

Erstellen benutzerdefinierter Dashboards und Warnungen für Splunk mithilfe von Syslogs aus FTD

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Syslog-Einstellungen für FTD konfigurieren](#)

[Konfigurieren einer Dateneingabe in der Splunk-Enterprise-Instanz](#)

[SPL-Abfragen ausführen und Dashboards erstellen](#)

[Warnmeldungen auf Basis von SPL-Abfragen konfigurieren](#)

[Überprüfung](#)

[Protokolle anzeigen](#)

[Anzeigen der Echtzeit-Dashboards](#)

[Prüfen, ob Warnungen ausgelöst wurden](#)

Einleitung

Dieses Dokument beschreibt eine schrittweise Anleitung für die Konfiguration von FTD zum Senden von Syslogs an Splunk und die Verwendung dieser Protokolle zum Erstellen benutzerdefinierter Dashboards und Warnungen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, vor dem Durchgehen des Konfigurationsleitfadens Kenntnis von diesen Themen zu haben:

- Syslog
- Grundkenntnisse der Suchprozesssprache (SPL) von Splunk

In diesem Dokument wird außerdem davon ausgegangen, dass Sie bereits eine Splunk Enterprise-Instanz auf einem Server installiert haben und auf die Webschnittstelle zugreifen können.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Firepower Threat Defense (FTD) mit Version 7.2.4
- Cisco FirePOWER Management Center (FMC) mit Version 7.2.4
- Splunk Enterprise-Instanz (Version 9.4.3), die auf einem Windows-Computer ausgeführt wird

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration.

Hintergrundinformationen

Cisco FTD-Geräte generieren detaillierte Syslogs zu Zugriffsversuchen, Zugriffskontrollrichtlinien und Verbindungsereignissen. Die Integration dieser Protokolle mit Splunk ermöglicht leistungsstarke Analysen und Echtzeitwarnungen für Netzwerksicherheitsvorgänge.

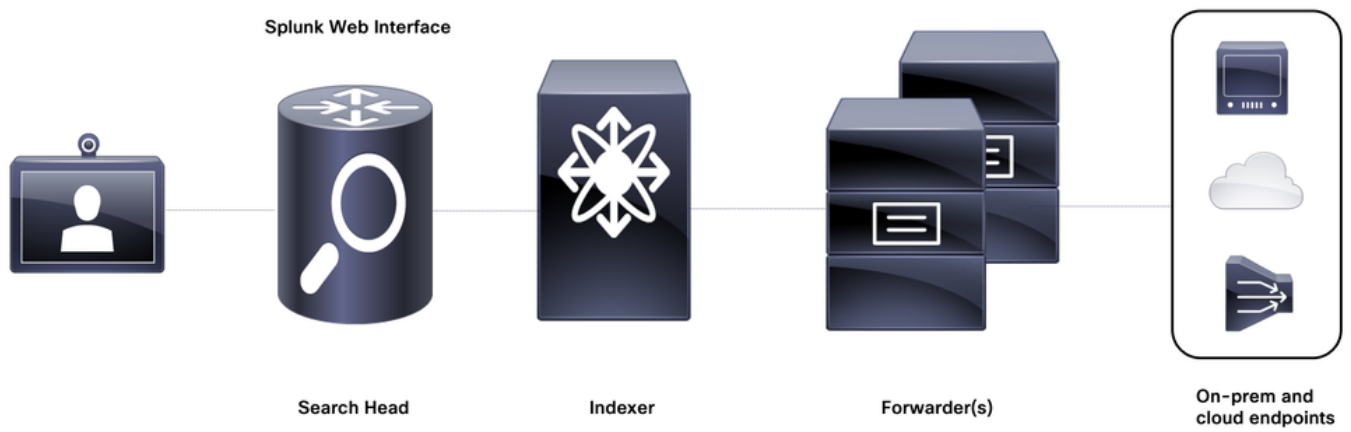
Splunk ist eine Echtzeit-Datenanalyseplattform, die entwickelt wurde, um maschinengenerierte Daten zu erfassen, zu indizieren, zu durchsuchen und zu visualisieren. Splunk ist besonders effektiv in Cybersicherheitsumgebungen als ein Security Information and Event Management (SIEM) Tool aufgrund seiner Fähigkeit,:

- Aufnahme von Protokolldaten skaliert
- Komplexe Suchvorgänge mit SPL durchführen
- Erstellen von Dashboards und Warnungen
- Integration mit Sicherheits-Orchestrierungs- und Reaktionssystemen

Splunk verarbeitet Daten über eine strukturierte Pipeline, um unstrukturierte oder halbstrukturierte Maschinendaten nützlich und umsetzbar zu machen. Die wichtigsten Phasen dieser Pipeline werden häufig als IPIS bezeichnet, das für Folgendes steht:

- Eingabe
- Parsing
- Indizierung
- Suche

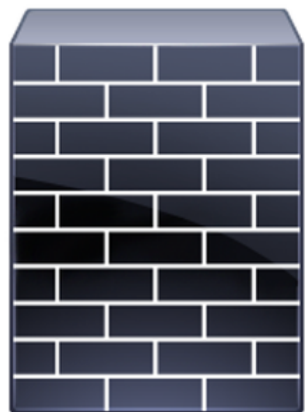
Das folgende Diagramm zeigt die wichtigsten Komponenten der zugrunde liegenden Architektur, die zur Realisierung der IPIS-Pipeline verwendet werden:



Splunk-Basisarchitektur

Konfigurieren

Netzwerkdiagramm



**Firepower Threat
Defense device**



**Syslog server with the
Splunk Search Head**

Netzwerkdiagramm



Anmerkung: Für die Laborumgebung für dieses Dokument sind keine separaten Forwarder- und Indexerinstanzen erforderlich. Der Windows-Computer, d. h. der Syslog-Server, auf dem die Splunk Enterprise-Instanz installiert ist, fungiert als Indexer und Suchkopf.

Konfigurationen

Syslog-Einstellungen für FTD konfigurieren

Schritt 1: Konfigurieren Sie die vorläufigen Syslog-Einstellungen auf dem FMC für das FTD unter Geräte > Plattformeinstellungen, um die Protokolle an den Syslog-Server zu senden, auf dem die Splunk-Instanz ausgeführt wird.

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

Plattformeinstellungen auf FTD - Syslog

Schritt 2: Konfigurieren Sie die IP-Adresse des Computers, auf dem die Splunk Enterprise-Instanz installiert ist und als Syslog-Server ausgeführt wird. Definieren Sie die Felder wie erwähnt.

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	

Plattformeinstellungen auf FTD - Syslog-Server hinzugefügt

Schritt 3: Fügen Sie ein Protokollierungsziel für Syslog-Server hinzu. Die Protokollierungsebene kann entsprechend Ihrer Auswahl oder Ihrem Anwendungsfall festgelegt werden.

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			

Plattformeinstellungen auf FTD - Protokollziel hinzufügen

Add Logging Filter

Logging Destination

Syslog Servers

Event Class

Filter on Severity

debugging

+ Add

Event Class	Syslog Severity	
No records to display		

Cancel

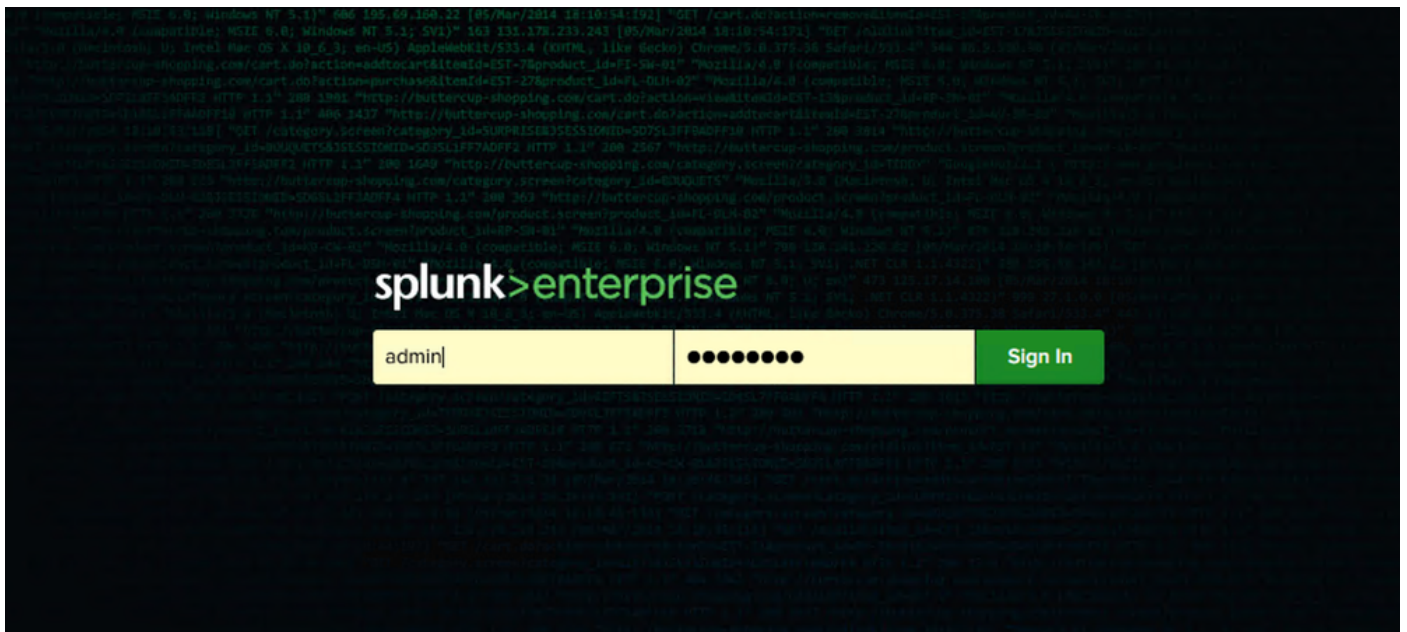
OK

Plattformeinstellungen auf FTD - Schweregrad für Protokollierungsziel festlegen

Stellen Sie die Änderungen der Plattformeinstellungen nach Abschluss dieser Schritte auf dem FTD bereit.

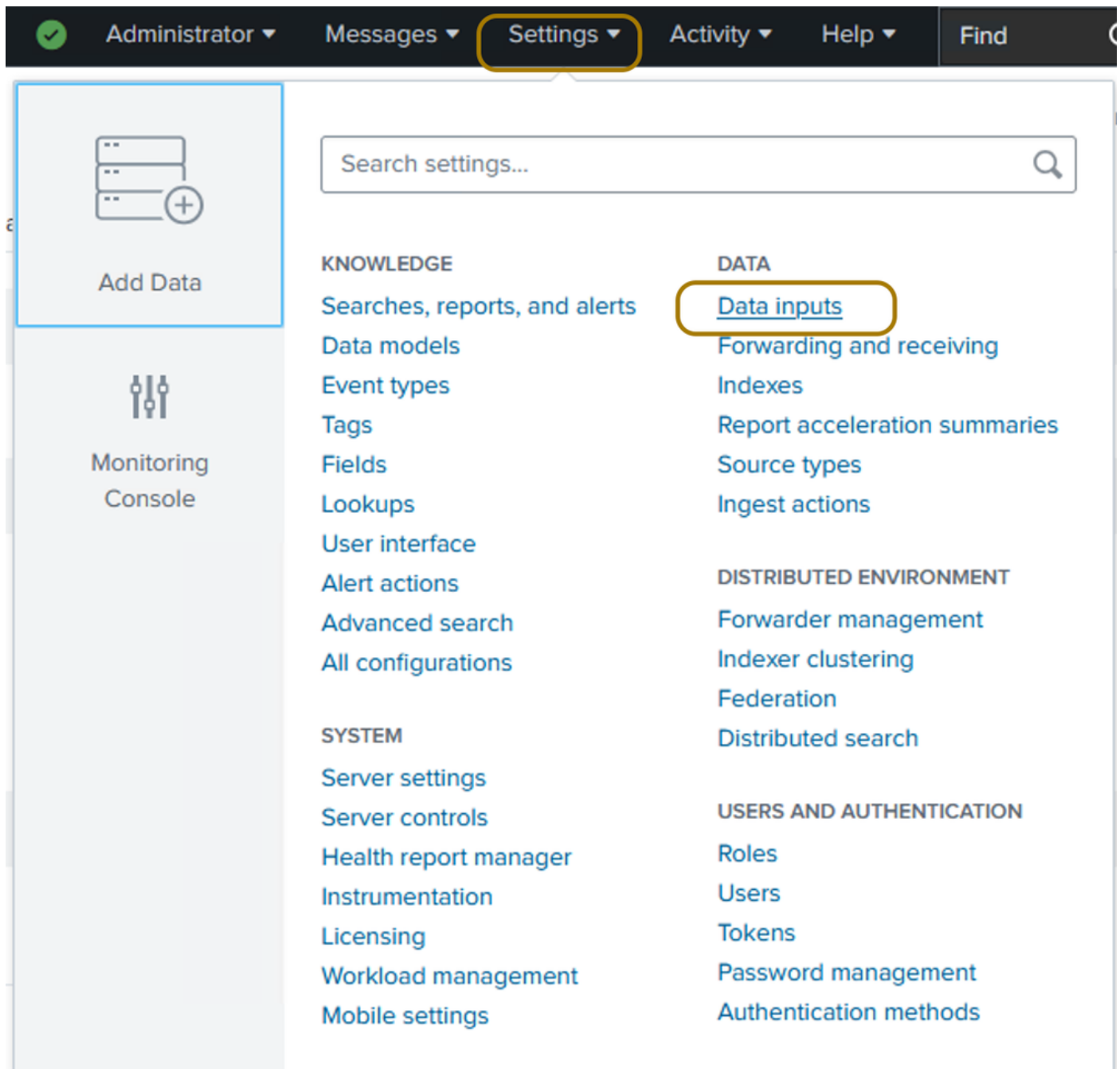
Konfigurieren einer Dateneingabe in der Splunk-Enterprise-Instanz

Schritt 1: Melden Sie sich bei der Webschnittstelle Ihrer Splunk Enterprise-Instanz an.



Splunk-Webschnittstelle - Anmeldeseite

Schritt 2: Definieren Sie eine Dateneingabe, damit Sie die Syslogs auf Splunk speichern und indizieren können. Navigieren Sie nach der Anmeldung zu Einstellungen > Daten > Dateneingaben.



Navigieren zu Dateneingaben auf Splunk

Schritt 3. Wählen Sie UDP und klicken Sie auf der nächsten Seite auf New Local UDP.

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

Klicken Sie auf "UDP" für eine UDP-Dateneingabe.

splunkenterprise

Apps

Administrator

Messages

Settings

Activity

Help

Find

UDP

Data inputs > UDP

filter

25 per page

New Local UDP

Neue lokale UDP-Eingabe erstellen

Schritt 4: Geben Sie den Port ein, an den die Syslogs gesendet werden. Dieser muss mit dem in den FTD-Syslog-Einstellungen konfigurierten Port übereinstimmen, in diesem Fall mit dem Port 5156. Um die Syslogs nur von einer Quelle (dem FTD) zu akzeptieren, setzen Sie das Feld Nur Verbindung akzeptieren von auf die IP-Adresse der Schnittstelle auf dem FTD, die mit dem Splunk-Server kommuniziert. Klicken Sie auf Next (Weiter).

splunkenterprise

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?

Port- und FTD-IP-Adresse angeben

Schritt 5: Sie können den Quelltyp und die Indexfeldwerte aus den vordefinierten Werten auf Splunk suchen und auswählen, wie im nächsten Bild hervorgehoben. Die Standardeinstellungen können für die übrigen Felder verwendet werden.

Einstellungen für die Dateneingabe konfigurieren

Schritt 6: Überprüfen Sie die Einstellungen, und klicken Sie auf Senden.

Einstellungen zur Dateneingabe überprüfen

SPL-Abfragen ausführen und Dashboards erstellen

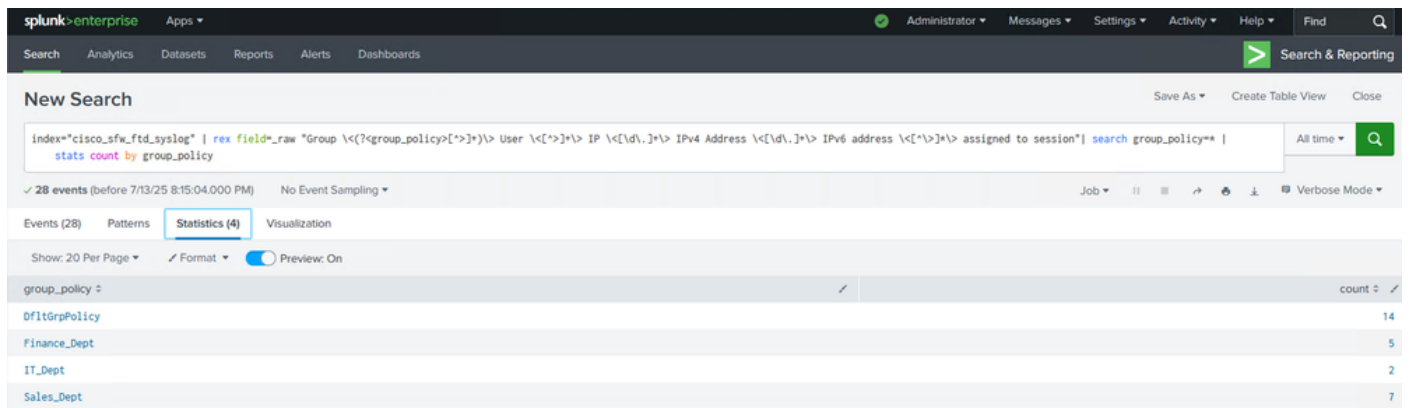
Schritt 1: Navigieren Sie zur App "Search and Reporting on Splunk".

Navigieren Sie zur App "Suchen und Reporting".

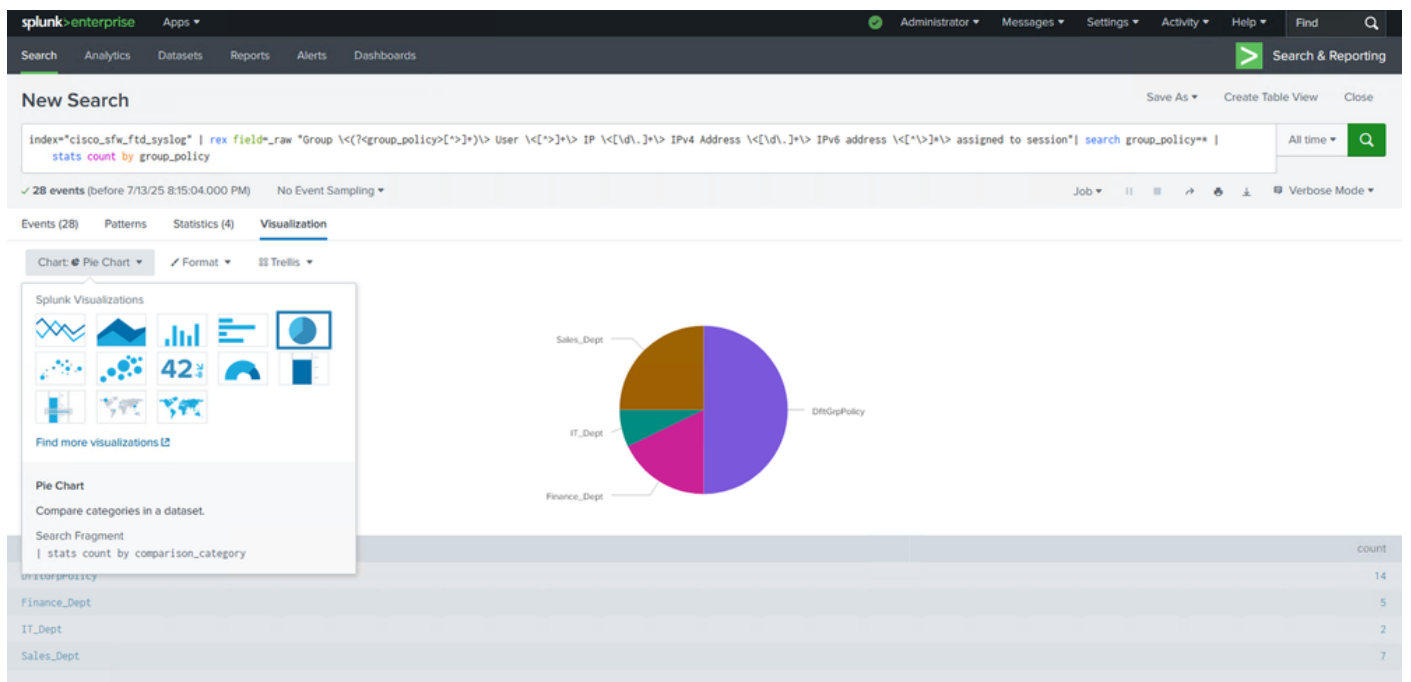
Schritt 2. Formulieren und führen Sie eine SPL-Abfrage entsprechend den Daten aus, die Sie visualisieren möchten. Sie können jedes Protokoll vollständig (im ausführlichen Modus) unter der Registerkarte Ereignisse sehen, die Anzahl der Verbindungen pro Gruppenrichtlinie in der Registerkarte Statistik und diese Daten mit diesen Statistiken unter der Registerkarte Visualisierung visualisieren.

Time	Event
6/24/25 10:58:43.000 PM	Jun 24 22:58:43 : 2025 Jun 25 05:01:01 UTC a3a8bea6-8828-11ef-aa8a-b652b0561baa : XFTD-svc-4-722051: Group <Sales_Dept> User : IP : IPv4 Address : IPv6 address <::> assigned to session group_policy = Sales_Dept : host = : source = udp:5156
6/24/25 8:32:58.000 PM	Jun 24 20:32:58 : 2025 Jun 25 02:35:16 UTC a3a8bea6-8828-11ef-aa8a-b652b0561baa : XFTD-svc-4-722051: Group <IT_Dept> User : IP : IPv4 Address : IPv6 address <::> assigned to session group_policy = IT_Dept : host = : source = udp:5156
6/24/25 8:29:15.000 PM	Jun 24 20:29:15 : 2025 Jun 25 02:31:33 UTC a3a8bea6-8828-11ef-aa8a-b652b0561baa : XFTD-svc-4-722051: Group <Sales_Dept> User : IP : IPv4 Address : IPv6 address <::> assigned to session group_policy = Sales_Dept : host = : source = udp:5156
6/24/25 8:27:27.000 PM	Jun 24 20:27:27 : 2025 Jun 25 02:29:45 UTC a3a8bea6-8828-11ef-aa8a-b652b0561baa : XFTD-svc-4-722051: Group <Sales_Dept> User : IP : IPv4 Address : IPv6 address <::> assigned to session group_policy = Sales_Dept : host = : source = udp:5156
6/24/25 8:26:59.000 PM	Jun 24 20:26:59 : 2025 Jun 25 02:29:17 UTC a3a8bea6-8828-11ef-aa8a-b652b0561baa : XFTD-svc-4-722051: Group <Finance_Dept> User : IP : IPv4 Address : IPv6 address <::> assigned to session

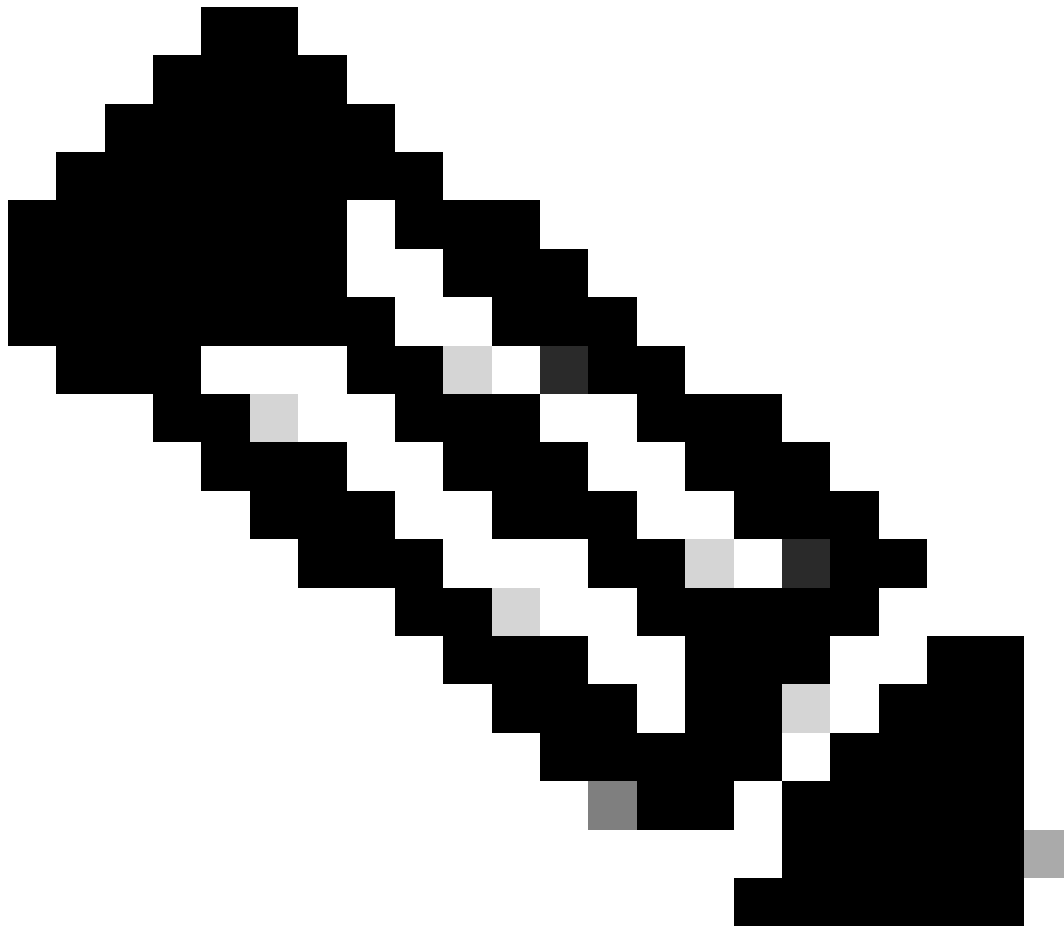
Suchen nach Ereignissen mithilfe von SPL-Abfragen



Registerkarte "Statistik" überprüfen

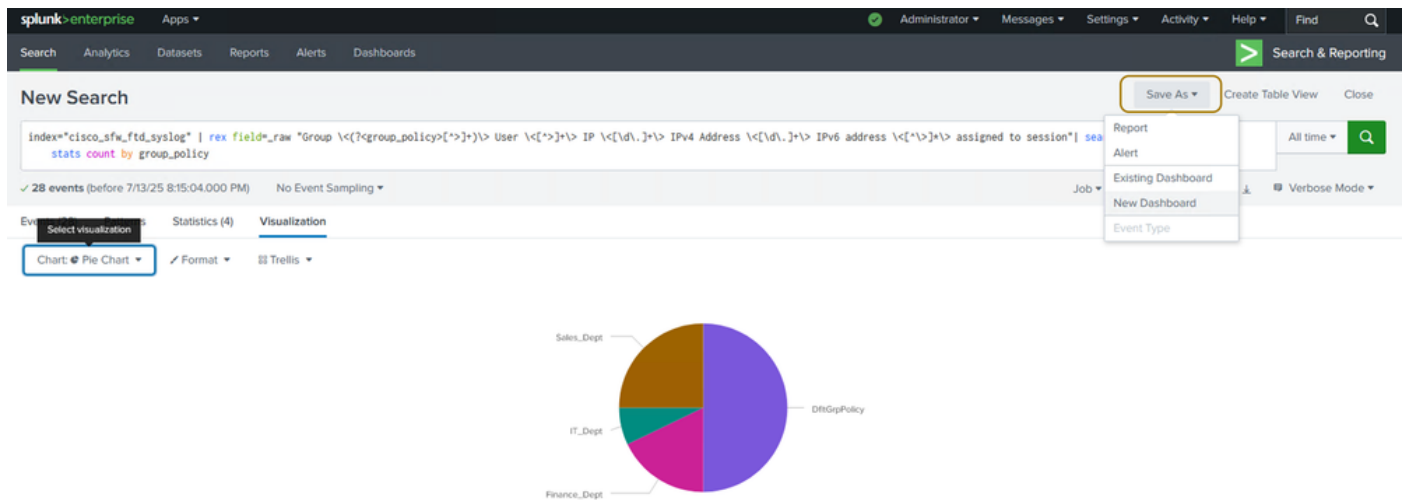


Auf der Registerkarte Visualisierung wird das Diagramm angezeigt.



Anmerkung: In diesem Beispiel werden durch die Abfrage Protokolle für erfolgreiche Remotezugriff-VPN-Verbindungen über verschiedene Gruppenrichtlinien abgerufen. Ein Tortendiagramm wurde verwendet, um die Anzahl und den Prozentsatz erfolgreicher Verbindungen pro Gruppenrichtlinie darzustellen. Je nach Ihren Anforderungen und Vorlieben können Sie auch eine andere Art der Visualisierung verwenden, z. B. einen Balkendiagramm.

Schritt 3. Klicken Sie auf Speichern unter und wählen Sie Neu oder Bestehendes Dashboard, je nachdem, ob Sie bereits ein Dashboard haben, dem Sie diesen Bereich hinzufügen möchten, oder ob Sie ein neues erstellen möchten. In diesem Beispiel wird das letzte Dashboard veranschaulicht.



Speichern des Panels in einem Dashboard

Schritt 4: Geben Sie einen Titel für das Dashboard, das Sie erstellen, und geben Sie einen Titel für das Bedienfeld ein, das das Tortendiagramm enthält.

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

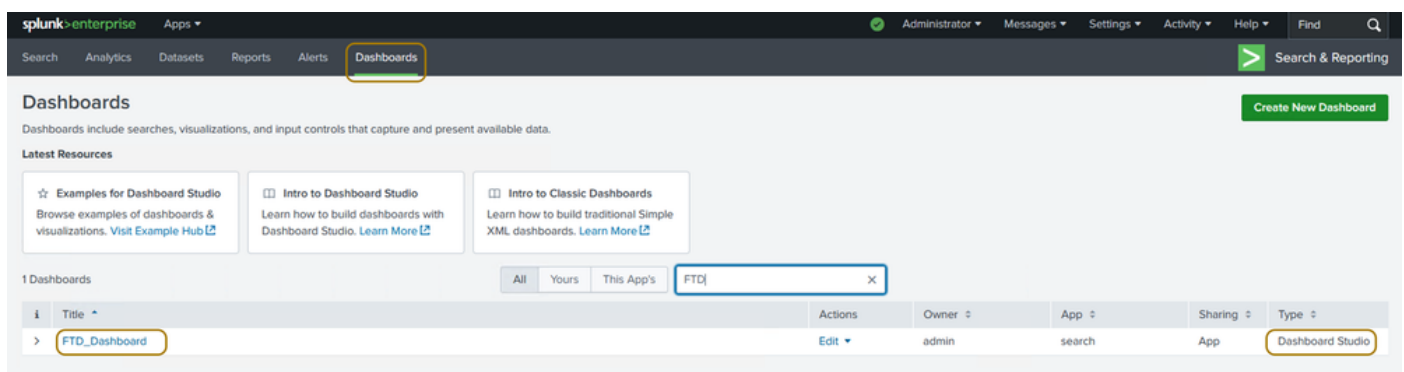
Cancel

Save to Dashboard

Sie können die Berechtigungen in App auf Privat oder Freigegeben festlegen, je nachdem, ob nur Sie das Dashboard anzeigen sollen oder andere Benutzer mit Zugriff auf die Splunk-Instanz ebenfalls zugelassen sind. Wählen Sie außerdem je nachdem, ob Sie eine präzise Kontrolle über die Panel-Einstellungen und das Layout des Dashboards wünschen oder nicht, den Modus Classic oder Dashboard Studio aus, um Ihr Dashboard zu erstellen.

Schritt 5 (optional). Führen Sie weitere SPL-Abfragen in diesem Dashboard als Bedienfelder aus, und speichern Sie sie entsprechend Ihren Anforderungen. Gehen Sie dazu wie zuvor beschrieben vor.

Schritt 6: Navigieren Sie zur Registerkarte Dashboard, um das erstellte Dashboard zu suchen und auszuwählen. Klicken Sie darauf, um die zugehörigen Bereiche anzuzeigen, zu bearbeiten oder neu anzuordnen.



Anzeigen des Dashboard

Warnmeldungen auf Basis von SPL-Abfragen konfigurieren

Schritt 1: Navigieren Sie zur Such- und Reporting-App, um Ihre SPL-Abfrage zu erstellen und auszuführen, damit sichergestellt ist, dass die richtigen Protokolle abgerufen werden, die zum Auslösen der Warnung verwendet werden.

splunk>enterprise

Apps

Administrator

Messages

Settings

Activity

Help

Find

Search

Analytics

Datasets

Reports

Alerts

Dashboards

Search & Reporting

New Search

Index="cisco_sfw_ftd_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

29 events (before 7/13/25 10:02:12.000 PM)

No Event Sampling

Job

Verbose Mode

Events (29)

Patterns

Statistics (3)

Visualization

Timeline format

Zoom Out

Zoom to Selection

Deselect

1 hour per column

Format

Show: 20 Per Page

View: List

Prev

1

2

Next

< Hide Fields

All Fields

SELECTED FIELDS

auth_status 1

host 1

source 1

INTERESTING FIELDS

index 1

punct 2

source_type 1

splunk_server 1

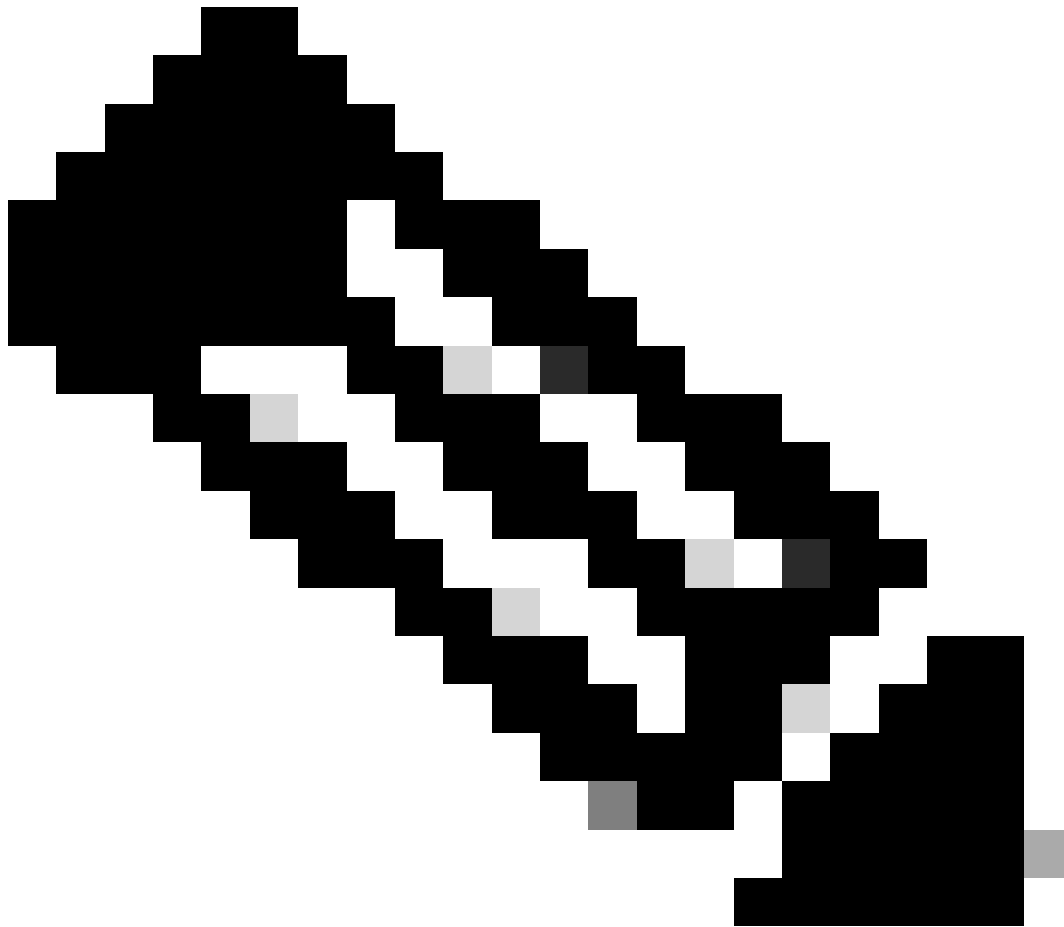
timestamp 1

user_ip 3

+ Extract New Fields

i	Time	Event
>	6/24/25 1:03:22.000 AM	Jun 24 01:03:22 : 2025 Jun 24 07:05:40 UTC a3a8bea6-0828-11ef-aa8a-b652b0561baa : %FTD-auth-6-113015: AAA user authentication Rejected : reason = Invalid password : local database : user = [REDACTED] user IP = [REDACTED] auth_status = Rejected host = [REDACTED] source = udp:5156
>	6/24/25 1:03:19.000 AM	Jun 24 01:03:19 : 2025 Jun 24 07:05:37 UTC a3a8bea6-0828-11ef-aa8a-b652b0561baa : %FTD-auth-6-113015: AAA user authentication Rejected : reason = Invalid password : local database : user = [REDACTED] user IP = [REDACTED] auth_status = Rejected host = [REDACTED] source = udp:5156
>	6/23/25 4:57:36.000 AM	Jun 23 04:57:36 : 2025 Jun 23 10:59:54 UTC a3a8bea6-0828-11ef-aa8a-b652b0561baa : %FTD-auth-6-113015: AAA user authentication Rejected : reason = Invalid password : local database : user = [REDACTED] user IP = [REDACTED] auth_status = Rejected host = [REDACTED] source = udp:5156
>	6/23/25 4:57:23.000 AM	Jun 23 04:57:23 : 2025 Jun 23 10:59:41 UTC a3a8bea6-0828-11ef-aa8a-b652b0561baa : %FTD-auth-6-113015: AAA user authentication Rejected : reason = Invalid password : local database : user = [REDACTED] user IP = [REDACTED] auth_status = Rejected host = [REDACTED] source = udp:5156
>	6/23/25 4:57:11.000 AM	Jun 23 04:57:11 : 2025 Jun 23 10:59:29 UTC a3a8bea6-0828-11ef-aa8a-b652b0561baa : %FTD-auth-6-113015: AAA user authentication Rejected : reason = Invalid password : local database : user = [REDACTED] user IP = [REDACTED] auth_status = Rejected host = [REDACTED] source = udp:5156

Ausführen von SPL-Abfragen zum Erstellen entsprechender Warnungen



Anmerkung: In diesem Beispiel wird die Abfrage verwendet, um fehlgeschlagene Authentifizierungsprotokolle für das Remotezugriffs-VPN abzurufen, um Warnungen auszulösen, wenn die Anzahl der fehlgeschlagenen Versuche innerhalb eines bestimmten Zeitraums einen bestimmten Schwellenwert überschreitet.

Schritt 3: Klicken Sie auf Speichern unter und wählen Sie Warnmeldung.



Warnmeldung speichern

Schritt 4: Geben Sie einen Titel für die Warnmeldung ein. Geben Sie alle weiteren Details und Parameter ein, die für die Konfiguration der Warnmeldung erforderlich sind, und klicken Sie auf

Speichern. Die für diese Warnung verwendeten Einstellungen wurden hier erwähnt.

<#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

Zusätzliche Einstellungen für die Warnungserstellung

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 ?	☐	

Zusätzliche Einstellungen für die Warnungserstellung

Trigger Actions

+ Add Actions ▾

When triggered

▼

 Add to Triggered Alerts

Remove

Severity

Medium ▾

Info

Low

✓ Medium

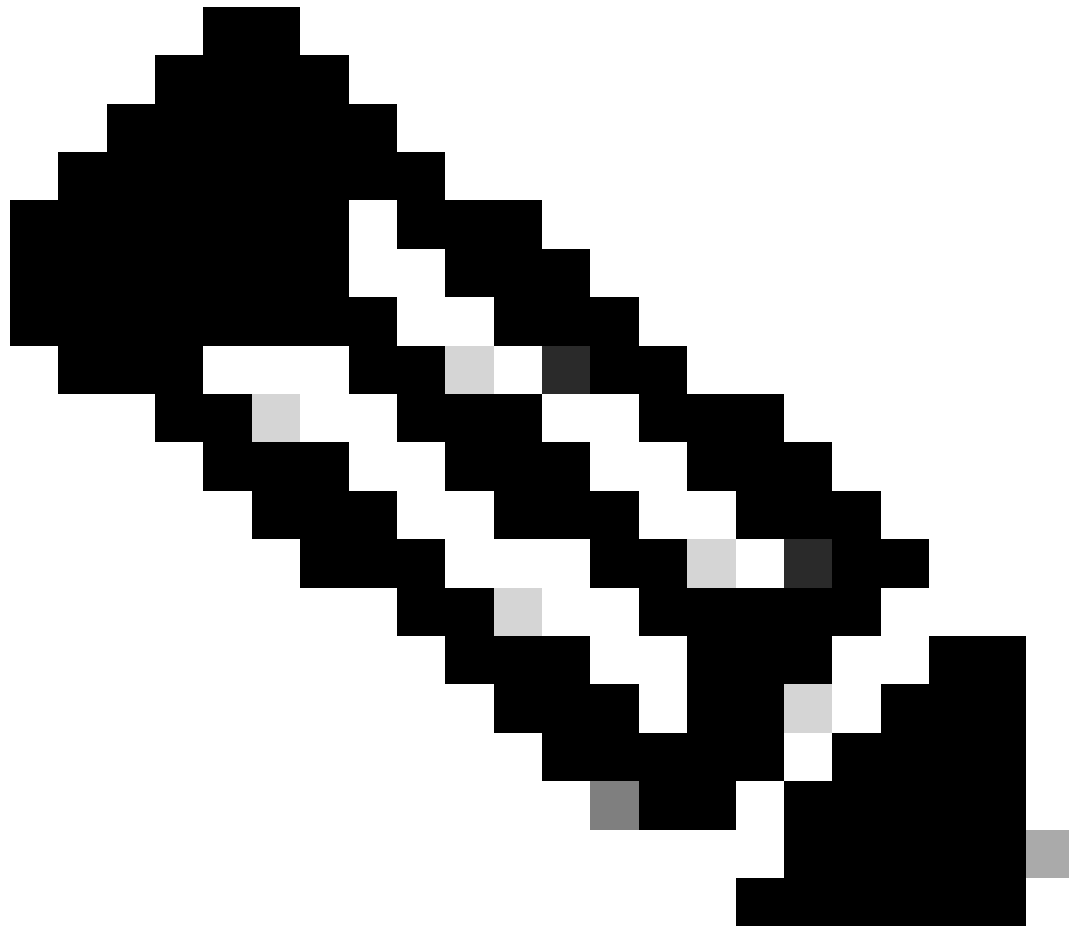
High

Critical

Cancel

Save

Zusätzliche Einstellungen für die Warnungserstellung



Anmerkung: Wenn Sie die Warnungen für jedes Ergebnis auslösen möchten, müssen Sie auch die Drosselungseinstellungen entsprechend definieren.

Überprüfung

Nachdem Sie die Dashboard- und Warnmeldungen erstellt haben, können Sie die Konfigurationen, den Datenfluss, die Dashboards und die Echtzeit-Warnmeldungen anhand der Anweisungen in diesem Abschnitt überprüfen.

Protokolle anzeigen

Mit der Such-App können Sie überprüfen, ob die von der Firewall gesendeten Protokolle empfangen und für den Splunk-Suchkopf sichtbar sind. Dies kann überprüft werden, indem die neuesten indizierten Protokolle (Suchindex = "cisco_sfw_ftd_syslog") und der zugehörige Zeitstempel überprüft werden.

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: main Index: w_ftd_syslog

Open bookmarks (Ctrl+B)

290,844 events (7/13/25 1:00:00.000 AM to 7/14/25 1:36:08.000 AM) No Event Sampling

Job Fast Mode

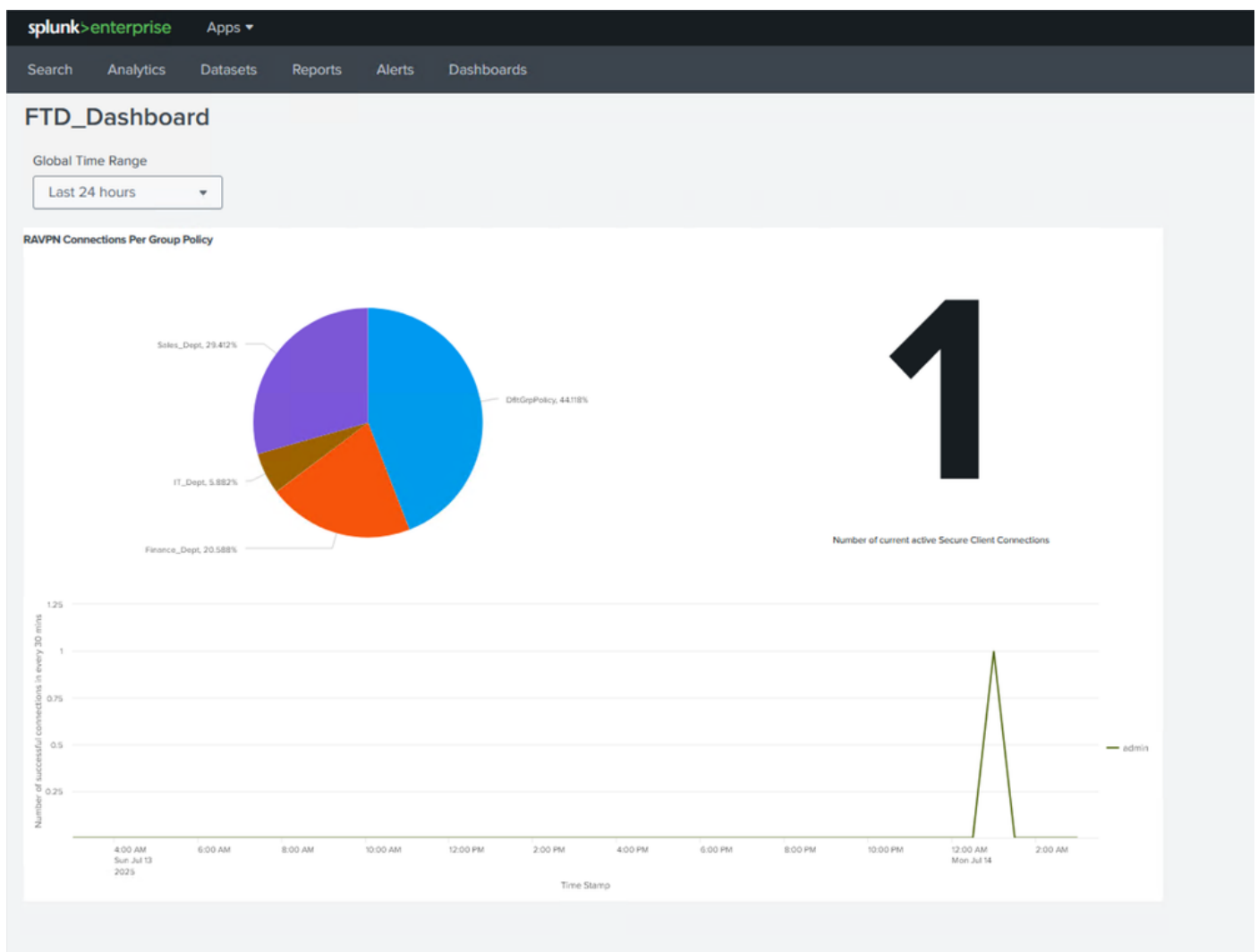
Protokolle überprüfen und anzeigen

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

Protokolle überprüfen und anzeigen

Anzeigen der Echtzeit-Dashboards

Sie können zum benutzerdefinierten Dashboard navigieren, das Sie erstellt haben, und die Änderungen in jedem der Bereiche anzeigen, wenn neue Daten und Protokolle aus dem FTD generiert werden.



Dashboards anzeigen

Prüfen, ob Warnungen ausgelöst wurden

Um die Informationen zu den Warnungen zu überprüfen, können Sie zum Abschnitt Suchen, Berichte und Warnungen navigieren, um die letzten Warnungsinformationen anzuzeigen. Klicken Sie auf Letzte anzeigen, um weitere Informationen zu den Jobs und Suchen zu erhalten.

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	EditRunView Recent	Alert	2025-07-14 01:24:00 Pacific Daylight Time	none	admin	search
Exceeding maximum number of failed alerts	EditRunView Recent	Alert	2025-07-14 01:24:00 Pacific Daylight Time	none	admin	search

Warnungen prüfen und anzeigen

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

< Prev1234567Next >

	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)	JobPauseStopRestartDownload

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

Warnungen prüfen und anzeigen

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

Real-time

26 of 33,995 events matchedNo Event Sampling

JobPauseStopRestartDownloadFast Mode

EventsPatternsStatistics (1)Visualization

Show: 20 Per PageFormat

user_ip	reject_count

15

Statistiken für ausgelöste Warnmeldungen überprüfen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.