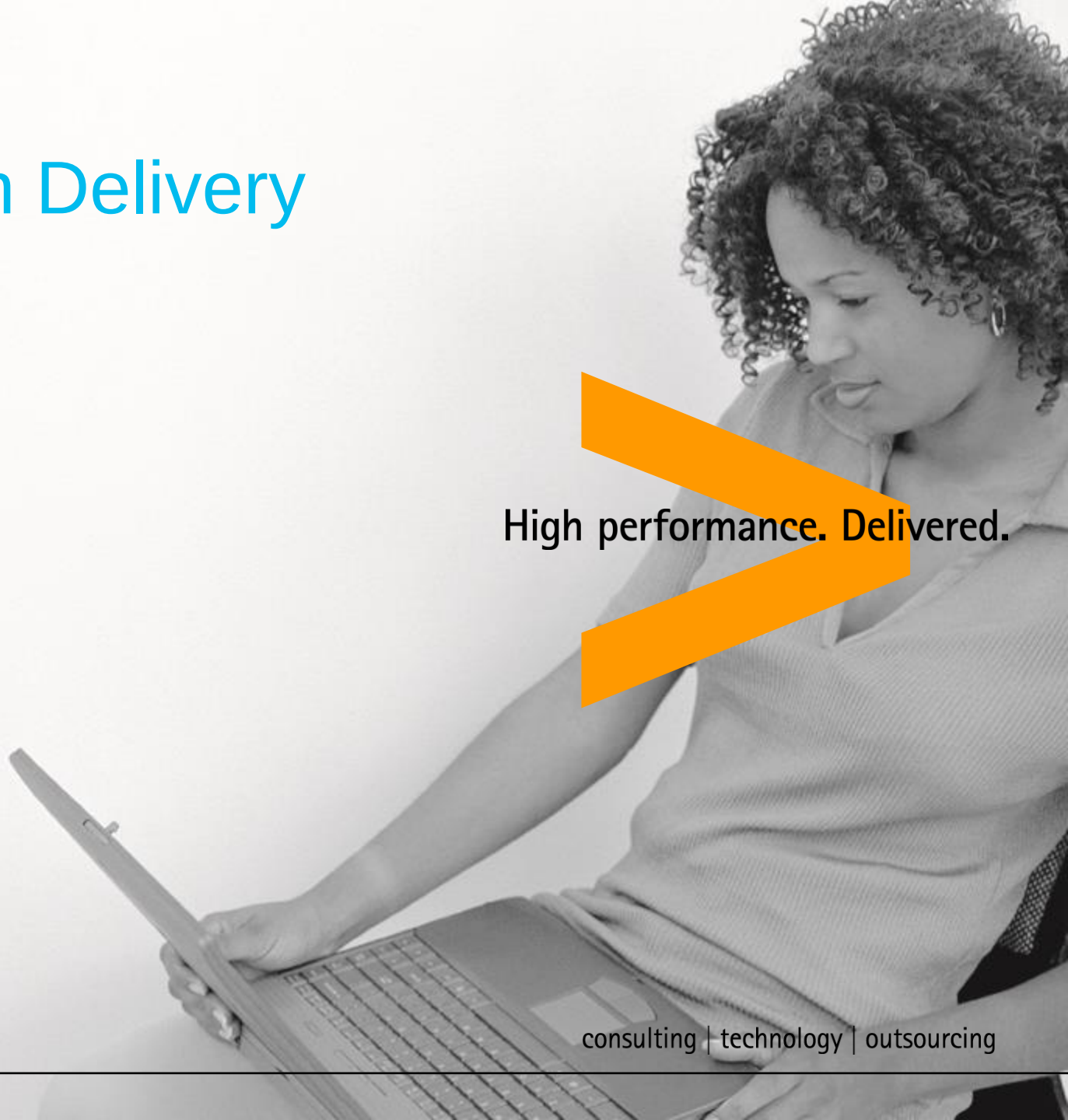
Application Delivery

Splunk



consulting | technology | outsourcing

Goals for Splunk

i. **Why Splunk?** – Problems With Log Data

ii. What Is **Splunk**? – Ultimate Soln. For Log Processing

iii. How Does It Work? – **Splunk Components**

iv. **Hands-On**:- Log Collection & Analysis

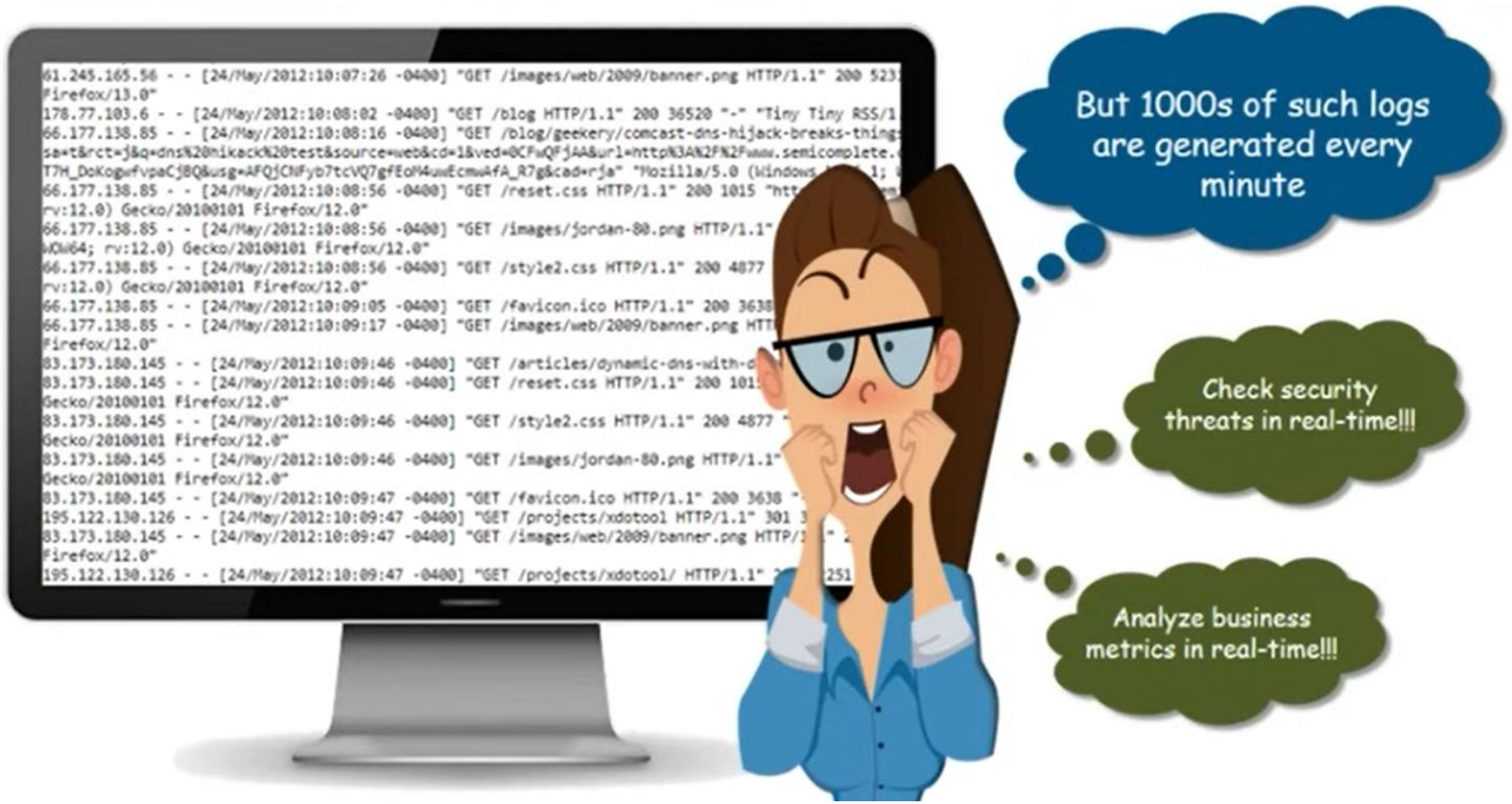
Goals for Splunk

*Logs are the go-to achieves for gaining company-wide **Operational Intelligence**.*

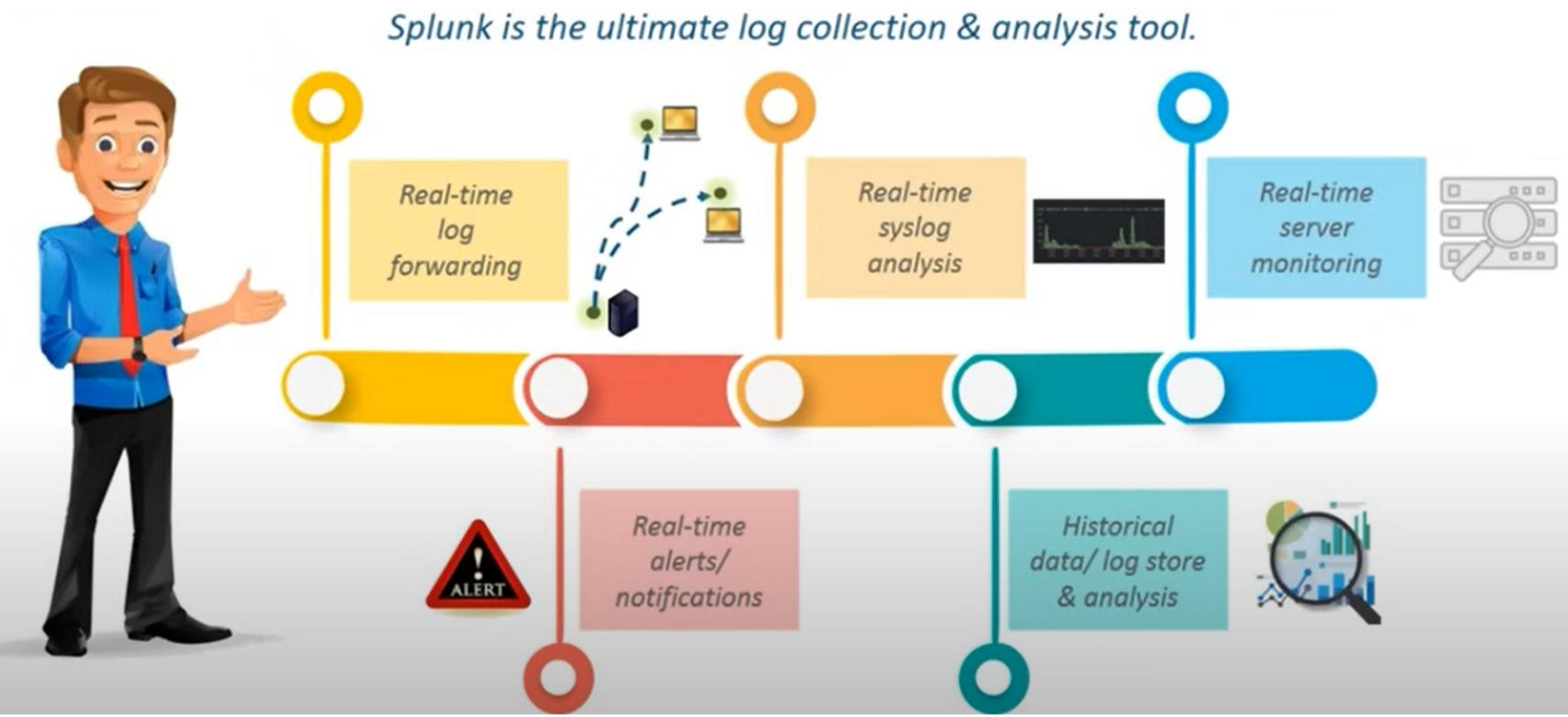
- *Source of IP traffic*
- *Security threats*
- *Network vulnerability*
- *Network traffic & spike*

- *System performance*
- *CPU usage & load*
- *User access logs*
- *App performance monitoring*

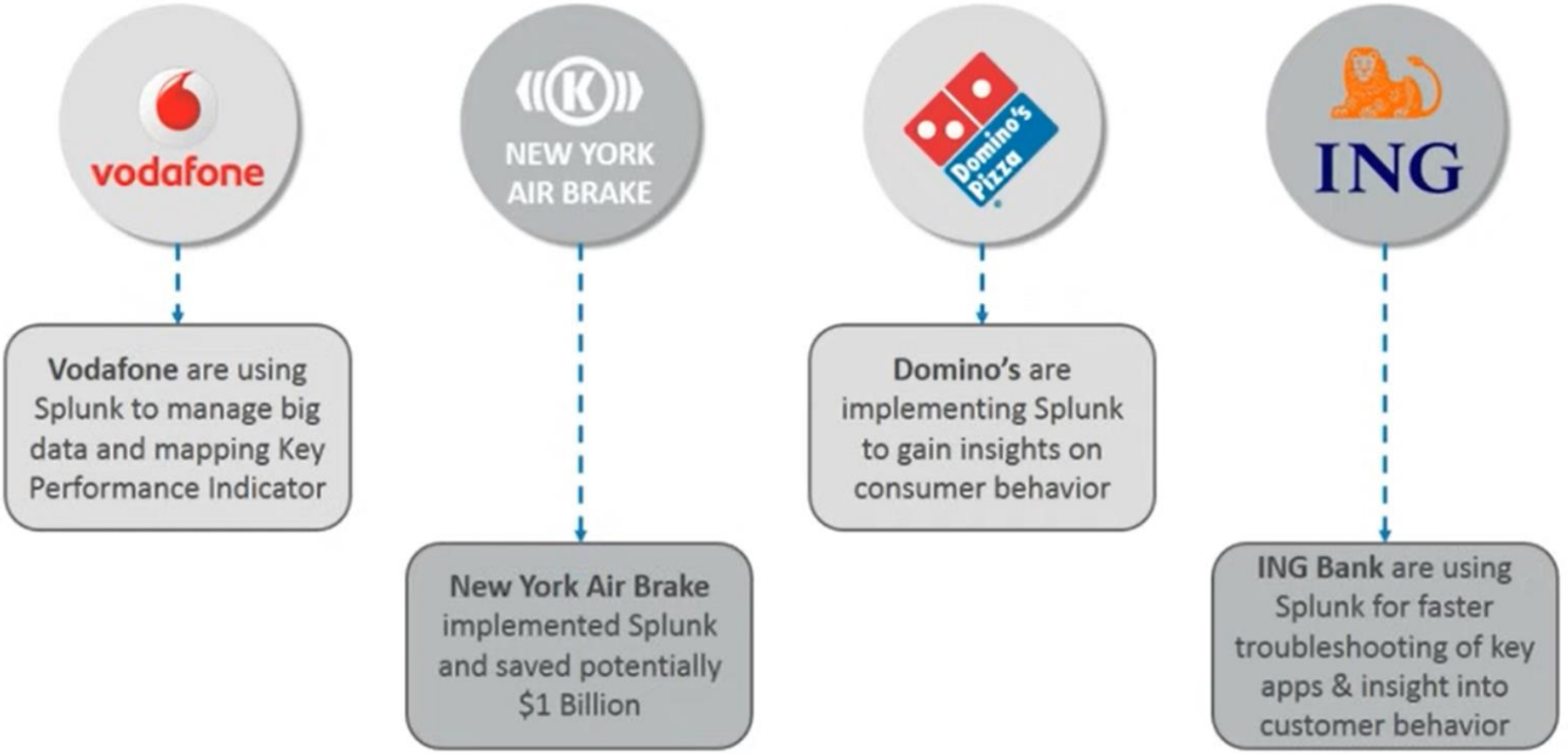
Explore Logs - Challenges



Explore Logs – Solution- Splunk



Explore Logs – Splunk - Usecases



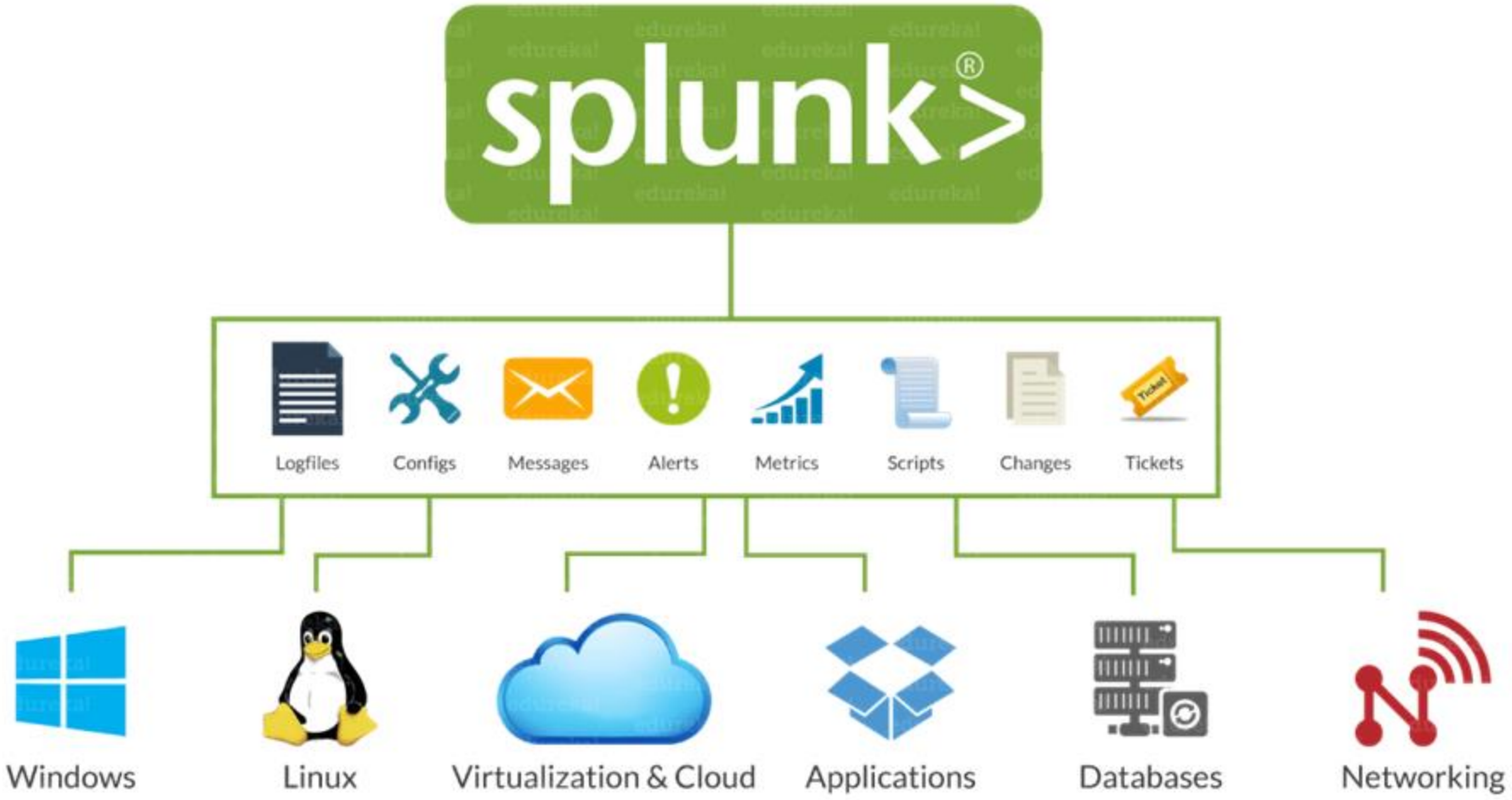
Case: Domino's

Case: Domino's

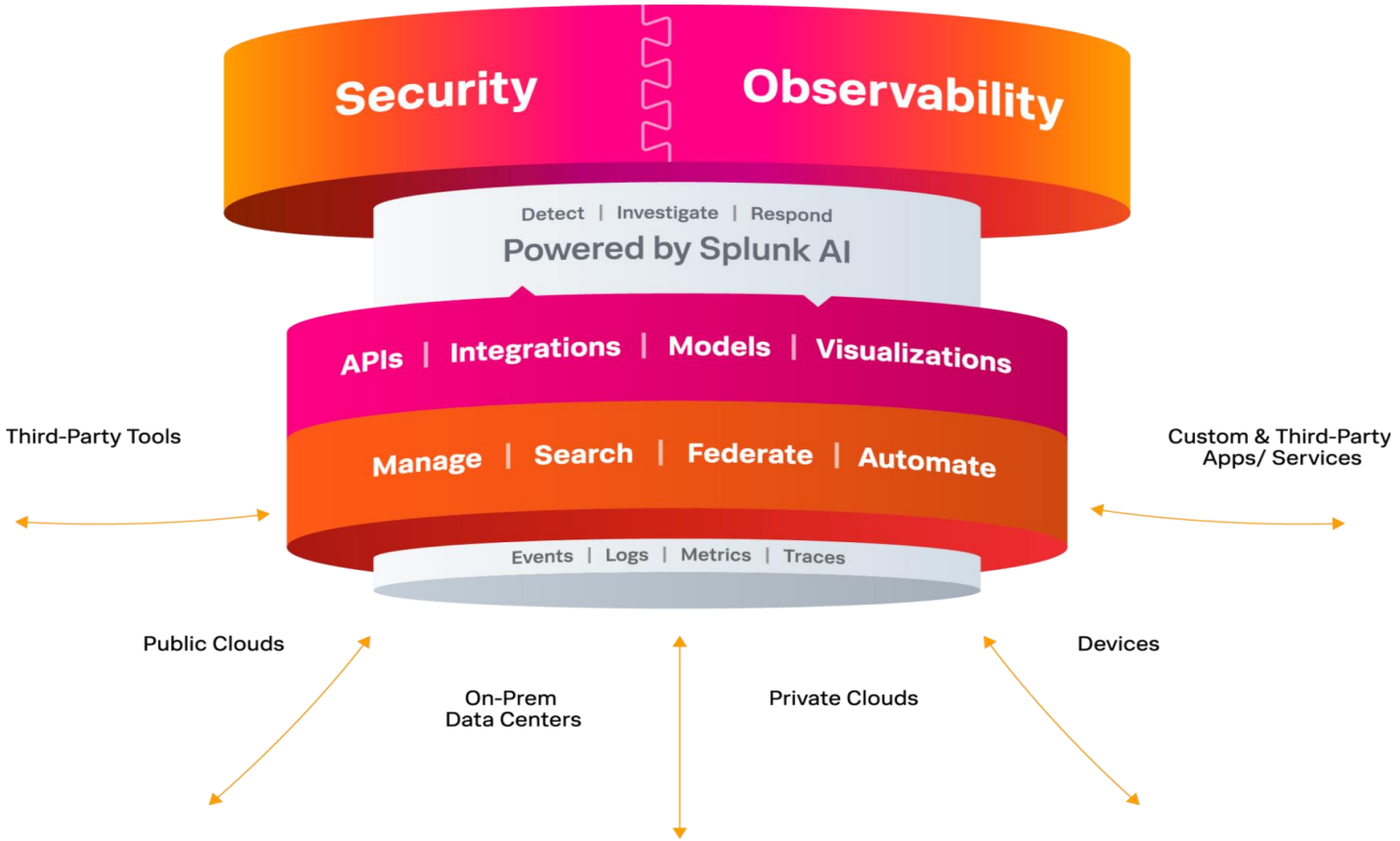
Splunk

- Splunk is a one-stop solution as it automatically pulls data from various sources and accepts data in any format such as .csv, json, config files, etc.
- Splunk is the easiest tool to install and allows functionality like searching, analyzing, reporting as well as visualizing machine data.
- It has a huge market in the IT infrastructure and business.
- Many big players in the industry are using splunk such as Dominos, Adobe, Bosch, Vodafone, Coca-Cola etc.

Splunk


splunk>
Logfiles
Configs
Messages
Alerts
Metrics
Scripts
Changes
Tickets
Windows
Linux
Virtualization & Cloud
Applications
Databases
Networking

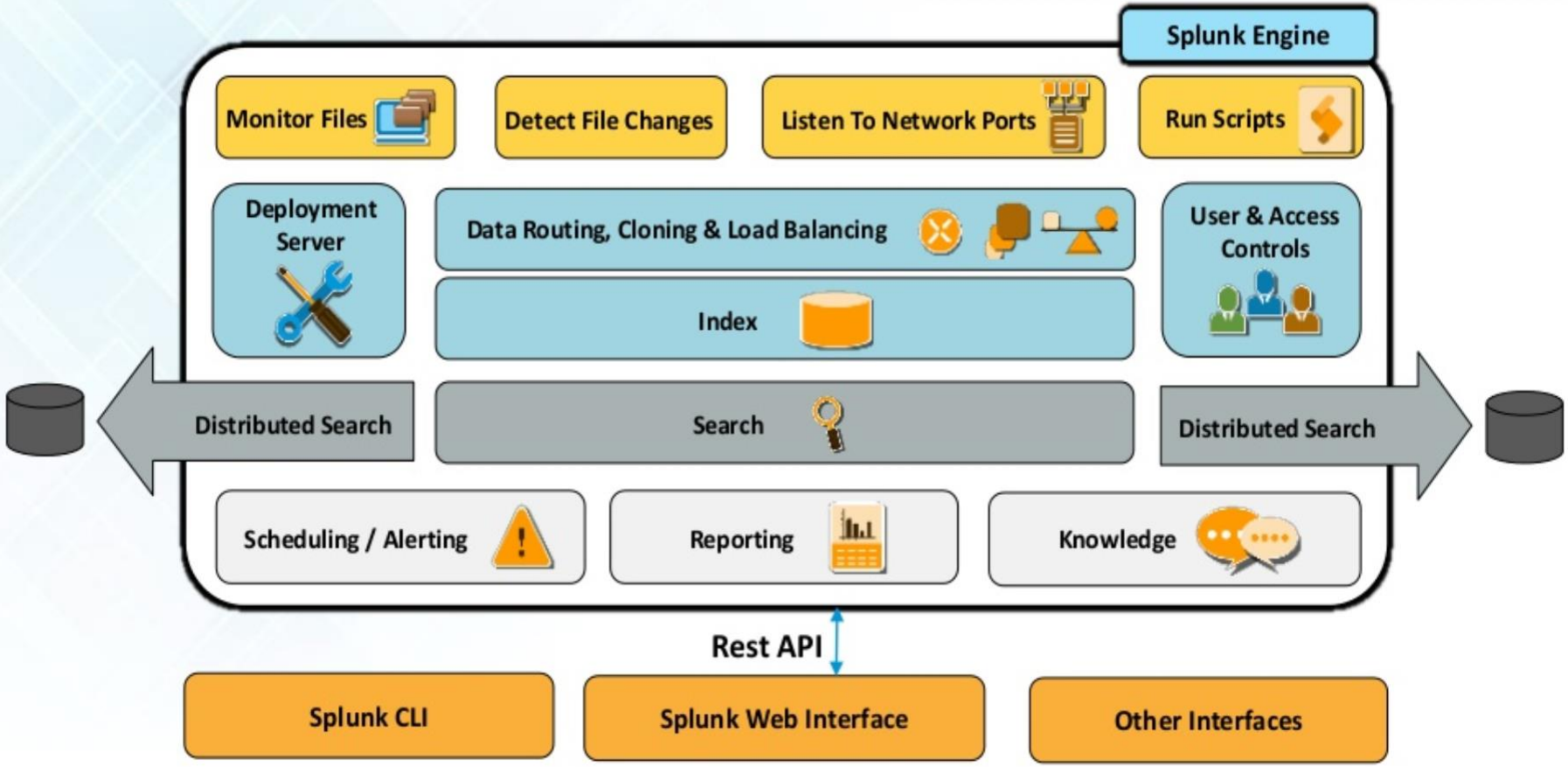
Splunk


Security
Observability
Detect | Investigate | Respond
Powered by Splunk AI
APIs | Integrations | Models | Visualizations
Manage | Search | Federate | Automate
Events | Logs | Metrics | Traces
Third-Party Tools
Custom & Third-Party Apps/ Services
Public Clouds
On-Prem Data Centers
Private Clouds
Devices

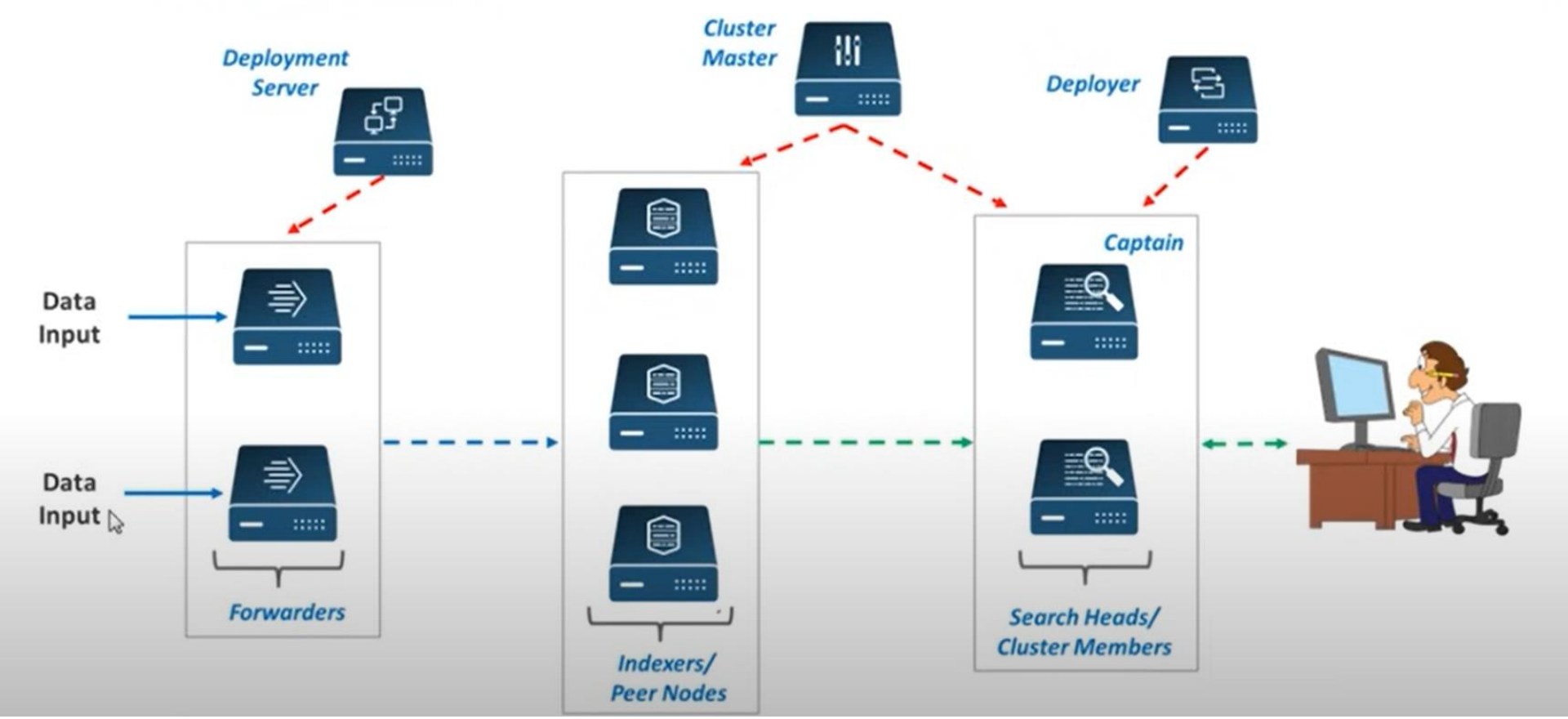
Splunk

- Splunk collects data in real-time from multiple systems.
- It accepts data in any form, example- log file, .csv, json, config etc.
- Splunk can pull data from database, cloud and any other OS
- It analyze and visualize the data for better performance.
- Splunk give alerts/ event notifications.
- Provides real-time visibility.
- It satisfies industry needs like horizontal scalability (using many systems in parallel)

Splunk Architecture



Splunk Components



Splunk Architecture

- Splunk CLI/ splunk web interface or any other interface interacts with the search head.
- This communication happens via Rest API.
- It can be used to search head to make distributed searches, setup knowledge objects for operational intelligence, perform scheduling/ alerting and create reports or dashboards for visualization.
- It can also be used to run scripts for automating data forwarding from remote Splunk forwarders to pre-defined network ports.
- After that you can monitor the files that are coming at real time and analyze if there are any anomalies and set alert/ reminders accordingly.
- It can be used to perform routing, cloning and load balancing of the data that is coming in from the forwarder, before they are stored in an indexer.
- It can also be used to create multiple users to perform various operations on the indexed data.

Splunk vs Other Tools

Features	Splunk	Sumo Logic	ELK
Searching	✓	✓	Only possible with Integrations
Analysis	✓	✓	Only possible with Integrations
Visualization Dashboard	✓	✓	Only possible with Integrations
SaaS Setup	✓	✓	✓
On Premise Setup	✓	✗	✓
Input any data type	✓	✓	Needs plugins
Plugins & Integration	✓	✓	✓
Customer Support	✓	Available; but not proficient	Available; but not proficient
Documentation & Community	✓	✗	✓

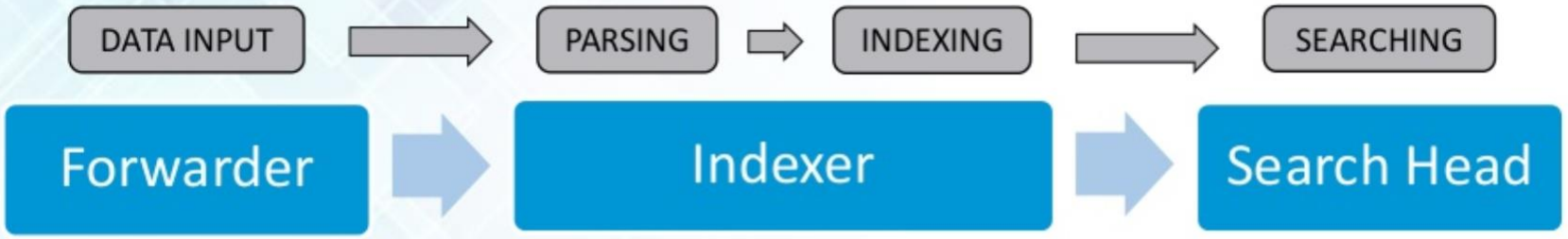
Installing Splunk

- **Best practice**: Do not run Splunk as ***super-user***
  - For example, **root** on *NIX, **administrator** on Windows
- Create a user account that is used to run Splunk
  - For input, Splunk must be able to access data sources
    - On *NIX, **`/var/log`** is not typically open to non-root accounts
  - On *NIX, non-root accounts cannot access ports < 1024
  - On Windows
    - Use a domain account if Splunk has to connect to other servers
    - Otherwise, use a local machine account that can run services
  - Make sure the Splunk account can access scripts used for inputs and alerts

Installing Splunk

Usage	Splunk Enterprise	Universal Forwarder
splunkd	**8089**	**8089**
Splunk Web	**8000**	-
Web app-server proxy	**8065**	-
KV Store	**8191**	-
S2S receiving port(s)	No default	-
Any network/http input(s)	No default	No default
Index replication port(s)	Optional (no default)	-
Search replication port(s)	Optional (no default)	-

Splunk Components



- Collects the data from remote machines
- Forwards the data to the Indexer in real-time

- Processes the incoming data in real-time
- Stores & Indexes the data on disk

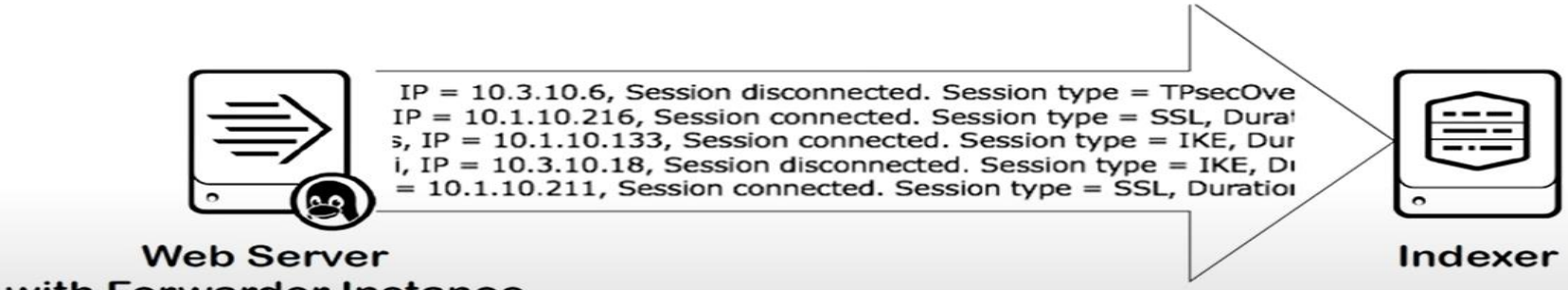
- End users interact with Splunk through Search Head
- Allows users to do searching, analysis & visualization

Splunk Components

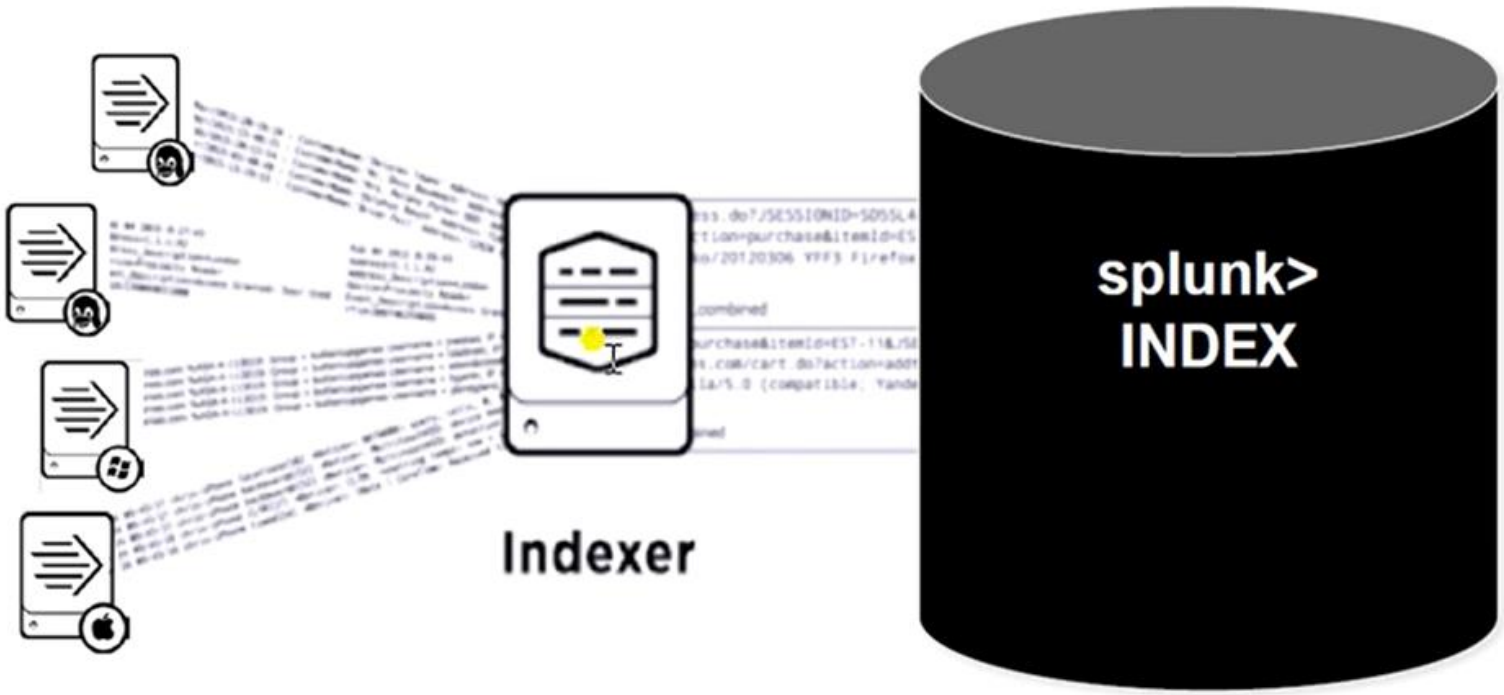
Forwarder

Indexer

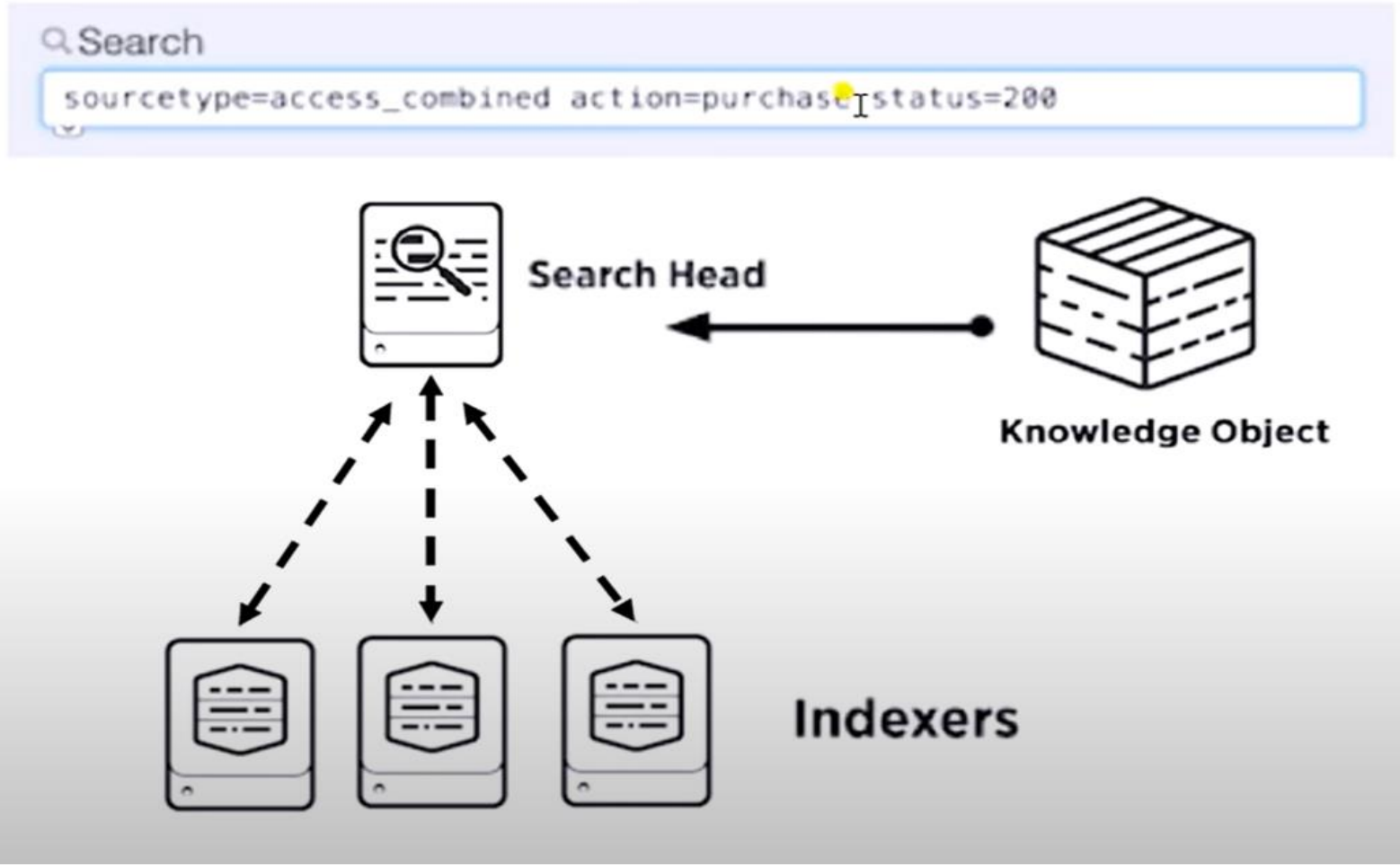
Search Head



Splunk Components



Standalone Splunk Deployment



Knowledge Object

- Splunk knowledge objects are a set of user-defined searches, fields, and reports that enrich your data and give it structure.
- A knowledge object could be a piece of search or a piece of data being ingested.
- It could also just be a group of data.
- Data enrichment done using knowledge objects.

What are all of the Splunk Knowledge Objects?

- Index: A collection of data that is searchable and that can be retrieved using Splunk's search language. Data is stored in indexes according to a set of rules and configurations.
- Source types: Labels that help Splunk determine the format of incoming data. Source types determine how data should be parsed and interpreted, allowing Splunk to extract fields and transform the data.

What are all of the Splunk Knowledge Objects?

- Fields: Key-value pairs that contain specific data values extracted from events. Fields can be created automatically or defined manually by users. To create a field manually, you can use the Fields menu to create a new field and define its attributes.
- Search-time field extractions: configurations that allow users to create new fields based on the content of existing fields. They can be defined through configuration files.

What are all of the Splunk Knowledge Objects?

- Lookups: Tables of data used to add context to events or map fields to different values. They're typically created from CSV files or databases and can be used in searches and visualizations.
- Tags: Labels that can be applied to events, fields, or sources to categorize and group them. Tags can be created manually or defined through search-time extractions.

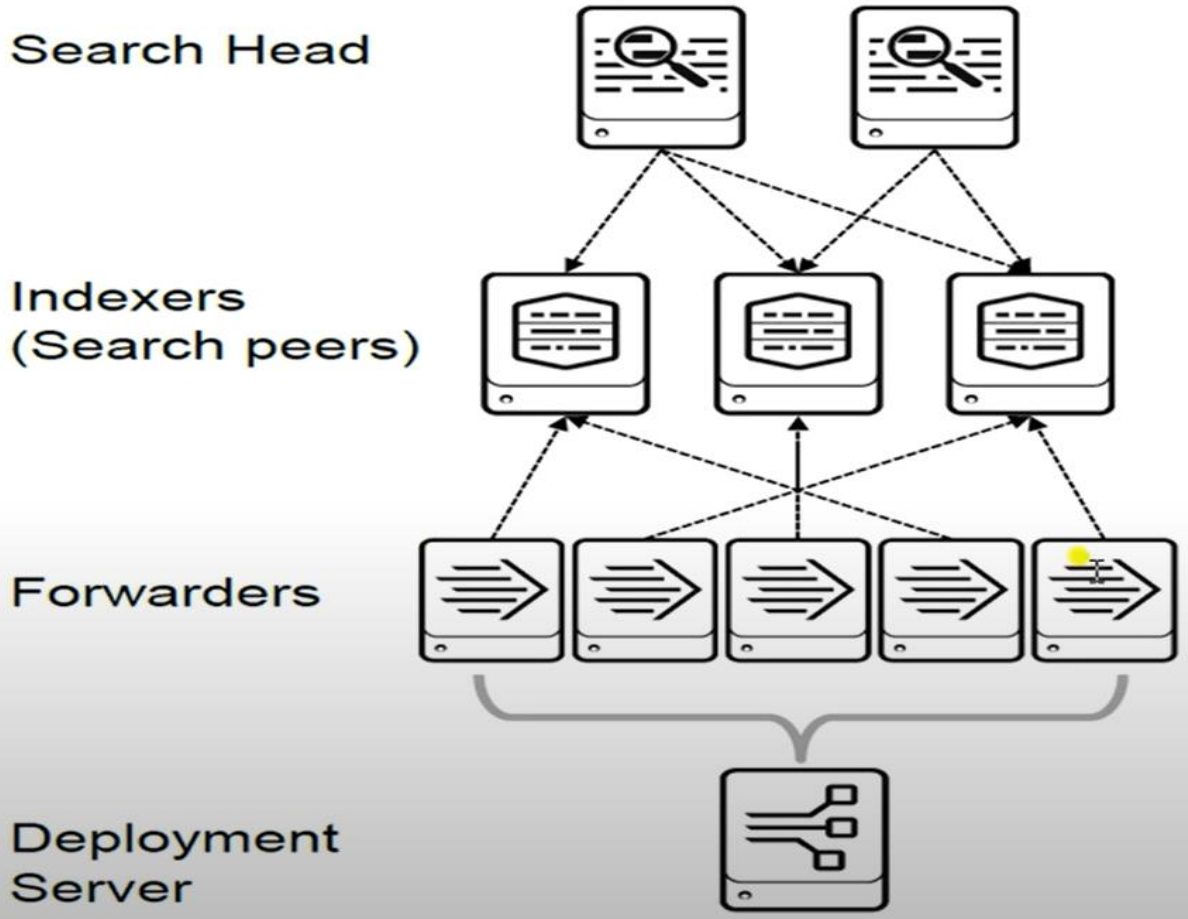
What are all the Splunk Knowledge Objects?

- Event types: Named collections of events that share similar characteristics or properties. Their purpose is to simplify searches, provide a higher level of abstraction, and help with reporting and alerting.
- Alerts: Configurations that trigger an action when a specific condition is met, specifically: sending notifications or running scripts.
- Reports: Saved searches that are scheduled to run at specific intervals and generate visualizations or summaries of data.
- Dashboards: Customizable displays that show real-time or historical data in the form of charts, tables, or other visualizations.

What are Knowledge Object tags?

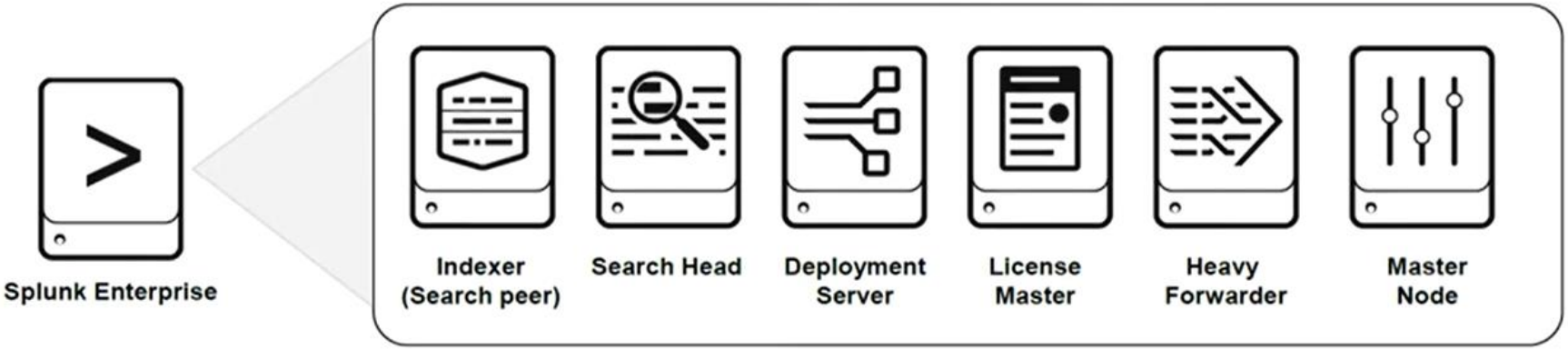
- Tags can help you centralize the naming conventions behind your data and knowledge objects.

Distributed Splunk Deployment

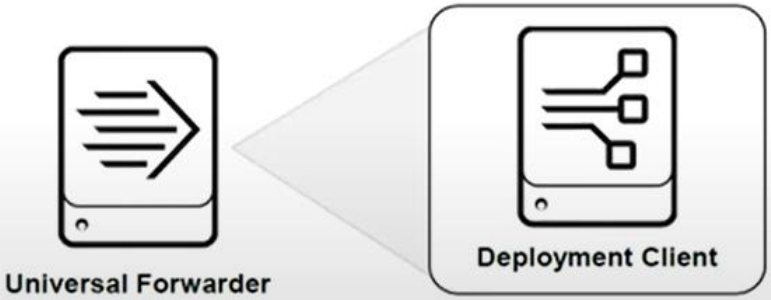


Enterprise Splunk Deployment

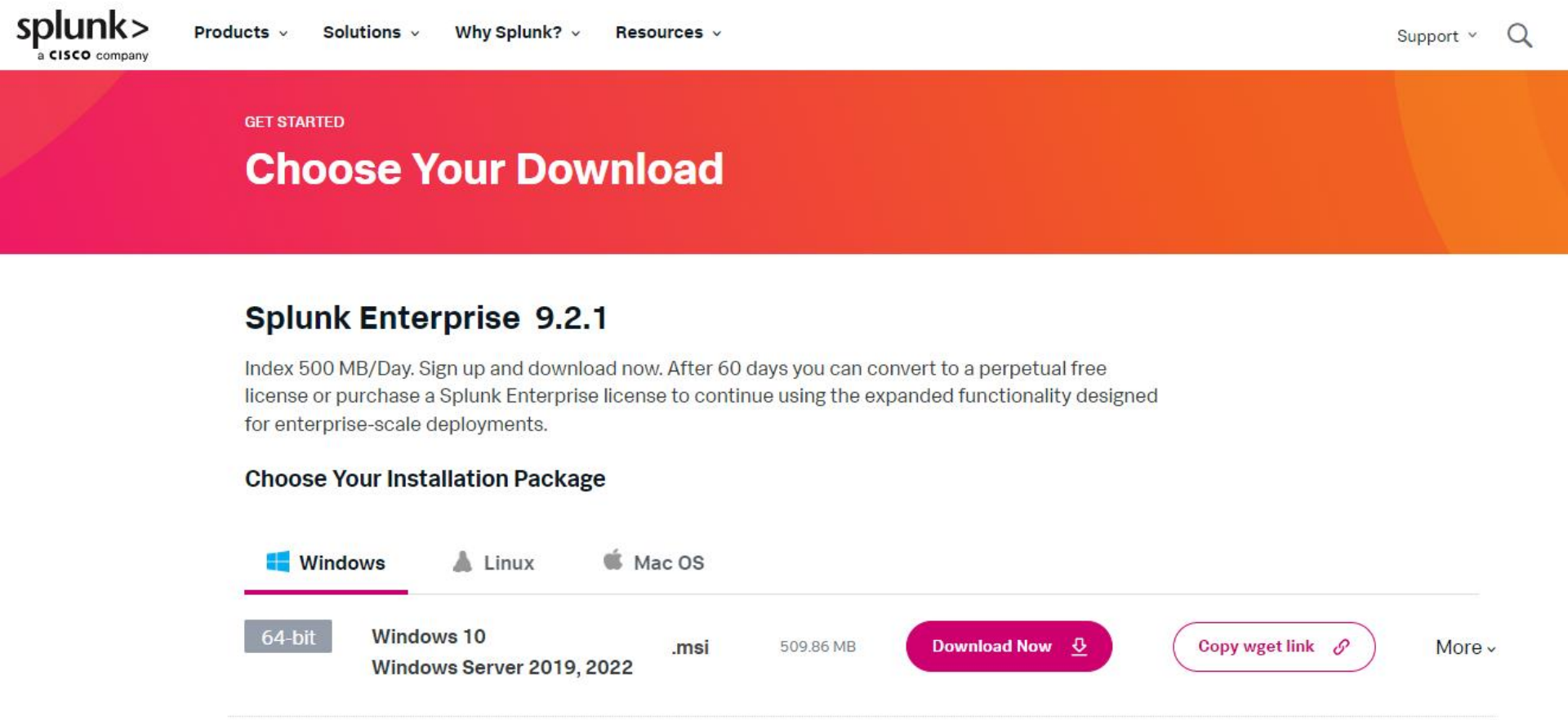
- Included in the Splunk Enterprise software package



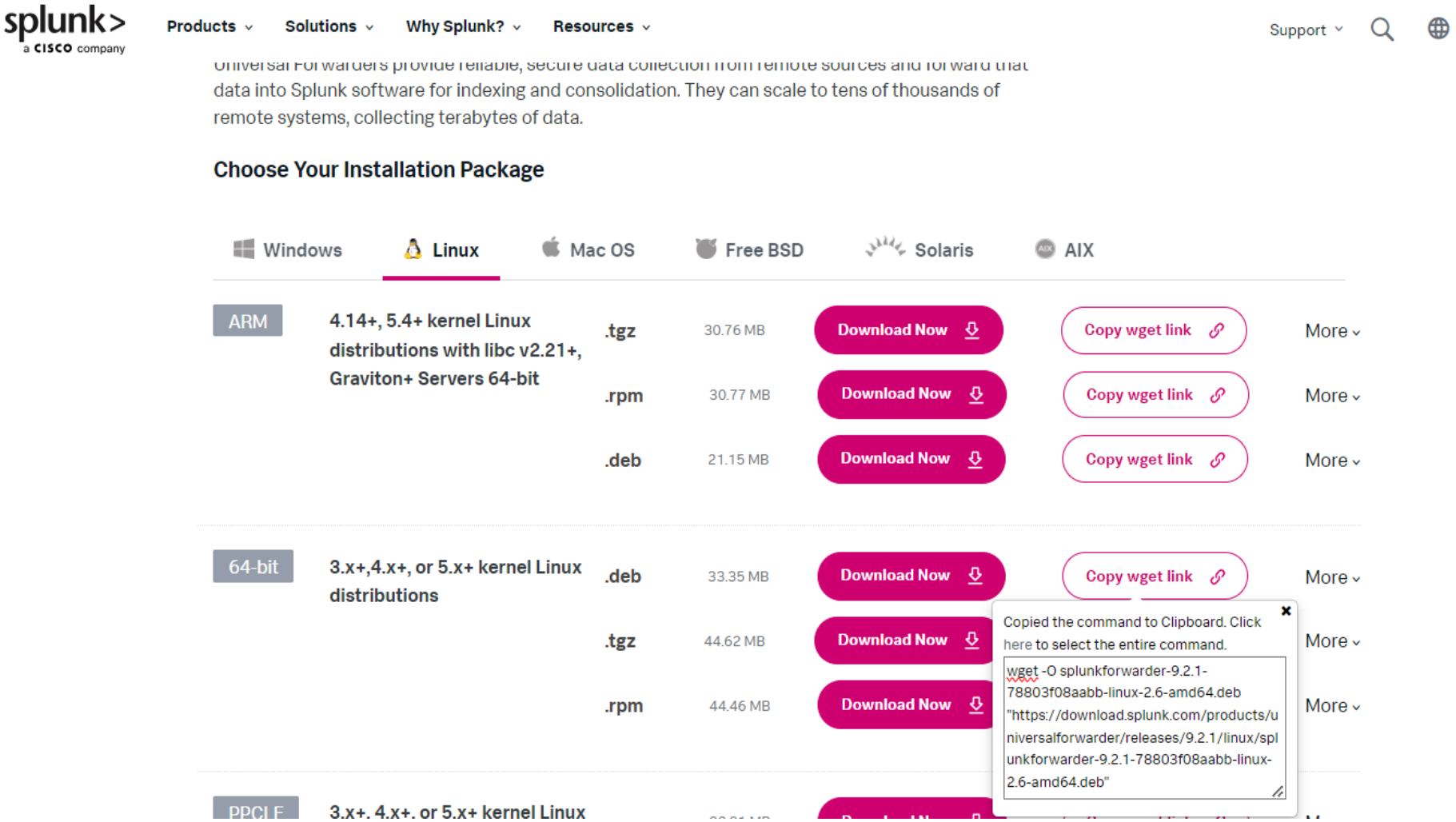
- Included in the Universal Forwarder software package



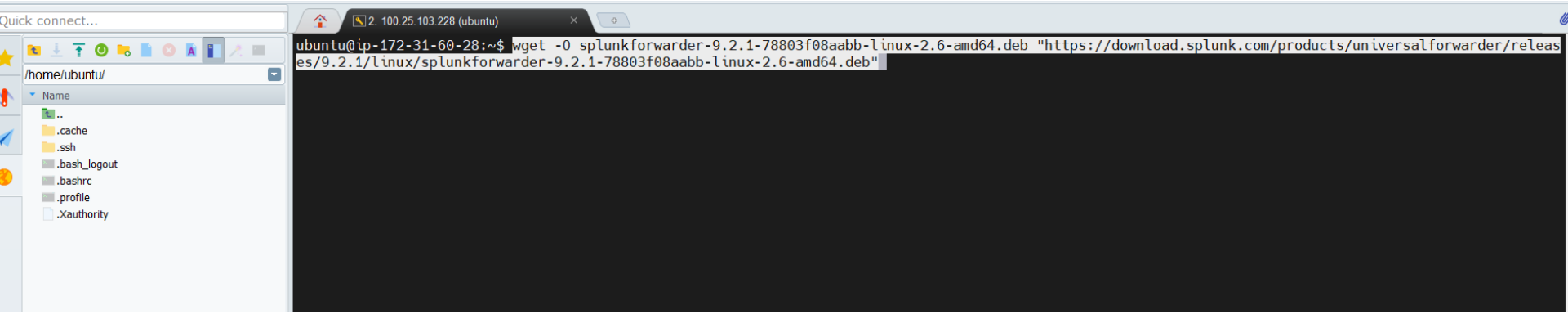
Install Splunk on Windows

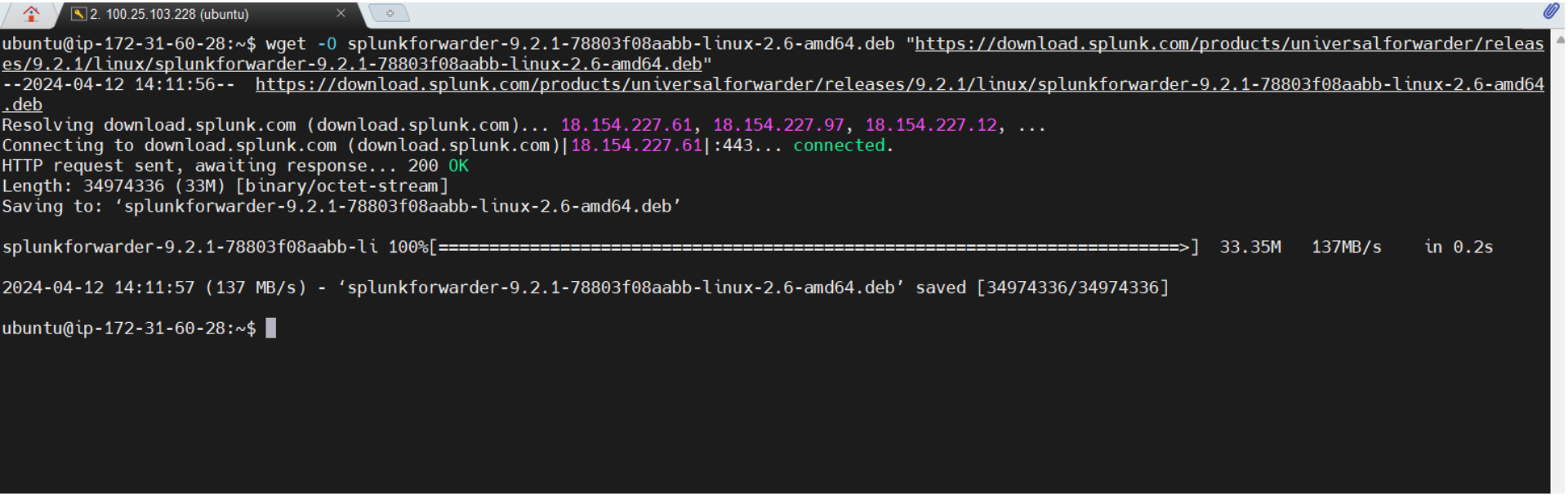


Install Splunk Universal Forwarder on Ubuntu



Install Splunk Universal Forwarder on Ubuntu



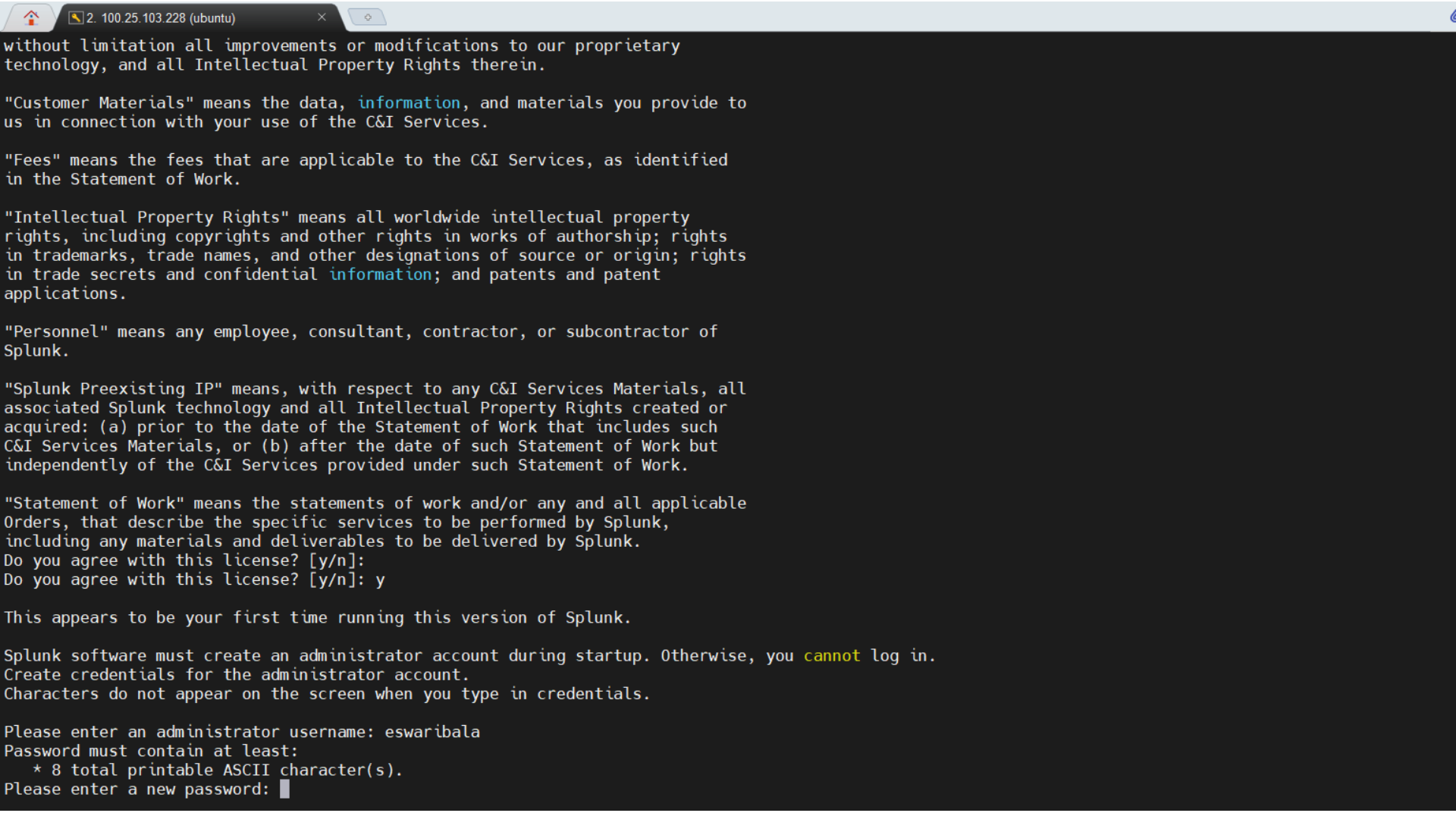


Install Splunk Universal Forwarder on Ubuntu

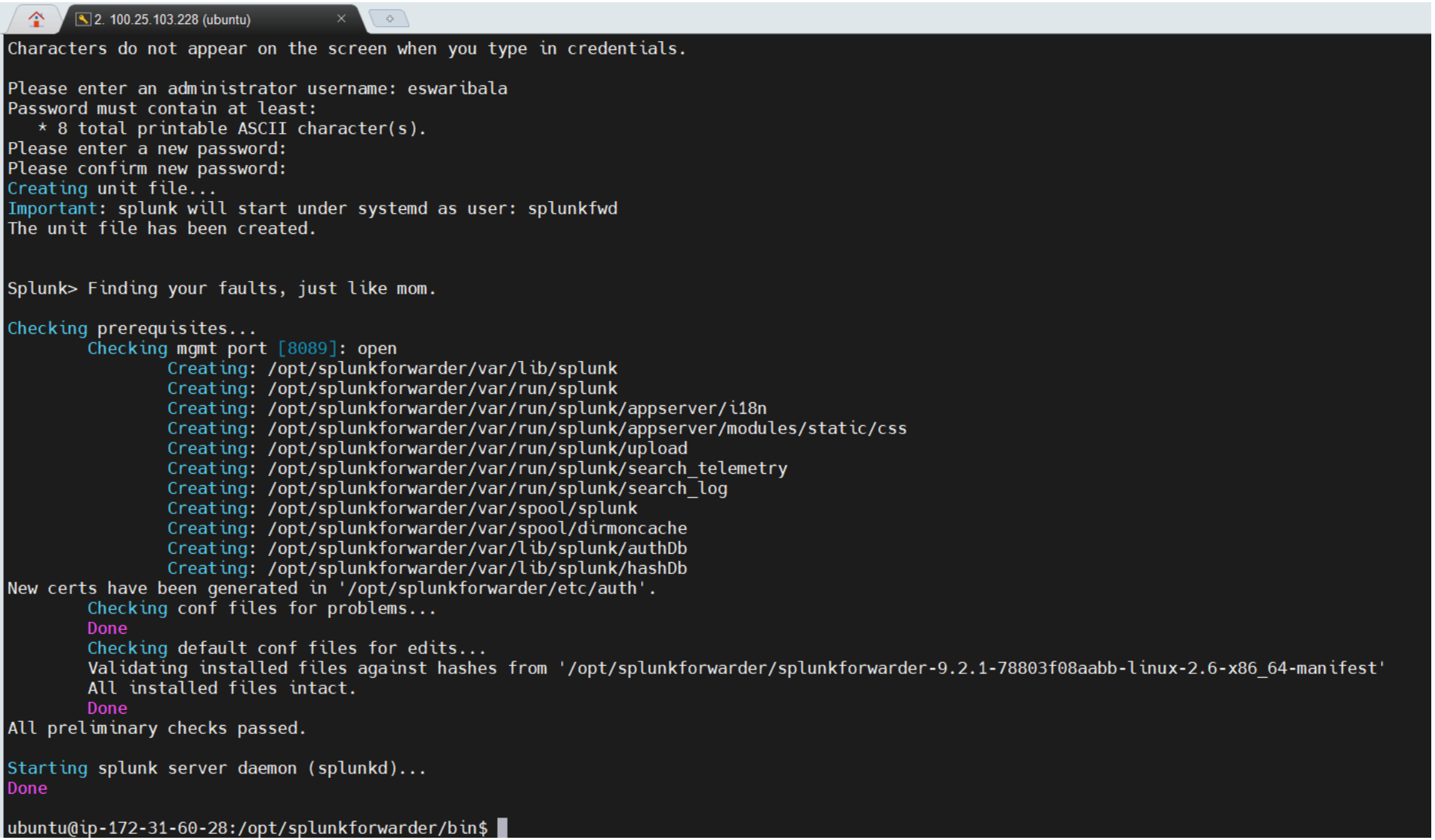
```
ubuntu@ip-172-31-60-28:~$ ls
splunkforwarder-9.2.1-78803f08aabb-linux-2.6-amd64.deb
ubuntu@ip-172-31-60-28:~$ sudo dpkg -i splunkforwarder-9.2.1-78803f08aabb-linux-2.6-amd64.deb
Selecting previously unselected package splunkforwarder.
(Reading database ... 65273 files and directories currently installed.)
Preparing to unpack splunkforwarder-9.2.1-78803f08aabb-linux-2.6-amd64.deb ...
Unpacking splunkforwarder (9.2.1+78803f08aabb) ...
Setting up splunkforwarder (9.2.1+78803f08aabb) ...
complete
ubuntu@ip-172-31-60-28:~$
```

```
2. 100.25.103.228 (ubuntu)
ubuntu@ip-172-31-60-28:~$ cd /opt
ubuntu@ip-172-31-60-28:/opt$ ls
splunkforwarder
ubuntu@ip-172-31-60-28:/opt$ cd splunkforwarder
ubuntu@ip-172-31-60-28:/opt/splunkforwarder$ ls
README-splunk.txt  cmake          etc  include  license-eula.txt  share                                                  swidtag
bin                copyright.txt  ftr  lib      openssl           splunkforwarder-9.2.1-78803f08aabb-linux-2.6-x86_64-manifest  uf
ubuntu@ip-172-31-60-28:/opt/splunkforwarder$ cd bin
ubuntu@ip-172-31-60-28:/opt/splunkforwarder/bin$ ls
2to3-3.7     bzip2            genRootCA.sh            idle3.7       pip3         prigreypng   pripngtopam  scripts       splunk-tlsd          wheel
S3benchmark  classify         genSignedServerCert.sh  openssl       pip3.7       pripalpng    priweavepng  setSplunkEnv  splunkd
btool        copyright.txt    genWebCert.sh           pcre2-config  prichunkpng  pripamtopng  pydoc3       slim          splunkmon
btprobe      easy_install-3.7 idle3                   pid_check.sh  priforgepng  pripnglsch   pydoc3.7     splunk        supervisor-simulator
ubuntu@ip-172-31-60-28:/opt/splunkforwarder/bin$ ./splunk start
```

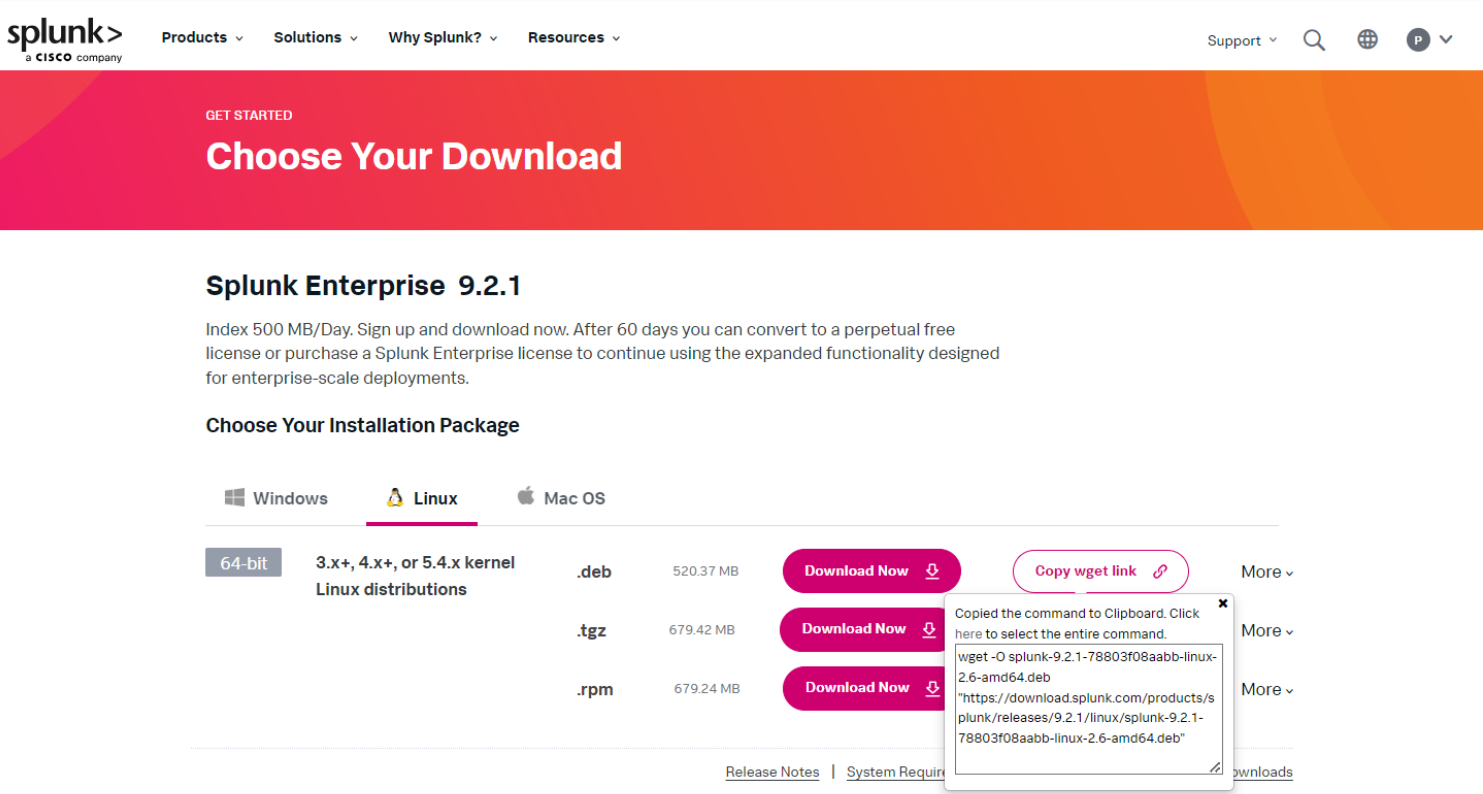
Install Splunk Universal Forwarder on Ubuntu



Install Splunk Universal Forwarder on Ubuntu



Splunk Enterprise for Ubuntu



Splunk Enterprise for Ubuntu

- Splunk Receiver
- http://52.201.69.229:8000/en-GB/app/launcher/home

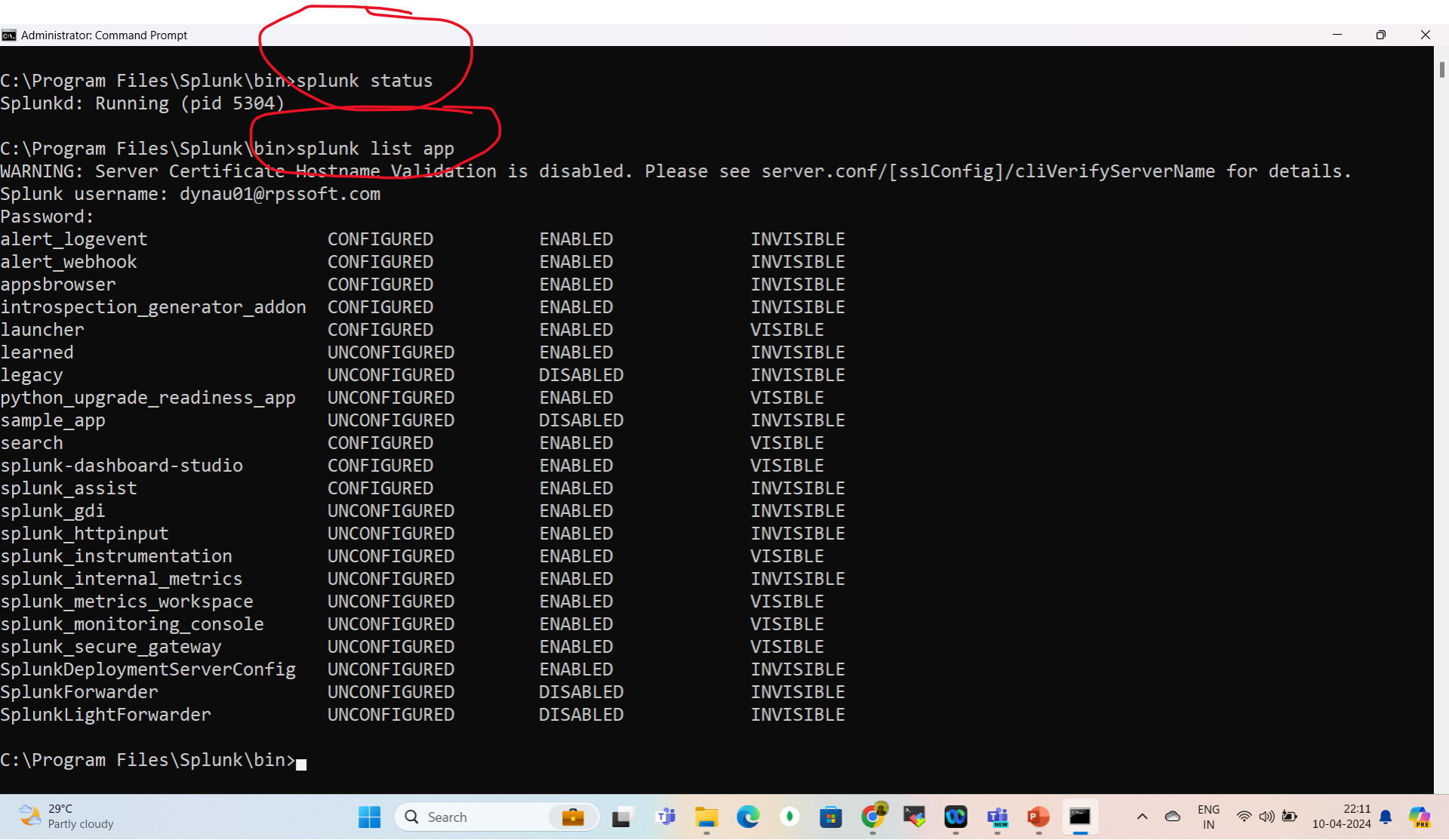
- Splunk Heavy Forwarder
- http://52.204.111.128:8000/en-GB/app/launcher/home

- Splunk Universal Forwarder
- 34.224.63.207:8089

Work with the CLI on Windows

- To run CLI commands in Splunk Enterprise on Windows, use PowerShell or the command prompt as an administrator.
  - Open a PowerShell window or command prompt as an administrator.
  - Change to the Splunk Enterprise bin directory.
  - Run a Splunk command by typing in splunk followed by the subcommand and any required arguments.

Work with the CLI on Windows



Splunk Access your data, no matter where you are

Machine learning and AI

Predict and prevent, don't just react. Improve security and business outcomes by bringing machine-level intelligence to your data.

Data streaming

Collect, process and distribute data to Splunk and other destinations in milliseconds with real-time stream processing.

Scalable index

Collect and ingest data from thousands of sources and counting, all at terabyte scale.

Collaborative tools

Interact and collaborate from anywhere with mobile, TV and augmented reality capabilities.

Analytics workspace

React instantly with visualization. Convert logs into metrics, boost search and monitoring performance, and streamline alerting functions.

Powerful dashboards

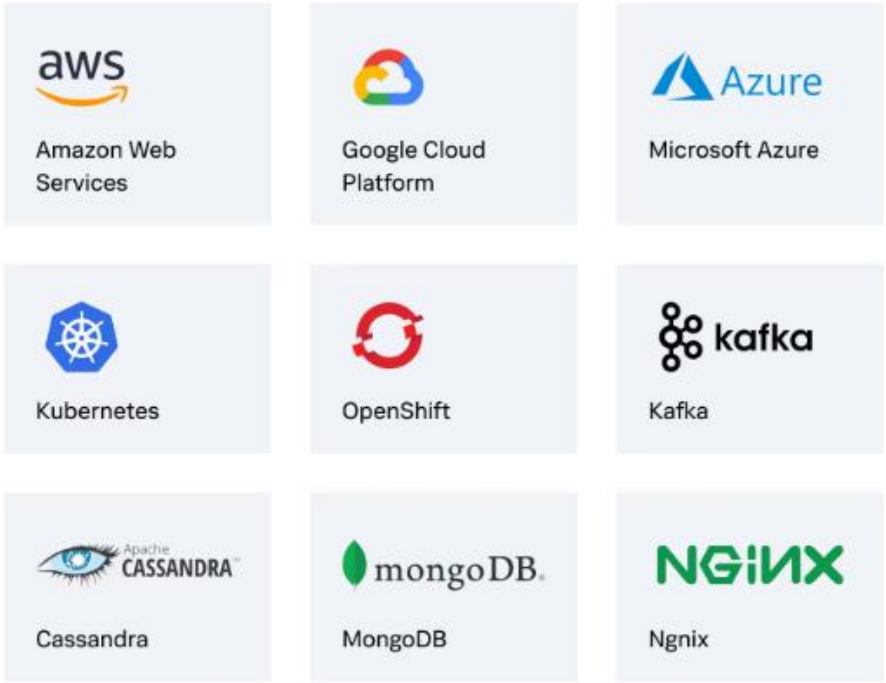
Easily communicate even your most complex data stories using our intuitive dashboard-building experience.

Splunk Integrations

INTEGRATIONS

Over 2,300 out-of-the-box integrations

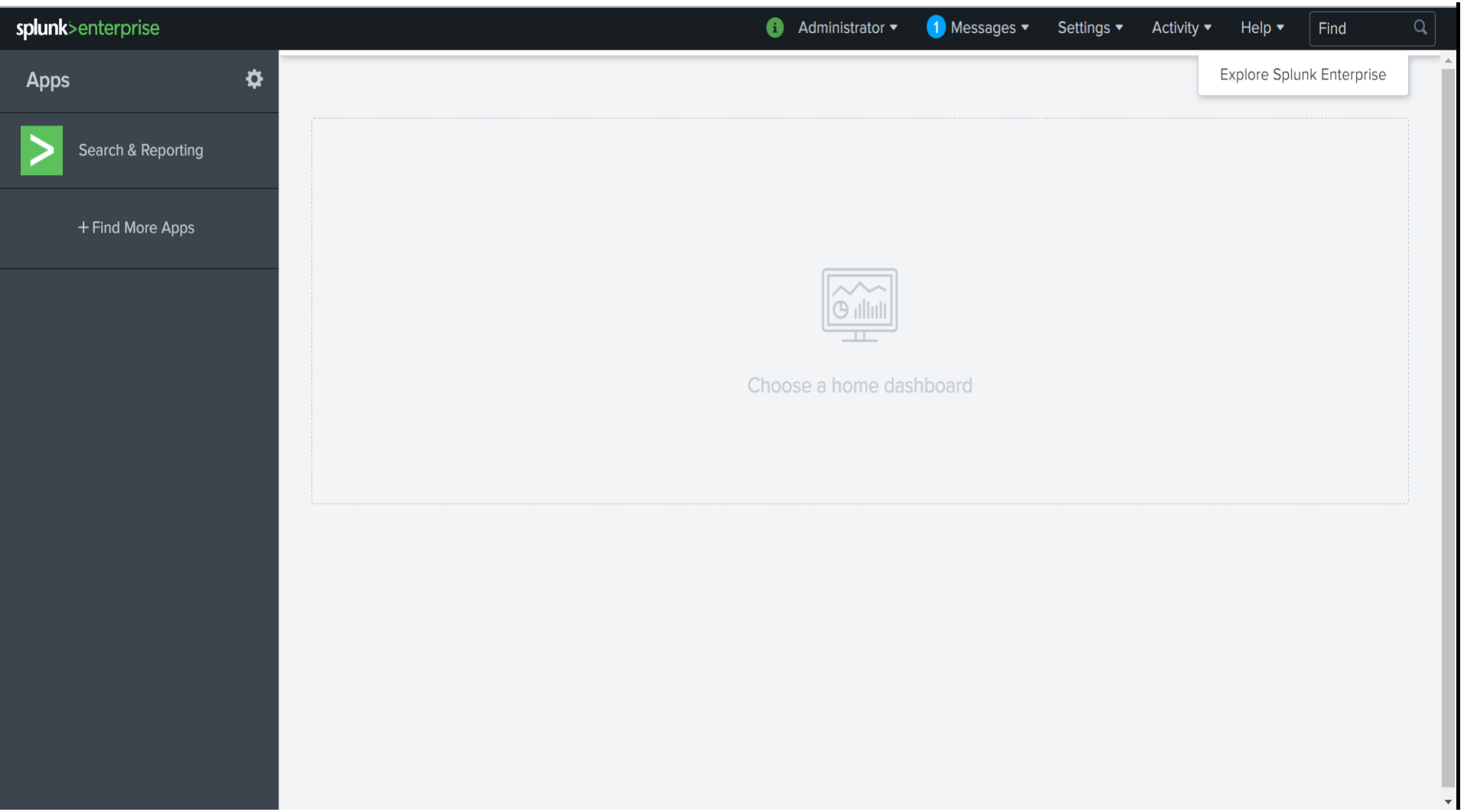
View All Integrations



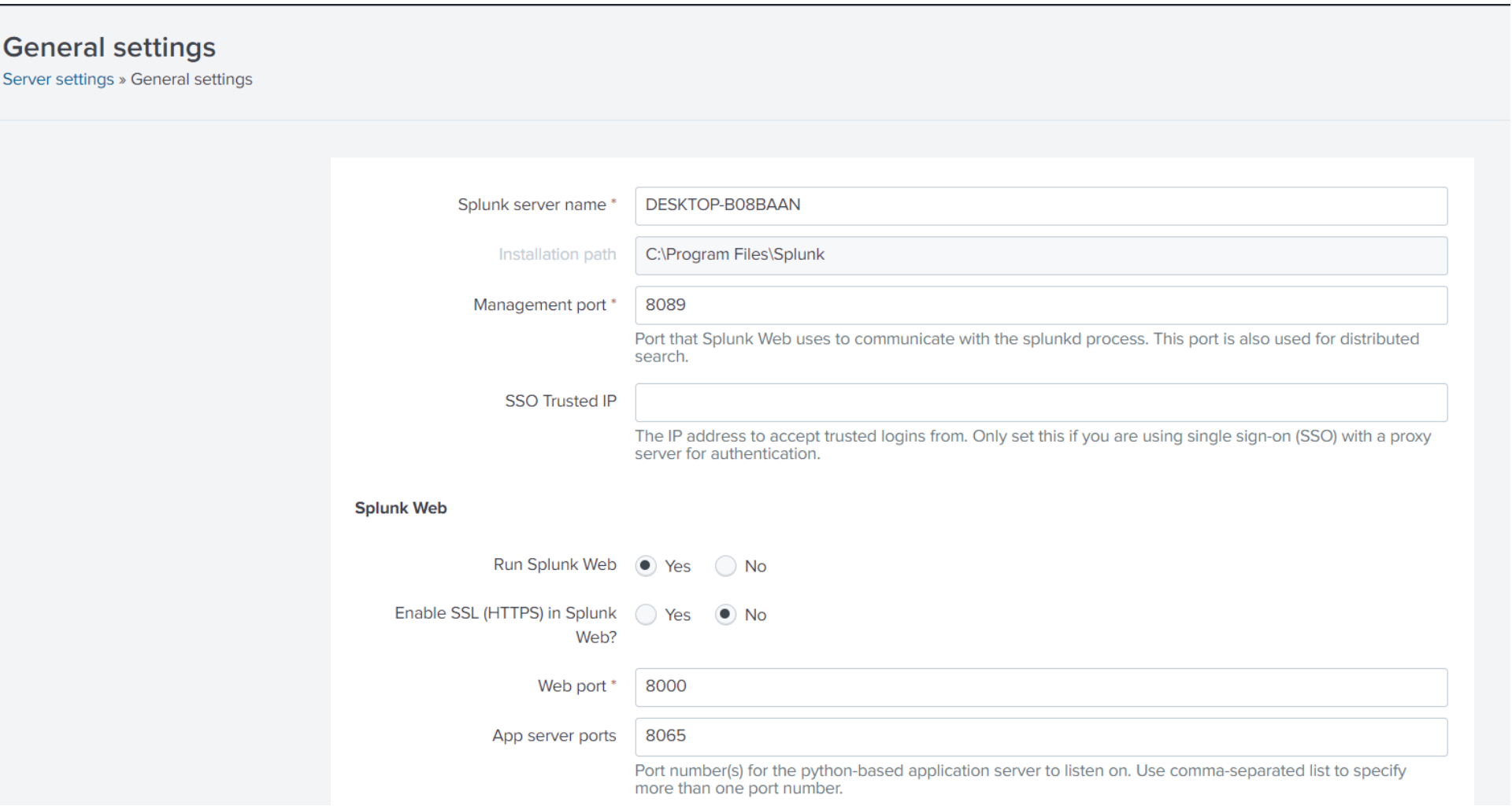
Splunk Users

Persona	Industry Role	Activities
Administrator	network engineer, system administrator	• Configures, administers, optimizes, and secures the Splunk Enterprise deployment. • Sets up user accounts and permissions. • Gets data into Splunk Enterprise.
Knowledge Manager	data analyst, system administrator	• Oversees knowledge object creation, normalization, and usage across teams, departments, and deployments. • Gets the data into Splunk Enterprise, or works with the administrator to do so. • Creates and shares data models.
Search User	data analyst, IT professional, network engineer, security analyst, system administrator	• Uses Search to investigate server problems, understand configurations, monitor user activities, and troubleshoot escalated problems. • Builds reports and dashboards to monitor the health, performance, activity, and capacity of their IT infrastructure. • Identifies patterns and trends that are indicators of routine problems.
Pivot User	business professional, data analyst, executive, IT professional, manager, system administrator	• Uses Pivot to build reports based on data models created by the Knowledge Manager. • Creates reports and dashboards to monitor their businesses. • Identifies trends in the health and performance of their businesses.
Developer	system integrator, professional developer	• Integrates data and functionality of applications with Splunk Enterprise. • Builds Splunk apps and add-ons with custom dashboards and data visualizations.

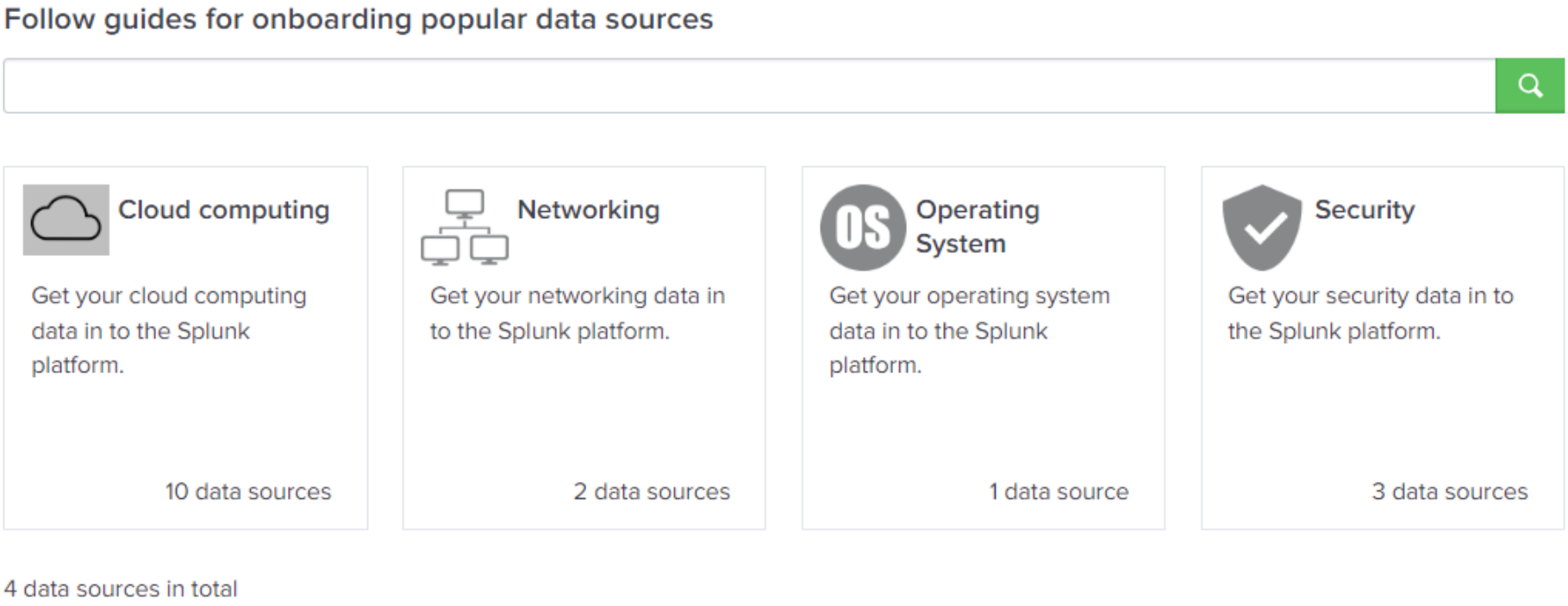
Splunk Handson



Splunk Handson



Add Data to Splunk



Add Data to Splunk

upload

files from my computer

Local log files

Local structured files (e.g. CSV)

Tutorial for adding data

monitor

files and ports on this Splunk indexer

Files - WMI - TCP/UDP - Scripts

Modular inputs for external data sources

forward

data from Splunk forwarder

Files - TCP/UDP - Scripts

Help me install the universal forwarder

Monitor Data

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.

Active Directory monitoring
Index and monitor Active Directory.

The Splunk Apps

- An app is an application running on Project Splunk.
- Apps are designed to analyze and display knowledge around a particular source or set of data.
- A Splunk app is a packaged collection of knowledge objects and extensions.
- Most of which are represented as files in the Splunk platform installation in your app's directory, $SPLUNK_HOME/etc/apps/appname/.

The Splunk Apps

- An application might contain any or all of the following configurations:
  - Dashboards and support searches that incorporate data source and structure information.
  - Authentication and other interfaces for the management of data sources.
  - An application can allow the use of one or more add-ons to facilitate data collection or configuration.

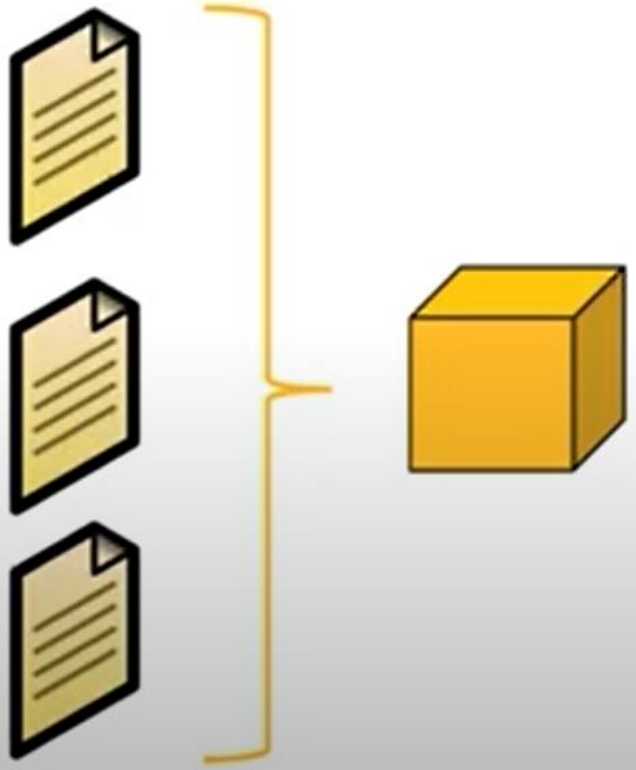
The Splunk Apps

- Apps extend Splunk's functionality
- Apps can be created by third parties, individuals, or Splunk
- Apps that are built by Splunk carry the "Splunk Built" logo
- Apps that are certified by Splunk carry the "Splunk Certified" logo

- Other apps may not have passed the Splunk Certification, but that doesn't mean they aren't useful!

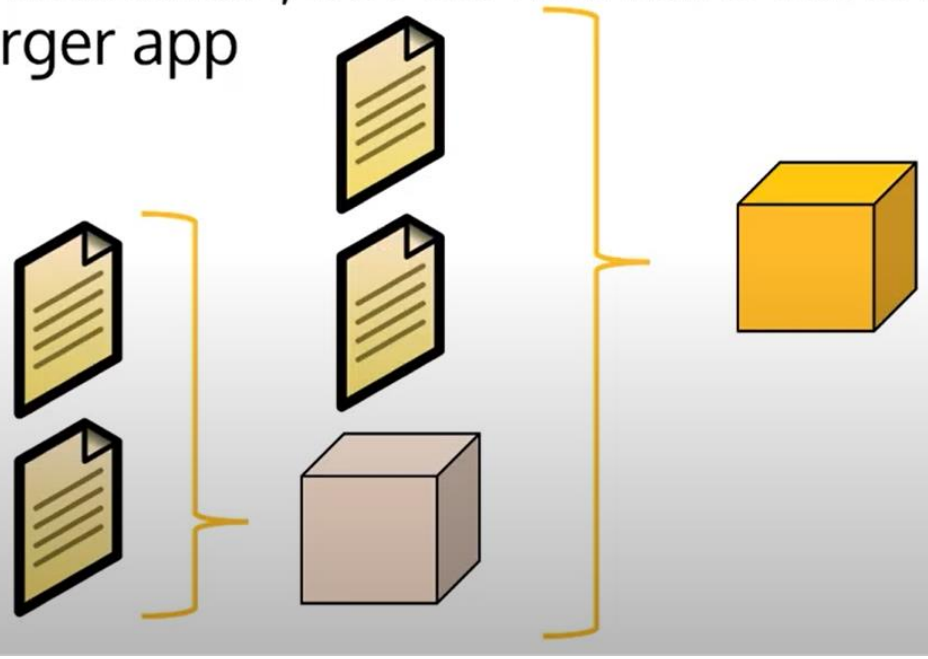
The Splunk Apps

- An app is a collection of Splunk configuration files



The Splunk Apps

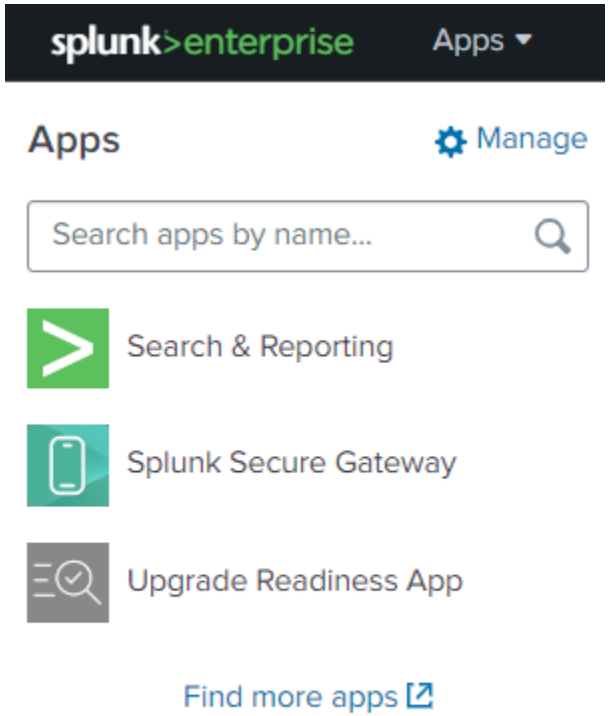
- An add-on is a subset of an app
- Add-ons specify data collection, but do not have GUIs because they are part of the larger app



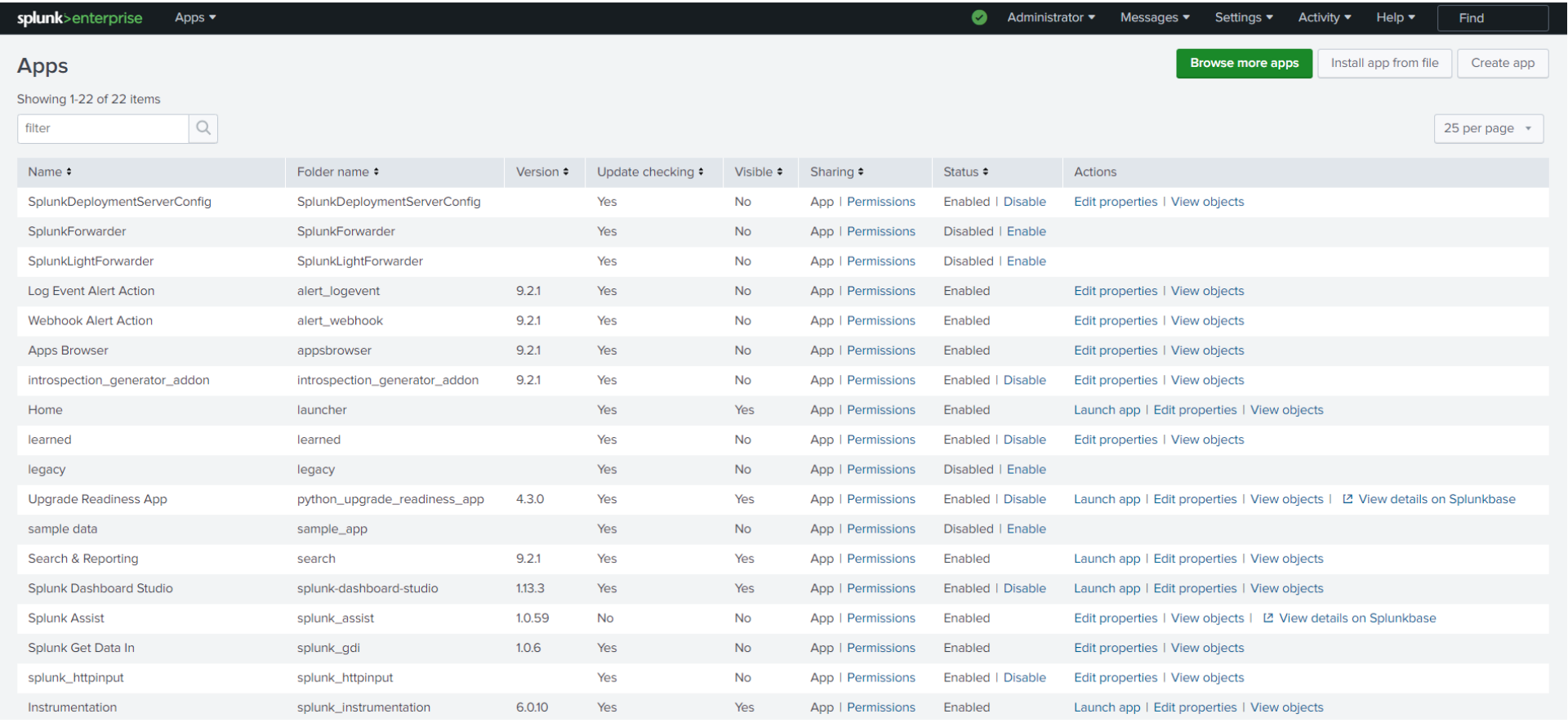
The Splunk Apps

- Apps are downloaded from Splunkbase.com
- Most apps are free, however there are a few premium apps for which you'll need a license.
- These include:
  - Splunk App for Enterprise Security
  - Splunk App for PCI Compliance
  - Splunk App for VMware
  - Splunk App for Microsoft Exchange

The Splunk Apps



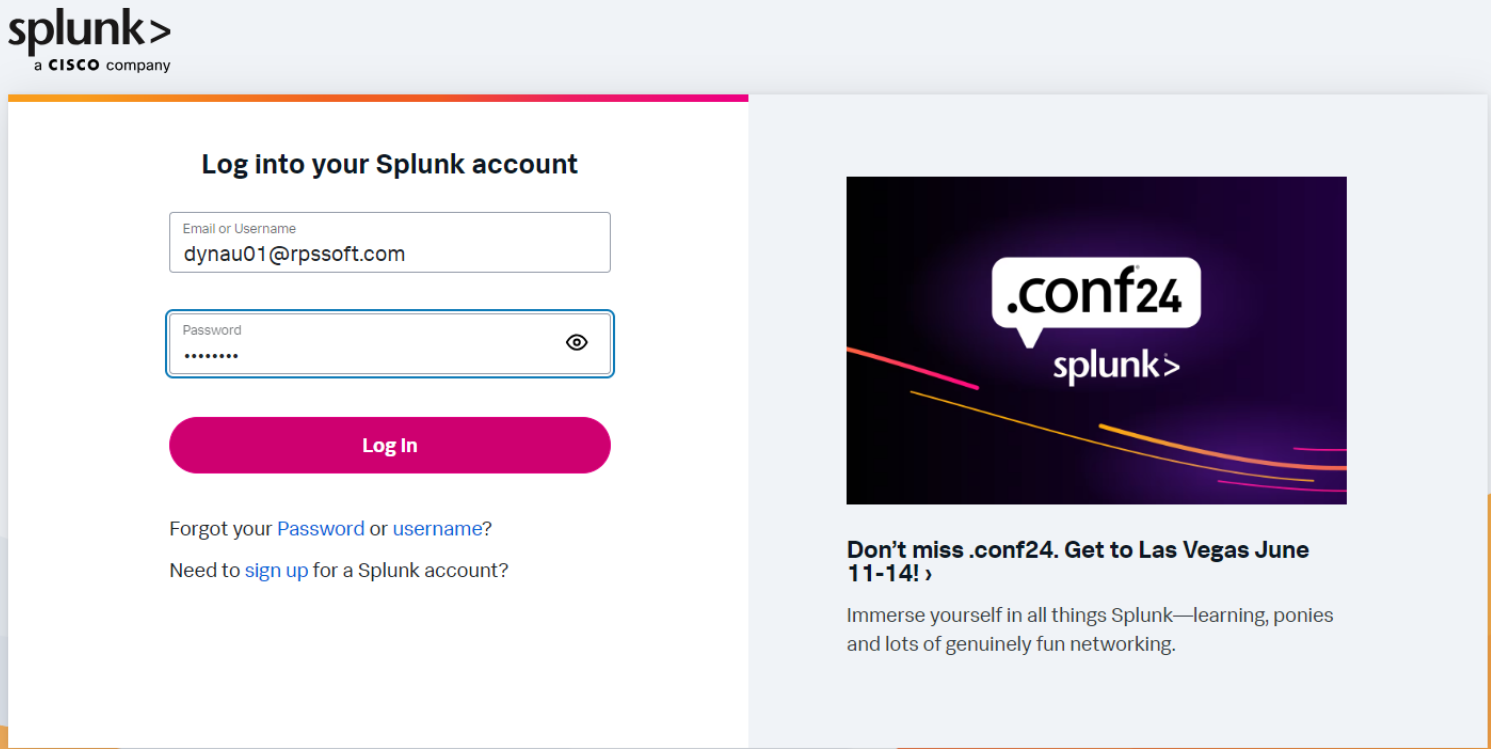
The Splunk Apps



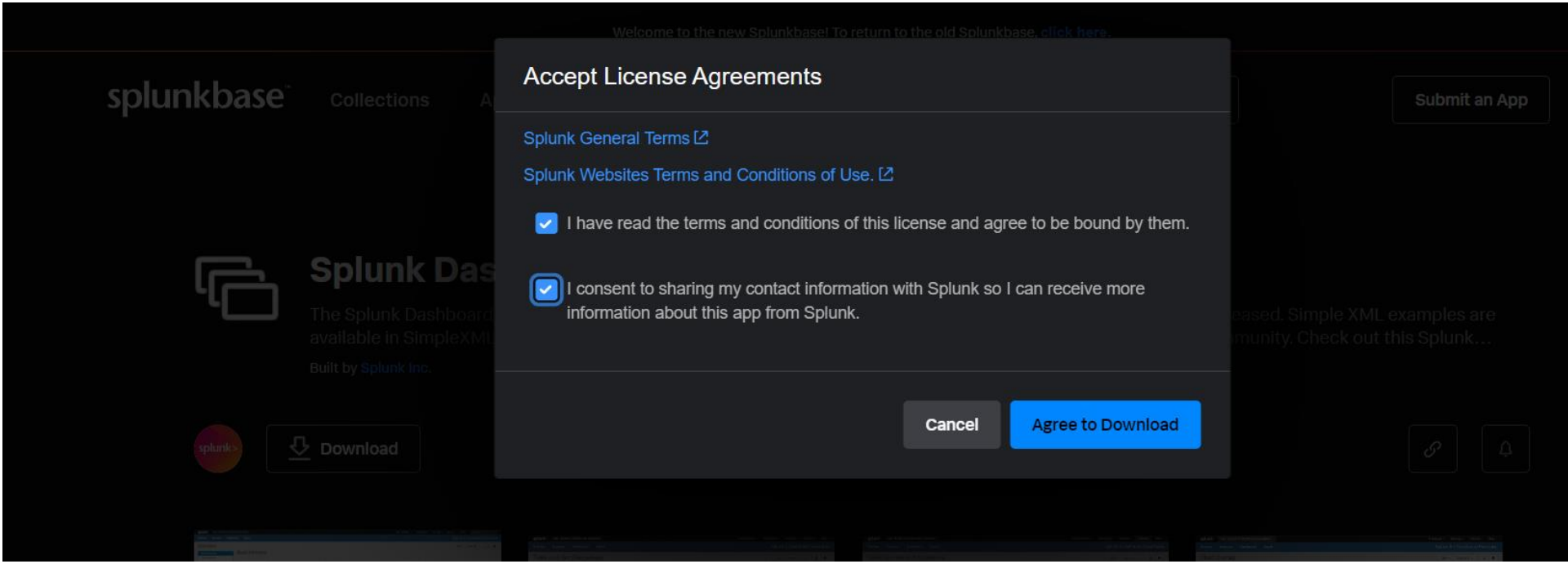
Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkDeploymentServerConfig	SplunkDeploymentServerConfig		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable	
Log Event Alert Action	alert_logevent	9.2.1	Yes	No	App | Permissions	Enabled	Edit properties | View objects
Webhook Alert Action	alert_webhook	9.2.1	Yes	No	App | Permissions	Enabled	Edit properties | View objects
Apps Browser	appsbrowser	9.2.1	Yes	No	App | Permissions	Enabled	Edit properties | View objects
introspection_generator_addon	introspection_generator_addon	9.2.1	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Home	launcher		Yes	Yes	App | Permissions	Enabled	Launch app | Edit properties | View objects
learned	learned		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
legacy	legacy		Yes	No	App | Permissions	Disabled | Enable	
Upgrade Readiness App	python_upgrade_readiness_app	4.3.0	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | View details on Splunkbase
sample data	sample_app		Yes	No	App | Permissions	Disabled | Enable	
Search & Reporting	search	9.2.1	Yes	Yes	App | Permissions	Enabled	Launch app | Edit properties | View objects
Splunk Dashboard Studio	splunk-dashboard-studio	1.13.3	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects
Splunk Assist	splunk_assist	1.0.59	No	No	App | Permissions	Enabled	Edit properties | View objects | View details on Splunkbase
Splunk Get Data In	splunk_gdi	1.0.6	Yes	No	App | Permissions	Enabled	Edit properties | View objects
splunk_httpinput	splunk_httpinput		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Instrumentation	splunk_instrumentation	6.0.10	Yes	Yes	App | Permissions	Enabled	Launch app | Edit properties | View objects

The Splunk Search For Apps

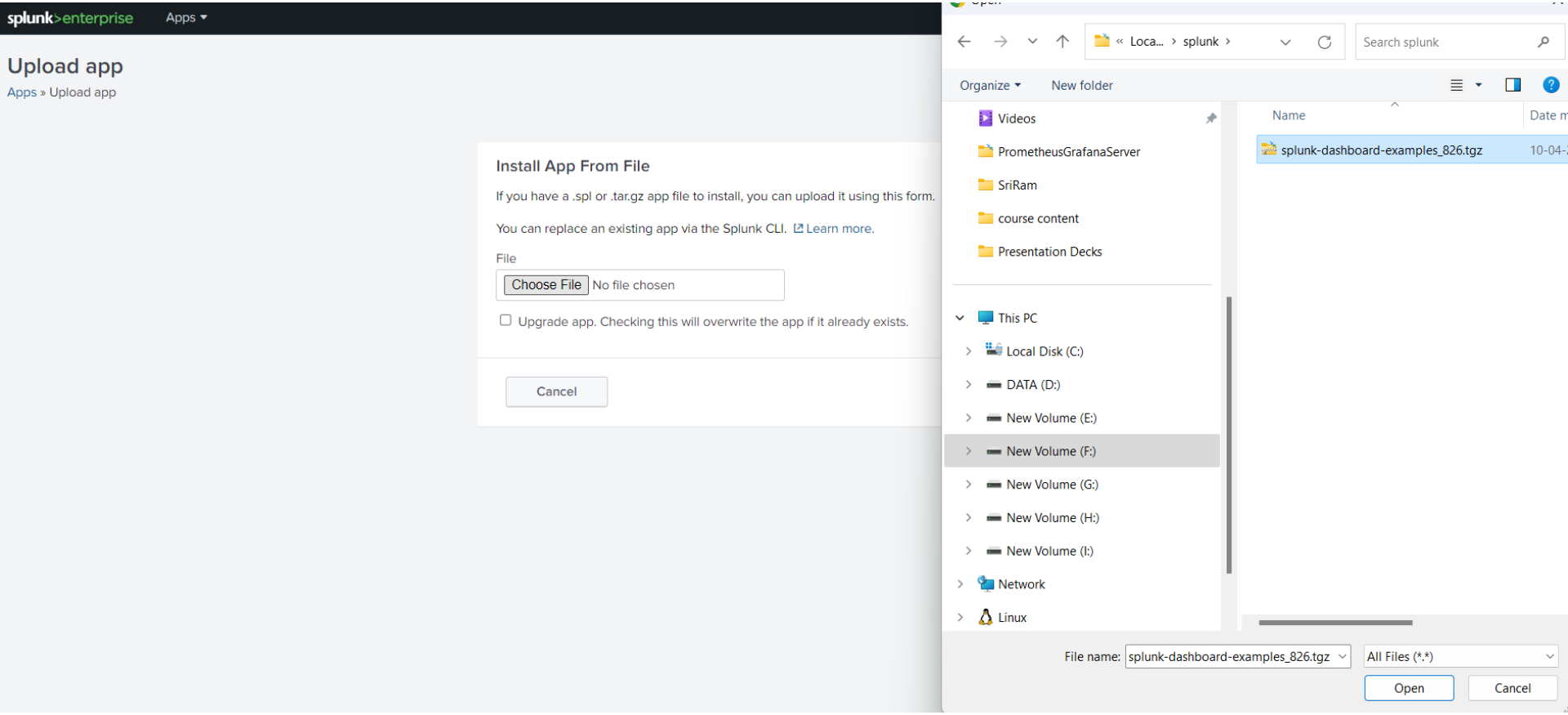
The Splunk Search For Apps



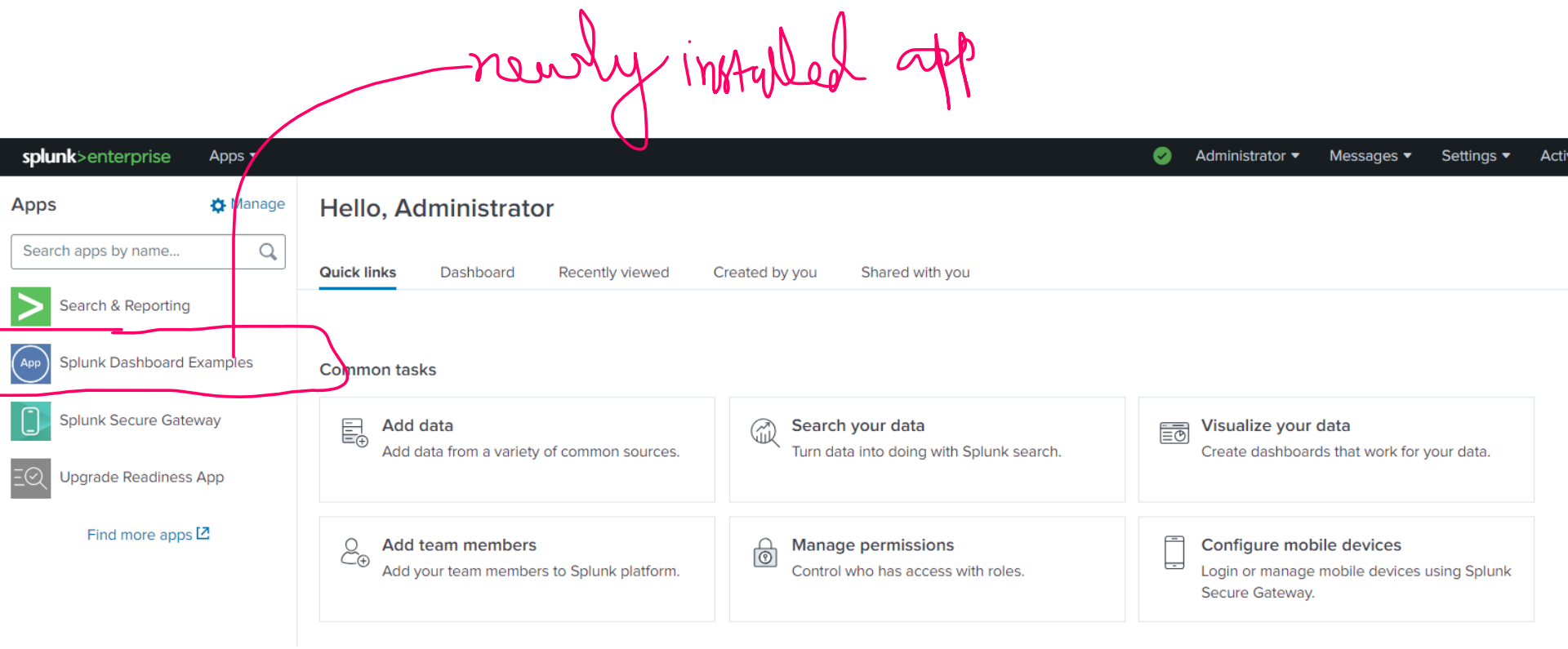
The Splunk Search For Apps



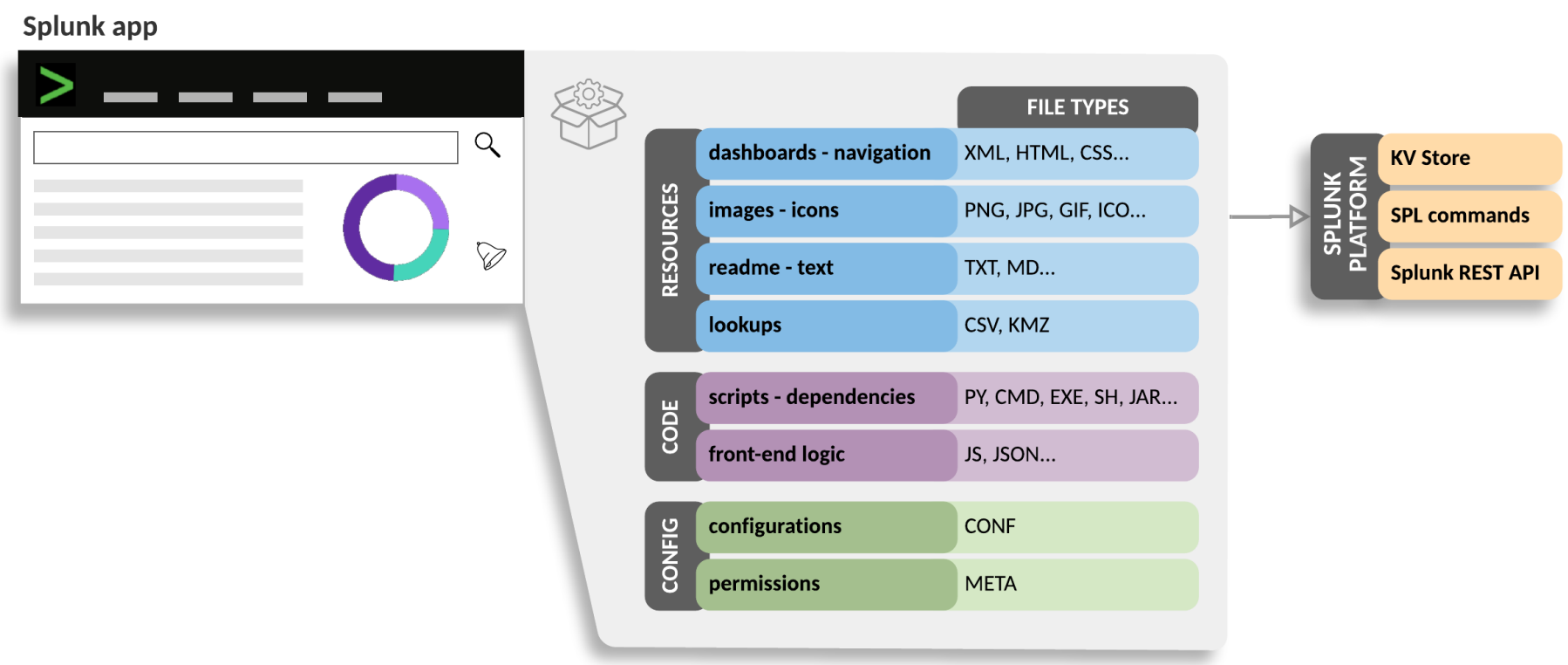
The Splunk Search For Apps



The Splunk Search For Apps

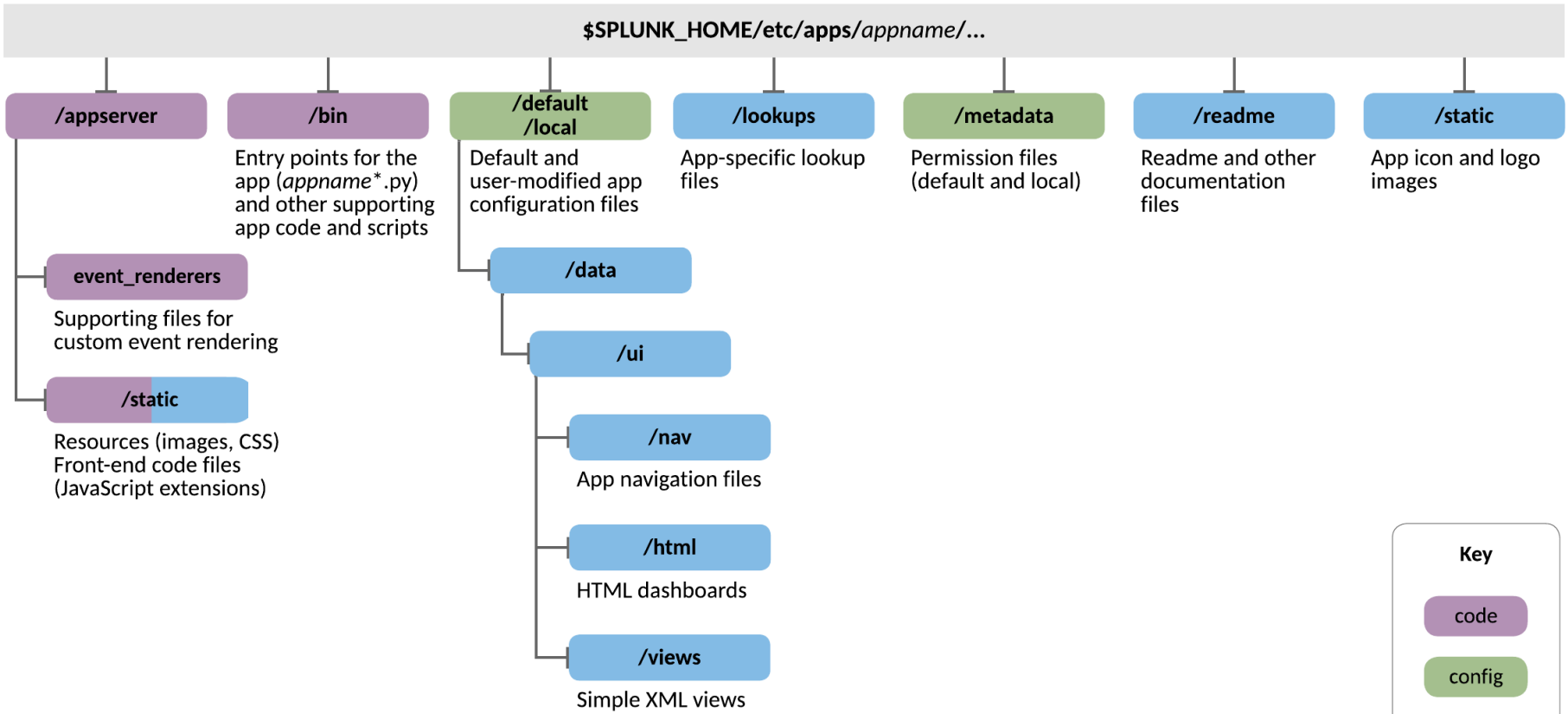


The Splunk Apps



Anatomy of a Splunk app

The Directory Structure of Splunk App



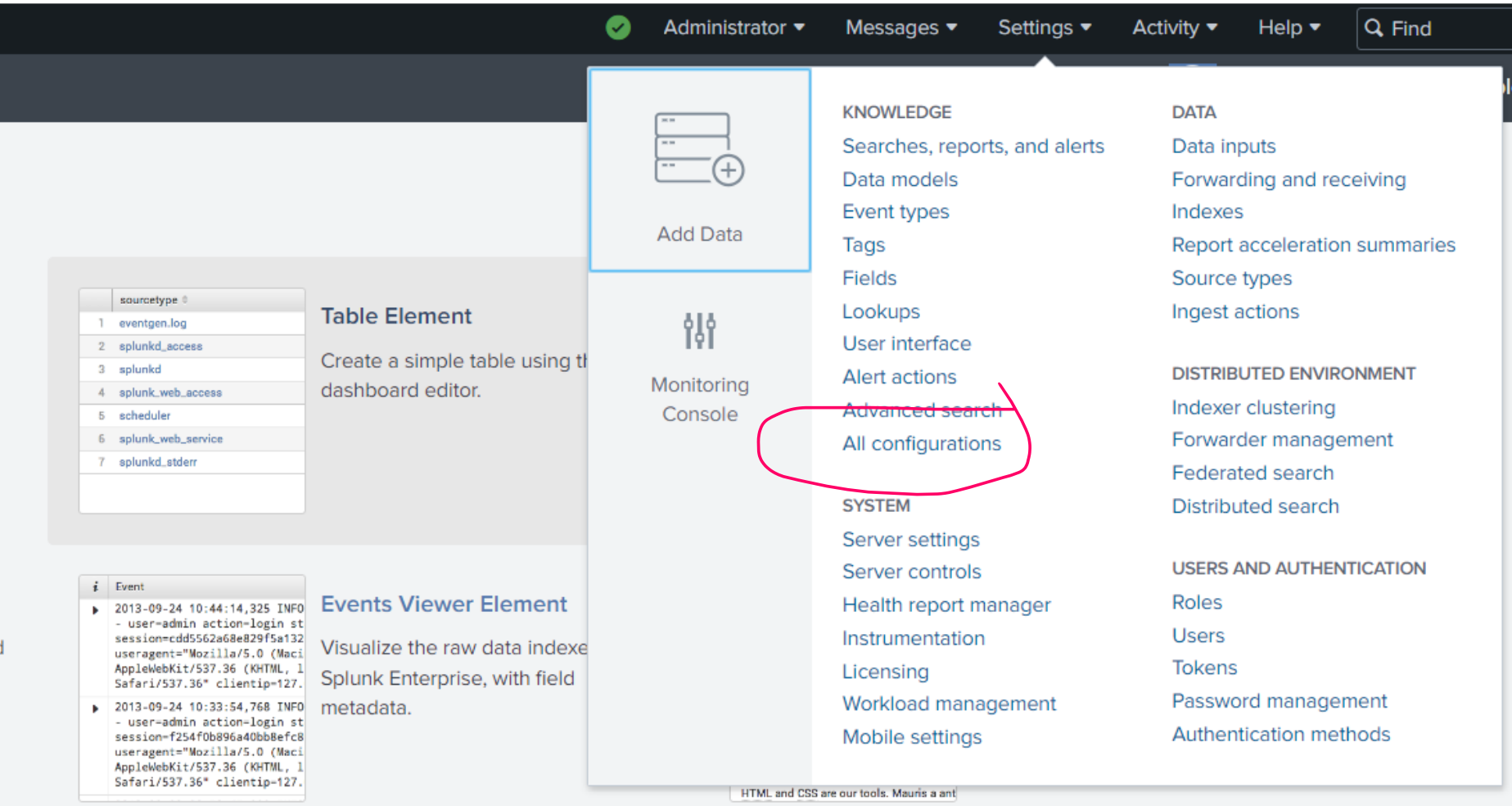
Directory structure of a Splunk app

App permissions and deploying

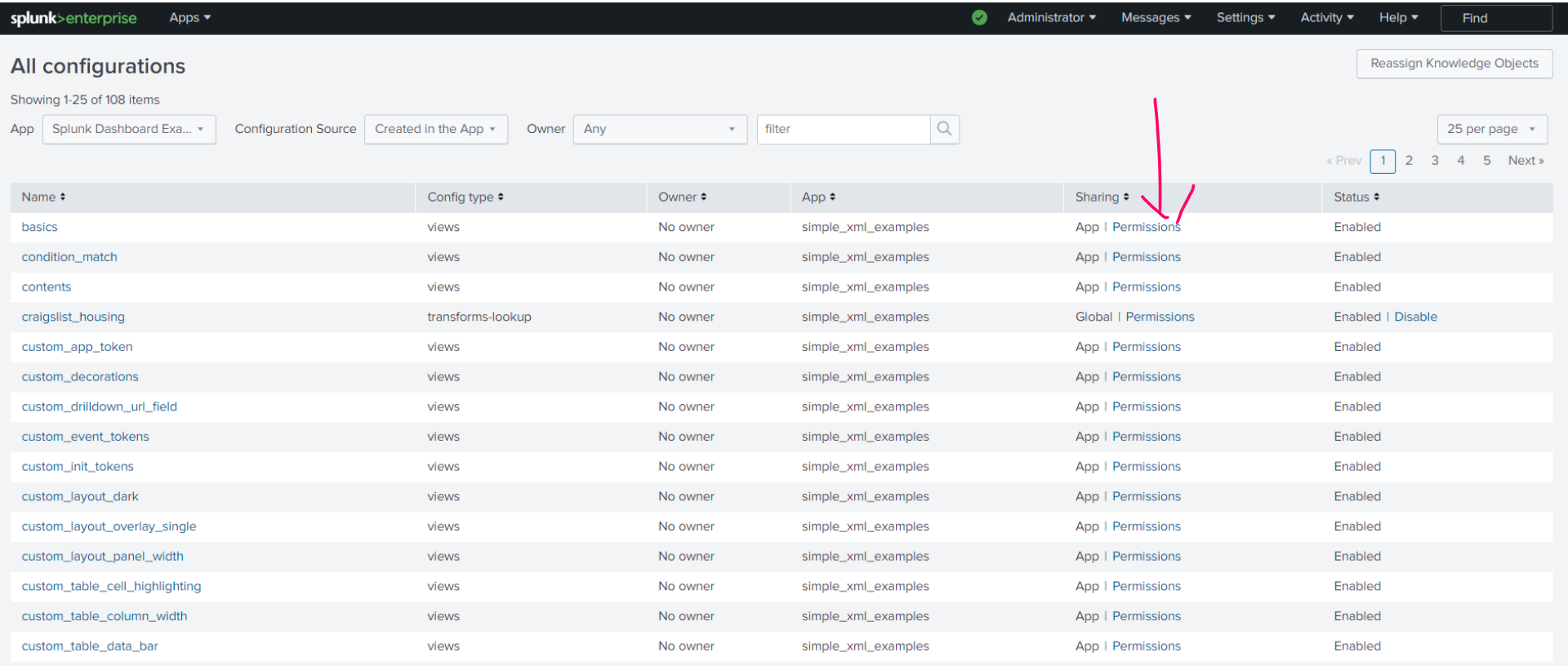
- Set app permissions using Splunk Web
  - During app development, we can use Splunk Web to set permissions on a per-object and per-app basis.
  - These updates are saved in the app's local.meta file.
  - If we want to keep these permissions as part of our released app package, we must migrate them to the default.meta file.

  - In Splunk Web, open your app.
    - Go to Settings > Knowledge, then click a category of objects or click All configurations.
    - Click Permissions for the object for which you want to edit permissions.
    - Select an option for the app context, then set read and write permissions for all the roles listed.
    - Click Save.

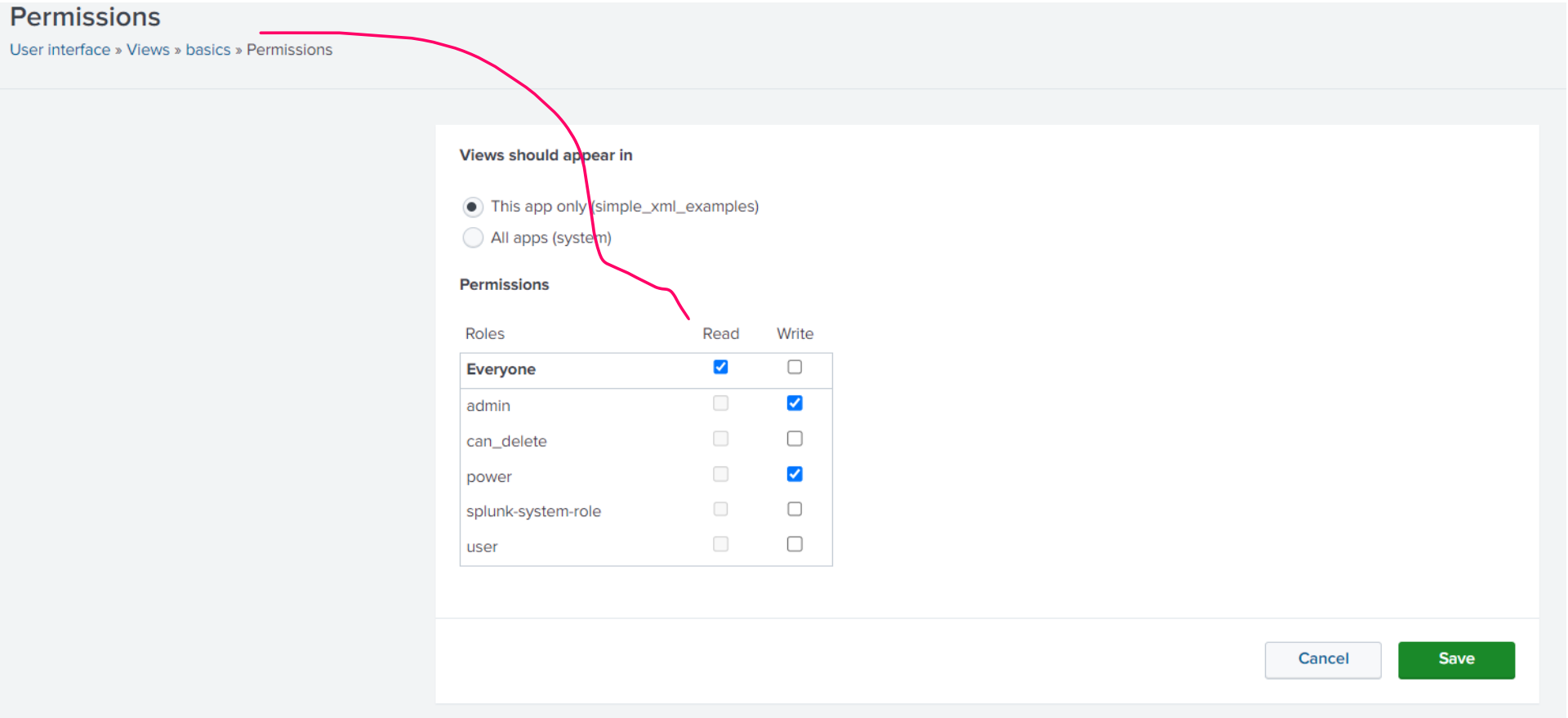
App permissions and deploying



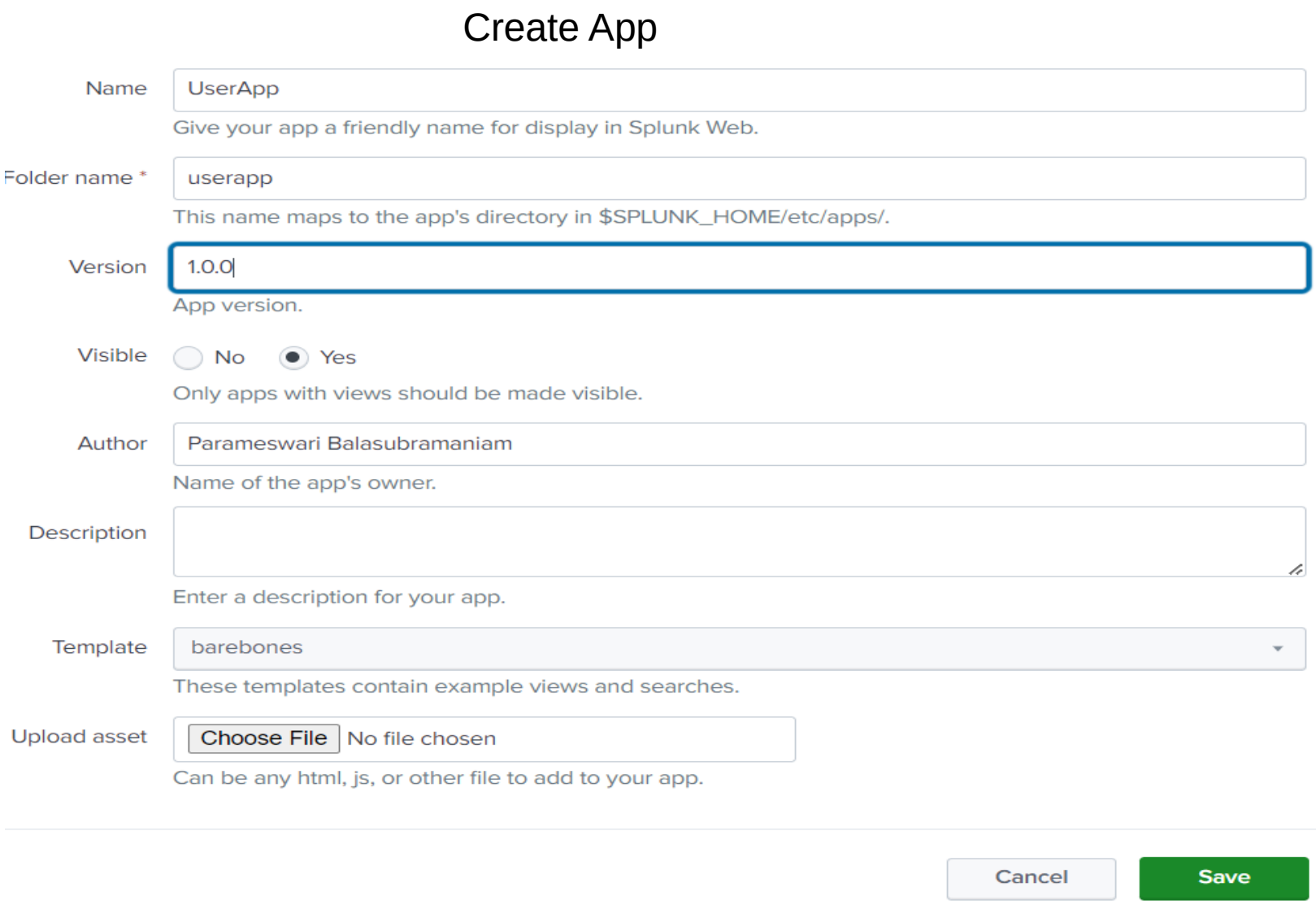
App permissions and deploying



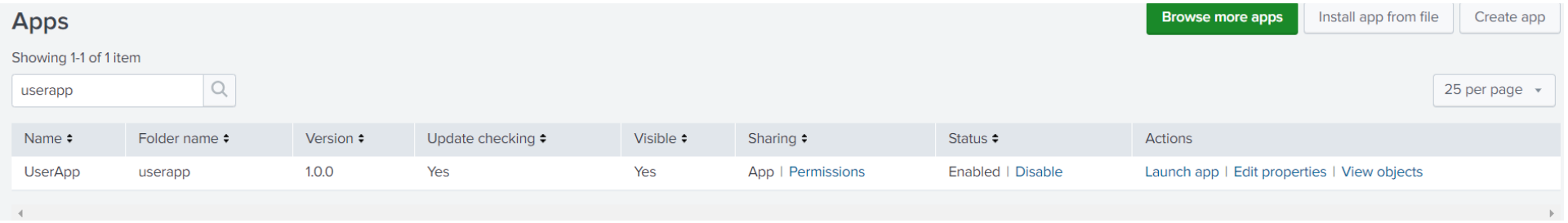
App permissions and deploying

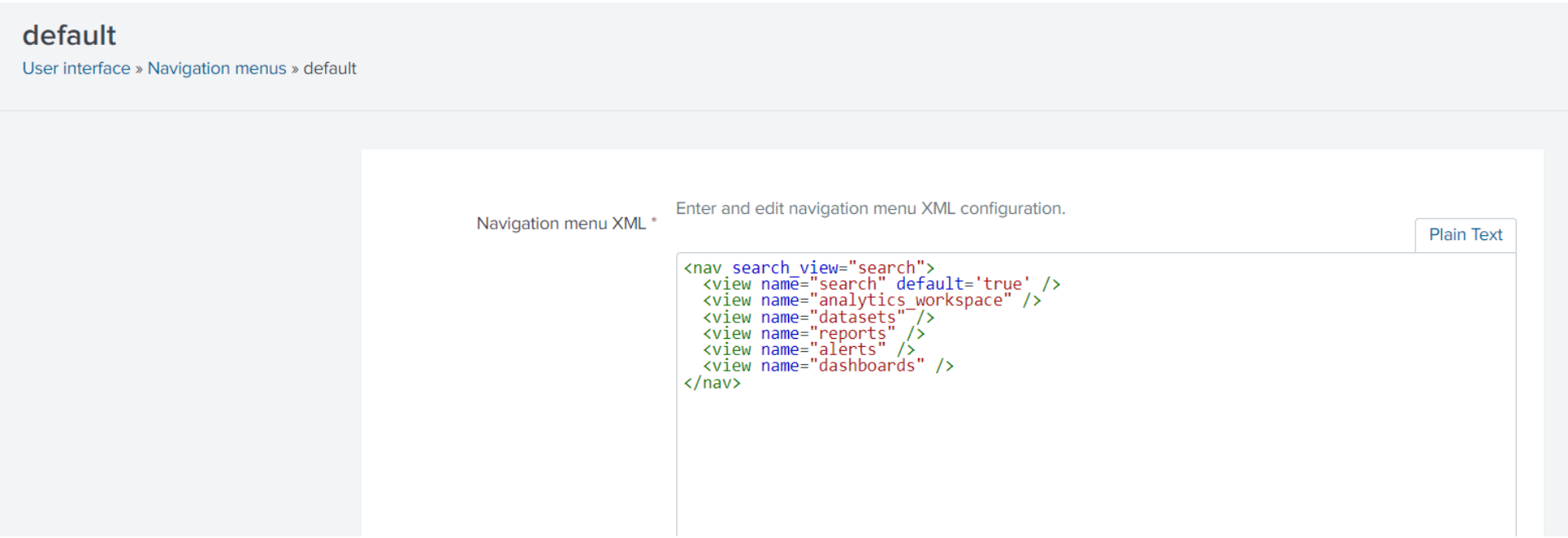


Splunk Scripted App – Create App



Splunk Scripted App – Check App





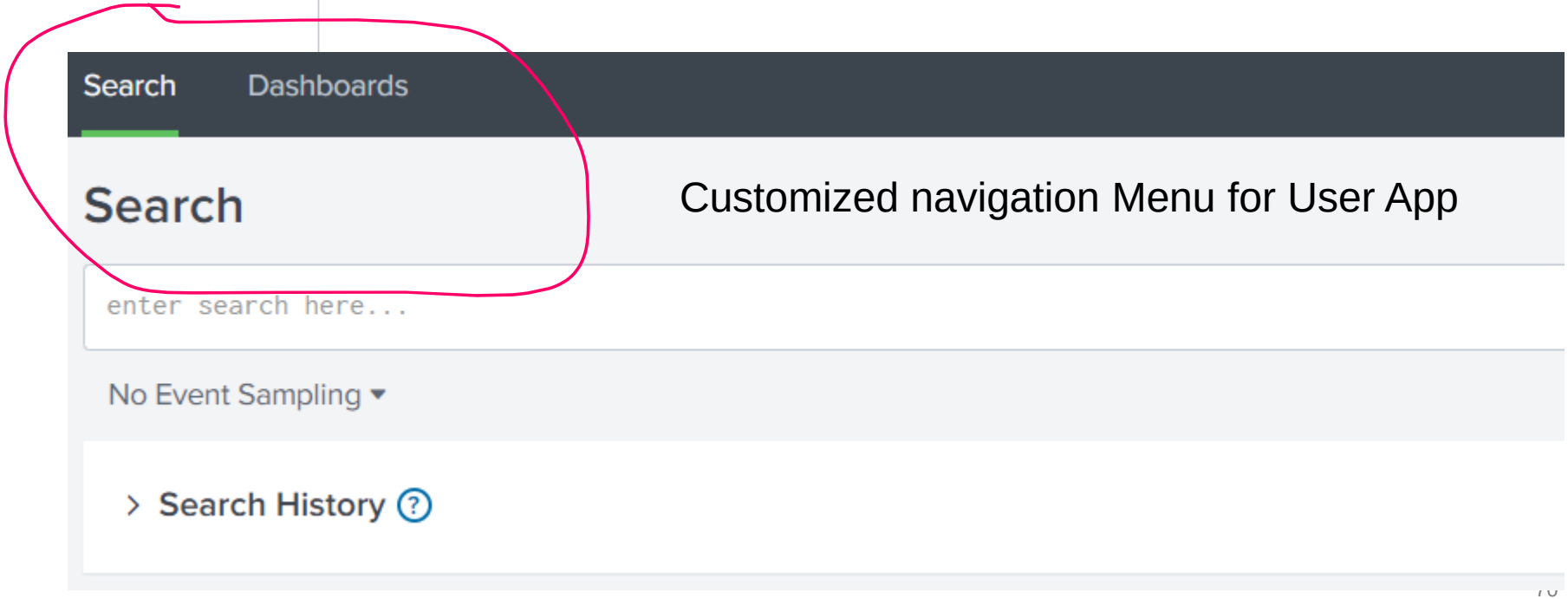
Splunk Scripted App – Check App

Navigation menu XML *

Enter and edit navigation menu XML configuration.

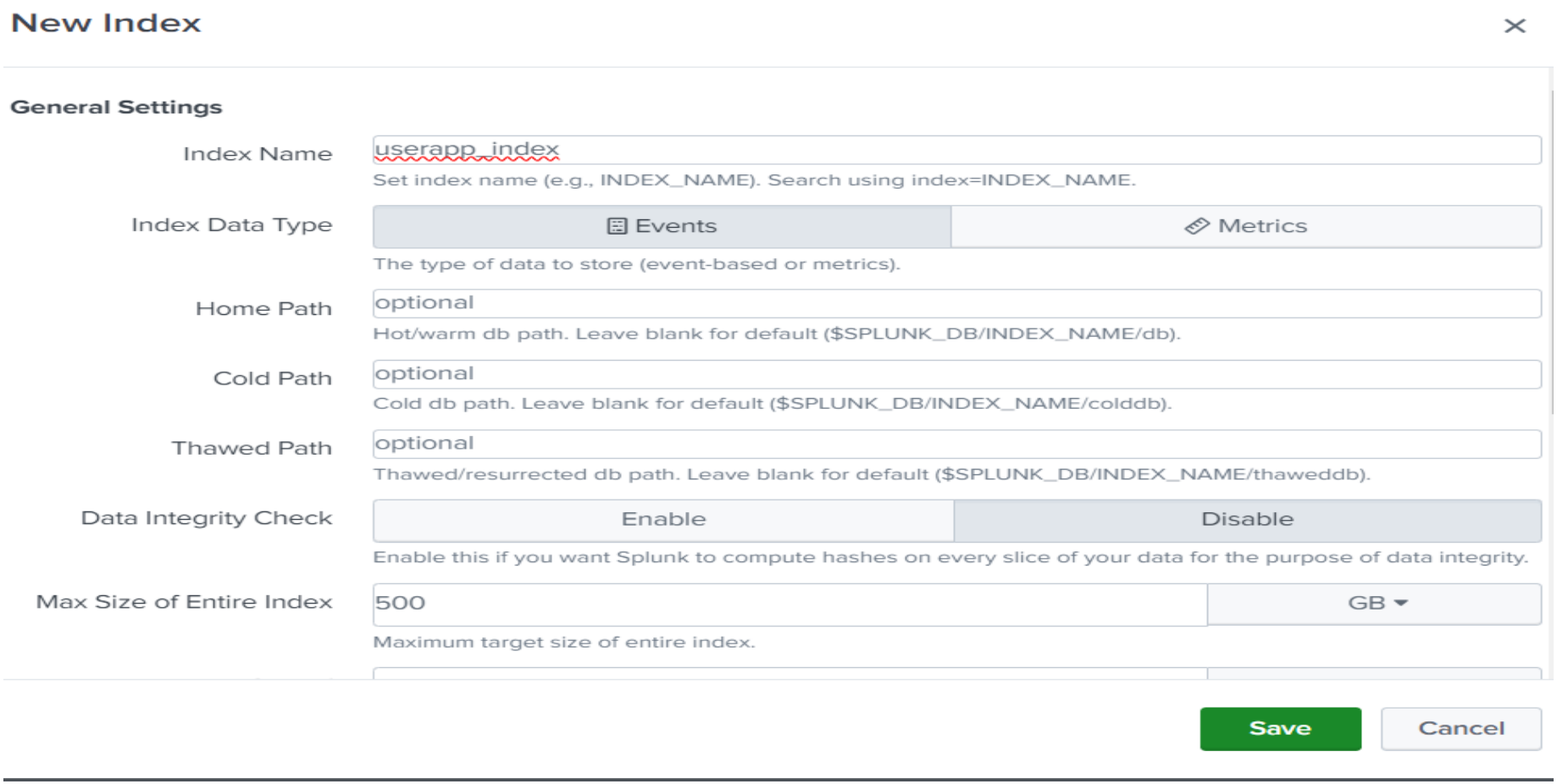
Plain Text

```
<nav search_view="search">
  <view name="search" default='true' />

  <view name="dashboards" />
</nav>
```

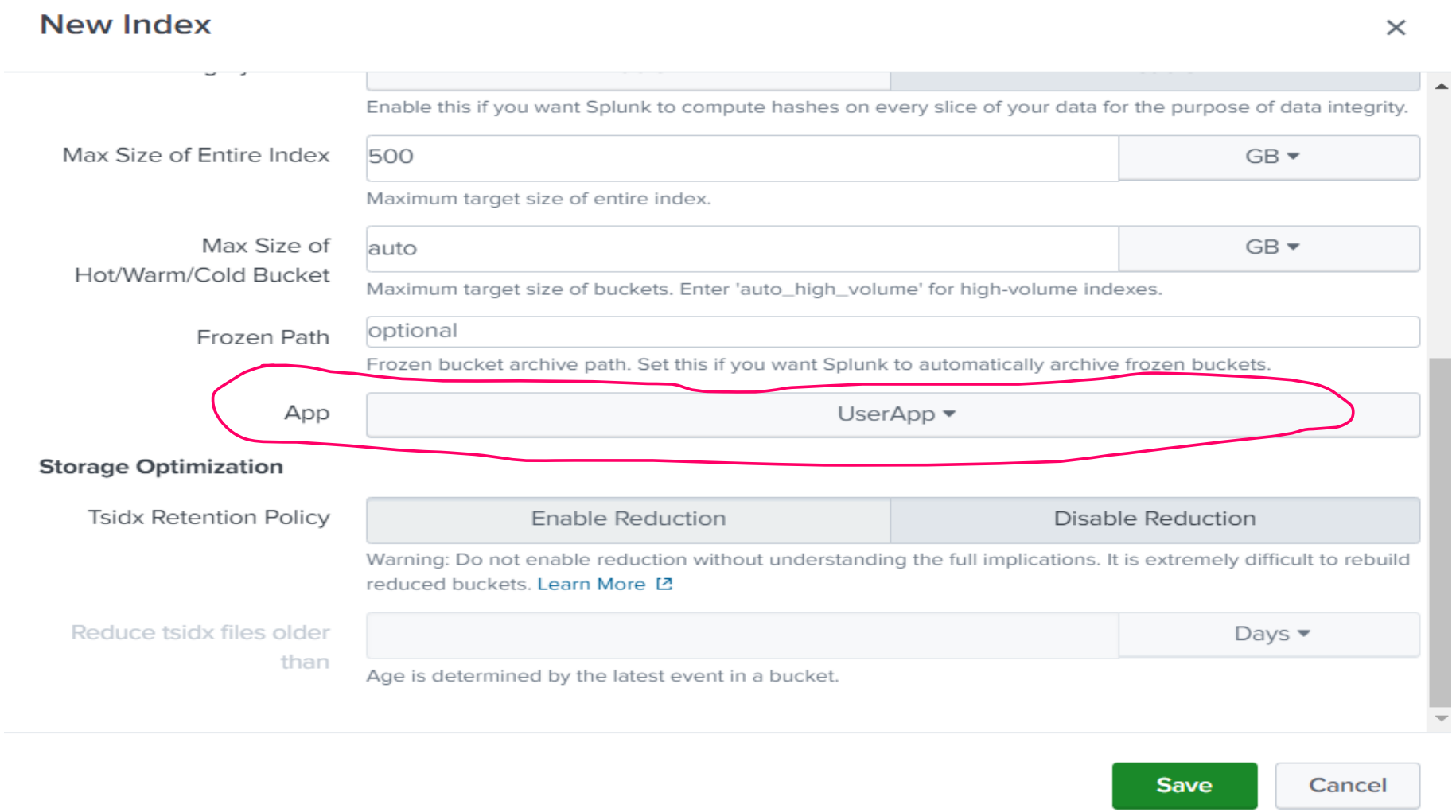


Customized navigation Menu for User App

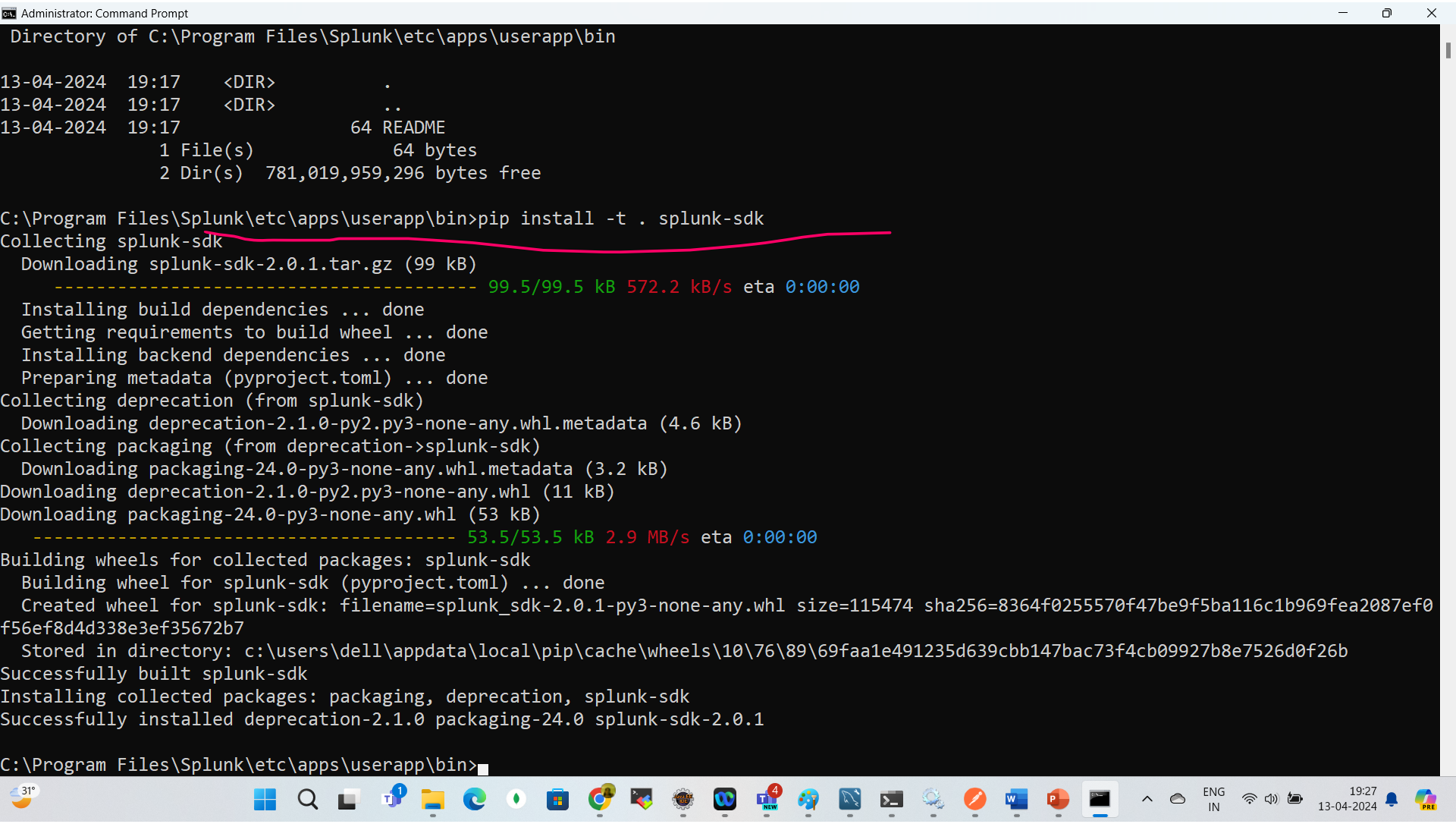
Splunk Scripted App – Check App



Splunk Scripted App – Check App



Splunk Scripted App – Check App

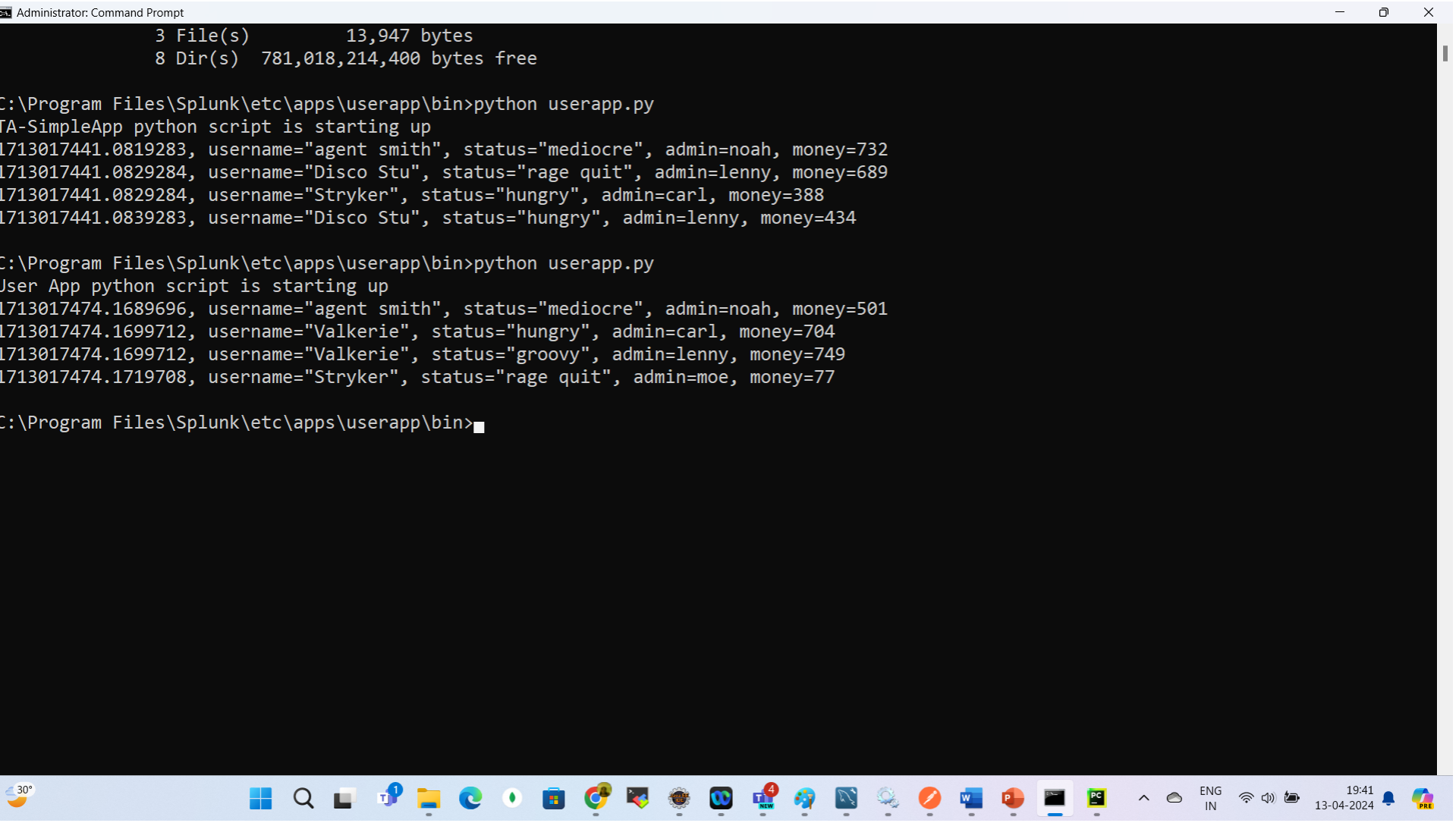


Splunk Scripted App – Check App

userapp.py

```
# So we can run this scipt under python 2 or 3
from __future__ import print_function

import sys  # for sys.stderr.write()
import time  # for strftime
from datetime import datetime  # for datetime.utcnow()
import random  # to provide random data for this example

sys.stderr.write("User App python script is starting up\n")

# output a single event
print(str(time.time()) + ", username=\"agent smith\", status=\"mediocre\", admin=noah, money=" + str(
    random.randint(1, 1000)))

# output three events, each one separated by a newline (each line will be a unique event)
for x in range(0, 3):
    strEvent = str(time.time()) + ", "
    strEvent += "username=\"" + random.choice(["Stryker", "Valkerie", "Disco Stu"]) + "\", "
    strEvent += "status=\"" + random.choice(["groovy", "hungry", "rage quit"]) + "\", "
    strEvent += "admin=" + random.choice(["lenny", "carl", "moe"]) + ", "
    strEvent += "money=" + str(random.randint(1, 1000))
    print(strEvent)
```

Splunk Scripted App – Check App

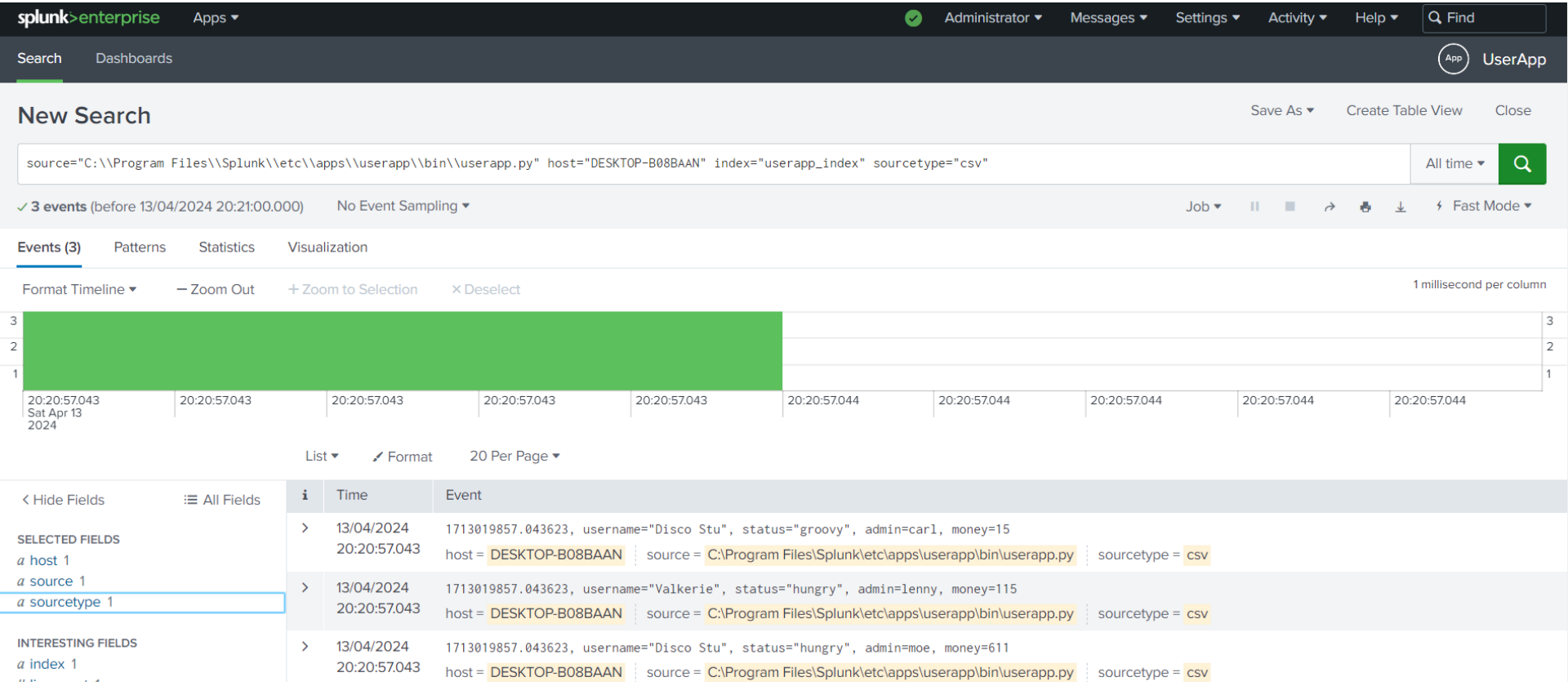


Splunk Scripted App – Check App

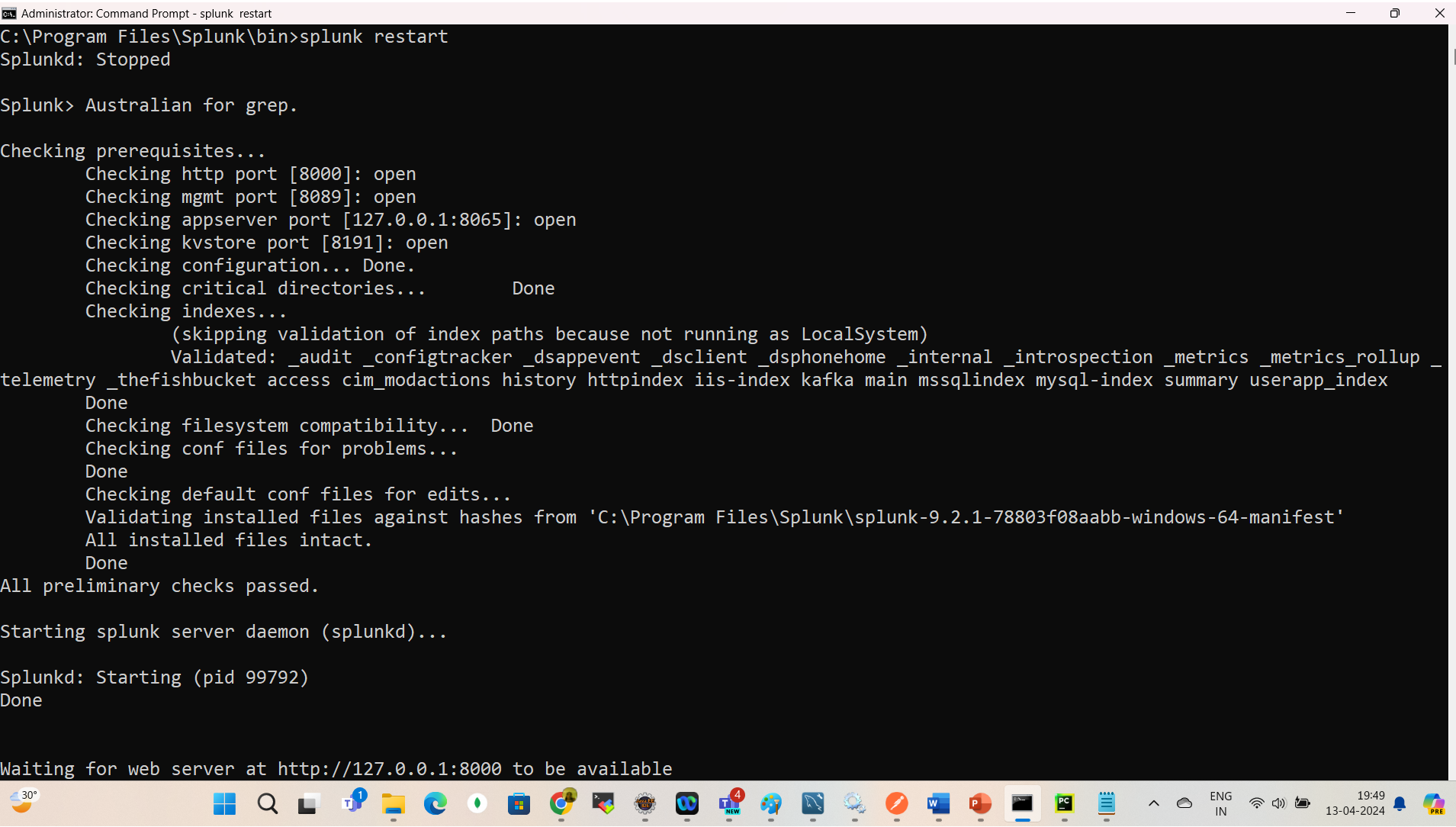
Review

Input Type	Script
Command	$SPLUNK_HOME\etc\apps\userapp\bin\userapp.py
Interval	60.0
Source name override	N/A
Source Type	csv
App Context	userapp
Host	DESKTOP-B08BAAN
Index	userapp_index

Splunk Scripted App – Check App



Splunk Scripted App – Check App



Splunk Addon

- An add-on offers unique features for helping to collect, standardize, and enrich data sources. It may include the following features or all of them:
  - Data source input configurations.
  - Splunk Business data sorting and transformation settings for structuring the data.
  - Lookup files for data enrichment.
  - Supporting knowledge objects.

Download, configure, and install the Splunk Add-on for Windows

- Download the Splunk Add-on for Windows.
- Unarchive the downloaded file into an accessible location.
- Configure the Splunk Add-on for Windows.
- Enable the input stanzas for the Windows data that you want the add-on to collect.
- After enabling input stanzas, copy the Splunk Add-on for Windows folder to %SPLUNK_HOME%\etc\deployment-apps on the deployment server (the Splunk Enterprise instance that runs Forwarder Management.)
- Restart Splunk Enterprise on the deployment server.
- Write down the host name or IP address and management port of the deployment server. You need it later to configure deployment clients.

Types of forwarders in Splunk

- A forwarder is any Splunk Enterprise instance that forwards data to another Splunk Enterprise instance, such as:
  - An Indexer
  - Another forwarder
  - A third-party system (heavy forwaders only)

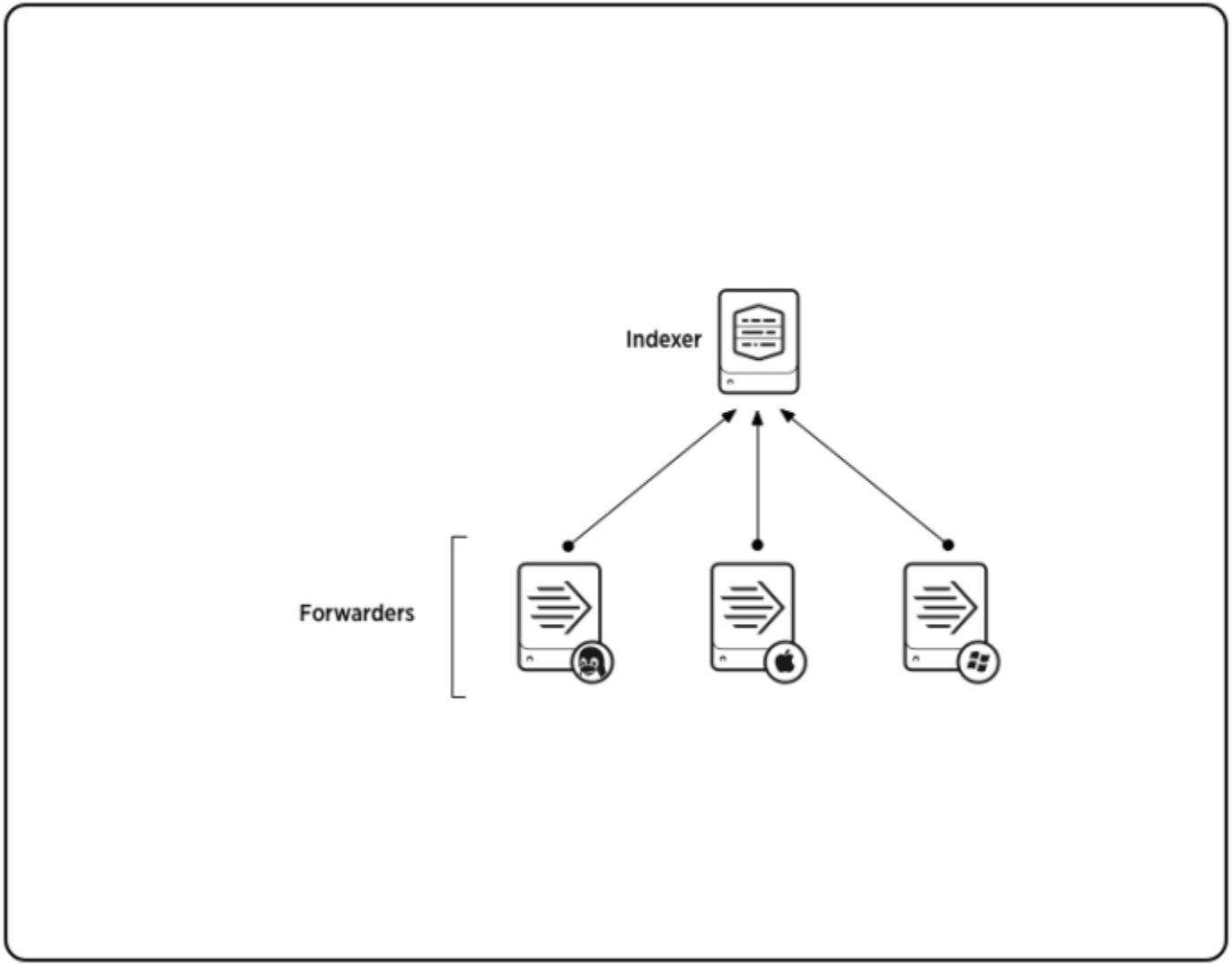
Types of forwarders in Splunk

- Splunk Enterprise has three types of forwarders:
  - A universal forwarder contains only the components required for forwarding data, nothing more, nothing less.
    - In general, it is the best tool for sending data to indexers.
  - A heavy forwarder is a full Splunk Enterprise instance that can index, search, change and forward data.
    - Certain features from a full Splunk Enterprise instance are disabled in order to reduce system resource use.
  - A light forwarder is also a full Splunk Enterprise instance, with even more features disabled to achieve as small a resource footprint as possible.
    - Deprecated as of Splunk Enterprise version 6.0, the light forwarder is replaced by the universal forwarder for almost all purposes.

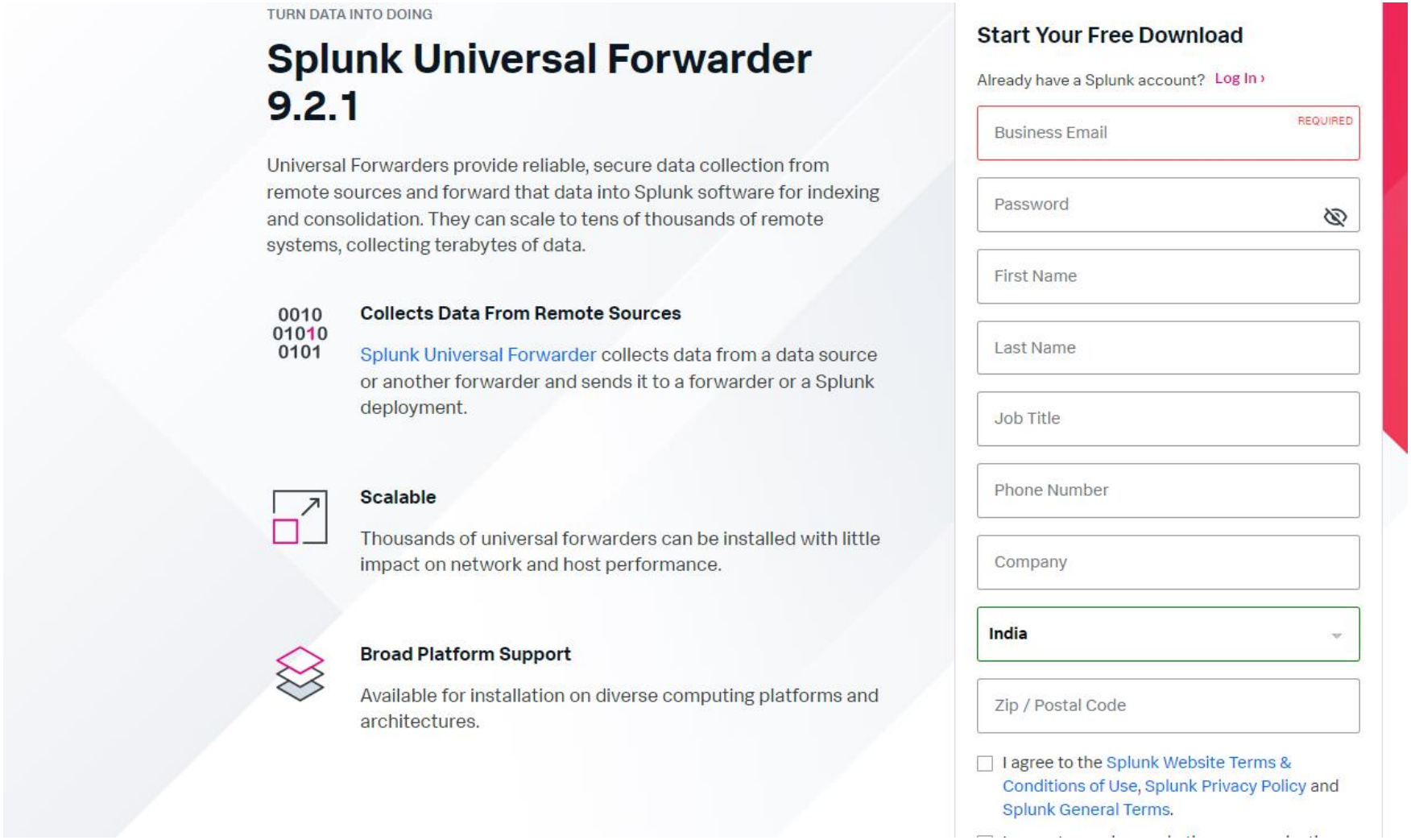
How a universal forwarder works

- A universal forwarder collects data from a variety of places — whether data sources or other forwarders — and then sends it to a forwarder or a Splunk deployment.
- So, what can you do with universal forwarders? Capabilities include:
  - Tagging metadata (source, source type and host)
  - Configuring buffering
  - Compressing data
  - Securing via SSL
  - Using any available network ports

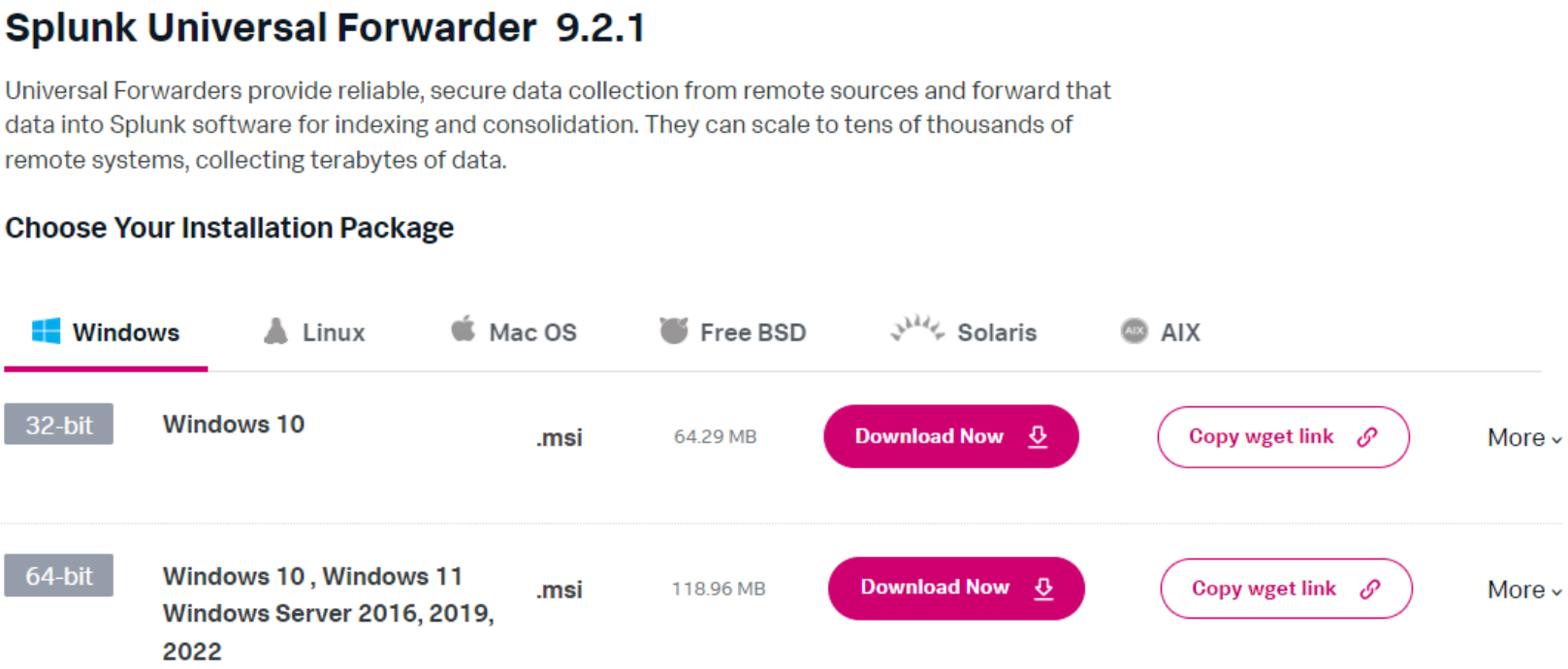
How a universal forwarder works



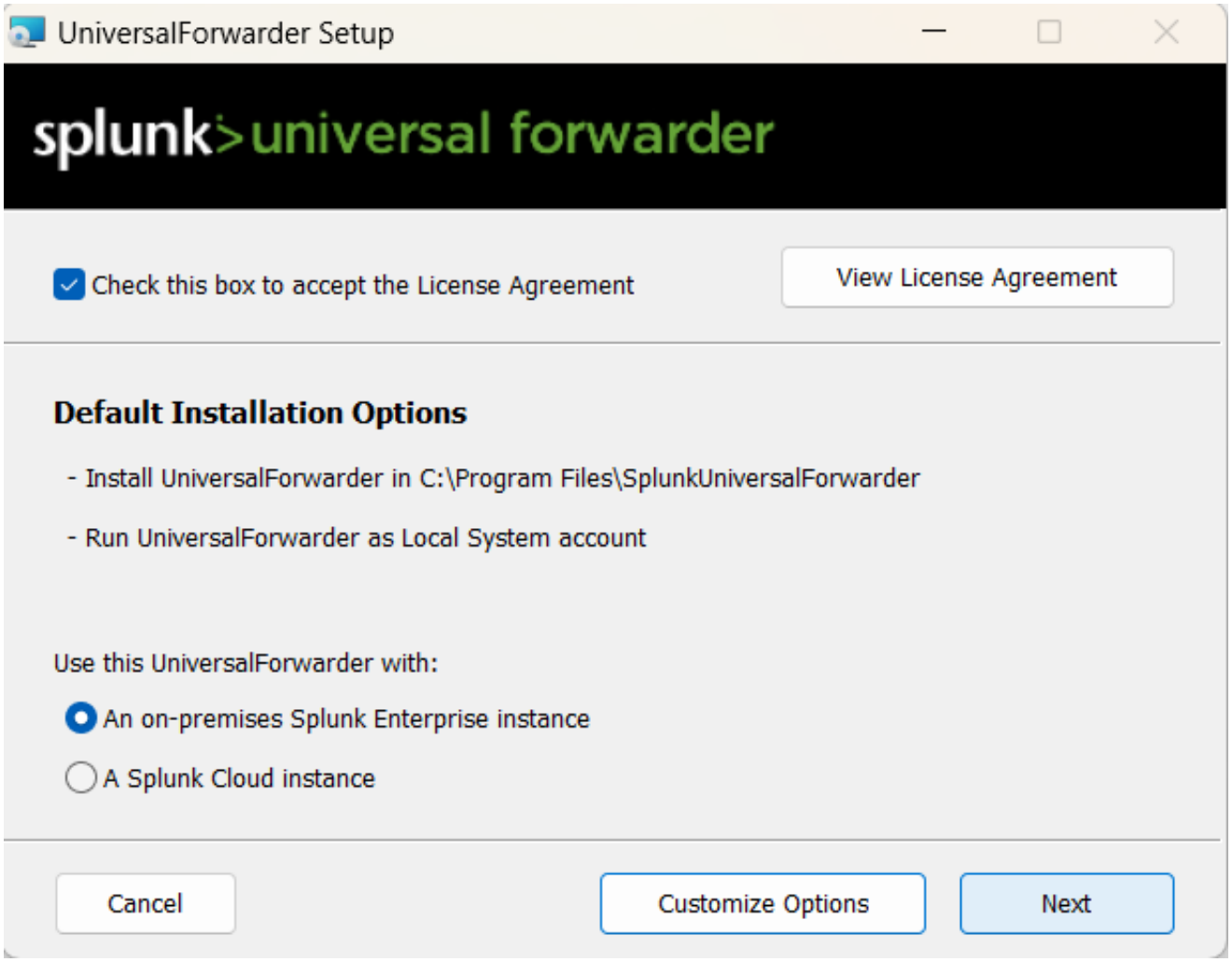
Obtain Splunk Universal Forwarder



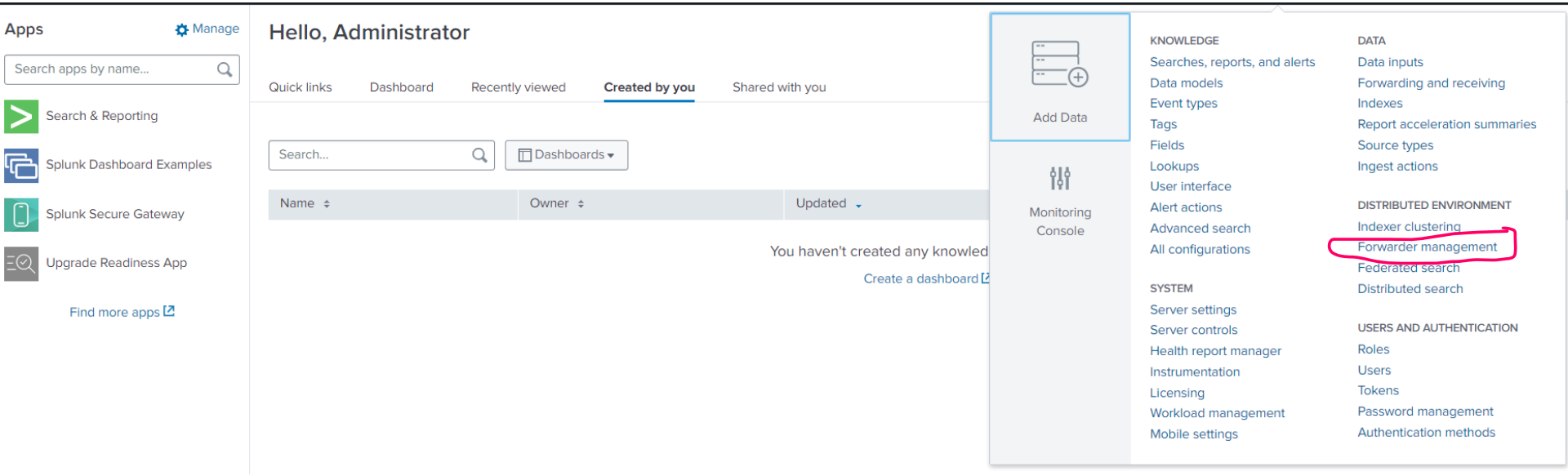
Obtain Splunk Universal Forwarder



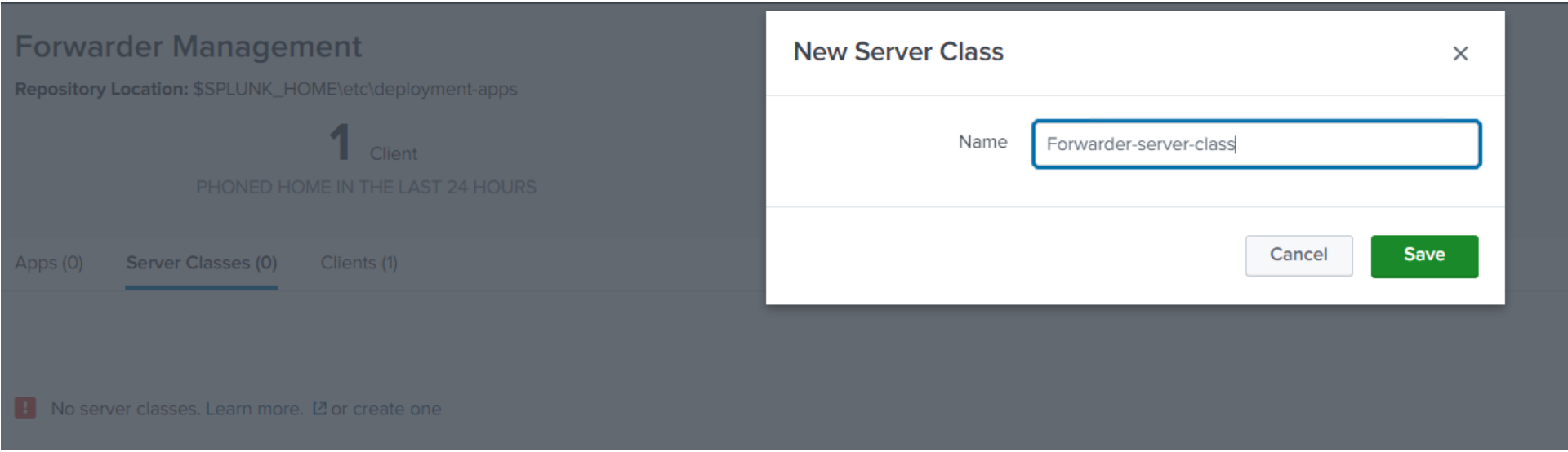
Obtain Splunk Universal Forwarder



Splunk Universal Forwarder After Installation



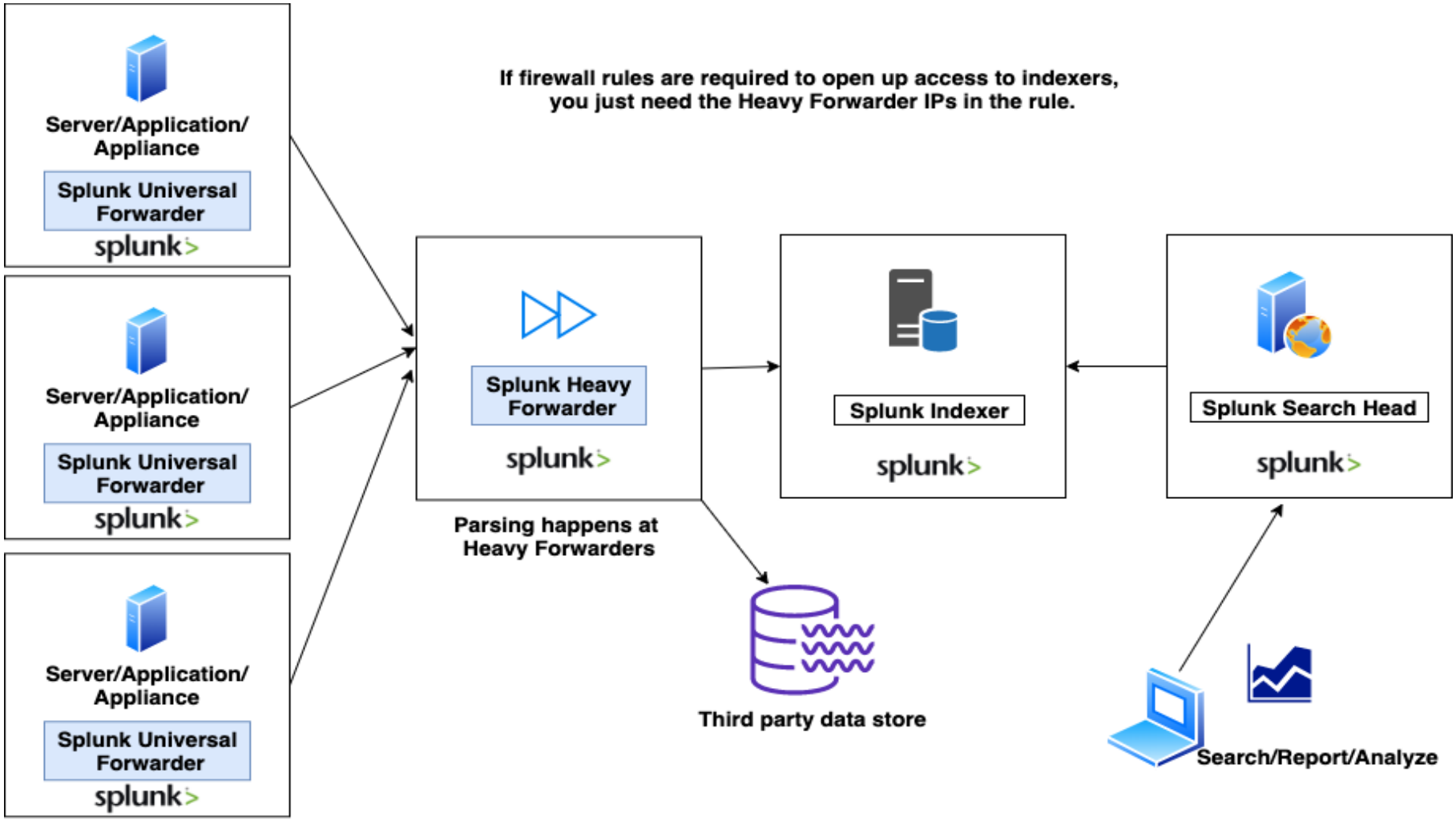
Splunk Universal Forwarder Server Class



Splunk list app

```
ples.

C:\Windows\System32>splunk list app
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for
details.
Your session is invalid.  Please login.
Splunk username: dynau01@rpssoft.com
Password:
alert_logevent                CONFIGURED         ENABLED            INVISIBLE
alert_webhook                 CONFIGURED         ENABLED            INVISIBLE
appsbrowser                   CONFIGURED         ENABLED            INVISIBLE
introspection_generator_addon CONFIGURED         ENABLED            INVISIBLE
launcher                      CONFIGURED         ENABLED            VISIBLE
learned                       UNCONFIGURED       ENABLED            INVISIBLE
legacy                        UNCONFIGURED       DISABLED           INVISIBLE
python_upgrade_readiness_app  UNCONFIGURED       ENABLED            VISIBLE
sample_app                    UNCONFIGURED       DISABLED           INVISIBLE
search                        CONFIGURED         ENABLED            VISIBLE
simple_xml_examples           CONFIGURED         ENABLED            VISIBLE
splunk-dashboard-studio       CONFIGURED         ENABLED            VISIBLE
splunk_assist                 CONFIGURED         ENABLED            INVISIBLE
splunk_gdi                    UNCONFIGURED       ENABLED            INVISIBLE
splunk_httpinput              UNCONFIGURED       ENABLED            INVISIBLE
splunk_instrumentation        UNCONFIGURED       ENABLED            VISIBLE
splunk_internal_metrics       UNCONFIGURED       ENABLED            INVISIBLE
splunk_metrics_workspace      UNCONFIGURED       ENABLED            VISIBLE
splunk_monitoring_console     UNCONFIGURED       ENABLED            VISIBLE
splunk_secure_gateway         UNCONFIGURED       ENABLED            VISIBLE
SplunkDeploymentServerConfig  UNCONFIGURED       ENABLED            INVISIBLE
SplunkForwarder               UNCONFIGURED       DISABLED           INVISIBLE
```

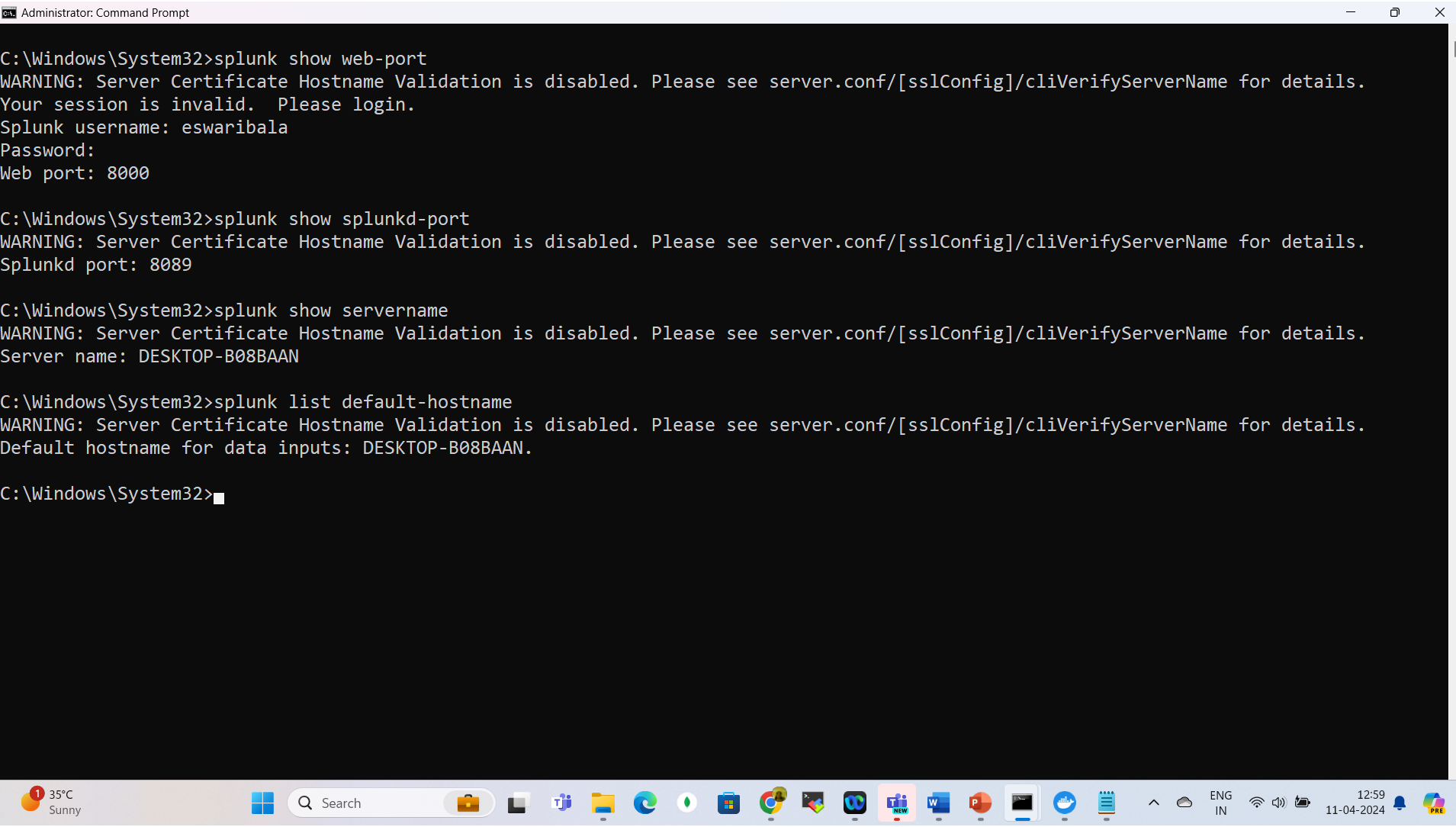
Splunk Heavy Forwarder



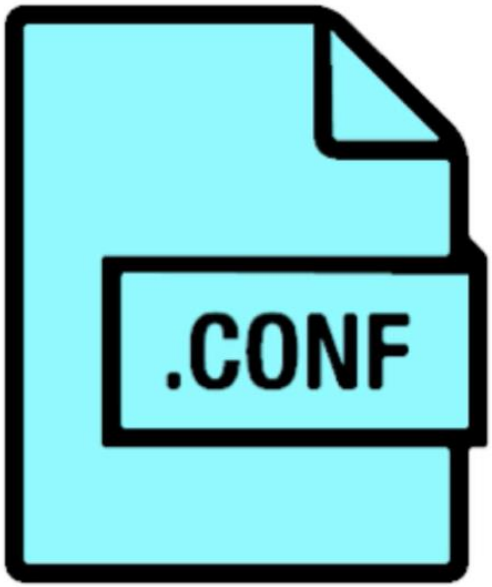
Splunk Universal vs Heavy Forwarder

Universal Forwarder	Heavy Forwarder
Splunk Universal Forwarder binary	Splunk Enterprise binary (used by Indexers, Search Heads and other Splunk processes)
Collects and sends data to Indexers or Heavy Forwarders	Receives data from Universal Forwarders and sends it to Indexers, or other third party data stores. Acts as intermediary in routing data
Does not parse data (except when the data is structured such as CSV)	Parses data, which includes Line breaking, timestamp extraction and extracting index-time fields
Cannot index data	Can optionally index data
Built-in license. No additional license required	Forwarder license required. Requires access to Enterprise license stack if indexing is required.

Splunk Cli


Administrator: Command Prompt
C:\Windows\System32>splunk show web-port
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Your session is invalid. Please login.
Splunk username: eswaribala
Password:
Web port: 8000
C:\Windows\System32>splunk show splunkd-port
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Splunkd port: 8089
C:\Windows\System32>splunk show servername
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Server name: DESKTOP-B08BAAN
C:\Windows\System32>splunk list default-hostname
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Default hostname for data inputs: DESKTOP-B08BAAN.
C:\Windows\System32>
35°C
Sunny
Search
ENG
IN
12:59
11-04-2024

Splunk Configuration Files



Splunk runs on configuration (.conf) files

- Every behavior and function within Splunk is defined in a .conf file

Multiple copies of the same configuration file

- Evaluated by Splunk based on precedence

Common Configuration Files

`inputs.conf`

- Governs data inputs such as forwarders and file system monitoring

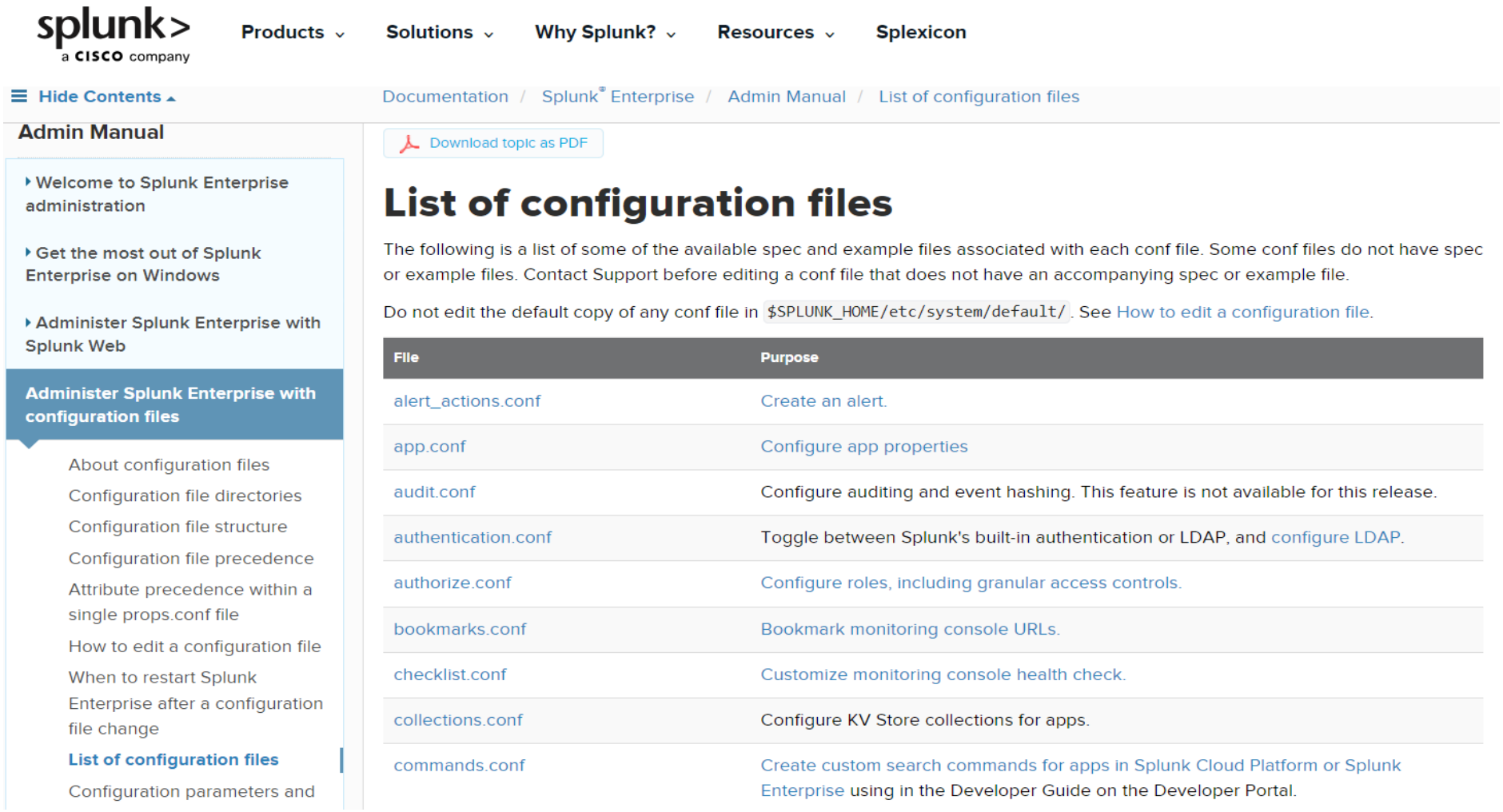
`props.conf`

- Governs indexing property behavior

`transforms.conf`

- Settings and values that govern data transformation

Common Configuration Files



splunk> a cisco company

Products Solutions Why Splunk? Resources Splexicon

Hide Contents

Documentation / Splunk® Enterprise / Admin Manual / List of configuration files

Admin Manual

- Welcome to Splunk Enterprise administration
- Get the most out of Splunk Enterprise on Windows
- Administer Splunk Enterprise with Splunk Web
- **Administer Splunk Enterprise with configuration files**
  - About configuration files
  - Configuration file directories
  - Configuration file structure
  - Configuration file precedence
  - Attribute precedence within a single props.conf file
  - How to edit a configuration file
  - When to restart Splunk Enterprise after a configuration file change
  - **List of configuration files**
  - Configuration parameters and

Download topic as PDF

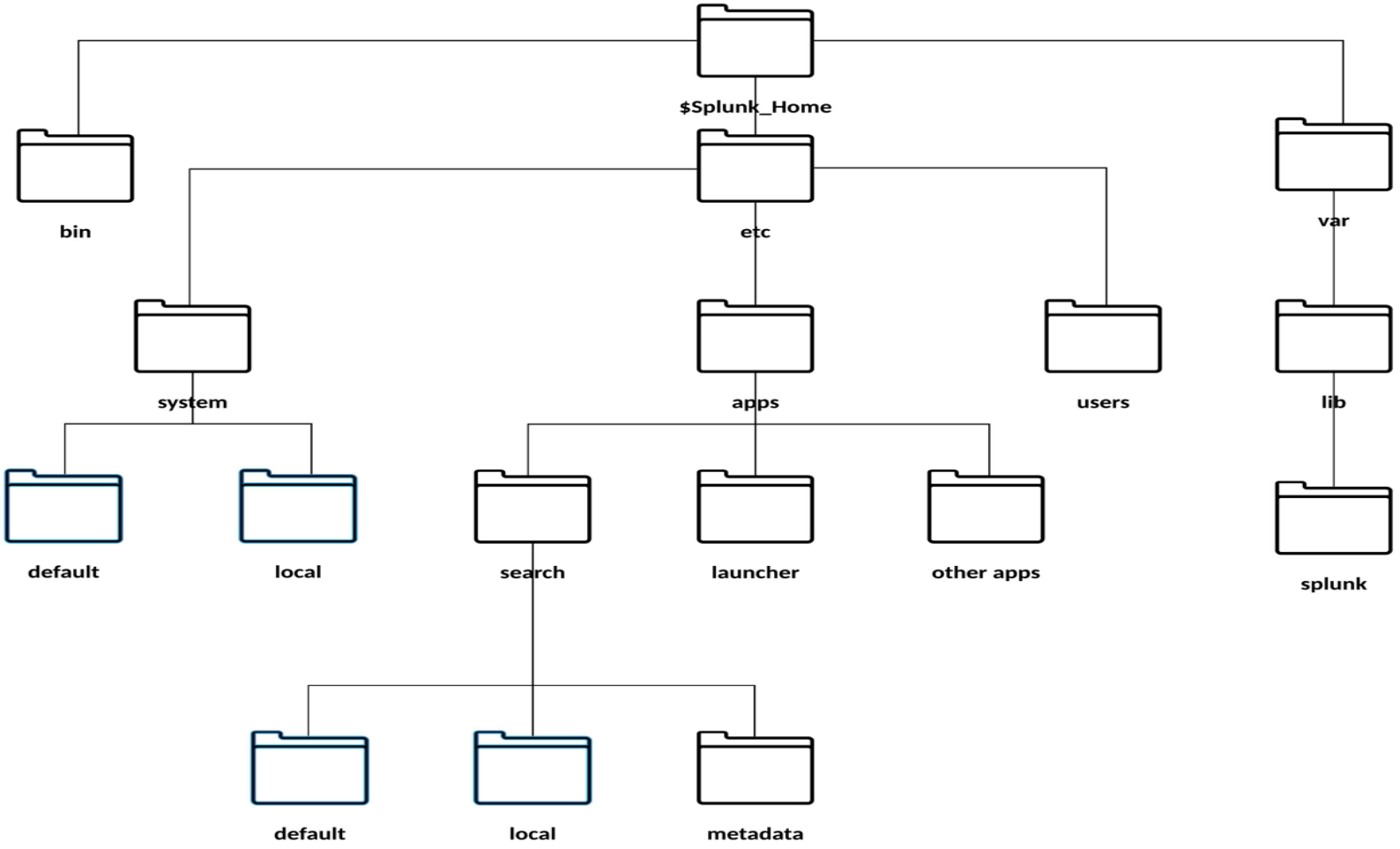
List of configuration files

The following is a list of some of the available spec and example files associated with each conf file. Some conf files do not have spec or example files. Contact Support before editing a conf file that does not have an accompanying spec or example file.

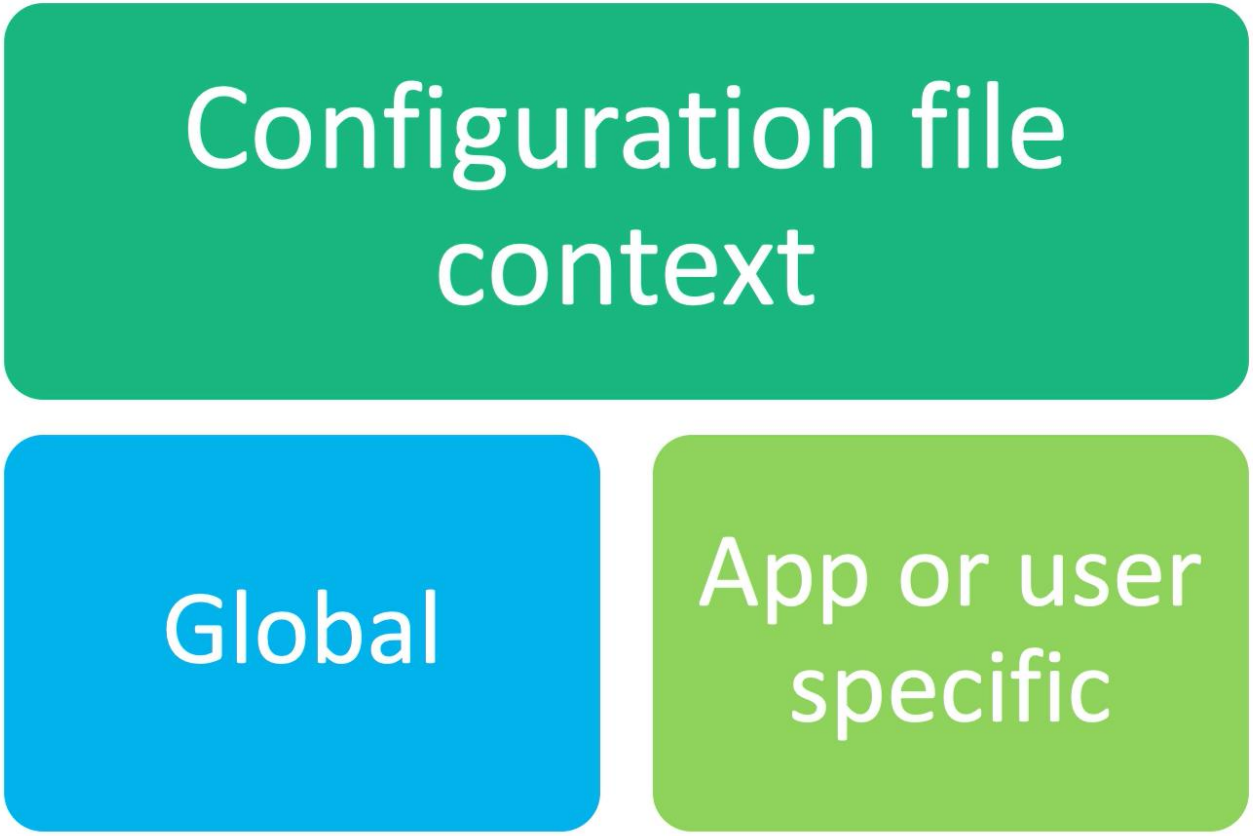
Do not edit the default copy of any conf file in `$SPLUNK_HOME/etc/system/default/`. See How to edit a configuration file.

File	Purpose
alert_actions.conf	Create an alert.
app.conf	Configure app properties
audit.conf	Configure auditing and event hashing. This feature is not available for this release.
authentication.conf	Toggle between Splunk's built-in authentication or LDAP, and configure LDAP.
authorize.conf	Configure roles, including granular access controls.
bookmarks.conf	Bookmark monitoring console URLs.
checklist.conf	Customize monitoring console health check.
collections.conf	Configure KV Store collections for apps.
commands.conf	Create custom search commands for apps in Splunk Cloud Platform or Splunk Enterprise using in the Developer Guide on the Developer Portal.

Common Configuration Files



Common Configuration Files



Common Configuration Files

Global context

System **local** directory

⇢App **local** directories

⇢App **default** directories

⇢System **default** directory

Common Configuration Files

App or User Context

User directories for **current user**

- App directories for **currently running app** (local, followed by default)
  - App directories for **all other apps** (local, followed by default)
    - **System** directories (local, followed by default)

Common Configuration Files- What's inside

- Stanzas
- Attribute = value pairs

app.conf

```
[id]
group = <group-name>
name = <app-name>
version = <version-number>
```

Common Configuration Files- What's inside

Global context

1. System local
2. App local
3. App default
4. System default

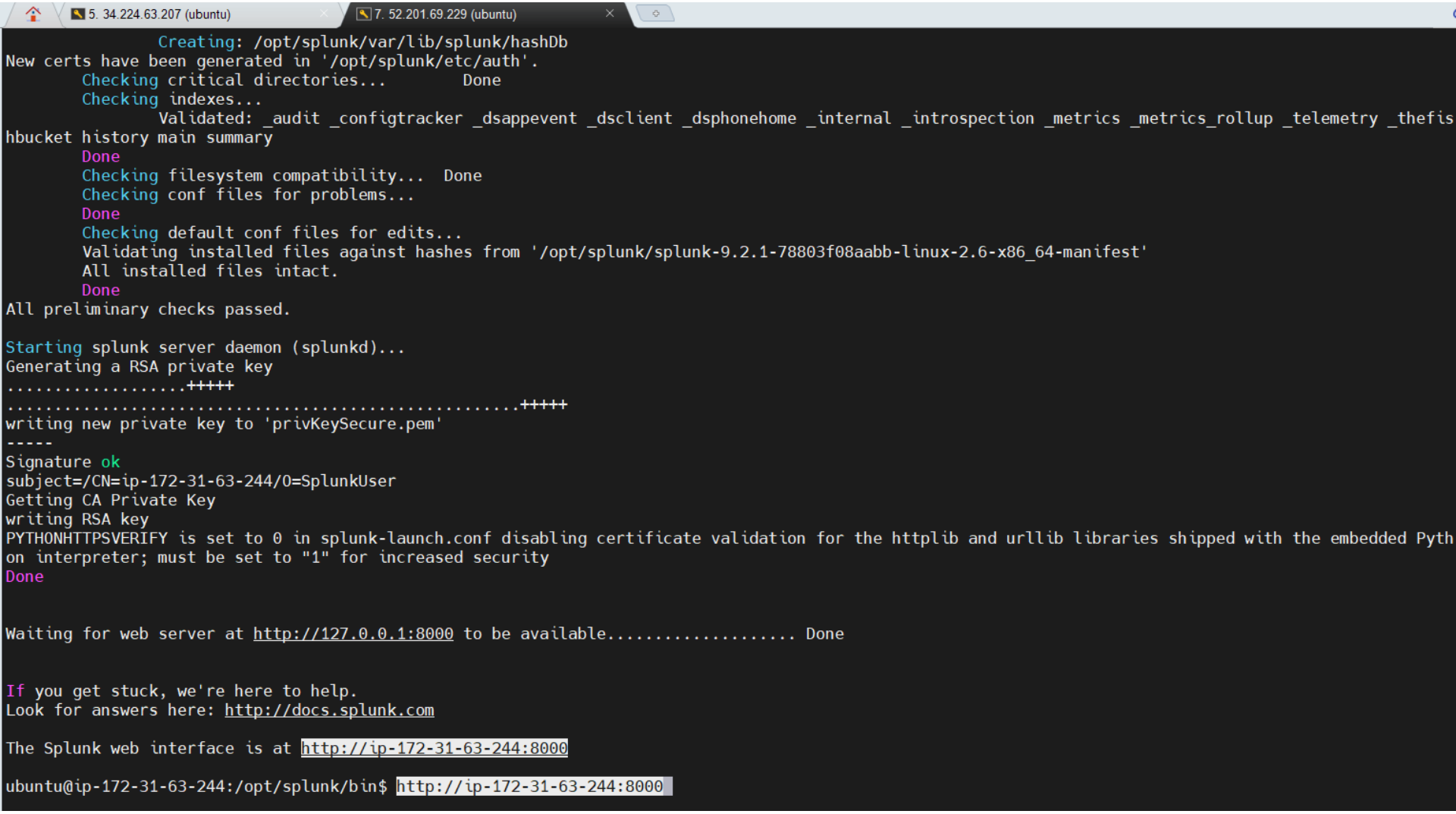
App or user context

1. User directories for the current user
2. App directories for the currently running app
3. App directories for all other apps
4. System directories

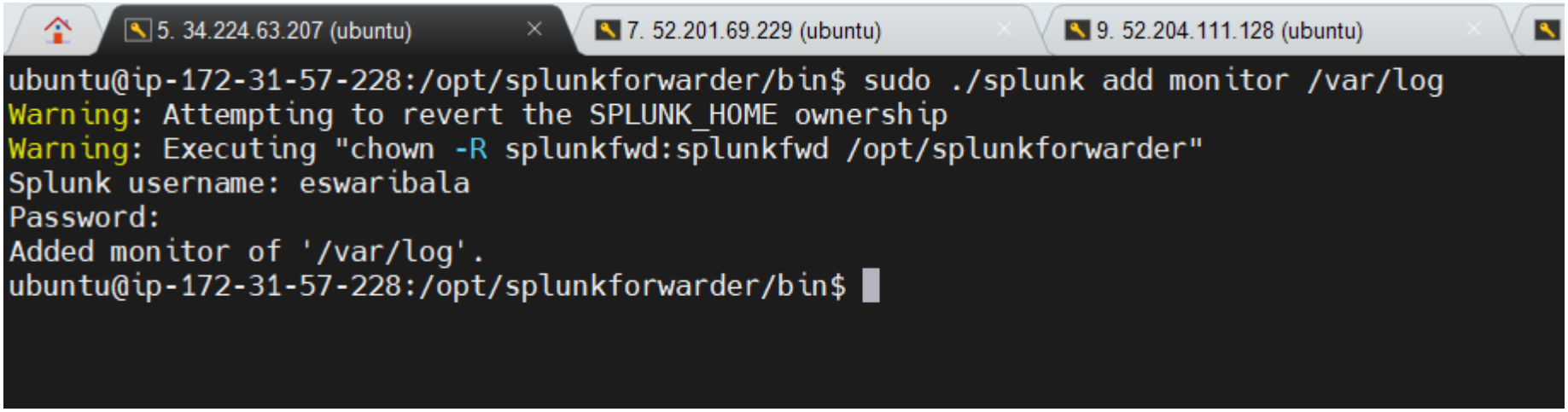
Splunk Enterprise for Ubuntu

```
splunk-9.2.1-78803f08aabb-linux-2.6-a 100%[=============================================================================>] 520.37M   116MB/s    in 4.4s

2024-04-12 15:11:16 (118 MB/s) - 'splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb' saved [545652596/545652596]

ubuntu@ip-172-31-63-244:~$ ls
splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb
ubuntu@ip-172-31-63-244:~$ sudo dpkg -i splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 65273 files and directories currently installed.)
Preparing to unpack splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb ...
Unpacking splunk (9.2.1+78803f08aabb) ...

Setting up splunk (9.2.1+78803f08aabb) ...
complete
ubuntu@ip-172-31-63-244:~$ cd /opt
ubuntu@ip-172-31-63-244:/opt$ ls
splunk
ubuntu@ip-172-31-63-244:/opt$ cd splunk
ubuntu@ip-172-31-63-244:/opt/splunk$ ls
README-splunk.txt  cmake          etc  include  license-eula.txt  opt              share                                                swidtag
bin                copyright.txt  ftr  lib      openssl           quarantined_files  splunk-9.2.1-78803f08aabb-linux-2.6-x86_64-manifest
ubuntu@ip-172-31-63-244:/opt/splunk$ cd bin
ubuntu@ip-172-31-63-244:/opt/splunk/bin$ ls
2to3-3.7                  exporttool             locktool                      prichunkpng  pyvenv-3.7                splunk
ColdStorageArchiver.py    fill_summary_index.py  mongod                        priforgepng  rapidDiag                 splunk-optimize
ColdStorageArchiver_GCP.py  genAuditKeys.py      mongod-3.6                    prigreypng   recover-metadata          splunk-optimize-lex
S3benchmark               genRootCA.sh           mongod-4.0                    pripalpng    rest_handler.py           splunk-tlsd
bloom                     genSignedServerCert.py mongodump                     pripamtopng  runScript.py              splunkd
bottle.py                 genSignedServerCert.sh mongorestore                  pripnglsch   safe_restart_cluster_master.py  splunkmon
btool                     genWebCert.py          noah_self_storage_archiver.py pripngtopam  scripts                   supervisor-simulator
btprobe                   genWebCert.sh          node                          priweavepng  scrubber.py               tarit.py
bzip2                     idle3                  openssl                       pydoc3       searchtest                tocsv.py
classify                  idle3.7                parse_xml_buckets.py          pydoc3.7     setSplunkEnv              tsidx_scan.py
coldToFrozenExample.py    importtool             pcre2-config                  python       shc_upgrade_template.py   tsidxprobe
compsup                   installit.py           pcregextest                   python3      signtool                  tsidxprobe_plo
copyright.txt             jars                   pid_check.sh                  python3.7    slim                      untarit.py
dbmanipulator.py          jsmin                  pip3                          python3.7m   spl-lang-server-sockets   walklex
easy_install-3.7          locktest               pip3.7                        pyvenv       spl2-orchestrator         wheel
ubuntu@ip-172-31-63-244:/opt/splunk/bin$
```

Splunk Enterprise for Ubuntu



Splunk Universal Forwarder inputs.conf

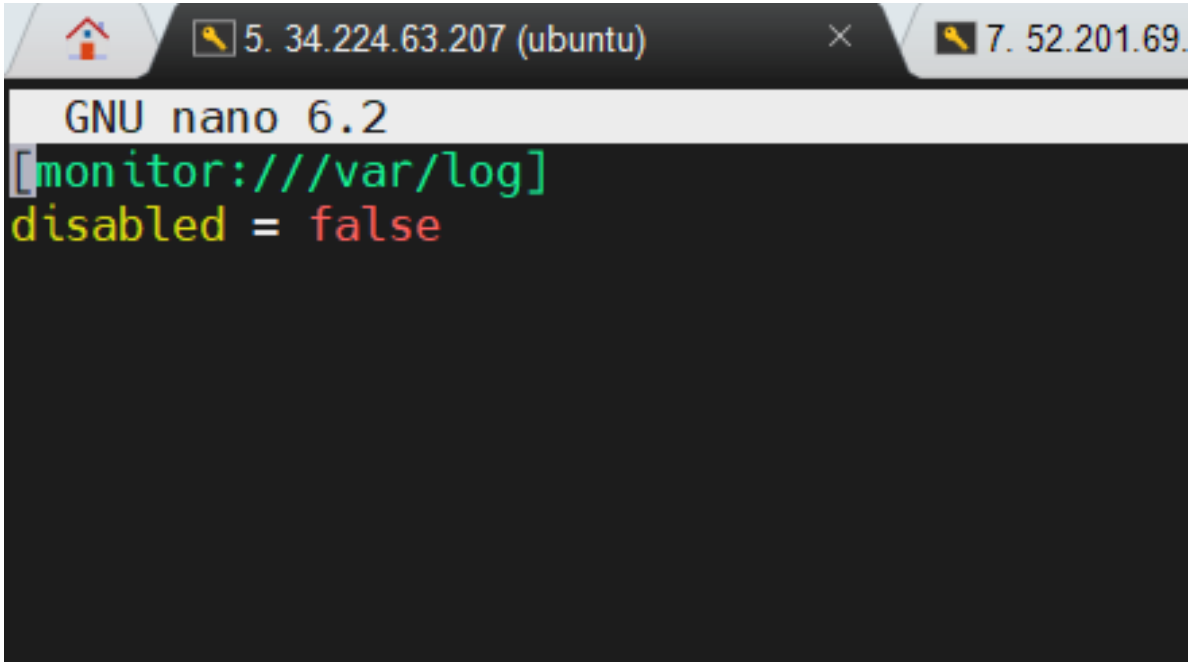


Splunk Universal Forwarder inputs.conf

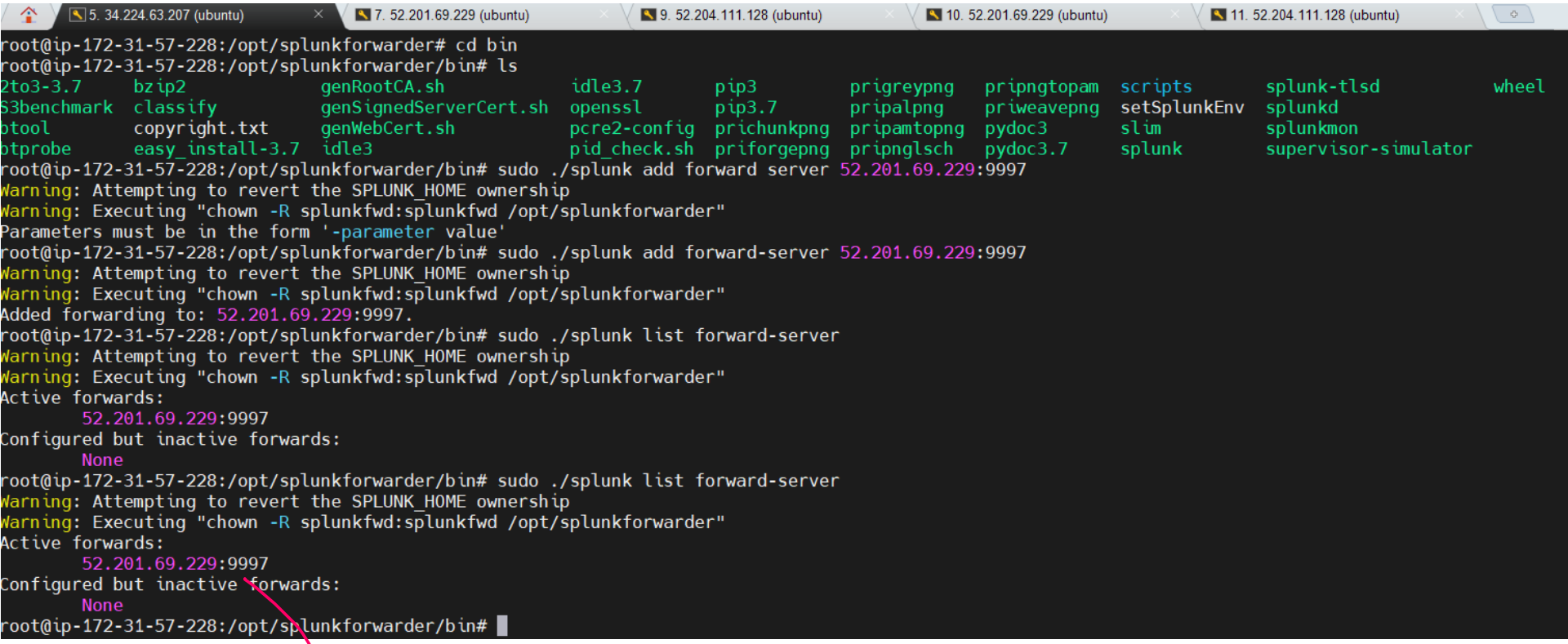
```
ubuntu@ip-172-31-57-228:/opt/splunkforwarder/bin$ cd ..
ubuntu@ip-172-31-57-228:/opt/splunkforwarder$ cd etc
ubuntu@ip-172-31-57-228:/opt/splunkforwarder/etc$ cd apps/search
ubuntu@ip-172-31-57-228:/opt/splunkforwarder/etc/apps/search$ ls
default  local  metadata
ubuntu@ip-172-31-57-228:/opt/splunkforwarder/etc/apps/search$ cd local
-bash: cd: local: Permission denied
ubuntu@ip-172-31-57-228:/opt/splunkforwarder/etc/apps/search$ ls
default  local  metadata
ubuntu@ip-172-31-57-228:/opt/splunkforwarder/etc/apps/search$ cd local
-bash: cd: local: Permission denied
ubuntu@ip-172-31-57-228:/opt/splunkforwarder/etc/apps/search$ sudo cd local
sudo: cd: command not found
sudo: "cd" is a shell built-in command, it cannot be run directly.
sudo: the -s option may be used to run a privileged shell.
sudo: the -D option may be used to run a command in a specific directory.
ubuntu@ip-172-31-57-228:/opt/splunkforwarder/etc/apps/search$ cd ..
ubuntu@ip-172-31-57-228:/opt/splunkforwarder/etc/apps$ ls
SplunkUniversalForwarder  introspection_generator_addon  journald_input  learned  search  splunk_httpinput  splunk_internal_metrics
ubuntu@ip-172-31-57-228:/opt/splunkforwarder/etc/apps$ sudo su
root@ip-172-31-57-228:/opt/splunkforwarder/etc/apps# cd search
root@ip-172-31-57-228:/opt/splunkforwarder/etc/apps/search# cd local
root@ip-172-31-57-228:/opt/splunkforwarder/etc/apps/search/local# ls
inputs.conf
root@ip-172-31-57-228:/opt/splunkforwarder/etc/apps/search/local#
```

Splunk Universal Forwarder inputs.conf

Inputs.conf

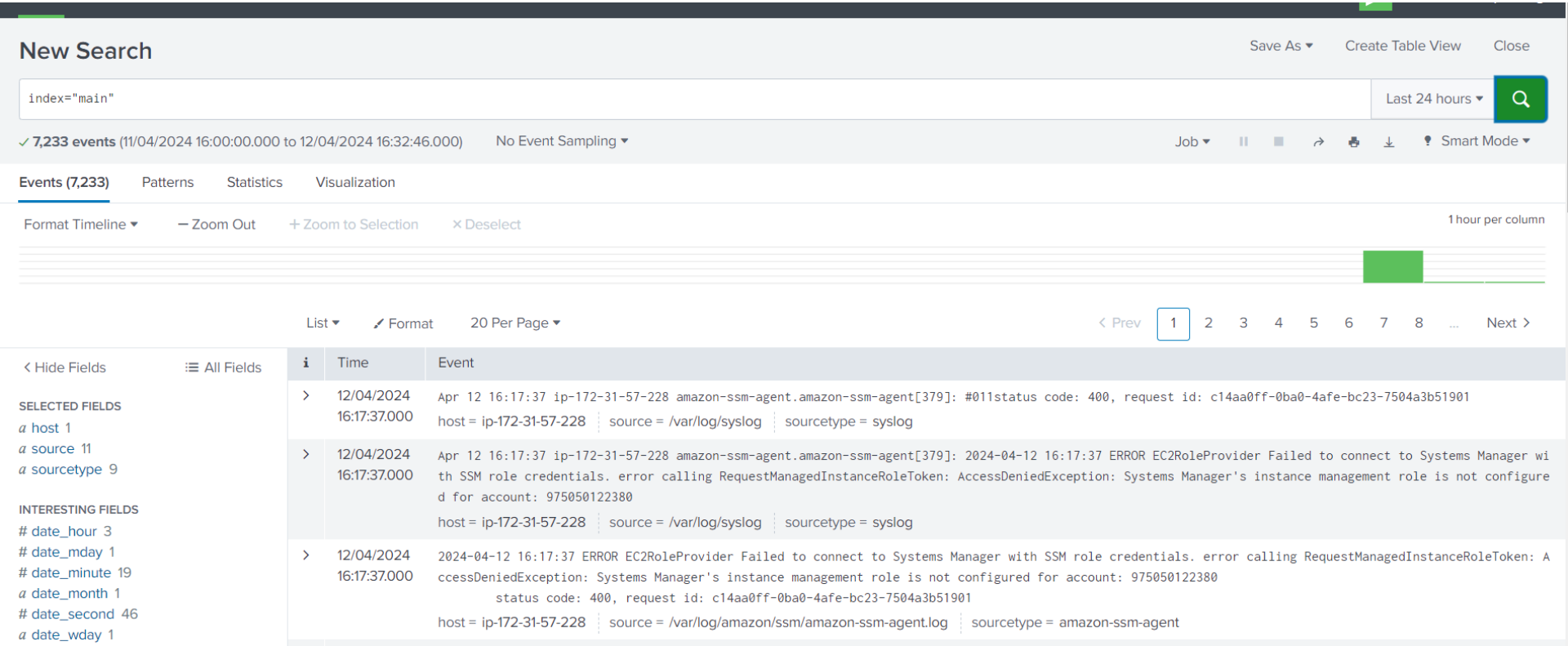


Splunk Universal Forwarder outputs.conf

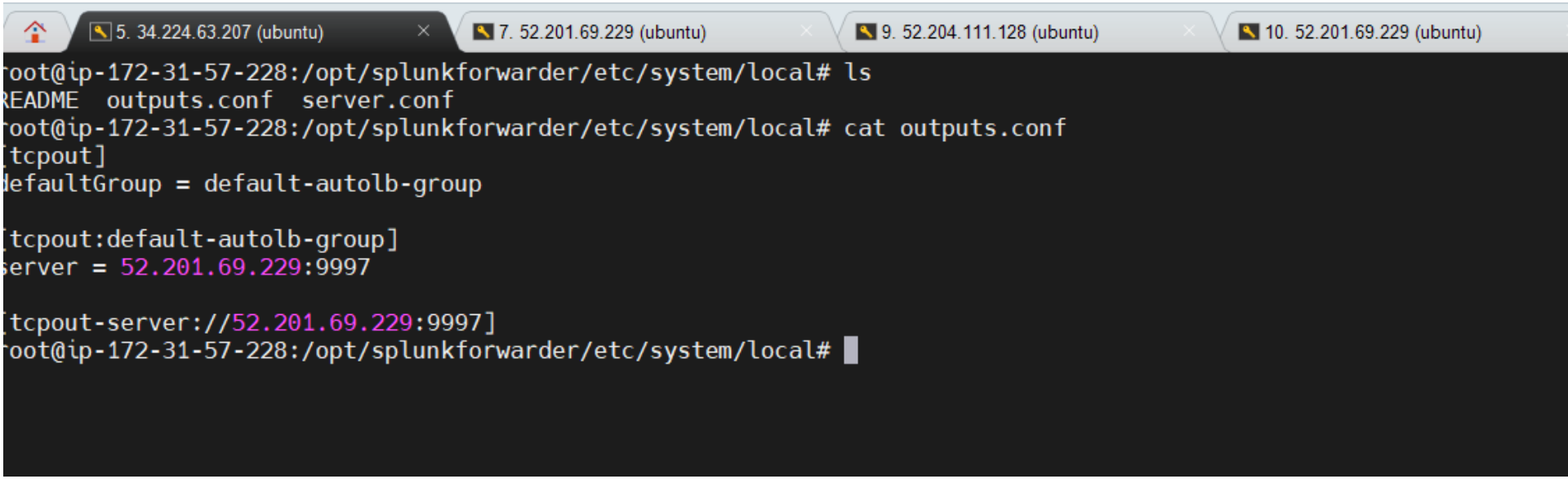


Inactive forwards --- > add port 9997 in network firewall in aws

Splunk Receiver



Splunk Universal Forwarder outputs.conf



Common Configuration Files- What's inside

Btool

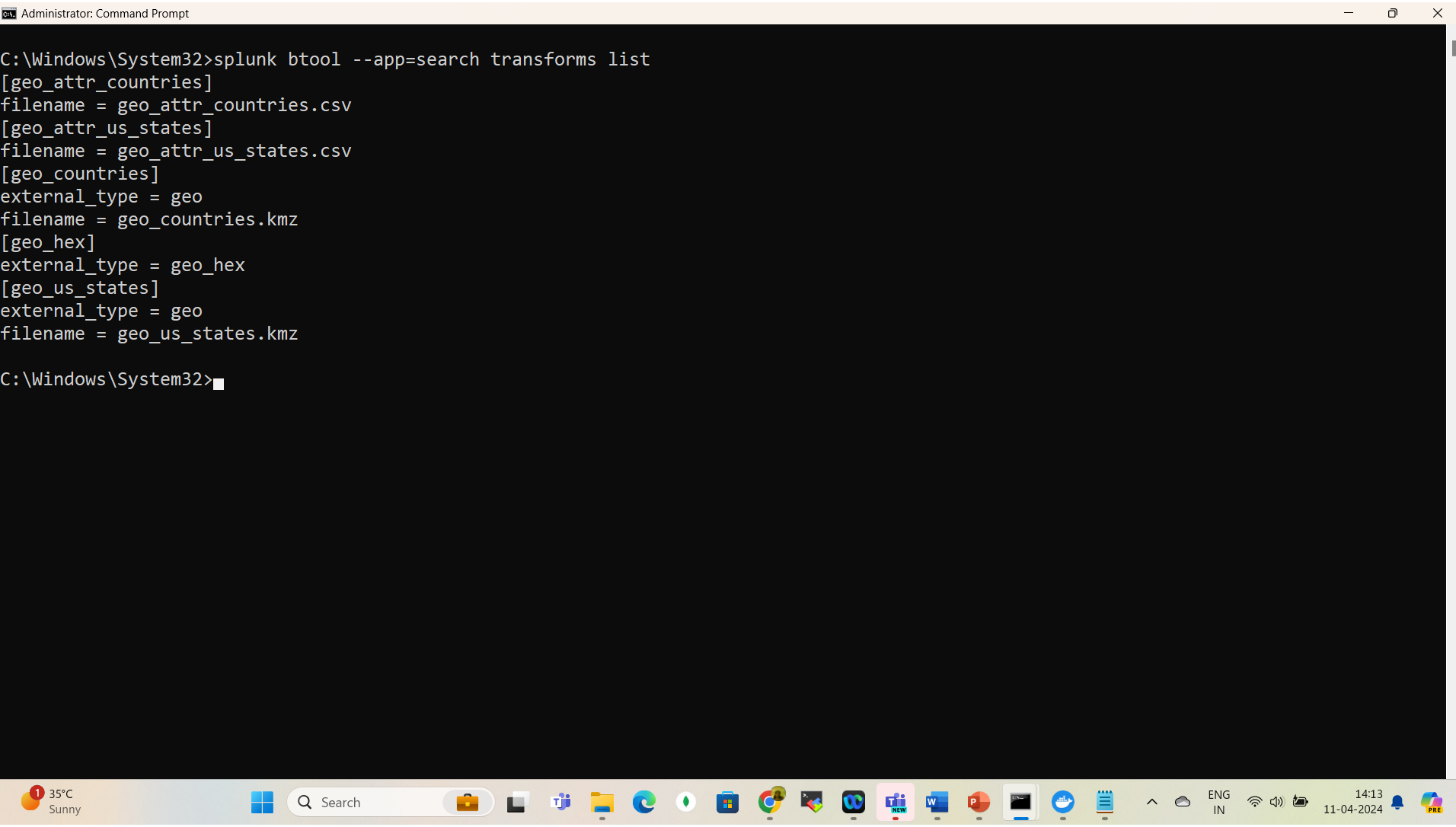
Troubleshoot

Merged configurations

Common Configuration Files- What's inside

```
C:\Windows\System32>splunk btool transforms list
[access-extractions]
CAN_OPTIMIZE = True
CLEAN_KEYS = True
DEFAULT_VALUE =
DEPTH_LIMIT = 1000
DEST_KEY =
FORMAT =
KEEP_EMPTY_VALS = False
LOOKAHEAD = 4096
MATCH_LIMIT = 100000
MV_ADD = False
REGEX = ^[[nspaces:clientip]]\s++[[nspaces:ident]]\s++[[nspaces:user]]\s++[[sbstring:req_time]]\s++[[access-request]]\s++[[nspaces:stat
us]]\s++[[nspaces:bytes]](?:\s++"(?<referer>[[bc_domain:referer_]]?+[^"]*+)"(?:\s++[[qstring:useragent]](?:\s++[[qstring:cookie]])?+)?+
)?[[all:other]]
SOURCE_KEY = _raw
WRITE_META = False
[access-request]
CAN_OPTIMIZE = True
CLEAN_KEYS = True
DEFAULT_VALUE =
DEPTH_LIMIT = 1000
DEST_KEY =
FORMAT =
KEEP_EMPTY_VALS = False
LOOKAHEAD = 4096
MATCH_LIMIT = 100000
MV_ADD = False
REGEX = "\s*+[[reqstr:method]]?(?:\s++[[bc_uri]](?:\s++[[reqstr:version]])*)?\s*+"
SOURCE_KEY = _raw
WRITE_META = False
[ad-kv]
CAN_OPTIMIZE = True
```

Common Configuration Files- What's inside



How Splunk Stores Data

- In Splunk, you store data in indexes made up of buckets of files.
- Buckets contain data structures that enable Splunk to determine if the data contains terms or words.
- Buckets also contain compressed, raw data.
- This data is typically reduced to 15% of its original size, once compressed, to help Splunk store data efficiently.

How Splunk Stores Data

- Bucket storage can contain a significant amount of data but the largest storage consumption from Splunk comes from metadata.
- Around 35% of the original size of data stored is searchable metadata which Splunk uses to determine how to return search results.
- Splunk stores data at around a 50% reduction in size from the original.
- This is before replication.
- This amount is just a baseline, however, since data compresses differently by type.
- If you are unsure how to anticipate your storage needs, a 50% size estimate is a good place to start.

Splunk Storage Calculation Example

- Consider a Splunk deployment with a data ingest of 10gb/day, on a single server with no replication.
- This requires the following storage capacity:

- 10gb/day * .15 (raw data) = 1.5gb/day

- 10gb/day * .35 (metadata) = 3.5gb/day

- Total = 5gb/day

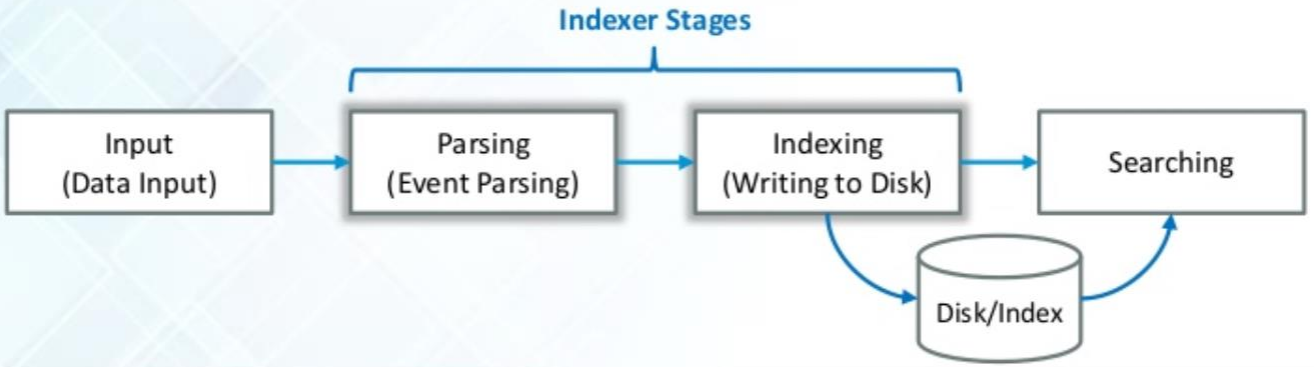
Splunk Storage Calculation Example

- Assuming you keep all data in warm or cold storage, the total storage capacity is a function of the number of days.

- For 90 days data retention: 5gb * 90 days = 450gb

- For 1 year retention: 5gb * 365 days = 1825gb

Indexer for Data Storage and Processing



In the Parsing stage, only relevant data is converted into events:

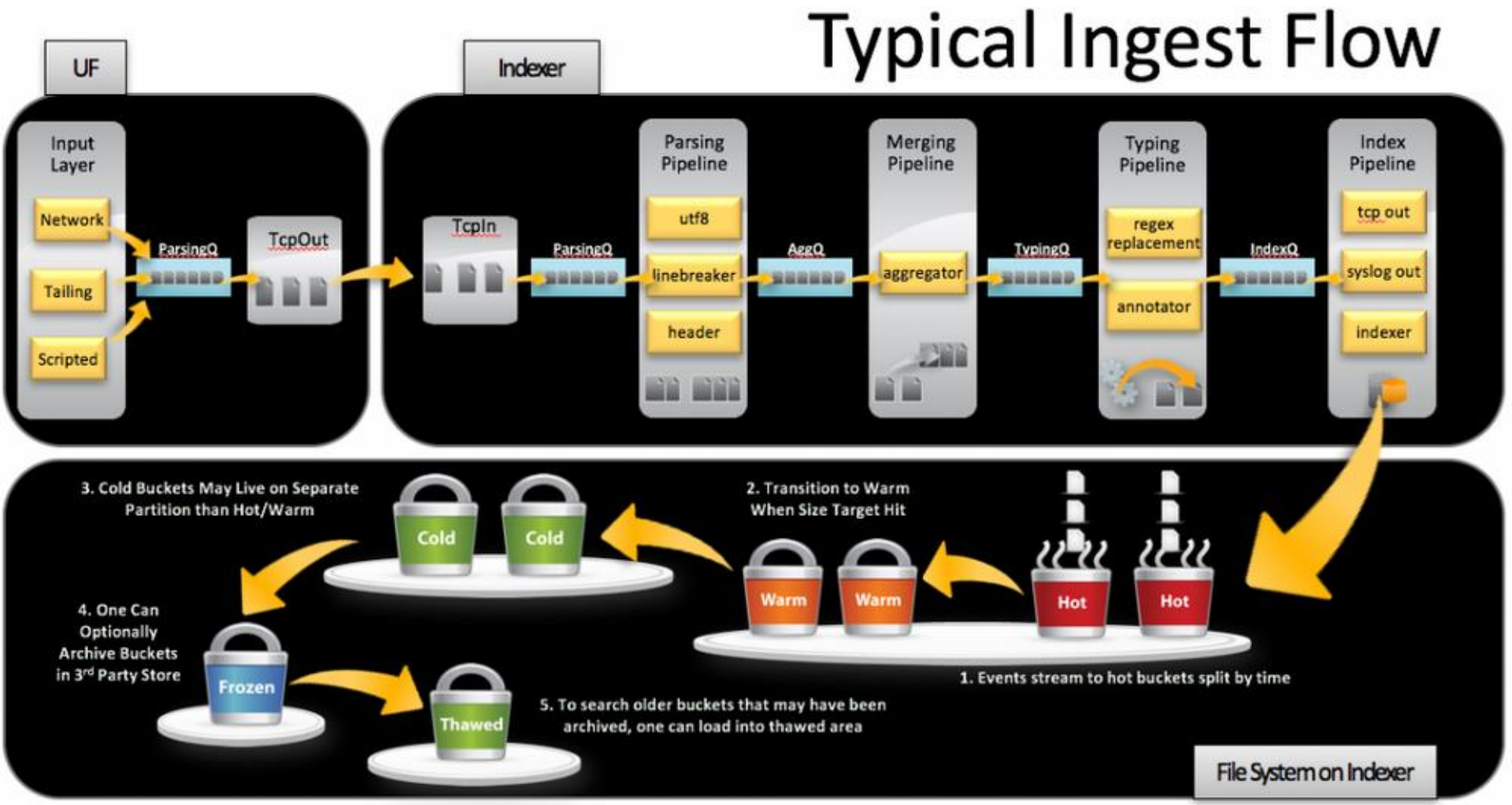
- Customer Region
- Order revenue
- Time of purchase
- Device used by customers
- Coupons/ Offers used

In the Indexing stage, events are sorted and indexed for storage based on:

- Sales by Geography
- Order revenue
- Time of purchase
- Device preferred by customers
- Coupons/ Offers used

* The details mentioned in this slide are representative in nature and data present might not be accurate.

Indexer for Data Storage and Processing



Indexes

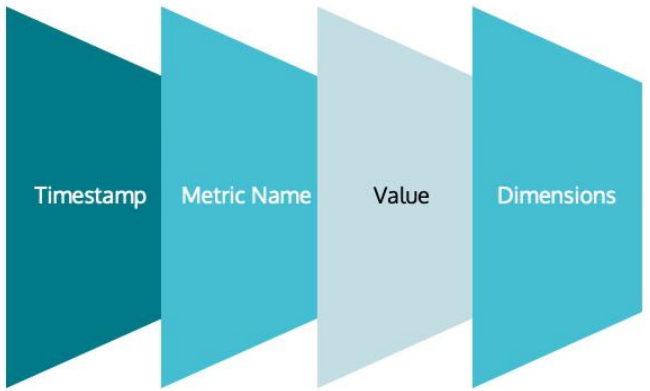
- Repository of Splunk events
- Built-in or custom
- Indexes contain three types of data
  1. Raw data in compressed form
  2. Indexes that point to the raw data
  3. Metadata

Meta data can be timestamp, source, host etc.,

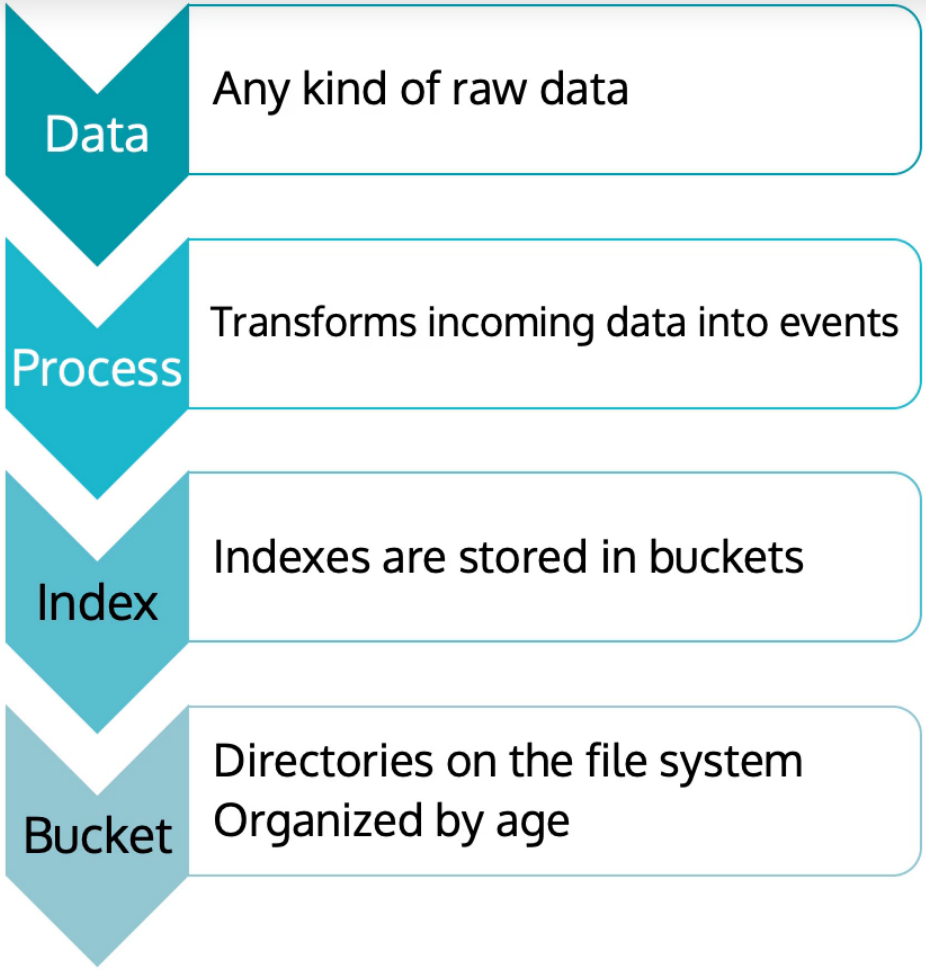
Index Types

- Event
  - The default type
  - Can handle any type of data

- Metrics
  - Optimized to store and retrieve *metrics data*



Index Structure

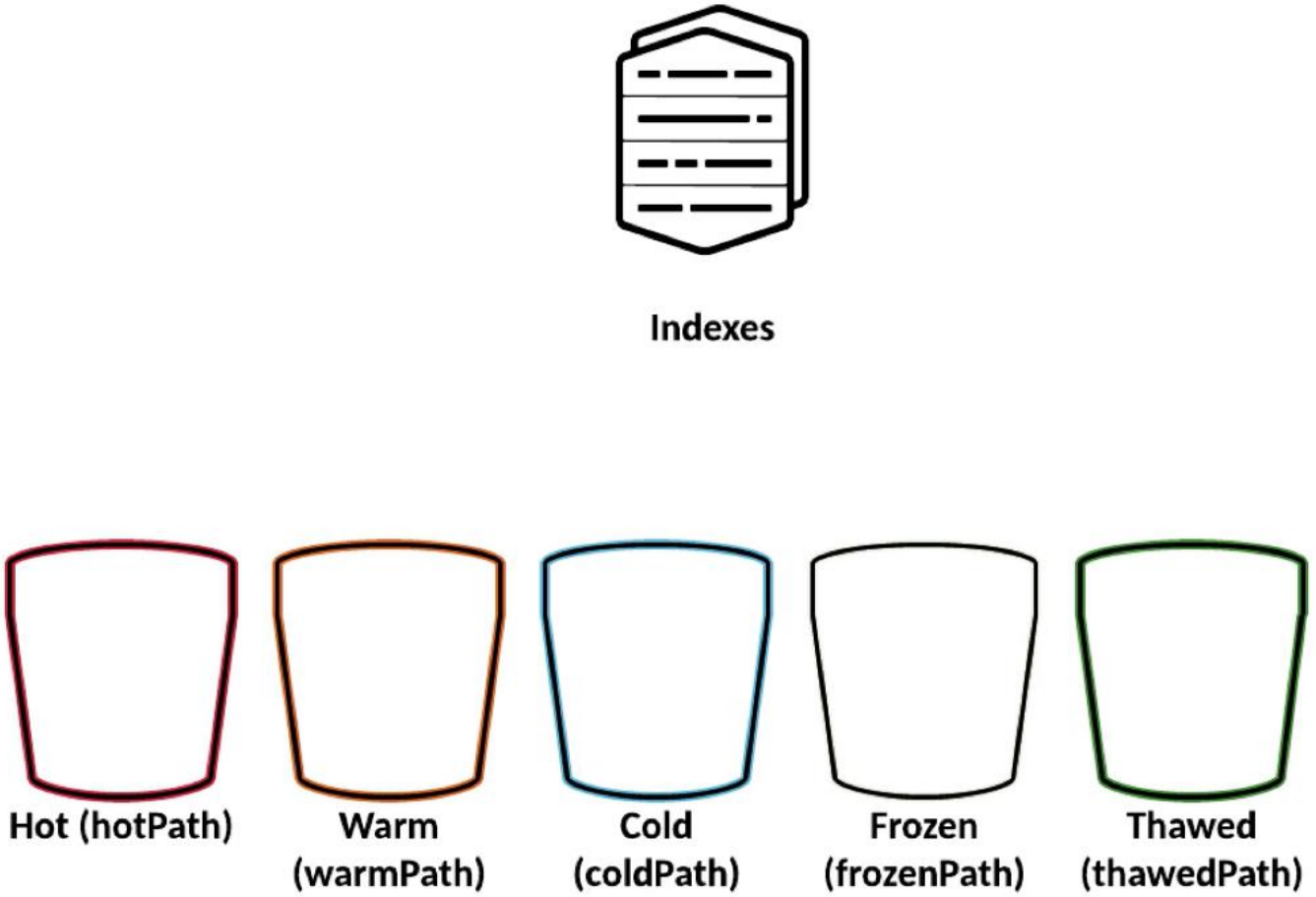


- `host`, source, `sourcetype`
- Character set encoding
- Line breaks
- Timestamps
- Metadata

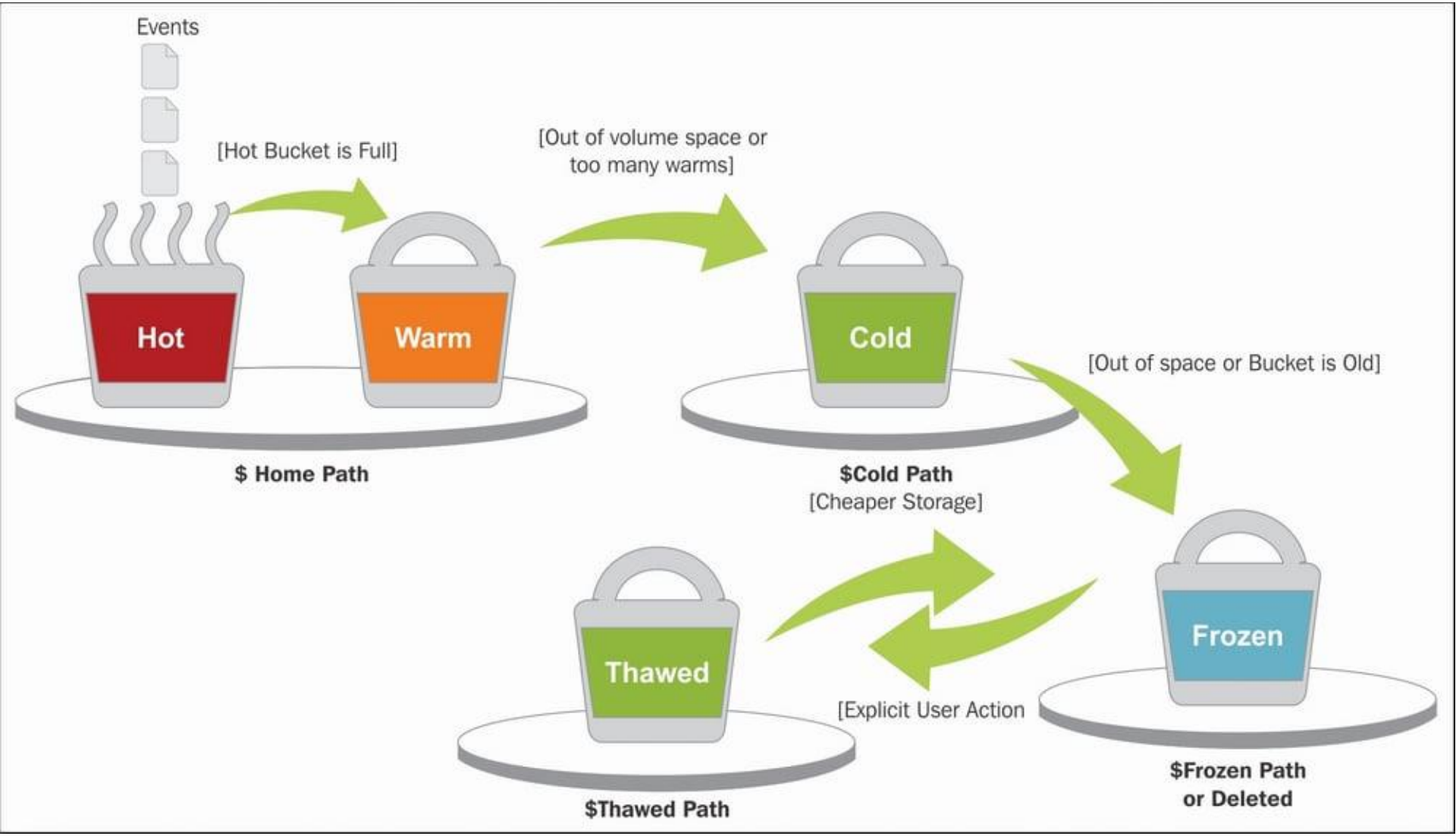
- `$SPLUNK_HOME/var/lib/splunk/*`

- `main`, `_internal`, `_audit`

Index Structure

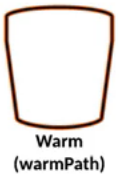


Index Structure

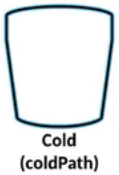


Buckets

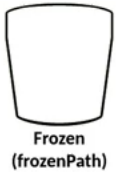
$SPLUNK_HOME/var/lib/splunk/defaultdb/db/*



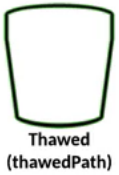
$SPLUNK_HOME/var/lib/splunk/defaultdb/db/*



$SPLUNK_HOME/var/lib/splunk/defaultdb/colddb/*



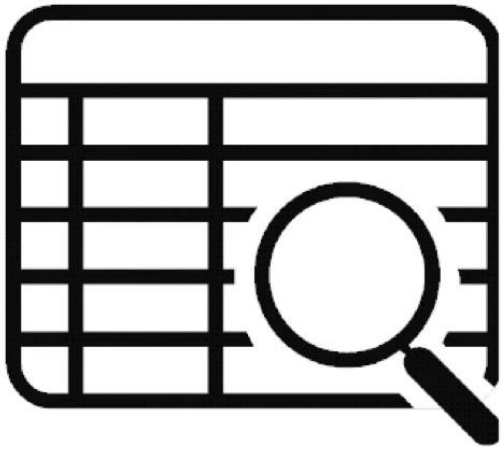
Location that you specify



$SPLUNK_HOME/var/lib/splunk/defaultdb/thaweddb/*

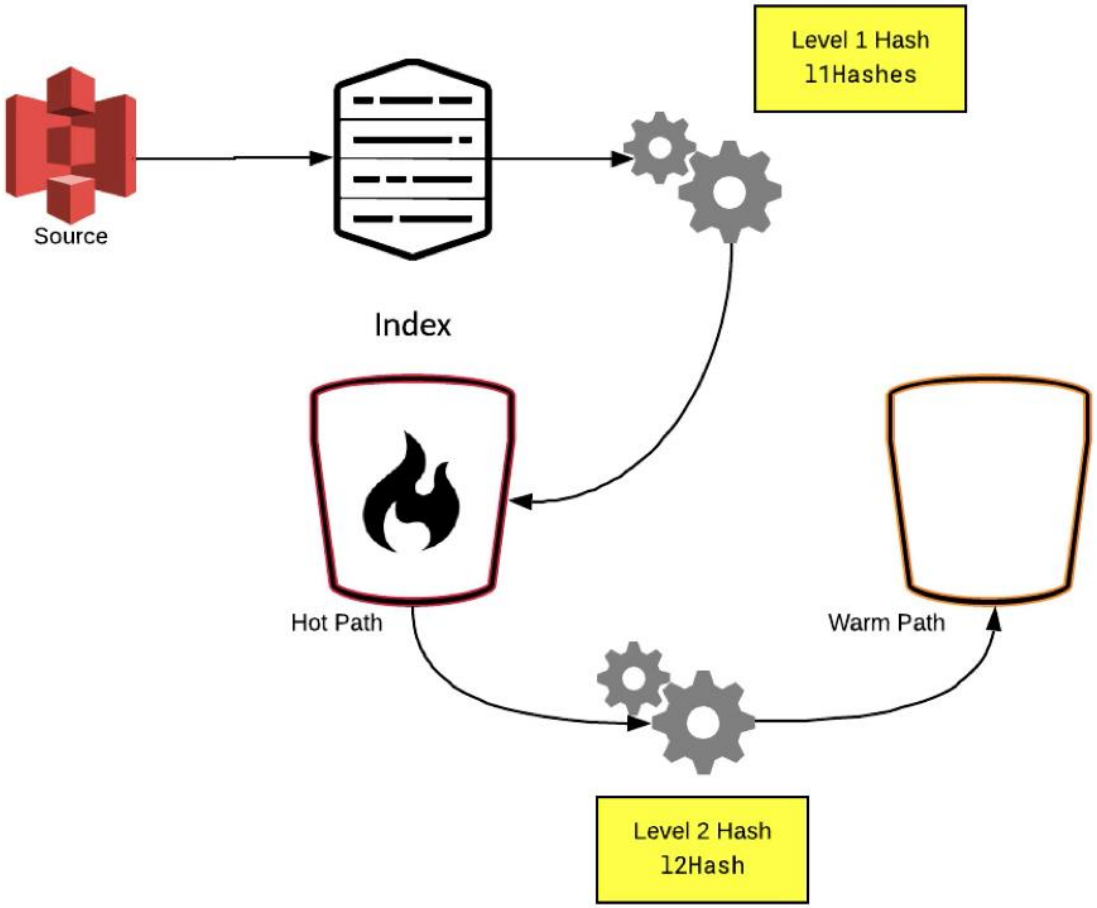
Buckets – Data Integrity Checks

How Data Integrity Works



- Splunk's double hash
  - Computes a hash on newly indexed data
  - Computes another hash on the same data when it moves buckets
  - Stores both hash files in the /rawdata directory

Buckets – Data Integrity Checks



Buckets – Data Integrity Checks

Command Line Options

- Check hashes to validate data

```
./splunk check-integrity -bucketPath [ bucket path ] [ -verbose ]
```

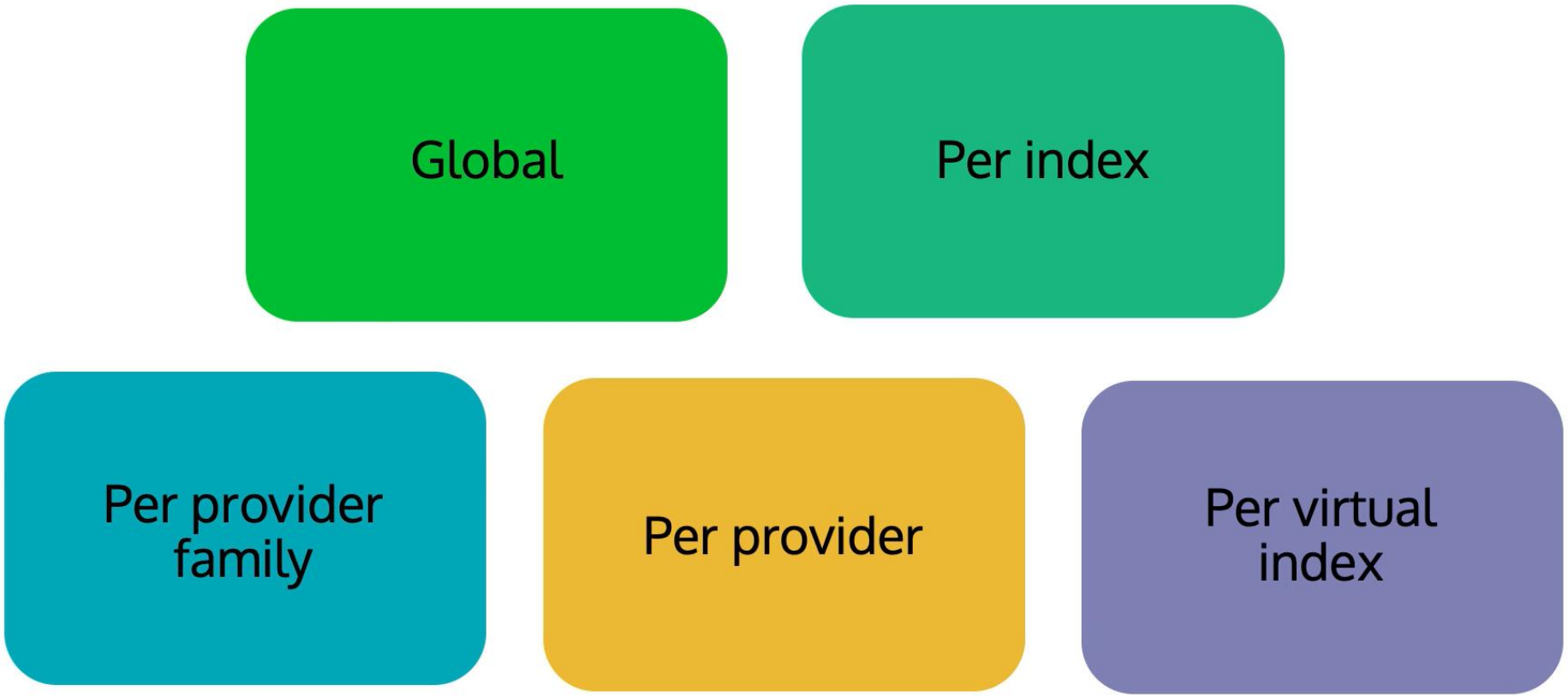
- Configure data integrity control

```
enableDataIntegrityControl=true
```

- Regenerate hashes

```
./splunk generate-hash-files -bucketPath [ bucket path ] [ verbose ]
```

Index.conf


Global
Per index
Per provider family
Per provider
Per virtual index

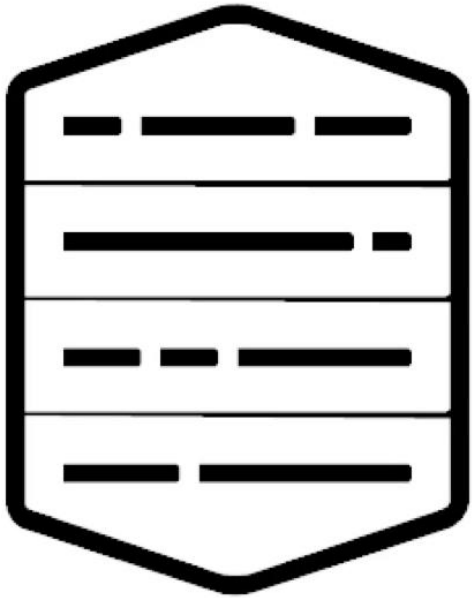
Index.conf

Global Settings

- Defined either at the beginning of the file or in the `[default]` stanza
- Each index.conf file has only one `[default]` stanza

Index.conf

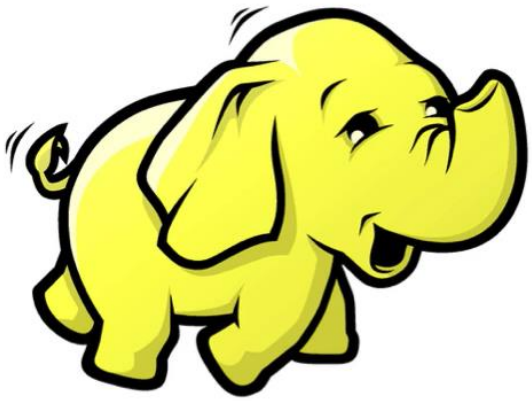
Per Index Options



- Options under an [<index>] stanza
- A few of the many options
  - Set bucket paths
  - Set database sizes
  - Specify event or metric data types

Index.conf

Per Provider Options

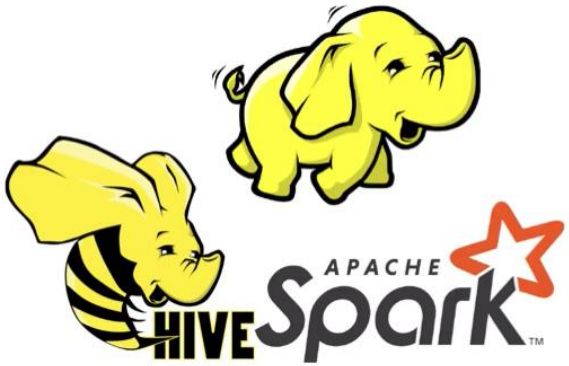


- Options for External Resource Providers (ERPs)
- All provider stanzas begin with

```
[provider: ]
```

Index.conf

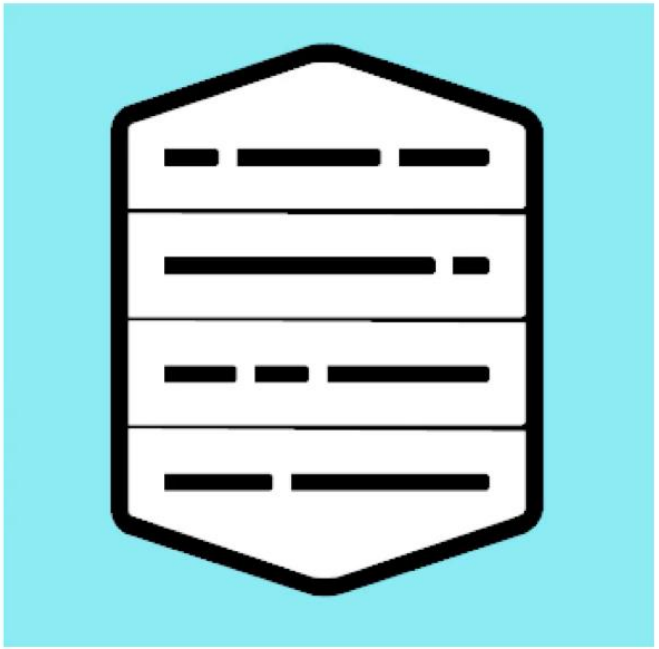
Per Provider Family Options



- Properties that are common to multiple providers
- All properties that can be used in a family can be used in a provider
- Stanzas for provider families begin with `[provider-family:  ]`

Index.conf

Per Virtual Index Options



- Common for the Hadoop family
- Let Splunk access data stored in external systems and push computations to those systems

Fish Bucket- Special Index – Search which Files Indexed

- Fish bucket in Splunk is a sub-directory that maintains CRC (Cyclic Redundancy Check) state for monitored files.
- It contains seek pointers and CRCs and keeps track of how much of your file has been indexed into Splunk.
- The default location of the fish bucket sub-directory is the $splunk_home/var/lib/splunk.

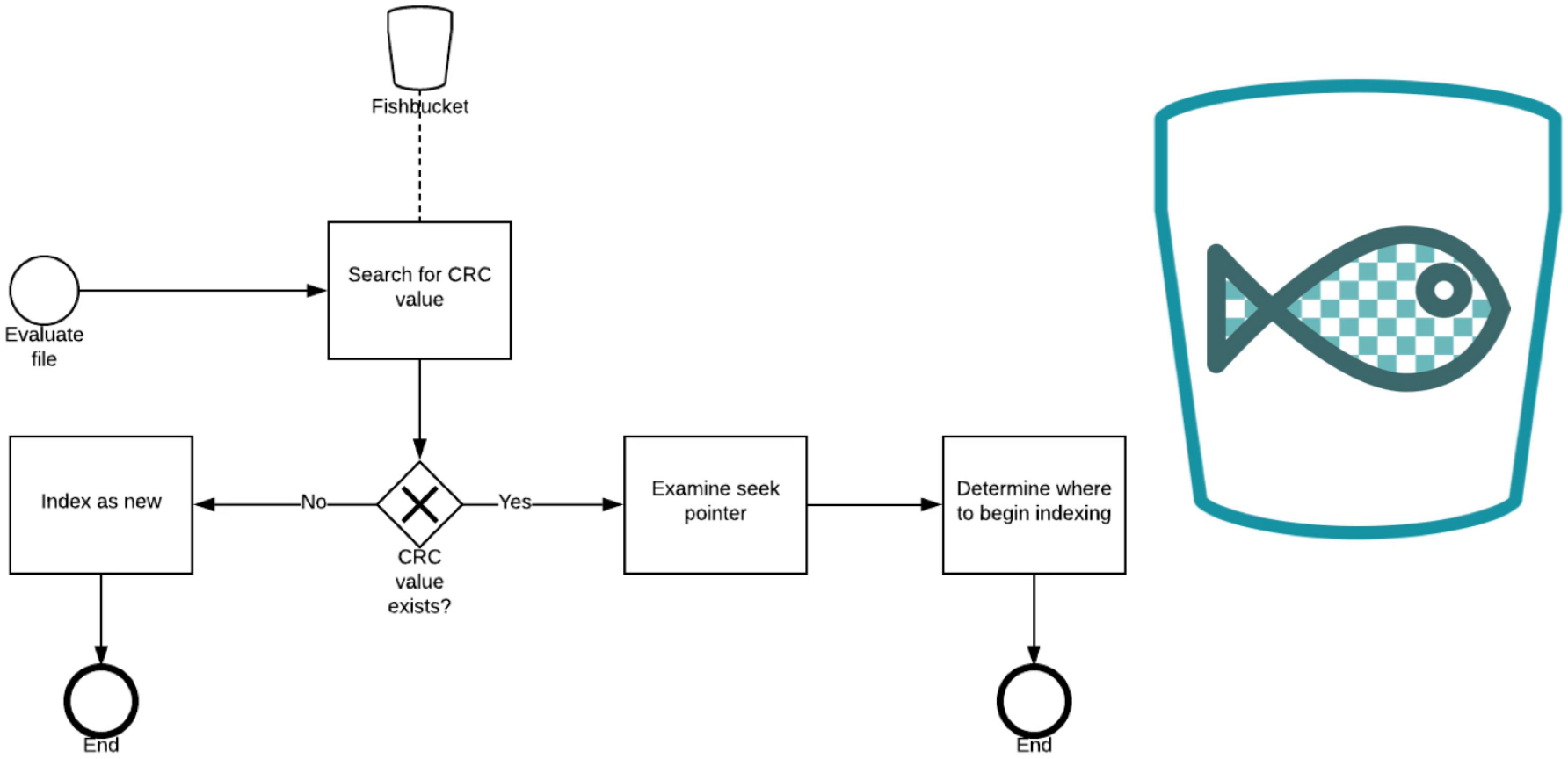
Fish Bucket- Special Index – Search which Files Indexed

- CRC helps Splunk to determine if it has read a file before or not.
- To prevent re-indexing a previously-read file Splunk runs a cyclic redundancy check against first and last 256 bytes of a file.
- When Splunk is restarted file monitor processor checks if CRC is present in its database.
- If CRC is found and seek pointer is same as previous, then Splunk knows file has already been ingested and if CRC is not present or seek pointer is different than Splunk re-ingests whole file again.

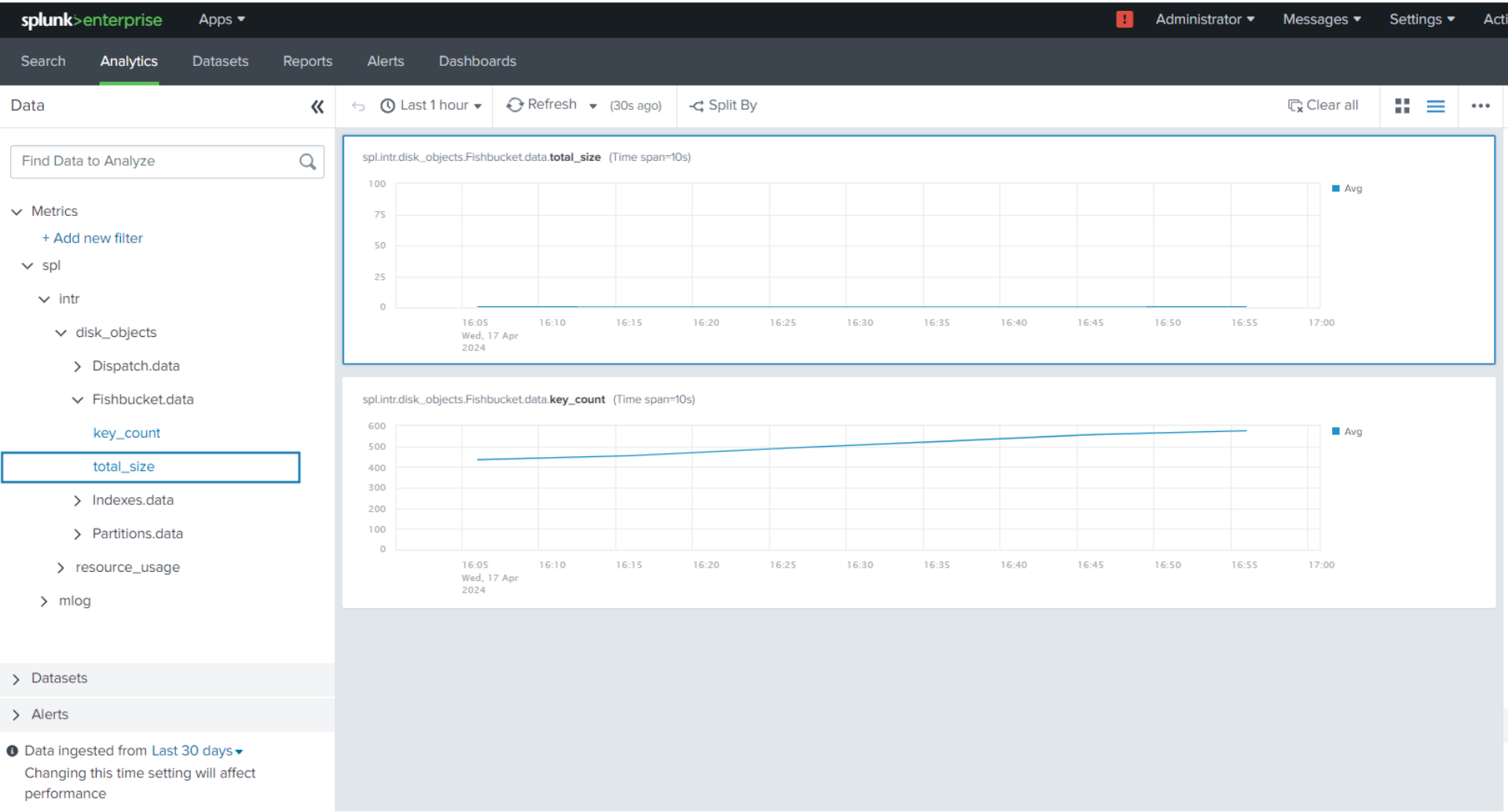
Fish Bucket- Special Index – Search which Files Indexed

- CRC helps Splunk to determine if it has read a file before or not.
- To prevent re-indexing a previously-read file Splunk runs a cyclic redundancy check against first and last 256 bytes of a file.
- When Splunk is restarted file monitor processor checks if CRC is present in its database.
- If CRC is found and seek pointer is same as previous, then Splunk knows file has already been ingested and if CRC is not present or seek pointer is different than Splunk re-ingests whole file again.

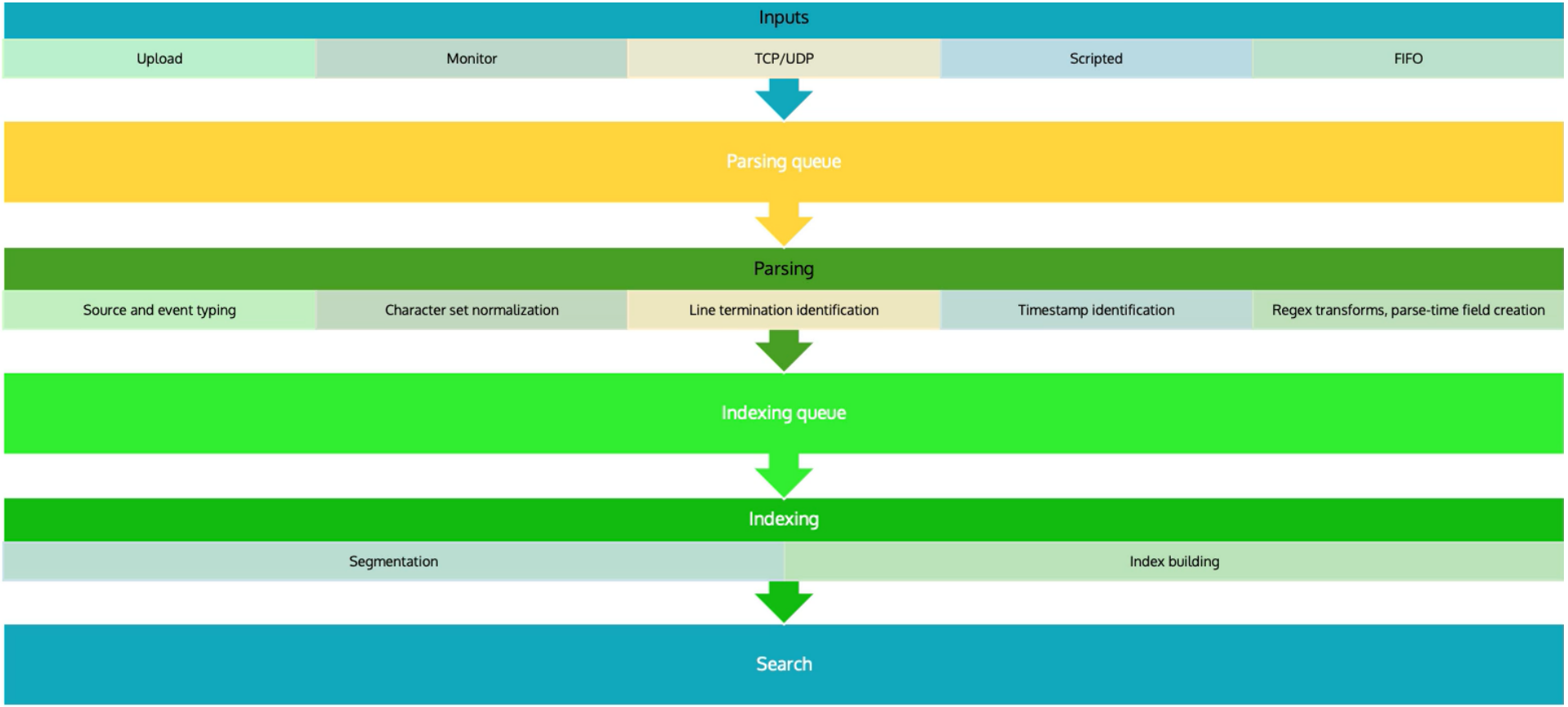
Fish Bucket- Special Index – Search which Files Indexed



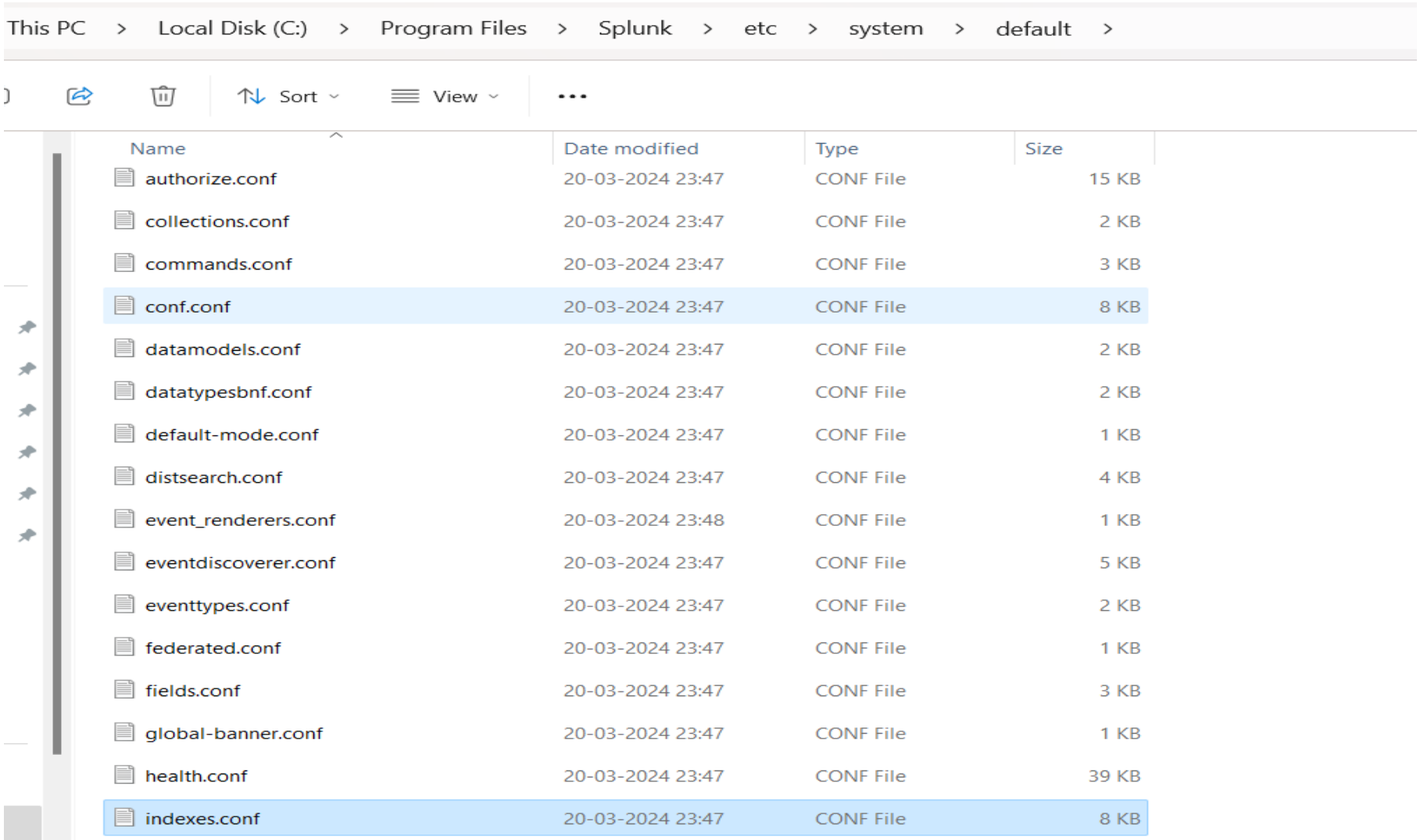
Fish Bucket- Special Index – Search which Files Indexed



Splunk Data Pipeline



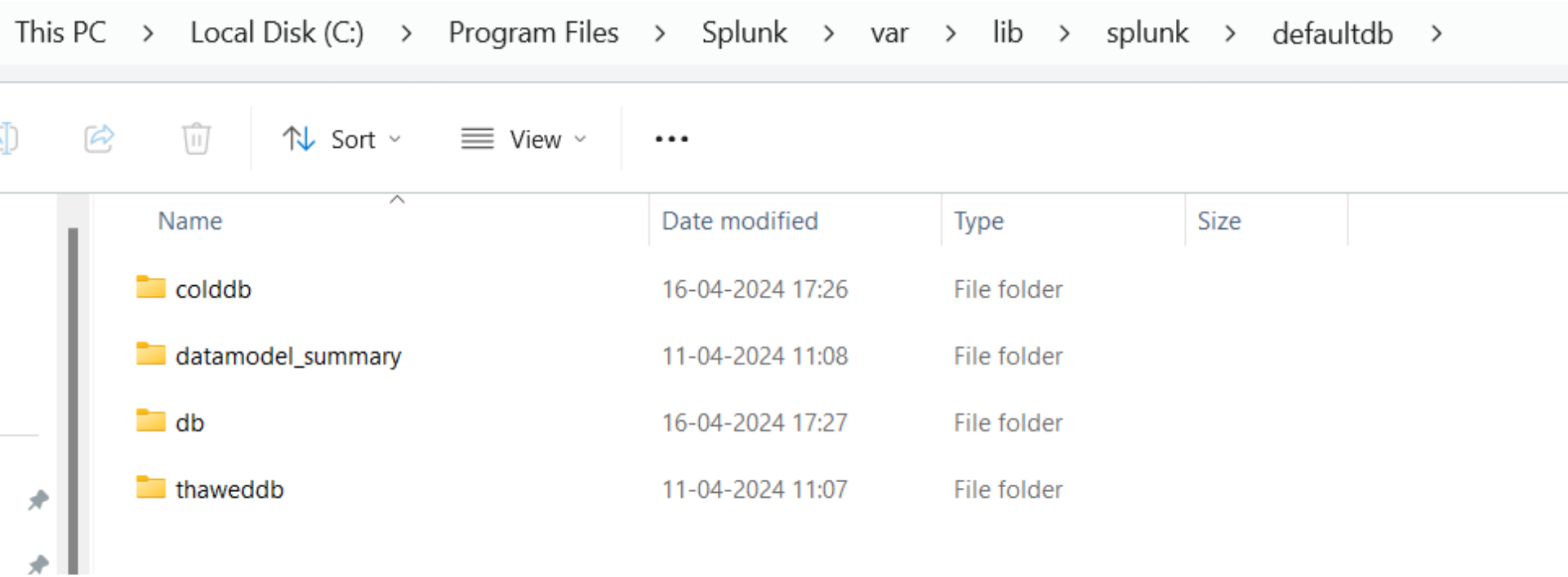
Splunk Index files



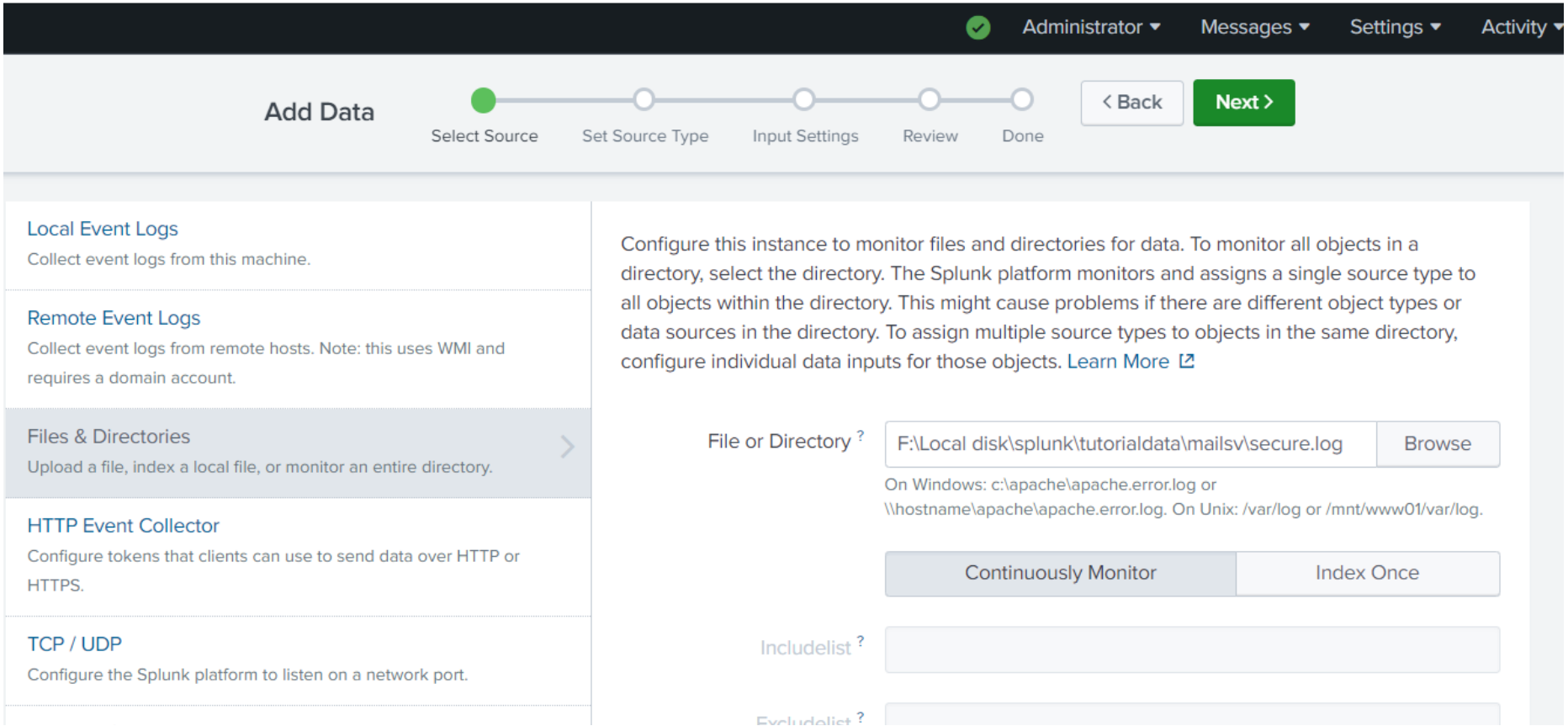
Splunk Index files

```
#Version 9.2.1
#DO NOT EDIT THIS FILE!
# Changes to default files will be lost on update and are difficult to
# manage and support.
#
# Please make any changes to system defaults by overriding them in
# apps or $SPLUNK_HOME/etc/system/local
# (See "Configuration file precedence" in the web documentation).
#
# To override a specific setting, copy the name of the stanza and
# setting to the file where you wish to override it.
#
# This file configures Splunk's indexes and their properties.
#

########################################################################################
# "global" params (not specific to individual indexes)
########################################################################################
sync = 0
indexThreads = auto
memPoolMB = auto
defaultDatabase = main
enableRealtimeSearch = true
suppressBannerList =
maxRunningProcessGroups = 8
maxRunningProcessGroupsLowPriority = 1
bucketRebuildMemoryHint = auto
serviceOnlyAsNeeded = true
serviceSubtaskTimingPeriod = 30
serviceInactiveIndexesPeriod = 60
maxBucketSizeCacheEntries = 0
processTrackerServiceInterval = 1
hotBucketTimeRefreshInterval = 10
rtRouterThreads = 0
rtRouterQueueSize = 10000
selfStorageThreads = 2
fileSystemExecutorWorkers = 5
hotBucketStreaming.extraBucketBuildingCmdlineArgs =

########################################################################################
```

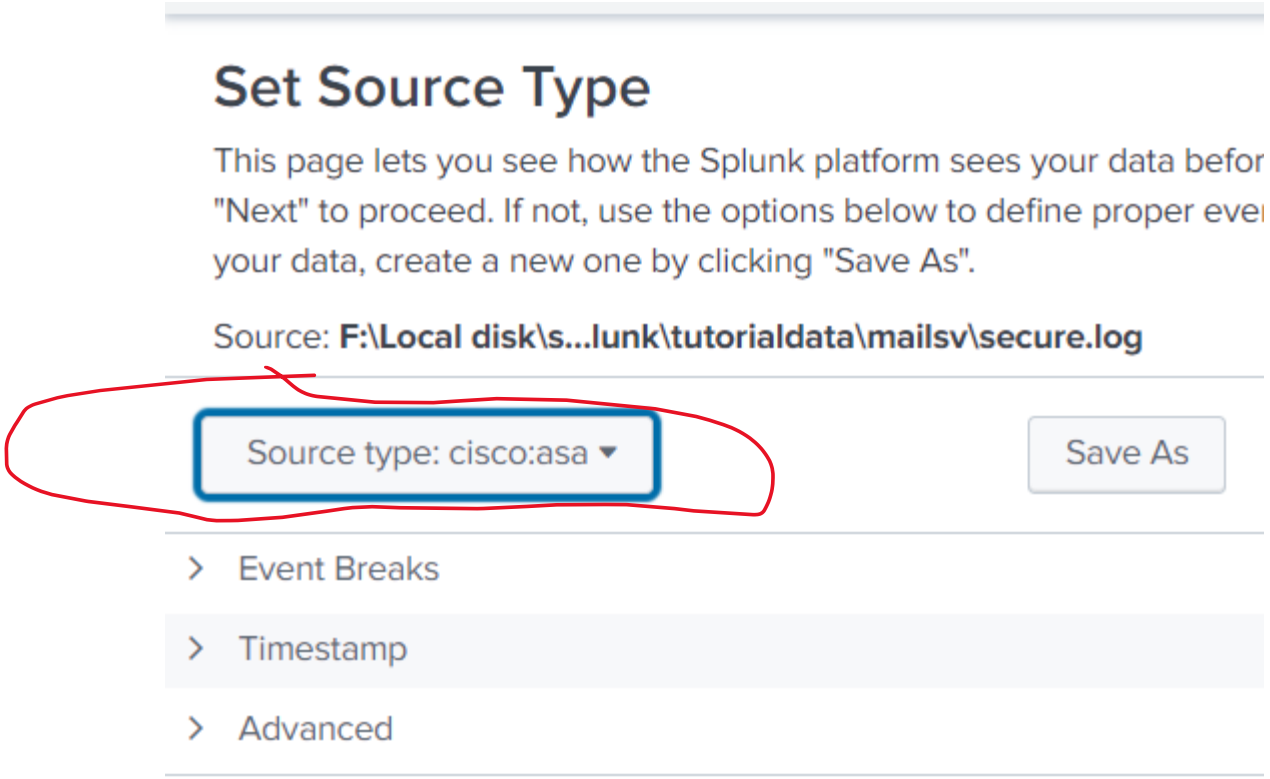
Splunk Buckets in file system



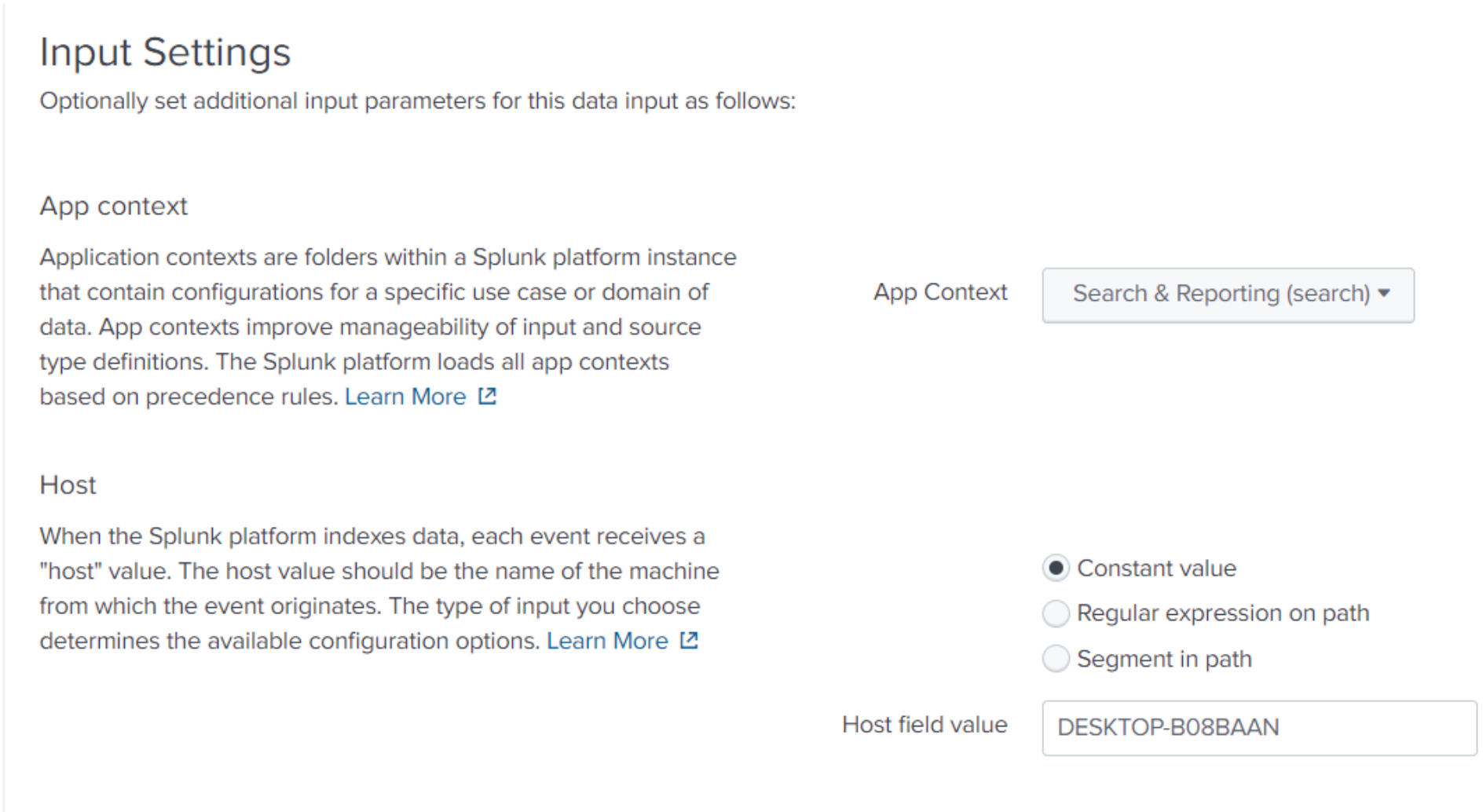
Splunk Add Data



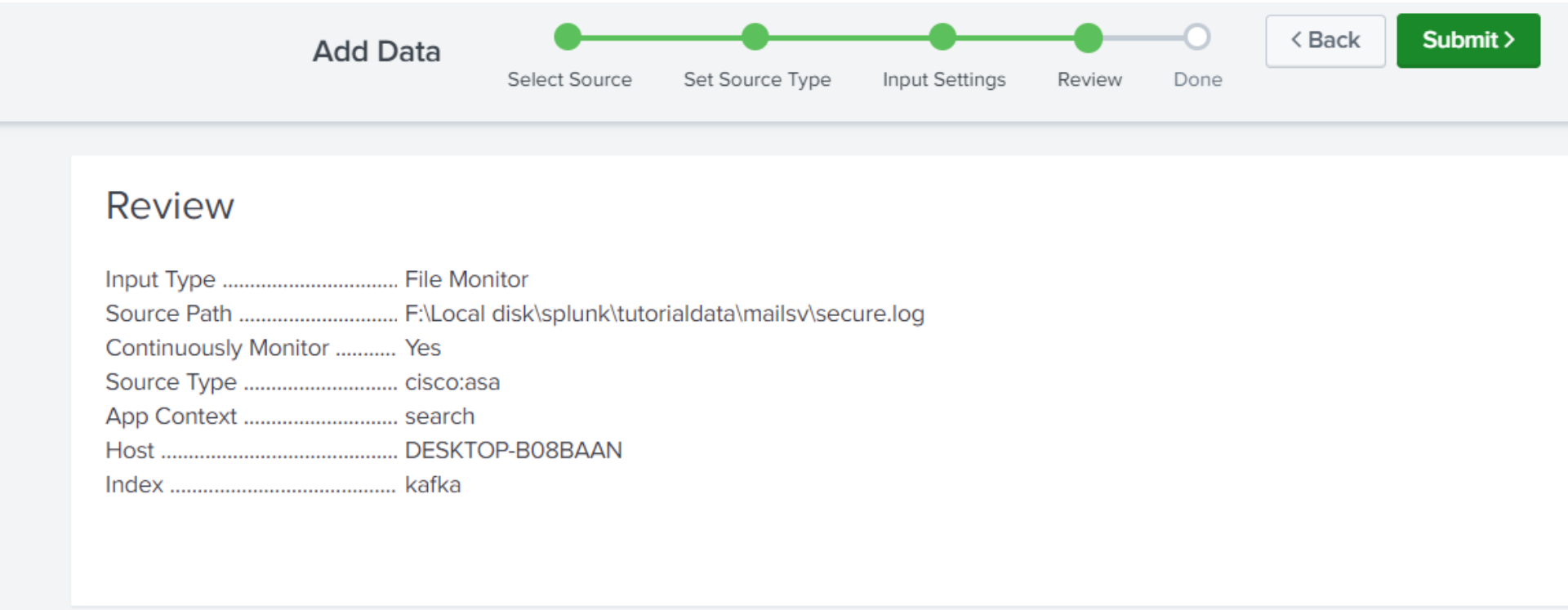
Splunk Add Data



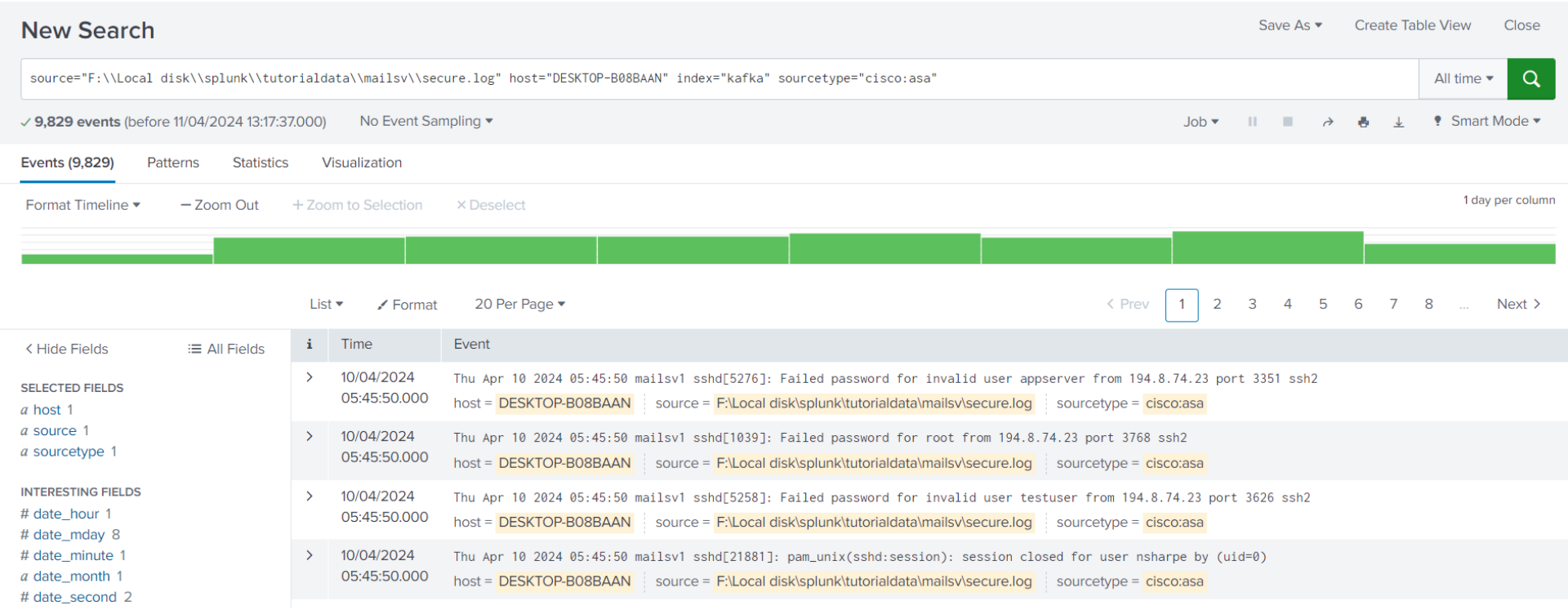
Splunk Add Data



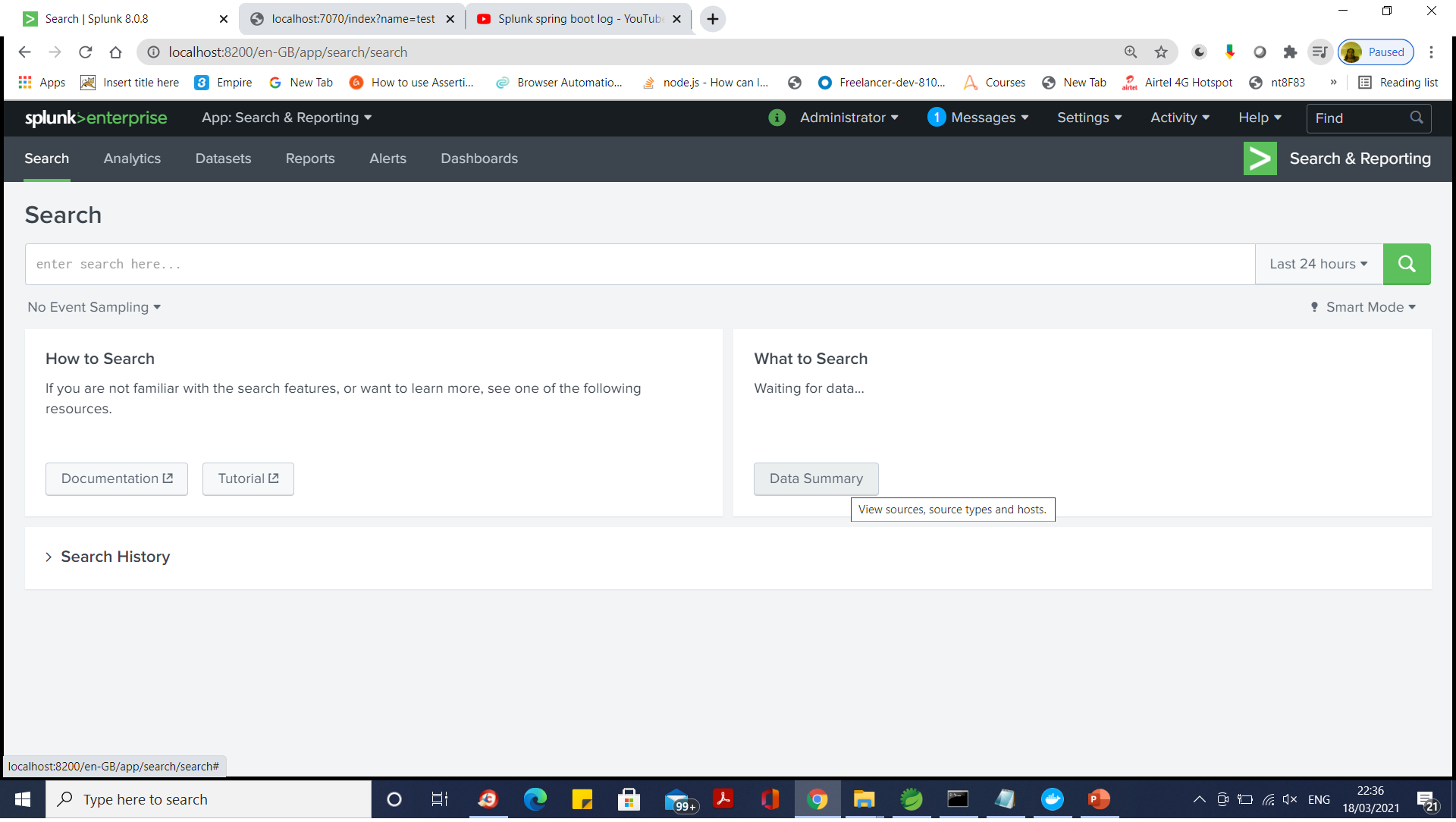
Splunk Add Data



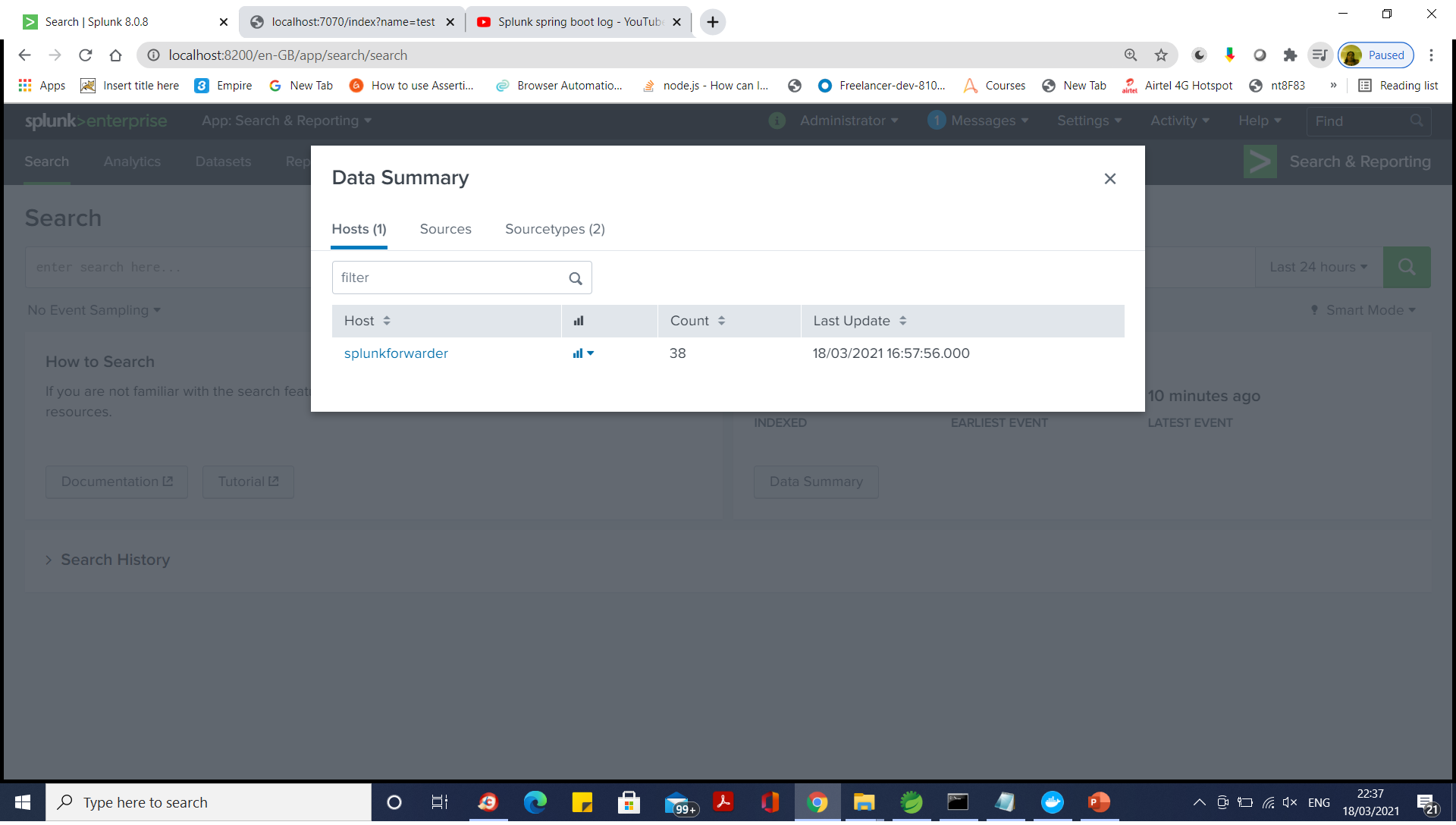
Splunk Add Data



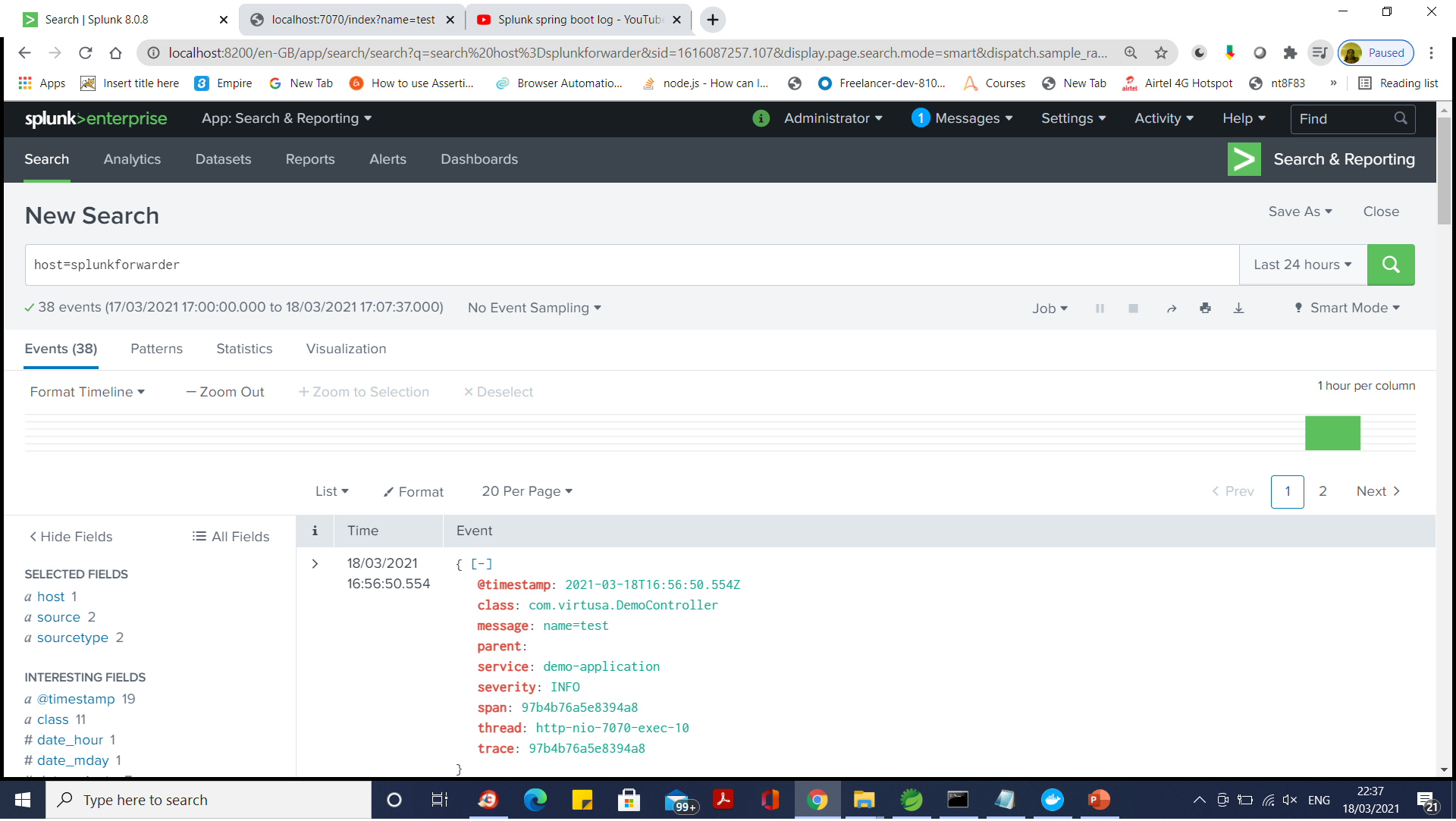
Splunk Handson



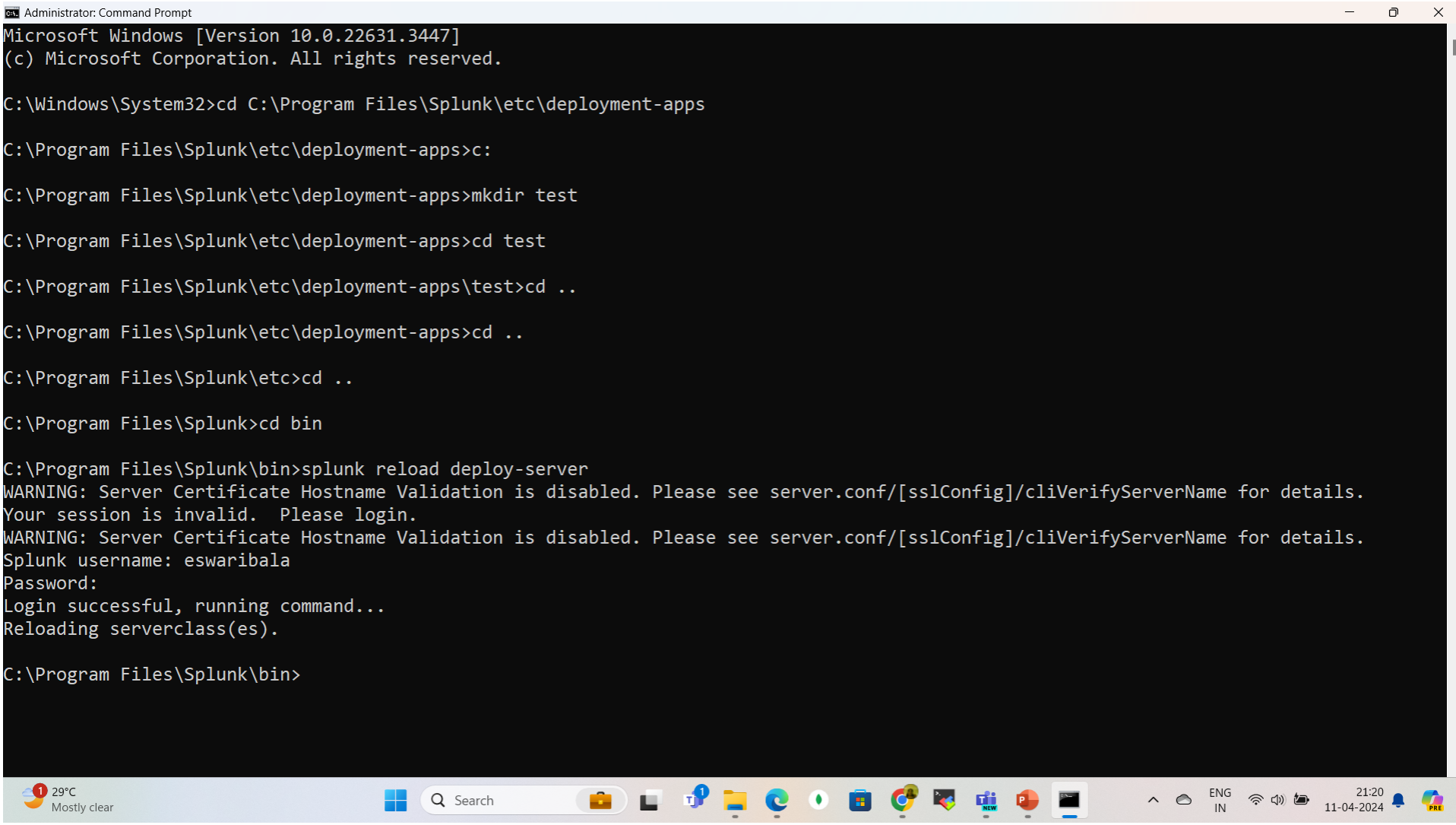
Splunk Handson



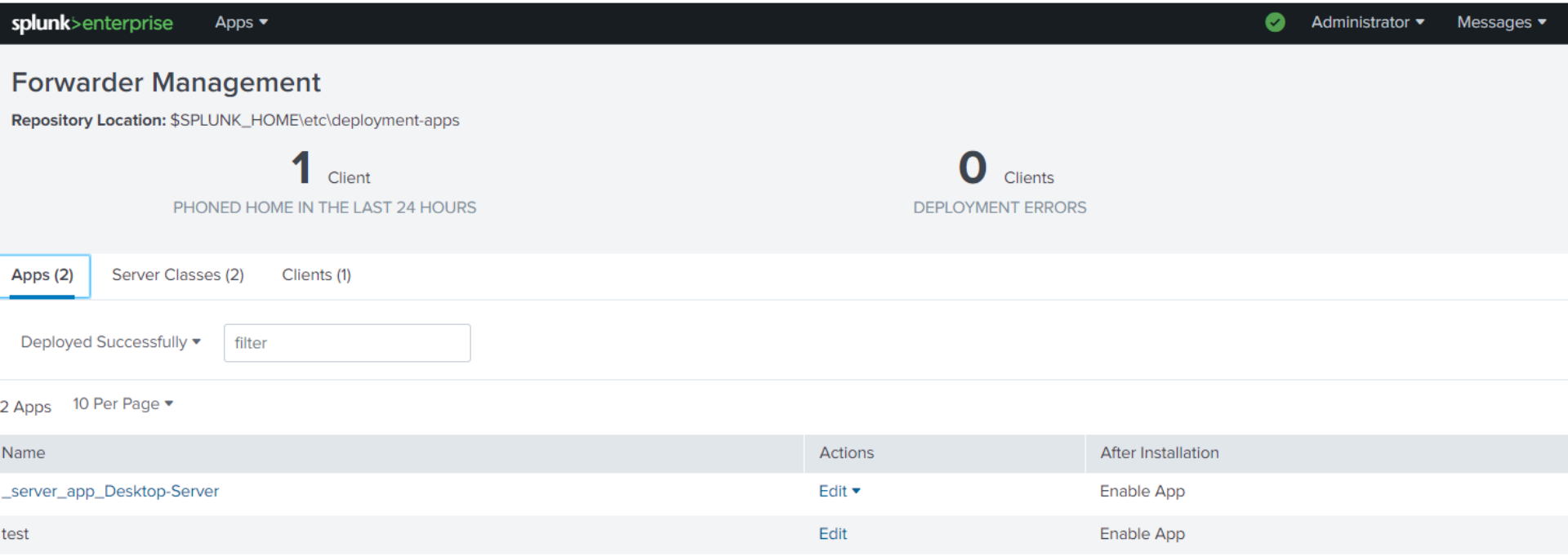
Splunk Handson



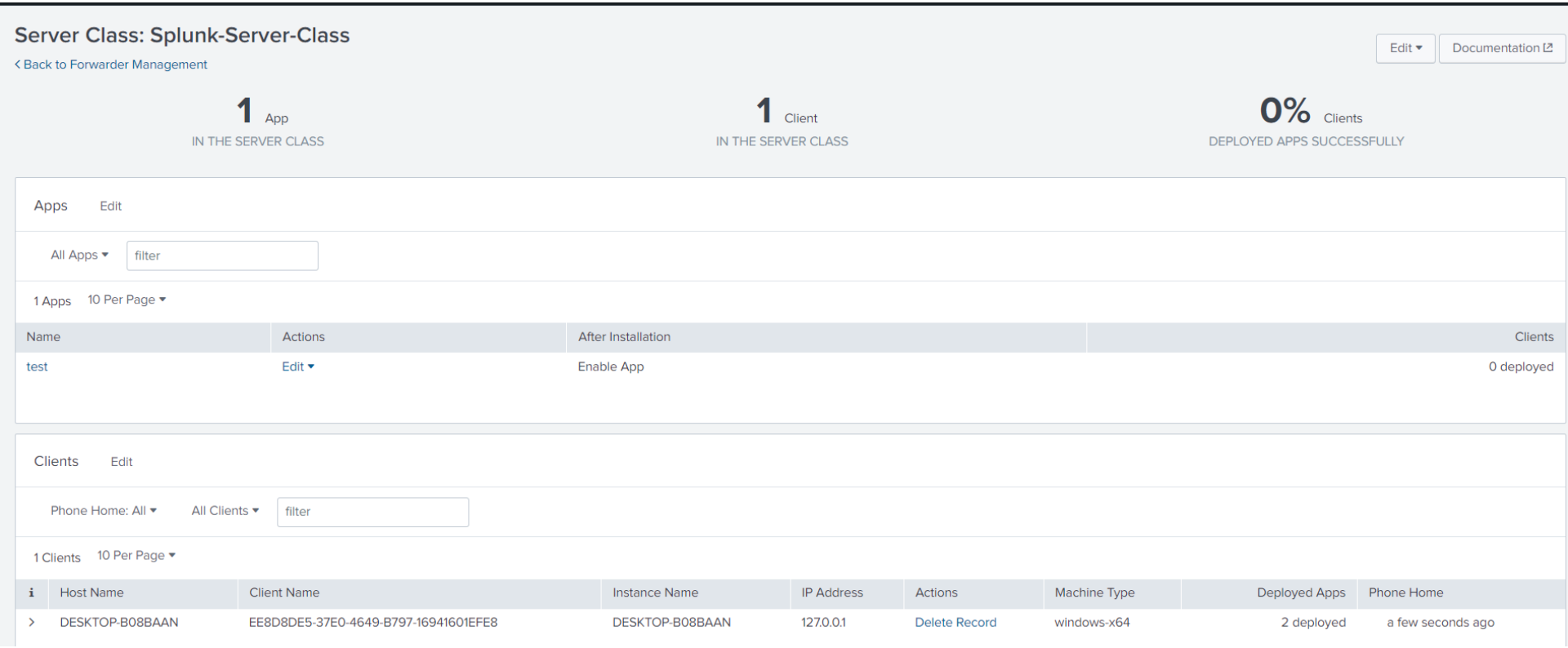
Creating App



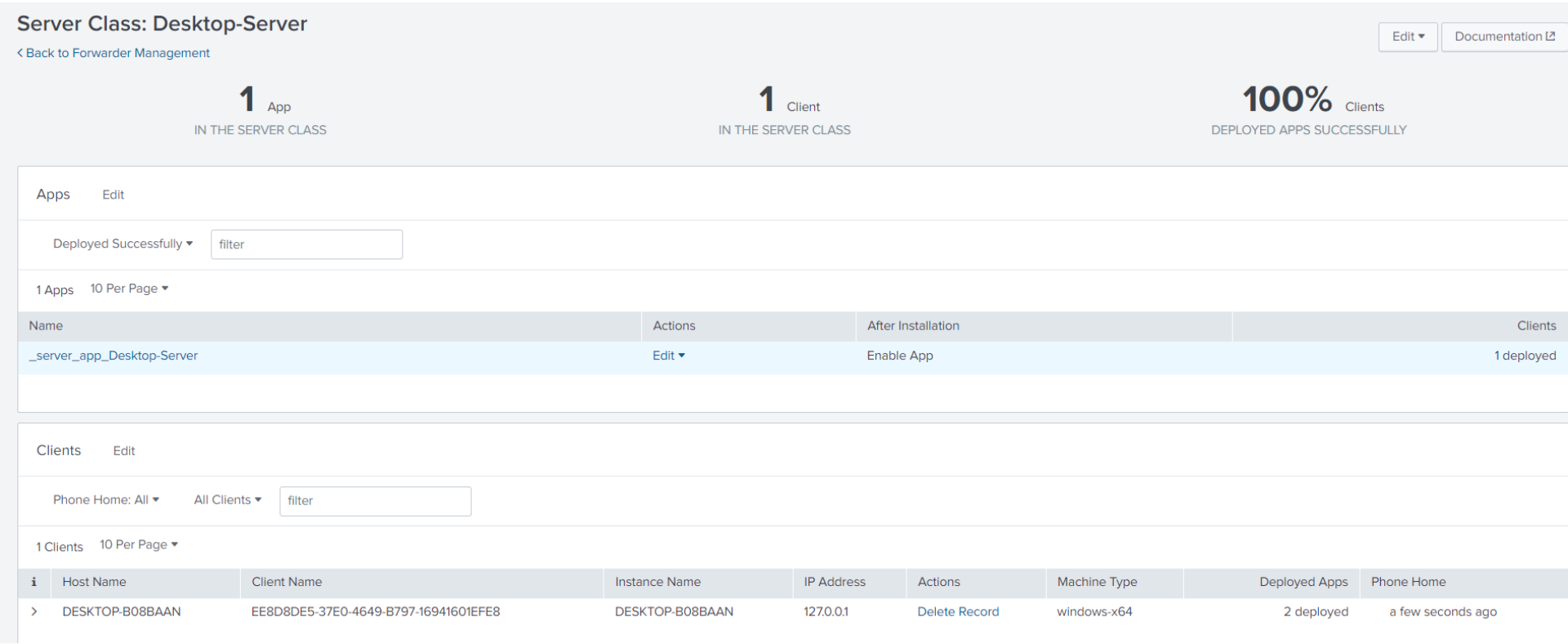
Creating App



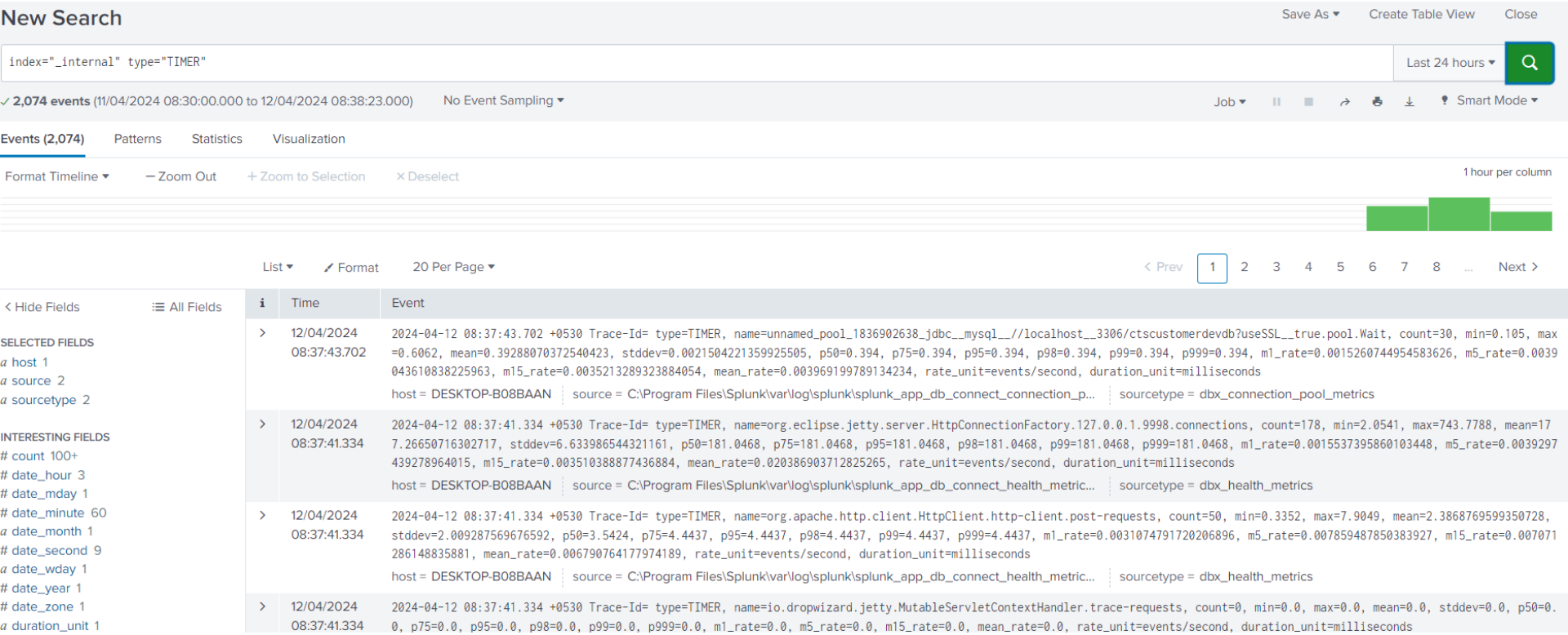
Creating App



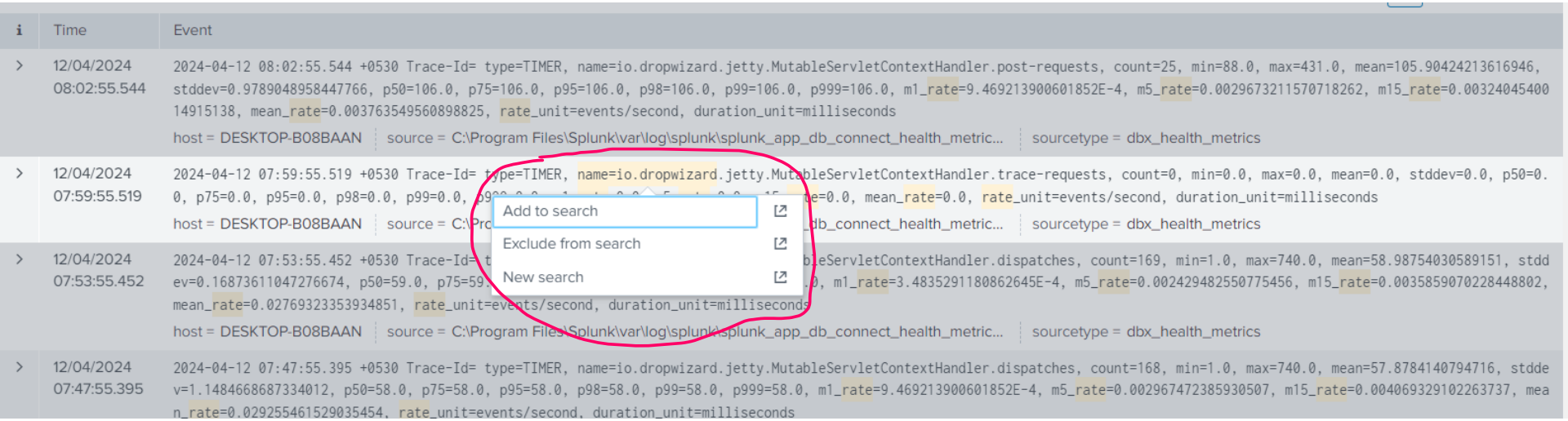
Creating App



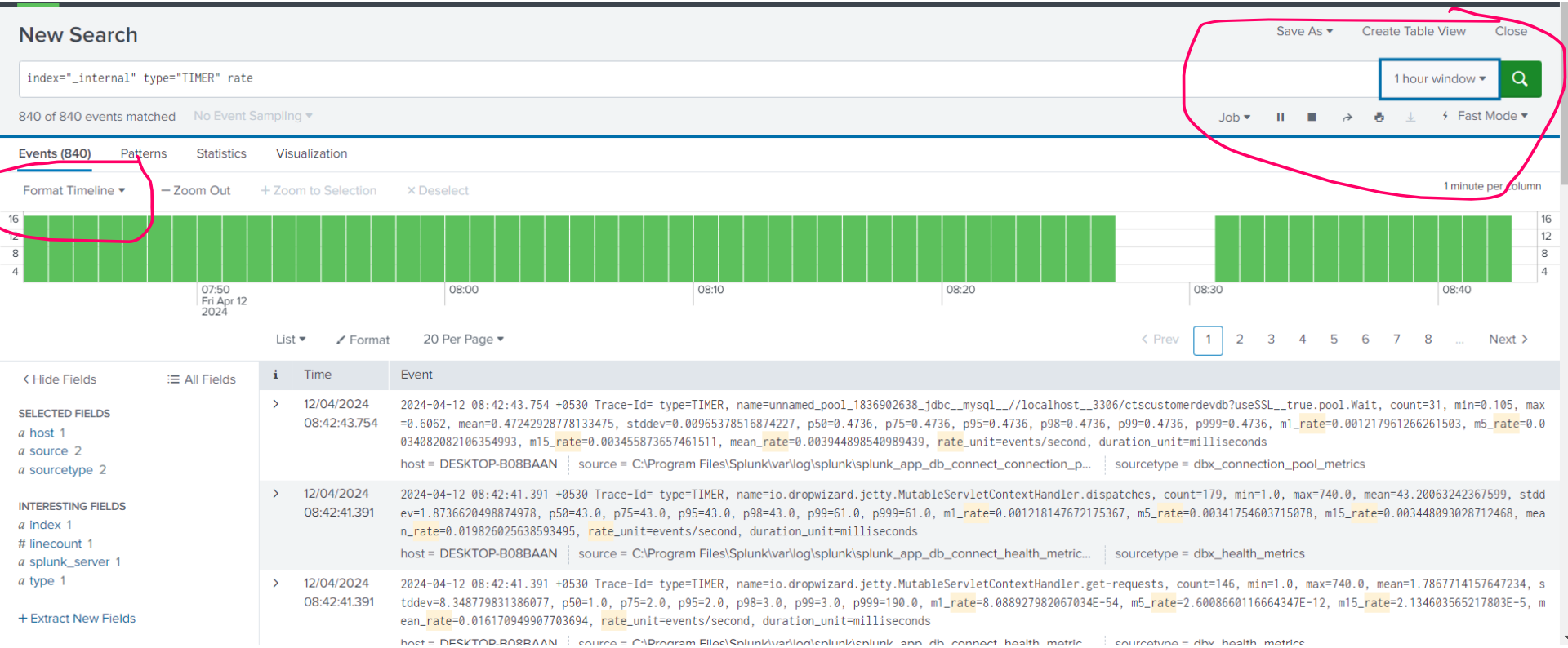
Search Fields



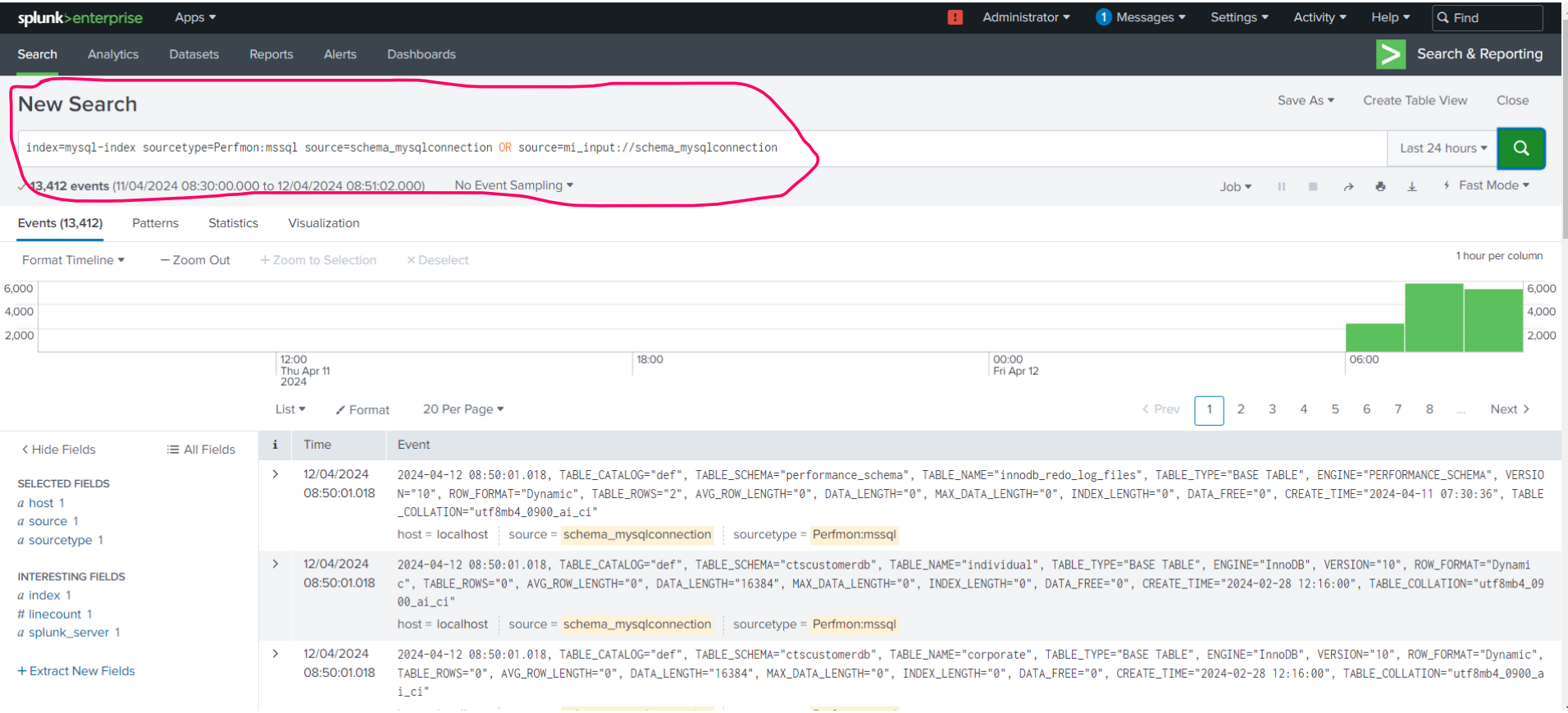
Search Fields



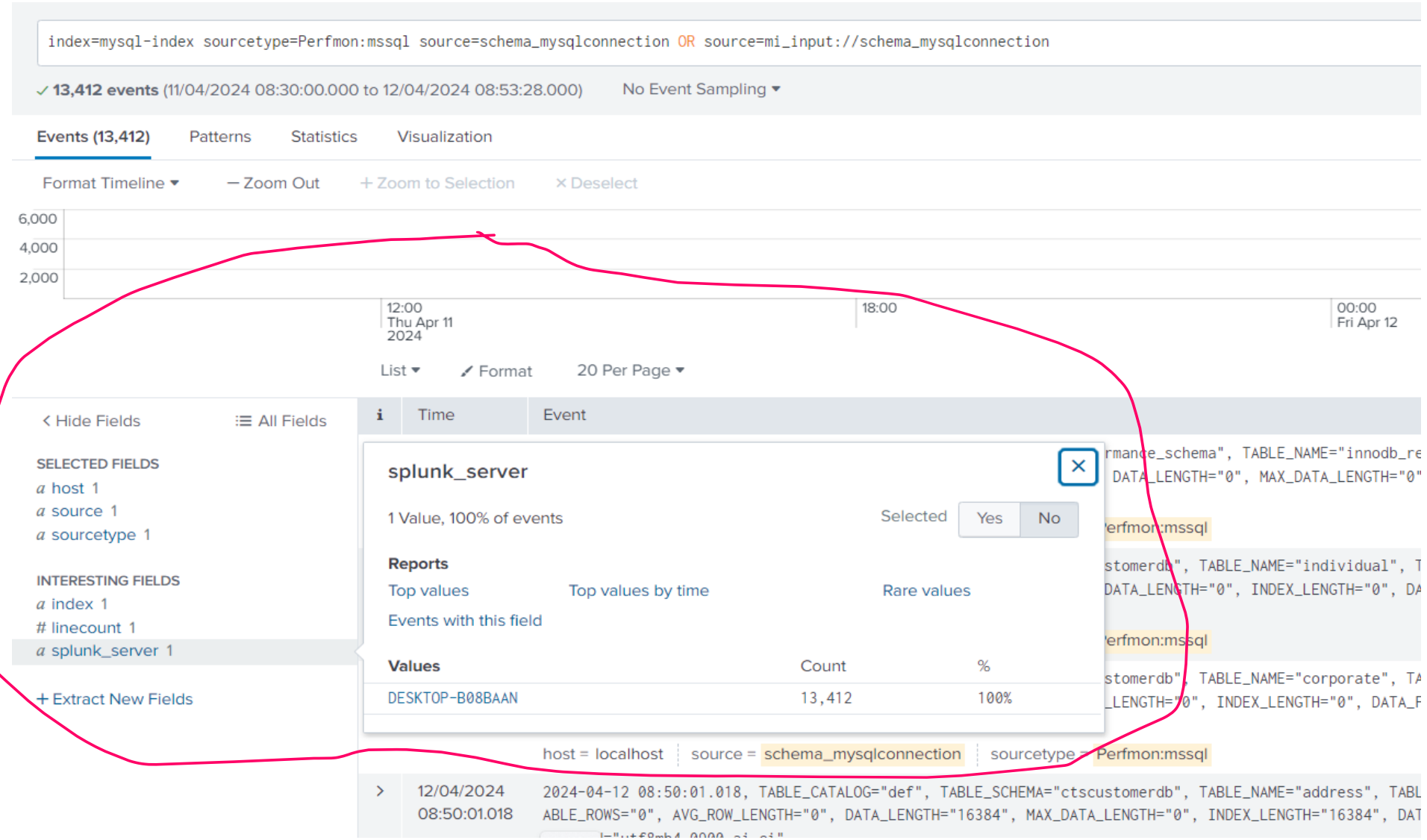
Search Fields



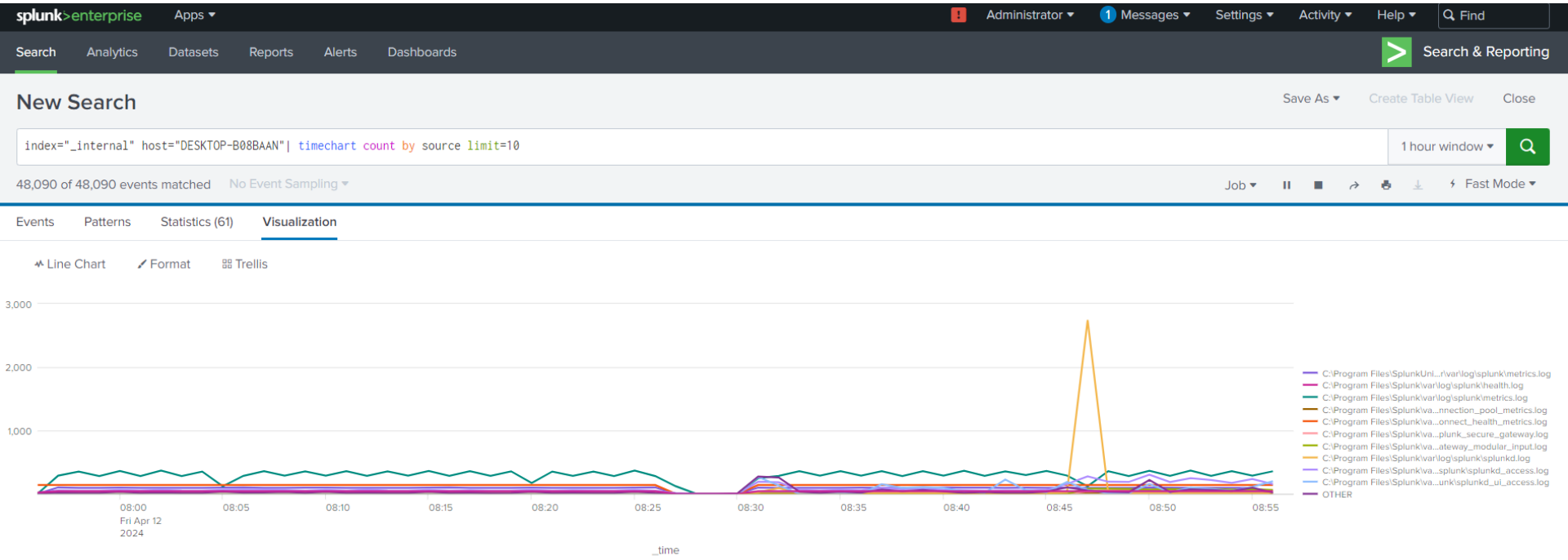
Search Fields



Search Fields

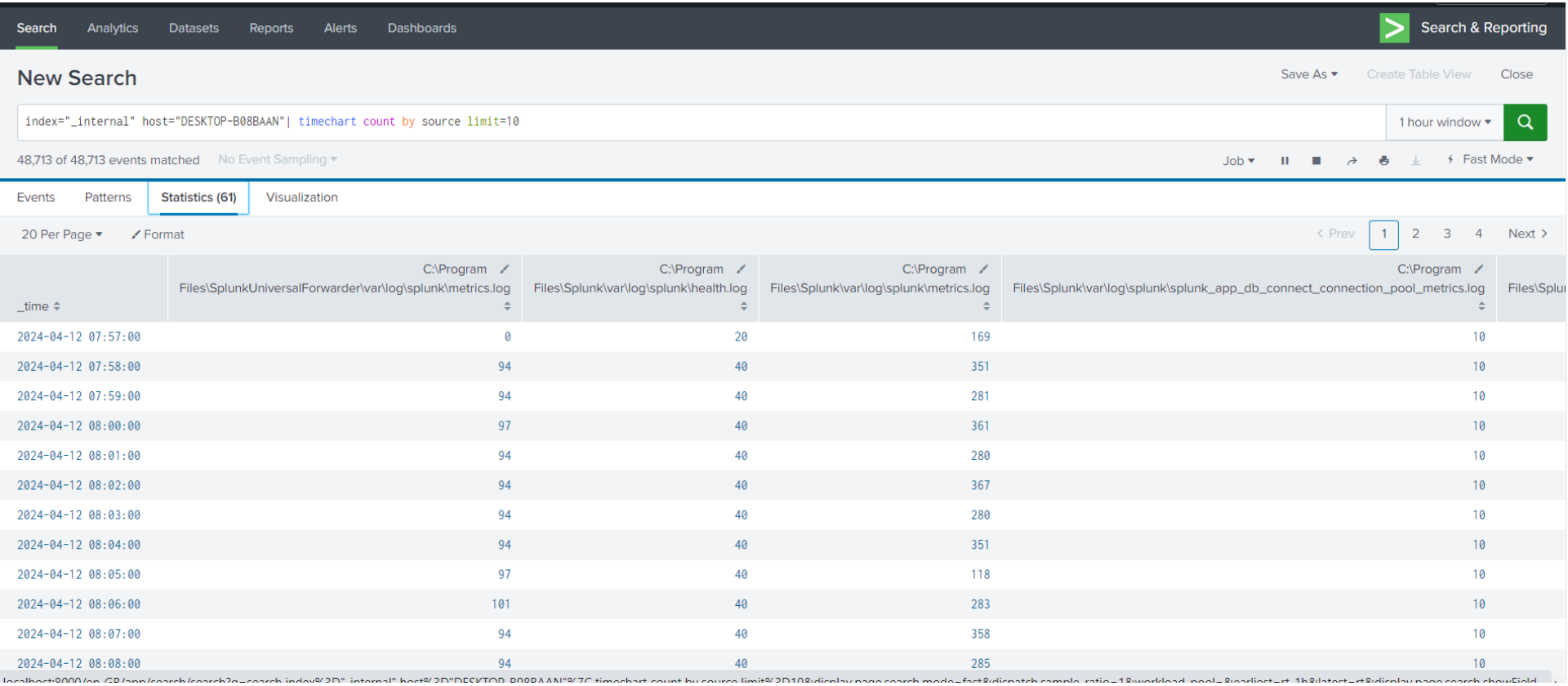


Reports

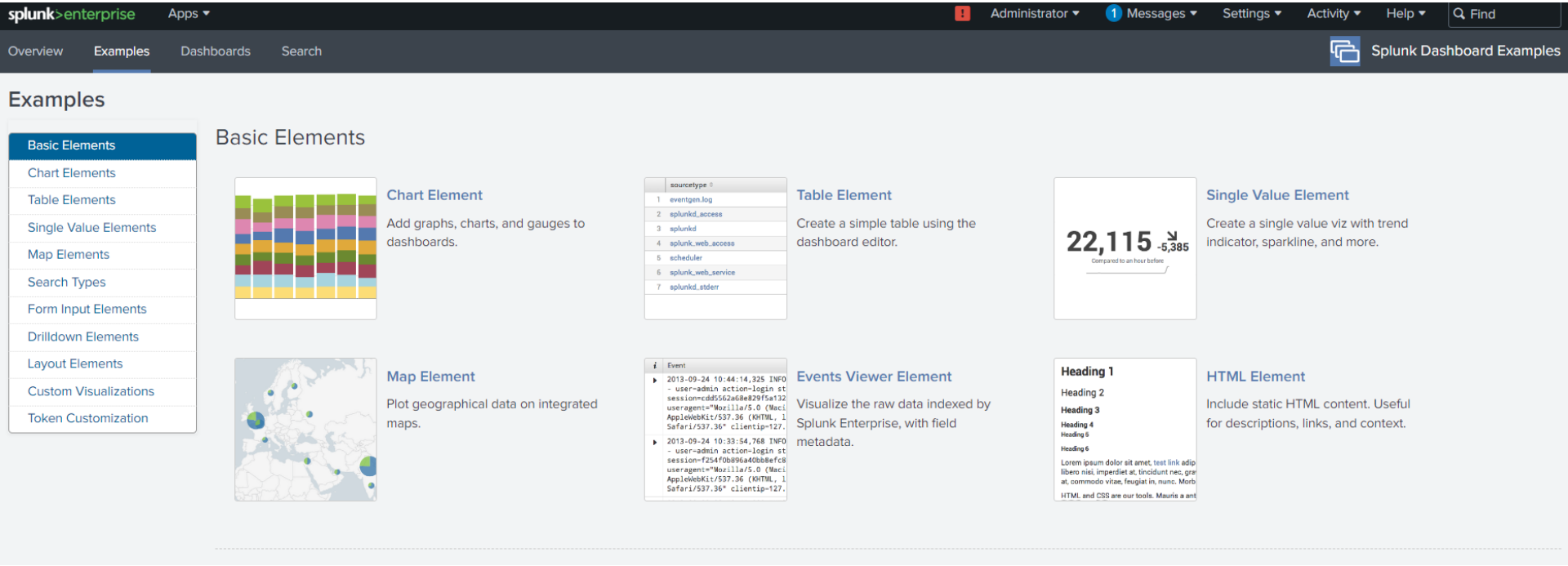


_time	C:\Program Files\SplunkUniversalForwarder\var\log\splunk\metrics.log	C:\Program Files\Splunk\var\log\splunk\health.log	C:\Program Files\Splunk\var\log\splunk\metrics.log	C:\Program Files\Splunk\var\log\splunk\splunk_app_db_conn
2024-04-12 07:56:00	0	20	0	
2024-04-12 07:57:00	101	40	286	
2024-04-12 07:58:00	94	40	351	

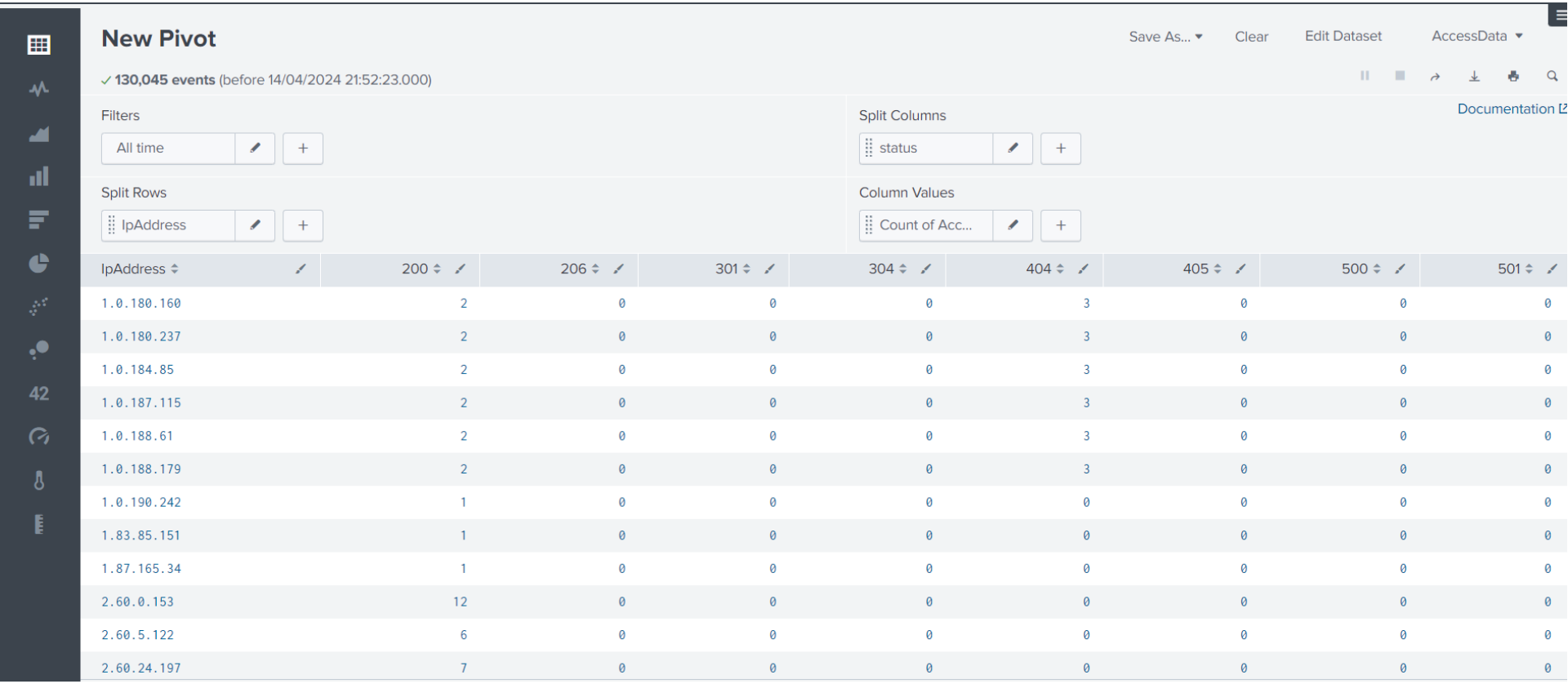
Statistics


Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index="_internal" host="DESKTOP-B08BAAN"| timechart count by source limit=10
1 hour window
48,713 of 48,713 events matched
No Event Sampling
Job
Fast Mode
Events
Patterns
Statistics (61)
Visualization
20 Per Page
Format
Prev
1
2
3
4
Next
_time
C:\Program Files\SplunkUniversalForwarder\var\log\splunk\metrics.log
C:\Program Files\Splunk\var\log\splunk\health.log
C:\Program Files\Splunk\var\log\splunk\metrics.log
C:\Program Files\Splunk\var\log\splunk\splunk_app_db_connect_connection_pool_metrics.log
2024-04-12 07:57:00 0 20 169 10
2024-04-12 07:58:00 94 40 351 10
2024-04-12 07:59:00 94 40 281 10
2024-04-12 08:00:00 97 40 361 10
2024-04-12 08:01:00 94 40 280 10
2024-04-12 08:02:00 94 40 367 10
2024-04-12 08:03:00 94 40 280 10
2024-04-12 08:04:00 94 40 351 10
2024-04-12 08:05:00 97 40 118 10
2024-04-12 08:06:00 101 40 283 10
2024-04-12 08:07:00 94 40 358 10
2024-04-12 08:08:00 94 40 285 10

Switch Apps

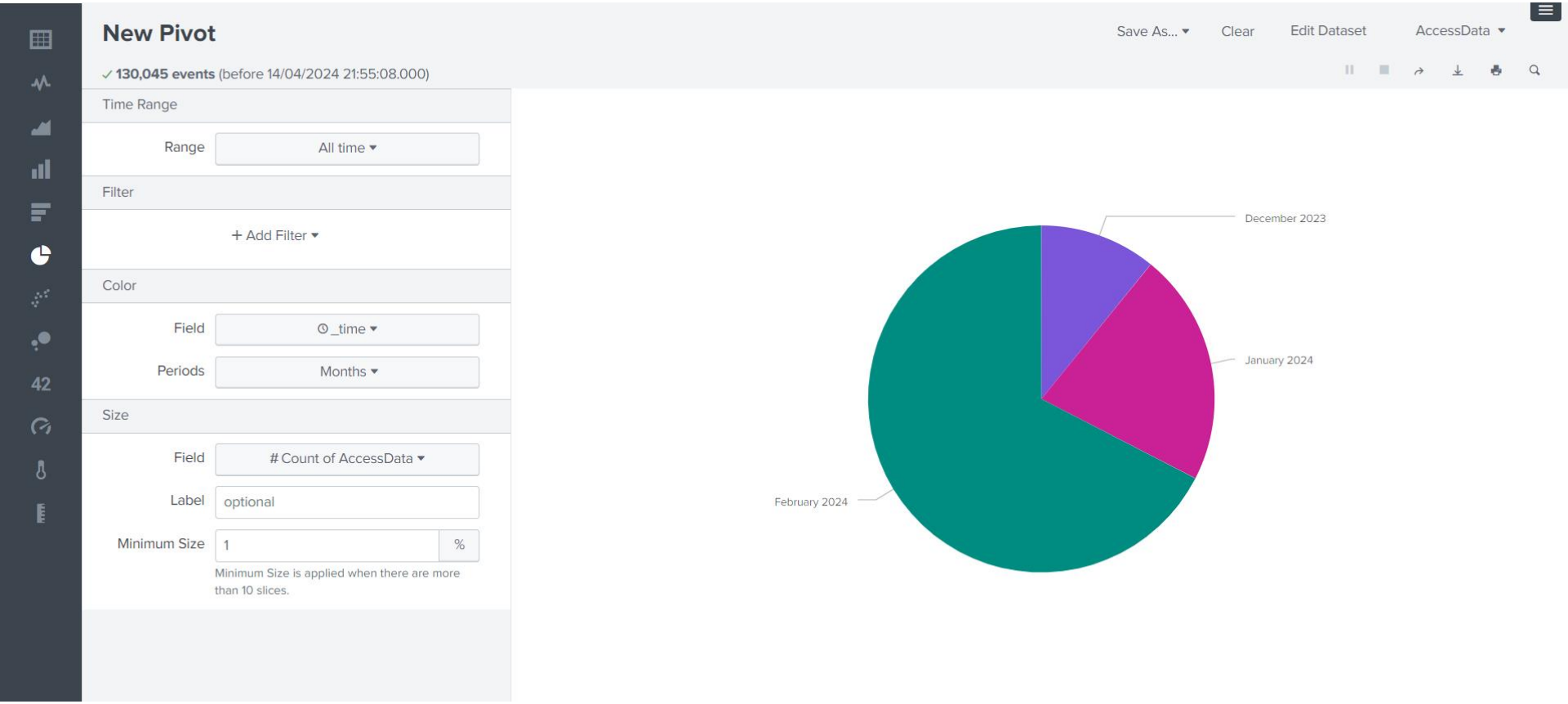

splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Overview
Examples
Dashboards
Search
Splunk Dashboard Examples
Examples
Basic Elements
Chart Elements
Table Elements
Single Value Elements
Map Elements
Search Types
Form Input Elements
Drilldown Elements
Layout Elements
Custom Visualizations
Token Customization
Basic Elements
Chart Element
Add graphs, charts, and gauges to dashboards.
sourcetype
1 eventgen.log
2 splunkd_access
3 splunkd
4 splunk_web_access
5 scheduler
6 splunk_web_service
7 splunkd_stderr
Table Element
Create a simple table using the dashboard editor.
22,115
-5,385
Compared to an hour before
Single Value Element
Create a single value viz with trend indicator, sparkline, and more.
Map Element
Plot geographical data on integrated maps.
Event
Events Viewer Element
Visualize the raw data indexed by Splunk Enterprise, with field metadata.
Heading 1
Heading 2
Heading 3
Heading 4
Heading 5
Heading 6
HTML Element
Include static HTML content. Useful for descriptions, links, and context.

Pivot Table

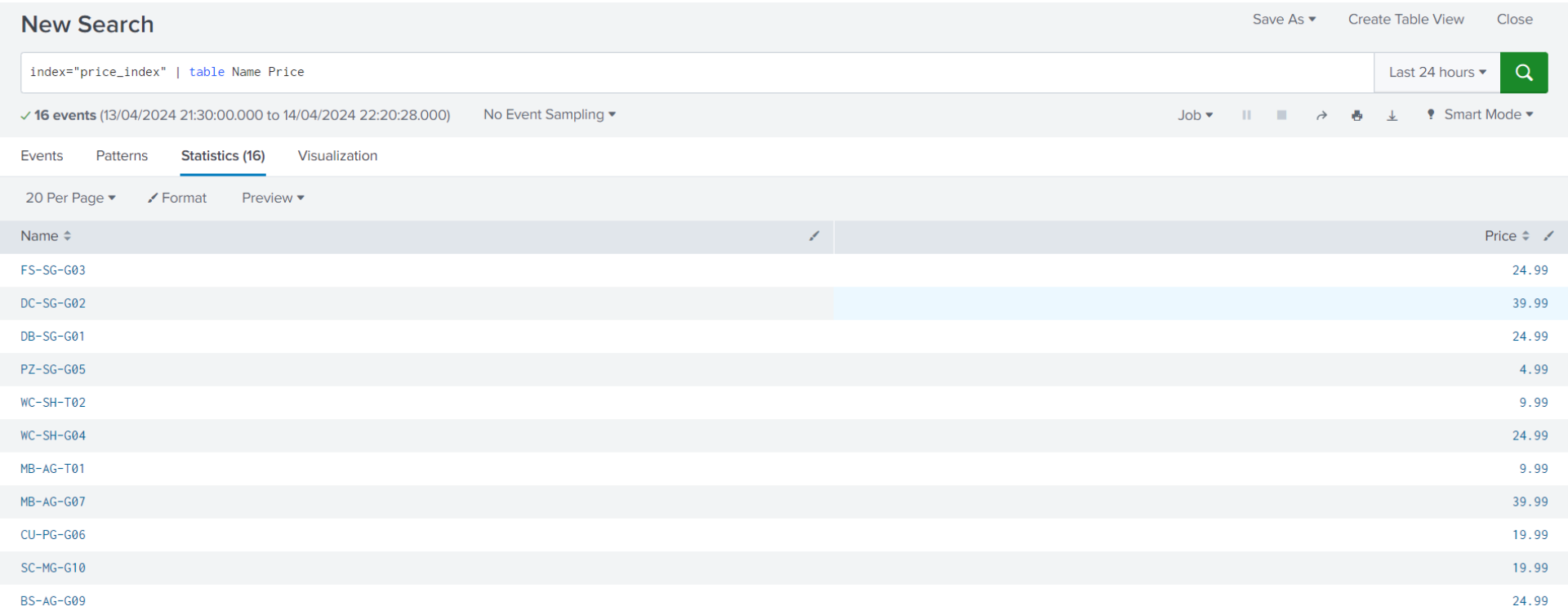


IpAddress	200	206	301	304	404	405	500	501
1.0.180.160	2	0	0	0	3	0	0	0
1.0.180.237	2	0	0	0	3	0	0	0
1.0.184.85	2	0	0	0	3	0	0	0
1.0.187.115	2	0	0	0	3	0	0	0
1.0.188.61	2	0	0	0	3	0	0	0
1.0.188.179	2	0	0	0	3	0	0	0
1.0.190.242	1	0	0	0	0	0	0	0
1.83.85.151	1	0	0	0	0	0	0	0
1.87.165.34	1	0	0	0	0	0	0	0
2.60.0.153	12	0	0	0	0	0	0	0
2.60.5.122	6	0	0	0	0	0	0	0
2.60.24.197	7	0	0	0	0	0	0	0

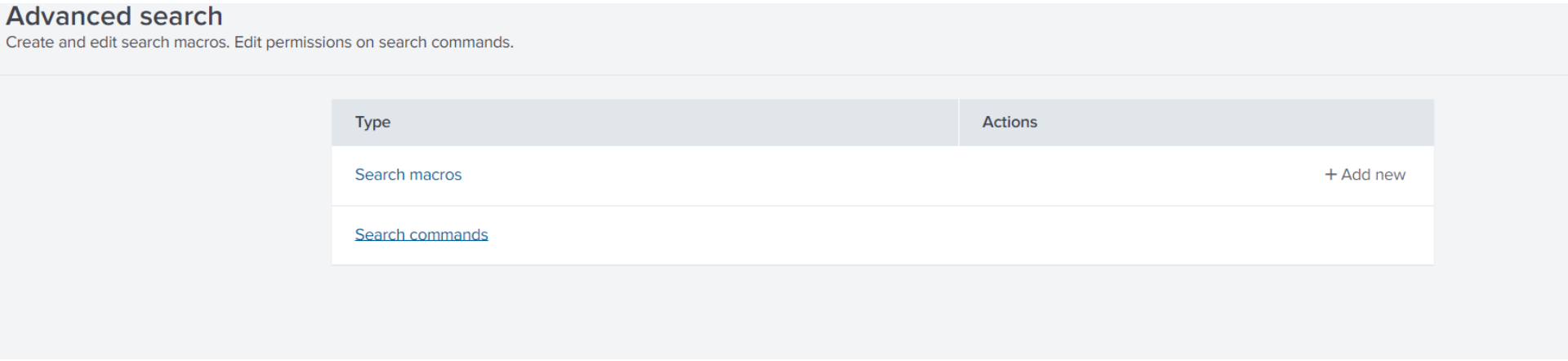
Pivot Table


New Pivot
Save As...
Clear
Edit Dataset
AccessData
130,045 events (before 14/04/2024 21:55:08.000)
Time Range
Range
All time
Filter
+ Add Filter
Color
Field
_time
Periods
Months
Size
Field
Count of AccessData
Label
optional
Minimum Size
1
%
Minimum Size is applied when there are more than 10 slices.
December 2023
January 2024
February 2024

Macros

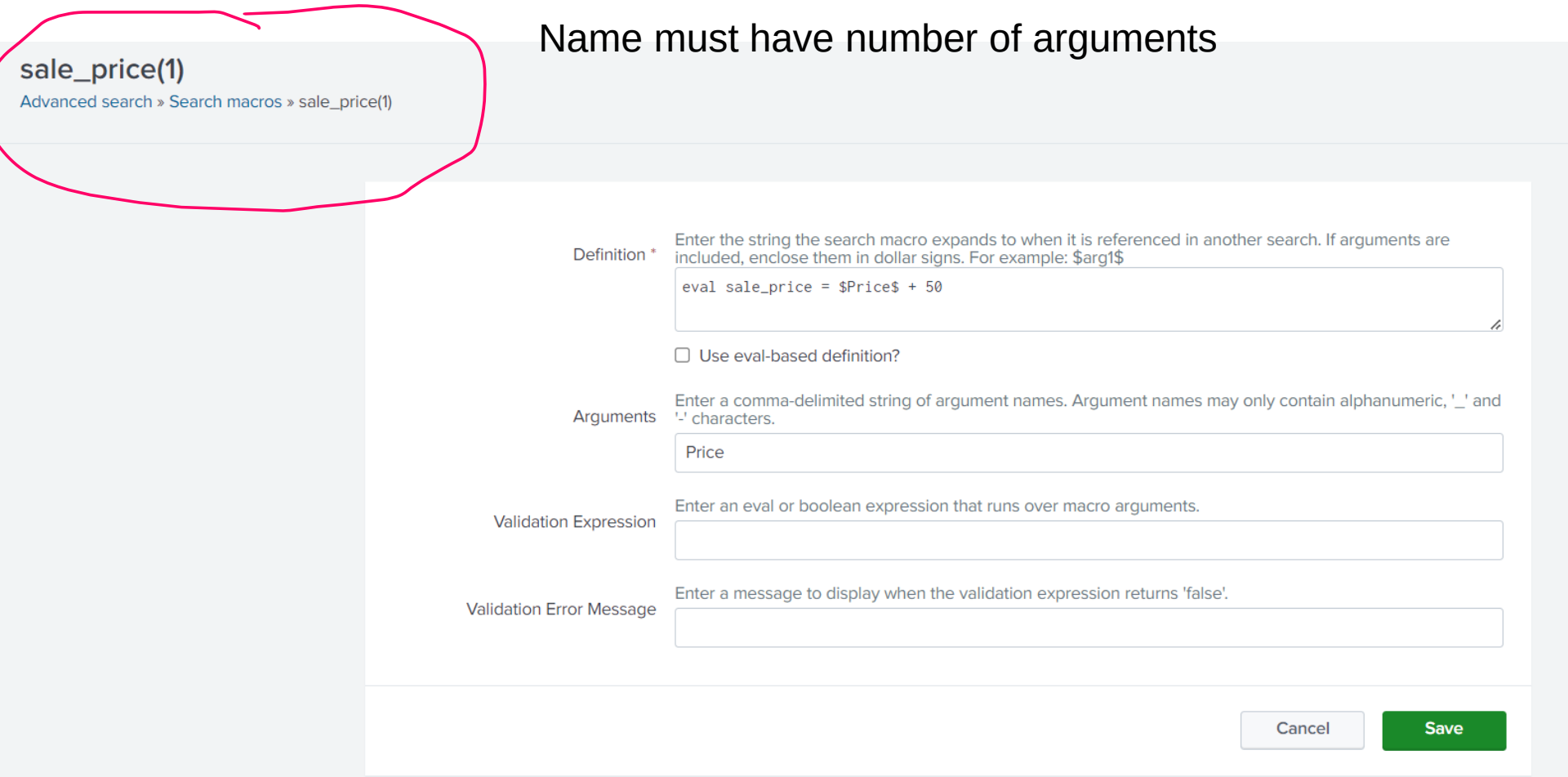

New Search
Save As
Create Table View
Close
index="price_index" | table Name Price
Last 24 hours
16 events (13/04/2024 21:30:00.000 to 14/04/2024 22:20:28.000)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (16)
Visualization
20 Per Page
Format
Preview
Name
Price
FS-SG-G03 24.99
DC-SG-G02 39.99
DB-SG-G01 24.99
PZ-SG-G05 4.99
WC-SH-T02 9.99
WC-SH-G04 24.99
MB-AG-T01 9.99
MB-AG-G07 39.99
CU-PG-G06 19.99
SC-MG-G10 19.99
BS-AG-G09 24.99

Macros

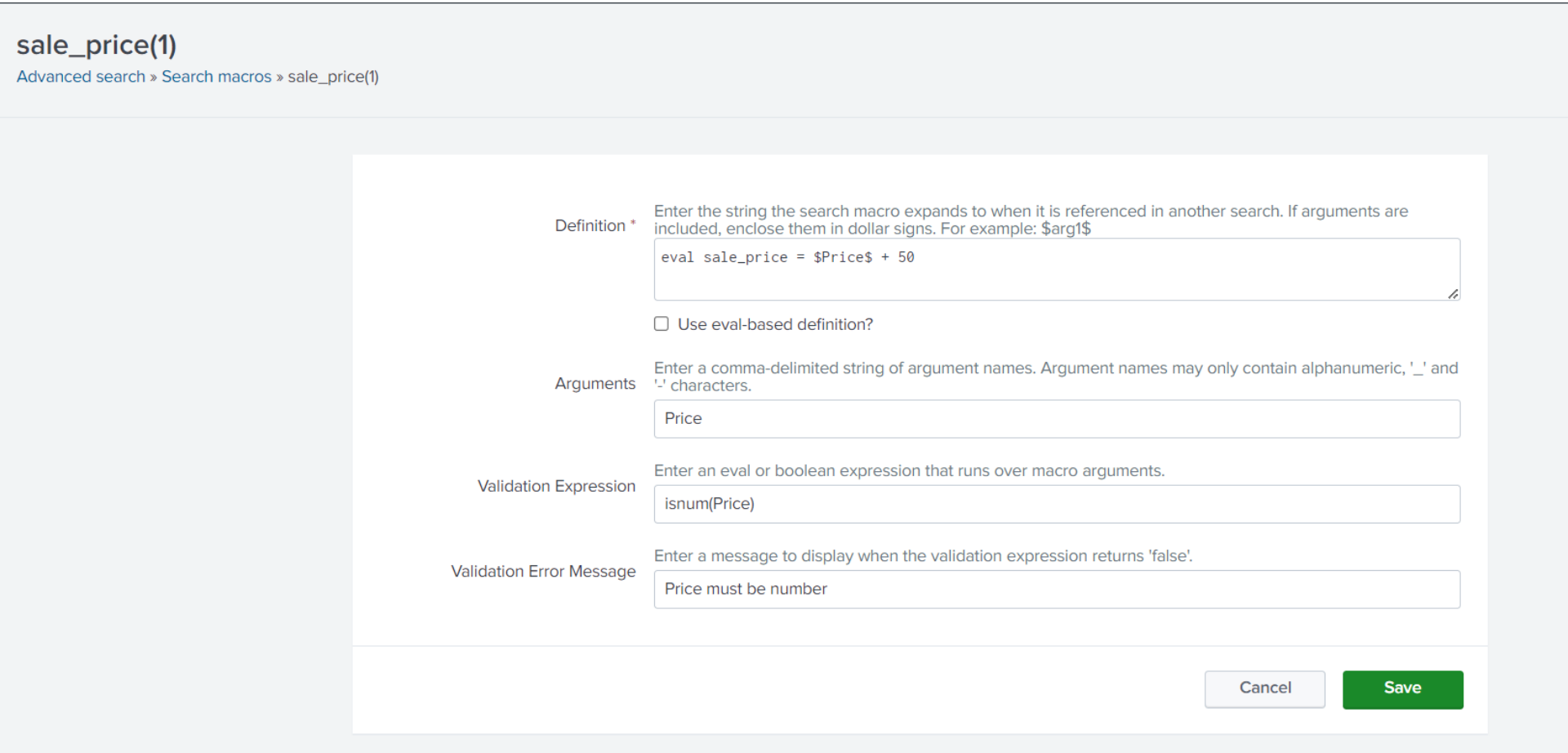

Advanced search
Create and edit search macros. Edit permissions on search commands.
Type
Actions
Search macros
+ Add new
Search commands

Macros

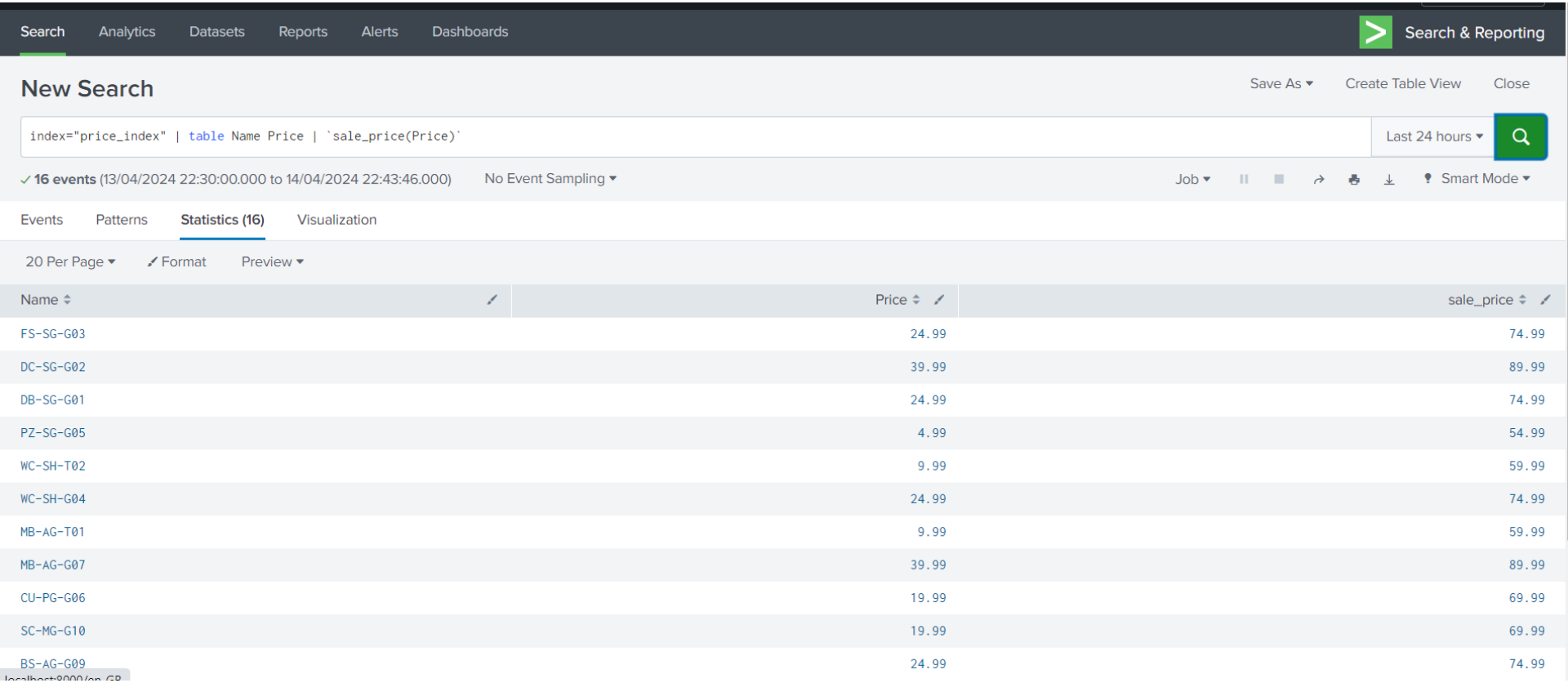
Name must have number of arguments



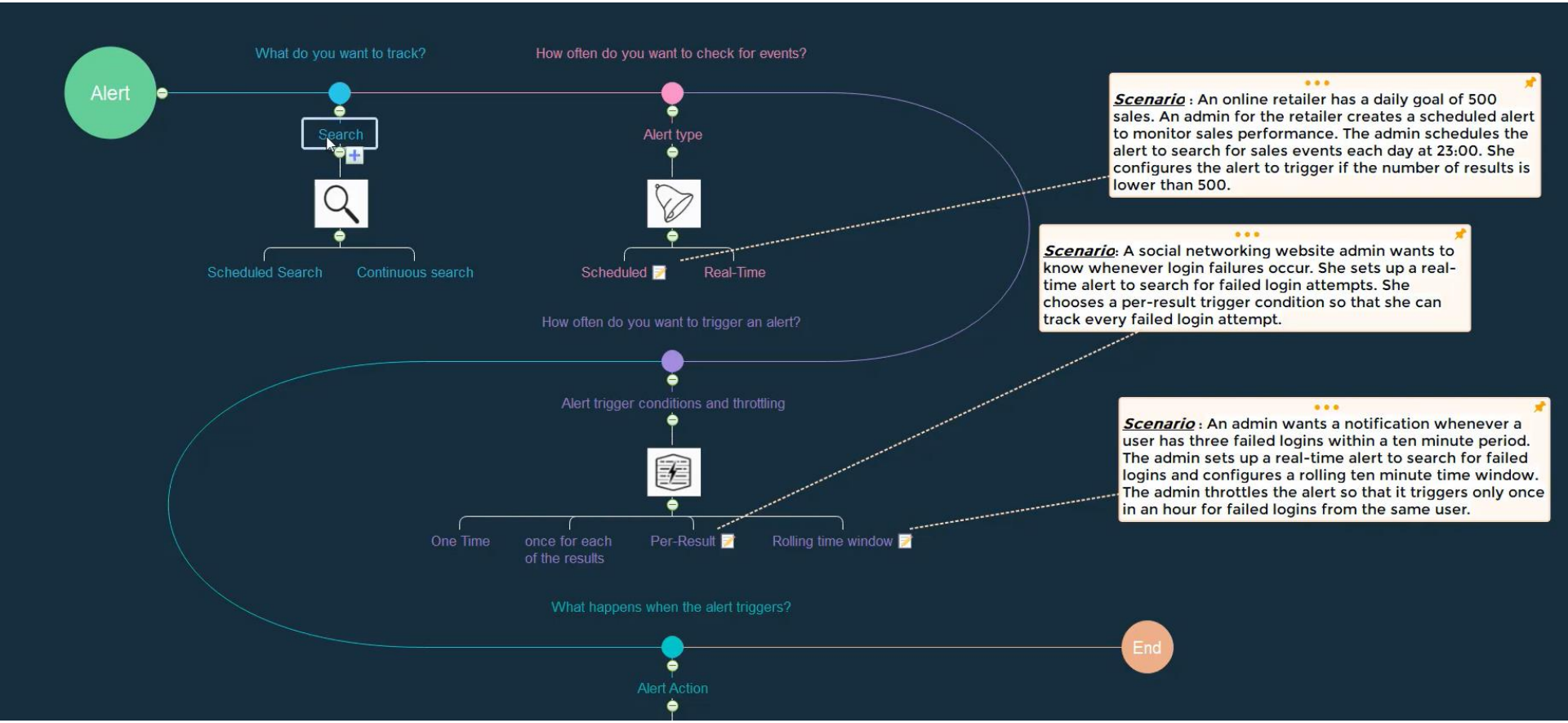
Macros


sale_price(1)
Advanced search » Search macros » sale_price(1)
Definition *
Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: $arg1$
eval sale_price = $Price$ + 50
Use eval-based definition?
Arguments
Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.
Price
Validation Expression
Enter an eval or boolean expression that runs over macro arguments.
isnum(Price)
Validation Error Message
Enter a message to display when the validation expression returns 'false'.
Price must be number
Cancel
Save

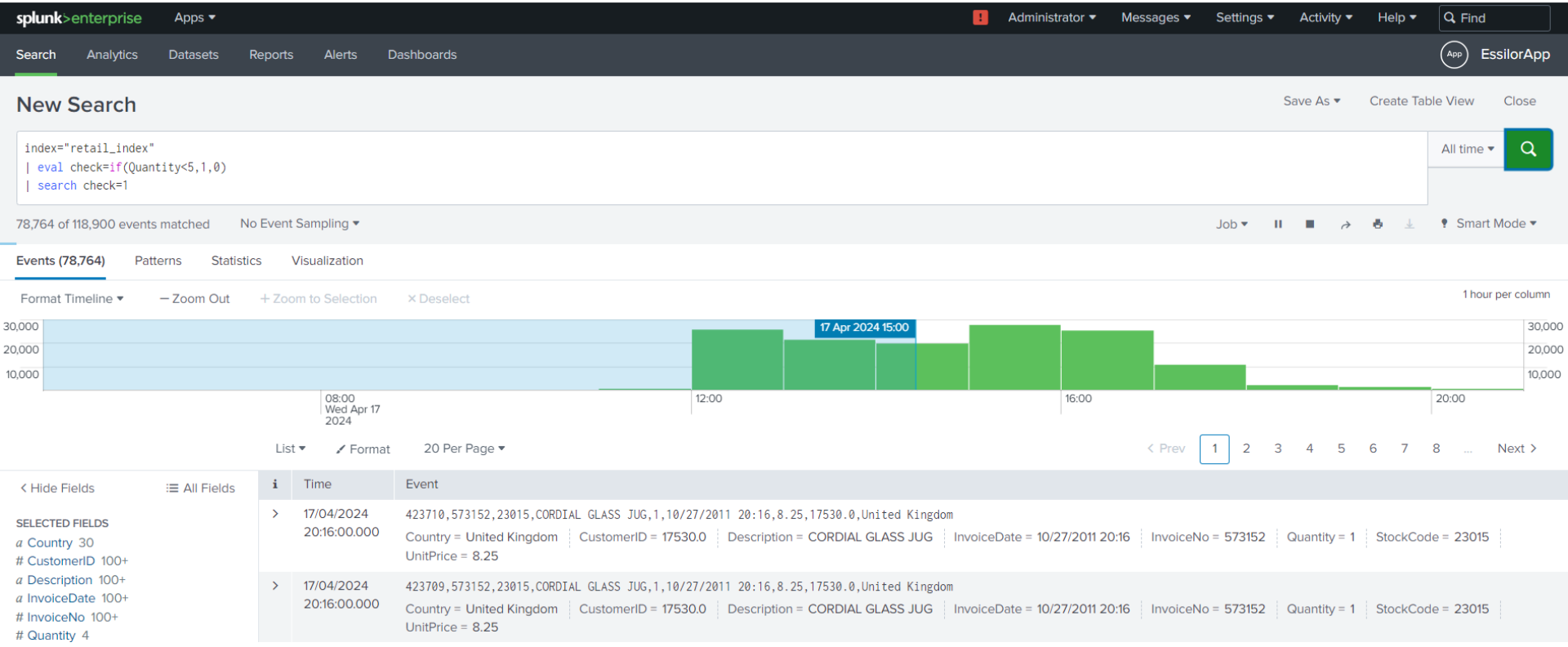
Macros


Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index="price_index" | table Name Price | `sale_price(Price)`
Last 24 hours
16 events (13/04/2024 22:30:00.000 to 14/04/2024 22:43:46.000)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (16)
Visualization
20 Per Page
Format
Preview
Name
Price
sale_price
FS-SG-G03 24.99 74.99
DC-SG-G02 39.99 89.99
DB-SG-G01 24.99 74.99
PZ-SG-G05 4.99 54.99
WC-SH-T02 9.99 59.99
WC-SH-G04 24.99 74.99
MB-AG-T01 9.99 59.99
MB-AG-G07 39.99 89.99
CU-PG-G06 19.99 69.99
SC-MG-G10 19.99 69.99
BS-AG-G09 24.99 74.99

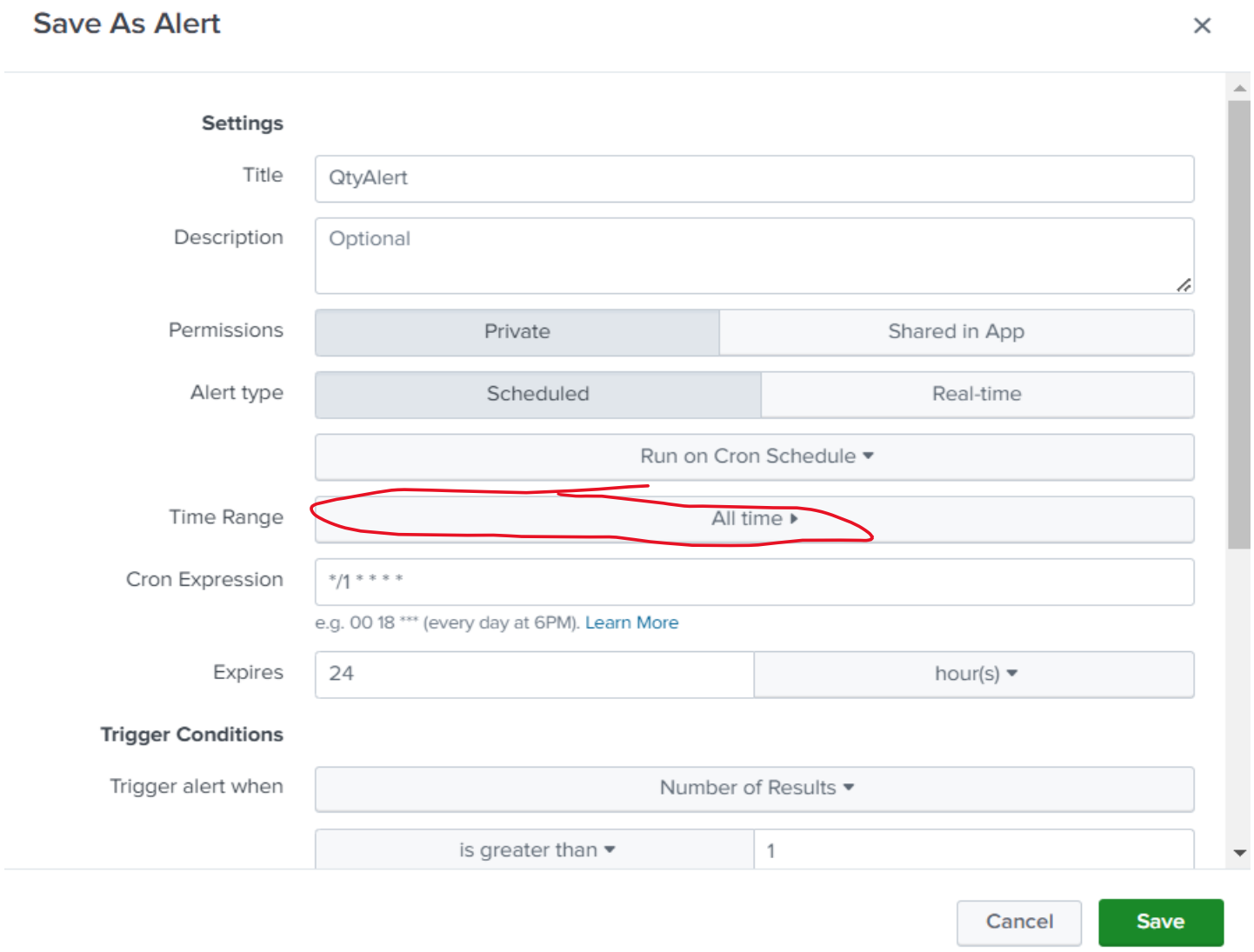
Alerts


Alert
What do you want to track?
How often do you want to check for events?
Search
Alert type
Scheduled Search
Continuous search
Scheduled
Real-Time
How often do you want to trigger an alert?
Alert trigger conditions and throttling
One Time
once for each of the results
Per-Result
Rolling time window
What happens when the alert triggers?
Alert Action
End
Scenario : An online retailer has a daily goal of 500 sales. An admin for the retailer creates a scheduled alert to monitor sales performance. The admin schedules the alert to search for sales events each day at 23:00. She configures the alert to trigger if the number of results is lower than 500.
Scenario: A social networking website admin wants to know whenever login failures occur. She sets up a real-time alert to search for failed login attempts. She chooses a per-result trigger condition so that she can track every failed login attempt.
Scenario : An admin wants a notification whenever a user has three failed logins within a ten minute period. The admin sets up a real-time alert to search for failed logins and configures a rolling ten minute time window. The admin throttles the alert so that it triggers only once in an hour for failed logins from the same user.

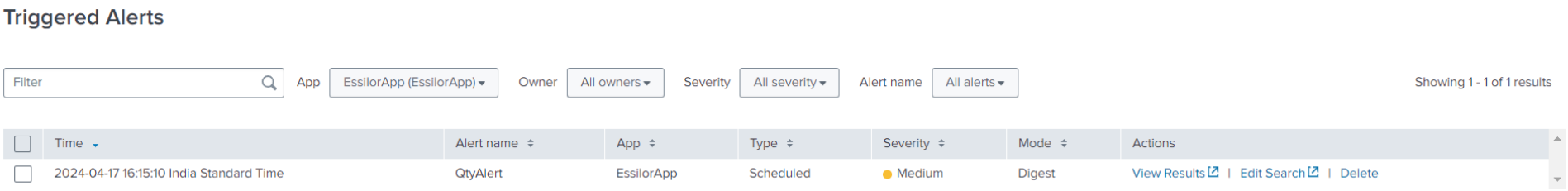
Alerts


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
EssilorApp
New Search
Save As
Create Table View
Close
index="retail_index"
| eval check=if(Quantity<5,1,0)
| search check=1
All time
78,764 of 118,900 events matched
No Event Sampling
Job
Smart Mode
Events (78,764)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
30,000
20,000
10,000
17 Apr 2024 15:00
08:00
Wed Apr 17
2024
12:00
16:00
20:00
List
Format
20 Per Page
Prev
1
2
3
4
5
6
7
8
Next
Hide Fields
All Fields
SELECTED FIELDS
a Country 30
CustomerID 100+
a Description 100+
a InvoiceDate 100+
InvoiceNo 100+
Quantity 4
Time
Event
17/04/2024
20:16:00.000
423710,573152,23015,CORDIAL GLASS JUG,1,10/27/2011 20:16,8.25,17530.0,United Kingdom
Country = United Kingdom
CustomerID = 17530.0
Description = CORDIAL GLASS JUG
InvoiceDate = 10/27/2011 20:16
InvoiceNo = 573152
Quantity = 1
StockCode = 23015
UnitPrice = 8.25
17/04/2024
20:16:00.000
423709,573152,23015,CORDIAL GLASS JUG,1,10/27/2011 20:16,8.25,17530.0,United Kingdom
Country = United Kingdom
CustomerID = 17530.0
Description = CORDIAL GLASS JUG
InvoiceDate = 10/27/2011 20:16
InvoiceNo = 573152
Quantity = 1
StockCode = 23015
UnitPrice = 8.25

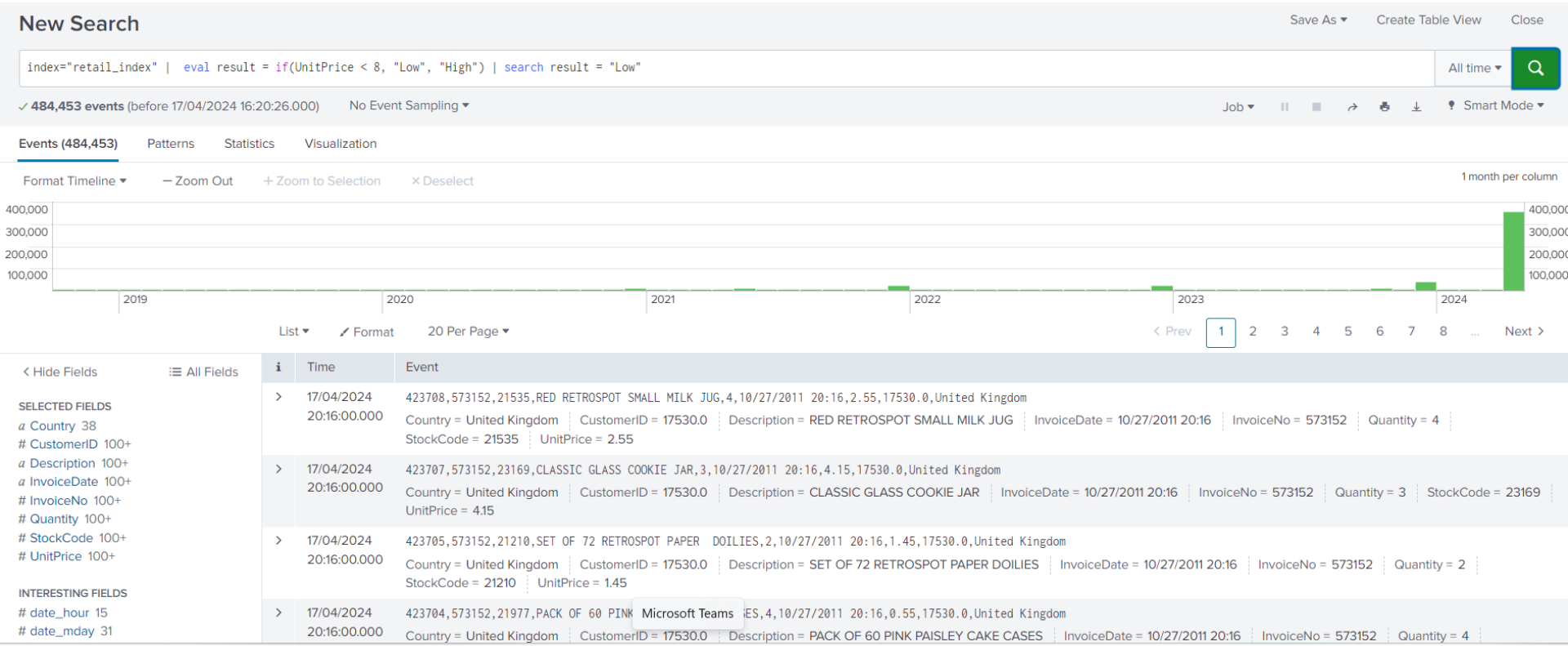
Alerts


Save As Alert
Settings
Title
QtyAlert
Description
Optional
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run on Cron Schedule
Time Range
All time
Cron Expression
*/1 * * * *
e.g. 00 18 *** (every day at 6PM). Learn More
Expires
24
hour(s)
Trigger Conditions
Trigger alert when
Number of Results
is greater than
1
Cancel
Save

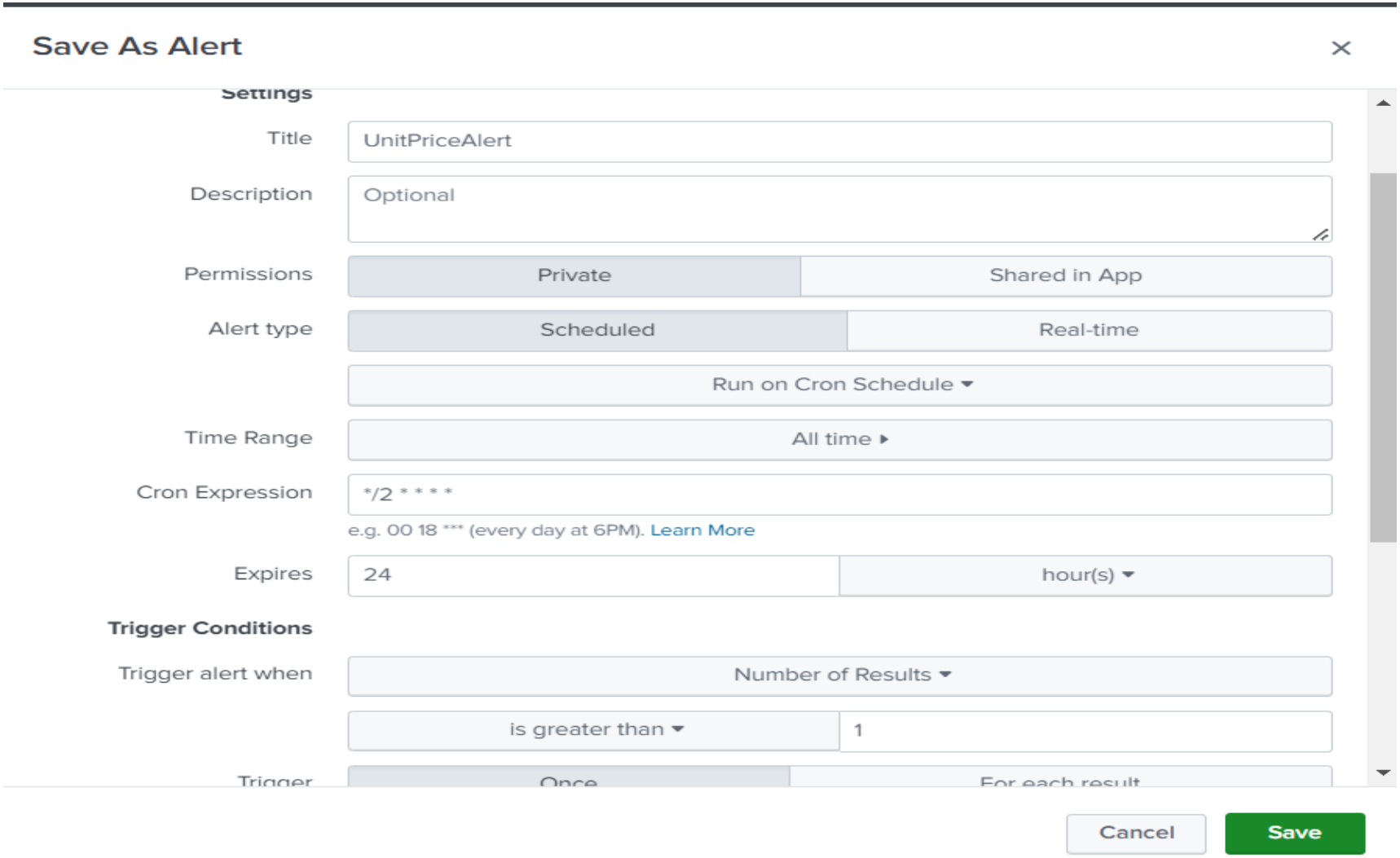
Alerts


Triggered Alerts
Filter
App
EssilorApp (EssilorApp)
Owner
All owners
Severity
All severity
Alert name
All alerts
Showing 1 - 1 of 1 results
Time
Alert name
App
Type
Severity
Mode
Actions
2024-04-17 16:15:10 India Standard Time
QtyAlert
EssilorApp
Scheduled
Medium
Digest
View Results | Edit Search | Delete

Alerts


New Search
Save As
Create Table View
Close
index="retail_index" | eval result = if(UnitPrice < 8, "Low", "High") | search result = "Low"
All time
484,453 events (before 17/04/2024 16:20:26.000)
No Event Sampling
Job
Smart Mode
Events (484,453)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 month per column
400,000
300,000
200,000
100,000
2019
2020
2021
2022
2023
2024
List
Format
20 Per Page
Prev
1
2
3
4
5
6
7
8
Next
Hide Fields
All Fields
SELECTED FIELDS
a Country 38
CustomerID 100+
a Description 100+
a InvoiceDate 100+
InvoiceNo 100+
Quantity 100+
StockCode 100+
UnitPrice 100+
INTERESTING FIELDS
date_hour 15
date_mday 31
Time
Event
17/04/2024 20:16:00.000
423708,573152,21535,RED RETROSPOT SMALL MILK JUG,4,10/27/2011 20:16,2.55,17530.0,United Kingdom
Country = United Kingdom | CustomerID = 17530.0 | Description = RED RETROSPOT SMALL MILK JUG | InvoiceDate = 10/27/2011 20:16 | InvoiceNo = 573152 | Quantity = 4 | StockCode = 21535 | UnitPrice = 2.55
17/04/2024 20:16:00.000
423707,573152,23169,CLASSIC GLASS COOKIE JAR,3,10/27/2011 20:16,4.15,17530.0,United Kingdom
Country = United Kingdom | CustomerID = 17530.0 | Description = CLASSIC GLASS COOKIE JAR | InvoiceDate = 10/27/2011 20:16 | InvoiceNo = 573152 | Quantity = 3 | StockCode = 23169 | UnitPrice = 4.15
17/04/2024 20:16:00.000
423705,573152,21210,SET OF 72 RETROSPOT PAPER DOILIES,2,10/27/2011 20:16,1.45,17530.0,United Kingdom
Country = United Kingdom | CustomerID = 17530.0 | Description = SET OF 72 RETROSPOT PAPER DOILIES | InvoiceDate = 10/27/2011 20:16 | InvoiceNo = 573152 | Quantity = 2 | StockCode = 21210 | UnitPrice = 1.45
17/04/2024 20:16:00.000
423704,573152,21977,PACK OF 60 PINK
Microsoft Teams
ES,4,10/27/2011 20:16,0.55,17530.0,United Kingdom
Country = United Kingdom | CustomerID = 17530.0 | Description = PACK OF 60 PINK PAISLEY CAKE CASES | InvoiceDate = 10/27/2011 20:16 | InvoiceNo = 573152 | Quantity = 4

Alerts


Save As Alert
Settings
Title
UnitPriceAlert
Description
Optional
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run on Cron Schedule
Time Range
All time
Cron Expression
*/2 * * * *
e.g. 00 18 *** (every day at 6PM). Learn More
Expires
24
hour(s)
Trigger Conditions
Trigger alert when
Number of Results
is greater than
1
Trigger
Once
For each result
Cancel
Save

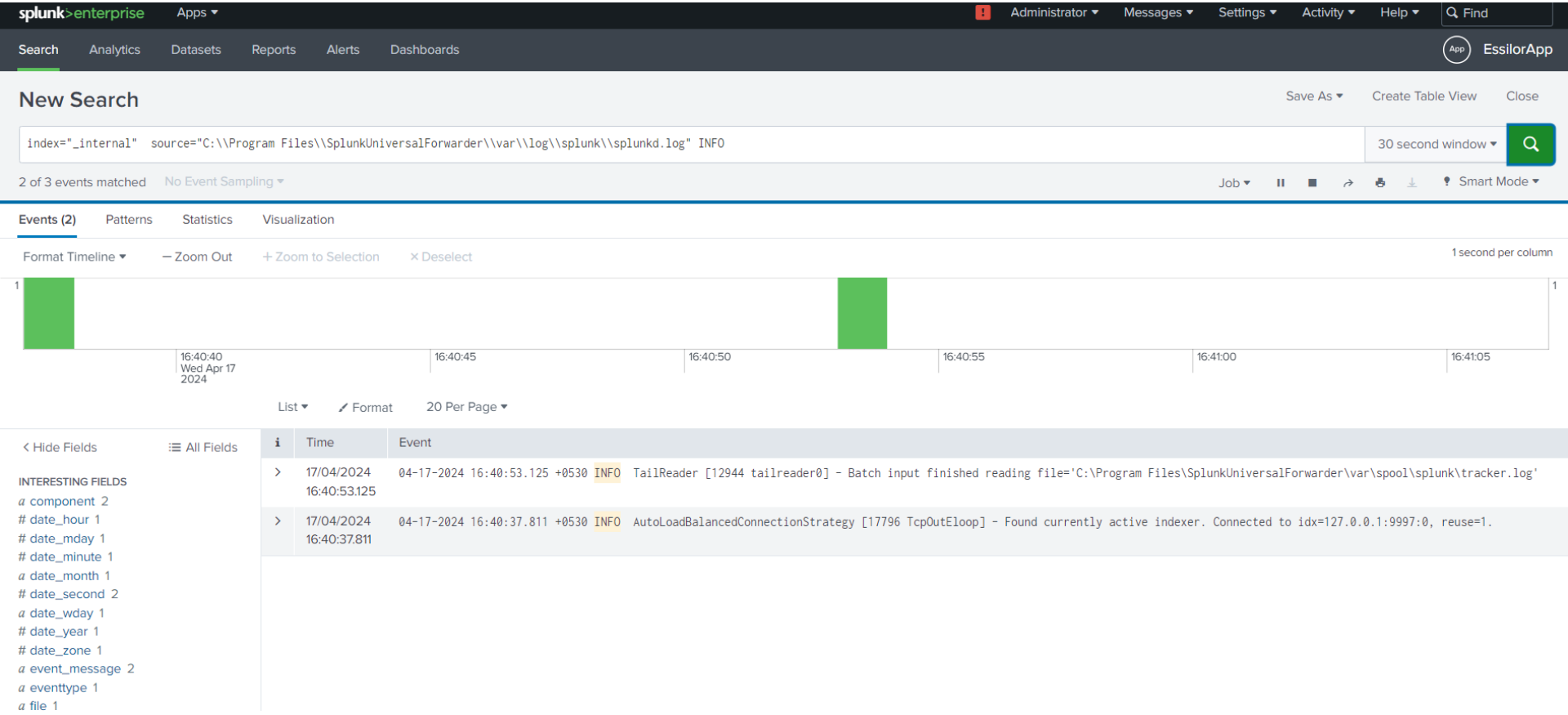
Alerts

Triggered Alerts

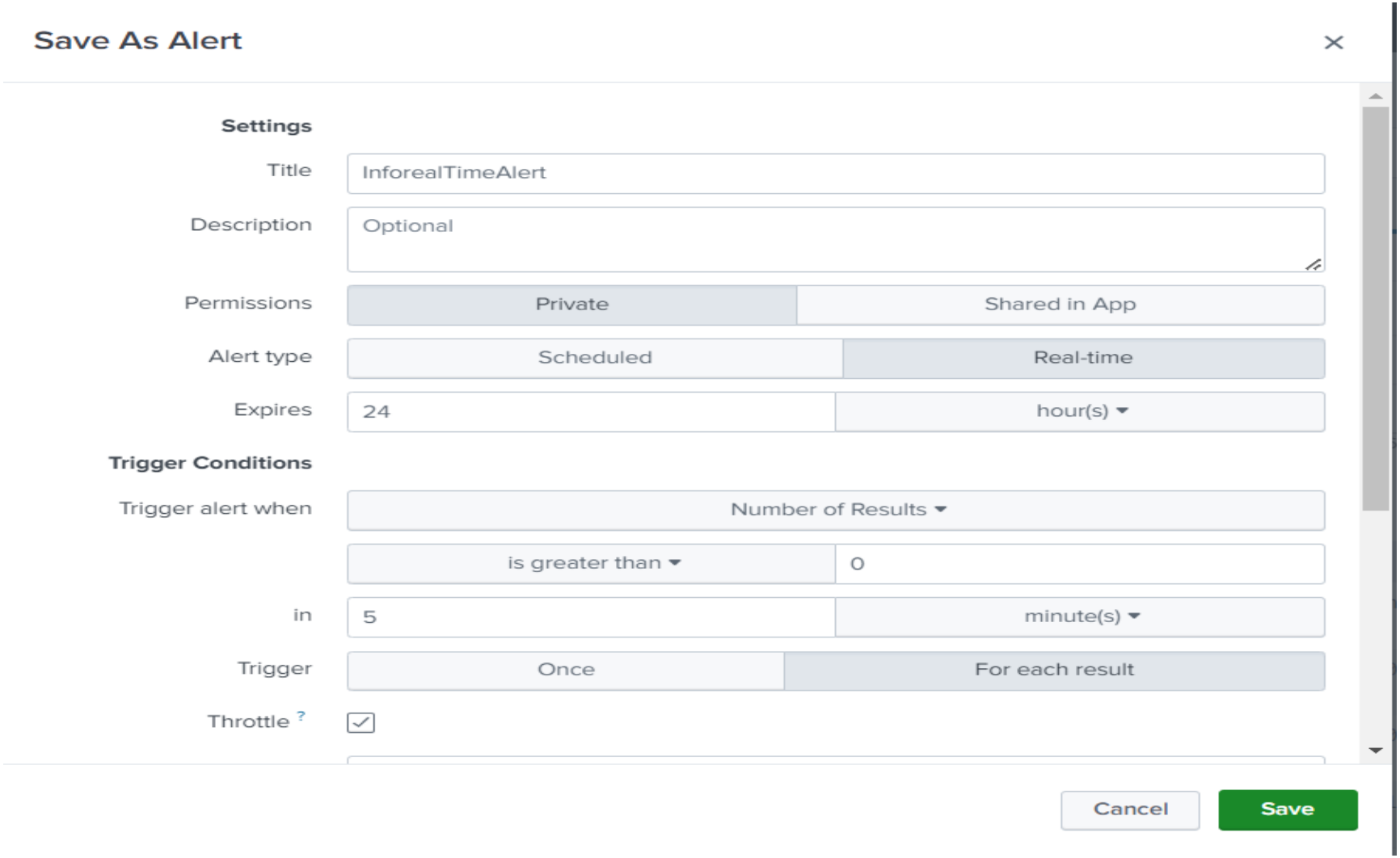
Filter | App: EssilorApp (EssilorApp) | Owner: eswaribala | Severity: All severity | Alert name: All alerts | Showing 1 - 8 of 8 results

Time	Alert name	App	Type	Severity	Mode	Actions
2024-04-17 16:26:14 India Standard Time	UnitPriceAlert	EssilorApp	Scheduled	Critical	Digest	View Results | Edit Search | Delete
2024-04-17 16:26:13 India Standard Time	QtyAlert	EssilorApp	Scheduled	Medium	Digest	View Results | Edit Search | Delete
2024-04-17 16:25:05 India Standard Time	QtyAlert	EssilorApp	Scheduled	Medium	Digest	View Results | Edit Search | Delete
2024-04-17 16:23:06 India Standard Time	QtyAlert	EssilorApp	Scheduled	Medium	Digest	View Results | Edit Search | Delete
2024-04-17 16:21:06 India Standard Time	QtyAlert	EssilorApp	Scheduled	Medium	Digest	View Results | Edit Search | Delete
2024-04-17 16:19:05 India Standard Time	QtyAlert	EssilorApp	Scheduled	Medium	Digest	View Results | Edit Search | Delete
2024-04-17 16:17:06 India Standard Time	QtyAlert	EssilorApp	Scheduled	Medium	Digest	View Results | Edit Search | Delete
2024-04-17 16:15:10 India Standard Time	QtyAlert	EssilorApp	Scheduled	Medium	Digest	View Results | Edit Search | Delete

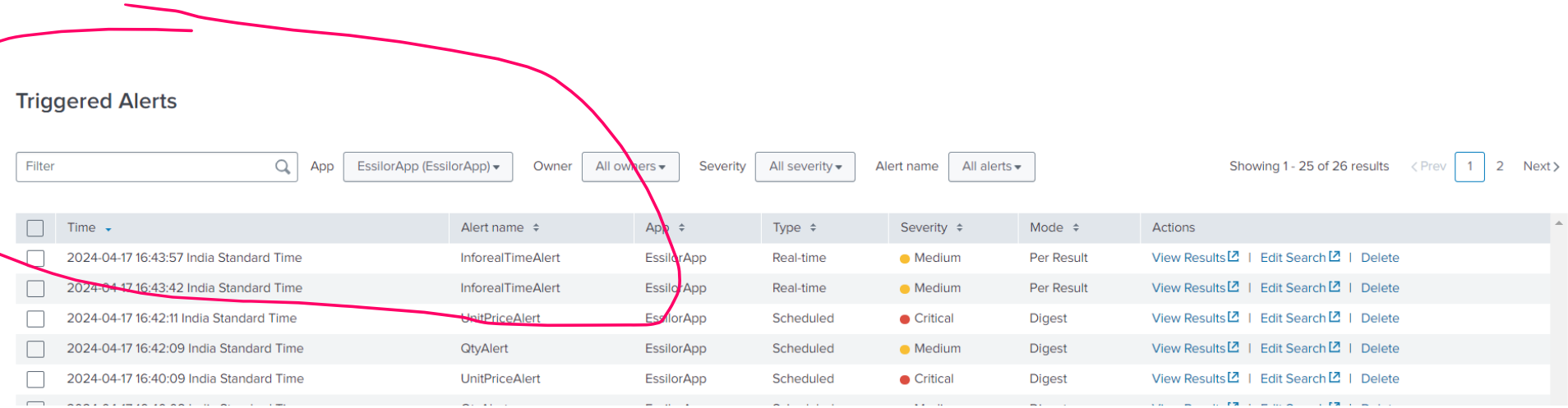
Alerts


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
EssilorApp
New Search
Save As
Create Table View
Close
index="_internal" source="C:\\Program Files\\SplunkUniversalForwarder\\var\\log\\splunk\\splunkd.log" INFO
30 second window
2 of 3 events matched
No Event Sampling
Job
Smart Mode
Events (2)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 second per column
16:40:40
Wed Apr 17
2024
16:40:45
16:40:50
16:40:55
16:41:00
16:41:05
List
Format
20 Per Page
Hide Fields
All Fields
INTERESTING FIELDS
a component 2
date_hour 1
date_mday 1
date_minute 1
a date_month 1
date_second 2
a date_wday 1
date_year 1
date_zone 1
a event_message 2
a eventtype 1
a file 1
Time
Event
17/04/2024
16:40:53.125
04-17-2024 16:40:53.125 +0530 INFO TailReader [12944 tailreader0] - Batch input finished reading file='C:\Program Files\SplunkUniversalForwarder\var\spool\splunk\tracker.log'
17/04/2024
16:40:37.811
04-17-2024 16:40:37.811 +0530 INFO AutoLoadBalancedConnectionStrategy [17796 TcpOutEloop] - Found currently active indexer. Connected to idx=127.0.0.1:9997:0, reuse=1.

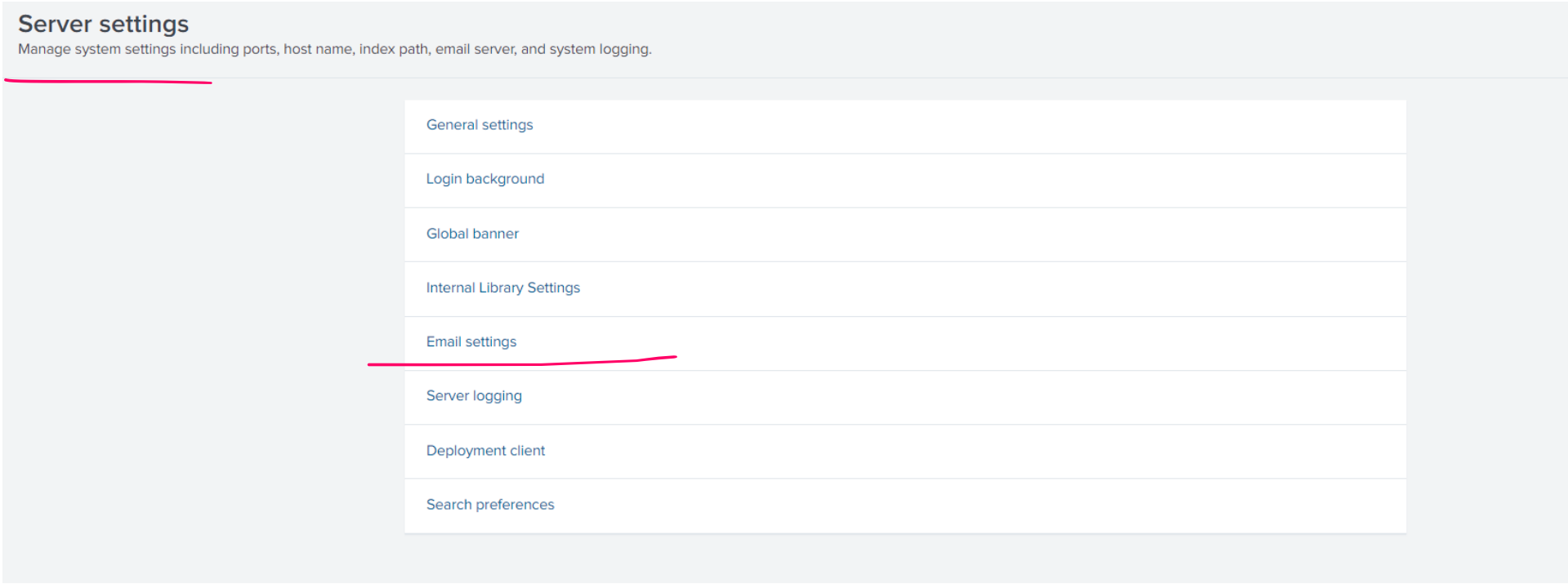
Real Time Alert



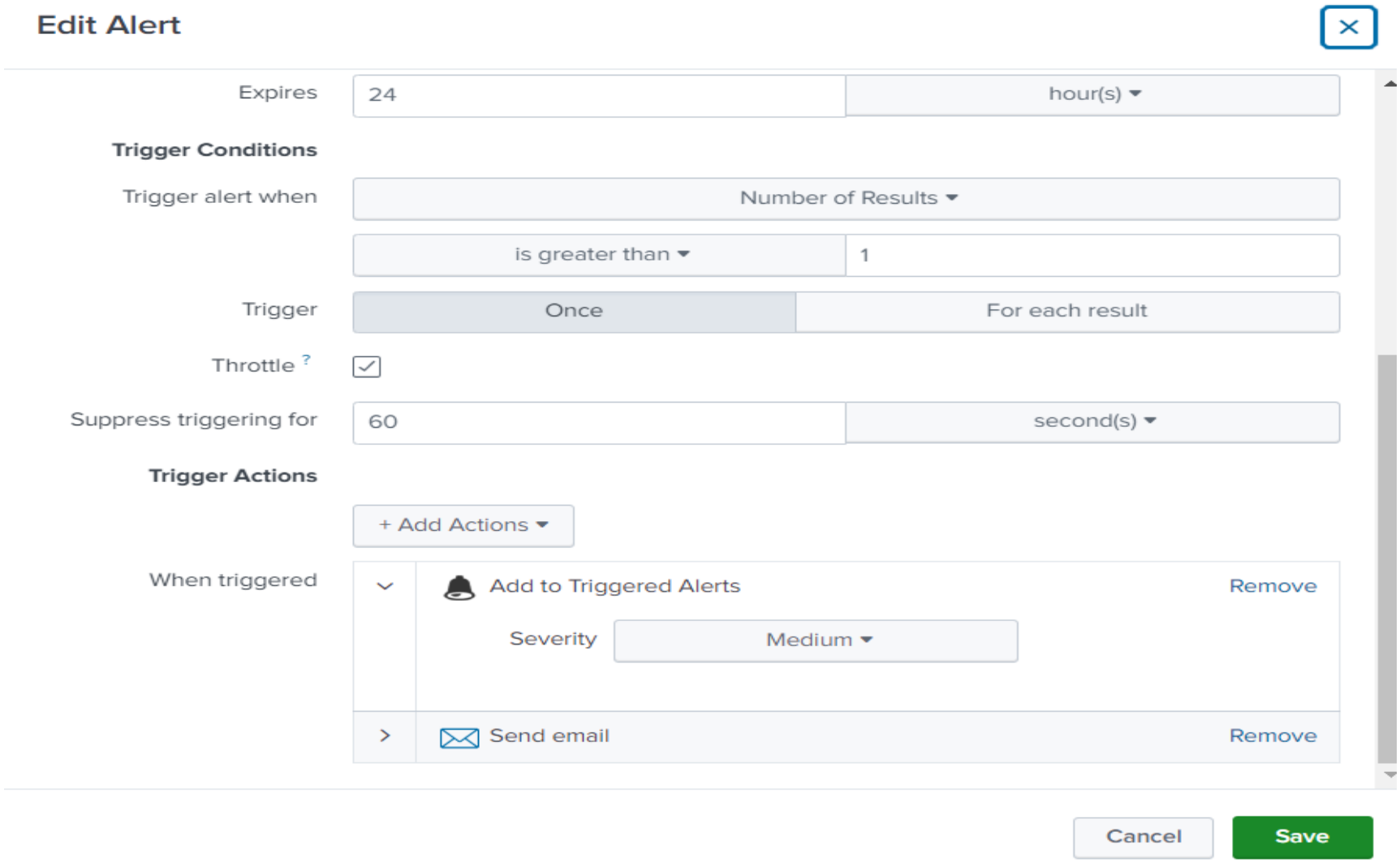
Real Time Alert



Email Settings



Email Settings



Deployment Server

- A deployment server is a Splunk Enterprise instance that acts as a centralized configuration manager for any number of other instances, called "deployment clients".
- Any full Splunk Enterprise instance - even one indexing data locally - can act as a deployment server.
- A deployment server cannot be a client of itself.

Deployment Server

- A deployment client is a Splunk instance remotely configured by a deployment server.
- Deployment clients can be universal forwarders, heavy forwarders, indexers, or search heads.
- Each deployment client belongs to one or more server classes.

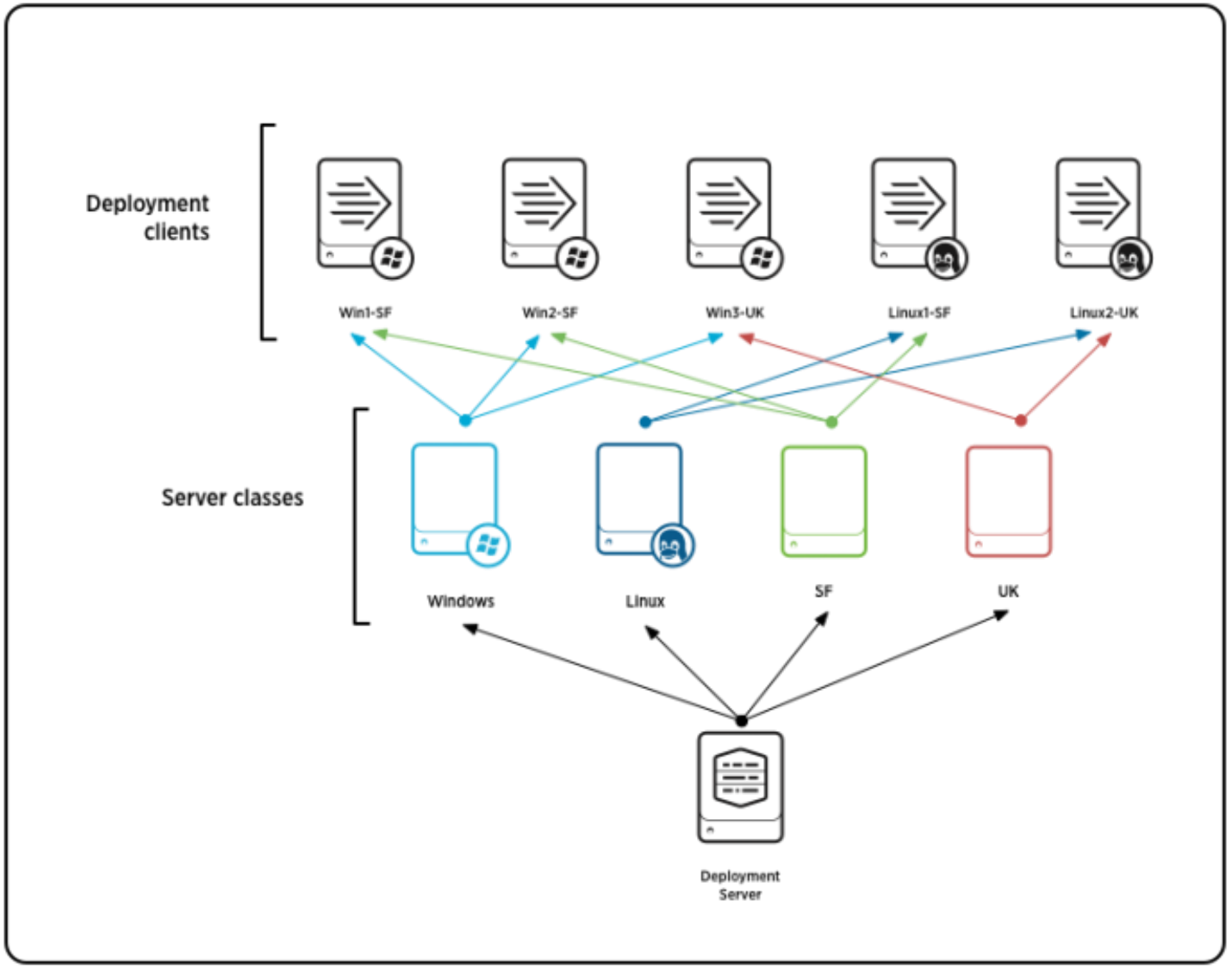
Deployment Server

- A deployment app is a set of content (including configuration files) maintained on the deployment server and deployed as a unit to clients of a server class.
- A deployment app might consist of just a single configuration file, or it can consist of many files.
- Over time, an app can be updated with new content and then redeployed to its designated clients.
- The deployment app can be an existing Splunk Enterprise app or one developed solely to group some content for deployment purposes.

Deployment Server

- A server class is a group of deployment clients that share one or more defined characteristics.
- For example, you can group all Windows clients into one server class and all Linux clients into another server class.
- You use server classes to map a group of deployment clients to one or more deployment apps.
- By creating a server class, you are telling the deployment server that a specific set of clients should receive configuration updates in the form of a specific set of apps.

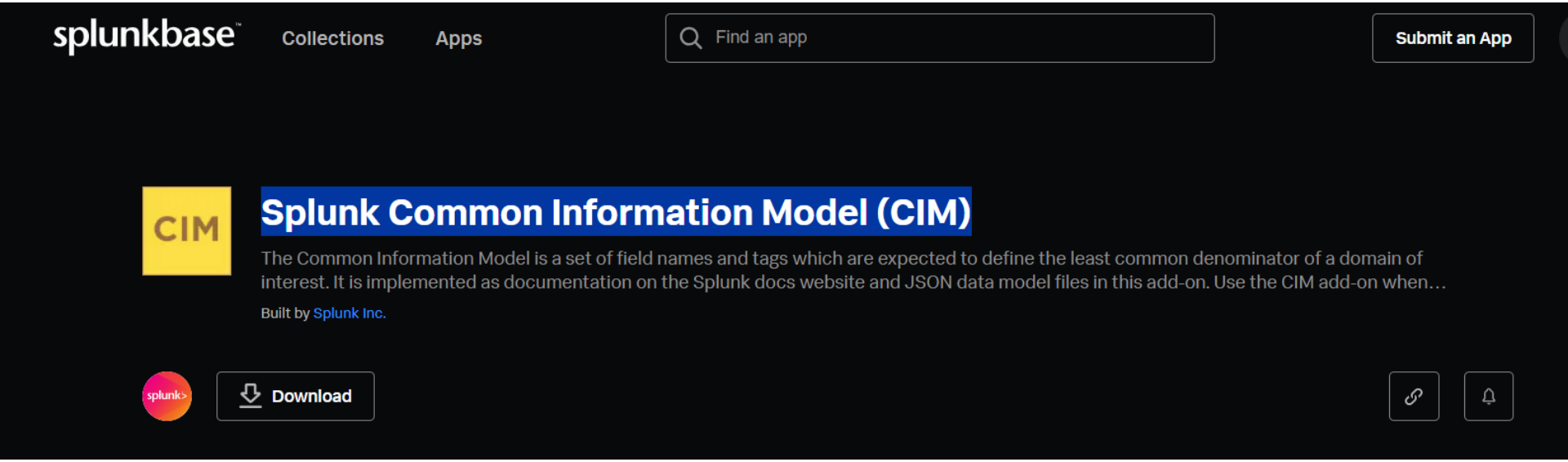
Deployment Server



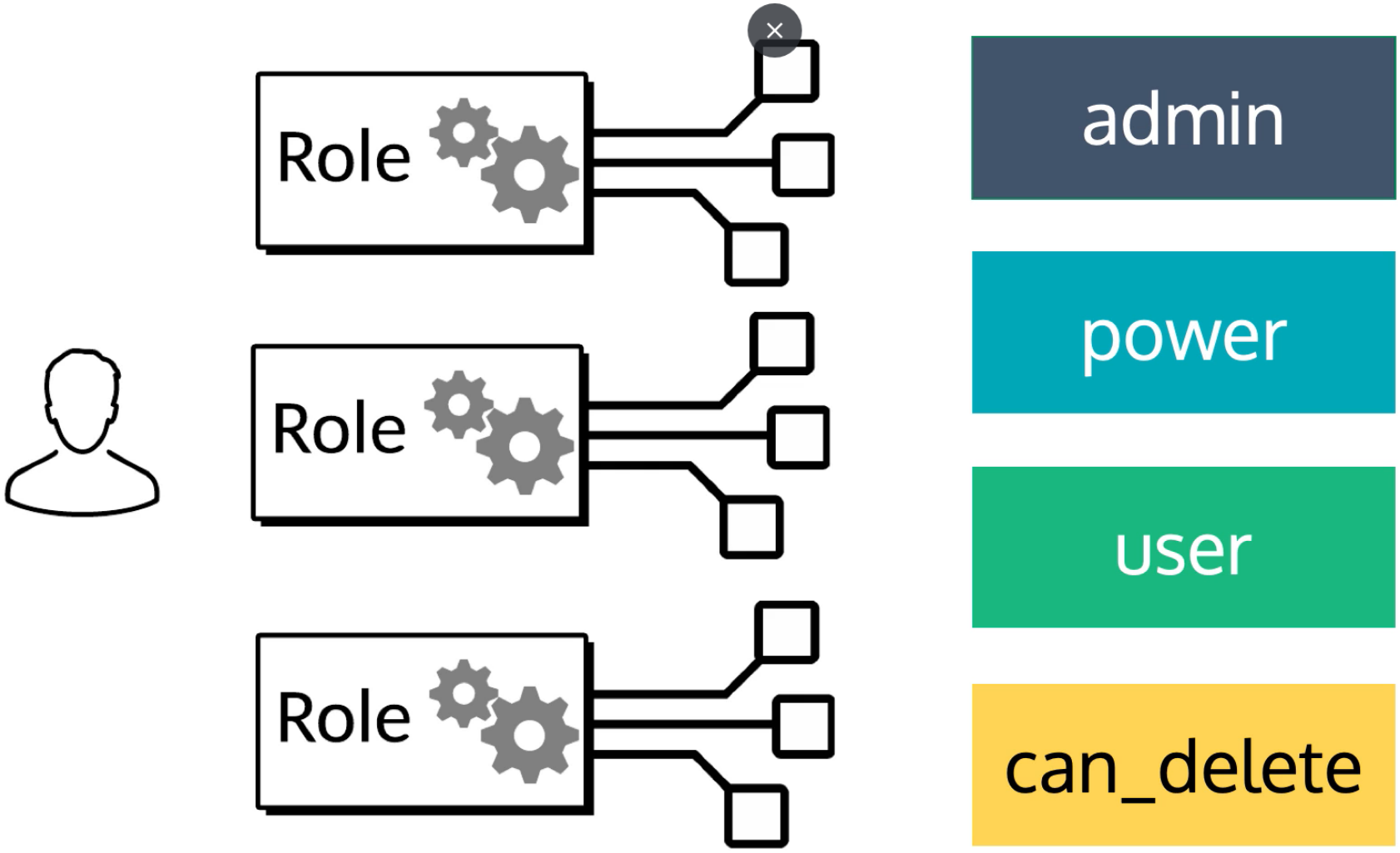
Deployment Server

Term	Meaning
deployment server	A Splunk Enterprise instance that acts as a centralized configuration manager. It deploys configuration updates to other instances. Also refers to the overall configuration update facility comprising deployment server, clients, and apps.
deployment client	A remotely configured Splunk Enterprise instance. It receives updates from the deployment server.
server class	A deployment configuration category shared by a group of deployment clients. A deployment client can belong to multiple server classes.
deployment app	A unit of content deployed to the members of one or more server classes.

Splunk Common Information Model (CIM)

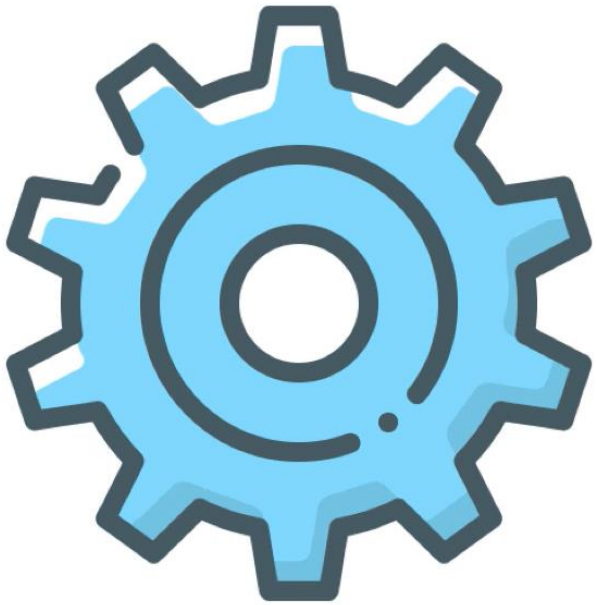


Authentication



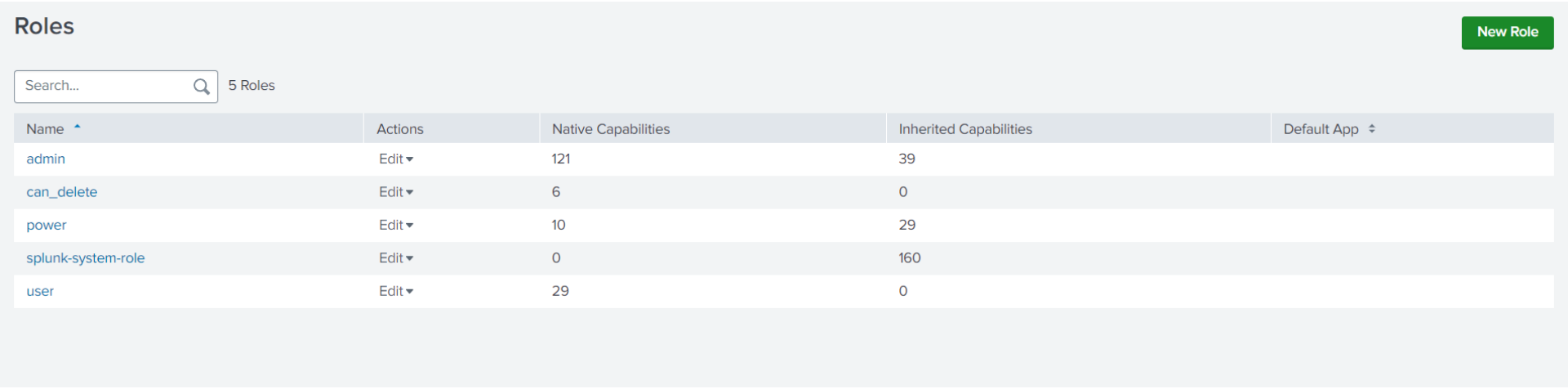
Authentication

Capabilities

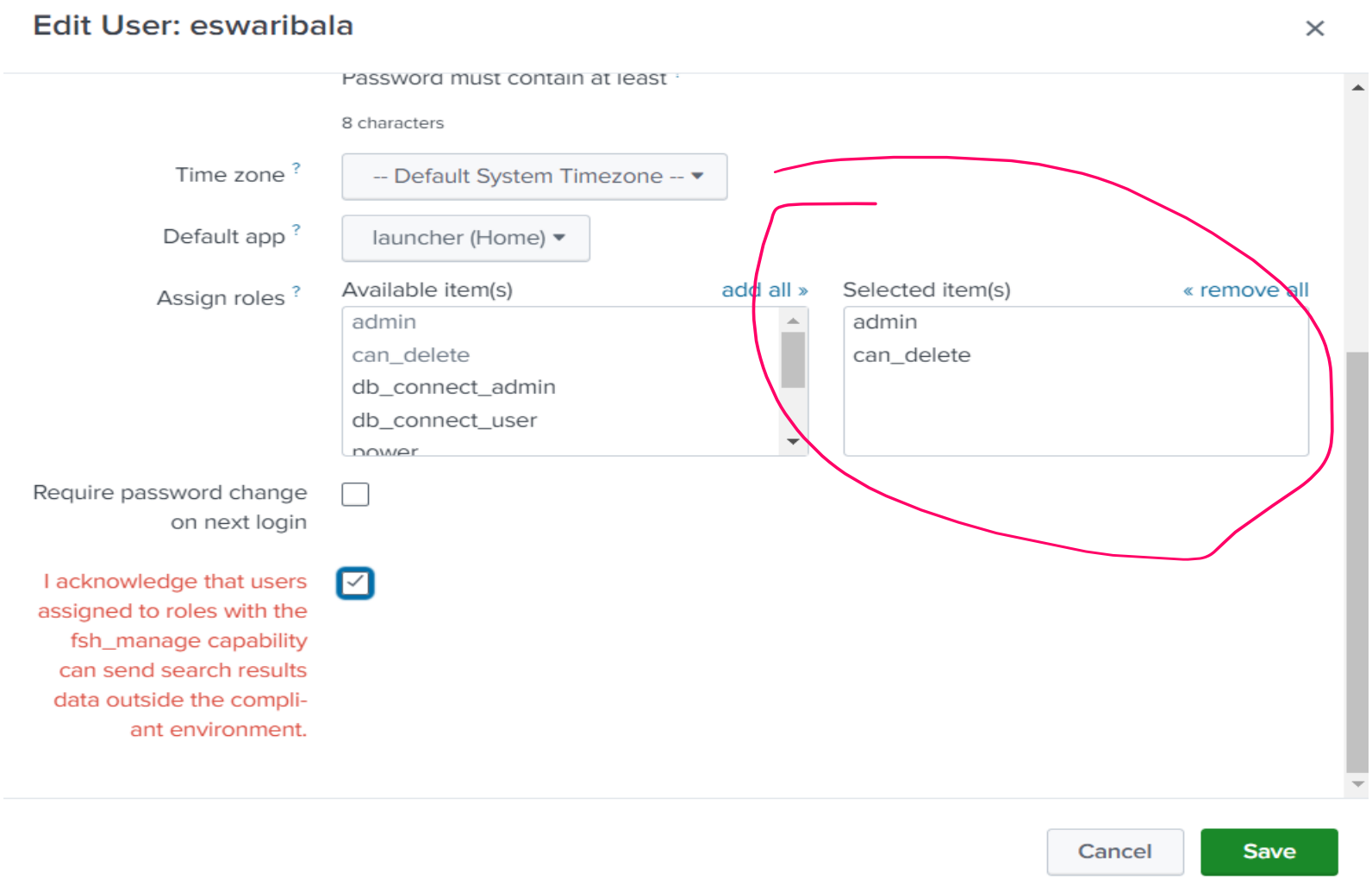


- Assigned to roles
- Additive in nature
- Can be used to granularly manage users in Splunk
- Can be added or removed in Splunk web, or in authorize.conf

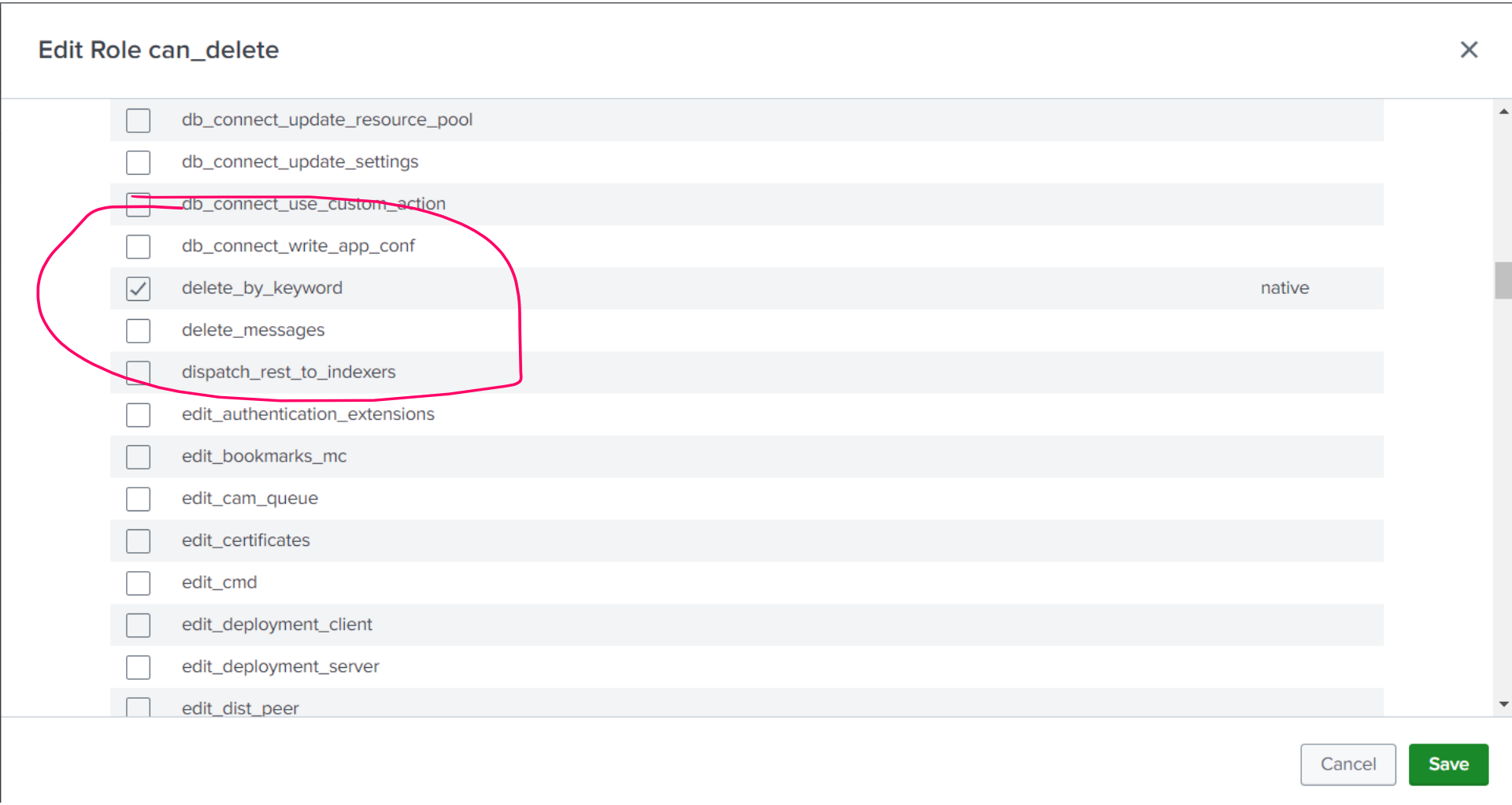
Authentication



Authentication



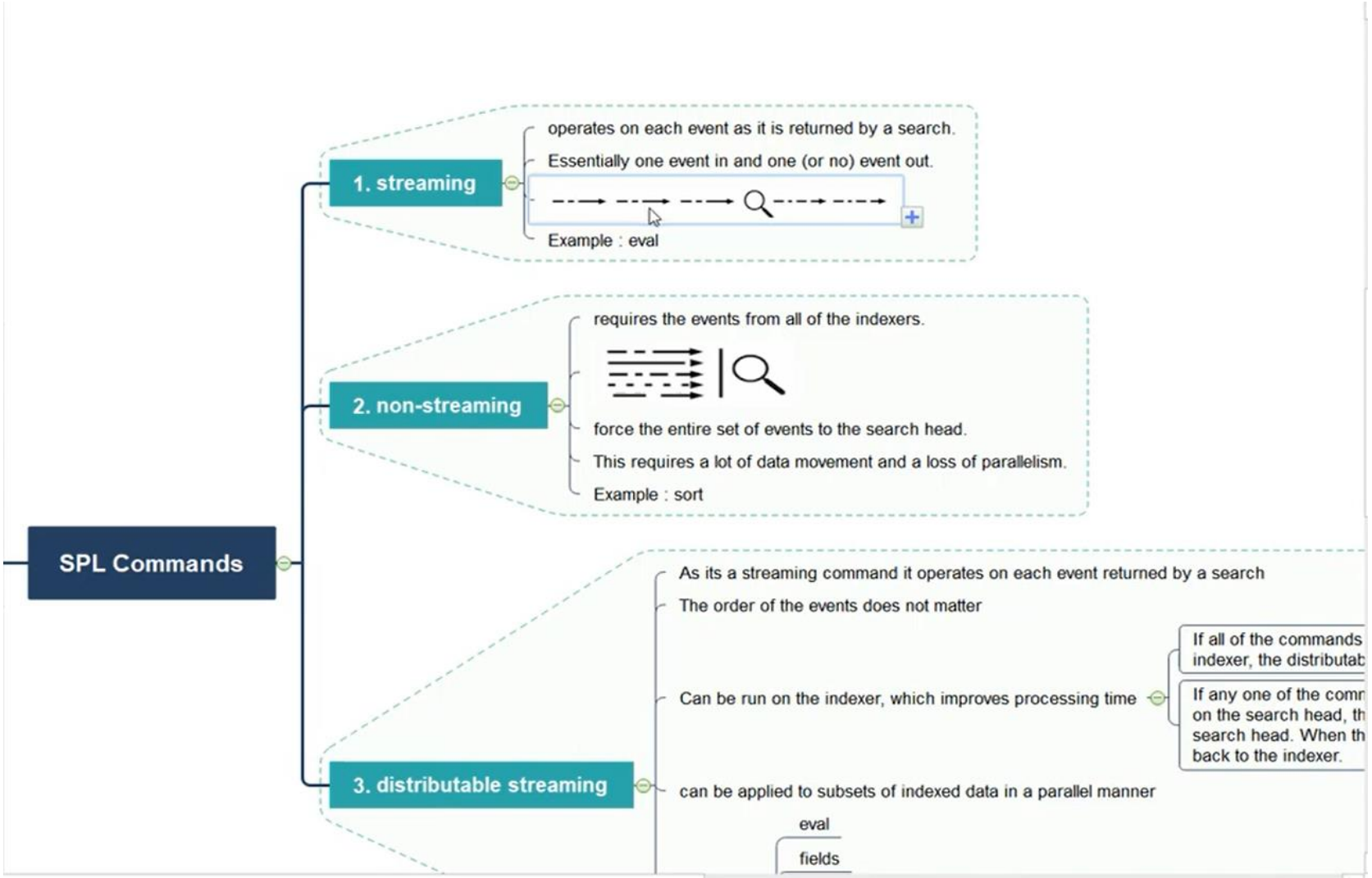
Authentication



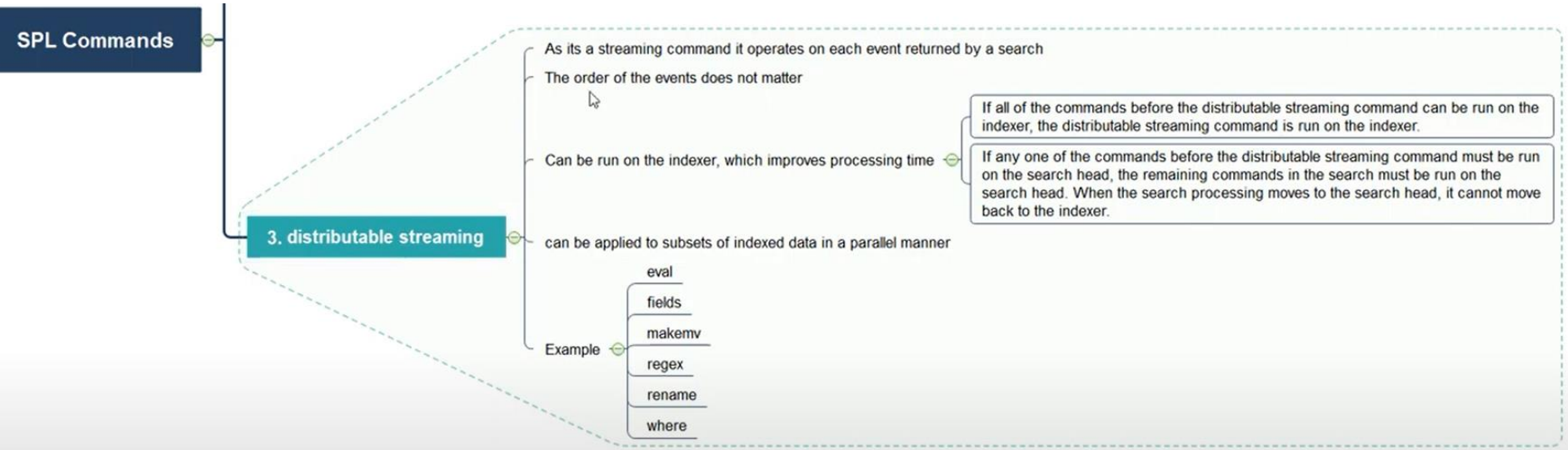
Splunk Types of Commands

- distributable streaming command
- centralized streaming command
- transforming command
- generating command
- orchestrating command
- dataset processing command

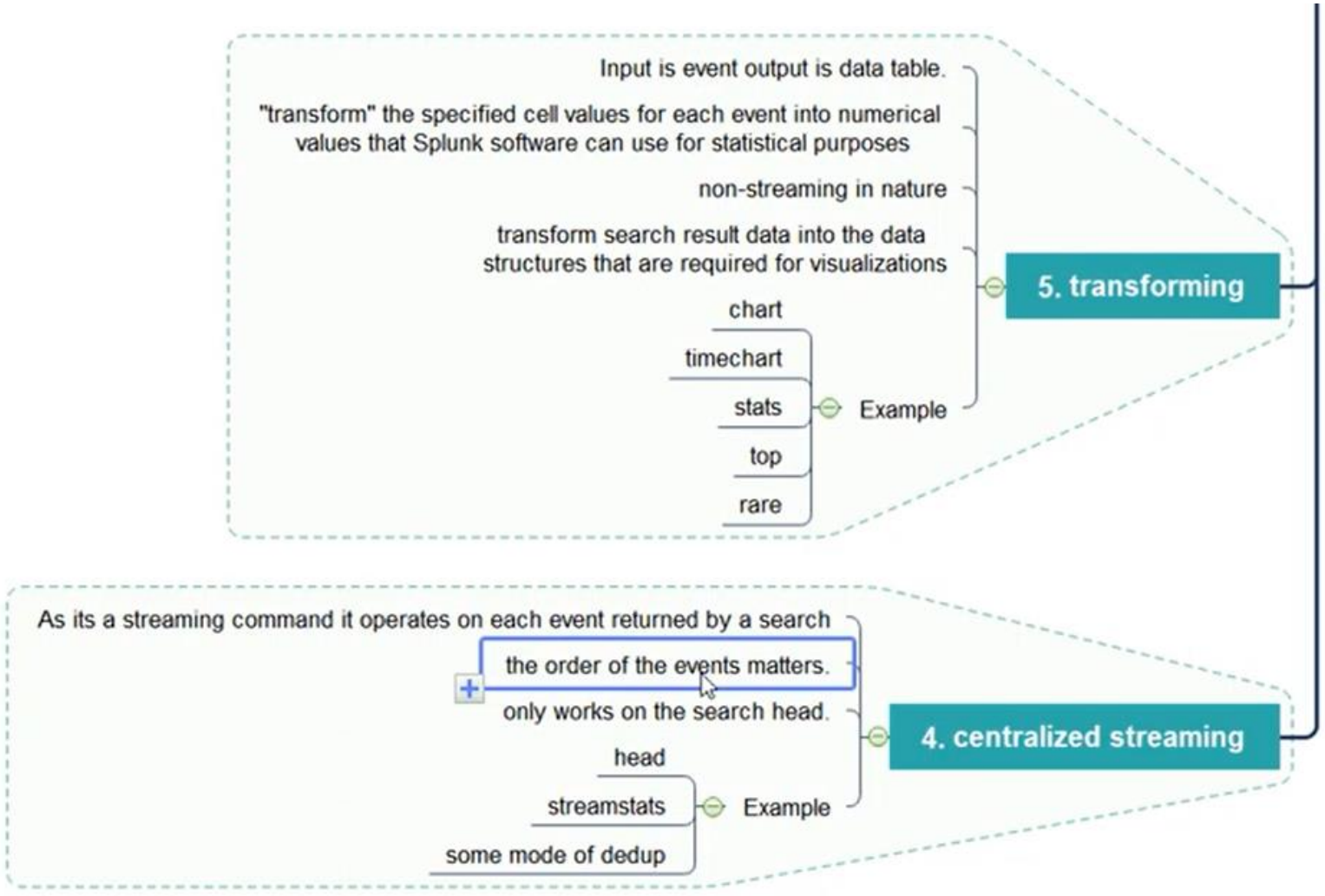
Splunk Types of Commands



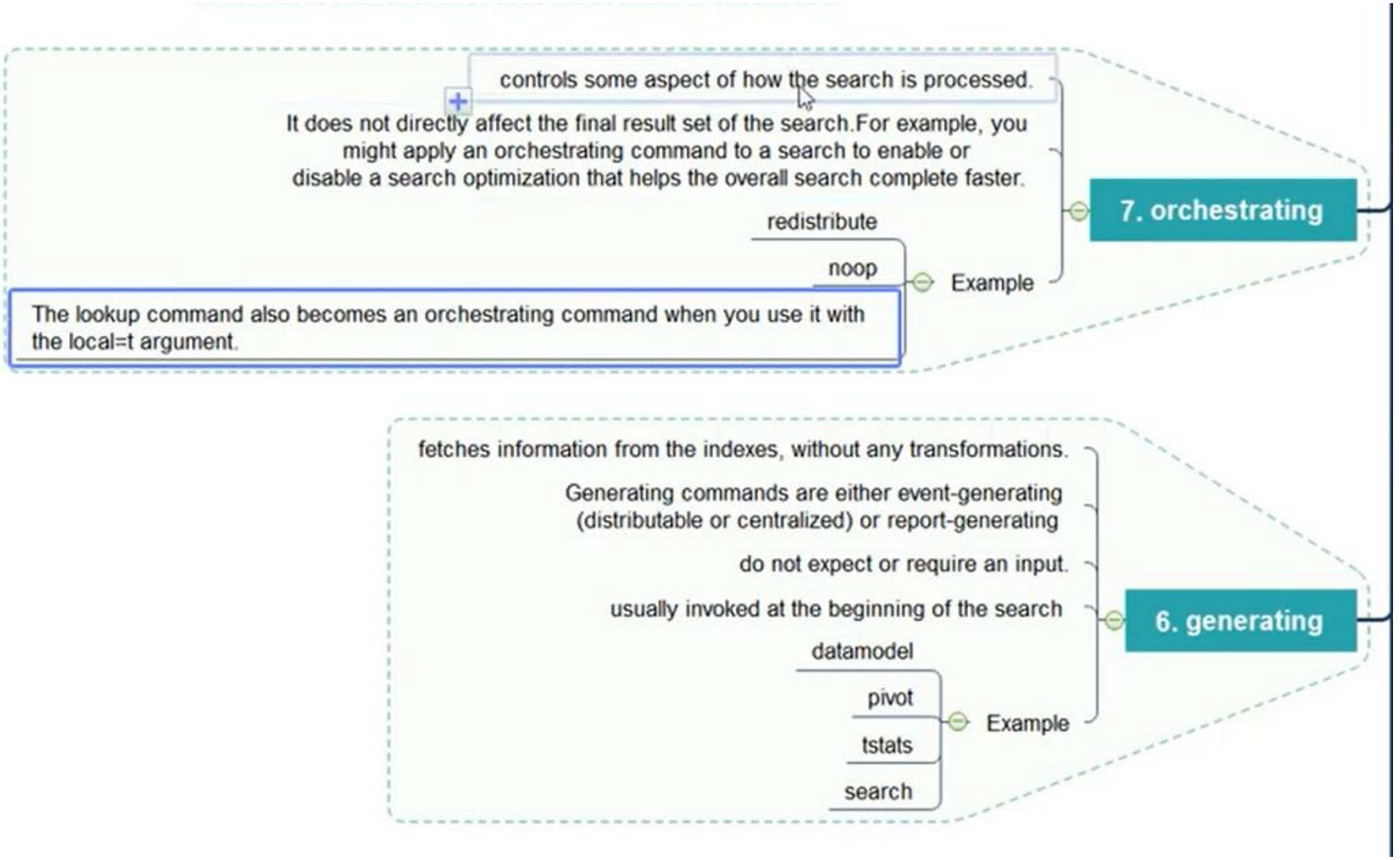
Splunk Types of Commands



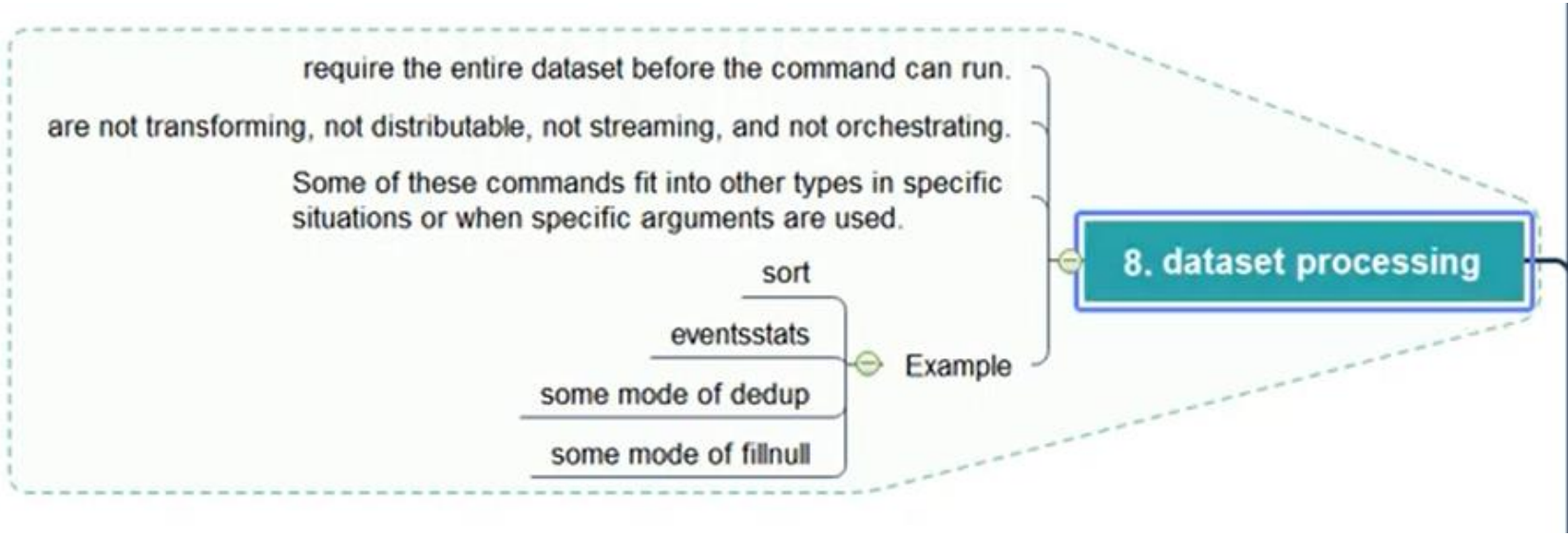
Splunk Types of Commands



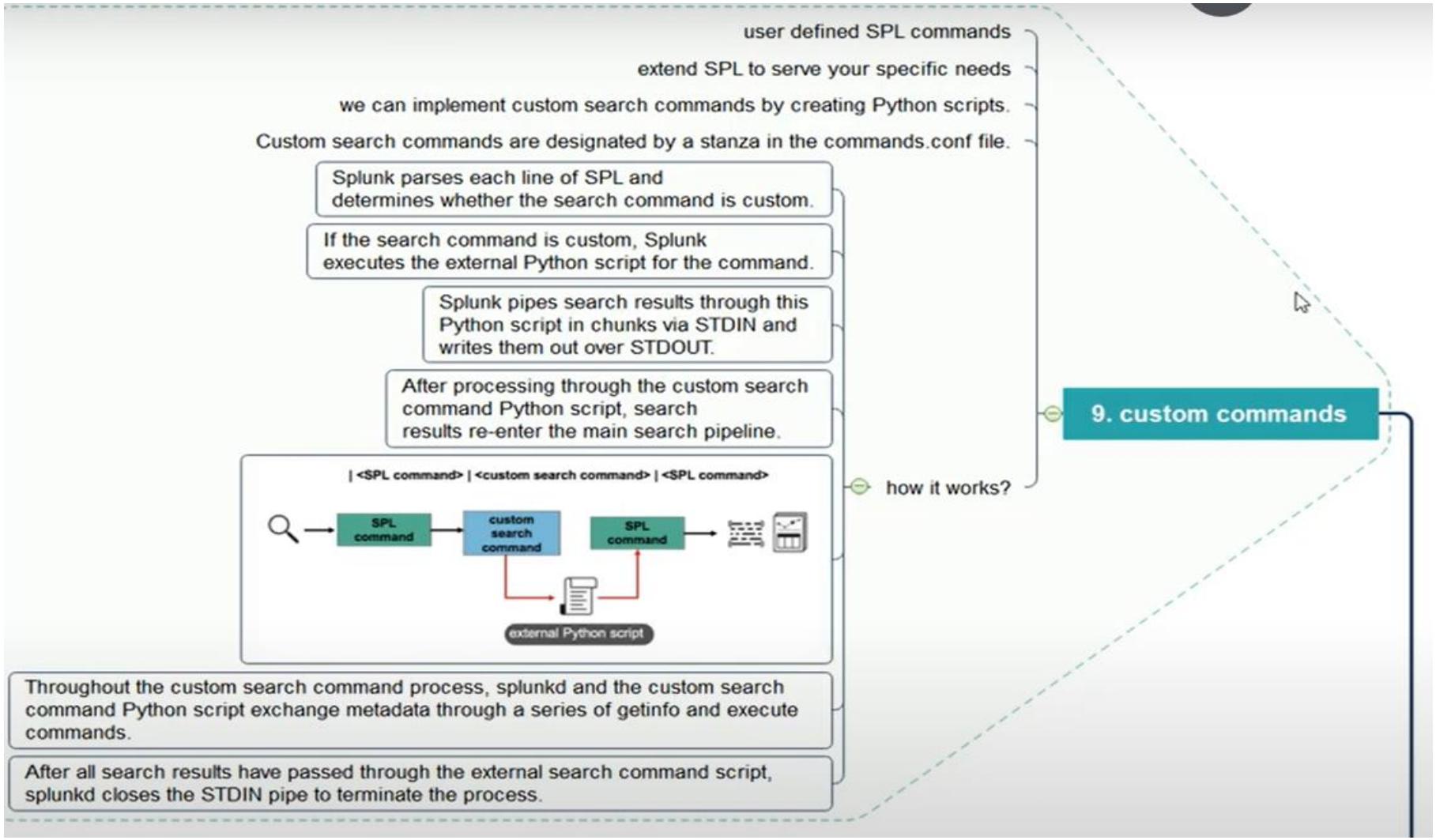
Splunk Types of Commands



Splunk Types of Commands



Splunk Types of Commands



Search commands

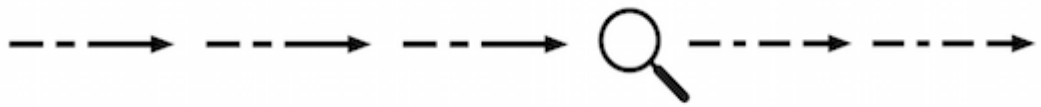
COMMAND	DESCRIPTION
`chart, timechart`	Returns results in a tabular output for (time-series) charting
`dedup X`	Removes duplicate results on a field X
`eval`	Calculates an expression (see **Calculations**)
`fields`	Removes fields from search results
`head/tail N`	Returns the first/last N results, where N is a positive integer
`lookup`	Adds field values from an external source
`rename`	Renames a field. Use wildcards (*) to specify multiple fields.
`rex`	Extract fields according to specified regular expression(s)
`search`	Filters results to those that match the search expression
`sort X`	Sorts the search results by the specified fields X

Search commands

`stats`	Provides statistics, grouped optionally by fields
`mstats`	Similar to stats but used on metrics instead of events
`table`	Displays data fields in table format.
`top/rare`	Displays the most/least common values of a field
`transaction`	Groups search results into **transactions**
`where`	Filters search results using eval expressions. For comparing two different fields.

Streaming and non-streaming commands

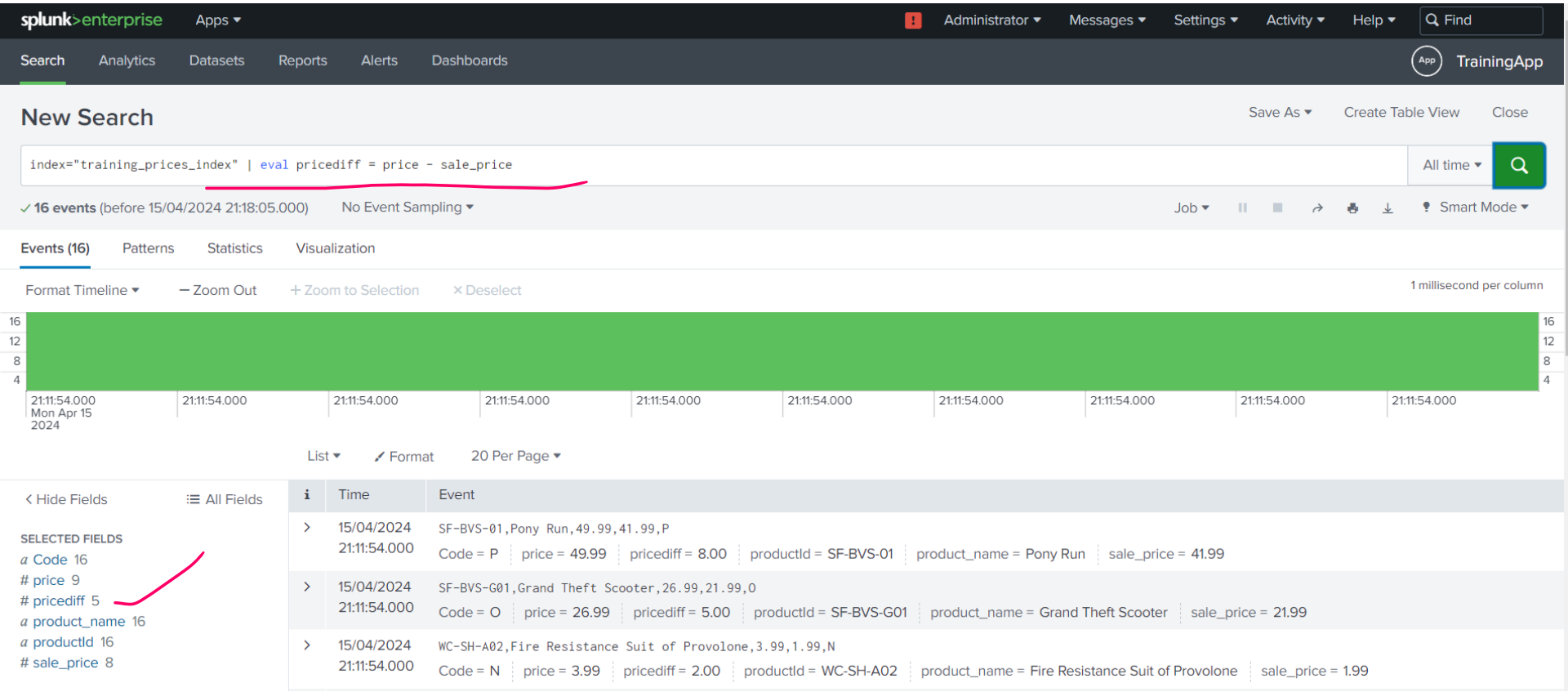
- A streaming command operates on each event as it is returned by a search.
- Essentially one event in and one (or no) event out.



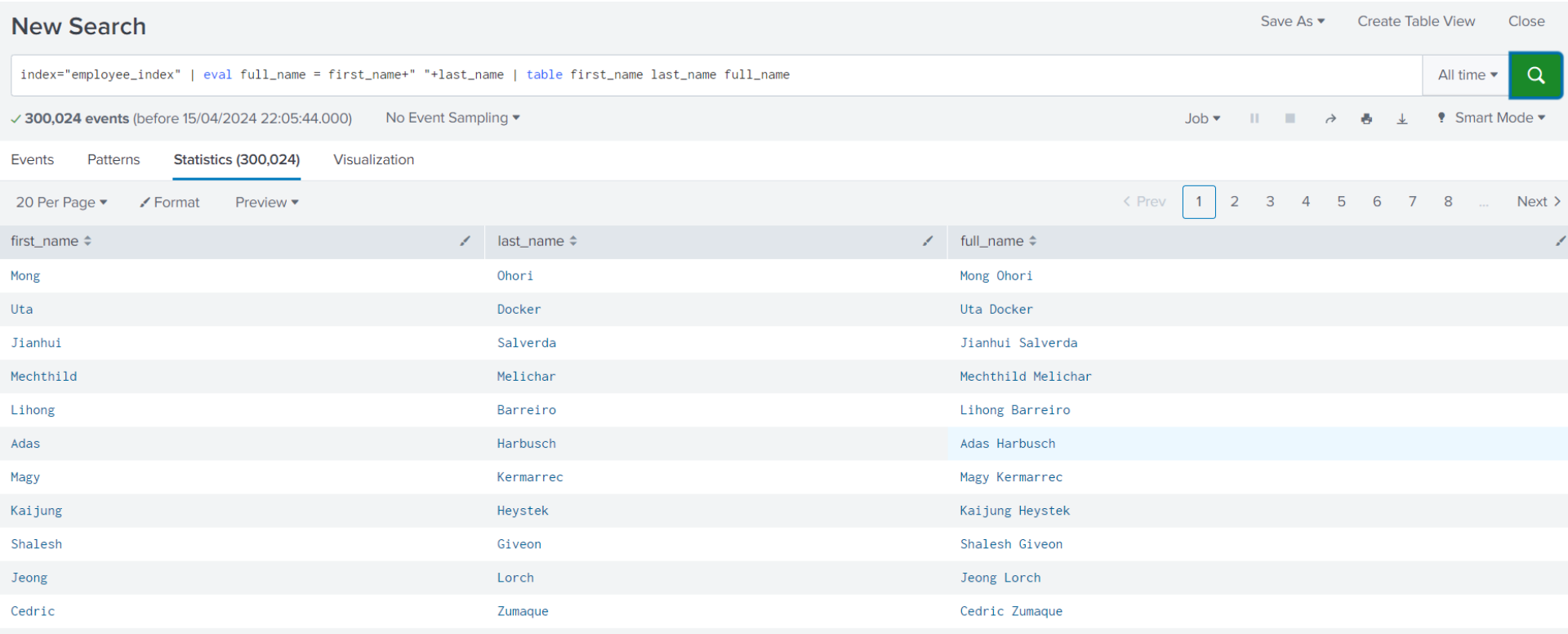
For example, the eval command can create a new field, full_name, to contain the concatenation of the value in the first_name field, a space, and the value in the last_name field.

... | eval full_name = first_name." ".last_name

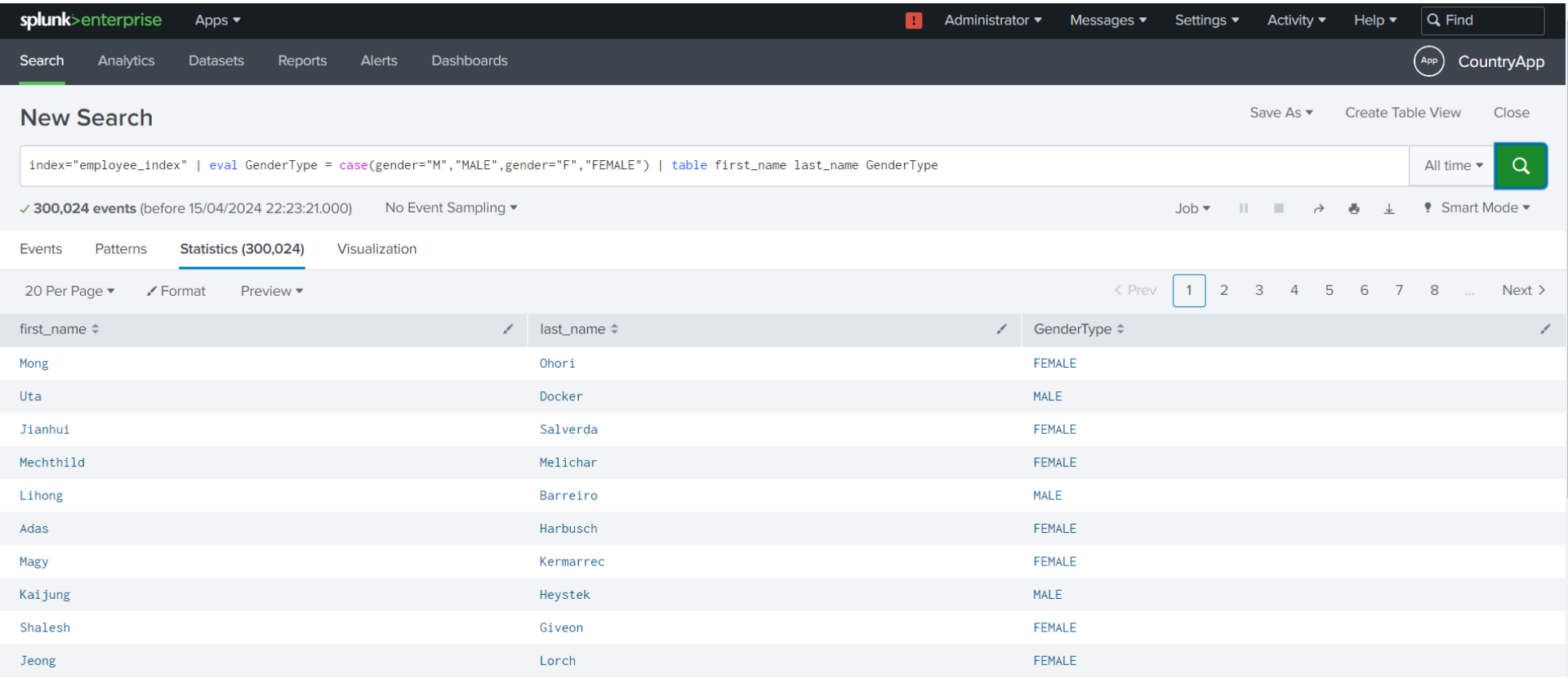
Streaming and non-streaming commands



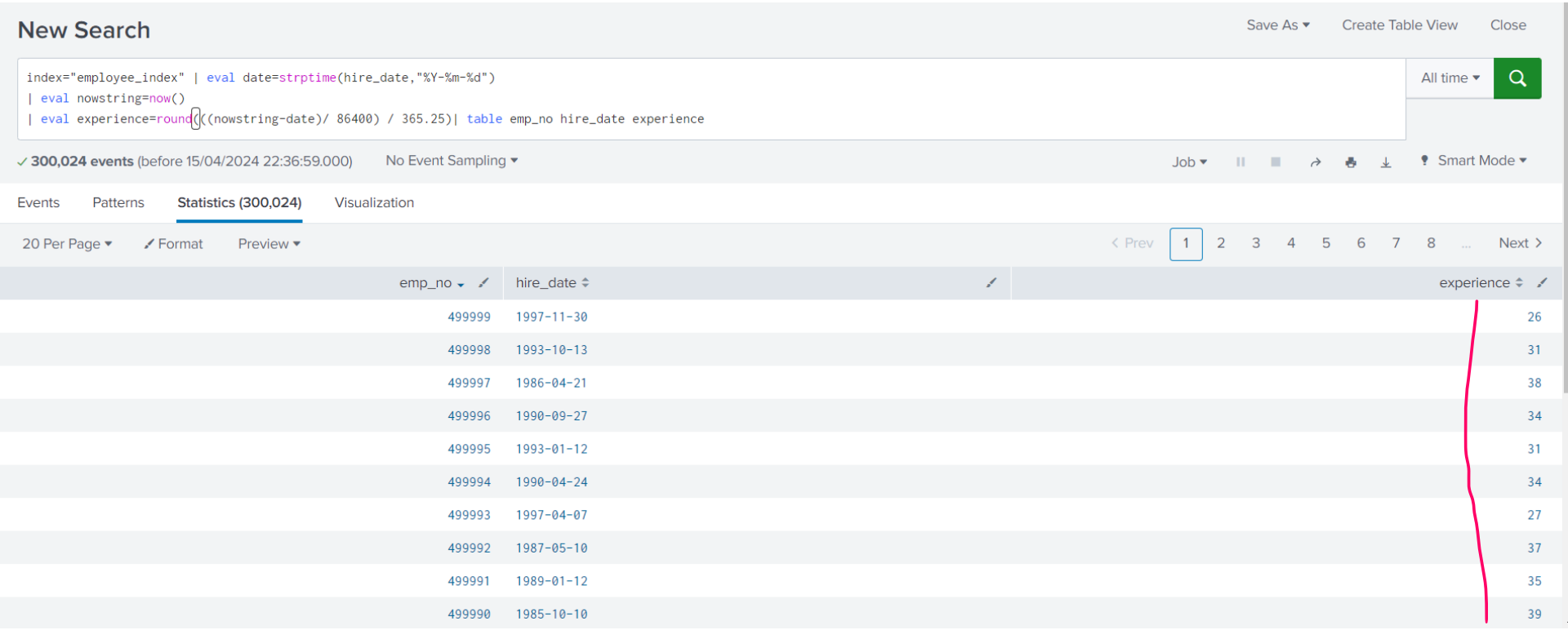
Creating new field in table using eval



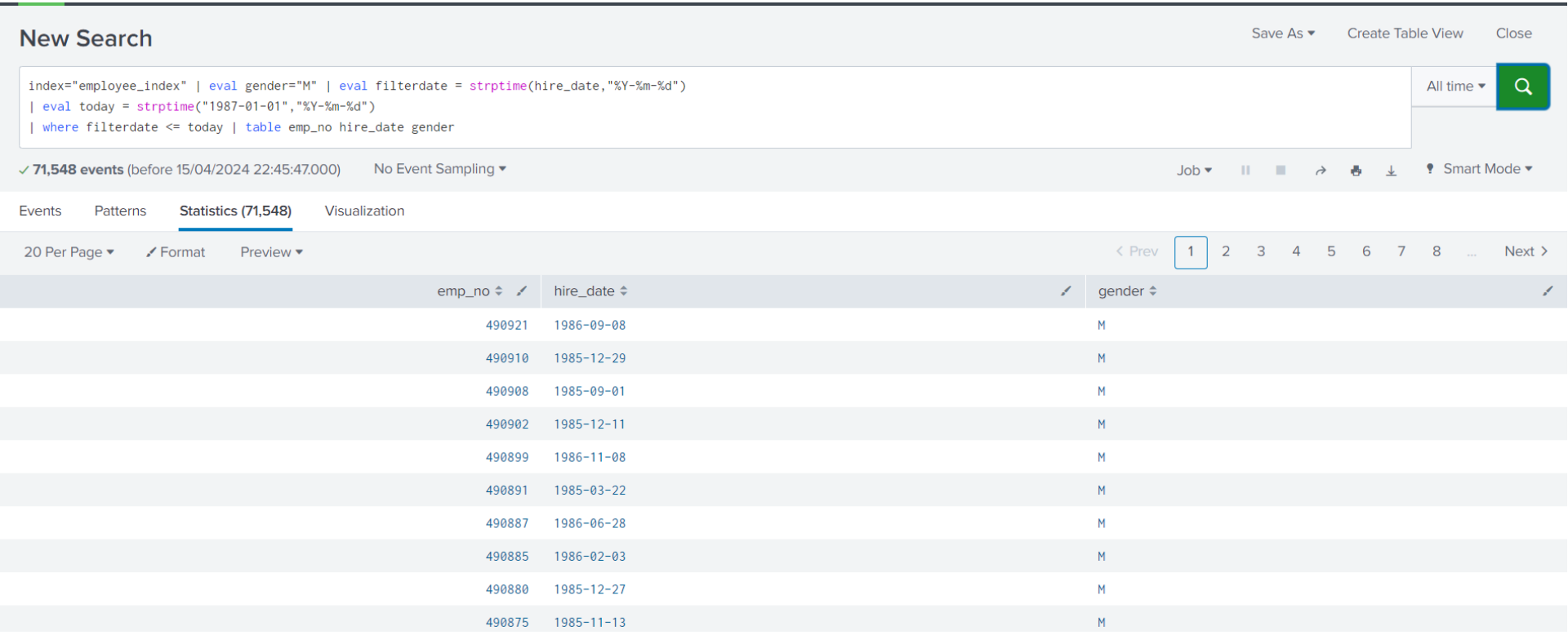
Creating new field in table using eval



Creating new field in table using eval

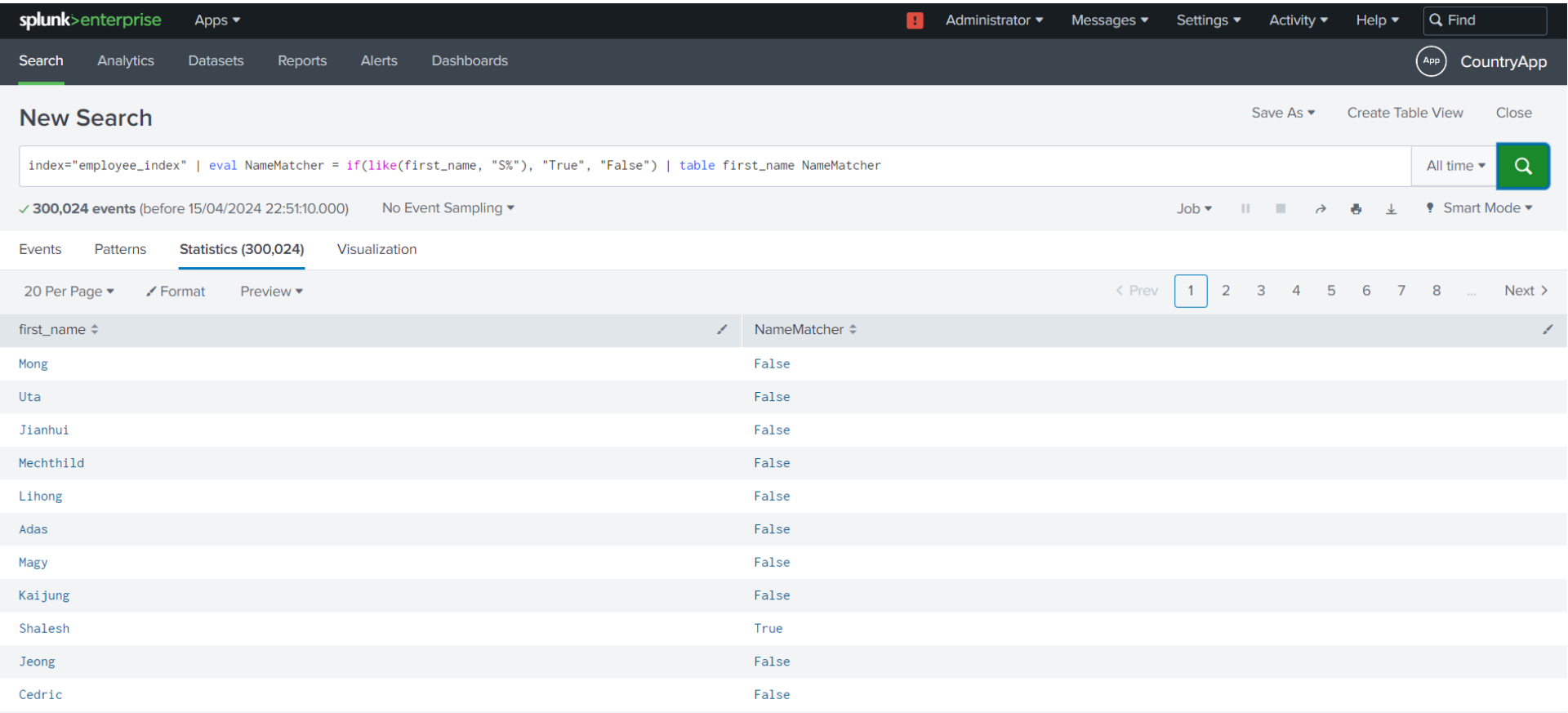


Creating new field in table using eval



emp_no	hire_date	gender
490921	1986-09-08	M
490910	1985-12-29	M
490908	1985-09-01	M
490902	1985-12-11	M
490899	1986-11-08	M
490891	1985-03-22	M
490887	1986-06-28	M
490885	1986-02-03	M
490880	1985-12-27	M
490875	1985-11-13	M

Creating new field in table using eval



Streaming and non-streaming commands

- A non-streaming command requires the events from all of the indexers before the command can operate on the entire set of events.
- Many transforming commands are non-streaming commands.
- There are also several commands that are not transforming commands but are also non-streaming.
- These non-transforming, non-streaming commands are most often dataset processing commands.

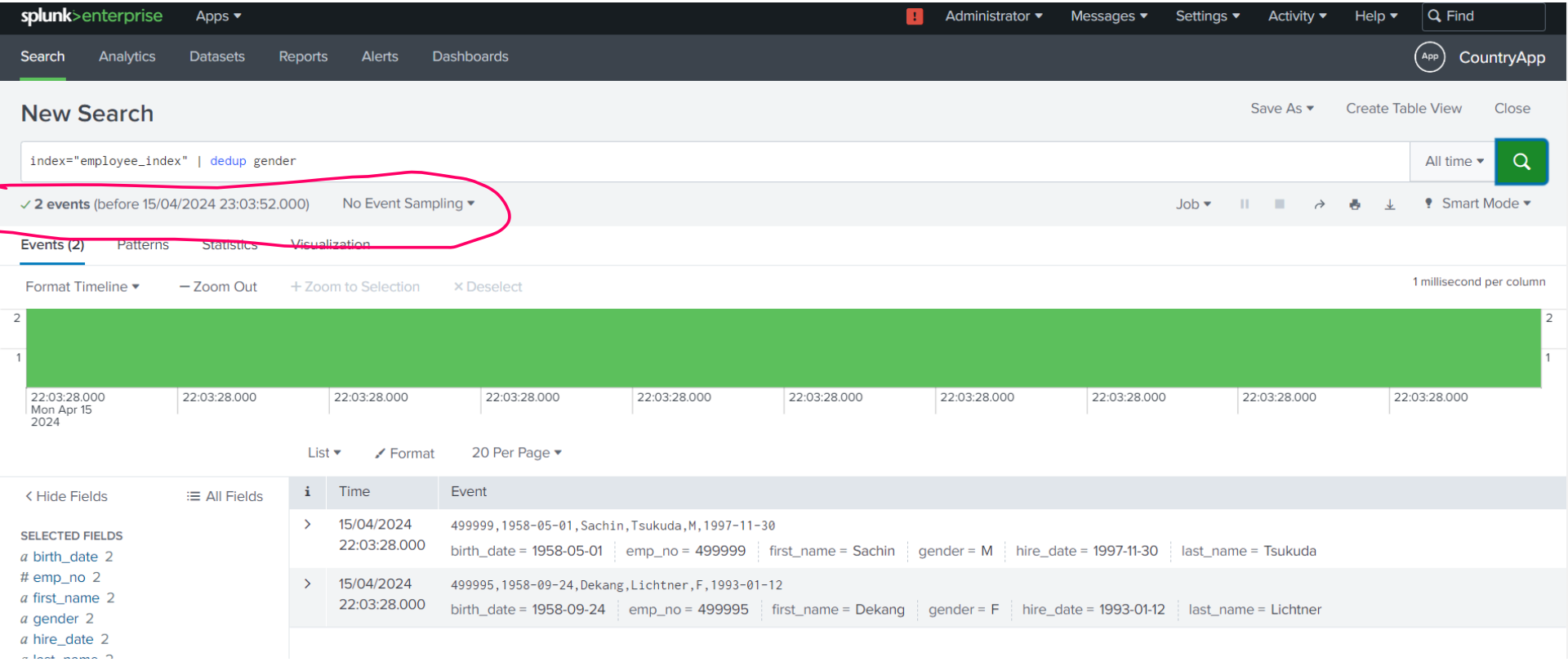
Streaming and non-streaming commands

- For example, before the sort command can begin to sort the events, the entire set of events must be received by the sort command.
- Other examples of non-streaming commands include dedup (in some modes), stats, and top.

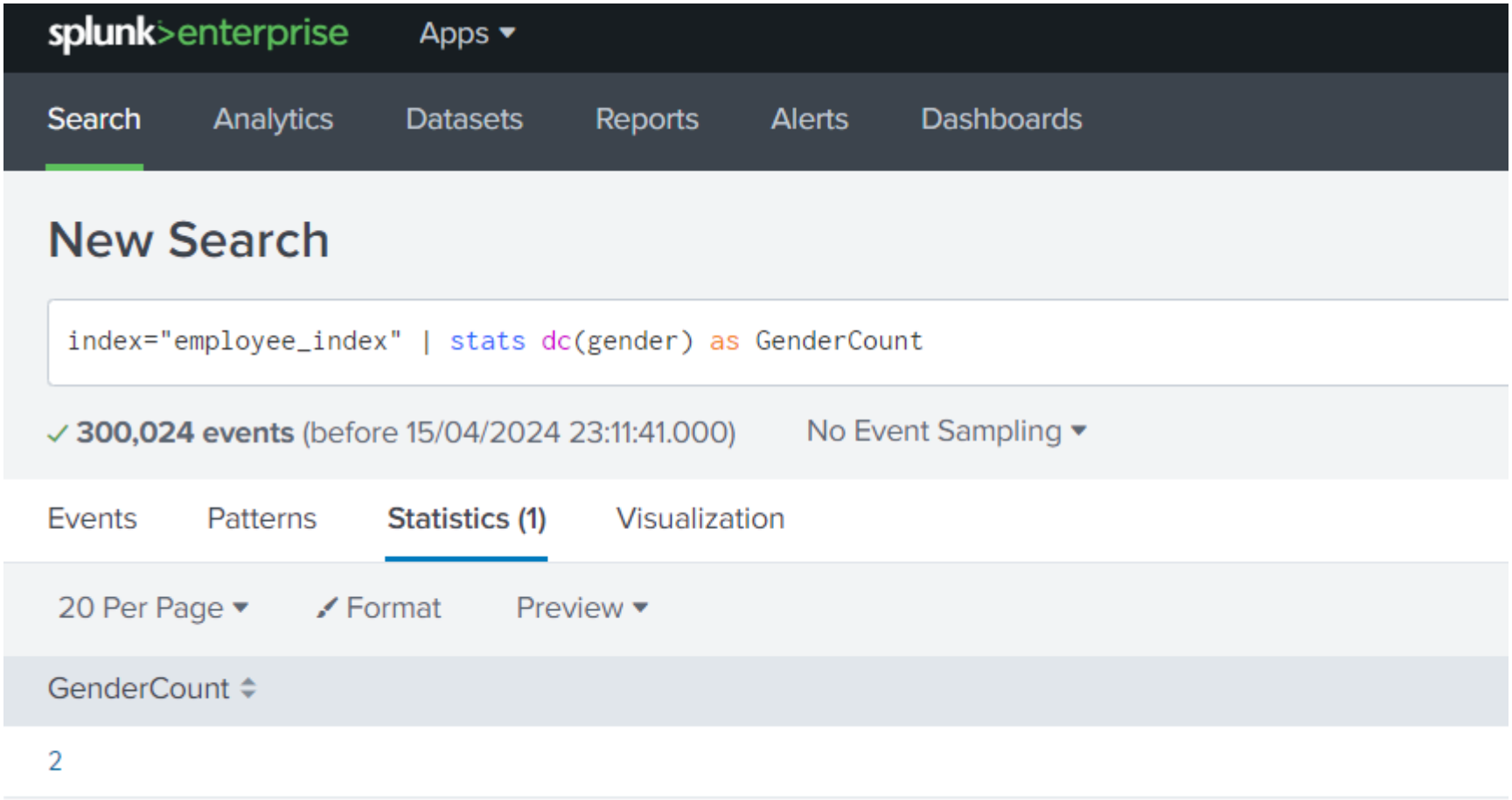
- Non-streaming commands force the entire set of events to the search head. This requires a lot of data movement and a loss of parallelism.

Streaming and non-streaming commands

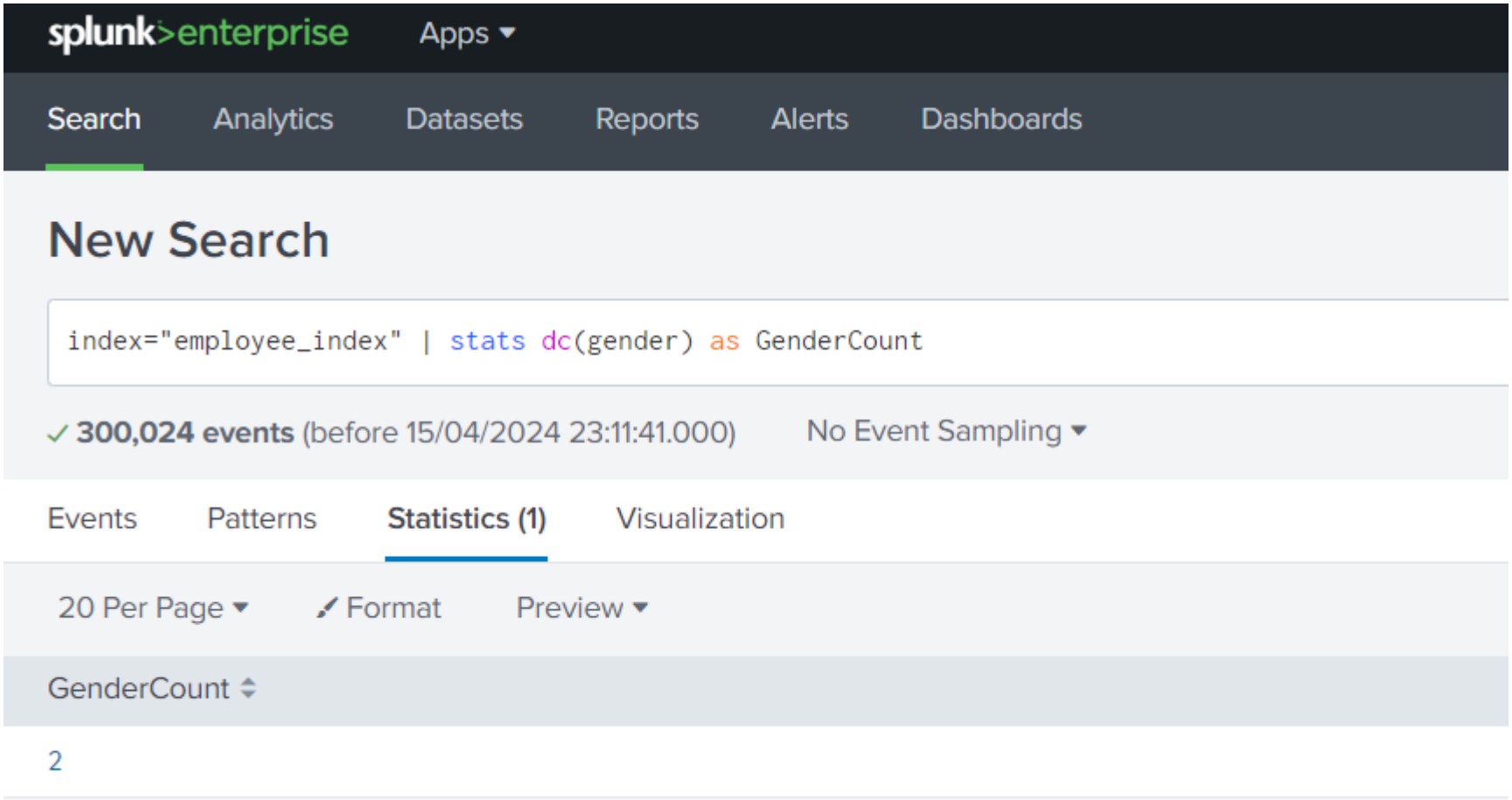
Dedup commands



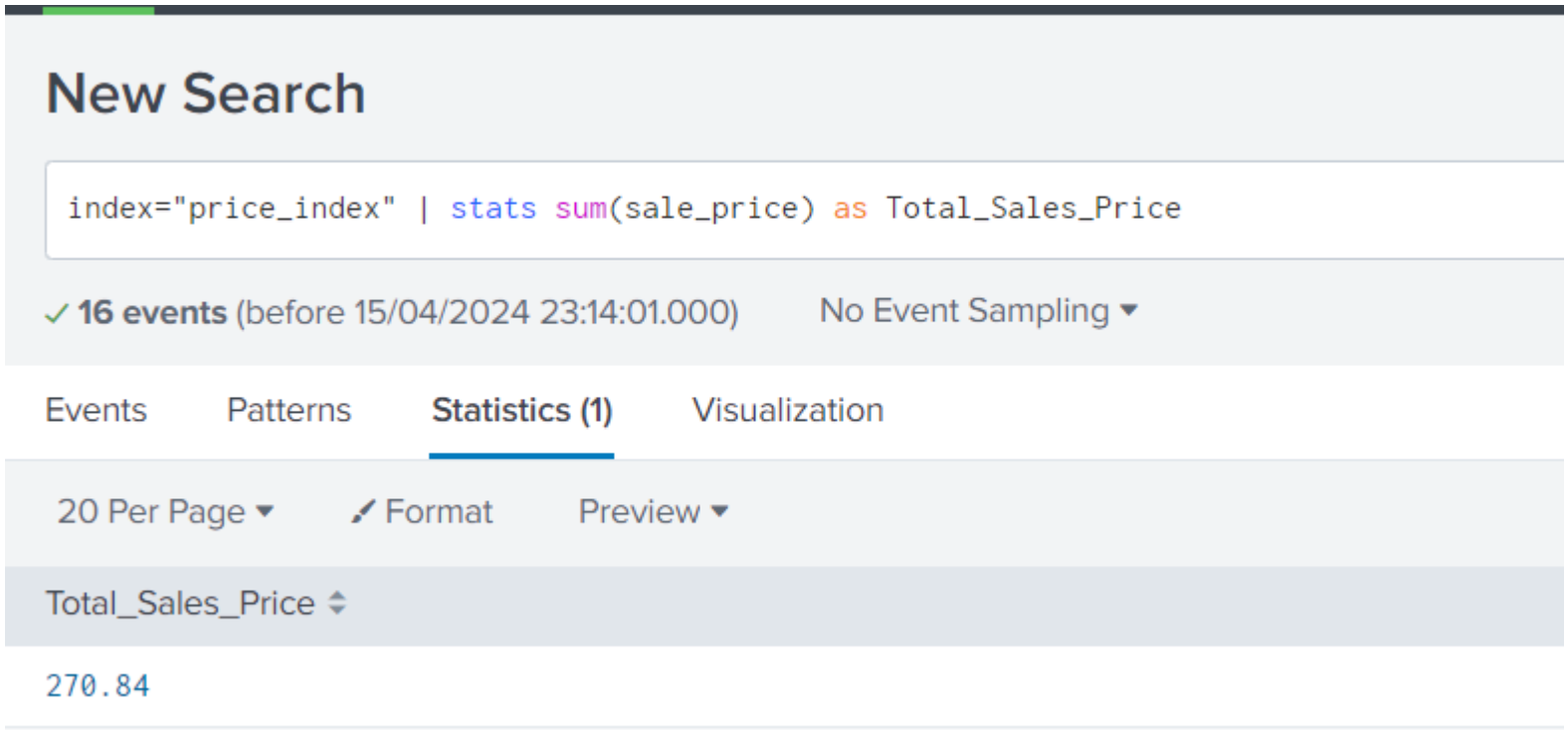
Stats distinct count commands



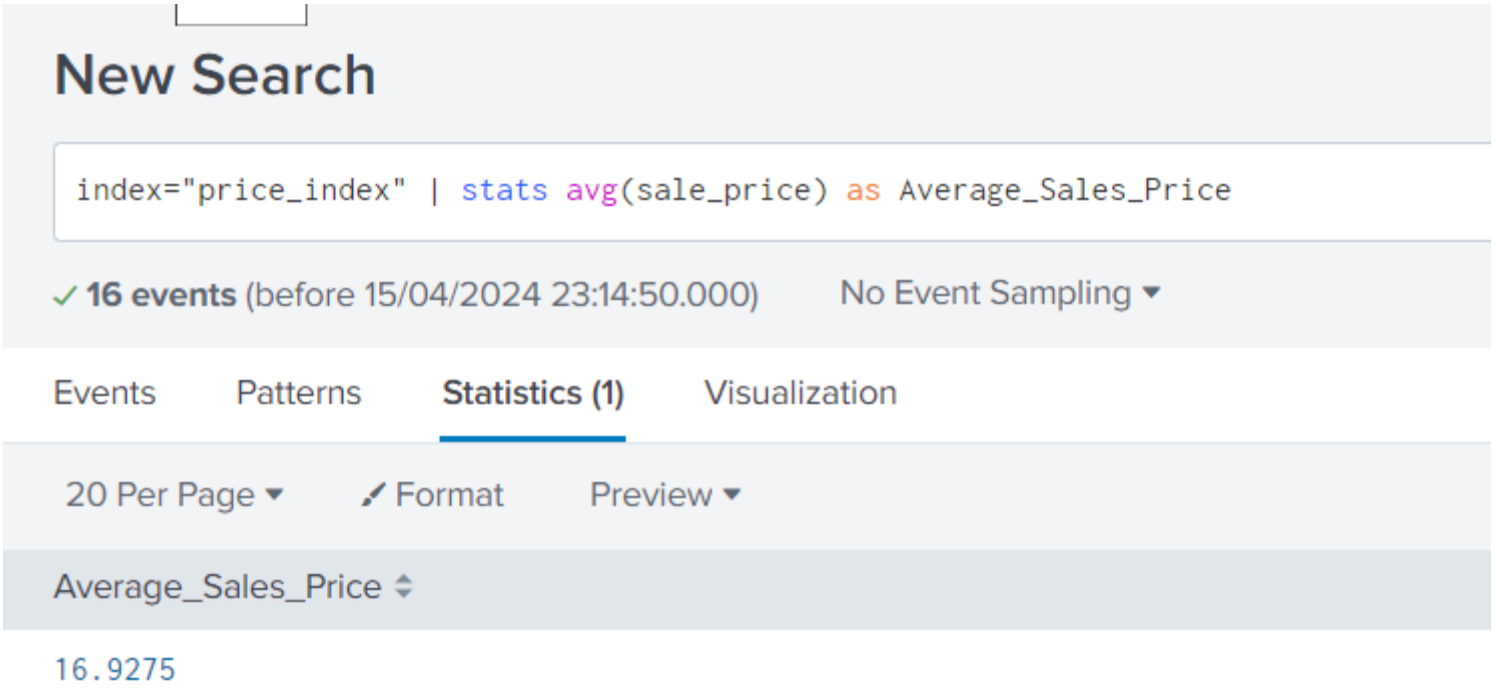
Stats distinct count commands



Stats sum commands



Stats sum commands



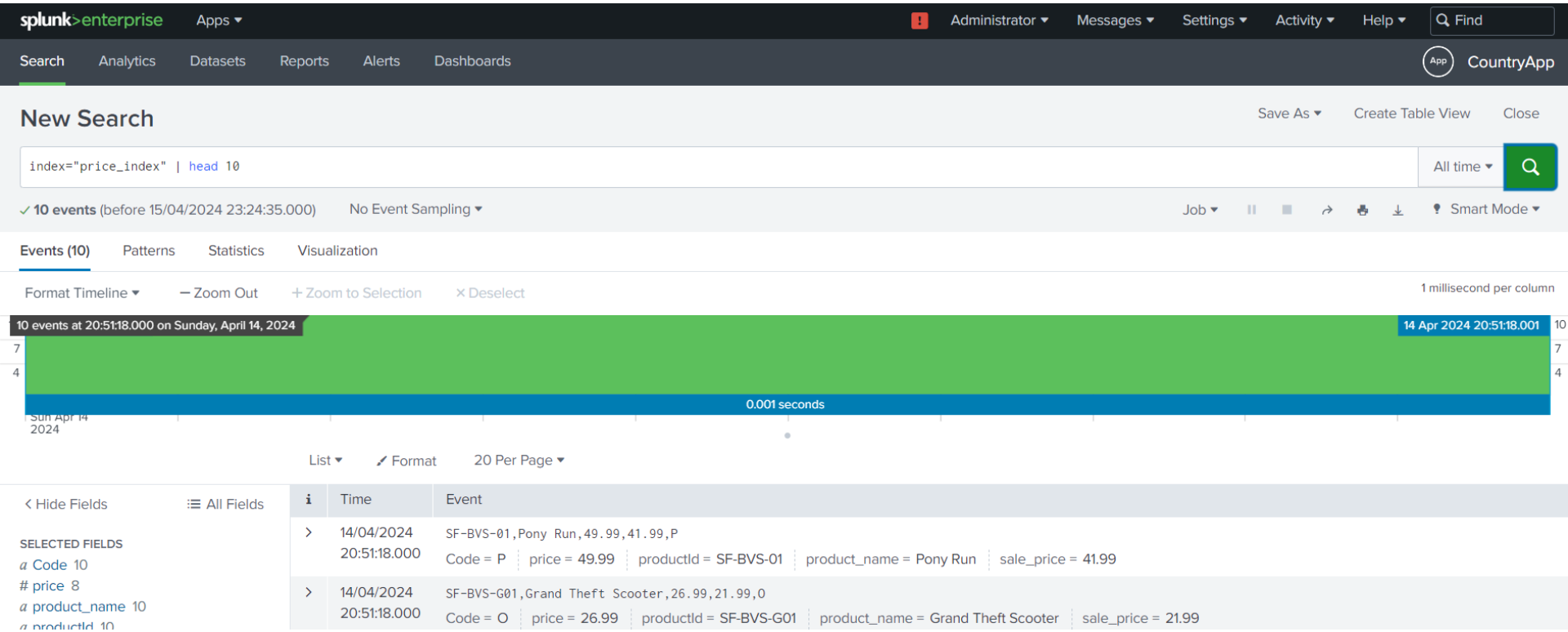
Stats commands

FUNCTION	RETURN VALUE USAGE: `STATS FOO=... / CHART BAR=... / TIMECHART T=...`
`avg(X)`	average of the values of field X
`count(X)`	number of occurrences of the field X. To indicate a specific field value to match, format X as `eval(field="desired_value")`.
`dc(X)`	count of distinct values of the field X
`earliest(X)` `latest(X)`	chronologically earliest/latest seen value of X
`max(X)`	maximum value of the field X. For non-numeric values of X, compute the max using alphabetical ordering.
`median(X)`	middle-most value of the field X
`min(X)`	minimum value of the field X. For non-numeric values of X, compute the min using alphabetical ordering.
`mode(X)`	most frequent value of the field X
`percN(Y)`	N-th percentile value of the field Y. N is a non-negative integer < 100.Example: `perc50(total)` = 50th percentile value of the field `total`.

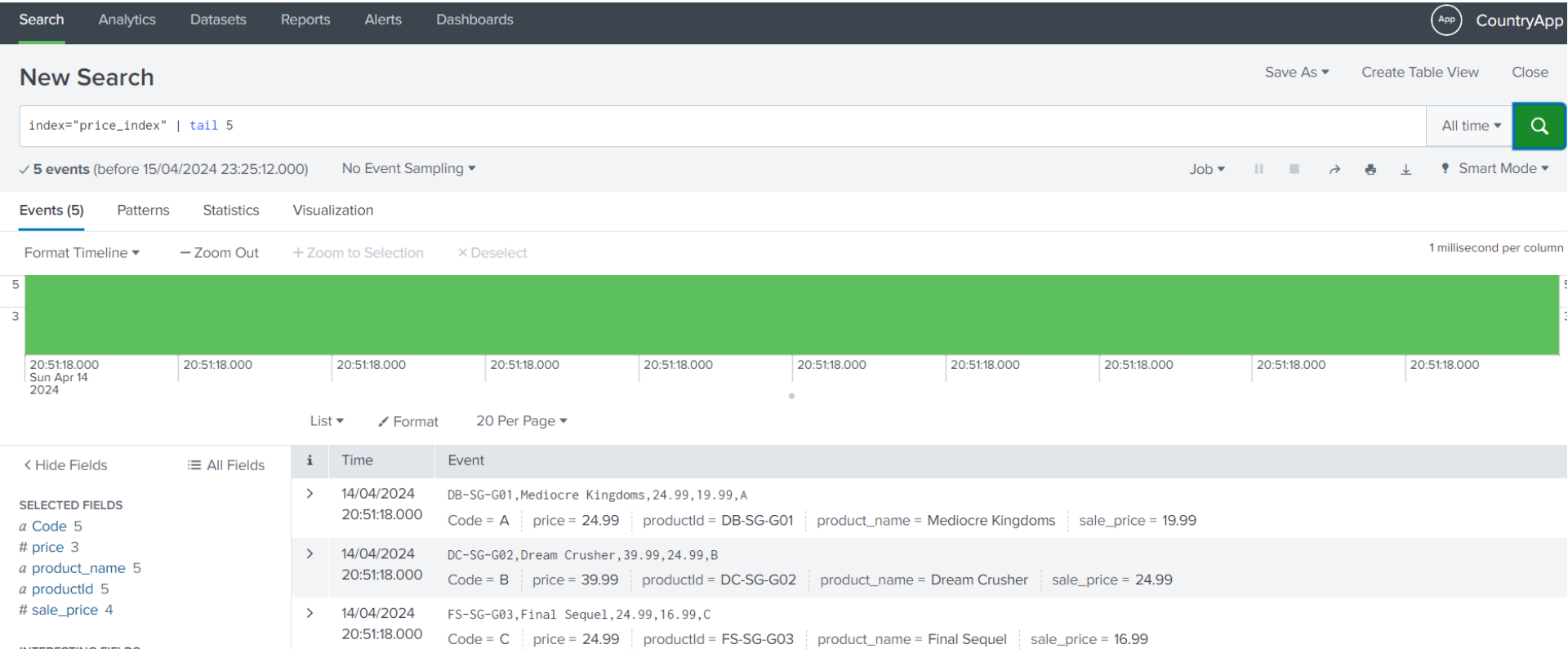
Stats commands

`range(X)`	difference between the max and min values of the field X
`stdev(X)`	sample standard deviation of the field X
`stdevp(X)`	population standard deviation of the field X
`sum(X)`	sum of the values of the field X
`sumsq(X)`	sum of the squares of the values of the field X
`values(X)`	list of all distinct values of the field X as a multi-value entry. The order of the values is alphabetical
`var(X)`	sample variance of the field X

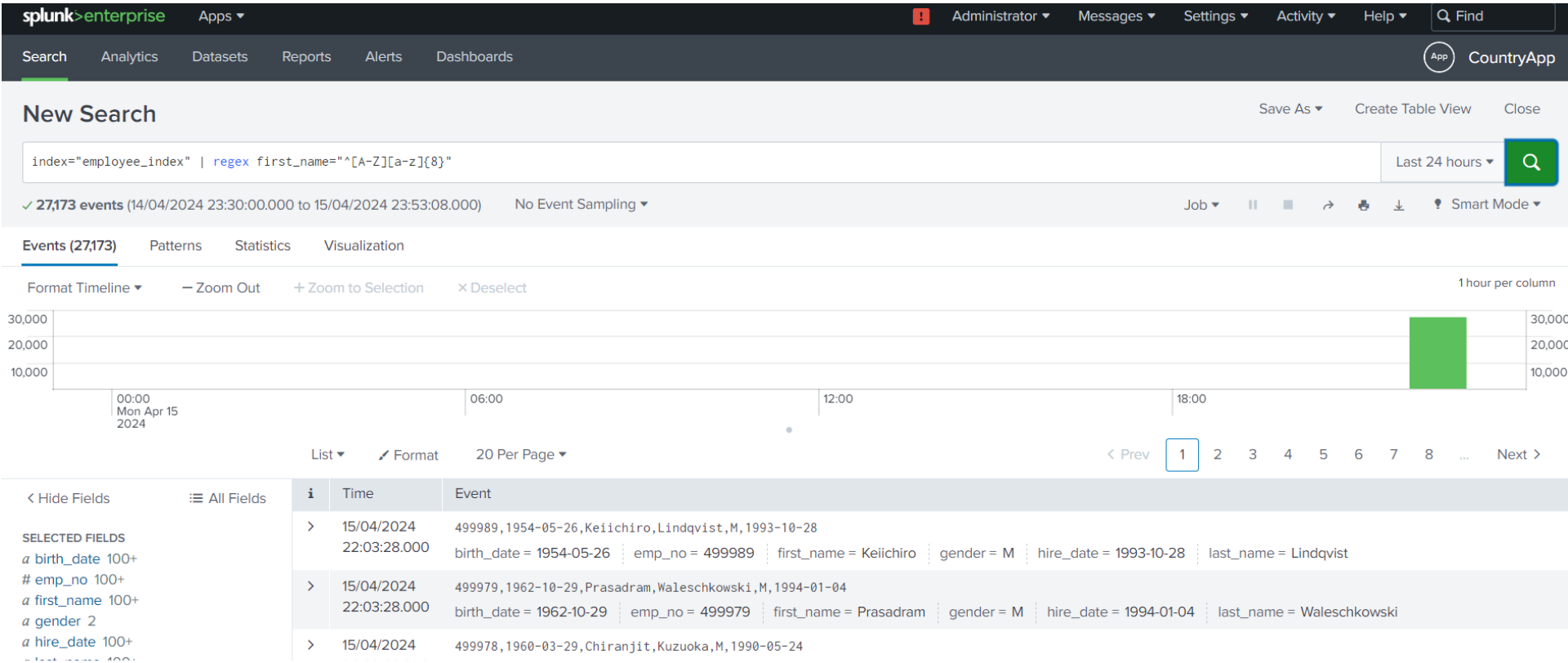
Head Tail commands



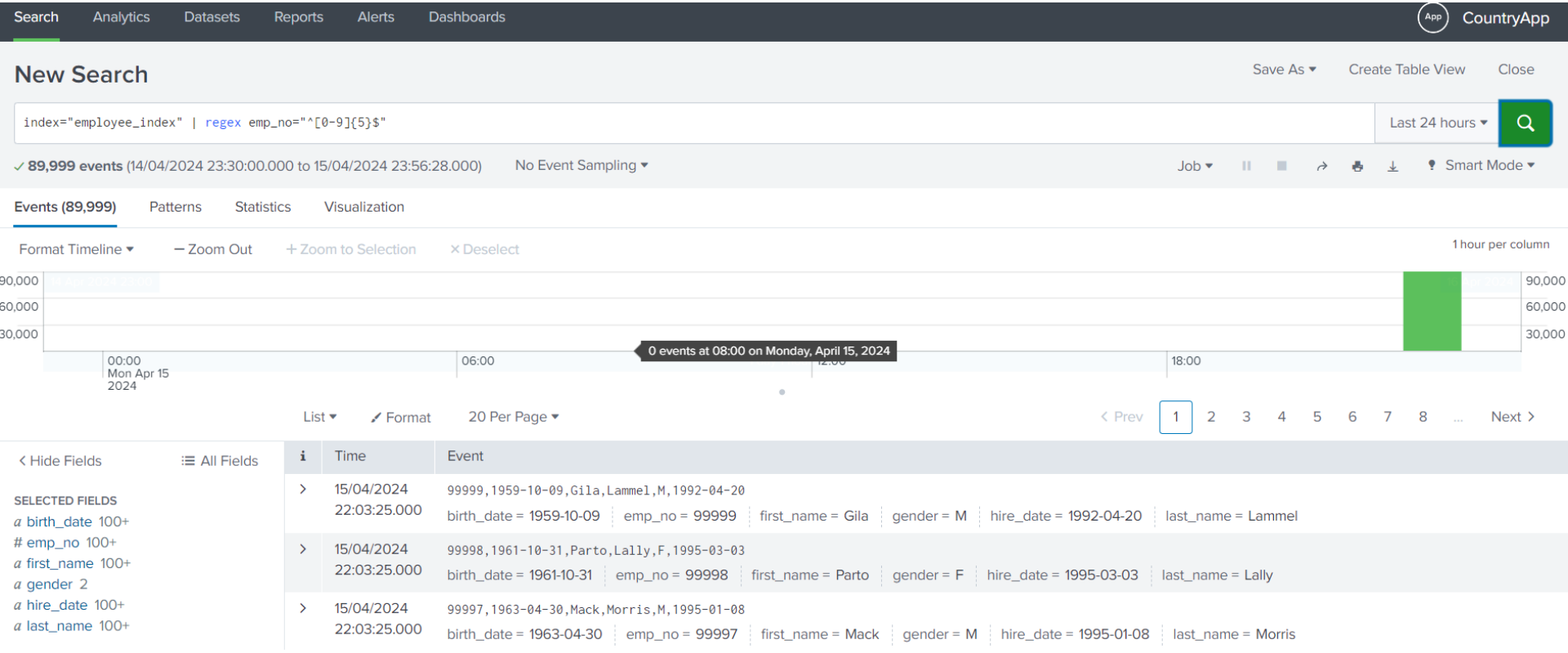
Head Tail commands



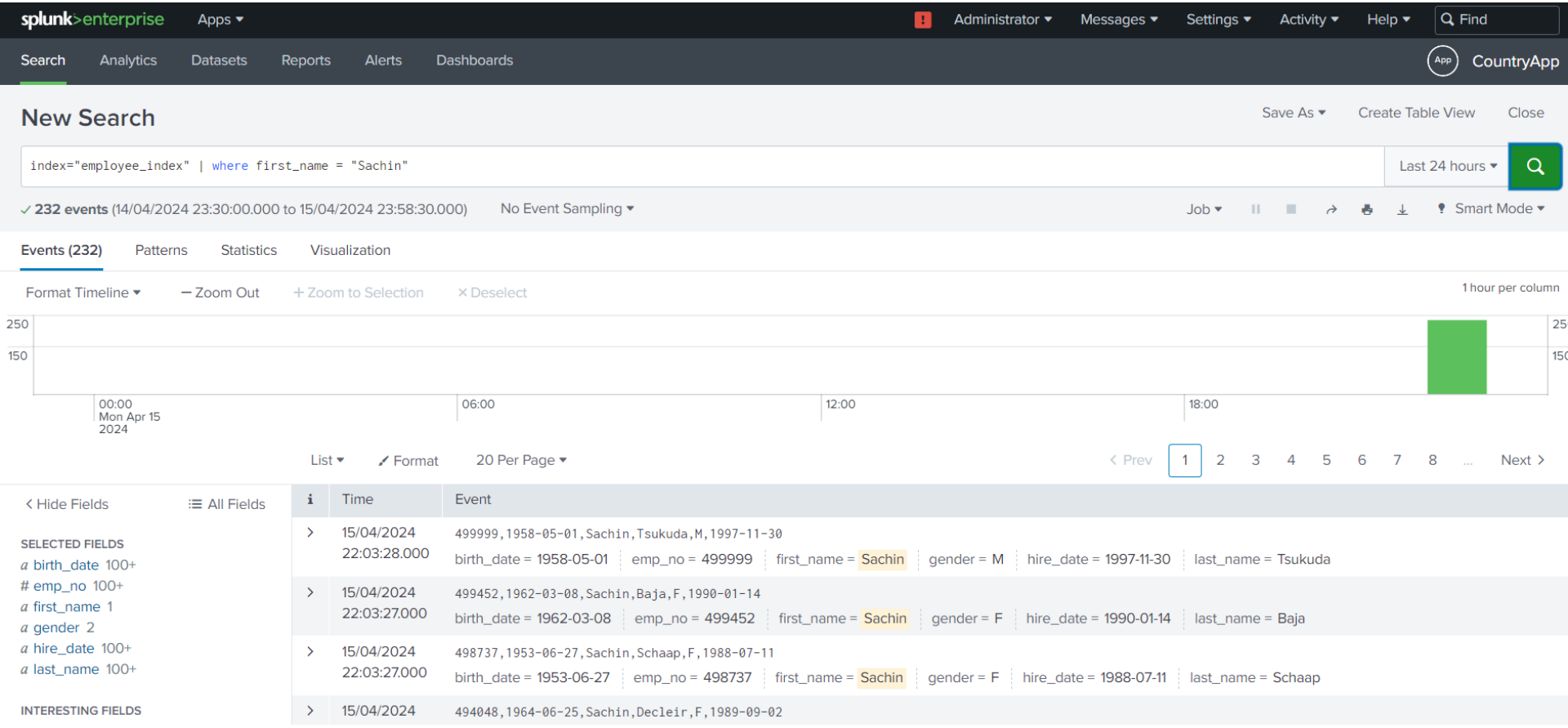
Regex commands



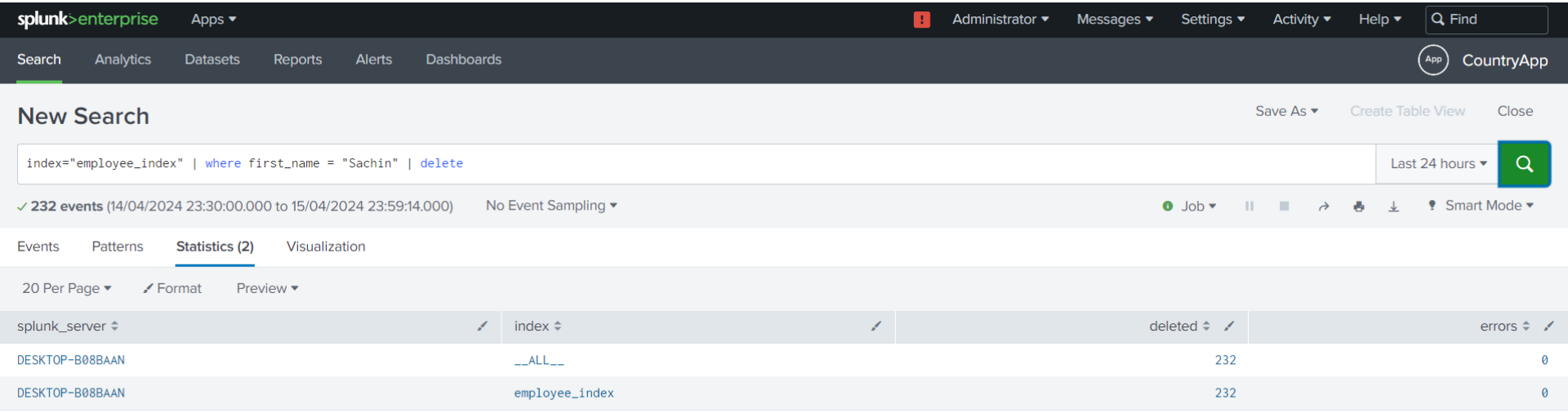
Regex commands



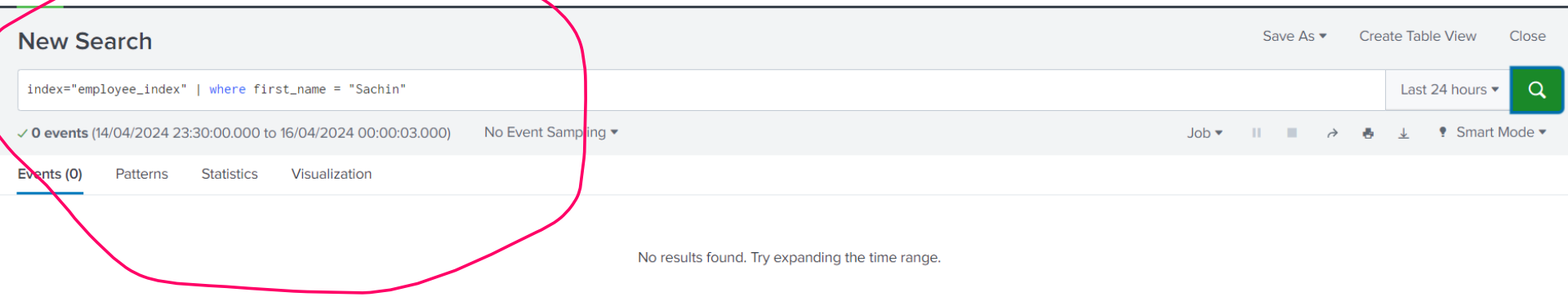
Where commands



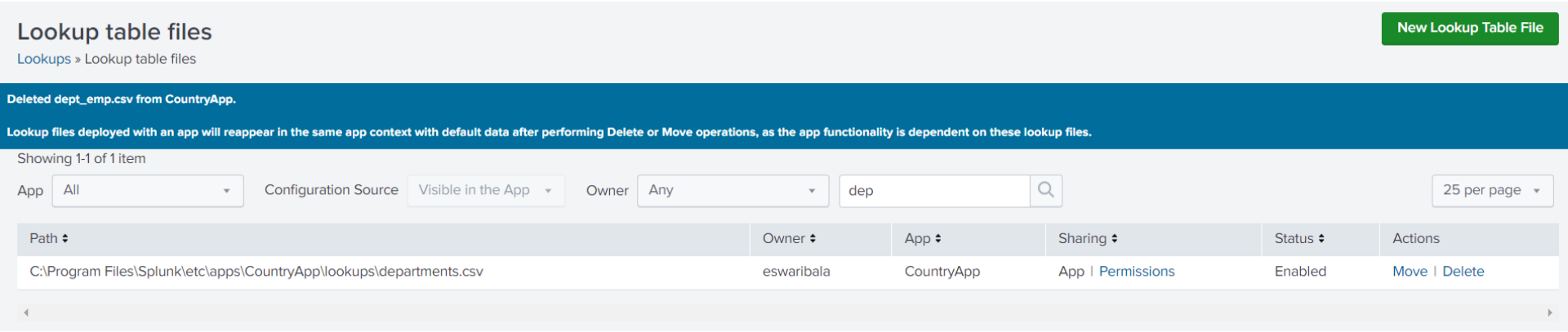
Delete commands (Refer can_delete)



Where commands



Lookup


Lookup table files
Lookups » Lookup table files
New Lookup Table File
Deleted dept_emp.csv from CountryApp.
Lookup files deployed with an app will reappear in the same app context with default data after performing Delete or Move operations, as the app functionality is dependent on these lookup files.
Showing 1-1 of 1 item
App All
Configuration Source Visible in the App
Owner Any
dep
25 per page
Path
Owner
App
Sharing
Status
Actions
C:\Program Files\Splunk\etc\apps\CountryApp\lookups\departments.csv
eswaribala
CountryApp
App | Permissions
Enabled
Move | Delete

Lookup

New Search

```
| inputlookup departments.csv
```

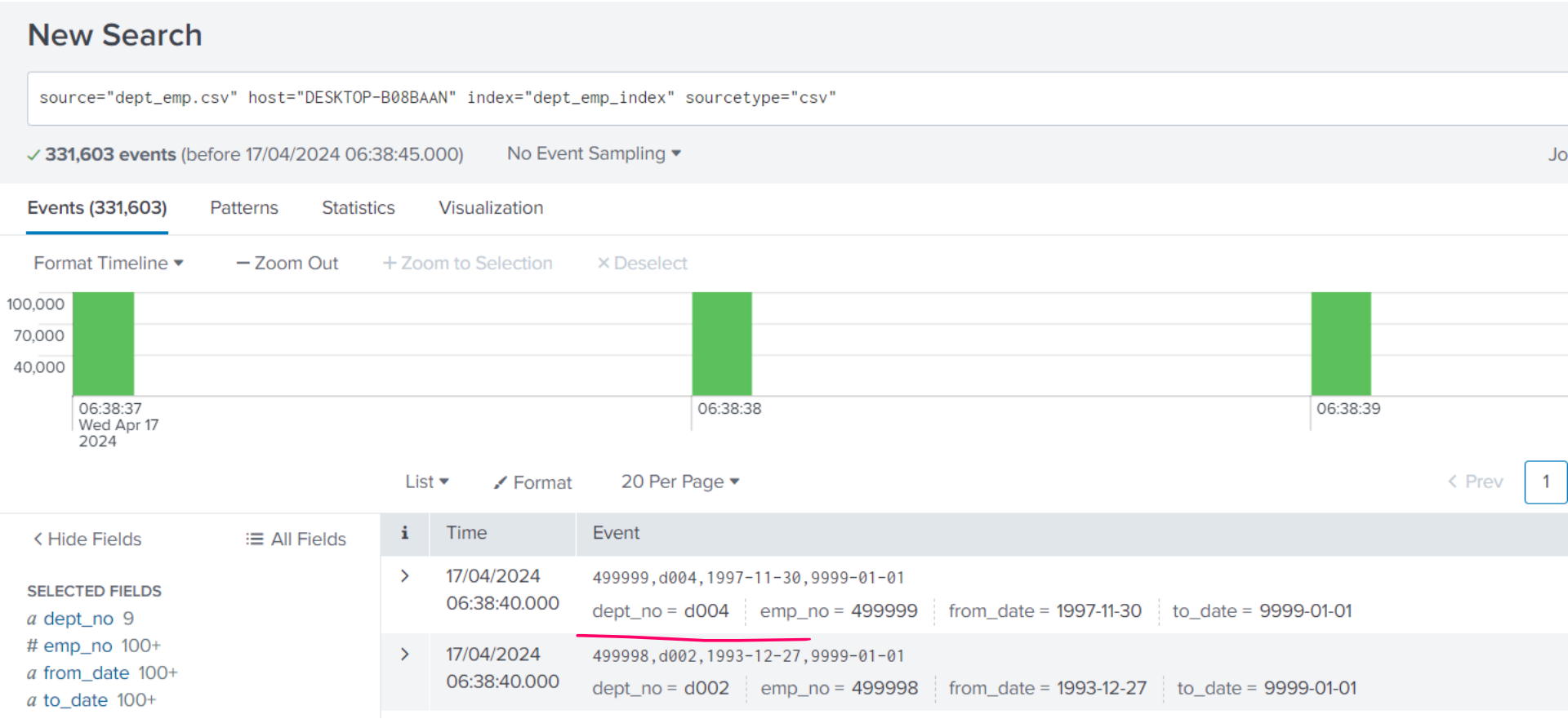
✓ 9 results (16/04/2024 06:30:00.000 to 17/04/2024 06:36:58.000) No Event Sampling

Events Patterns **Statistics (9)** Visualization

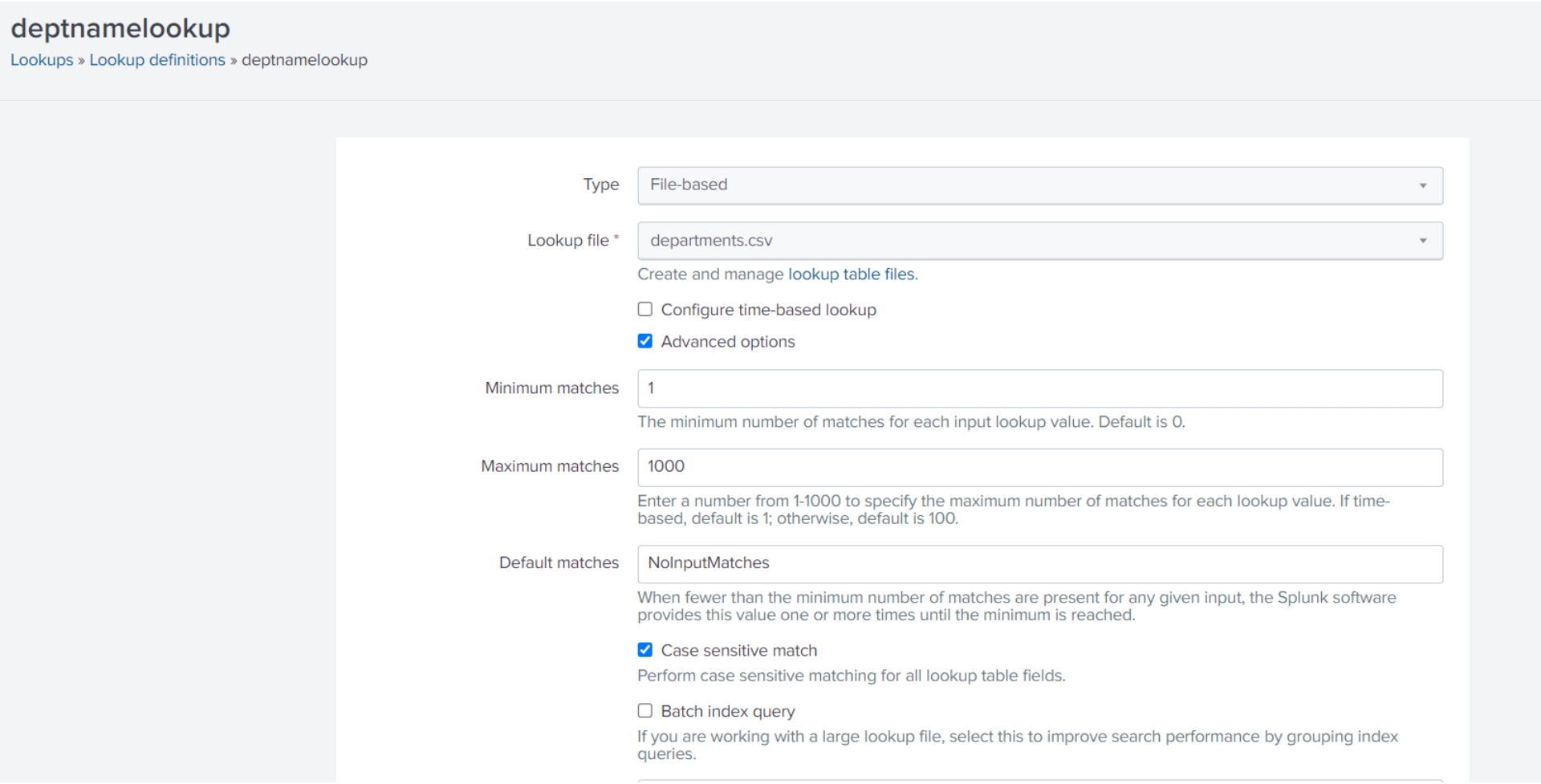
20 Per Page Format Preview

dept_name	dept_no
Customer Service	d009
Development	d005
Finance	d002
Human Resources	d003
Marketing	d001
Production	d004
Quality Management	d006
Research	d008
Sales	d007

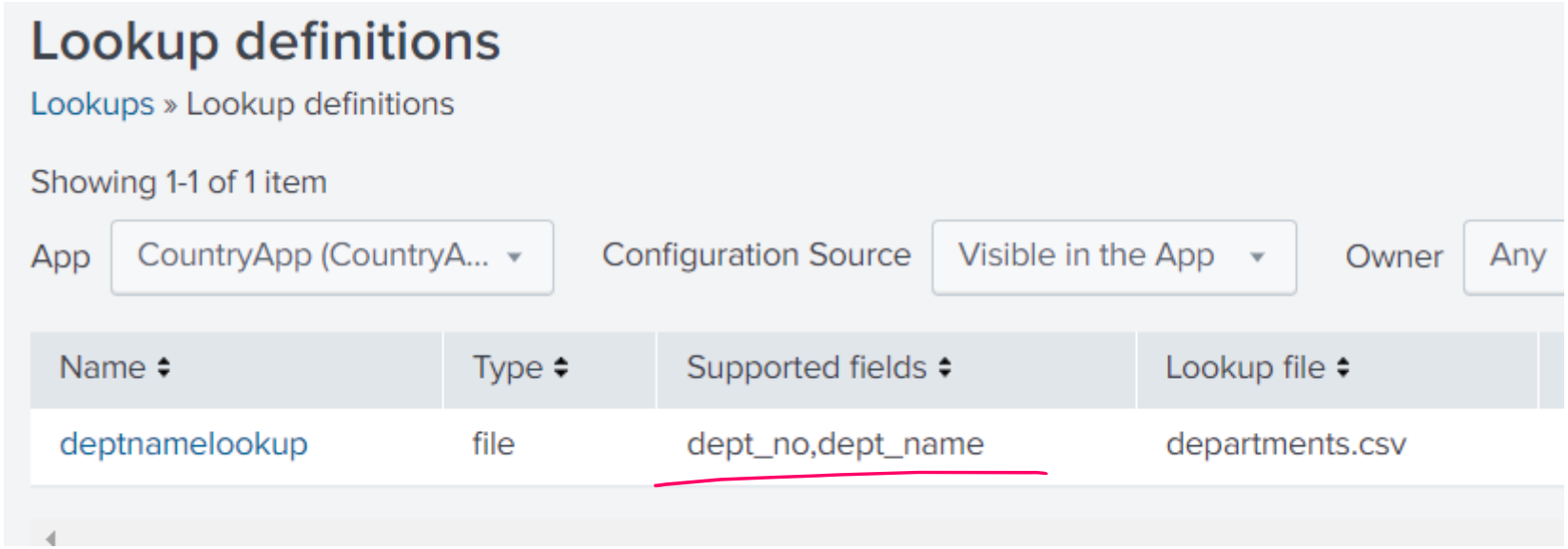
Lookup Needed



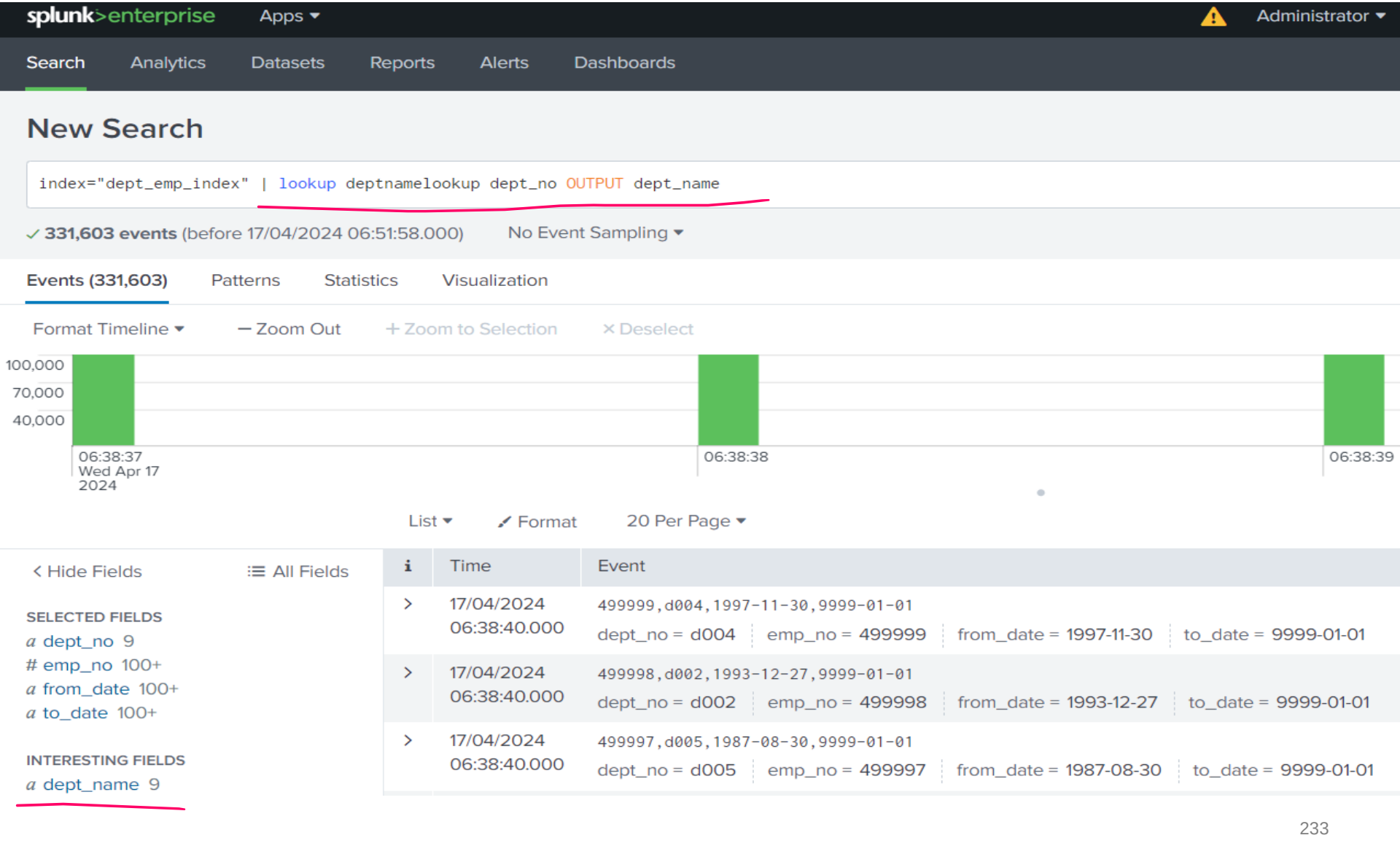
Lookup Definition



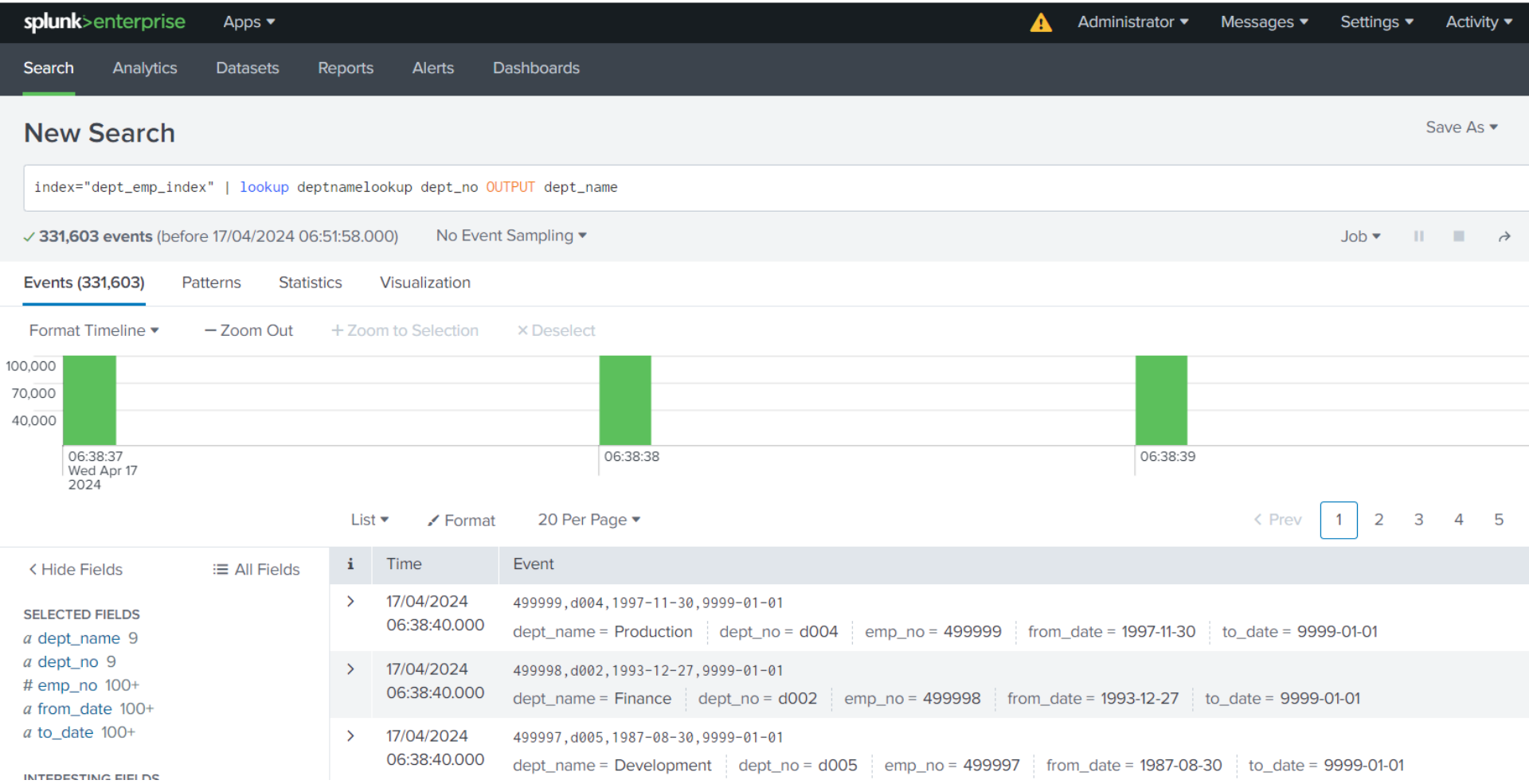
Lookup Definition



Lookup command



Lookup command



Lookup command

New Search

```
index="dept_emp_index" | lookup deptnamelookup dept_no OUTPUT dept_name | table emp_no dept_name
```

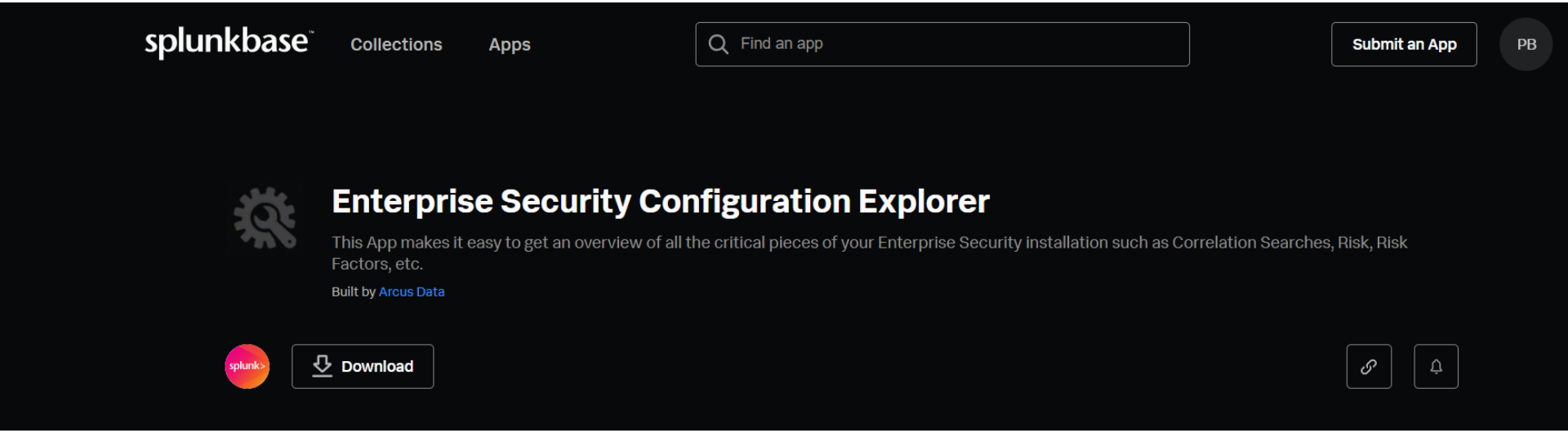
✓ **331,603 events** (before 17/04/2024 06:56:19.000) No Event Sampling

Events Patterns **Statistics (331,603)** Visualization

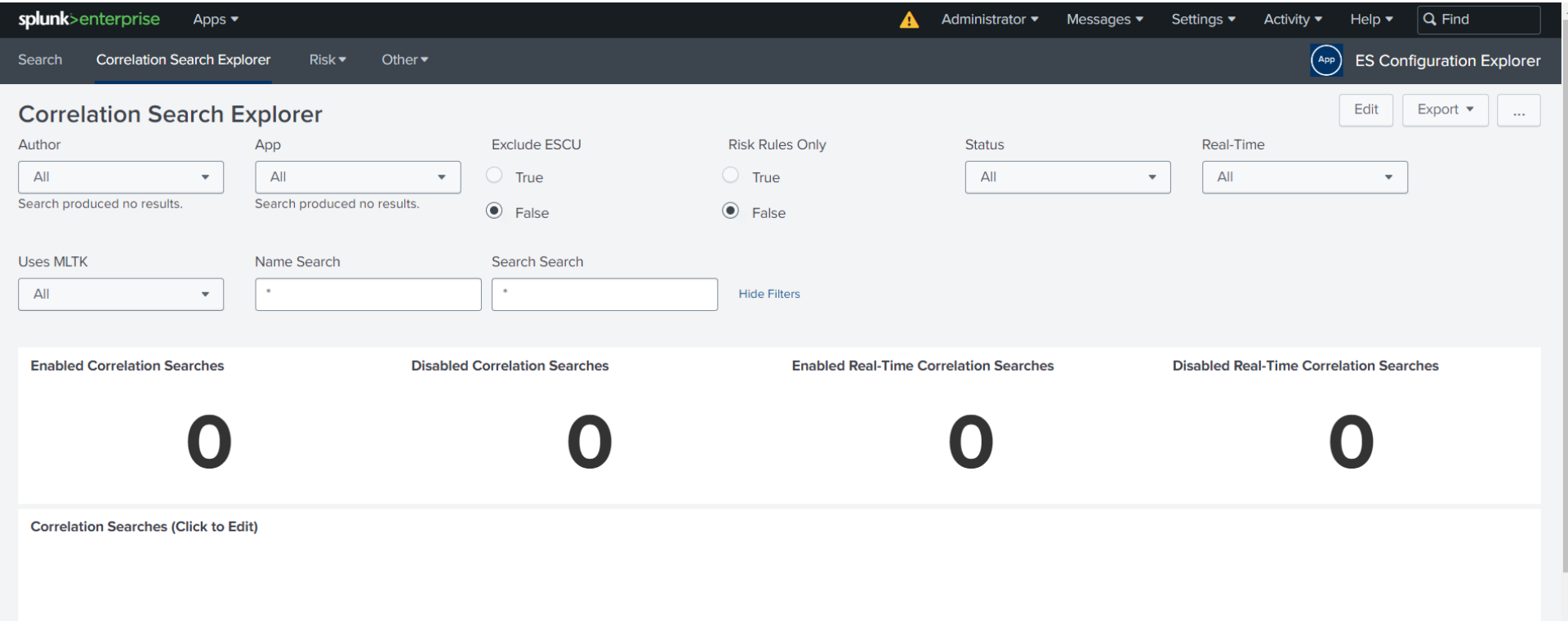
20 Per Page Format Preview

emp_no	dept_name
491815	Sales
491814	Development
491813	Production
491812	Human Resources
491811	Sales
491810	Production

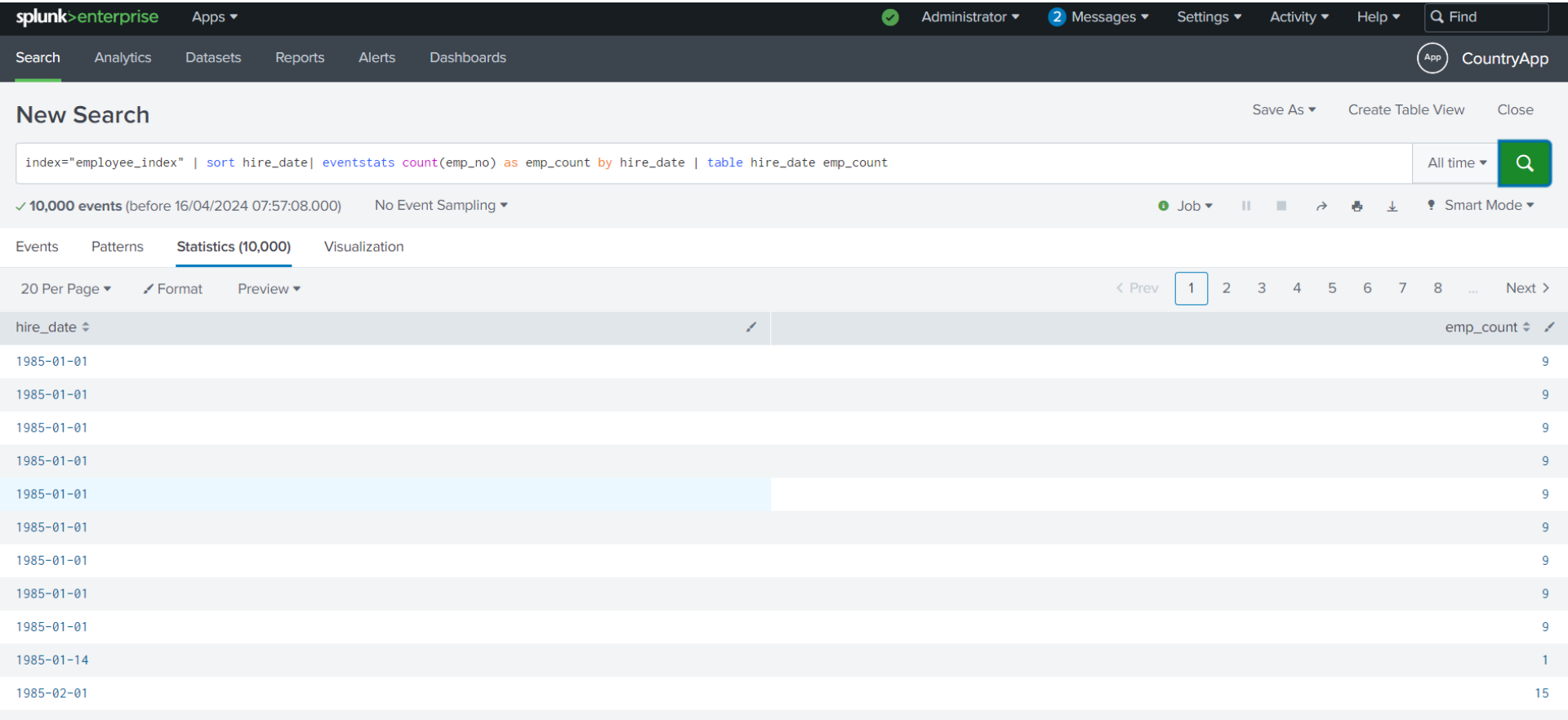
Correlation Search



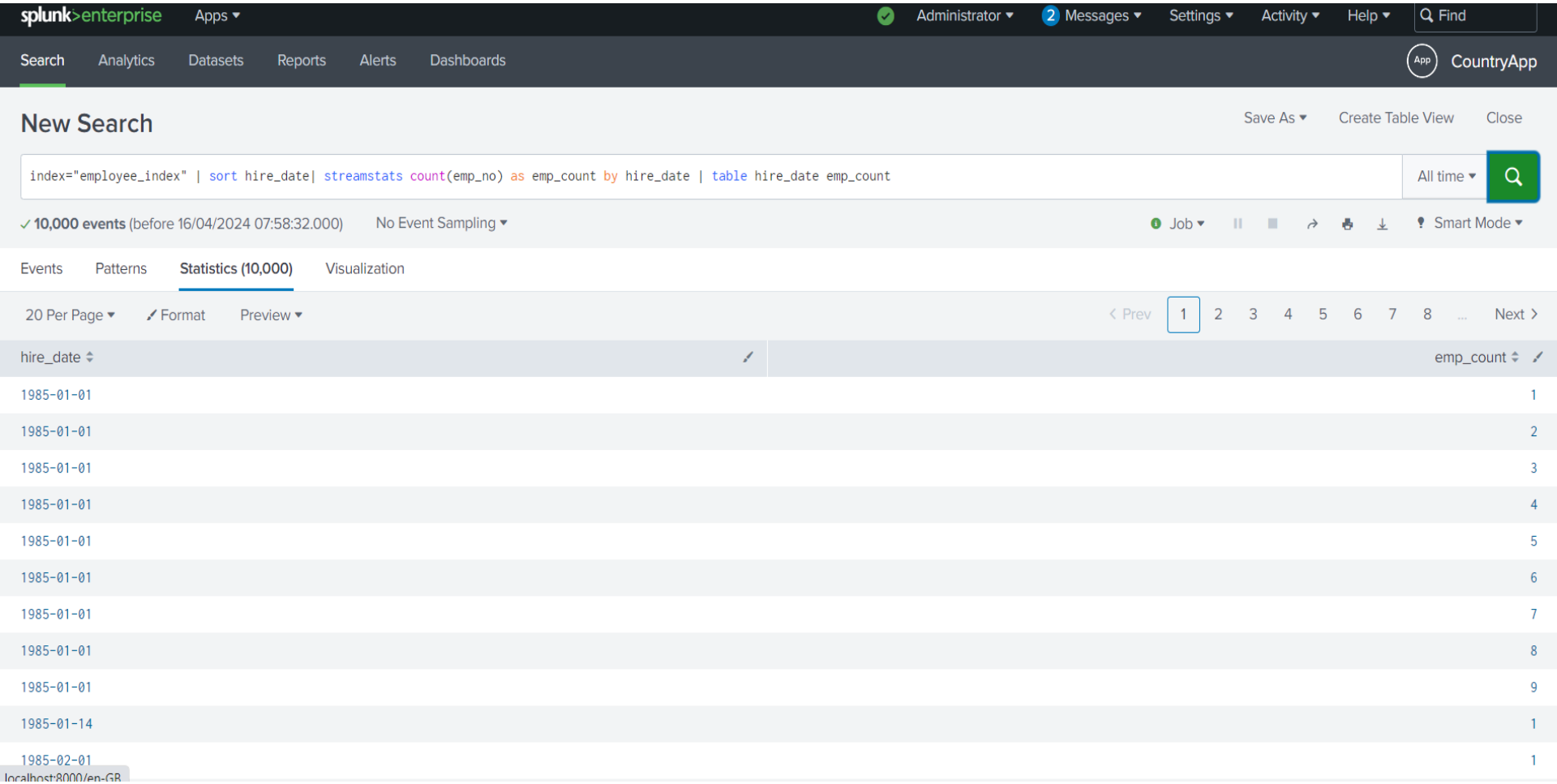
Correlation Search



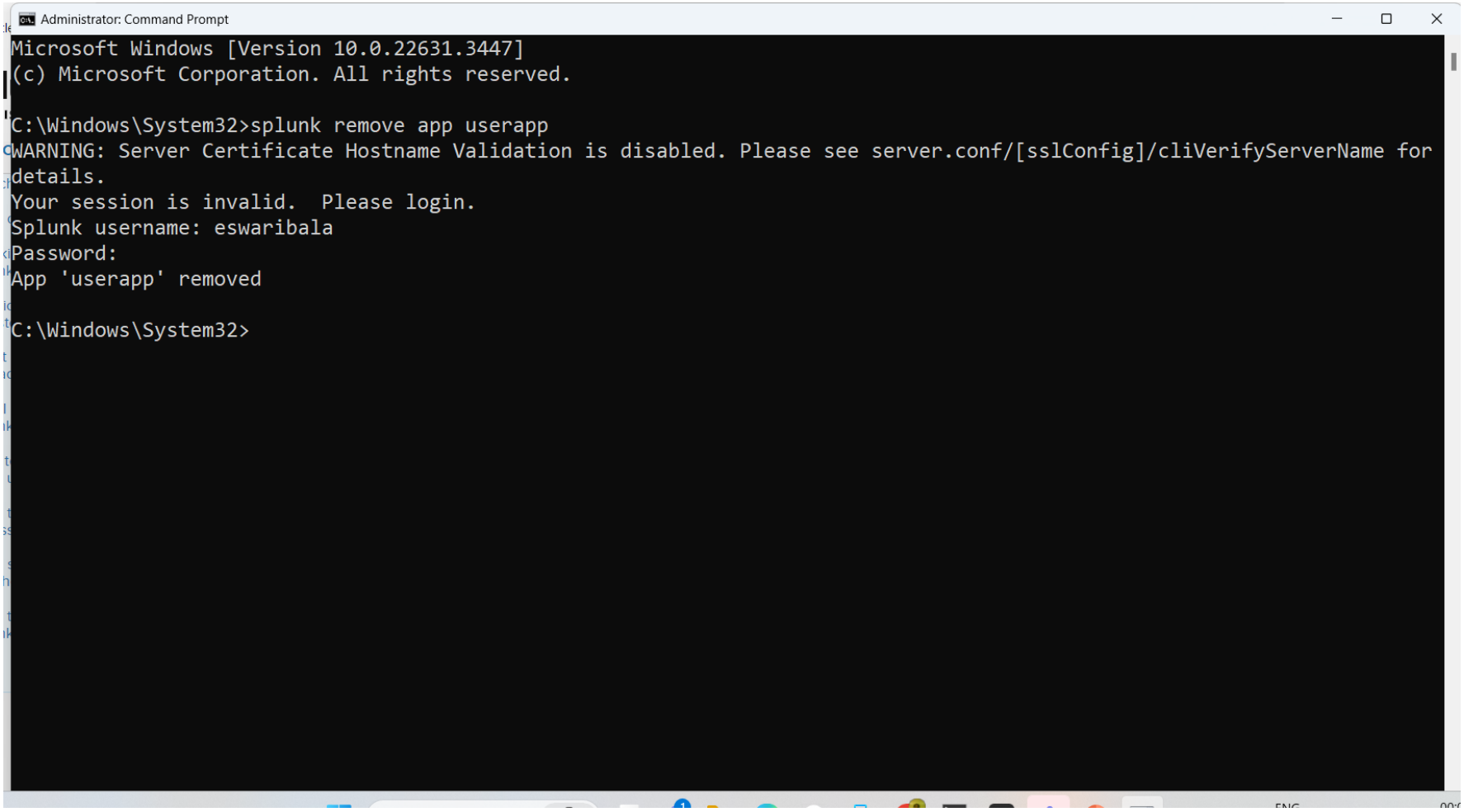
EventStats


splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
App
CountryApp
New Search
Save As
Create Table View
Close
index="employee_index" | sort hire_date| eventstats count(emp_no) as emp_count by hire_date | table hire_date emp_count
All time
10,000 events (before 16/04/2024 07:57:08.000)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (10,000)
Visualization
20 Per Page
Format
Preview
Prev
1
2
3
4
5
6
7
8
...
Next
hire_date
emp_count
1985-01-01 9
1985-01-01 9
1985-01-01 9
1985-01-01 9
1985-01-01 9
1985-01-01 9
1985-01-01 9
1985-01-01 9
1985-01-01 9
1985-01-01 9
1985-01-14 1
1985-02-01 15

StreamStats



Delete App


Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.3447]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\System32>splunk remove app userapp
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Your session is invalid. Please login.
Splunk username: eswaribala
Password:
App 'userapp' removed
C:\Windows\System32>

Distributable streaming

- A streaming command operates on each event returned by a search.
- For distributable streaming, the order of the events does not matter.
- A distributable streaming command is a command that can be run on the indexer, which improves processing time.
- The other commands in a search determine if the distributable streaming command is run on the indexer:

Distributable streaming

- A streaming command operates on each event returned by a search.
- For distributable streaming, the order of the events does not matter.
- A distributable streaming command is a command that can be run on the indexer, which improves processing time.
- The other commands in a search determine if the distributable streaming command is run on the indexer:

Distributable streaming

- Distributable streaming commands can be applied to subsets of indexed data in a parallel manner. For example, the rex command is streaming. It extracts fields and adds them to events at search time.

- Some of the common distributable streaming commands are: eval, fields, makemv, rename, regex, replace, strcat, typer, and where.

Centralized streaming

- For centralized streaming commands, the order of the events matters.
- A centralized streaming command applies a transformation to each event returned by a search.
- But unlike distributable streaming commands, a centralized streaming command only works on the search head.
- You might also hear the term "stateful streaming" to describe these commands.
- Centralized streaming commands include: head, streamstats, some modes of dedup, and some modes of cluster.

Transforming

- A transforming command orders the search results into a data table.
- These commands "transform" the specified cell values for each event into numerical values that Splunk software can use for statistical purposes.
- Transforming commands are not streaming.
- Also, transforming commands are required to transform search result data into the data structures that are required for visualizations such as column, bar, line, area, and pie charts.
- Transforming commands include: chart, timechart, stats, top, rare, and addtotals when it is used to calculate column totals (not row totals).

Generating

- A generating command fetches information from the indexes, without any transformations.
- Generating commands are either event-generating (distributable or centralized) or report-generating.
- Most report-generating commands are also centralized. Depending on which type the command is, the results are returned in a list or a table.
- Generating commands do not expect or require an input.
- Generating commands are usually invoked at the beginning of the search and with a leading pipe.
- That is, there cannot be a search piped into a generating command.
- The exception to this is the search command, because it is implicit at the start of a search and does not need to be invoked.
- Examples of generating commands include: dbinspect, datamodel, inputcsv, metadata, pivot, search, and tstats

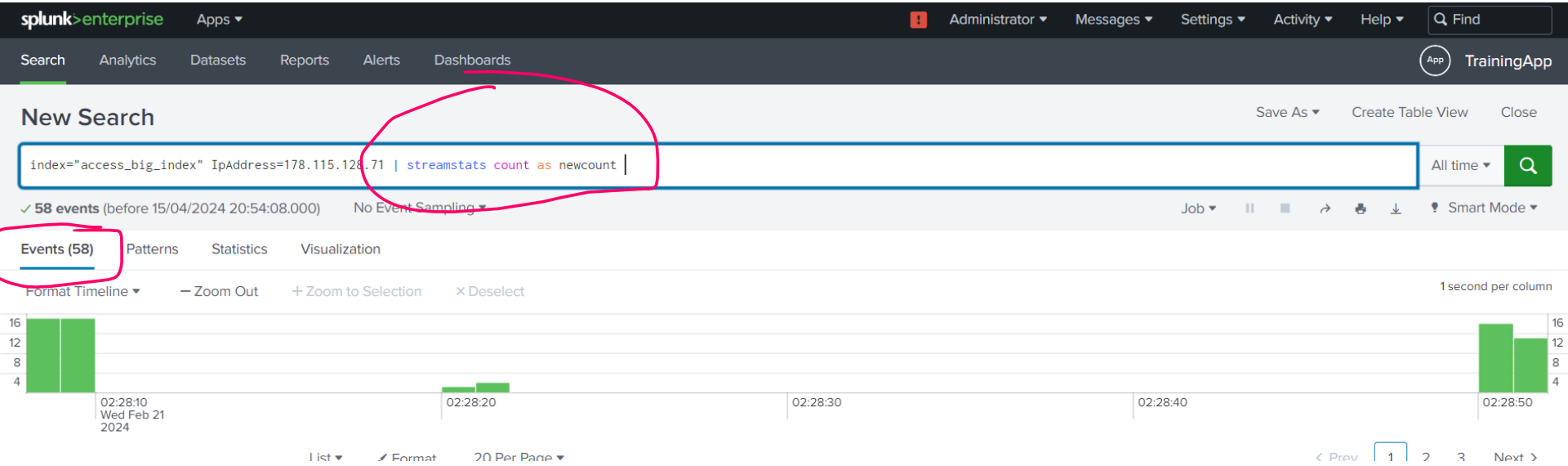
Orchestrating

- An orchestrating command is a command that controls some aspect of how the search is processed.
- It does not directly affect the final result set of the search.
- For example, you might apply an orchestrating command to a search to enable or disable a search optimization that helps the overall search complete faster.
- Examples of orchestrating commands include redistribute, noop, and localop.
- The lookup command also becomes an orchestrating command when you use it with the local=t argument.

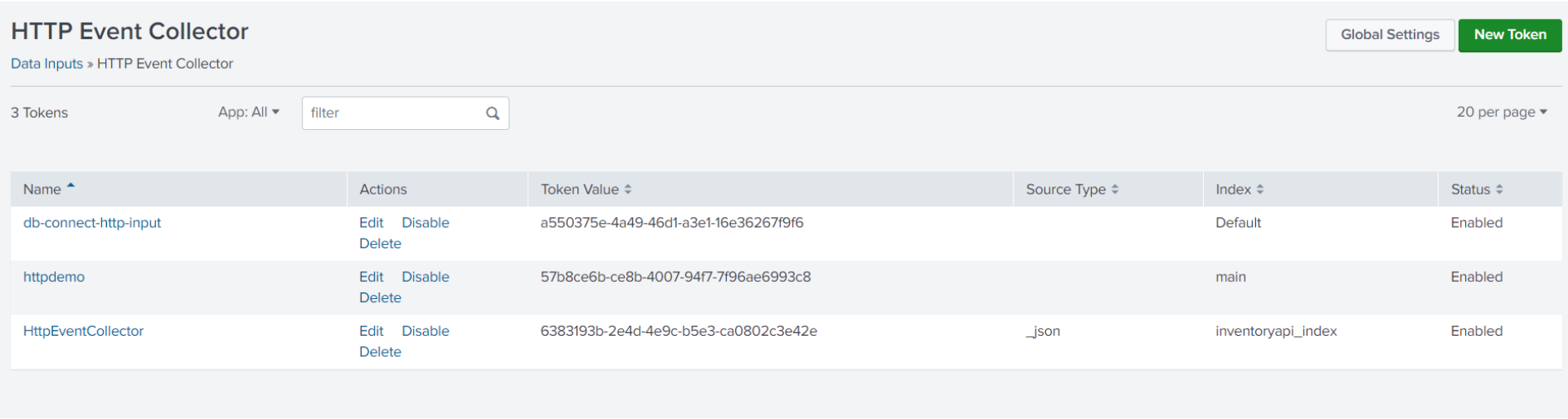
Dataset processing

- There are a handful of commands that require the entire dataset before the command can run.
- These commands are referred to as dataset processing commands.
- These commands are not transforming, not distributable, not streaming, and not orchestrating.
- Some of these commands fit into other types in specific situations or when specific arguments are used.
- Examples of data processing commands include: sort, eventstats, and some modes of cluster, dedup, and fillnull.

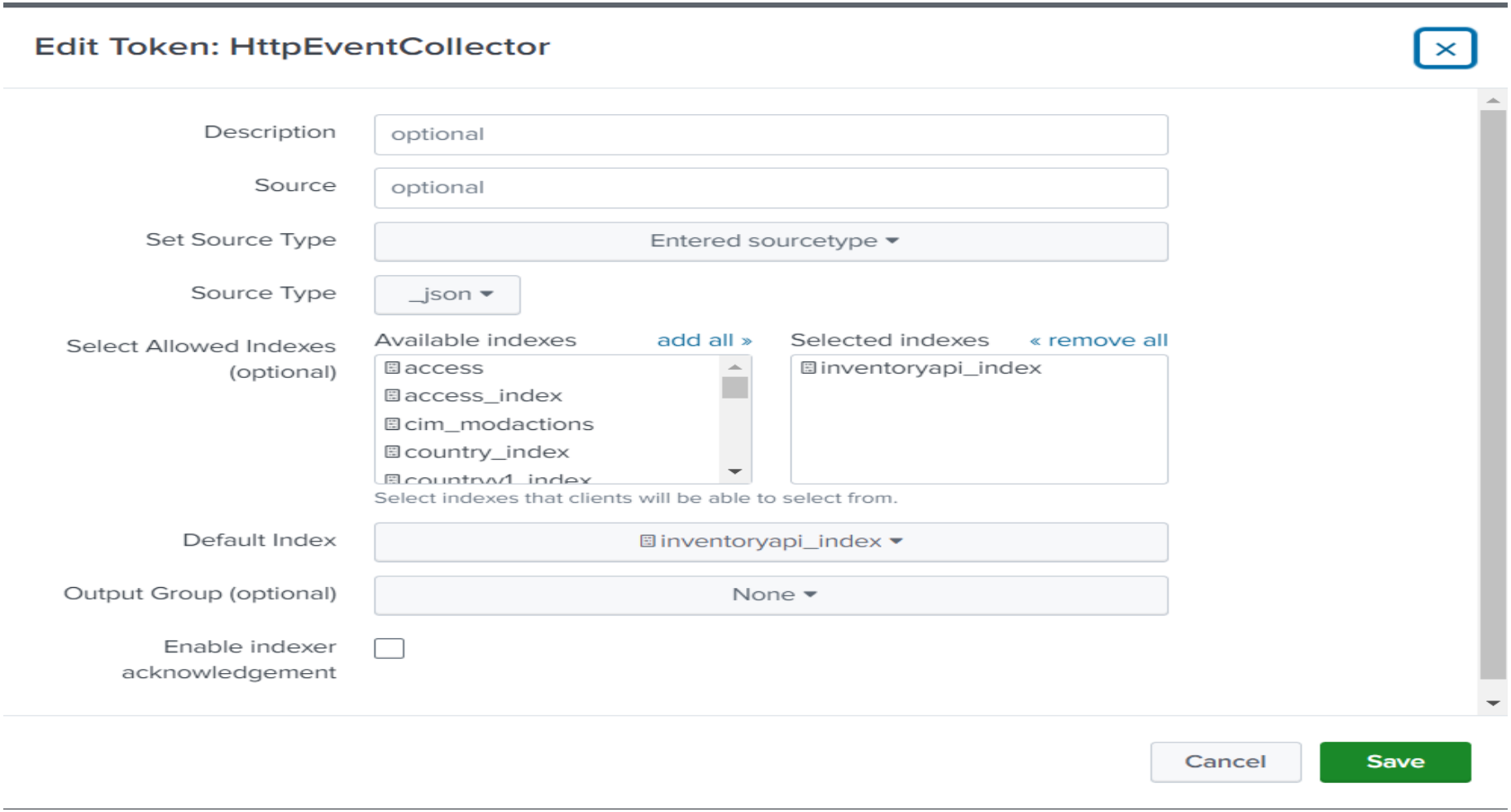
Authentication



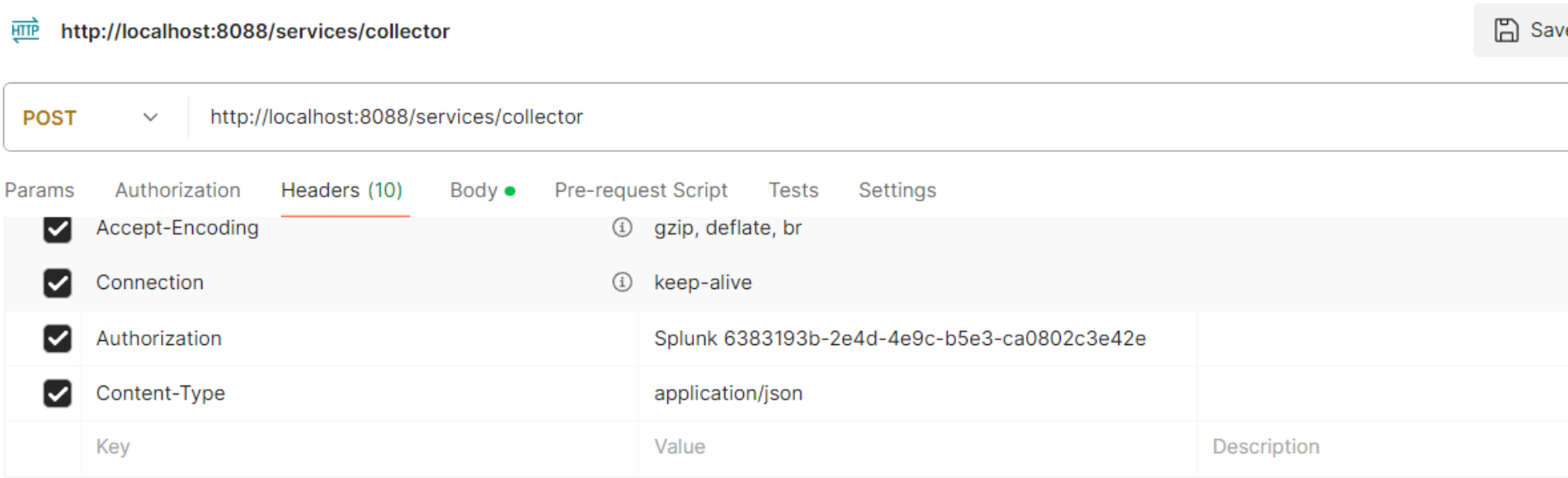
Splunk Http Event Collector



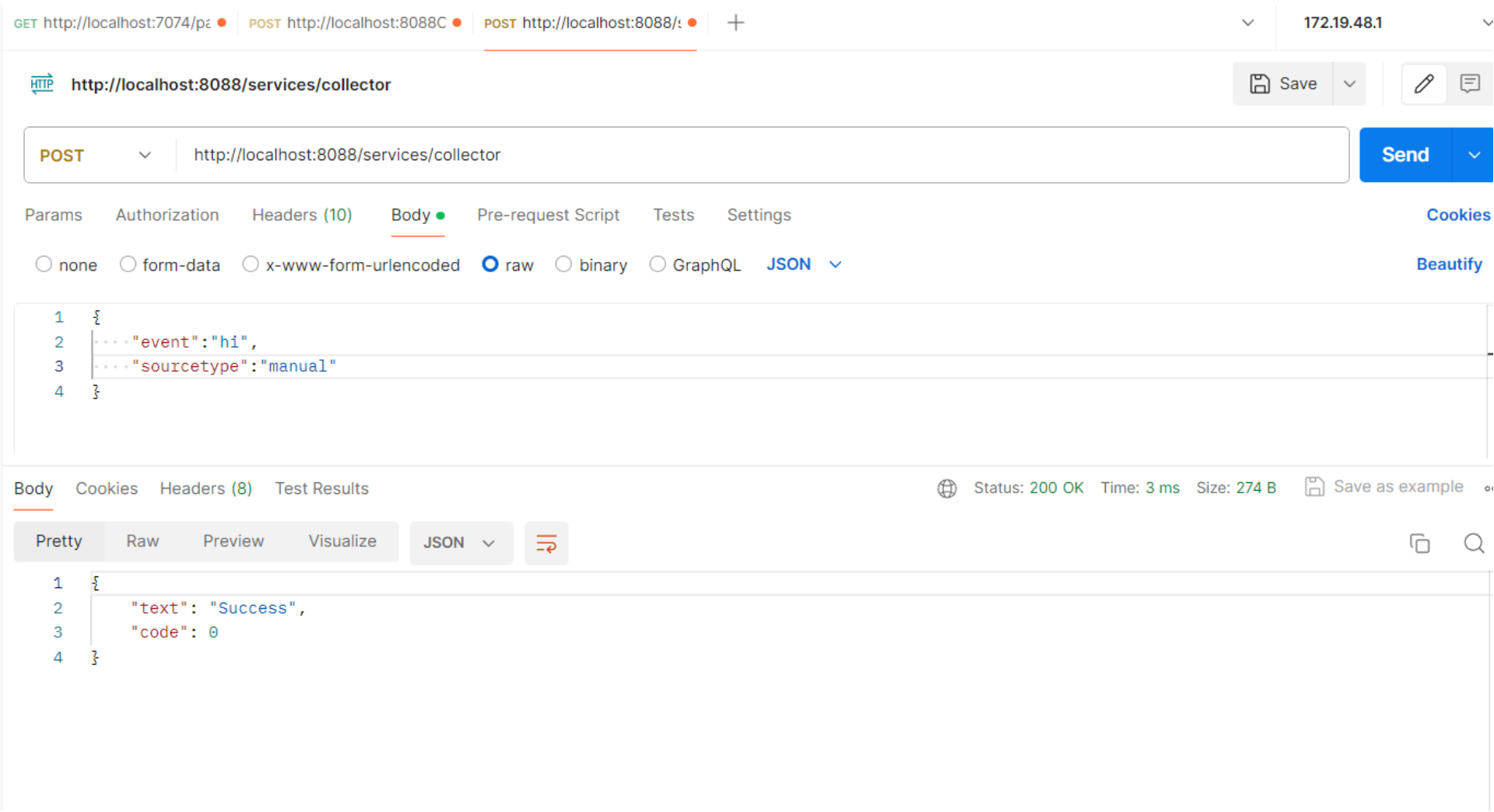
Splunk Http Event Collector



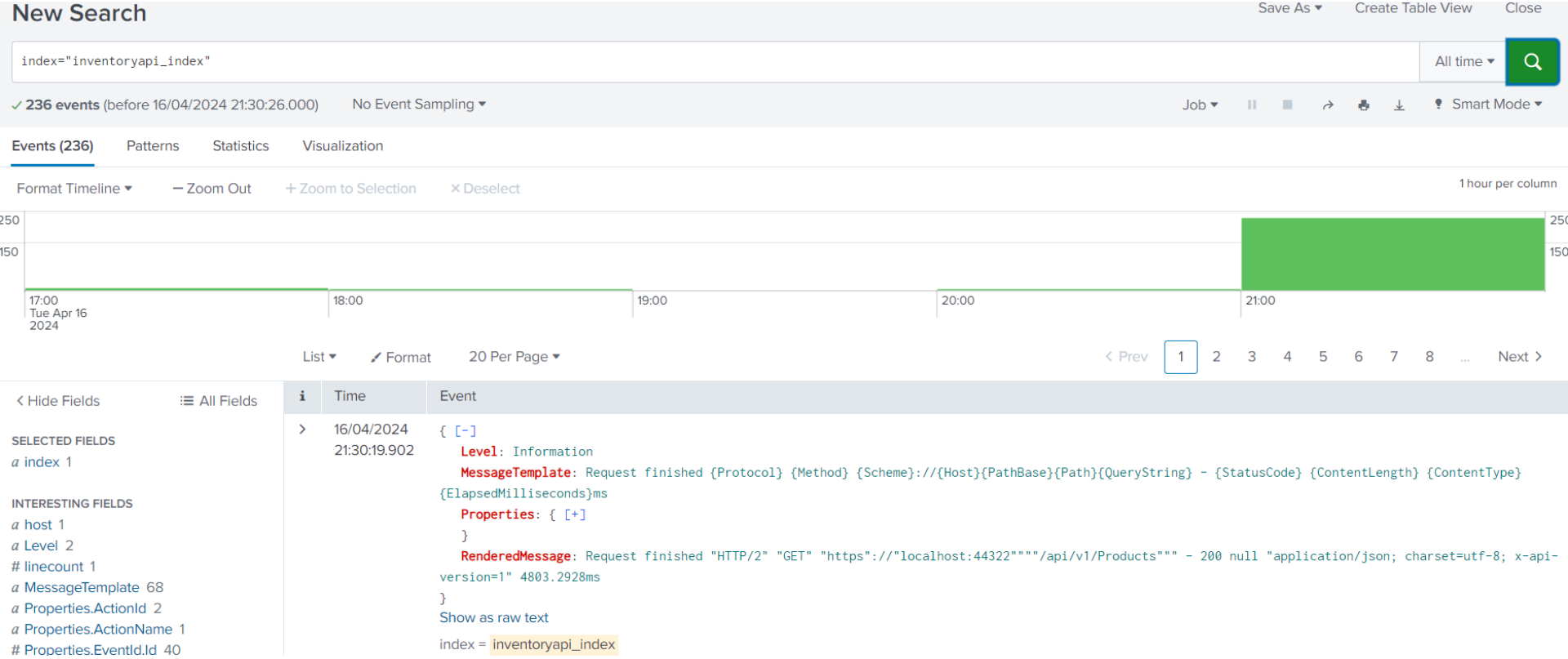
Splunk Http Event Collector



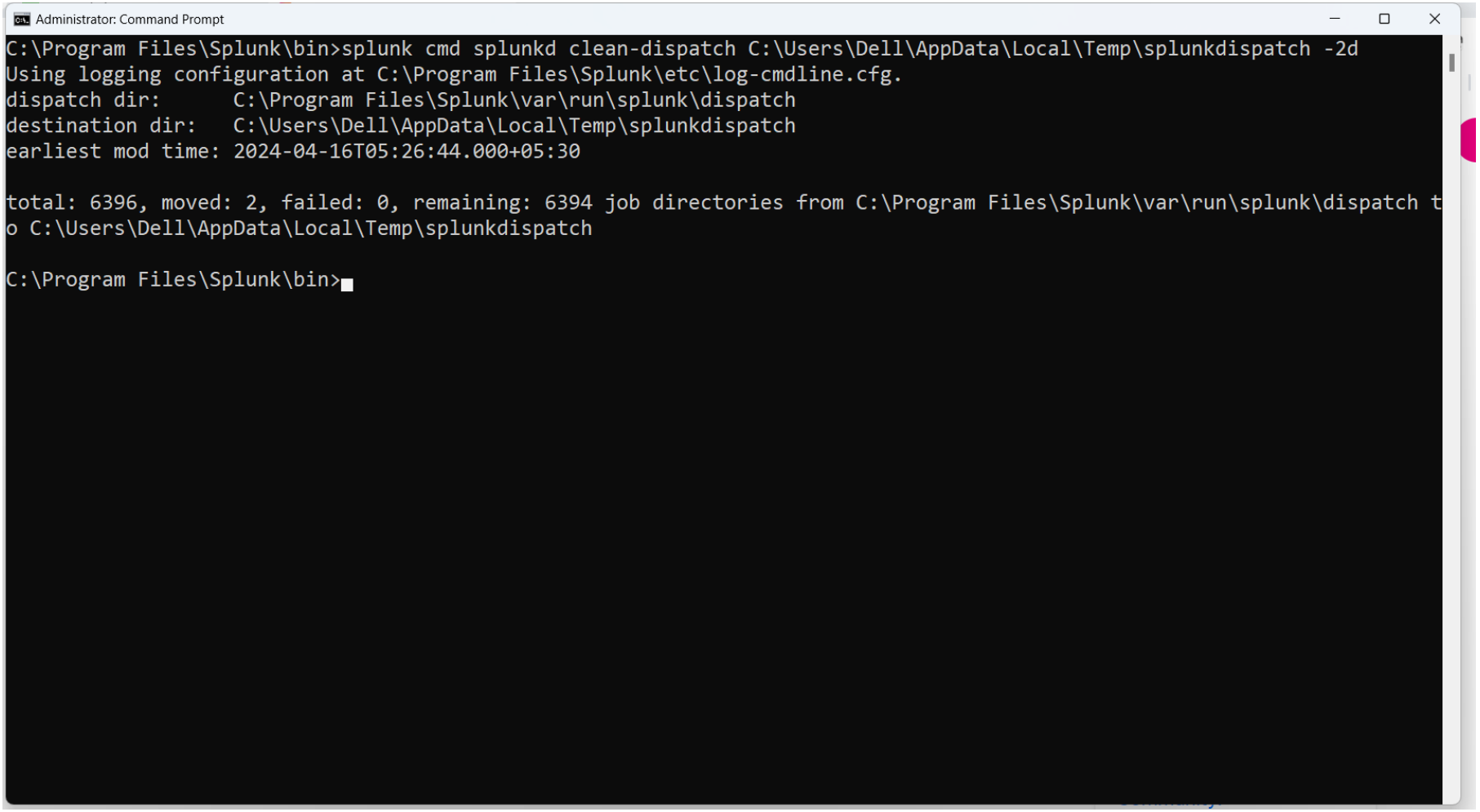
Splunk Http Event Collector



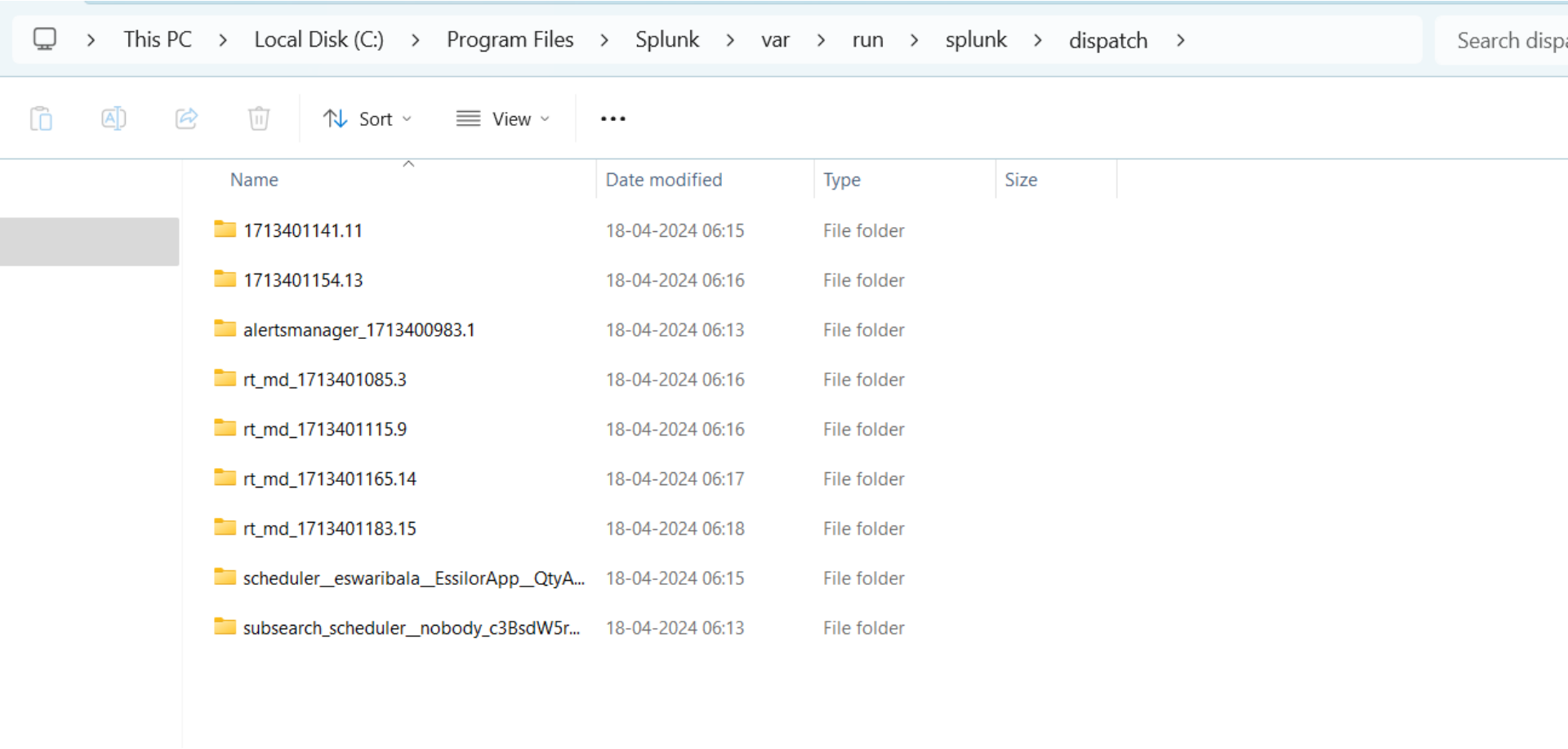
Splunk Http Event Collector



Splunk clean dispatch – too many queries

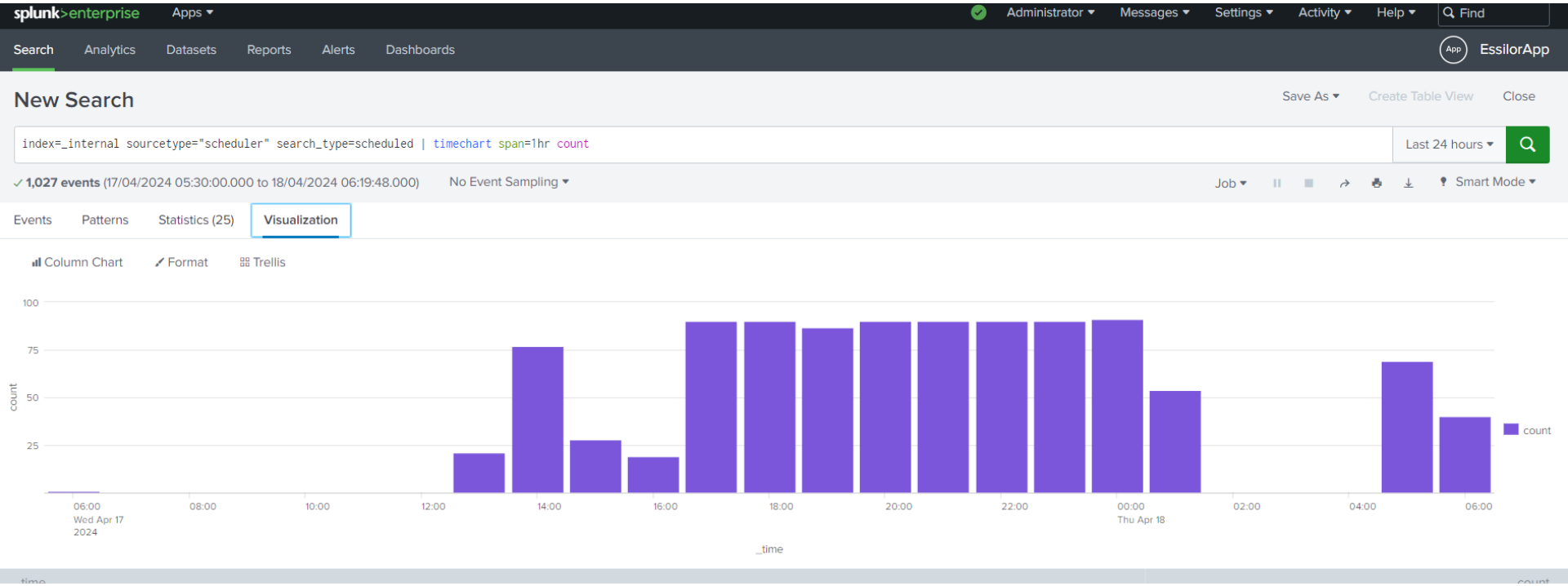


Splunk clean dispatch – too many queries



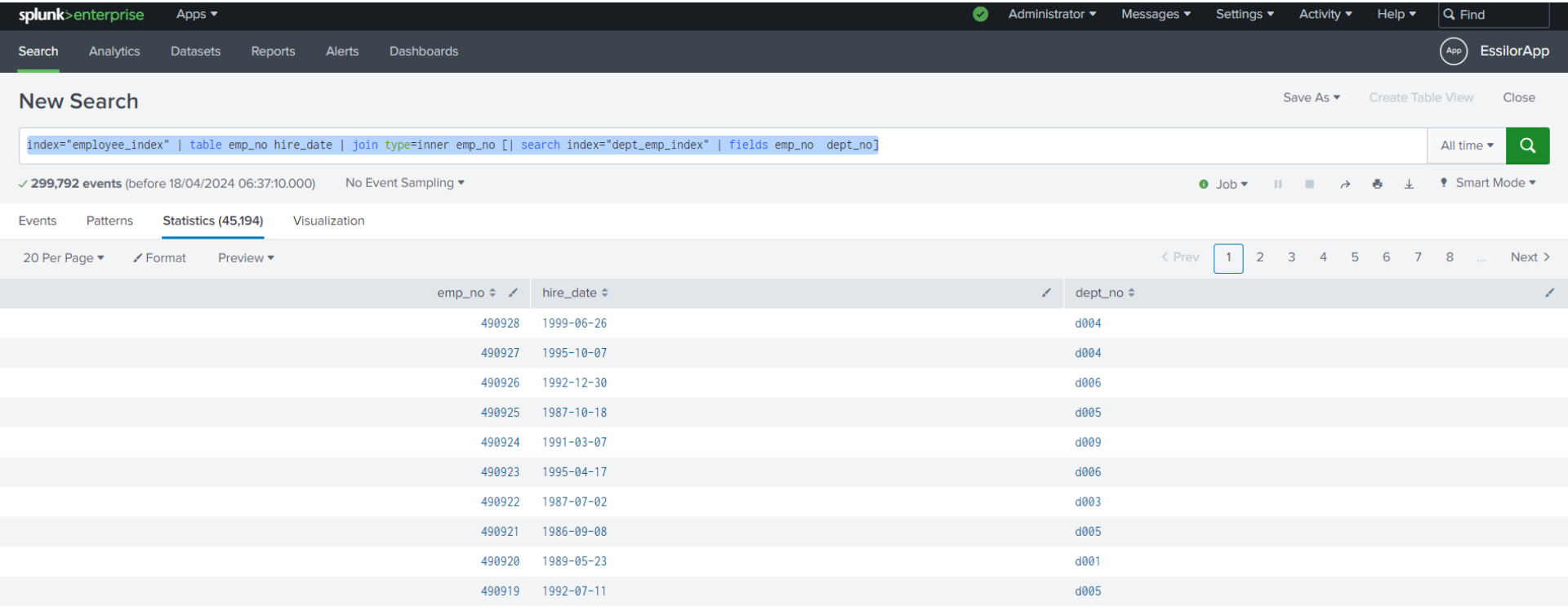
Find the number of saved searches run throughout the day.

index=_internal sourcetype="scheduler" search_type=scheduled | timechart span=1hr count



join

- index="employee_index" | table emp_no hire_date | join type=inner emp_no [| search index="dept_emp_index" | fields emp_no dept_no]



emp_no	hire_date	dept_no
490928	1999-06-26	d004
490927	1995-10-07	d004
490926	1992-12-30	d006
490925	1987-10-18	d005
490924	1991-03-07	d009
490923	1995-04-17	d006
490922	1987-07-02	d003
490921	1986-09-08	d005
490920	1989-05-23	d001
490919	1992-07-11	d005

Questions

Module Summary