Search & Reporting										
Alert to notify more than 10 failed attempts in 10 minutes Save Save As View Create Table View Close										
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 Real-time										
26 of 33,995 events matched No Event Sampling Job II Stop Refresh Download Fast Mode										
Events Patterns Statistics (1) Visualization										
Show: 20 Per Page Format										
user_ip reject_count										
15										

هلي غشت مت يذل هيبنتل تاي اصالح ال نم ق قحتل

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا