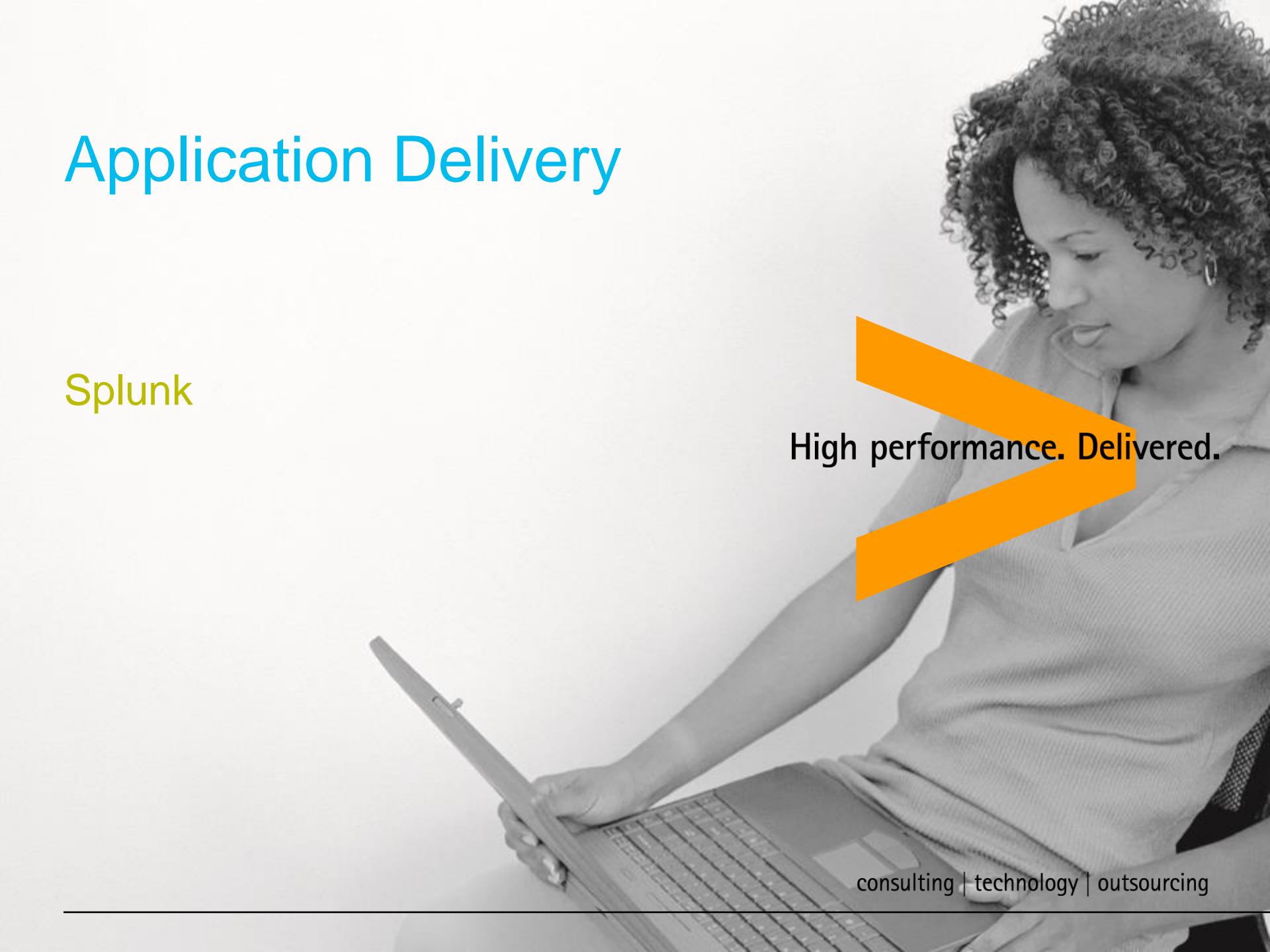


Application Delivery

Splunk

A black and white photograph of a woman with curly hair, wearing a light-colored shirt, sitting at a desk and working on a laptop. She is looking down at the screen. A large orange diagonal bar starts from the top right and extends towards the center of the image.

High performance. Delivered.

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



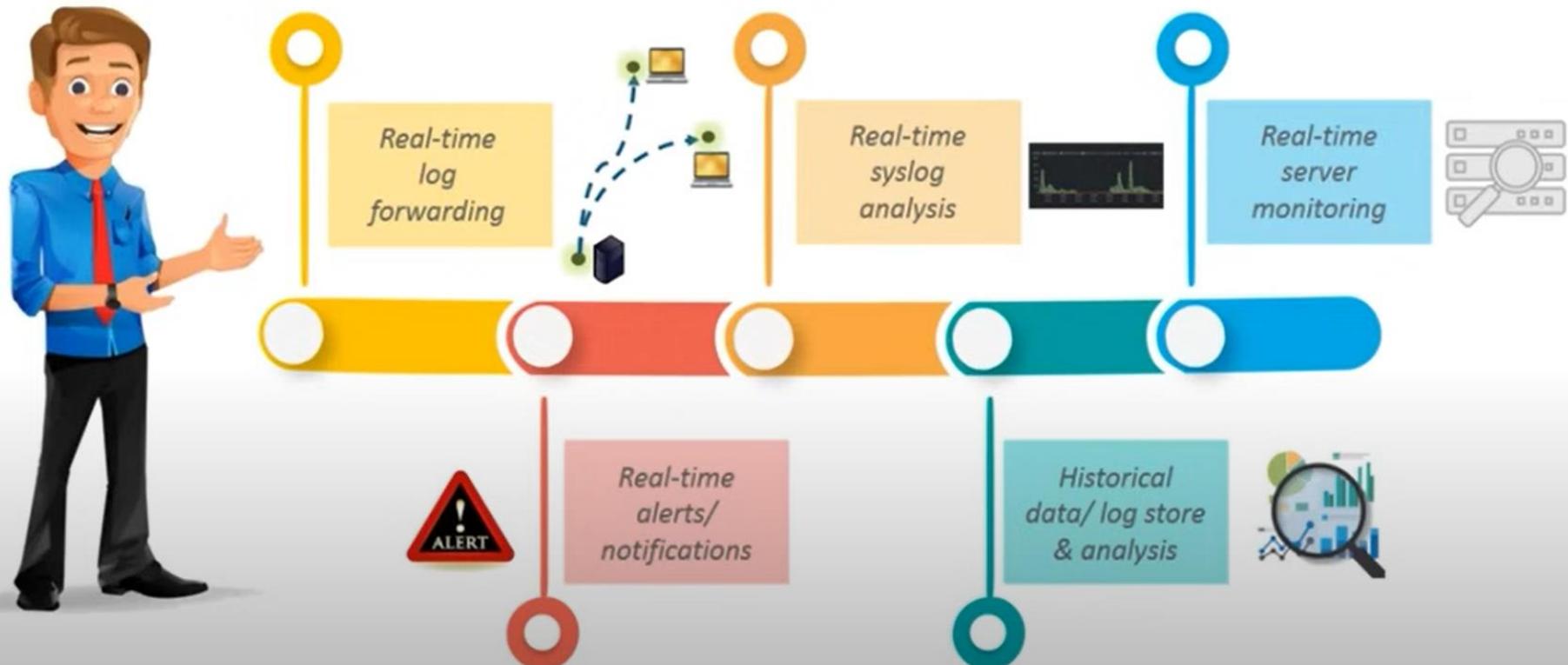
But 1000s of such logs
are generated every
minute

Check security
threats in real-time!!!

Analyze business
metrics in real-time!!!

Explore Logs – Solution- Splunk

Splunk is the ultimate log collection & analysis tool.



Explore Logs – Splunk - Usecases



Vodafone are using Splunk to manage big data and mapping Key Performance Indicator



New York Air Brake implemented Splunk and saved potentially \$1 Billion

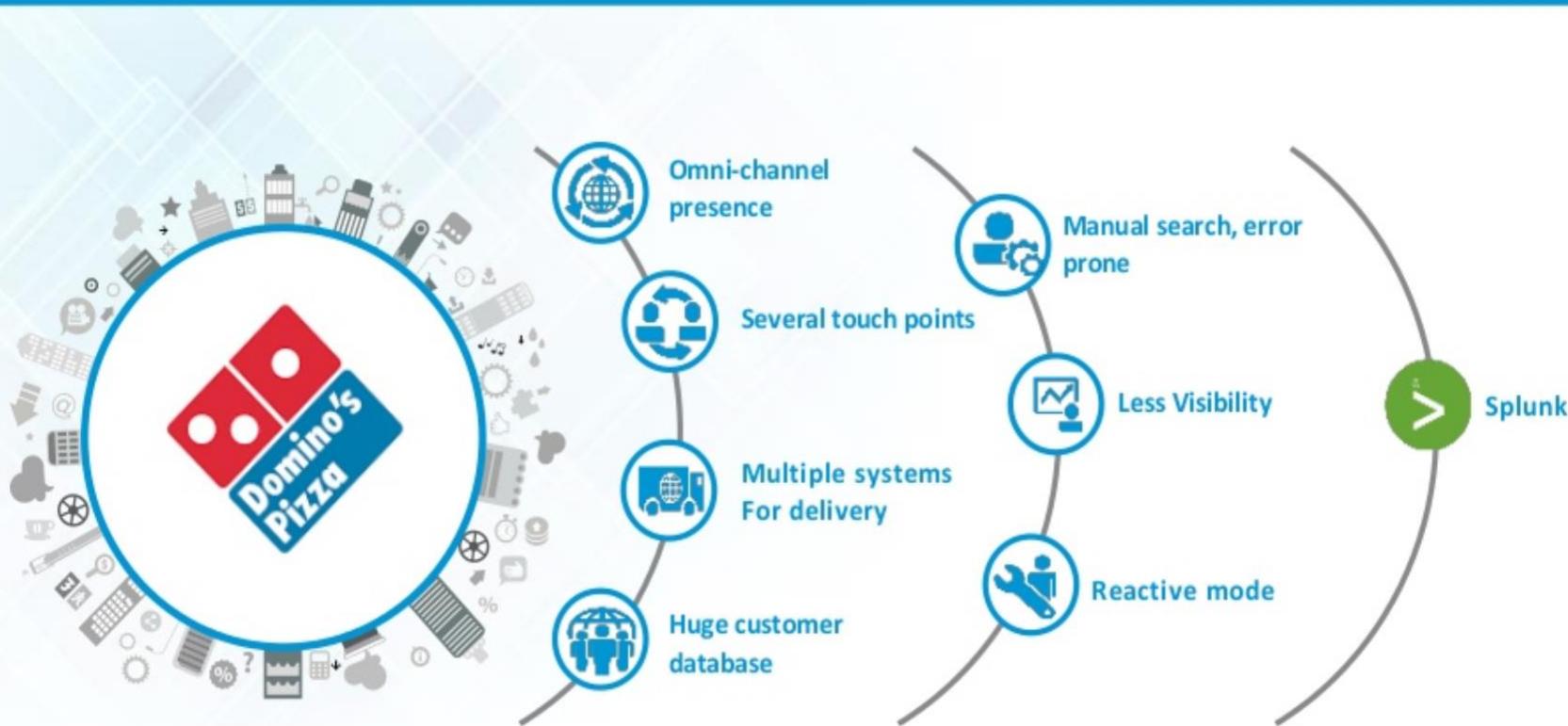


Domino's are implementing Splunk to gain insights on consumer behavior



ING Bank are using Splunk for faster troubleshooting of key apps & insight into customer behavior

Case: Domino's



Case: Domino's



Interactive map

- Shows all the orders coming from across US in real time
- Brought employee satisfaction



Real-time Feedback

- Employees constantly see what customers are saying
- Helped them understand customer expectations



Dashboard

- Used to keep score and set targets
- Compare performance with previous week



Payment Process

- Analysed the speed of different payment modes
- Determine error free payments modes



Promotional Support

- Track how various promotional offers are impacting in real-time
- Initially, determining the impact of promotions took almost a day



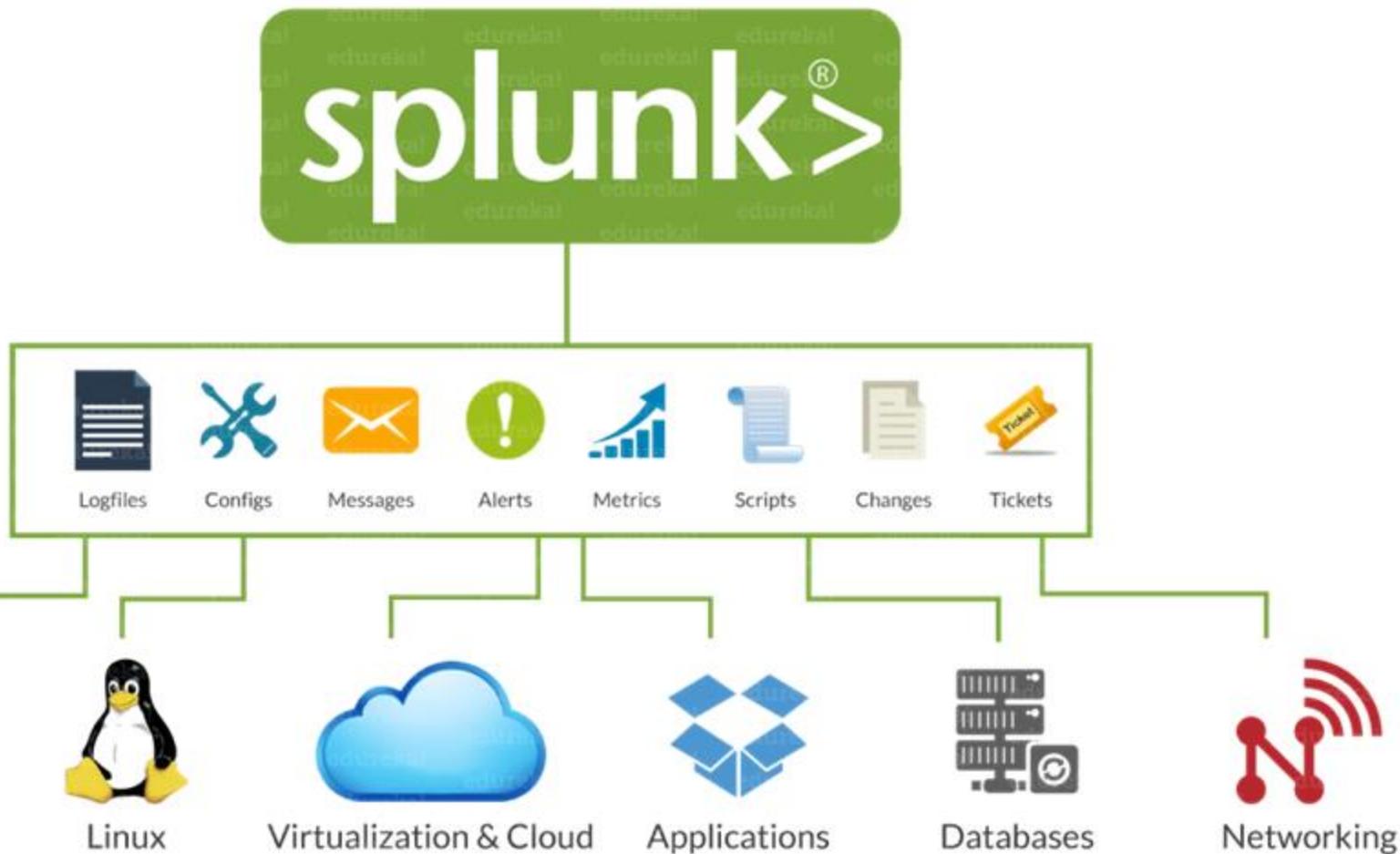
Performance Monitor

- Monitor the performance of Domino's in-house developed point of sales systems

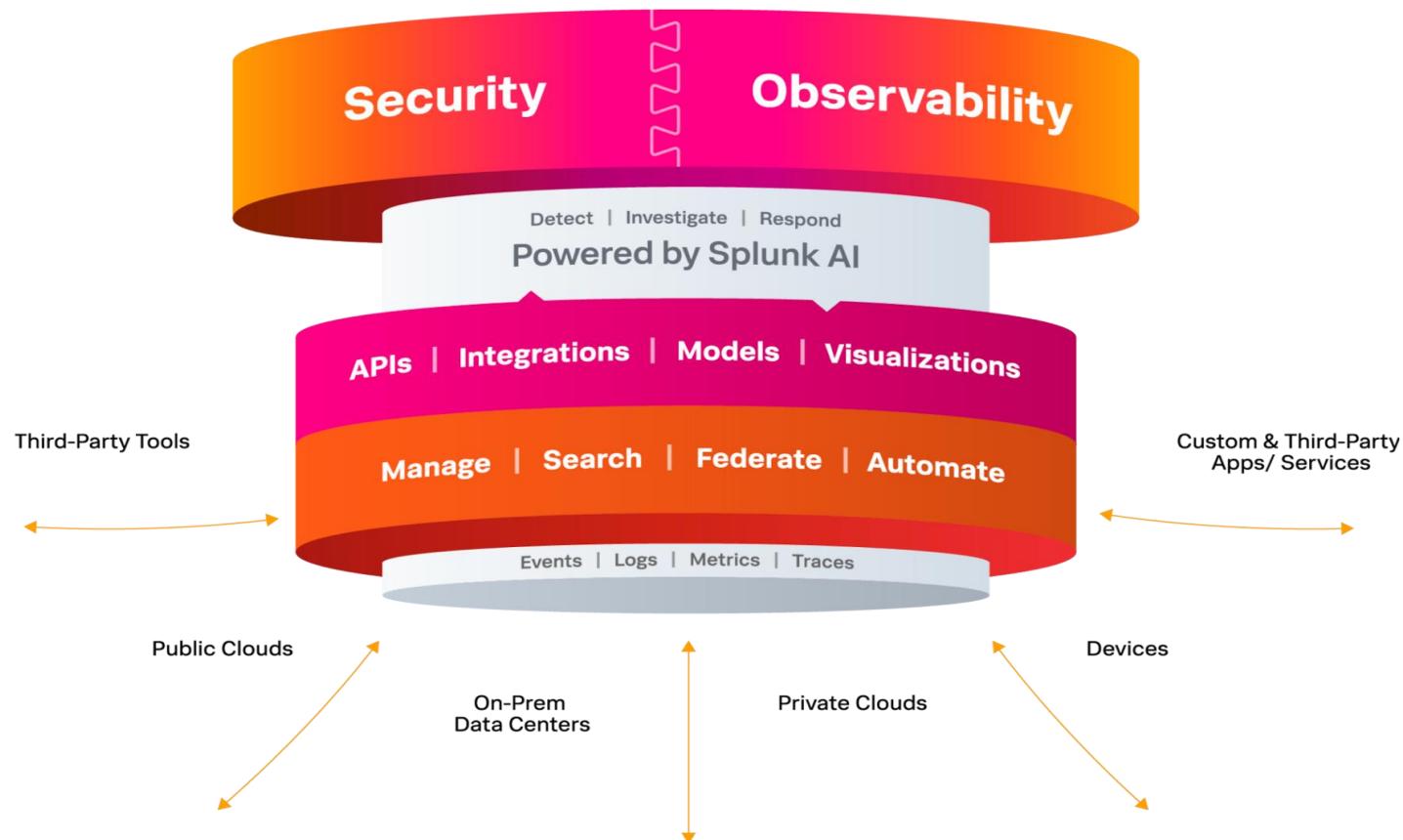
Splunk

- 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



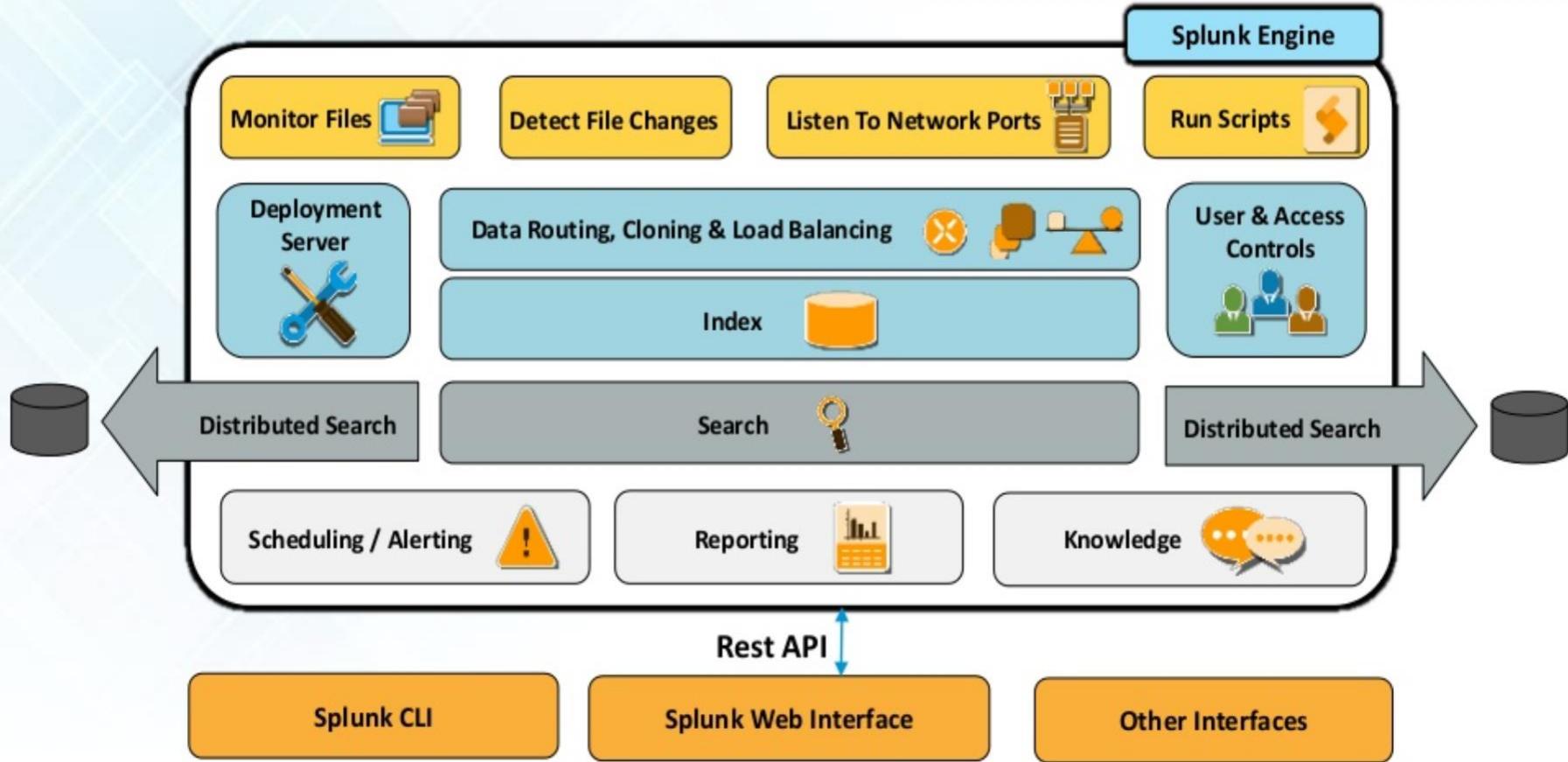
Splunk



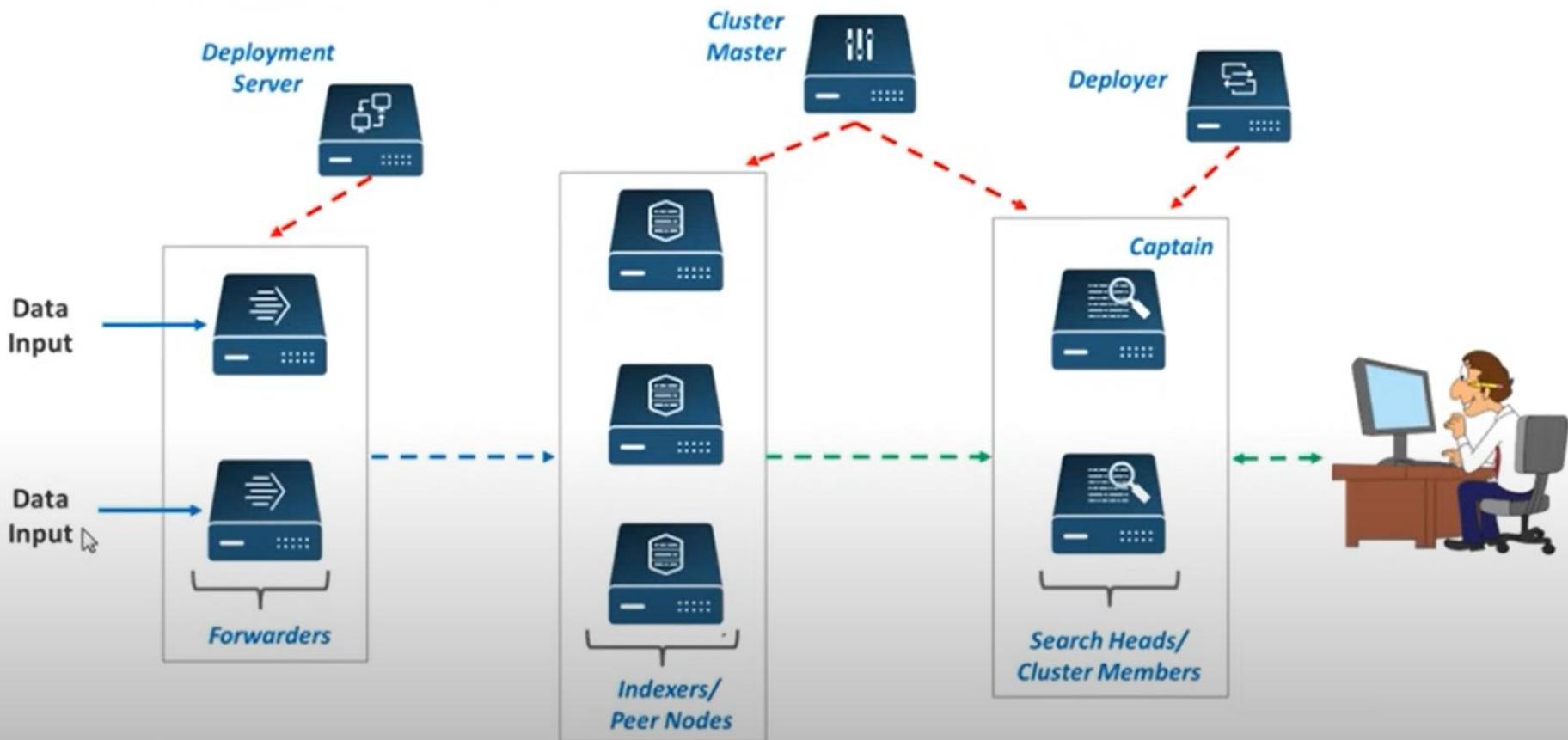
Splunk

- 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	✓	✗	✓

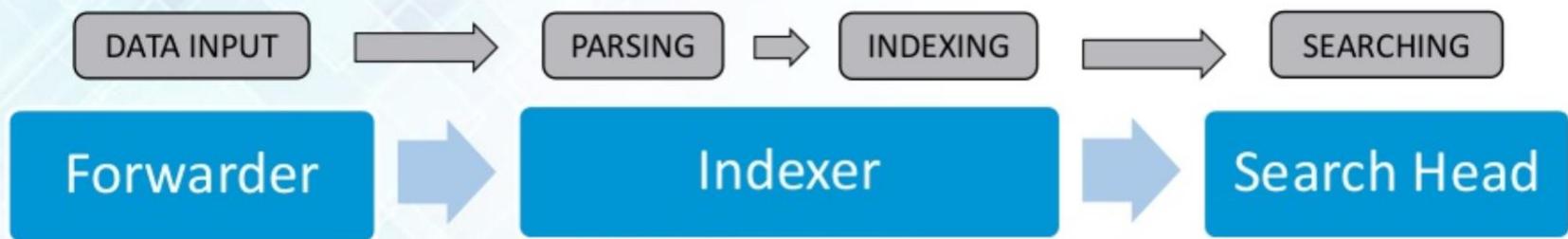
Installing Splunk

- **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

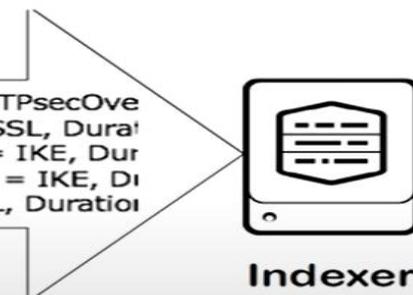


Search Head



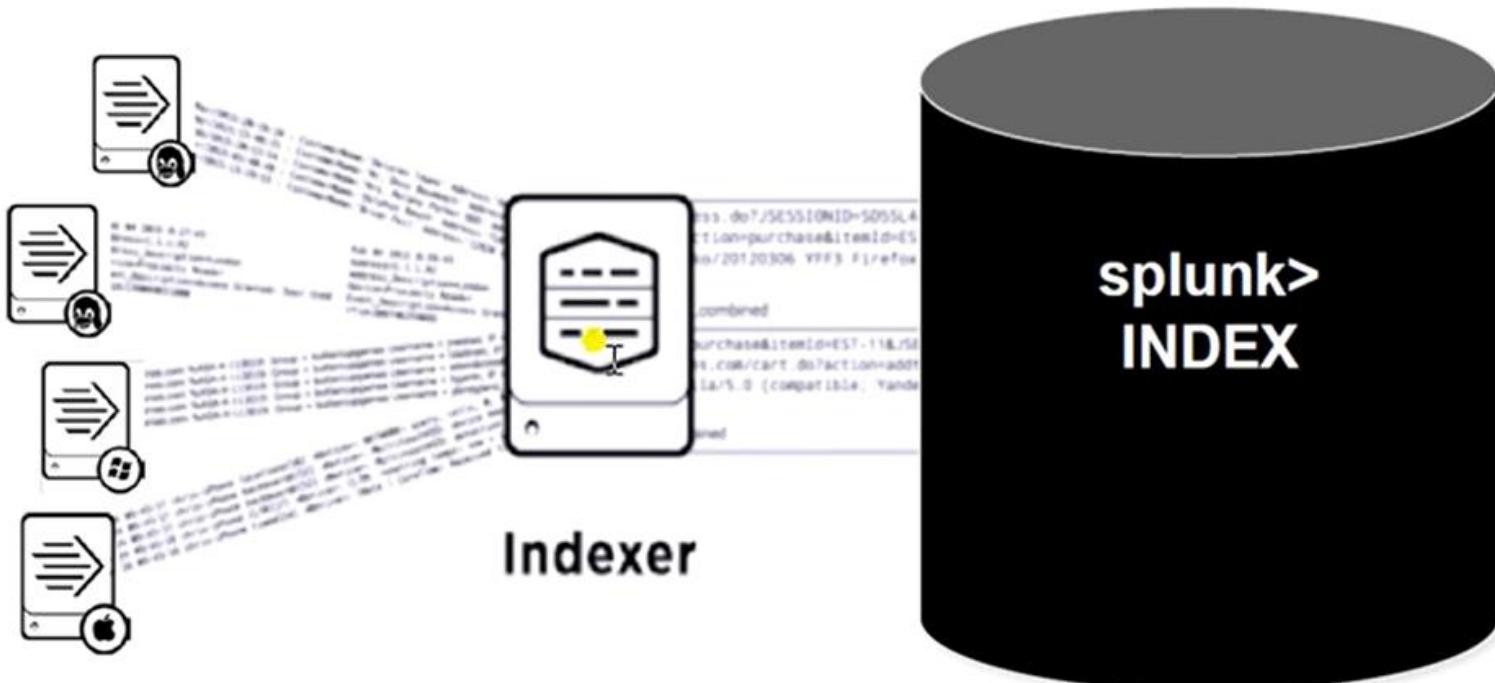
**Web Server
with Forwarder Instance**

IP = 10.3.10.6, Session disconnected. Session type = TPsecOve
IP = 10.1.10.216, Session connected. Session type = SSL, Durat
s, IP = 10.1.10.133, Session connected. Session type = IKE, Dur
i, IP = 10.3.10.18, Session disconnected. Session type = IKE, Di
= 10.1.10.211, Session connected. Session type = SSL, Duratio

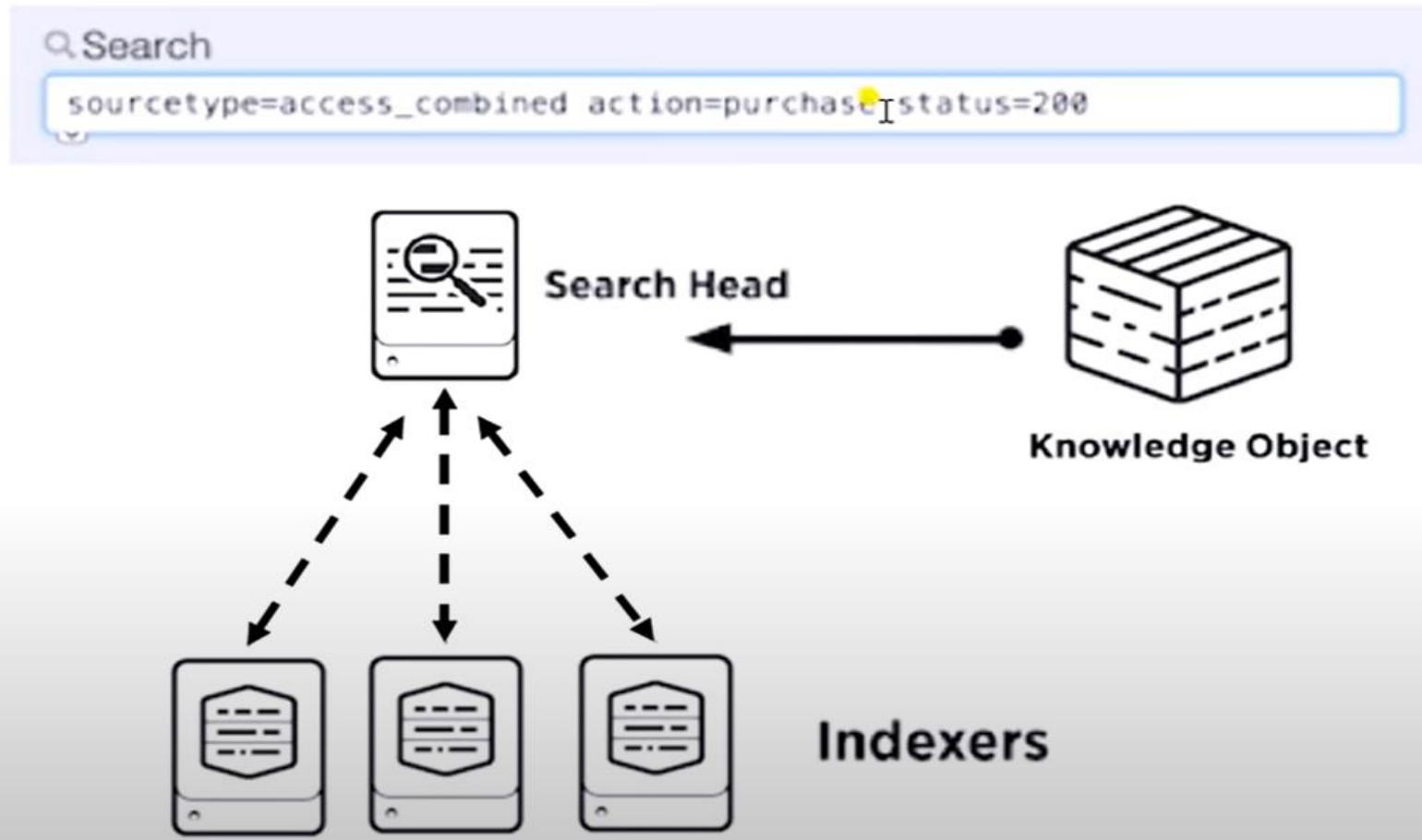


Indexer

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.

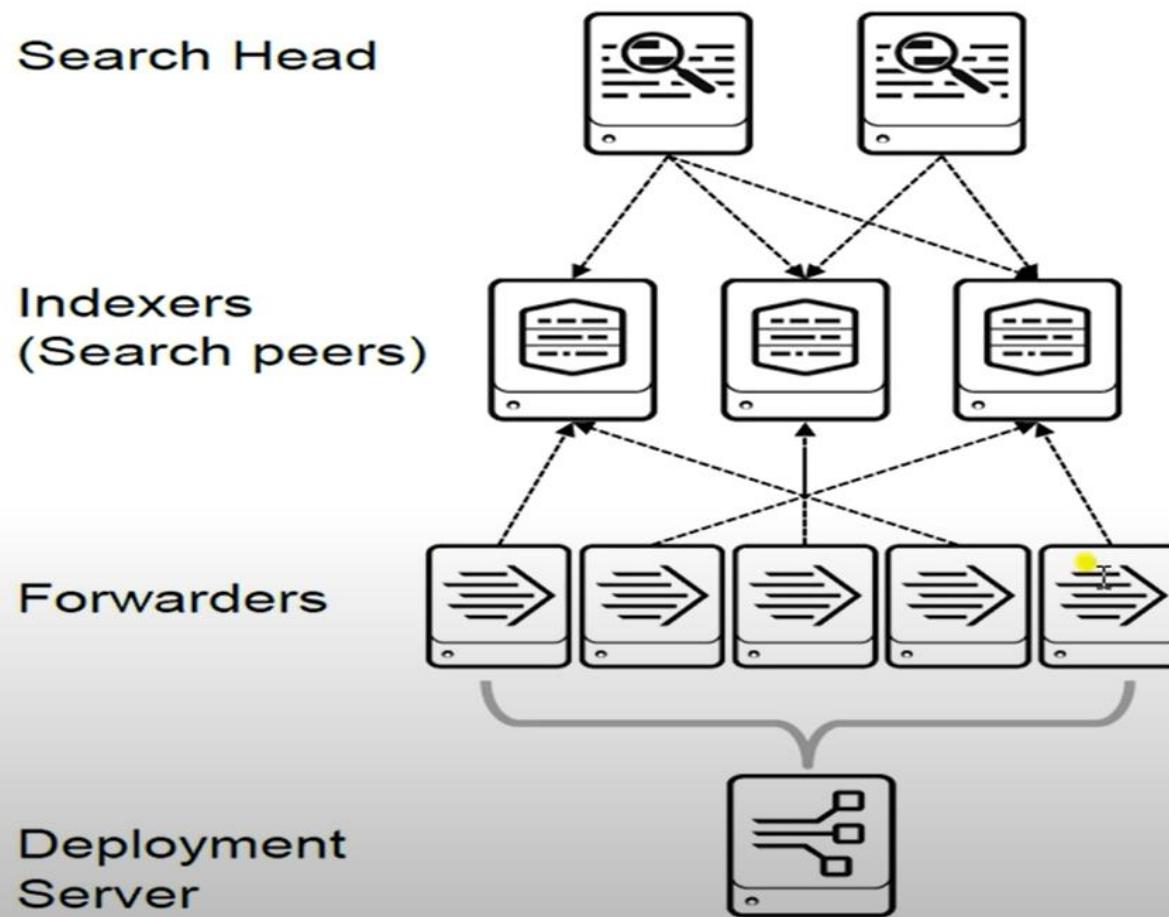
What are all the Splunk Knowledge Objects?

- 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?

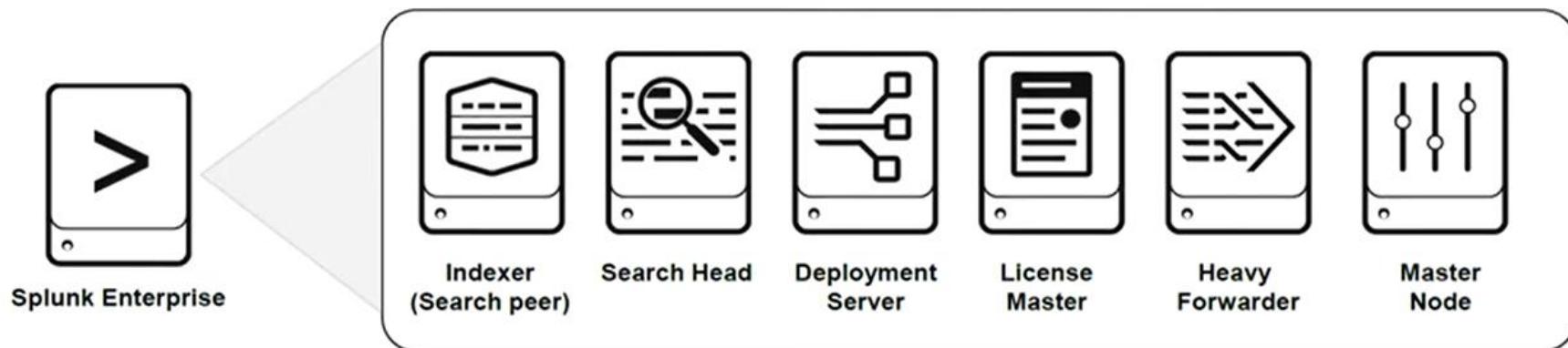
- Tags can help you centralize the naming conventions behind your data and knowledge objects.

Distributed Splunk Deployment

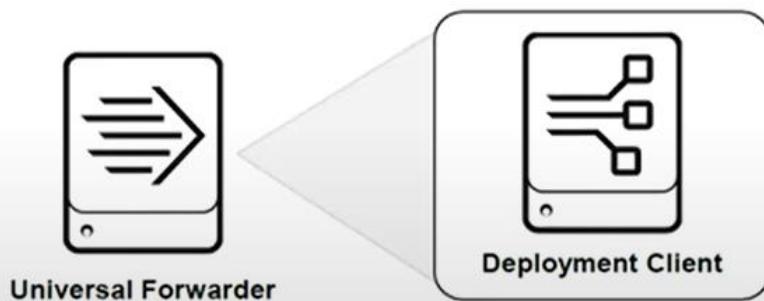


Enterprise Splunk Deployment

- Included in the Splunk Enterprise software package



- Included in the Universal Forwarder software package



Install Splunk on Windows



Products ▾ Solutions ▾ Why Splunk? ▾ Resources ▾

Support ▾



GET STARTED

Choose Your Download

Splunk Enterprise 9.2.1

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package



Windows



Linux



Mac OS

64-bit

Windows 10

Windows Server 2019, 2022

.msi

509.86 MB

Download Now

Copy wget link

More ▾

Install Splunk Universal Forwarder on Ubuntu



Products ▾ Solutions ▾ Why Splunk? ▾ Resources ▾

Support ▾

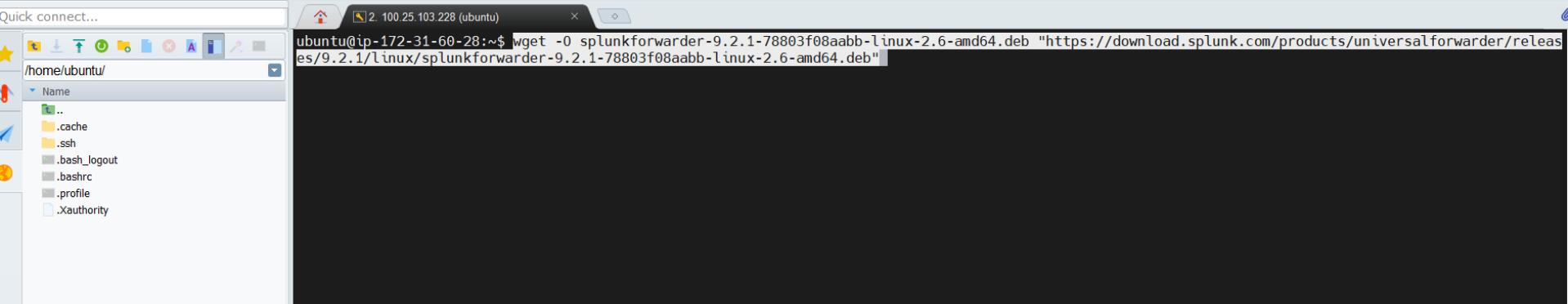
Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

Choose Your Installation Package

	Windows	Linux	Mac OS	Free BSD	Solaris	AIX		
ARM								
		4.14+, 5.4+ kernel Linux distributions with libc v2.21+, Graviton+ Servers 64-bit		.tgz	30.76 MB	Download Now	Copy wget link	More ▾
				.rpm	30.77 MB	Download Now	Copy wget link	More ▾
				.deb	21.15 MB	Download Now	Copy wget link	More ▾
64-bit		3.x+, 4.x+, or 5.x+ kernel Linux distributions		.deb	33.35 MB	Download Now	Copy wget link	More ▾
				.tgz	44.62 MB	Download Now		More ▾
				.rpm	44.46 MB	Download Now		More ▾
PPC E	3.x+, 4.x+, or 5.x+ kernel Linux							

Copied the command to Clipboard. Click here to select the entire command.
`wget -O splunkforwarder-9.2.1-78803f08aabb-linux-2.6-amd64.deb
"https://download.splunk.com/products/universalforwarder/releases/9.2.1/linux/splunkforwarder-9.2.1-78803f08aabb-linux-2.6-amd64.deb"`

Install Splunk Universal Forwarder on Ubuntu



```
ubuntu@ip-172-31-60-28:~$ wget -O splunkforwarder-9.2.1-78803f08aabb-linux-2.6-amd64.deb "https://download.splunk.com/products/universalforwarder/releases/9.2.1/linux/splunkforwarder-9.2.1-78803f08aabb-linux-2.6-amd64.deb"
```

```
ubuntu@ip-172-31-60-28:~$ wget -O splunkforwarder-9.2.1-78803f08aabb-linux-2.6-amd64.deb "https://download.splunk.com/products/universalforwarder/releases/9.2.1/linux/splunkforwarder-9.2.1-78803f08aabb-linux-2.6-amd64.deb"
--2024-04-12 14:11:56-- https://download.splunk.com/products/universalforwarder/releases/9.2.1/linux/splunkforwarder-9.2.1-78803f08aabb-linux-2.6-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 18.154.227.61, 18.154.227.97, 18.154.227.12, ...
Connecting to download.splunk.com (download.splunk.com)|18.154.227.61|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 34974336 (33M) [binary/octet-stream]
Saving to: 'splunkforwarder-9.2.1-78803f08aabb-linux-2.6-amd64.deb'

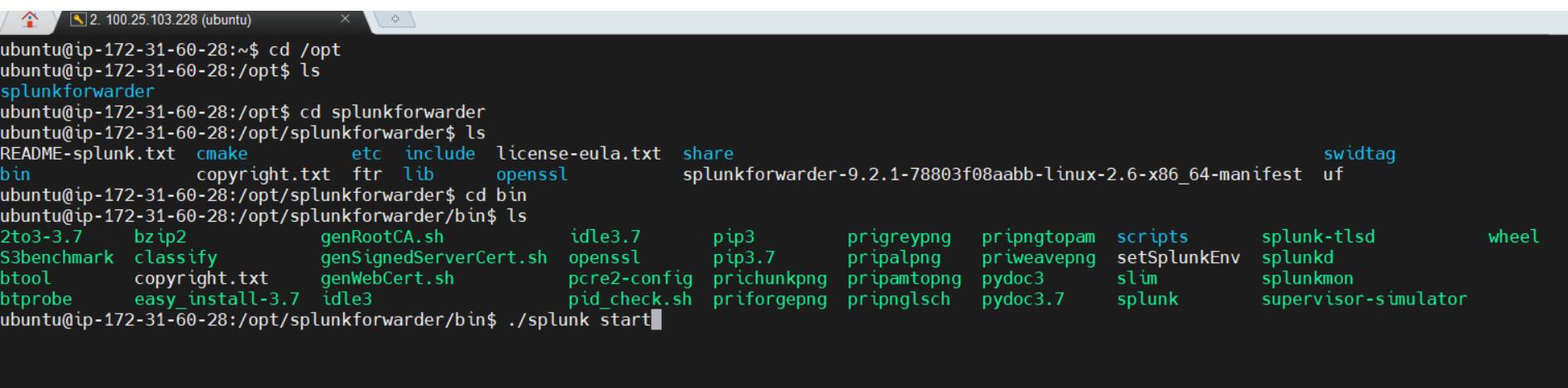
splunkforwarder-9.2.1-78803f08aabb-li 100%[=====] 33.35M  137MB/s   in 0.2s

2024-04-12 14:11:57 (137 MB/s) - 'splunkforwarder-9.2.1-78803f08aabb-linux-2.6-amd64.deb' saved [34974336/34974336]

ubuntu@ip-172-31-60-28:~$
```

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:~$ █
```



```
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      prialpalpng  priweavepng  setSplunkEnv  splunkd
btool       copyright.txt  genWebCert.sh  pcre2-config  prichunkpng  priamtopng   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

```
2. 100.25.103.228 (ubuntu) x +  
without limitation all improvements or modifications to our proprietary  
technology, and all Intellectual Property Rights therein.  
"Customer Materials" means the data, information, and materials you provide to  
us in connection with your use of the C&I Services.  
"Fees" means the fees that are applicable to the C&I Services, as identified  
in the Statement of Work.  
"Intellectual Property Rights" means all worldwide intellectual property  
rights, including copyrights and other rights in works of authorship; rights  
in trademarks, trade names, and other designations of source or origin; rights  
in trade secrets and confidential information; and patents and patent  
applications.  
"Personnel" means any employee, consultant, contractor, or subcontractor of  
Splunk.  
"Splunk Preexisting IP" means, with respect to any C&I Services Materials, all  
associated Splunk technology and all Intellectual Property Rights created or  
acquired: (a) prior to the date of the Statement of Work that includes such  
C&I Services Materials, or (b) after the date of such Statement of Work but  
independently of the C&I Services provided under such Statement of Work.  
"Statement of Work" means the statements of work and/or any and all applicable  
Orders, that describe the specific services to be performed by Splunk,  
including any materials and deliverables to be delivered by Splunk.  
Do you agree with this license? [y/n]:  
Do you agree with this license? [y/n]: y  
  
This appears to be your first time running this version of Splunk.  
  
Splunk software must create an administrator account during startup. Otherwise, you cannot log in.  
Create credentials for the administrator account.  
Characters do not appear on the screen when you type in credentials.  
  
Please enter an administrator username: eswaribala  
Password must contain at least:  
* 8 total printable ASCII character(s).  
Please enter a new password: █
```

Install Splunk Universal Forwarder on Ubuntu

```
2. 100.25.103.228 (ubuntu) x +  
Characters do not appear on the screen when you type in credentials.  
Please enter an administrator username: eswaribala  
Password must contain at least:  
    * 8 total printable ASCII character(s).  
Please enter a new password:  
Please confirm new password:  
Creating unit file...  
Important: splunk will start under systemd as user: splunkfwd  
The unit file has been created.  
  
Splunk> Finding your faults, just like mom.  
  
Checking prerequisites...  
  Checking mgmt port [8089]: open  
    Creating: /opt/splunkforwarder/var/lib/splunk  
    Creating: /opt/splunkforwarder/var/run/splunk  
    Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n  
    Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css  
    Creating: /opt/splunkforwarder/var/run/splunk/upload  
    Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry  
    Creating: /opt/splunkforwarder/var/run/splunk/search_log  
    Creating: /opt/splunkforwarder/var/spool/splunk  
    Creating: /opt/splunkforwarder/var/spool/dirmoncache  
    Creating: /opt/splunkforwarder/var/lib/splunk/authDb  
    Creating: /opt/splunkforwarder/var/lib/splunk/hashDb  
New certs have been generated in '/opt/splunkforwarder/etc/auth'.  
  Checking conf files for problems...  
  Done  
  Checking default conf files for edits...  
  Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.2.1-78803f08aabb-linux-2.6-x86_64-manifest'  
  All installed files intact.  
  Done  
All preliminary checks passed.  
  
Starting splunk server daemon (splunkd)...  
Done  
ubuntu@ip-172-31-60-28:/opt/splunkforwarder/bin$
```

Splunk Enterprise for Ubuntu

The screenshot shows the Splunk website's download section for Ubuntu. At the top, there's a navigation bar with links for Products, Solutions, Why Splunk?, Resources, Support, and a search icon. Below the navigation is a red banner with the text "GET STARTED" and "Choose Your Download". The main content area is titled "Splunk Enterprise 9.2.1" and describes it as indexing 500 MB/Day. It offers a 60-day trial or purchase of a perpetual free license or enterprise-scale deployments. Below this, there's a heading "Choose Your Installation Package" with tabs for Windows, Linux (which is selected), and Mac OS. Under the Linux tab, there are three download options: ".deb" (520.37 MB), ".tgz" (679.42 MB), and ".rpm" (679.24 MB). Each option has a "Download Now" button and a "Copy wget link" button. A tooltip for the ".deb" link shows the command: "Copied the command to Clipboard. Click here to select the entire command." The command is: `wget -O splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb "https://download.splunk.com/products/splunk/releases/9.2.1/linux/splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb"`. At the bottom of the page, there are links for "Release Notes" and "System Requirements".

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

```
C:\Program Files\Splunk\bin>splunk status
Splunkd: Running (pid 5304)

C:\Program Files\Splunk\bin>splunk list app
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
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
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
SplunkLightForwarder       UNCONFIGURED    DISABLED      INVISIBLE

C:\Program Files\Splunk\bin>
```

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](#)



Amazon Web Services



Google Cloud Platform



Microsoft Azure



Kubernetes



OpenShift



Kafka



Cassandra



mongoDB



Nginx

Splunk Users

Persona	Industry Role	Activities
Administrator	network engineer, system administrator	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Integrates data and functionality of applications with Splunk Enterprise.Builds Splunk apps and add-ons with custom dashboards and data visualizations.

Splunk Handson

splunk>enterprise

Administrator 1 Messages Settings Activity Help Find

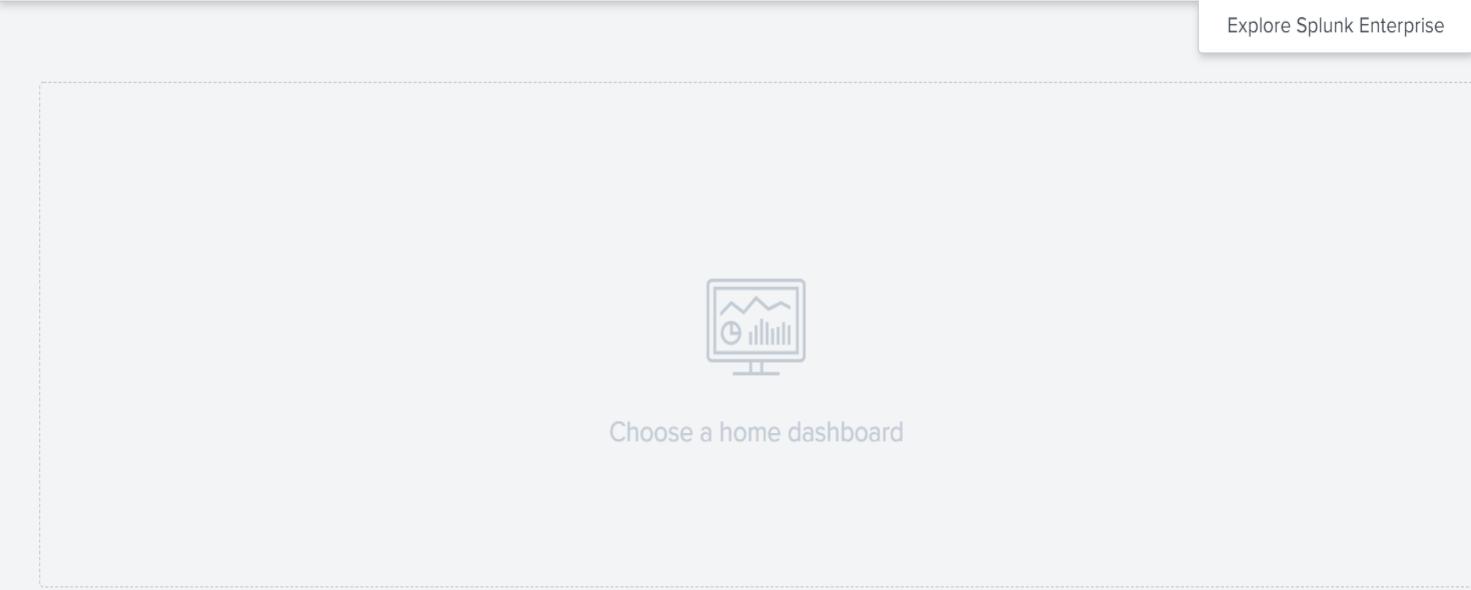
Explore Splunk Enterprise

Apps

> Search & Reporting

+ Find More Apps

Choose a home dashboard



The screenshot shows the Splunk Enterprise web interface. At the top, there's a dark header bar with the 'splunk>enterprise' logo, user information ('Administrator'), and navigation links ('Messages', 'Settings', 'Activity', 'Help', 'Find'). A search bar is on the far right. Below the header is a sidebar on the left labeled 'Apps' with a gear icon. It lists 'Search & Reporting' with a green 'greater than' icon and a link to '+ Find More Apps'. The main content area is a large white space with a dashed border, containing a central icon of a computer monitor displaying a chart, and the text 'Choose a home dashboard' below it. In the top right corner of the main area, there's a small callout box with the text 'Explore Splunk Enterprise'.

Splunk Handson

General settings

Server settings » General settings

Splunk server name * DESKTOP-B08BAAN

Installation path C:\Program Files\Splunk

Management port * 8089
Port that Splunk Web uses to communicate with the splunkd process. This port is also used for distributed search.

SSO Trusted IP

The IP address to accept trusted logins from. Only set this if you are using single sign-on (SSO) with a proxy server for authentication.

Splunk Web

Run Splunk Web Yes No

Enable SSL (HTTPS) in Splunk Web? Yes No

Web port * 8000

App server ports 8065
Port number(s) for the python-based application server to listen on. Use comma-separated list to specify more than one port number.

Add Data to Splunk

Follow guides for onboarding popular data sources



Cloud computing

Get your cloud computing data in to the Splunk platform.

10 data sources



Networking

Get your networking data in to the Splunk platform.

2 data sources



Operating System

Get your operating system data in to the Splunk platform.

1 data source



Security

Get your security data in to the Splunk platform.

3 data sources

4 data sources in total

Add Data to Splunk



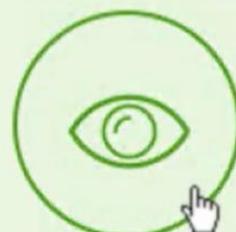
upload

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

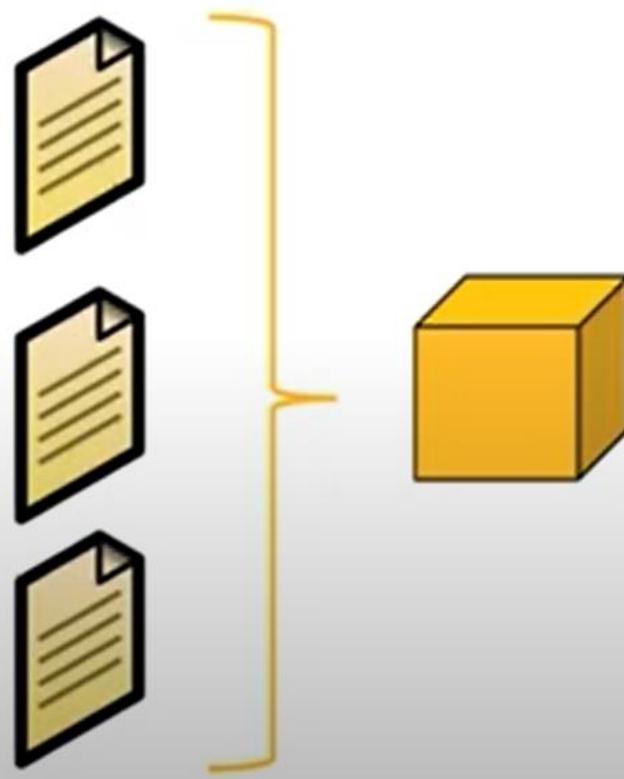


- Apps extend Splunk's functionality
- Apps can be created by third parties, individuals, or Splunk
- Apps that are built by Splunk carry the "Splunk Built" logo
- Apps that are certified by Splunk carry the "Splunk Certified" logo

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

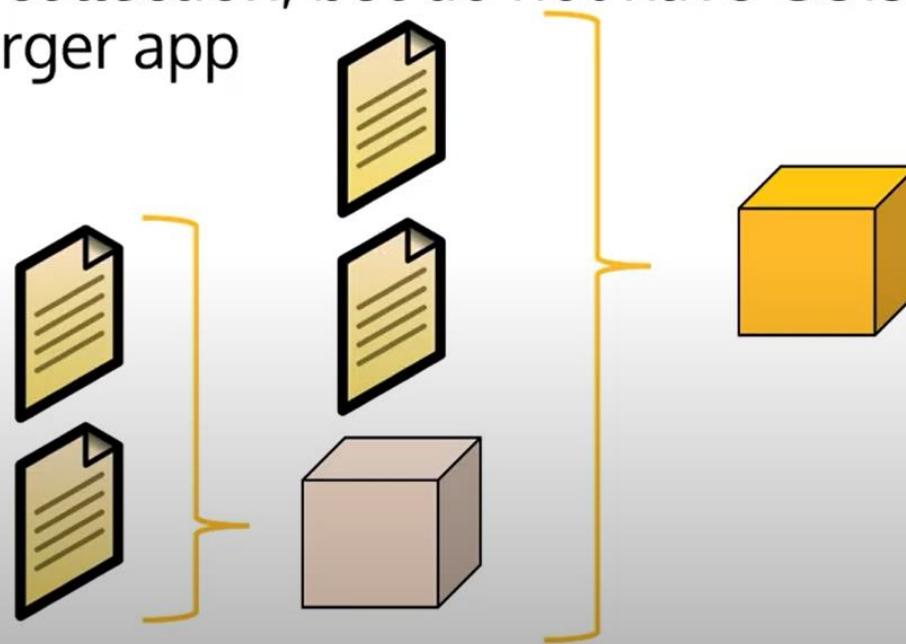
The Splunk Apps

- 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 screenshot shows the Splunk Enterprise App Store interface. At the top, there is a dark header bar with the text "splunk>enterprise" on the left and "Apps ▾" on the right. Below the header, the word "Apps" is centered above a search bar. To the right of the search bar is a "Manage" button with a gear icon. The search bar contains the placeholder text "Search apps by name..." and features a magnifying glass icon on its right side. Below the search bar, three app cards are displayed: "Search & Reporting" (represented by a green square with a white right-pointing arrow), "Splunk Secure Gateway" (represented by a teal square with a white smartphone icon), and "Upgrade Readiness App" (represented by a grey square with a white icon containing a checkmark and a gear). At the bottom of the list, there is a link "Find more apps" followed by a blue "↗" icon.

splunk>enterprise Apps ▾

Apps Manage

Search apps by name...

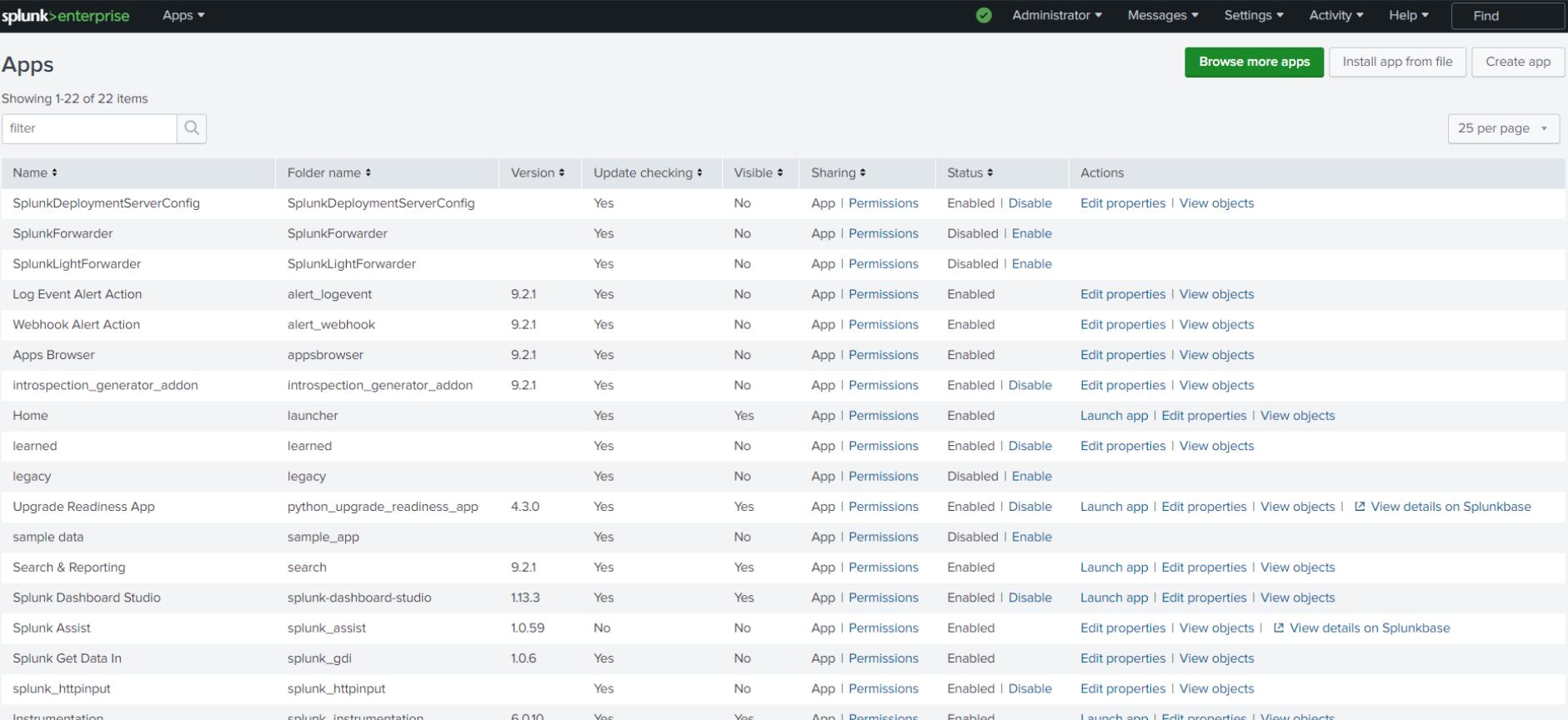
Search & Reporting

Splunk Secure Gateway

Upgrade Readiness App

Find more apps ↗

The Splunk Apps



The screenshot shows the Splunk Apps interface. At the top, there's a navigation bar with 'splunk>enterprise' and 'Apps'. On the right of the nav bar are links for 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' search bar. Below the nav bar, the word 'Apps' is displayed in a large font. To the right of 'Apps' are three buttons: 'Browse more apps' (green), 'Install app from file' (white), and 'Create app' (white). A message 'Showing 1-22 of 22 items' is above a search bar with a 'filter' input and a magnifying glass icon. To the right of the search bar is a dropdown for '25 per page'. The main area is a table with 22 rows, each representing an app. The columns are: Name, Folder name, Version, Update checking, Visible, Sharing, Status, and Actions. The 'Actions' column contains links like 'Edit properties' and 'View objects'.

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

splunkbase™ Collections Apps

Get more out of Splunk
with applications

Q Dash

X

 Dashboard Monitoring

 Dashboard Assistant

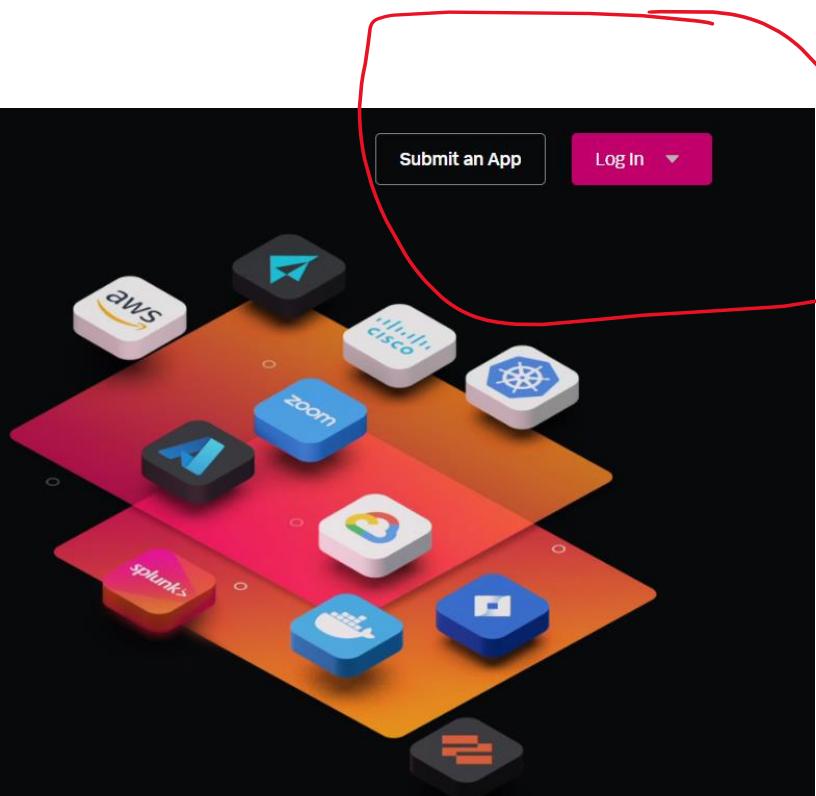
 Dashboard PDF Exporter

 Dashboard use cases for TA-LDAP

 Dashboard and Jobs Monitor

Submit an App

Log In ▾



The Splunk Search For Apps

splunk>
a CISCO company

Log into your Splunk account

Email or Username

Password
 ④

Log In

Forgot your [Password or username?](#)
Need to [sign up](#) for a Splunk account?



Don't miss .conf24. Get to Las Vegas June 11-14! ›

Immerse yourself in all things Splunk—learning, ponies and lots of genuinely fun networking.

The Splunk Search For Apps

Welcome to the new Splunkbase! To return to the old Splunkbase, [click here](#).

Accept License Agreements

Splunk General Terms [\[link\]](#)

Splunk Websites Terms and Conditions of Use. [\[link\]](#)

I have read the terms and conditions of this license and agree to be bound by them.

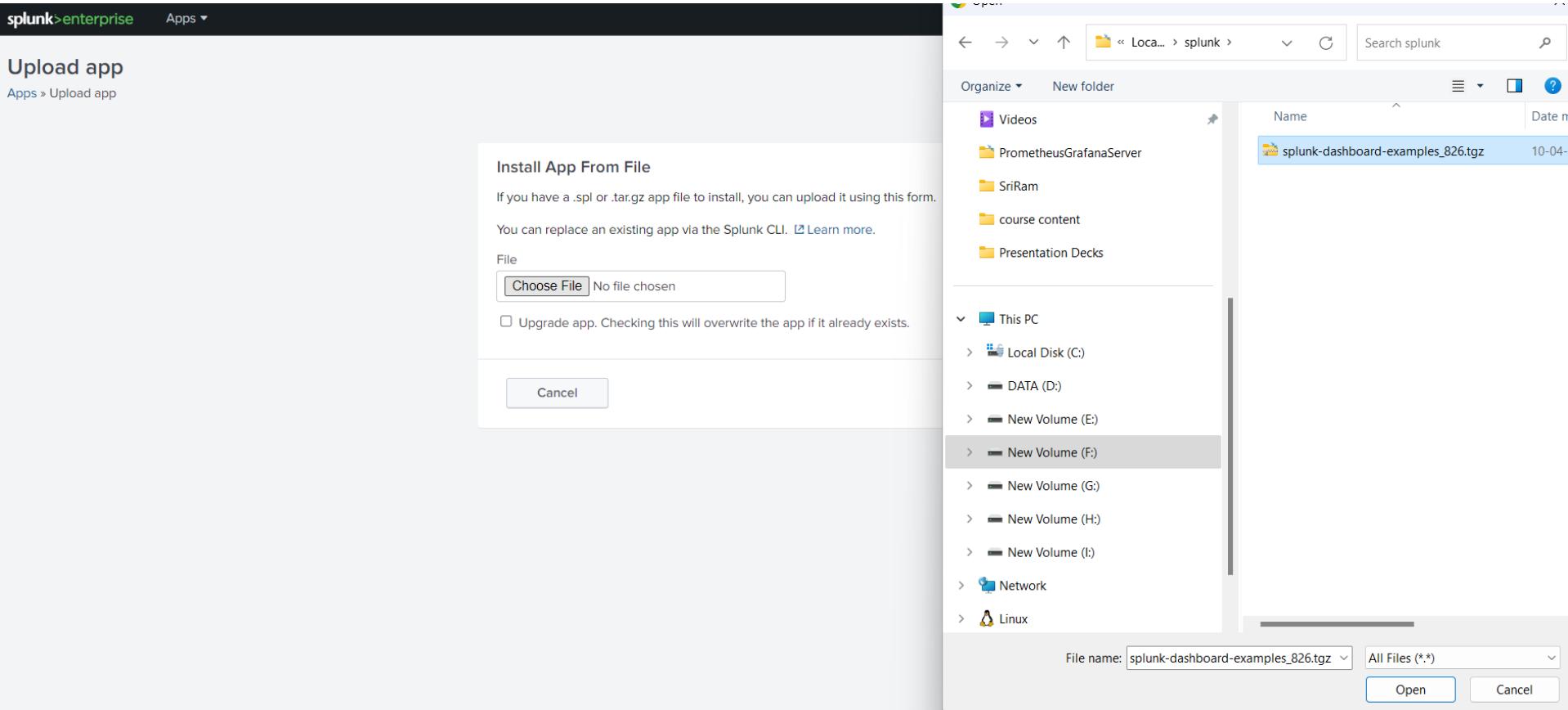
I consent to sharing my contact information with Splunk so I can receive more information about this app from Splunk.

[Cancel](#) [Agree to Download](#)

Splunk Dashboard
The Splunk Dashboard app provides a central location for monitoring your Splunk environment. It includes dashboards for system health, search activity, and user authentication. The app is available in SimpleXML and REST API formats.
Built by [Splunk Inc.](#)

[Download](#)

The Splunk Search For Apps



The Splunk Search For Apps

newly installed app

The screenshot shows the Splunk Enterprise interface with a red annotation. A red circle highlights the 'Search apps by name...' input field and the magnifying glass icon. A red bracket groups the first two items in the 'Common tasks' section: 'Add data' and 'Search your data'. Above the 'Common tasks' section, a red curly brace groups the 'Search & Reporting' and 'Splunk Dashboard Examples' items under the heading 'Common tasks'.

splunk>enterprise Apps **Administrator** Messages Settings

Apps Manage

Hello, Administrator

Quick links Dashboard Recently viewed Created by you Shared with you

Search apps by name... Manage

Search & Reporting

Splunk Dashboard Examples

Common tasks

Add data Add data from a variety of common sources.

Search your data Turn data into doing with Splunk search.

Visualize your data Create dashboards that work for your data.

Add team members Add your team members to Splunk platform.

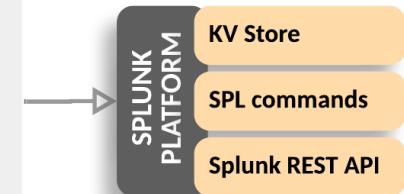
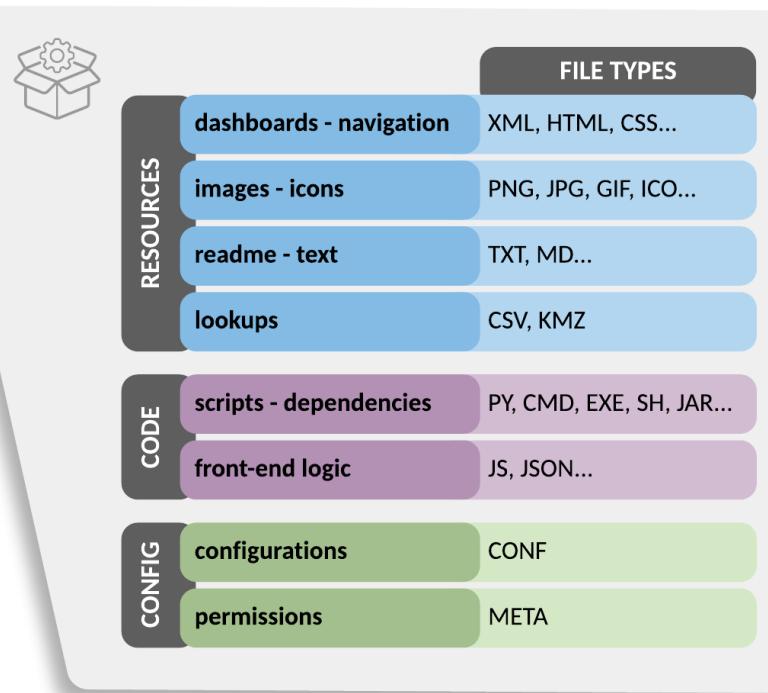
Manage permissions Control who has access with roles.

Configure mobile devices Login or manage mobile devices using Splunk Secure Gateway.

Find more apps [Find more apps](#)

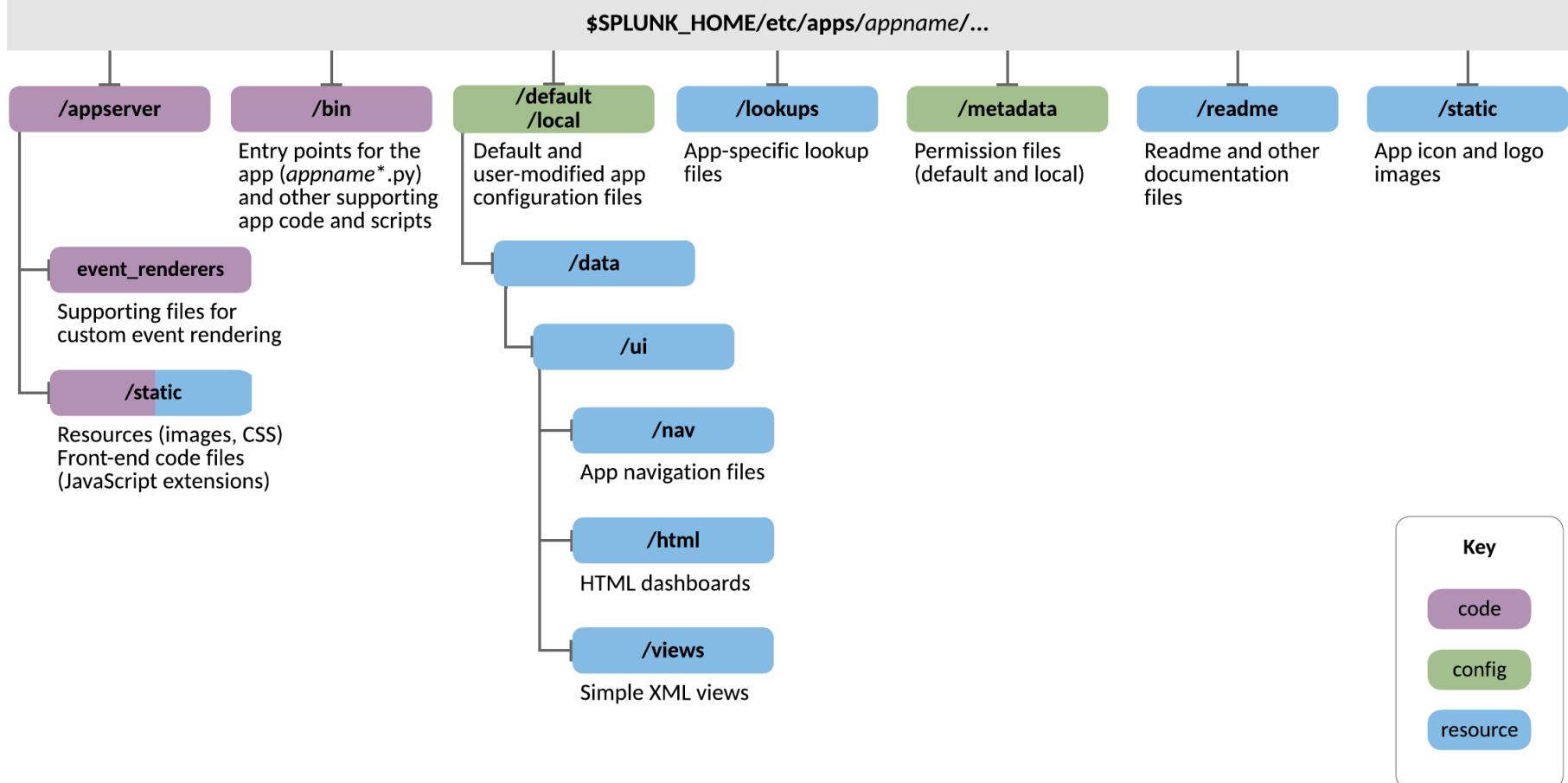
The Splunk Apps

Splunk app



Anatomy of a Splunk app

The Directory Structure of Splunk App



Key

code

config

resource

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

The screenshot shows the Splunk web interface with a dark theme. At the top is a navigation bar with links for Administrator, Messages, Settings, Activity, Help, and a search bar labeled "Find". Below the navigation bar is a sidebar containing several sections:

- Add Data**: Contains links for Searches, reports, and alerts; Data models; Event types; Tags; Fields; Lookups; User interface; Alert actions; Advanced search (which is circled in red); and All configurations.
- Monitoring Console**: Contains links for Server settings; Server controls; Health report manager; Instrumentation; Licensing; Workload management; and Mobile settings.
- KNOWLEDGE**: Contains links for Searches, reports, and alerts; Data models; Event types; Tags; Fields; Lookups; User interface; Alert actions; Advanced search; and All configurations.
- DATA**: Contains links for Data inputs; Forwarding and receiving; Indexes; Report acceleration summaries; Source types; and Ingest actions.
- DISTRIBUTED ENVIRONMENT**: Contains links for Indexer clustering; Forwarder management; Federated search; and Distributed search.
- SYSTEM**: Contains links for Roles; Users; Tokens; Password management; and Authentication methods.
- USERS AND AUTHENTICATION**: Contains links for Roles; Users; Tokens; Password management; and Authentication methods.

On the left side of the main content area, there are two cards:

- Table Element**: A card with a title and a brief description: "Create a simple table using the dashboard editor." It includes a code snippet:

```
sourceType: 0
1 eventgen.log
2 splunkd.access
3 splunkd
4 splunk_web.access
5 scheduler
6 splunk_web.service
7 splunkd.stderr
```
- Events Viewer Element**: A card with a title and a brief description: "Visualize the raw data index in Splunk Enterprise, with field metadata." It includes a code snippet:

```
i Event
▶ 2013-09-24 10:44:14,325 INFO
- user=admin action=login st
session=cdd562a68e829f5a132
useragent="Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.1 Icinga/1.8.0 Safari/537.36" clientip=127.0.0.1
▶ 2013-09-24 10:33:54,768 INFO
- user=admin action=login st
session=f254f0b896a40bb8efc8
useragent="Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.1 Icinga/1.8.0 Safari/537.36" clientip=127.0.0.1
```

At the bottom center of the sidebar, there is a footer note: "HTML and CSS are our tools. Mauris a ante."

App permissions and deploying

The screenshot shows the Splunk Enterprise interface for managing app configurations. The top navigation bar includes 'splunk enterprise', 'Apps ▾', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' search bar. Below the navigation is a search bar with filters: 'Configuration Source' (set to 'Created in the App'), 'Owner' (set to 'Any'), and a 'filter' input field. To the right of the search bar are buttons for 'Reassign Knowledge Objects' and '25 per page'. The main content area is titled 'All configurations' and displays 108 items. The table has columns: 'Name', 'Config type', 'Owner', 'App', 'Sharing', and 'Status'. A red arrow points to the 'Sharing' column header. The data rows show various app names like 'basics', 'condition_match', etc., with their respective details.

Name	Config type	Owner	App	Sharing	Status
basics	views	No owner	simple_xml_examples	App Permissions	Enabled
condition_match	views	No owner	simple_xml_examples	App Permissions	Enabled
contents	views	No owner	simple_xml_examples	App Permissions	Enabled
craigslist_housing	transforms-lookup	No owner	simple_xml_examples	Global Permissions	Enabled Disable
custom_app_token	views	No owner	simple_xml_examples	App Permissions	Enabled
custom_decorations	views	No owner	simple_xml_examples	App Permissions	Enabled
custom_drilldown_url_field	views	No owner	simple_xml_examples	App Permissions	Enabled
custom_event_tokens	views	No owner	simple_xml_examples	App Permissions	Enabled
custom_init_tokens	views	No owner	simple_xml_examples	App Permissions	Enabled
custom_layout_dark	views	No owner	simple_xml_examples	App Permissions	Enabled
custom_layout_overlay_single	views	No owner	simple_xml_examples	App Permissions	Enabled
custom_layout_panel_width	views	No owner	simple_xml_examples	App Permissions	Enabled
custom_table_cell_highlighting	views	No owner	simple_xml_examples	App Permissions	Enabled
custom_table_column_width	views	No owner	simple_xml_examples	App Permissions	Enabled
custom_table_data_bar	views	No owner	simple_xml_examples	App Permissions	Enabled

App permissions and deploying

Permissions

User interface » Views » basics » Permissions

Views should appear in

This app only (simple_xml_examples)
 All apps (system)

Permissions

Roles	Read	Write
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input checked="" type="checkbox"/>
splunk-system-role	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>

[Cancel](#) [Save](#)

Splunk Scripted App – Create App

Create App

Name Give your app a friendly name for display in Splunk Web.

Folder name * This name maps to the app's directory in \$SPLUNK_HOME/etc/apps/.

Version App version.

Visible No Yes Only apps with views should be made visible.

Author Name of the app's owner.

Description Enter a description for your app.

Template These templates contain example views and searches.

Upload asset Can be any html, js, or other file to add to your app.

Cancel

Save

Splunk Scripted App – Check App

Apps								Browse more apps	Install app from file	Create app
Showing 1-1 of 1 item								25 per page ▾		
Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions			
UserApp	userapp	1.0.0	Yes	Yes	App Permissions	Enabled Disable	Launch app Edit properties View objects			

default

User interface » Navigation menus » default

Enter and edit navigation menu XML configuration.

Navigation menu XML *

Plain Text

```
<nav search_view="search">
  <view name="search" default="true" />
  <view name="analytics_workspace" />
  <view name="datasets" />
  <view name="reports" />
  <view name="alerts" />
  <view name="dashboards" />
</nav>
```

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>
```

Search Dashboards

Search

enter search here...

No Event Sampling ▾

> Search History ?

Customized navigation Menu for User App

Splunk Scripted App – Check App

New Index

X

General Settings

Index Name

userapp_index

Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type

Events

Metrics

The type of data to store (event-based or metrics).

Home Path

optional

Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path

optional

Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path

optional

Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check

Enable

Disable

Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index

500

GB ▾

Maximum target size of entire index.

Save

Cancel

Splunk Scripted App – Check App

New Index

X

Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index GB ▾
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket GB ▾
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App ▾

Storage Optimization

Tsidx Retention Policy Enable Reduction Disable Reduction
Warning: Do not enable reduction without understanding the full implications. It is extremely difficult to rebuild reduced buckets. [Learn More ↗](#)

Reduce tsidx files older than Days ▾
Age is determined by the latest event in a bucket.

Save

Cancel

Splunk Scripted App – Check App

```
Administrator: Command Prompt
Directory of C:\Program Files\Splunk\etc\apps\userapp\bin

13-04-2024 19:17    <DIR>        .
13-04-2024 19:17    <DIR>        ..
13-04-2024 19:17                64 README
                           1 File(s)       64 bytes
                           2 Dir(s)  781,019,959,296 bytes free

C:\Program Files\Splunk\etc\apps\userapp\bin>pip install -t . splunk-sdk
Collecting splunk-sdk
  Downloading splunk-sdk-2.0.1.tar.gz (99 kB)
    99.5/99.5 kB 572.2 kB/s eta 0:00:00
Installing build dependencies ... done
Getting requirements to build wheel ... done
Installing backend dependencies ... done
Preparing metadata (pyproject.toml) ... done
Collecting deprecation (from splunk-sdk)
  Downloading deprecation-2.1.0-py2.py3-none-any.whl.metadata (4.6 kB)
Collecting packaging (from deprecation->splunk-sdk)
  Downloading packaging-24.0-py3-none-any.whl.metadata (3.2 kB)
Downloading deprecation-2.1.0-py2.py3-none-any.whl (11 kB)
Downloading packaging-24.0-py3-none-any.whl (53 kB)
  53.5/53.5 kB 2.9 MB/s eta 0:00:00
Building wheels for collected packages: splunk-sdk
  Building wheel for splunk-sdk (pyproject.toml) ... done
  Created wheel for splunk-sdk: filename=splunk_sdk-2.0.1-py3-none-any.whl size=115474 sha256=8364f0255570f47be9f5ba116c1b969fea2087ef0f56ef8d4d338e3ef35672b7
  Stored in directory: c:\users\dell\appdata\local\pip\cache\wheels\10\76\89\69faa1e491235d639ccb147bac73f4cb09927b8e7526d0f26b
Successfully built splunk-sdk
Installing collected packages: packaging, deprecation, splunk-sdk
Successfully installed deprecation-2.1.0 packaging-24.0 splunk-sdk-2.0.1

C:\Program Files\Splunk\etc\apps\userapp\bin>
```

Splunk Scripted App – Check App

```
userapp.py ×
1 # So we can run this script under python 2 or 3
2 from __future__ import print_function
3
4 import sys # for sys.stderr.write()
5 import time # for strftime
6 from datetime import datetime # for datetime.utcnow()
7 import random # to provide random data for this example
8
9 sys.stderr.write("User App| python script is starting up\n")
10
11 # output a single event
12 print(str(time.time()) + ", username=\"agent smith\", status=\"mediocre\", admin=noah, money=" + str(
13     random.randint(1, 1000)))
14
15 # output three events, each one separated by a newline (each line will be a unique event)
16 for x in range(0, 3):
17     strEvent = str(time.time()) + ", "
18     strEvent += "username=\"" + random.choice(["Stryker", "Valkerie", "Disco Stu"]) + "\", "
19     strEvent += "status=\"" + random.choice(["groovy", "hungry", "rage quit"]) + "\", "
20     strEvent += "admin=" + random.choice(["lenny", "carl", "moe"]) + ", "
21     strEvent += "money=" + str(random.randint(1, 1000))
22     print(strEvent)
```

Splunk Scripted App – Check App

```
Administrator: Command Prompt
3 File(s)      13,947 bytes
8 Dir(s)  781,018,214,400 bytes free

C:\Program Files\Splunk\etc\apps\userapp\bin>python userapp.py
TA-SimpleApp python script is starting up
1713017441.0819283, username="agent smith", status="mediocre", admin=noah, money=732
1713017441.0829284, username="Disco Stu", status="rage quit", admin=lenny, money=689
1713017441.0829284, username="Stryker", status="hungry", admin=carl, money=388
1713017441.0839283, username="Disco Stu", status="hungry", admin=lenny, money=434

C:\Program Files\Splunk\etc\apps\userapp\bin>python userapp.py
User App python script is starting up
1713017474.1689696, username="agent smith", status="mediocre", admin=noah, money=501
1713017474.1699712, username="Valkerie", status="hungry", admin=carl, money=704
1713017474.1699712, username="Valkerie", status="groovy", admin=lenny, money=749
1713017474.1719708, username="Stryker", status="rage quit", admin=moe, money=77

C:\Program Files\Splunk\etc\apps\userapp\bin>
```

The taskbar at the bottom of the screen displays various Windows icons, including the Start button, search, file explorer, edge browser, task view, and several pinned application icons such as Microsoft Word, Excel, and Powerpoint.

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>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Dashboards UserApp

New Search

source="C:\\Program Files\\Splunk\\etc\\apps\\userapp\\bin\\userapp.py" host="DESKTOP-B08BAAN" index="userapp_index" sourcetype="csv"

All time ▾

✓ 3 events (before 13/04/2024 20:21:00.000) No Event Sampling ▾ Job ▾ Fast Mode ▾

Events (3) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 millisecond per column

Time	Event
20:20:57.043 Sat Apr 13 2024	13/04/2024 1713019857.043623, username="Disco Stu", status="groovy", admin=carl, money=15 host = DESKTOP-B08BAAN source = C:\Program Files\Splunk\etc\apps\userapp\bin\userapp.py sourcetype = csv
20:20:57.043	13/04/2024 1713019857.043623, username="Valkerie", status="hungry", admin=lenny, money=115 host = DESKTOP-B08BAAN source = C:\Program Files\Splunk\etc\apps\userapp\bin\userapp.py sourcetype = csv
20:20:57.043	13/04/2024 1713019857.043623, username="Disco Stu", status="hungry", admin=moe, money=611 host = DESKTOP-B08BAAN source = C:\Program Files\Splunk\etc\apps\userapp\bin\userapp.py sourcetype = csv

List ▾ 20 Per Page ▾

< Hide Fields All Fields

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a index 1
...

Splunk Scripted App – Check App

```
Administrator: Command Prompt - splunk restart
C:\Program Files\Splunk\bin>splunk restart
Splunkd: Stopped

Splunk> Australian for grep.

Checking prerequisites...
Checking http port [8000]: open
Checking mgmt port [8089]: open
Checking appserver port [127.0.0.1:8065]: open
Checking kvstore port [8191]: open
Checking configuration... Done.
Checking critical directories...          Done
Checking indexes...
    (skipping validation of index paths because not running as LocalSystem)
    Validated: _audit _configtracker _dsappevent _dsclient _dsphonehome _internal _introspection _metrics _metrics_rollup _
telemetry _thefishbucket access cim_modactions history httpindex iis-index kafka main mssqlindex mysql-index summary userapp_index
    Done
Checking filesystem compatibility...  Done
Checking conf files for problems...
    Done
Checking default conf files for edits...
Validating installed files against hashes from 'C:\Program Files\Splunk\splunk-9.2.1-78803f08aabb-windows-64-manifest'
All installed files intact.
    Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...

Splunkd: Starting (pid 99792)
Done

Waiting for web server at http://127.0.0.1:8000 to be available
```

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 forwarders only)

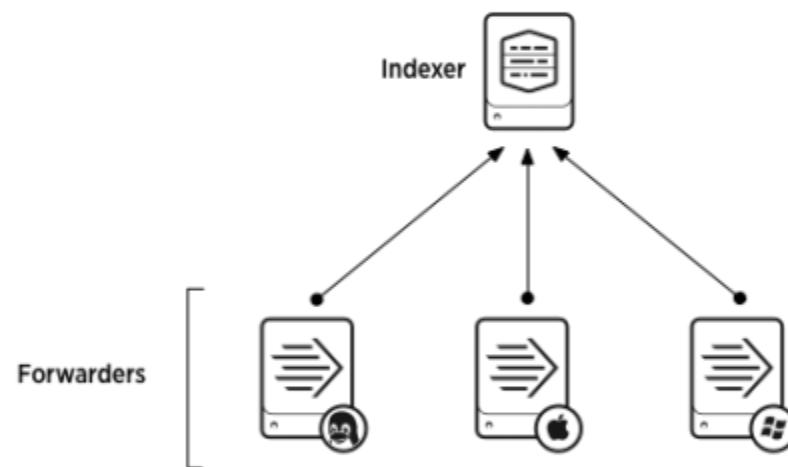
Types of forwarders in Splunk

- 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

TURN DATA INTO DOING

Splunk Universal Forwarder 9.2.1

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

0010
01010
0101

Collects Data From Remote Sources

Splunk Universal Forwarder collects data from a data source or another forwarder and sends it to a forwarder or a Splunk deployment.



Scalable

Thousands of universal forwarders can be installed with little impact on network and host performance.



Broad Platform Support

Available for installation on diverse computing platforms and architectures.

Start Your Free Download

Already have a Splunk account? [Log In](#)

Business Email REQUIRED

Password ?

First Name

Last Name

Job Title

Phone Number

Company

India ▼

Zip / Postal Code

I agree to the [Splunk Website Terms & Conditions of Use](#), [Splunk Privacy Policy](#) and [Splunk General Terms](#).

Obtain Splunk Universal Forwarder

Splunk Universal Forwarder 9.2.1

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

Choose Your Installation Package



Windows



Linux



Mac OS



FreeBSD



Solaris



AIX

32-bit

Windows 10

.msi

64.29 MB

[Download Now](#)

[Copy wget link](#)

More ▾

64-bit

Windows 10 , Windows 11
Windows Server 2016, 2019,
2022

.msi

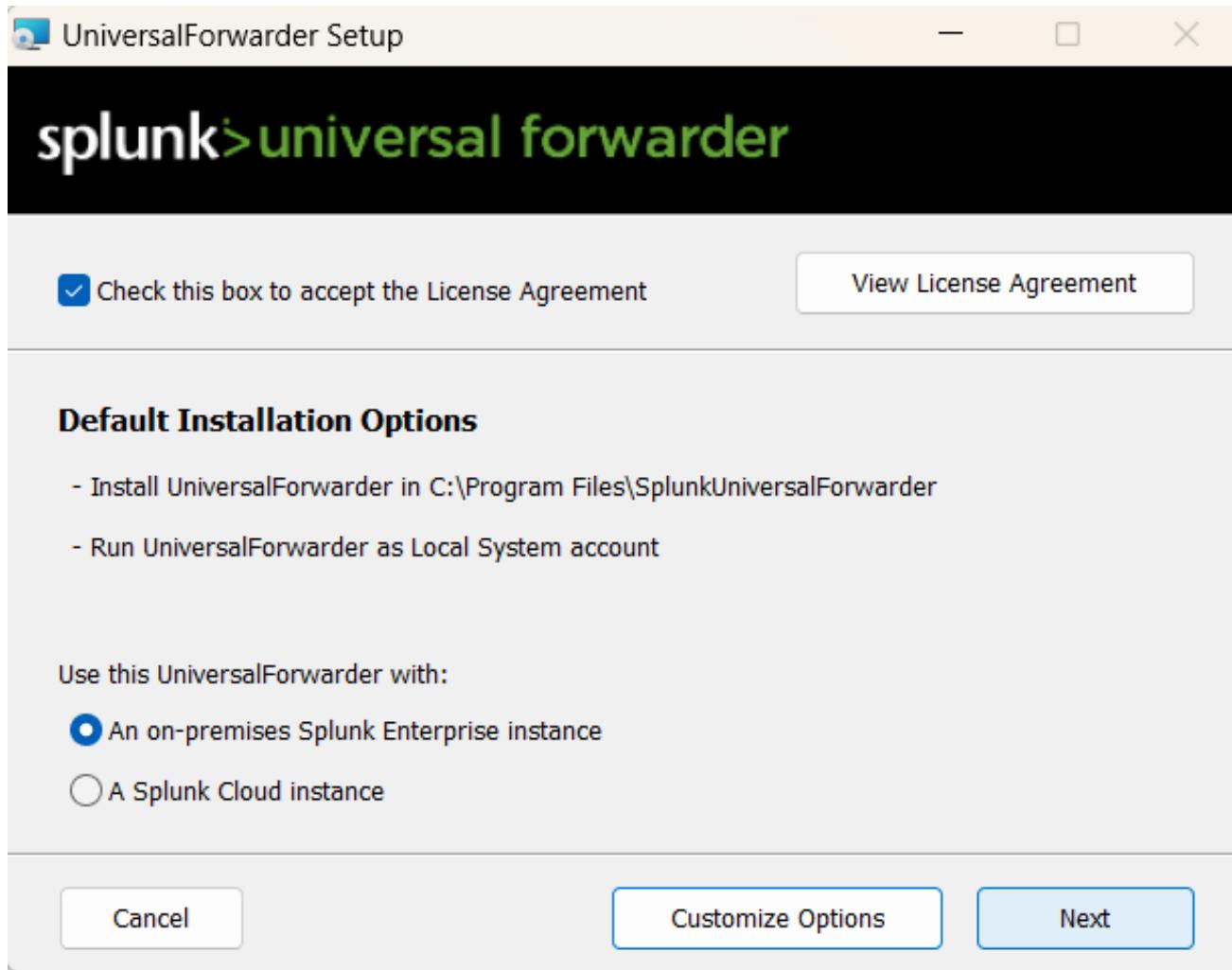
118.96 MB

[Download Now](#)

[Copy wget link](#)

More ▾

Obtain Splunk Universal Forwarder



Splunk Universal Forwarder After Installation

The screenshot shows the Splunk web interface after installation. The top navigation bar includes 'Hello, Administrator', 'Quick links', 'Dashboard', 'Recently viewed', 'Created by you' (which is underlined), and 'Shared with you'. The left sidebar lists various apps: Search & Reporting, Splunk Dashboard Examples, Splunk Secure Gateway, Upgrade Readiness App, and a 'Find more apps' link. The main content area displays a search bar, a dashboard dropdown, and a message stating 'You haven't created any knowledge' with a 'Create a dashboard' button. A large sidebar menu is open on the right, divided into several sections:

- DATA**
 - Data inputs
 - Forwarding and receiving
 - Indexes
 - Report acceleration summaries
 - Source types
 - Ingest actions
- KNOWLEDGE**
 - Searches, reports, and alerts
 - Data models
 - Event types
 - Tags
 - Fields
 - Lookups
 - User interface
 - Alert actions
 - Advanced search
 - All configurations
- DISTRIBUTED ENVIRONMENT**
 - Indexer clustering
 - Forwarder management** (this item is highlighted with a red rectangle)
 - Federated search
 - Distributed search
- SYSTEM**
 - Server settings
 - Server controls
 - Health report manager
 - Instrumentation
 - Licensing
 - Workload management
 - Mobile settings
- USERS AND AUTHENTICATION**
 - Roles
 - Users
 - Tokens
 - Password management
 - Authentication methods

Splunk Universal Forwarder Server Class

Forwarder Management

Repository Location: \$SPLUNK_HOME\etc\deployment-apps

1 Client
PHONED HOME IN THE LAST 24 HOURS

Apps (0) Server Classes (0) Clients (1)

No server classes. Learn more. [Create one](#)

New Server Class

Name:

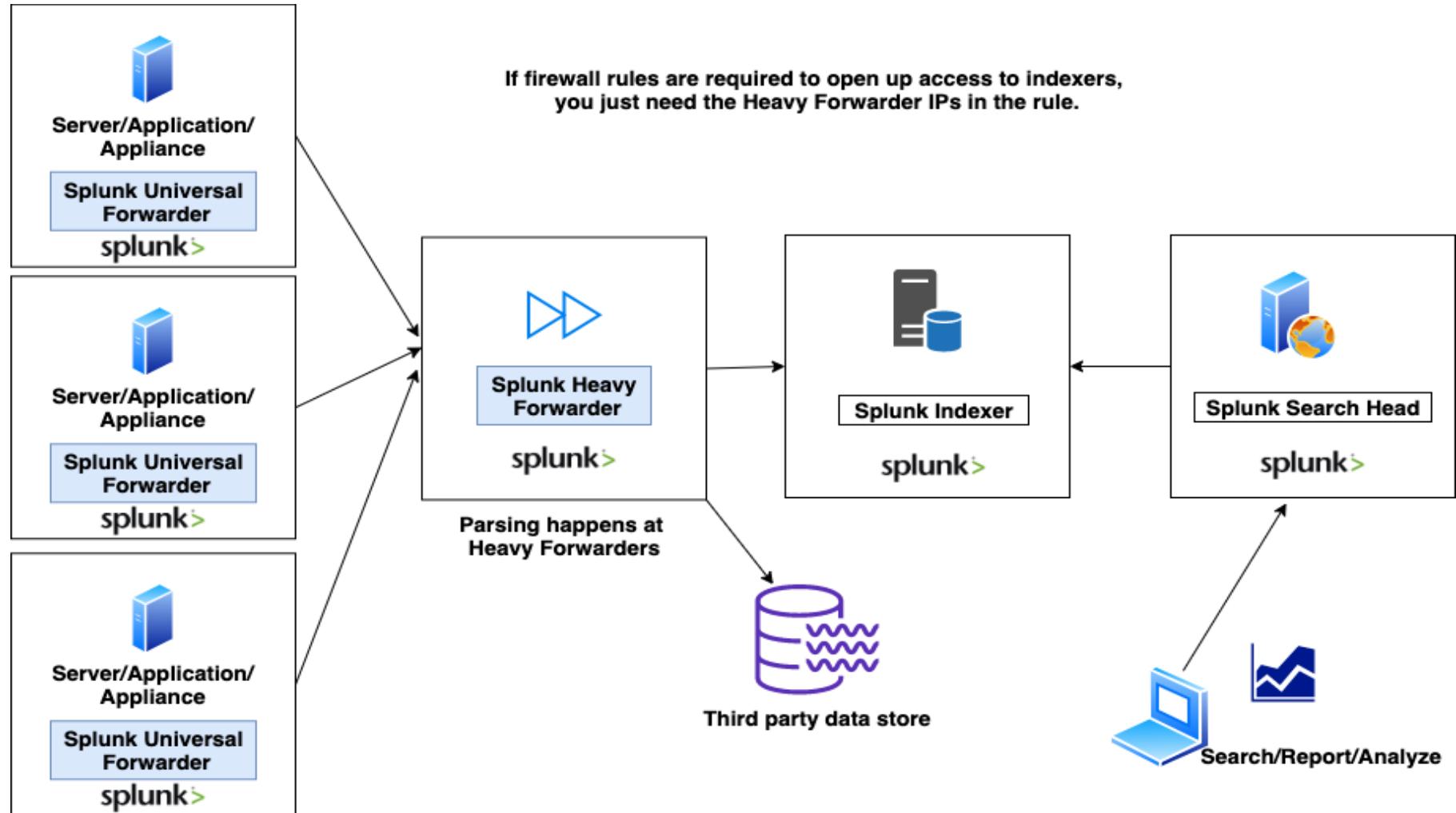
[Cancel](#) [Save](#)

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

Splunk Universal Forwarder binary

Collects and sends data to Indexers or Heavy Forwarders

Does not parse data (except when the data is structured such as CSV)

Cannot index data

Built-in license. No additional license required

Heavy Forwarder

Splunk Enterprise binary (used by Indexers, Search Heads and other Splunk processes)

Receives data from Universal Forwarders and sends it to Indexers, or other third party data stores. Acts as intermediary in routing data

Parses data, which includes Line breaking, timestamp extraction and extracting index-time fields

Can optionally index data

Forwarder license required. Requires access to Enterprise license stack if indexing is required.

Splunk Cli

C:\ 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>
```

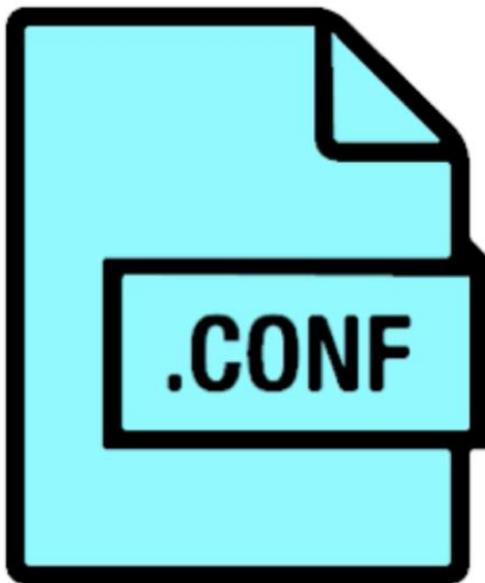


Search



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

[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](#)

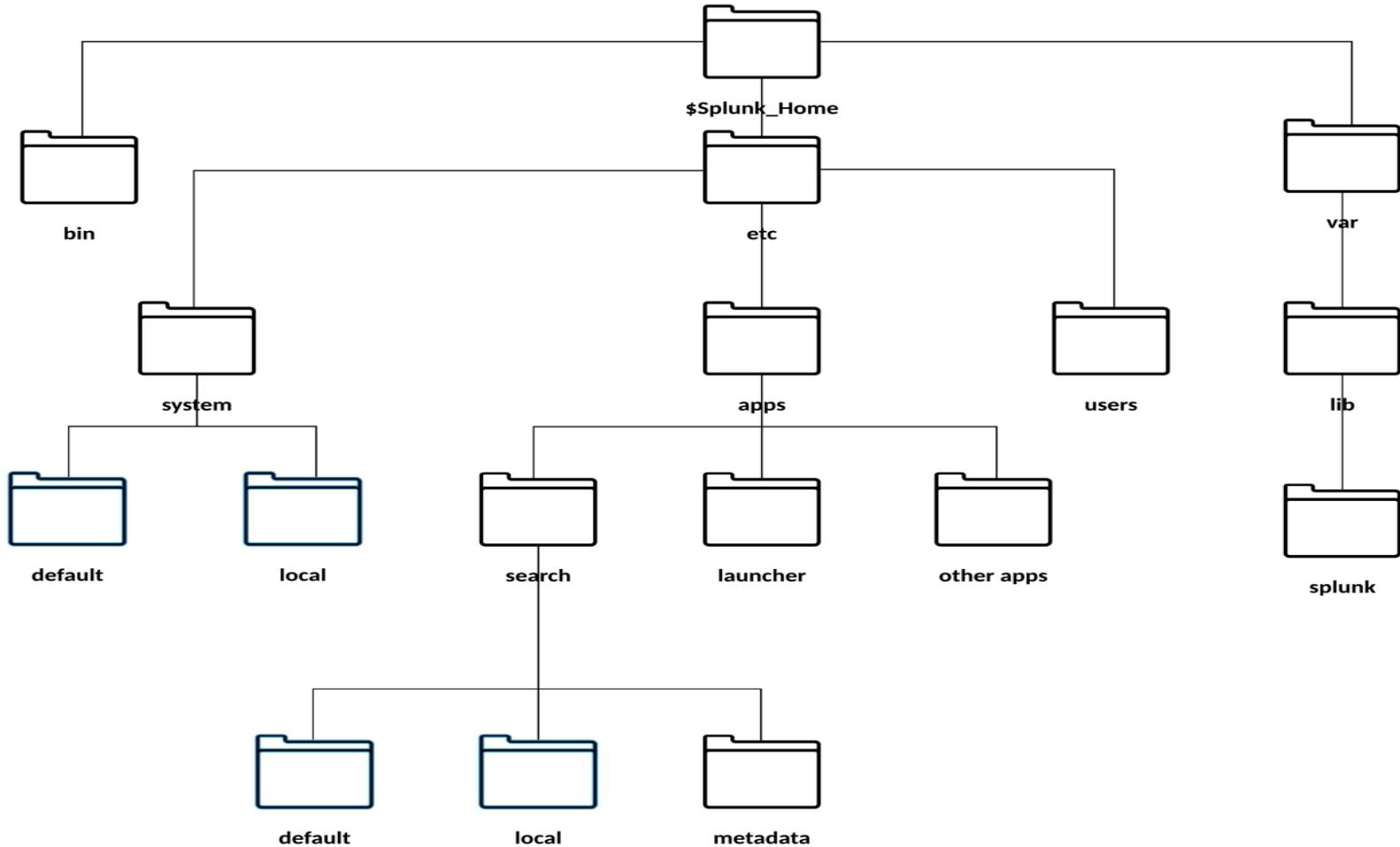
List of configuration files

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
<code>alert_actions.conf</code>	Create an alert.
<code>app.conf</code>	Configure app properties
<code>audit.conf</code>	Configure auditing and event hashing. This feature is not available for this release.
<code>authentication.conf</code>	Toggle between Splunk's built-in authentication or LDAP, and configure LDAP .
<code>authorize.conf</code>	Configure roles, including granular access controls.
<code>bookmarks.conf</code>	Bookmark monitoring console URLs.
<code>checklist.conf</code>	Customize monitoring console health check.
<code>collections.conf</code>	Configure KV Store collections for apps.
<code>commands.conf</code>	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

Configuration file
context

Global

App or user
specific

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
ColdStorageArchiver.py fill_summary_index.py mongod priforgetpng rapidDiag
ColdStorageArchiver_GCP.py genAuditKeys.py mongod-3.6 prigreypng recover-metadata
S3benchmark genRootCA.sh mongod-4.0 pripalpng rest_handler.py
bloom genSignedServerCert.py mongodump pri pamtopng runScript.py
bottle.py genSignedServerCert.sh mongorestore pri pamlsch safe_restart_cluster_master.py
btool genWebCert.py noah_self_storage_archiver.py pri pingtopam scripts
btprobe genWebCert.sh node pri weavepng scrubber.py
bzip2 idle3 openssl pydoc3 searchtest
classify idle3.7 parse_xml_buckets.py pydoc3.7 setSplunkEnv
coldToFrozenExample.py importtool pcre2-config python shc_upgrade_template.py
compsup installit.py pcregtest python3 signtool
copyright.txt jars pid_check.sh python3.7 slim
dbmanipulator.py jsmn pip3 python3.7m spl-lang-server-sockets
easy_install-3.7 locktest pip3.7 pyvenv spl2-orchestrator
ubuntu@ip-172-31-63-244:/opt/splunk/bin$ █
```

Splunk Enterprise for Ubuntu

```
Creating: /opt/splunk/var/lib/splunk/hashDb
New certs have been generated in '/opt/splunk/etc/auth'.
Checking critical directories... Done
Checking indexes...
Validated: _audit _configtracker _dsapp event _dsclient _dsphonehome _internal _introspection _metrics _metrics_rollup _telemetry _theft
hbucket history main summary
Done
Checking filesystem compatibility... Done
Checking conf files for problems...
Done
Checking default conf files for edits...
Validating installed files against hashes from '/opt/splunk/splunk-9.2.1-78803f08aabb-linux-2.6-x86_64-manifest'
All installed files intact.
Done
All preliminary checks passed.

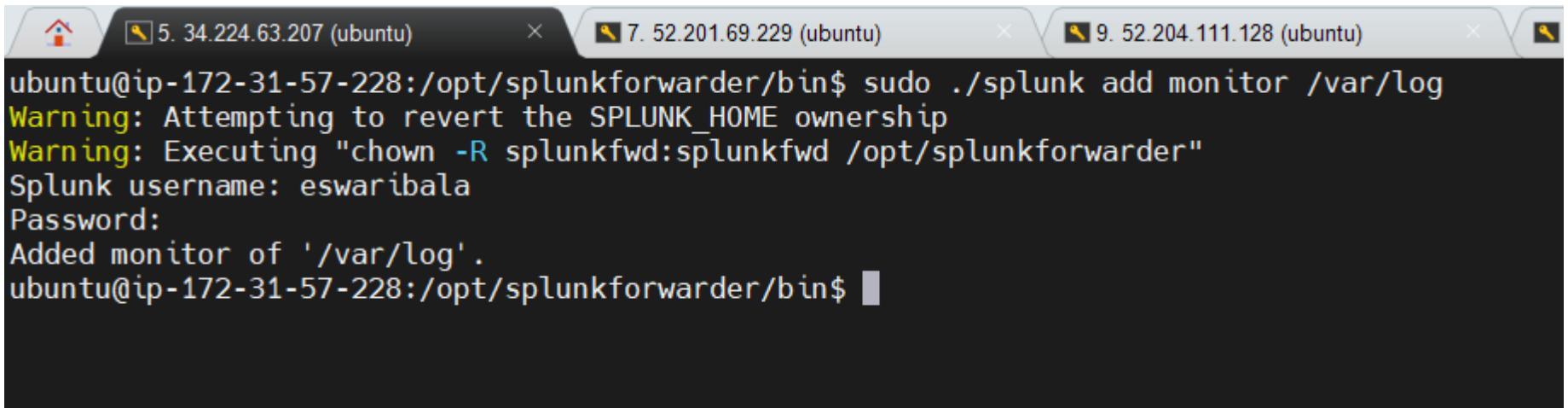
Starting splunk server daemon (splunkd)...
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=ip-172-31-63-244/0=SplunkUser
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done

Waiting for web server at http://127.0.0.1:8000 to be available..... Done

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://ip-172-31-63-244:8000
ubuntu@ip-172-31-63-244:/opt/splunk/bin$ http://ip-172-31-63-244:8000
```

Splunk Universal Forwarder inputs.conf



The screenshot shows a terminal window with three tabs open. The active tab is titled '7. 52.201.69.229 (ubuntu)'. The terminal output is as follows:

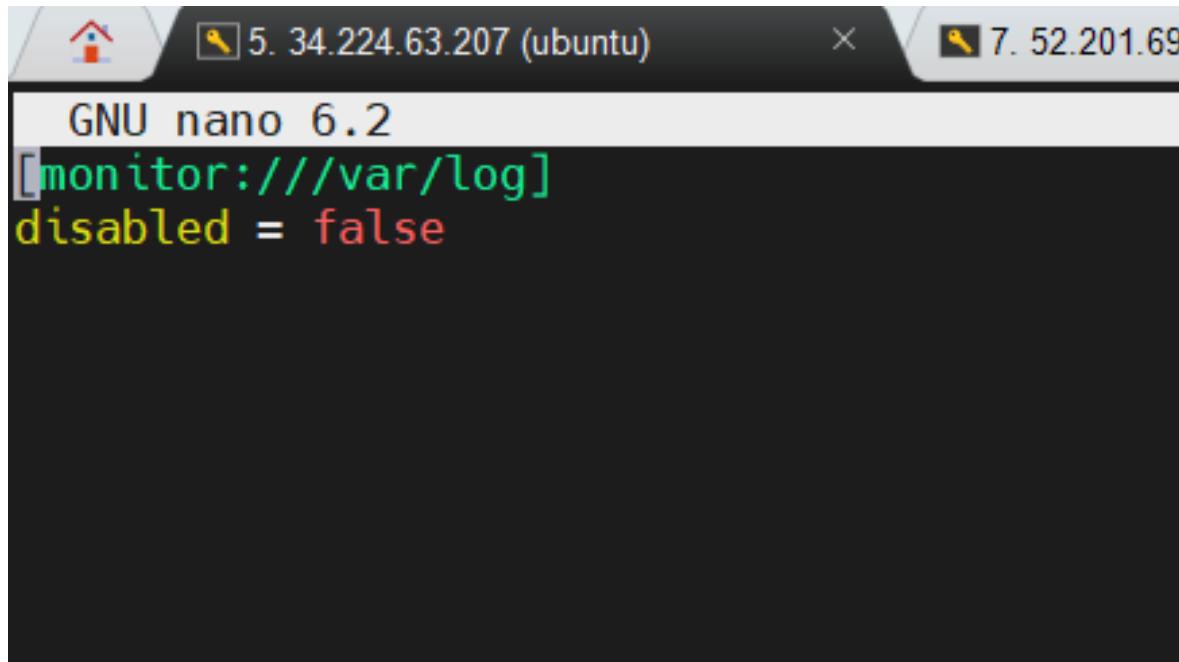
```
ubuntu@ip-172-31-57-228:/opt/splunkforwarder/bin$ sudo ./splunk add monitor /var/log
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Splunk username: eswaribala
Password:
Added monitor of '/var/log'.
ubuntu@ip-172-31-57-228:/opt/splunkforwarder/bin$
```

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



The image shows a terminal window titled "5. 34.224.63.207 (ubuntu)" with a nano editor open. The file contains the following configuration:

```
GNU nano 6.2
[monitor:///var/log]
disabled = false
```

Splunk Universal Forwarder outputs.conf

```
root@ip-172-31-57-228:/opt/splunkforwarder# cd bin
root@ip-172-31-57-228:/opt/splunkforwarder/bin# ls
2to3-3.7    bzip2      genRootCA.sh    idle3.7      pip3        prigreypng  pripngtopam scripts  splunk-tlsd   wheel
3$benchmark  classify   genSignedServerCert.sh openssl     pip3.7      pripalpng  priweavepng setSplunkEnv splunkd
btool       copyright.txt genWebCert.sh    pcre2-config prichunkpng priparamtopng pydoc3    slum      splunkmon
btprobe     easy_install-3.7 idle3      pid_check.sh  priforgepng pripnglsch  pydoc3.7   splunk   supervisor-simulator
root@ip-172-31-57-228:/opt/splunkforwarder/bin# sudo ./splunk add forward server 52.201.69.229:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Parameters must be in the form '-parameter value'
root@ip-172-31-57-228:/opt/splunkforwarder/bin# sudo ./splunk add forward-server 52.201.69.229:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added forwarding to: 52.201.69.229:9997.
root@ip-172-31-57-228:/opt/splunkforwarder/bin# sudo ./splunk list forward-server
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Active forwards:
  52.201.69.229:9997
Configured but inactive forwards:
  None
root@ip-172-31-57-228:/opt/splunkforwarder/bin# sudo ./splunk list forward-server
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Active forwards:
  52.201.69.229:9997
Configured but inactive forwards:
  None
root@ip-172-31-57-228:/opt/splunkforwarder/bin#
```

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

Splunk Receiver

New Search

Save As ▾ Create Table View Close

index="main" Last 24 hours 

✓ 7,233 events (11/04/2024 16:00:00.000 to 12/04/2024 16:32:46.000) No Event Sampling ▾ Job ▾  Smart Mode ▾

Events (7,233) Patterns Statistics Visualization

Format Timeline ▾    1 hour per column

List ▾  20 Per Page ▾  2 3 4 5 6 7 8 ... Next >

Time	Event
12/04/2024 16:17:37.000	Apr 12 16:17:37 ip-172-31-57-228 amazon-ssm-agent.amazon-ssm-agent[379]: #011status code: 400, request id: c14aa0ff-0ba0-4afe-bc23-7504a3b51901 host = ip-172-31-57-228 source = /var/log/syslog sourcetype = syslog
12/04/2024 16:17:37.000	Apr 12 16:17:37 ip-172-31-57-228 amazon-ssm-agent.amazon-ssm-agent[379]: 2024-04-12 16:17:37 ERROR EC2RoleProvider Failed to connect to Systems Manager with SSM role credentials. error calling RequestManagedInstanceRoleToken: AccessDeniedException: Systems Manager's instance management role is not configured for account: 975050122380 host = ip-172-31-57-228 source = /var/log/syslog sourcetype = syslog
12/04/2024 16:17:37.000	2024-04-12 16:17:37 ERROR EC2RoleProvider Failed to connect to Systems Manager with SSM role credentials. error calling RequestManagedInstanceRoleToken: AccessDeniedException: Systems Manager's instance management role is not configured for account: 975050122380 status code: 400, request id: c14aa0ff-0ba0-4afe-bc23-7504a3b51901 host = ip-172-31-57-228 source = /var/log/amazon/ssm/amazon-ssm-agent.log sourcetype = amazon-ssm-agent

< Hide Fields  All Fields

SELECTED FIELDS
a host 1
a source 11
a sourcetype 9

INTERESTING FIELDS
date_hour 3
date_mday 1
date_minute 19
date_month 1
date_second 46
a date_wday 1

Splunk Universal Forwarder outputs.conf

```
5. 34.224.63.207 (ubuntu)  x  7. 52.201.69.229 (ubuntu)  x  9. 52.204.111.128 (ubuntu)  x  10. 52.201.69.229 (ubuntu)
root@ip-172-31-57-228:/opt/splunkforwarder/etc/system/local# ls
README  outputs.conf  server.conf
root@ip-172-31-57-228:/opt/splunkforwarder/etc/system/local# cat outputs.conf
[tcpout]
defaultGroup = default-autolb-group

[tcpout:default-autolb-group]
server = 52.201.69.229:9997

[tcpout-server://52.201.69.229:9997]
root@ip-172-31-57-228:/opt/splunkforwarder/etc/system/local#
```

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:status]]\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

```
Administrator: Command Prompt
C:\Windows\System32>splunk btool --app=search transforms list
[geo_attr_countries]
filename = geo_attr_countries.csv
[geo_attr_us_states]
filename = geo_attr_us_states.csv
[geo_countries]
external_type = geo
filename = geo_countries.kmz
[geo_hex]
external_type = geo_hex
[geo_us_states]
external_type = geo
filename = geo_us_states.kmz

C:\Windows\System32>
```



The screenshot shows a Windows desktop environment. At the top, there is a command prompt window titled "Administrator: Command Prompt". The command entered was "splunk btool --app=search transforms list", which lists configuration files for geo-related transforms. Below the command prompt is the Windows taskbar, which includes the Start button, a search bar, and several pinned icons for applications like File Explorer, Microsoft Edge, and Microsoft Word. The system tray at the bottom right shows the date and time (11-04-2024, 14:13), battery status (ENG IN), and connectivity indicators.

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.

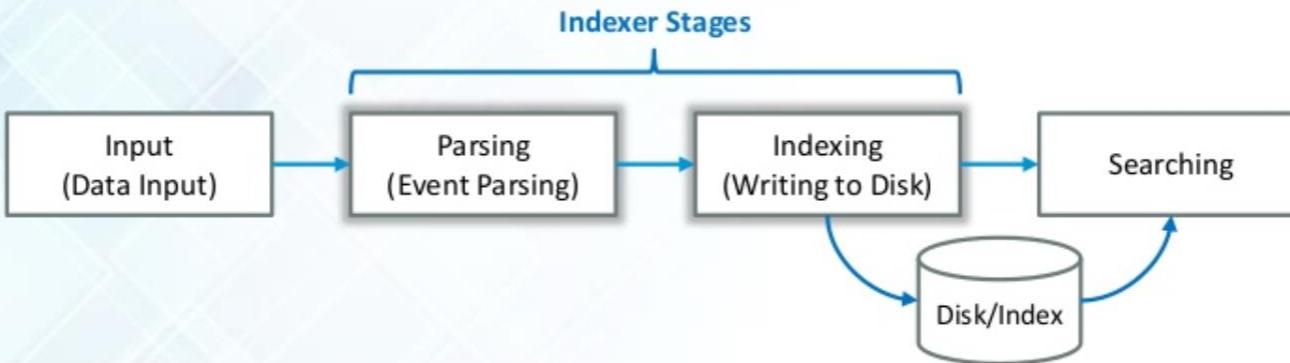
Splunk Storage Calculation Example

- Consider a Splunk deployment with a data ingest of 10gb/day, on a single server with no replication.
- This requires the following storage capacity:
- $10\text{gb/day} * .15 \text{ (raw data)} = 1.5\text{gb/day}$
- $10\text{gb/day} * .35 \text{ (metadata)} = 3.5\text{gb/day}$
- 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: $5\text{gb} * 90 \text{ days} = 450\text{gb}$
- For 1 year retention: $5\text{gb} * 365 \text{ days} = 1825\text{gb}$

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

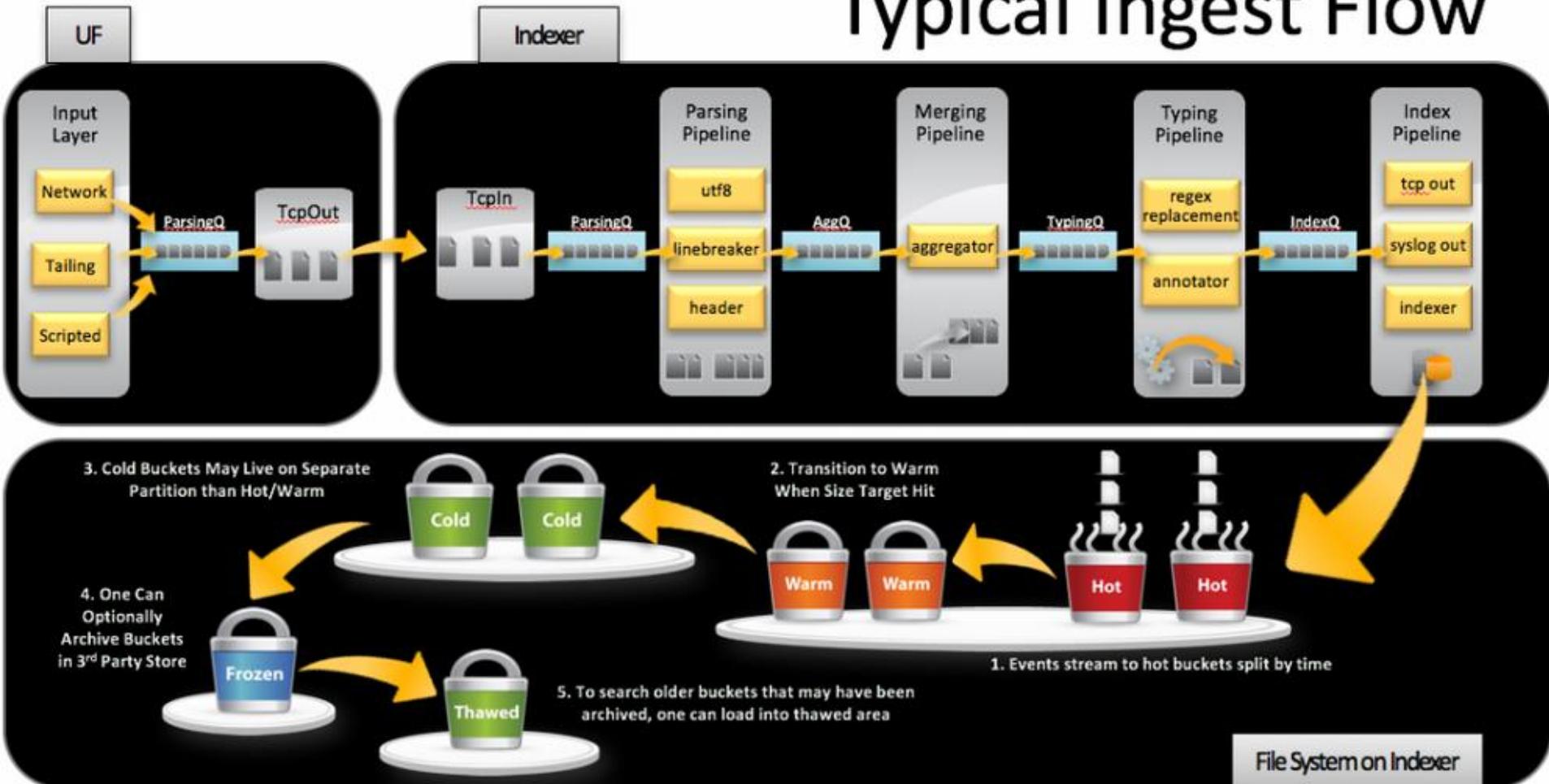
In the **Indexing stage**, events are sorted and indexed for storage based on:

- 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

Typical Ingest Flow



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

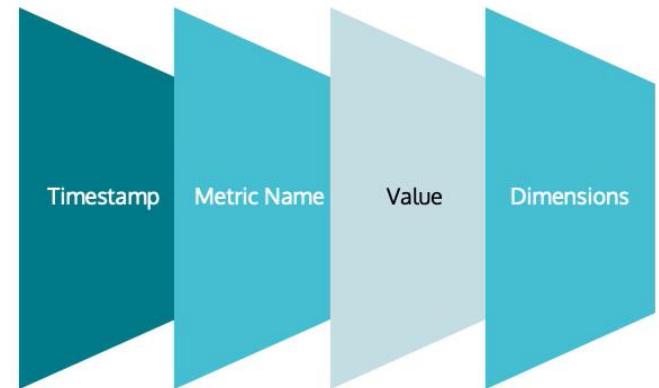
→ Event

- The default type
- Can handle any type of data

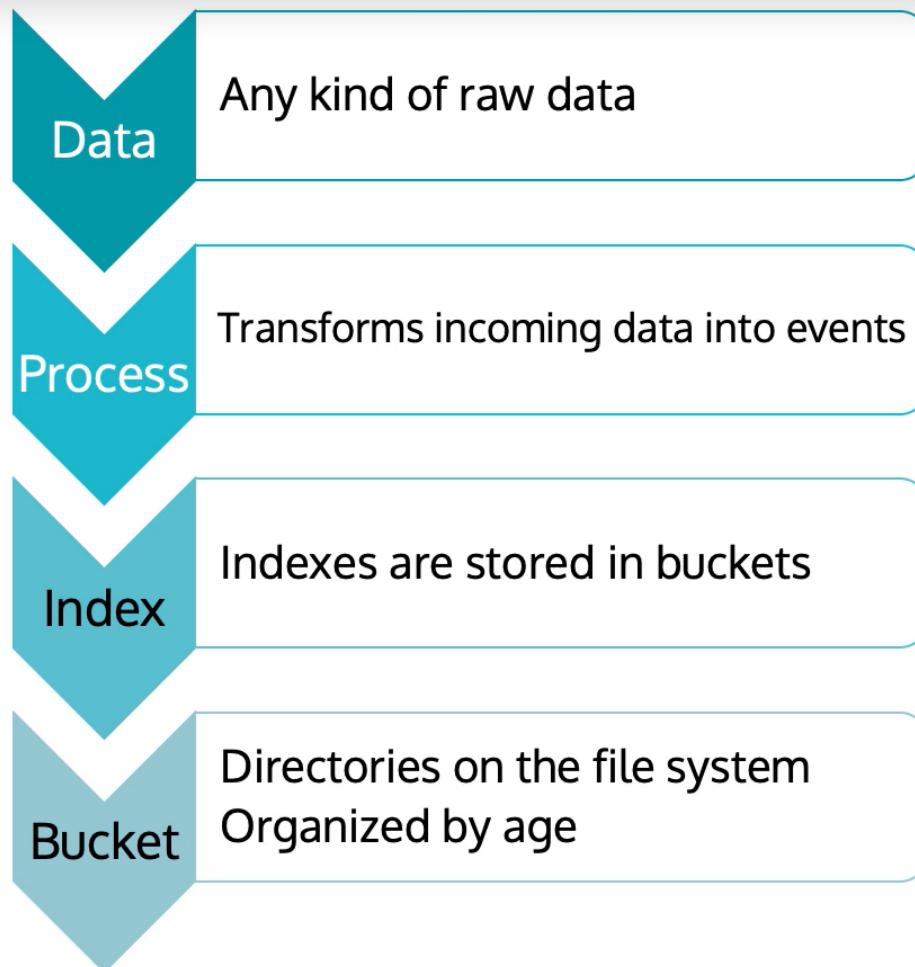


→ Metrics

- Optimized to store and retrieve *metrics data*



Index Structure

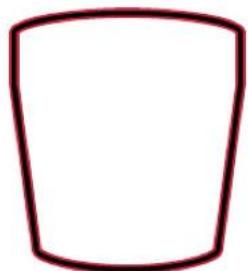


- host, source, sourcetype
- Character set encoding
- Line breaks
- Timestamps
- Metadata
- `$SPLUNK_HOME/var/lib/splunk/*`
- main, _internal, _audit

Index Structure



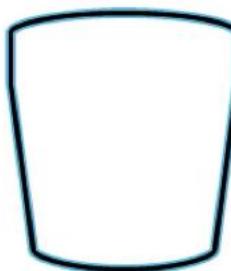
Indexes



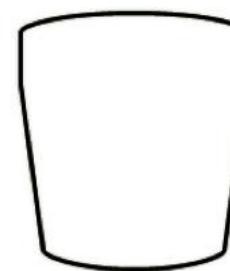
Hot (hotPath)



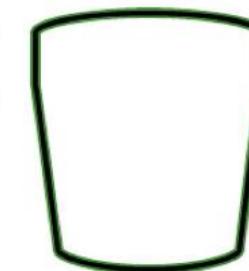
Warm
(warmPath)



Cold
(coldPath)

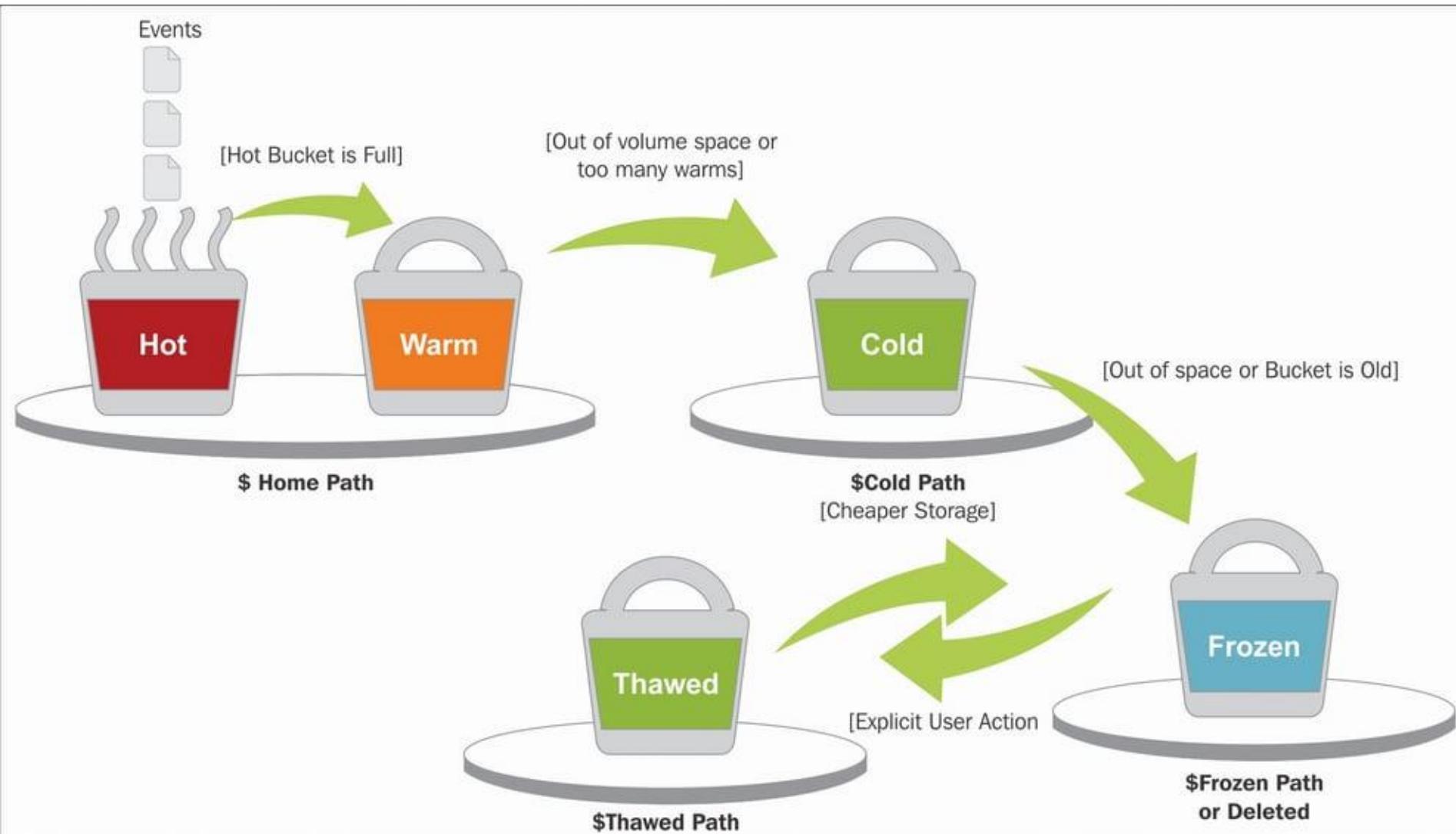


Frozen
(frozenPath)



Thawed
(thawedPath)

Index Structure



Buckets



Hot (hotPath)

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



Warm (warmPath)

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



Cold (coldPath)

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



Frozen (frozenPath)

Location that you specify

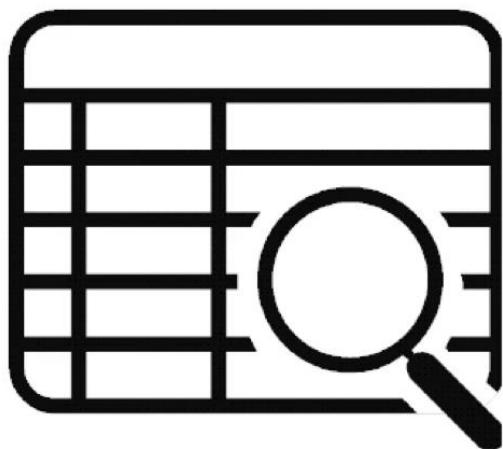


Thawed (thawedPath)

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

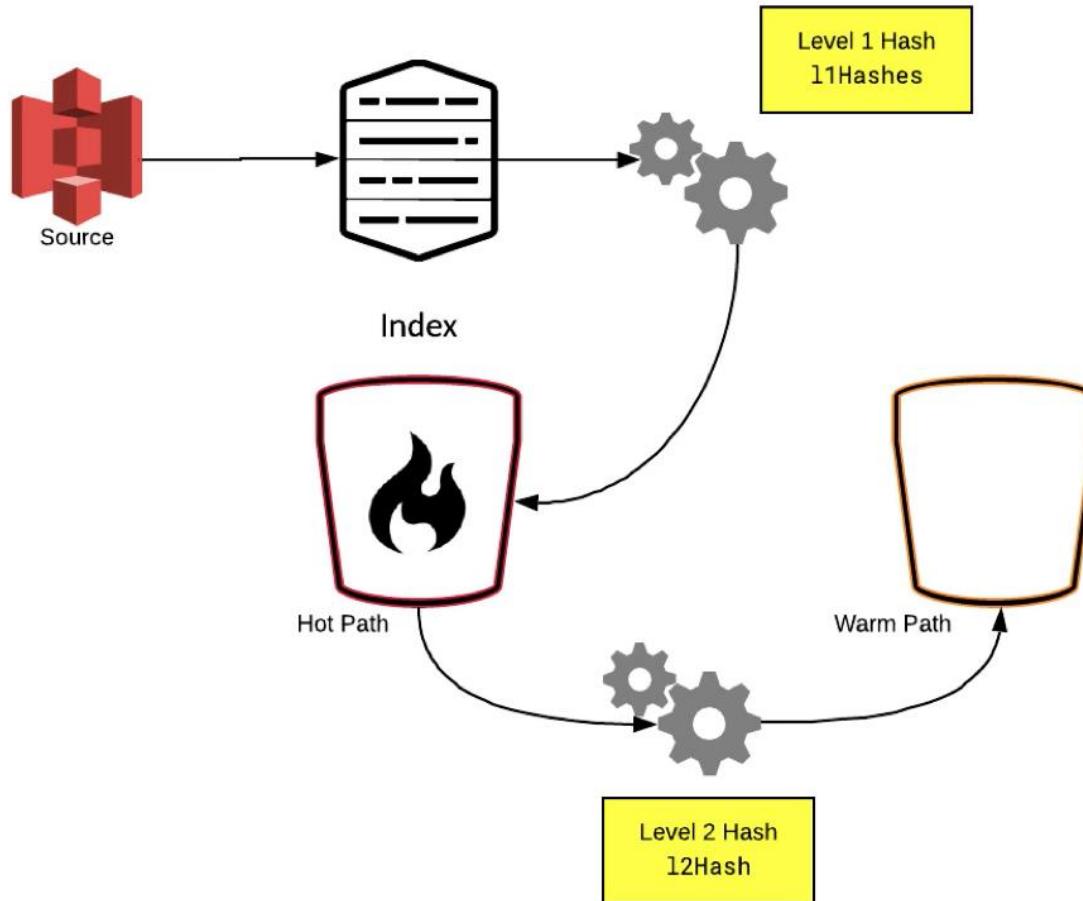
Buckets – Data Integrity Checks

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

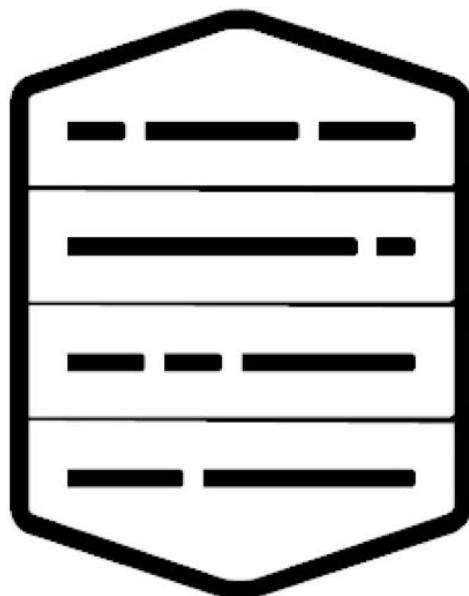
Global Settings



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

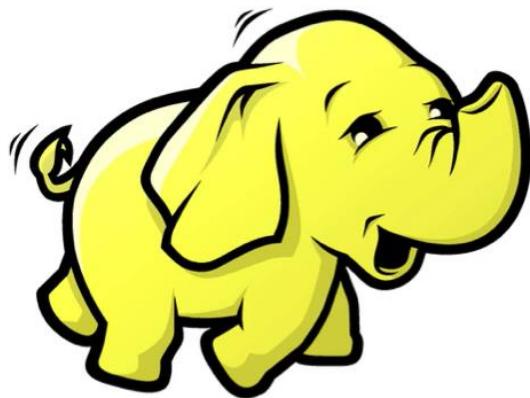
Index.conf

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

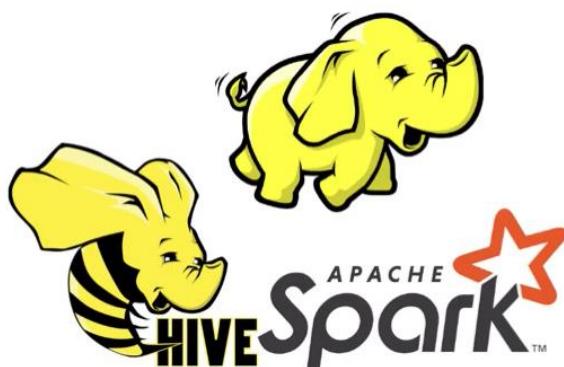
Per Provider Options



→ Options for External Resource Providers (ERPs)

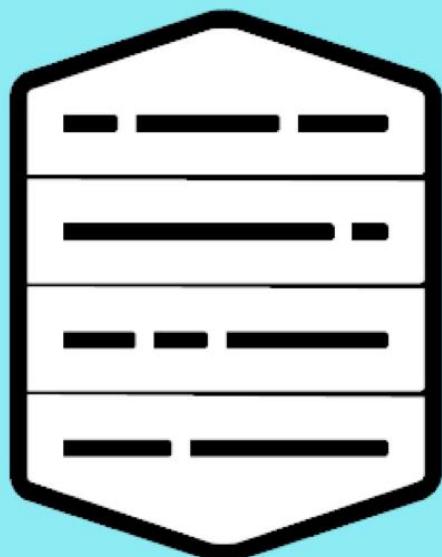
→ All provider stanzas begin with
[provider:]

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:]

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

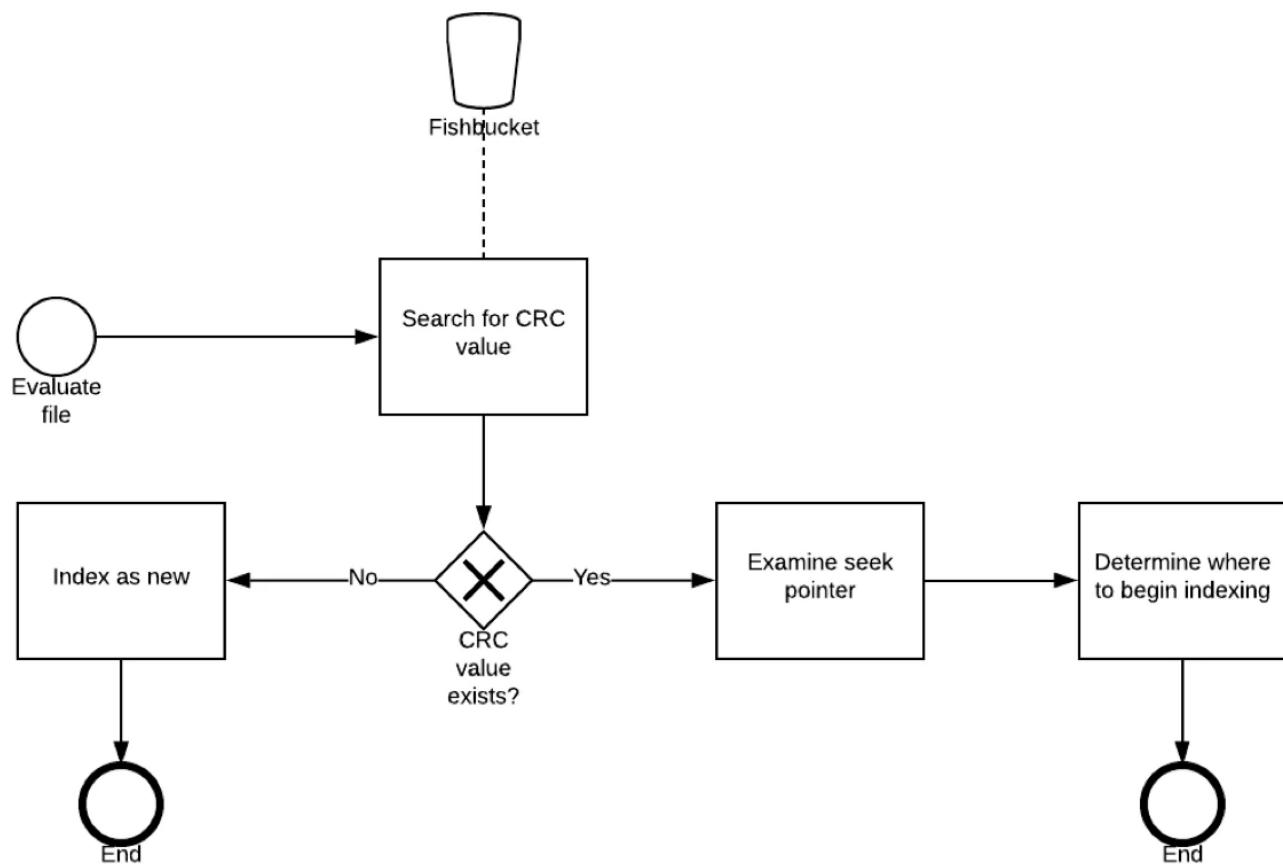
- CRC helps Splunk to determine if it has read a file before or not.
- To prevent re-indexing a previously-read file Splunk runs a cyclic redundancy check against first and last 256 bytes of a file.
- When Splunk is restarted file monitor processor checks if CRC is present in its database.
- If CRC is 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

The Fish Bucket



Fish Bucket- Special Index – Search which Files Indexed

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾

Search Analytics Datasets Reports Alerts Dashboards

Data Find Data to Analyze

Last 1 hour ▾ Refresh ▾ (30s ago) Split By Clear all

Metrics + Add new filter

spl

intr

disk_objects

Dispatch.data

Fishbucket.data

key_count

total_size

Indexes.data

Partitions.data

resource_usage

mlog

Datasets

Alerts

Data ingested from Last 30 days ▾
Changing this time setting will affect performance

spl.intr.disk_objects.Fishbucket.data.total_size (Time span=10s)

Avg

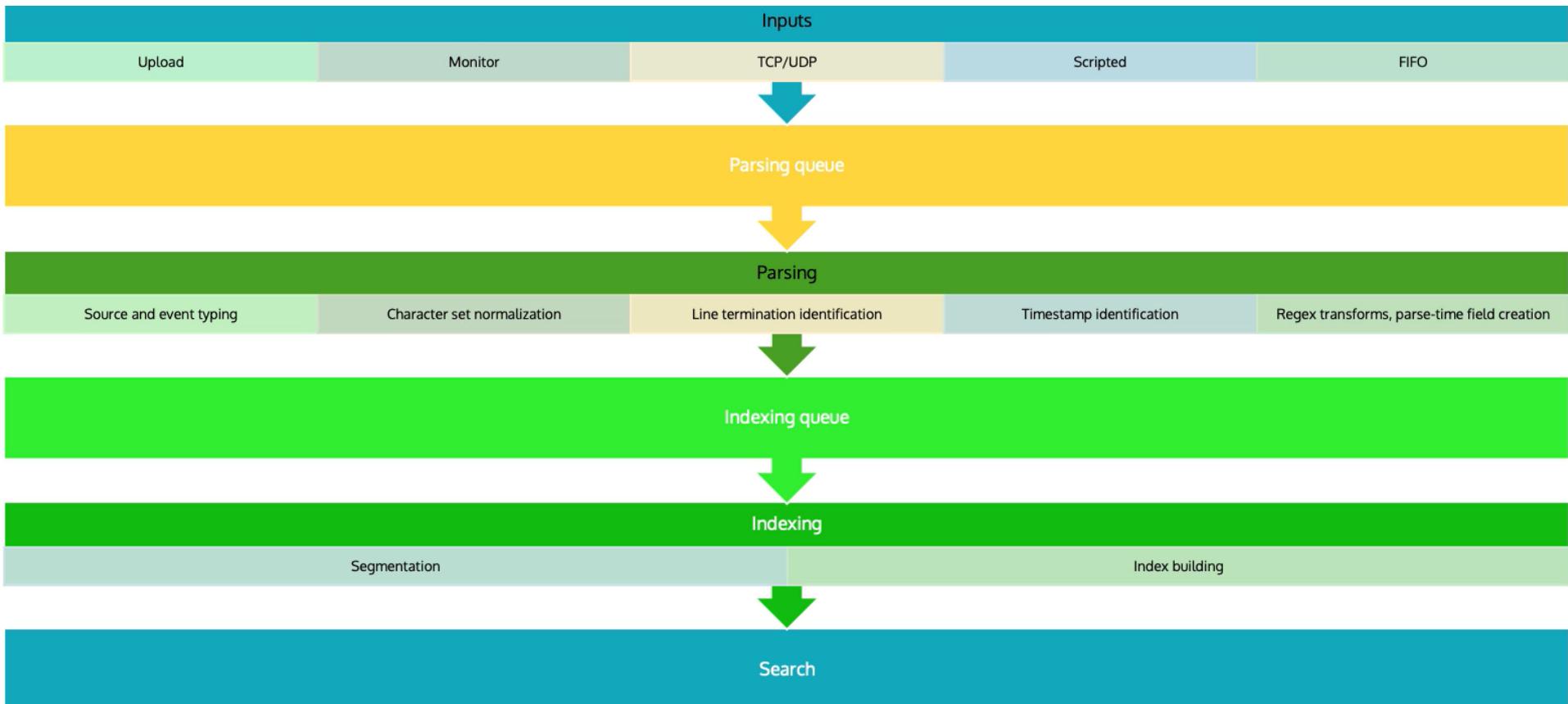
16:05 16:10 16:15 16:20 16:25 16:30 16:35 16:40 16:45 16:50 16:55 17:00
Wed, 17 Apr 2024

spl.intr.disk_objects.Fishbucket.data.key_count (Time span=10s)

Avg

16:05 16:10 16:15 16:20 16:25 16:30 16:35 16:40 16:45 16:50 16:55 17:00
Wed, 17 Apr 2024

Splunk Data Pipeline



Splunk Index files

This PC > Local Disk (C:) > Program Files > Splunk > etc > system > default >				
	Sort	View	...	
Name	Date modified	Type	Size	
authorize.conf	20-03-2024 23:47	CONF File	15 KB	
collections.conf	20-03-2024 23:47	CONF File	2 KB	
commands.conf	20-03-2024 23:47	CONF File	3 KB	
conf.conf	20-03-2024 23:47	CONF File	8 KB	
datamodels.conf	20-03-2024 23:47	CONF File	2 KB	
datatypebnf.conf	20-03-2024 23:47	CONF File	2 KB	
default-mode.conf	20-03-2024 23:47	CONF File	1 KB	
distsearch.conf	20-03-2024 23:47	CONF File	4 KB	
event_renderers.conf	20-03-2024 23:48	CONF File	1 KB	
eventdiscoverer.conf	20-03-2024 23:47	CONF File	5 KB	
eventtypes.conf	20-03-2024 23:47	CONF File	2 KB	
federated.conf	20-03-2024 23:47	CONF File	1 KB	
fields.conf	20-03-2024 23:47	CONF File	3 KB	
global-banner.conf	20-03-2024 23:47	CONF File	1 KB	
health.conf	20-03-2024 23:47	CONF File	39 KB	
indexes.conf	20-03-2024 23:47	CONF File	8 KB	

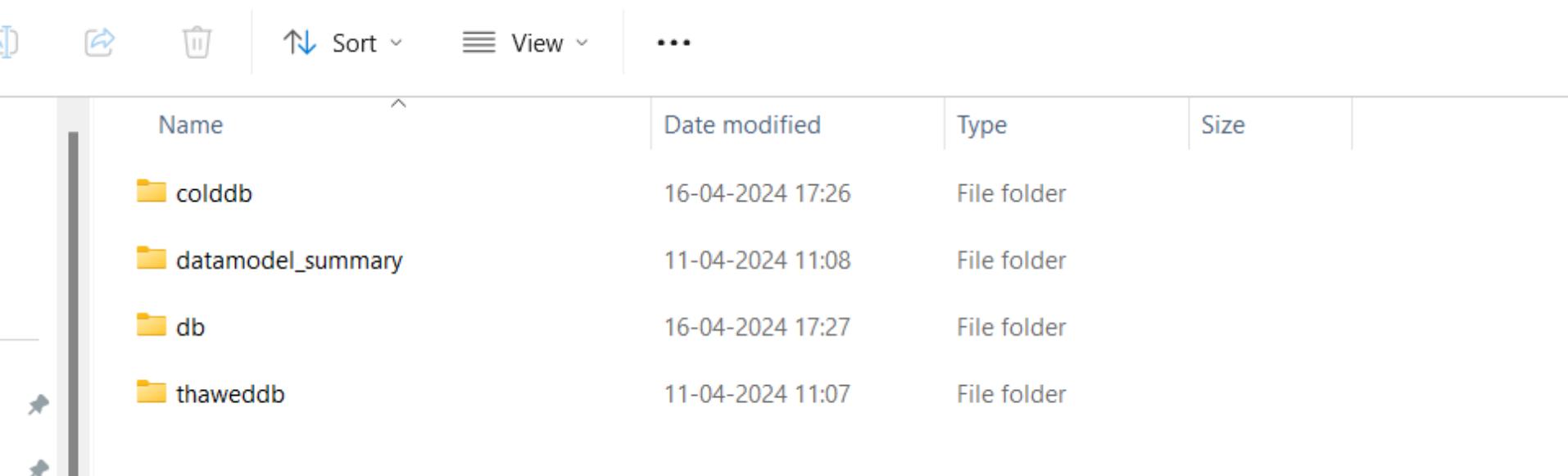
Splunk Index files

```
#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

This PC > Local Disk (C:) > Program Files > Splunk > var > lib > splunk > defaultdb >



A screenshot of a Windows File Explorer window. The address bar shows the path: This PC > Local Disk (C:) > Program Files > Splunk > var > lib > splunk > defaultdb >. The main pane displays a list of four file folders: colddb, datamodel_summary, db, and thaweddb. The columns are Name, Date modified, Type, and Size. The 'Name' column is sorted in ascending order.

Name	Date modified	Type	Size
colddb	16-04-2024 17:26	File folder	
datamodel_summary	11-04-2024 11:08	File folder	
db	16-04-2024 17:27	File folder	
thaweddb	11-04-2024 11:07	File folder	

Splunk Add Data

Administrator ▾ Messages ▾ Settings ▾ Activity ▾

Add Data Select Source Set Source Type Input Settings Review Done < Back Next >

Local Event Logs
Collect event logs from this machine.

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

Files & Directories >
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

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

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. [Learn More](#)

File or Directory ? [Browse](#)
On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Includelist ?

Excludelist ?

Splunk Add Data

Set Source Type

This page lets you see how the Splunk platform sees your data before "Next" to proceed. If not, use the options below to define proper events. If your data, create a new one by clicking "Save As".

Source: F:\Local disk\s...lunk\tutorialdata\mailsv\secure.log

Source type: cisco:asa ▾

Save As

> Event Breaks

> Timestamp

> Advanced

Splunk Add Data

Input Settings

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

App context

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

App Context

Search & Reporting (search) ▾

Host

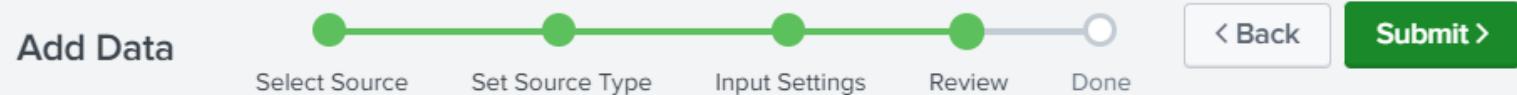
When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More ↗](#)

- Constant value
- Regular expression on path
- Segment in path

Host field value

DESKTOP-B08BAAN

Splunk Add Data



Review

Input Type File Monitor
Source Path F:\Local disk\splunk\tutorialdata\mailsv\secure.log
Continuously Monitor Yes
Source Type cisco:asa
App Context search
Host DESKTOP-B08BAAN
Index kafka

Splunk Add Data

New Search

[Save As ▾](#)[Create Table View](#)[Close](#)

```
source="F:\\Local disk\\splunk\\tutorialdata\\mailsv\\secure.log" host="DESKTOP-B08BAAN" index="kafka" sourcetype="cisco:asa"
```

All time ▾



✓ 9,829 events (before 11/04/2024 13:17:37.000) No Event Sampling ▾

Job ▾ II ■ ↗ + ↓ Smart Mode ▾

[Events \(9,829\)](#) [Patterns](#) [Statistics](#) [Visualization](#)

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

1 day per column

List ▾ Format 20 Per Page ▾

◀ Prev 1 2 3 4 5 6 7 8 ... Next >

◀ Hide Fields

☰ All Fields

i Time

Event

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

date_hour 1

date_mday 8

date_minute 1

a date_month 1

date_second 2

>	10/04/2024 05:45:50	Thu Apr 10 2024 05:45:50 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2 host = DESKTOP-B08BAAN source = F:\\Local disk\\splunk\\tutorialdata\\mailsv\\secure.log sourcetype = cisco:asa
>	10/04/2024 05:45:50.000	Thu Apr 10 2024 05:45:50 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 host = DESKTOP-B08BAAN source = F:\\Local disk\\splunk\\tutorialdata\\mailsv\\secure.log sourcetype = cisco:asa
>	10/04/2024 05:45:50.000	Thu Apr 10 2024 05:45:50 mailsv1 sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2 host = DESKTOP-B08BAAN source = F:\\Local disk\\splunk\\tutorialdata\\mailsv\\secure.log sourcetype = cisco:asa
>	10/04/2024 05:45:50.000	Thu Apr 10 2024 05:45:50 mailsv1 sshd[21881]: pam_unix(sshd:session): session closed for user nsharpe by (uid=0) host = DESKTOP-B08BAAN source = F:\\Local disk\\splunk\\tutorialdata\\mailsv\\secure.log sourcetype = cisco:asa

Splunk Handson

The screenshot shows the Splunk Enterprise search interface. At the top, there is a browser header with tabs for "Search | Splunk 8.0.8", "localhost:7070/index?name=test", and "Splunk spring boot log - YouTube". Below the browser is the Splunk navigation bar with links for "splunk>enterprise", "App: Search & Reporting", "Administrator", "Messages", "Settings", "Activity", "Help", and "Find". The main content area is titled "Search" and contains a search bar with placeholder text "enter search here...". To the right of the search bar are filters for "Last 24 hours" and a green search button. Below the search bar, there is a section titled "How to Search" with a link to "Documentation" and "Tutorial". To the right, there is a section titled "What to Search" with a "Data Summary" button and a placeholder text "Waiting for data...". At the bottom left, there is a "Search History" section with a single entry: "> Search History". The bottom of the screen shows the Windows taskbar with various pinned icons and system status indicators.

Splunk Handson

The screenshot shows the Splunk Enterprise web interface. At the top, there are three browser tabs: "Search | Splunk 8.0.8", "localhost:7070/index?name=test", and "Splunk spring boot log - YouTube". The main navigation bar includes links for "splunk>enterprise", "App: Search & Reporting", "Administrator", "Messages", "Settings", "Activity", "Help", and "Find". On the left, there's a sidebar with sections for "Search", "Analytics", "Datasets", and "Reports". The "Search" section contains a search bar, a sampling dropdown, and a "How to Search" guide. A central modal window titled "Data Summary" is open, showing a table with one host entry: "splunkforwarder" with a count of 38 indexed events last updated on 18/03/2021 at 16:57:56.000. Below the table are buttons for "INDEXED", "EARLIEST EVENT", and "LATEST EVENT". The bottom of the screen shows the Windows taskbar with various pinned icons and a search bar.

Data Summary

Hosts (1) Sources Sourcetypes (2)

Host	Count	Last Update
splunkforwarder	38	18/03/2021 16:57:56.000

INDEXED EARLIEST EVENT LATEST EVENT

Documentation Tutorial Data Summary

> Search History

Splunk Handson

Search | Splunk 8.0.8 localhost:7070/index?name=test Splunk spring boot log - YouTube

localhost:8200/en-GB/app/search/search?q=search%20host%3Dsplunkforwarder&sid=1616087257.107&display.page.search.mode=smart&dispatch.sample_rate=1000

Apps Insert title here Empire New Tab How to use Asserti... Browser Automatio... node.js - How can I... Freelancer-dev-810... Courses New Tab Airtel 4G Hotspot nt8F83 Reading list

splunk>enterprise App: Search & Reporting Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

New Search Save As ▾ Close

host=splunkforwarder Last 24 hours

✓ 38 events (17/03/2021 17:00:00.000 to 18/03/2021 17:07:37.000) No Event Sampling Job ▾

Events (38) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ Format 20 Per Page ▾ 1 2 Next >

Time	Event
18/03/2021 16:56:50.554	{ [-] @timestamp: 2021-03-18T16:56:50.554Z class: com.virtusa.DemoController message: name=test parent: service: demo-application severity: INFO span: 97b4b76a5e8394a8 thread: http-nio-7070-exec-10 trace: 97b4b76a5e8394a8}

< Hide Fields All Fields

SELECTED FIELDS
a host 1
a source 2
a sourcetype 2

INTERESTING FIELDS
a @timestamp 19
a class 11
date_hour 1
date_mday 1

Type here to search

22:37 18/03/2021

Creating App

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.3447]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd C:\Program Files\Splunk\etc\deployment-apps

C:\Program Files\Splunk\etc\deployment-apps>c:

C:\Program Files\Splunk\etc\deployment-apps>mkdir test

C:\Program Files\Splunk\etc\deployment-apps>cd test

C:\Program Files\Splunk\etc\deployment-apps\test>cd ..

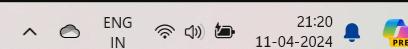
C:\Program Files\Splunk\etc\deployment-apps>cd ..

C:\Program Files\Splunk\etc>cd ..

C:\Program Files\Splunk>cd bin

C:\Program Files\Splunk\bin>splunk reload deploy-server
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Your session is invalid. Please login.
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Splunk username: eswaribala
Password:
Login successful, running command...
Reloading serverclass(es).

C:\Program Files\Splunk\bin>
```



Creating App

Forwarder Management

Repository Location: \$SPLUNK_HOME/etc/deployment-apps

1 Client

PHONED HOME IN THE LAST 24 HOURS

0 Clients

DEPLOYMENT ERRORS

Apps (2)

Server Classes (2) Clients (1)

Deployed Successfully ▾

filter

2 Apps 10 Per Page ▾

Name	Actions	After Installation
_server_app/Desktop-Server	Edit ▾	Enable App
test	Edit	Enable App

Creating App

Server Class: Splunk-Server-Class

[Back to Forwarder Management](#)

Edit ▾

Documentation ↗

1
App

IN THE SERVER CLASS

1
Client

IN THE SERVER CLASS

0%
Clients

DEPLOYED APPS SUCCESSFULLY

Apps Edit

All Apps ▾ filter

1 Apps 10 Per Page ▾

Name	Actions	After Installation	Clients
test	Edit ▾	Enable App	0 deployed

Clients Edit

Phone Home: All ▾ All Clients ▾ filter

1 Clients 10 Per Page ▾

i	Host Name	Client Name	Instance Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
>	DESKTOP-B08BAAN	EE8D8DE5-37E0-4649-B797-16941601EFE8	DESKTOP-B08BAAN	127.0.0.1	Delete Record	windows-x64	2 deployed	a few seconds ago

Creating App

Server Class: Desktop-Server

[Back to Forwarder Management](#)

[Edit ▾](#) [Documentation](#)

1 App

IN THE SERVER CLASS

1 Client

IN THE SERVER CLASS

100%

Clients

DEPLOYED APPS SUCCESSFULLY

Apps [Edit](#)

Deployed Successfully ▾

filter

1 Apps 10 Per Page ▾

Name	Actions	After Installation	Clients
_server_app_Desktop-Server	Edit ▾	Enable App	1 deployed

Clients [Edit](#)

Phone Home: All ▾

All Clients ▾

filter

1 Clients 10 Per Page ▾

i	Host Name	Client Name	Instance Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
>	DESKTOP-B08BAAN	EE8D8DE5-37E0-4649-B797-16941601EFE8	DESKTOP-B08BAAN	127.0.0.1	Delete Record	windows-x64	2 deployed	a few seconds ago

Search Fields

New Search

Save As ▾ Create Table View Close

index="_internal" type="TIMER"

Last 24 hours

✓ 2,074 events (11/04/2024 08:30:00.000 to 12/04/2024 08:38:23.000) No Event Sampling ▾

Job ▾

Events (2,074) Patterns Statistics Visualization

Format Timeline ▾ 1 hour per column

List ▾ 20 Per Page ▾		
All Fields		
Time		
Event		
12/04/2024 08:37:43.702 2024-04-12 08:37:43.702 +0530 Trace-Id= type=TIMER, name=unnamed_pool_1836902638_jdbc__mysql__//localhost__3306/ctscustomerdevdb?useSSL__true.pool.Wait, count=30, min=0.105, max=0.602, mean=0.39288070372540423, stddev=0.0021504221359925505, p50=0.394, p75=0.394, p95=0.394, p98=0.394, p99=0.394, m1_rate=0.0015260744954583626, m5_rate=0.003943610838225963, m15_rate=0.0035213289323884054, mean_rate=0.003969199789134234, rate_unit=events/second, duration_unit=milliseconds host = DESKTOP-B08BAAN source = C:\Program Files\Splunk\var\log\splunk\app_db_connect_connection_p... sourcetype = dbx_connection_pool_metrics		
12/04/2024 08:37:41.334 2024-04-12 08:37:41.334 +0530 Trace-Id= type=TIMER, name=org.eclipse.jetty.server.HttpConnectionFactory.127.0.0.1.9998.connections, count=178, min=2.0541, max=743.7788, mean=7.26650716302717, stddev=6.633986544321161, p50=181.0468, p75=181.0468, p95=181.0468, p98=181.0468, p99=181.0468, m1_rate=0.0015537395860103448, m5_rate=0.0039297439278964015, m15_rate=0.003510388877436884, mean_rate=0.020386903712825265, rate_unit=events/second, duration_unit=milliseconds host = DESKTOP-B08BAAN source = C:\Program Files\Splunk\var\log\splunk\app_db_connect_health_metric... sourcetype = dbx_health_metrics		
12/04/2024 08:37:41.334 2024-04-12 08:37:41.334 +0530 Trace-Id= type=TIMER, name=org.apache.http.client.HttpClient.http-client.post-requests, count=50, min=0.3352, max=7.9049, mean=2.3868769599350728, stddev=2.009287569676592, p50=3.5424, p75=4.4437, p95=4.4437, p98=4.4437, p99=4.4437, m1_rate=0.0031074791720206896, m5_rate=0.007859487850383927, m15_rate=0.007071286148835881, mean_rate=0.006790764177974189, rate_unit=events/second, duration_unit=milliseconds host = DESKTOP-B08BAAN source = C:\Program Files\Splunk\var\log\splunk\app_db_connect_health_metric... sourcetype = dbx_health_metrics		
12/04/2024 08:37:41.334 2024-04-12 08:37:41.334 +0530 Trace-Id= type=TIMER, name=io.dropwizard.jetty.MutableServletContextHandler.trace-requests, count=0, min=0.0, max=0.0, mean=0.0, stddev=0.0, p50=0.0, p75=0.0, p95=0.0, p98=0.0, p99=0.0, m1_rate=0.0, m5_rate=0.0, m15_rate=0.0, mean_rate=0.0, rate_unit=events/second, duration_unit=milliseconds		

< Prev 1 2 3 4 5 6 7 8 ... Next >

Selected Fields:
a host 1
a source 2
a sourcetype 2

Interesting Fields:
count 100+
date_hour 3
date_mday 1
date_minute 60
date_month 1
date_second 9
date_wday 1
date_year 1
date_zone 1
a duration_unit 1

Search Fields

i	Time	Event
>	12/04/2024 08:02:55.544	2024-04-12 08:02:55.544 +0530 Trace-Id= type=TIMER, name=io.dropwizard.jetty.MutableServletContextHandler.post-requests, count=25, min=88.0, max=431.0, mean=105.90424213616946, stddev=0.9789048958447766, p50=106.0, p75=106.0, p95=106.0, p98=106.0, p99=106.0, m1_rate=9.469213900601852E-4, m5_rate=0.0029673211570718262, m15_rate=0.0032404540014915138, mean_rate=0.003763549560898825, rate_unit=events/second, duration_unit=milliseconds host = DESKTOP-B08BAAN source = C:\Program Files\Splunk\var\log\splunk\splunk_app_db_connect_health_metric... sourcetype = dbx_health_metrics
>	12/04/2024 07:59:55.519	2024-04-12 07:59:55.519 +0530 Trace-Id= type=TIMER, name=io.dropwizard.jetty.MutableServletContextHandler.trace-requests, count=0, min=0.0, max=0.0, mean=0.0, stddev=0.0, p50=0.0, p75=0.0, p95=0.0, p98=0.0, p99=0.0, m1_rate=0.0, mean_rate=0.0, rate_unit=events/second, duration_unit=milliseconds host = DESKTOP-B08BAAN source = C:\Program Files\Splunk\var\log\splunk\splunk_app_db_connect_health_metric... sourcetype = dbx_health_metrics
>	12/04/2024 07:53:55.452	2024-04-12 07:53:55.452 +0530 Trace-Id= type=TIMER, name=io.dropwizard.jetty.MutableServletContextHandler.dispatches, count=169, min=1.0, max=740.0, mean=58.98754030589151, stddev=0.16873611047276674, p50=59.0, p75=59.0, m1_rate=3.4835291180862645E-4, m5_rate=0.002429482550775456, m15_rate=0.0035859070228448802, mean_rate=0.02769323353934851, rate_unit=events/second, duration_unit=milliseconds host = DESKTOP-B08BAAN source = C:\Program Files\Splunk\var\log\splunk\splunk_app_db_connect_health_metric... sourcetype = dbx_health_metrics
>	12/04/2024 07:47:55.395	2024-04-12 07:47:55.395 +0530 Trace-Id= type=TIMER, name=io.dropwizard.jetty.MutableServletContextHandler.dispatches, count=168, min=1.0, max=740.0, mean=57.8784140794716, stddev=0.1484668687334012, p50=58.0, p75=58.0, p95=58.0, p98=58.0, p99=58.0, m1_rate=9.469213900601852E-4, m5_rate=0.002967472385930507, m15_rate=0.004069329102263737, mean_rate=0.029255461529035454, rate_unit=events/second, duration_unit=milliseconds

Search Fields

New Search

index="_internal" type="TIMER" rate

840 of 840 events matched No Event Sampling ▾

Events (840) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 1 minute per column

16 12 8 4 16 12 8 4

07:50 Fri Apr 12 2024 08:00 08:10 08:20 08:30 08:40

List ▾ Format 20 Per Page ▾

< Prev 1 2 3 4 5 6 7 8 ... Next >

Hide Fields All Fields

SELECTED FIELDS
a host 1
a source 2
a sourcetype 2

INTERESTING FIELDS
a index 1
linecount 1
splunk_server 1
a type 1

+ Extract New Fields

i	Time	Event
>	12/04/2024 08:42:43.754	2024-04-12 08:42:43.754 +0530 Trace-Id= type=TIMER, name=unnamed_pool_1836902638.jdbc._mysql_/_localhost_3306/ctscustomerdevdb?useSSL=true.pool.Wait, count=31, min=0.105, max=0.6062, mean=0.47242928778133475, stddev=0.00965378516874227, p50=0.4736, p75=0.4736, p95=0.4736, p98=0.4736, p99=0.4736, m1_rate=0.001217961266261503, m5_rate=0.034082082106354993, m15_rate=0.003455873657461511, mean_rate=0.003944898540989439, rate_unit=events/second, duration_unit=milliseconds host = DESKTOP-B08BAAN source = C:\Program Files\Splunk\var\log\splunk\splunk_app_db_connect_connection_p... sourcetype = dbx_connection_pool_metrics
>	12/04/2024 08:42:41.391	2024-04-12 08:42:41.391 +0530 Trace-Id= type=TIMER, name=io.dropwizard.jetty.MutableServletContextHandler.dispatches, count=179, min=1.0, max=740.0, mean=43.20063242367599, stdDev=1.8736620498874978, p50=43.0, p75=43.0, p95=43.0, p98=43.0, p99=61.0, m1_rate=0.001218147672175367, m5_rate=0.00341754603715078, m15_rate=0.003448093028712468, mean_rate=0.019826025638593495, rate_unit=events/second, duration_unit=milliseconds host = DESKTOP-B08BAAN source = C:\Program Files\Splunk\var\log\splunk\splunk_app_db_connect_health_metric... sourcetype = dbx_health_metrics
>	12/04/2024 08:42:41.391	2024-04-12 08:42:41.391 +0530 Trace-Id= type=TIMER, name=io.dropwizard.jetty.MutableServletContextHandler.get-requests, count=146, min=1.0, max=740.0, mean=1.7867714157647234, stdDev=8.348779831386077, p50=1.0, p75=2.0, p95=2.0, p98=3.0, p99=3.0, p999=190.0, m1_rate=8.088927982067034E-54, m5_rate=2.6008660116664347E-12, m15_rate=2.134603565217803E-5, mean_rate=0.016170949907703694, rate_unit=events/second, duration_unit=milliseconds host = DESKTOP-B08BAAN source = C:\Program Files\Splunk\var\log\splunk\splunk_app_db_connect_health_metric... sourcetype = dbx_health_metrics

Search Fields

Splunk > enterprise Apps ▾

Administrator 1 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

New Search

index=mysql-index sourcetype=Perfmon:mssql source=schema_mysqlconnection OR source=mi_input://schema_mysqlconnection

13,412 events (11/04/2024 08:30:00.000 to 12/04/2024 08:51:02.000) No Event Sampling ▾

Save As Create Table View Close

Last 24 hours ▾

Events (13,412) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 1 hour per column

6,000 4,000 2,000

12:00 Thu Apr 11 2024 18:00 00:00 Fri Apr 12 06:00

6,000 4,000 2,000

List Format 20 Per Page ▾ 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields	All Fields	i Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1		> 12/04/2024 08:50:01.018	2024-04-12 08:50:01.018, TABLE_CATALOG="def", TABLE_SCHEMA="performance_schema", TABLE_NAME="innodb_redo_log_files", TABLE_TYPE="BASE TABLE", ENGINE="PERFORMANCE_SCHEMA", VERSION="10", ROW_FORMAT="Dynamic", TABLE_ROWS="2", AVG_ROW_LENGTH="0", DATA_LENGTH="0", MAX_DATA_LENGTH="0", INDEX_LENGTH="0", DATA_FREE="0", CREATE_TIME="2024-04-11 07:30:36", TABLE_COLLATION="utf8mb4_0900_ai_ci" host = localhost source = schema_mysqlconnection sourcetype = Perfmon:mssql
INTERESTING FIELDS a index 1 # linecount 1 a splunk_server 1		> 12/04/2024 08:50:01.018	2024-04-12 08:50:01.018, TABLE_CATALOG="def", TABLE_SCHEMA="ctscustomerdb", TABLE_NAME="individual", TABLE_TYPE="BASE TABLE", ENGINE="InnoDB", VERSION="10", ROW_FORMAT="Dynamic", TABLE_ROWS="0", AVG_ROW_LENGTH="0", DATA_LENGTH="16384", MAX_DATA_LENGTH="0", INDEX_LENGTH="0", DATA_FREE="0", CREATE_TIME="2024-02-28 12:16:00", TABLE_COLLATION="utf8mb4_00_ai_ci" host = localhost source = schema_mysqlconnection sourcetype = Perfmon:mssql
+ Extract New Fields		> 12/04/2024 08:50:01.018	2024-04-12 08:50:01.018, TABLE_CATALOG="def", TABLE_SCHEMA="ctscustomerdb", TABLE_NAME="corporate", TABLE_TYPE="BASE TABLE", ENGINE="InnoDB", VERSION="10", ROW_FORMAT="Dynamic", TABLE_ROWS="0", AVG_ROW_LENGTH="0", DATA_LENGTH="16384", MAX_DATA_LENGTH="0", INDEX_LENGTH="0", DATA_FREE="0", CREATE_TIME="2024-02-28 12:16:00", TABLE_COLLATION="utf8mb4_0900_ai_ci"

Search Fields

```
index=mysql-index sourcetype=Perfmon:mssql source=schema_mysqlconnection OR source=mi_input://schema_mysqlconnection
```

✓ 13,412 events (11/04/2024 08:30:00.000 to 12/04/2024 08:53:28.000) No Event Sampling ▾

Events (13,412) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect



List ▾ Format 20 Per Page ▾

< Hide Fields

All Fields



Time

Event

SELECTED FIELDS

a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS

a index 1
linecount 1
a splunk_server 1

+ Extract New Fields

splunk_server

1 Value, 100% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field

Values

Count

%

DESKTOP-B08BAAN

13,412

100%

host = localhost | source = schema_mysqlconnection | sourcetype = Perfmon:mssql

> 12/04/2024 2024-04-12 08:50:01.018, TABLE_CATALOG="def", TABLE_SCHEMA="ctscustomerdb", TABLE_NAME="address", TABL
08:50:01.018 ABLE_ROWS="0", AVG_ROW_LENGTH="0", DATA_LENGTH="16384", MAX_DATA_LENGTH="0", INDEX_LENGTH="16384", DAT
I="146mb4_0000_01_01"

Reports

Splunk > enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

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 ▾

48,090 of 48,090 events matched No Event Sampling ▾

Job ▾

Events Patterns Statistics (61) Visualization

Line Chart Format Trellis

Legend:

- 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\connection_pool_metrics.log
- C:\Program Files\Splunk\var\log\splunk\connect_health_metrics.log
- C:\Program Files\Splunk\var\log\splunk\secure_gateway.log
- C:\Program Files\Splunk\var\log\splunk\awesomemodules_input.log
- C:\Program Files\Splunk\var\log\splunkd.log
- C:\Program Files\Splunk\var\log\splunk\spunkd_access.log
- C:\Program Files\Splunk\var\log\splunk\ui_access.log
- OTHER

08:00 Fri Apr 12 2024 08:05 08:10 08:15 08:20 08:25 08:30 08:35 08:40 08:45 08:50 08:55

_time

_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\splunkd.log
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	
2024-04-12 07:59:00	64	40	261	

Statistics

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

New Search

index=_internal host="DESKTOP-B08BAAN" | timechart count by source limit=10

48,713 of 48,713 events matched No Event Sampling ▾

Save As ▾ Create Table View Close

1 hour window ▾

Events Patterns Statistics (61) Visualization

48,713 of 48,713 events matched No Event Sampling ▾

Job ▾ Job 1 2 3 4 Next >

20 Per Page ▾ Format

_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	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	

localhost:8000/en/GB/app/search/search?_search=index%2D%22internal%22%2Dhost%2D%22DESKTOP-B08BAAN%22%2Dtimechart%2Dcount%2Dby%2Dsource%2Dlimit%2D10&_display=page&search_mode=fact&dispatch_sample_ratio=1&workload_pool=8&lastest=1h&sorter=dispatch_by_page&search_showField=

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

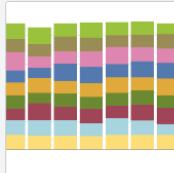


Chart Element

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.



Single Value Element

Create a single value viz with trend indicator, sparkline, and more.



Map Element

Plot geographical data on integrated maps.

Event
▶ 2013-09-24 10:44:14,325 INFO - user=admin action=login st session=cdd5562a68e829f5a132 userAgent="Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.116 Safari/537.36" clientip=127.0.0.1
▶ 2013-09-24 10:33:54,768 INFO - user=admin action=login st session=c254f000da40ba080000 userAgent="Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.116 Safari/537.36" clientip=127.0.0.1

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

Lorum ipsum dolor sit amet, test link odio libero nisi, impedit at, tincidunt nec, gravat, commodo vitae, feugiat in, nunc. Morbi HTML and CSS are our tools. Mauris a ant.

HTML Element

Include static HTML content. Useful for descriptions, links, and context.

Pivot Table

New Pivot

✓ 130,045 events (before 14/04/2024 21:52:23.000)

Save As... Clear Edit Dataset AccessData Documentation

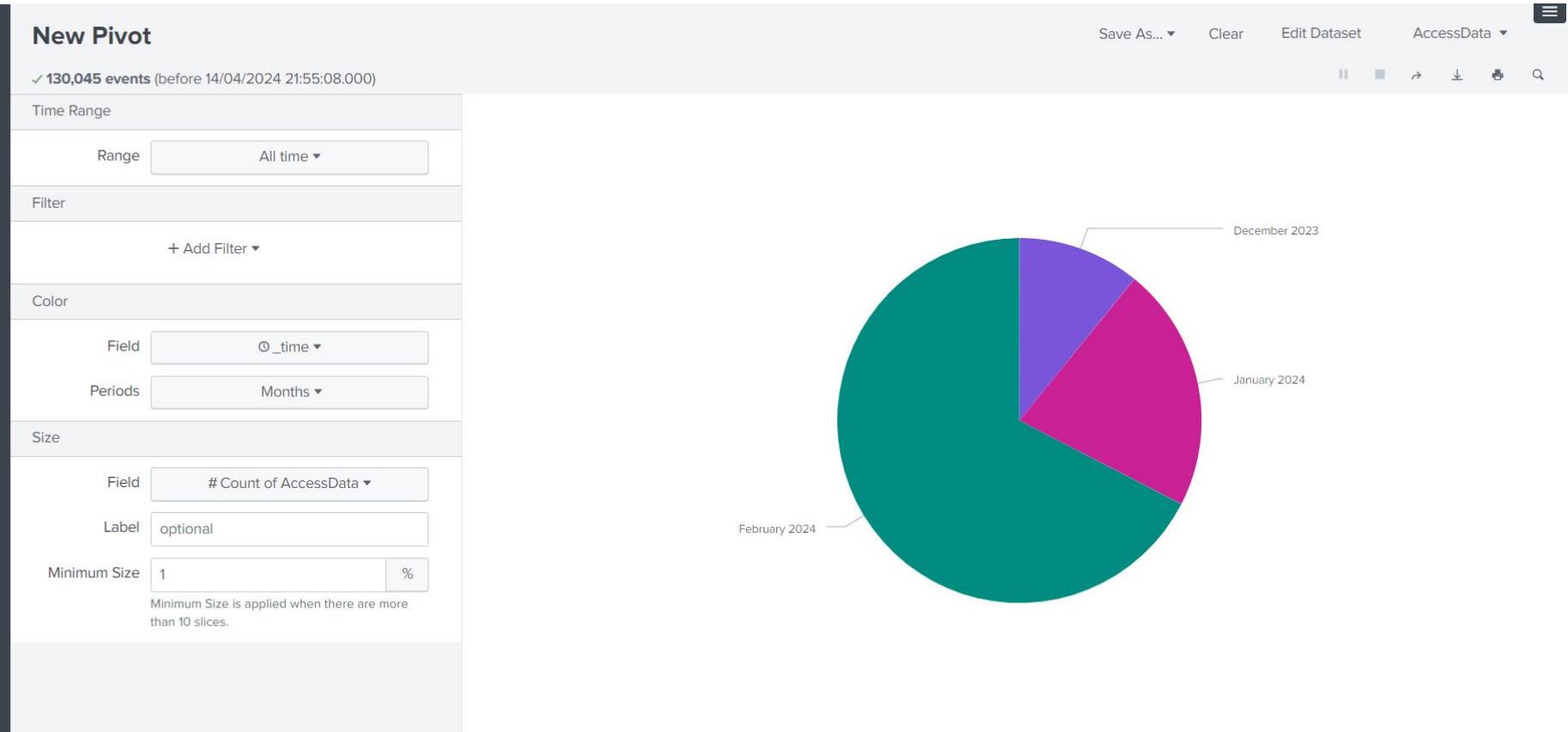
Filters

Split Columns

Column Values

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



Macros

New Search

index="price_index" table Name Price		Last 24 hours	Save As ▾	Create Table View	Close
✓ 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

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.

Validation Error Message Enter a message to display when the validation expression returns 'false'.

Cancel **Save**

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\$ <code>eval sale_price = \$Price\$ + 50</code>
<input type="checkbox"/> 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
<input type="button" value="Cancel"/> <input type="button" value="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 ▾ 

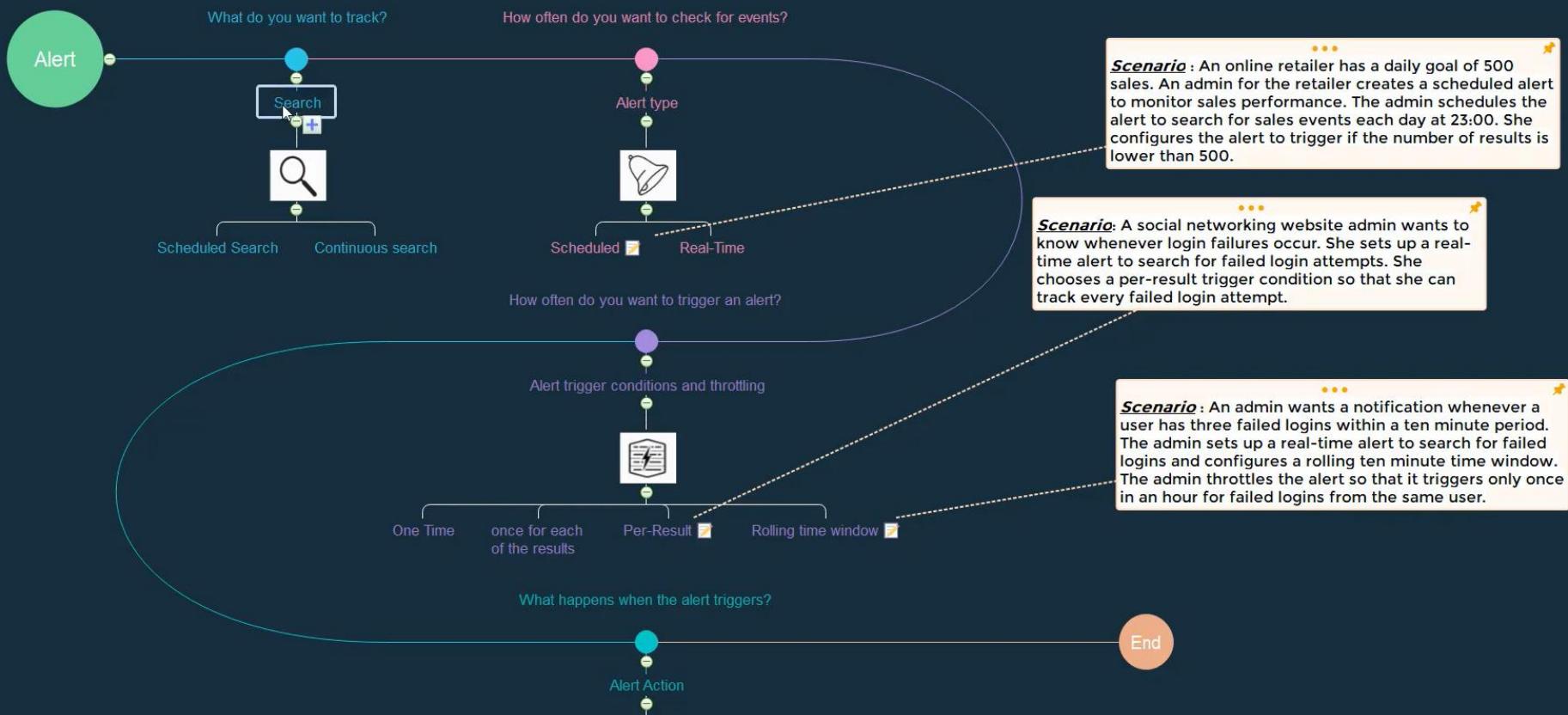
Events Patterns **Statistics (16)** Visualization Smart Mode ▾

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

localhost:8000/_api/GB

Alerts



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

08:00 Wed Apr 17 2024 12:00 16:00 20:00

0:00 10,000 20,000 30,000

08:00 12:00 16:00 20:00

0:00 10,000 20,000 30,000

List ▾ Format 20 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields All Fields

i	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

SELECTED FIELDS
a Country 30
CustomerID 100+
a Description 100+
a InvoiceDate 100+
InvoiceNo 100+
Quantity 4

Alerts

Save As Alert

X

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	Owner	Severity	Alert name	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



List ▾ Format 20 Per Page ▾

◀ Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields		All Fields		i Time	Event
SELECTED FIELDS				> 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
# CustomerID 100+				> 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
# InvoiceNo 100+				> 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
INTERESTING FIELDS				> 17/04/2024 20:16:00.000	423704,573152,21977,PACK OF 60 PINK Microsoft Teams CASES,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

X

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	Owner	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 ▾ Q 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 X Deselect 1 second per column

1 16:40:40 Wed Apr 17 2024 16:40:45 16:40:50 16:40:55 16:41:00 16:41:05 1

List ▾ Format 20 Per Page ▾

< Hide Fields ▪ All Fields

INTERESTING FIELDS

a component 2
date_hour 1
date_mday 1
date_minute 1
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

i	Time	Event
>	17/04/2024 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' 16:40:53.125
>	17/04/2024 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. 16:40:37.811

Real Time Alert

Save As Alert X

Settings

Title	InforealTimeAlert	
Description	Optional	
Permissions	Private	Shared in App
Alert type	Scheduled	Real-time
Expires	24	hour(s) ▾

Trigger Conditions

Trigger alert when	Number of Results ▾	
	is greater than ▾	0
in	5	minute(s) ▾
Trigger	Once	For each result
Throttle ?	<input checked="" type="checkbox"/>	

Cancel Save

Real Time Alert

Triggered Alerts

<input type="checkbox"/>	Time	Alert name	App	Type	Severity	Mode	Actions
<input type="checkbox"/>	2024-04-17 16:43:57 India Standard Time	InforealTimeAlert	EssilorApp	Real-time	● Medium	Per Result	View Results Edit Search Delete
<input type="checkbox"/>	2024-04-17 16:43:42 India Standard Time	InforealTimeAlert	EssilorApp	Real-time	● Medium	Per Result	View Results Edit Search Delete
<input type="checkbox"/>	2024-04-17 16:42:11 India Standard Time	UnitPriceAlert	EssilorApp	Scheduled	● Critical	Digest	View Results Edit Search Delete
<input type="checkbox"/>	2024-04-17 16:42:09 India Standard Time	QtyAlert	EssilorApp	Scheduled	● Medium	Digest	View Results Edit Search Delete
<input type="checkbox"/>	2024-04-17 16:40:09 India Standard Time	UnitPriceAlert	EssilorApp	Scheduled	● Critical	Digest	View Results Edit Search Delete

Email Settings

Server settings

Manage system settings including ports, host name, index path, email server, and system logging.

[General settings](#)

[Login background](#)

[Global banner](#)

[Internal Library Settings](#)

[Email settings](#)

[Server logging](#)

[Deployment client](#)

[Search preferences](#)

Email Settings

Edit Alert



Expires

24

hour(s) ▾

Trigger Conditions

Trigger alert when

Number of Results ▾

is greater than ▾

1

Trigger

Once

For each result

Throttle ?



Suppress triggering for

60

second(s) ▾

Trigger Actions

+ Add Actions ▾

When triggered



Add to Triggered Alerts

Remove

Severity

Medium ▾



Send email

Remove

Cancel

Save

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.

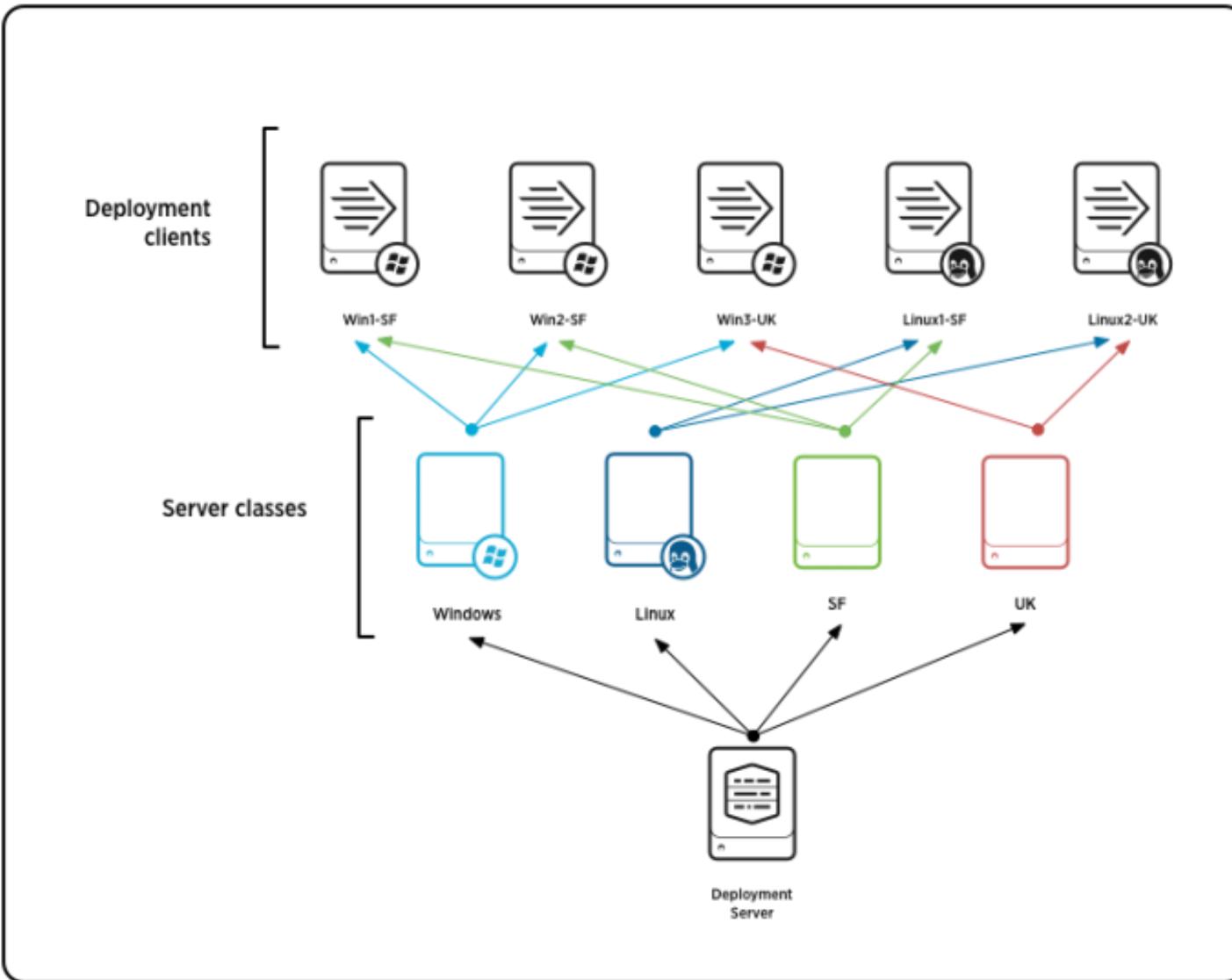
Deployment Server

- 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)

splunkbase™ Collections Apps

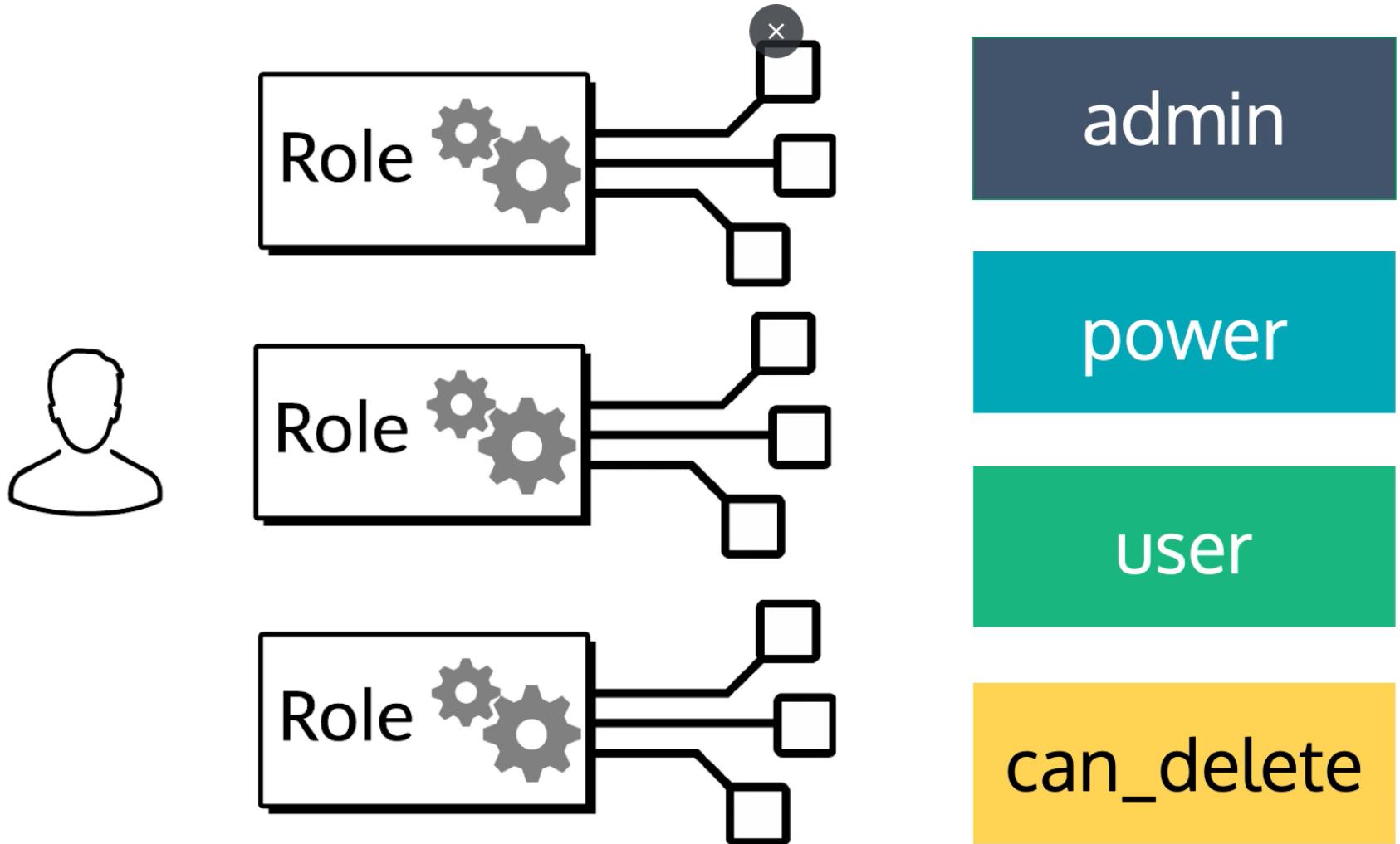
Find an app

[Submit an App](#)

CIM Splunk Common Information Model (CIM)
The Common Information Model is a set of field names and tags which are expected to define the least common denominator of a domain of interest. It is implemented as documentation on the Splunk docs website and JSON data model files in this add-on. Use the CIM add-on when...
Built by [Splunk Inc.](#)

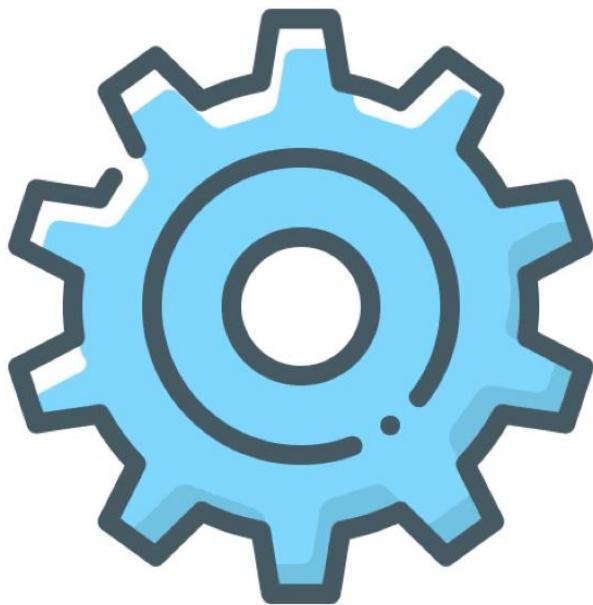
 [Download](#) [!\[\]\(e338d99edefc3916edc270ad6f6a51d9_img.jpg\)](#) [!\[\]\(0b759e369b253fa0ad2611ccce318bef_img.jpg\)](#)

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

Roles

New Role

Search...  5 Roles				
Name	Actions	Native Capabilities	Inherited Capabilities	Default App
admin	Edit ▾	121	39	
can_delete	Edit ▾	6	0	
power	Edit ▾	10	29	
splunk-system-role	Edit ▾	0	160	
user	Edit ▾	29	0	

Authentication

Edit User: eswaribala

X

Password must contain at least 8 characters

Time zone ? -- Default System Timezone --

Default app ? launcher (Home) ▾

Assign roles ? Available item(s)

admin
can_delete
db_connect_admin
db_connect_user
power

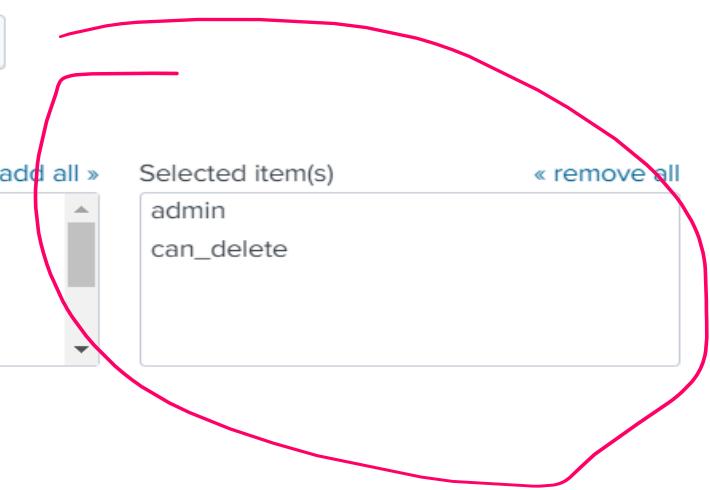
Selected item(s)

admin
can_delete

add all » « remove all

Require password change on next login

I acknowledge that users assigned to roles with the fsh_manage capability can send search results data outside the compliant environment.



Cancel Save

Authentication

Edit Role can_delete

X

<input type="checkbox"/>	db_connect_update_resource_pool	
<input type="checkbox"/>	db_connect_update_settings	
<input type="checkbox"/>	db_connect_use_custom_action	
<input type="checkbox"/>	db_connect_write_app_conf	
<input checked="" type="checkbox"/>	delete_by_keyword	native
<input type="checkbox"/>	delete_messages	
<input type="checkbox"/>	dispatch_rest_to_indexers	
<input type="checkbox"/>	edit_authentication_extensions	
<input type="checkbox"/>	edit_bookmarks_mc	
<input type="checkbox"/>	edit_cam_queue	
<input type="checkbox"/>	edit_certificates	
<input type="checkbox"/>	edit_cmd	
<input type="checkbox"/>	edit_deployment_client	
<input type="checkbox"/>	edit_deployment_server	
<input type="checkbox"/>	edit_dist_peer	

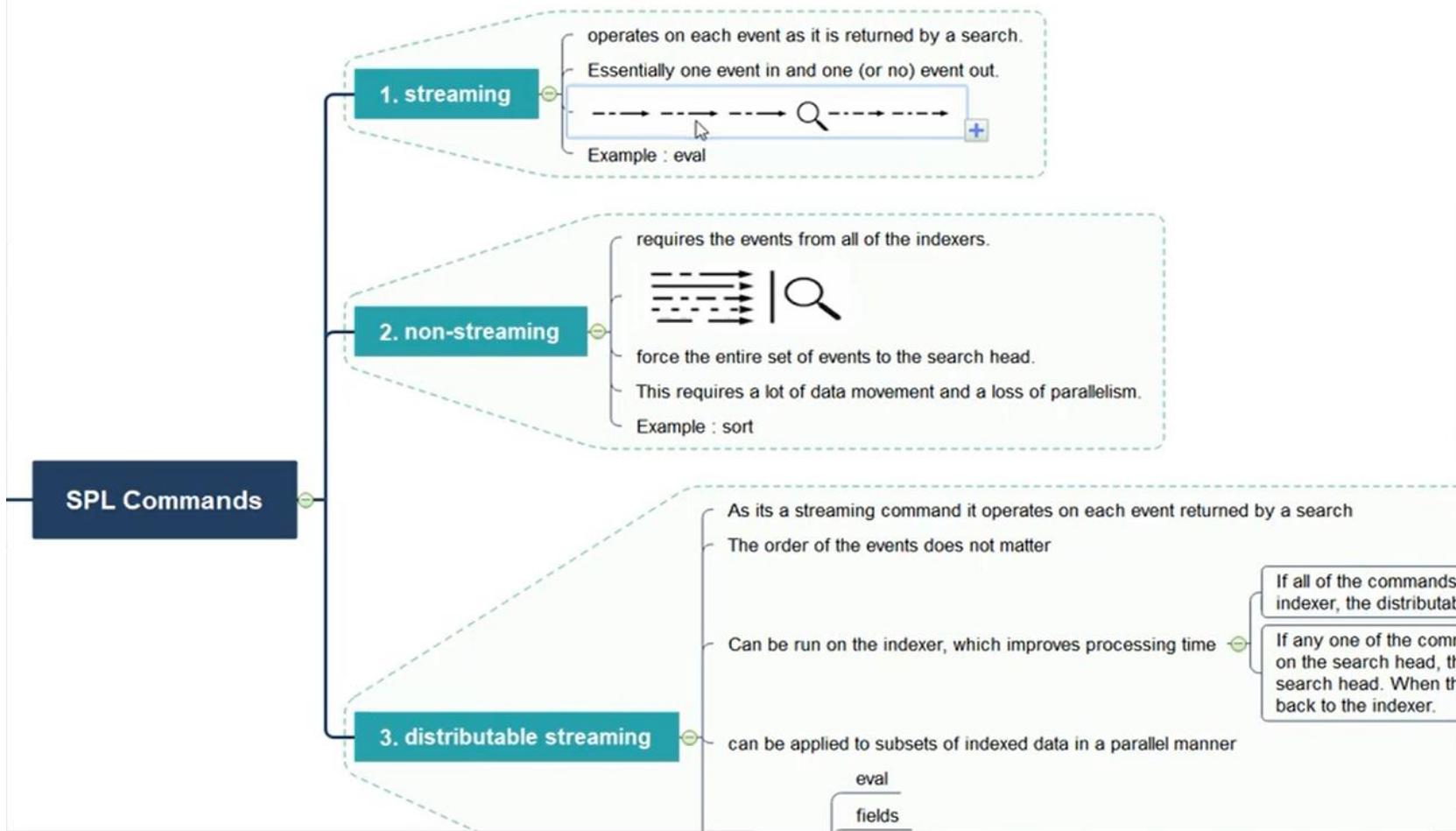
Cancel

Save

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

SPL Commands

3. distributable streaming

As its a streaming command it operates on each event returned by a search

The order of the events does not matter

Can be run on the indexer, which improves processing time

can be applied to subsets of indexed data in a parallel manner

Example

- eval
- fields
- makemv
- regex
- rename
- where

If all of the commands before the distributable streaming command can be run on the indexer, the distributable streaming command is run on the indexer.

If any one of the commands before the distributable streaming command must be run on the search head, the remaining commands in the search must be run on the search head. When the search processing moves to the search head, it cannot move back to the indexer.

Splunk Types of Commands

Input is event output is data table.
"transform" the specified cell values for each event into numerical values that Splunk software can use for statistical purposes

non-streaming in nature

transform search result data into the data structures that are required for visualizations

chart
timechart
stats
top
rare

5. transforming

Example

As its a streaming command it operates on each event returned by a search

the order of the events matters.

only works on the search head.

head

streamstats

some mode of dedup

4. centralized streaming

Example

Splunk Types of Commands

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.

redistribute

noop

Example

The lookup command also becomes an orchestrating command when you use it with the local=t argument.

7. orchestrating

fetches information from the indexes, without any transformations.

Generating commands are either event-generating (distributable or centralized) or report-generating

do not expect or require an input.

usually invoked at the beginning of the search

datamodel

pivot

tstats

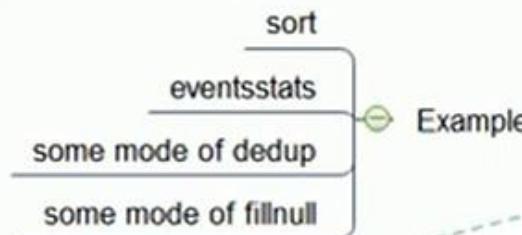
search

Example

6. generating

Splunk Types of Commands

require the entire dataset before the command can run.
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.



8. dataset processing

Splunk Types of Commands

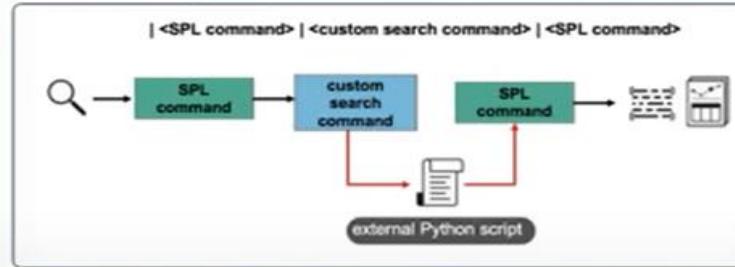
user defined SPL commands
extend SPL to serve your specific needs
we can implement custom search commands by creating Python scripts.
Custom search commands are designated by a stanza in the commands.conf file.

Splunk parses each line of SPL and determines whether the search command is custom.

If the search command is custom, Splunk executes the external Python script for the command.

Splunk pipes search results through this Python script in chunks via STDIN and writes them out over STDOUT.

After processing through the custom search command Python script, search results re-enter the main search pipeline.



Throughout the custom search command process, splunkd and the custom search command Python script exchange metadata through a series of getinfo and execute commands.

After all search results have passed through the external search command script, splunkd closes the STDIN pipe to terminate the process.

9. custom commands

how it works?

Search commands

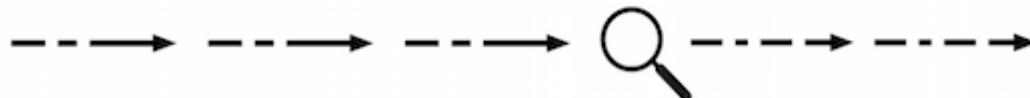
COMMAND	DESCRIPTION
chart, timechart	Returns results in a tabular output for (time-series) charting
dedup X	Removes duplicate results on a field X
eval	Calculates an expression (see Calculations)
fields	Removes fields from search results
head/tail N	Returns the first/last N results, where N is a positive integer
lookup	Adds field values from an external source
rename	Renames a field. Use wildcards (*) to specify multiple fields.
<u>rex</u>	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 <u>transactions</u>
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

Splunk > enterprise Apps ▾

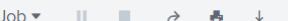
Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards TrainingApp

New Search Save As ▾ Create Table View Close

index="training_prices_index" | eval pricediff = price - sale_price

All time ▾ 

✓ 16 events (before 15/04/2024 21:18:05.000) No Event Sampling ▾ Job ▾  Smart Mode ▾

Events (16) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection X Deselect 1 millisecond per column

16
12
8
4

21:11:54.000 21:11:54.000 21:11:54.000 21:11:54.000 21:11:54.000 21:11:54.000 21:11:54.000 21:11:54.000 21:11:54.000 21:11:54.000

Mon Apr 15 2024

List ▾ Format 20 Per Page ▾

< Hide Fields : All Fields

SELECTED FIELDS

a Code 16
price 9
pricediff 5
a product_name 16
a productId 16
sale_price 8

i	Time	Event
>	15/04/2024 21:11:54.000	SF-BVS-01,Pony Run,49.99,41.99,P Code = P price = 49.99 pricediff = 8.00 productId = SF-BVS-01 product_name = Pony Run sale_price = 41.99
>	15/04/2024 21:11:54.000	SF-BVS-G01,Grand Theft Scooter,26.99,21.99,O Code = O price = 26.99 pricediff = 5.00 productId = SF-BVS-G01 product_name = Grand Theft Scooter sale_price = 21.99
>	15/04/2024 21:11:54.000	WC-SH-A02,Fire Resistance Suit of Provolone,3.99,1.99,N Code = N price = 3.99 pricediff = 2.00 productId = WC-SH-A02 product_name = Fire Resistance Suit of Provolone sale_price = 1.99

Creating new field in table using eval

New Search Save As ▾ Create Table View Close

```
index="employee_index" | eval full_name = first_name+" "+last_name | table first_name last_name full_name
```

All time Q

✓ 300,024 events (before 15/04/2024 22:05:44.000) No Event Sampling ▾ Job ▾ II ■ → ↻ 🔍 Smart Mode ▾

Events Patterns **Statistics (300,024)** Visualization

20 Per Page ▾ Format Preview ▾ ◀ Prev 1 2 3 4 5 6 7 8 ... Next >

first_name	last_name	full_name
Mong	Ohori	Mong Ohori
Uta	Docker	Uta Docker
Jianhui	Salverda	Jianhui Salverda
Mechthild	Melichar	Mechthild Melichar
Lihong	Barreiro	Lihong Barreiro
Adas	Harbusch	Adas Harbusch
Magy	Kermarrec	Magy Kermarrec
Kaijung	Heystek	Kaijung Heystek
Shalesh	Giveon	Shalesh Giveon
Jeong	Lorch	Jeong Lorch
Cedric	Zumaque	Cedric Zumaque

Creating new field in table using eval

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾

Search Analytics Datasets Reports Alerts Dashboards

CountryApp

New Search

Save As ▾ Create Table View Close

index="employee_index" | eval GenderType = case(gender="M","MALE",gender="F","FEMALE") | table first_name last_name GenderType

All time ▾

✓ 300,024 events (before 15/04/2024 22:23:21.000) No Event Sampling ▾ Job ▾ 1 2 3 4 5 6 7 8 ... Next >

Events Patterns Statistics (300,024) Visualization

20 Per Page ▾ Format Preview ▾

first_name	last_name	GenderType
Mong	Ohori	FEMALE
Uta	Docker	MALE
Jianhui	Salverda	FEMALE
Mechthild	Melichar	FEMALE
Lihong	Barreiro	MALE
Adas	Harbusch	FEMALE
Magy	Kermarrec	FEMALE
Kaijung	Heystek	MALE
Shalesh	Giveon	FEMALE
Jeong	Lorch	FEMALE

Creating new field in table using eval

New Search

Save As ▾ Create Table View Close

```
index="employee_index" | eval date=strptime(hire_date,"%Y-%m-%d")
| eval nowstring=now()
| eval experience=round(((nowstring-date)/ 86400) / 365.25)| table emp_no hire_date experience
```

All time ▾

✓ 300,024 events (before 15/04/2024 22:36:59.000) No Event Sampling ▾ Job ▾ II ■ ↻ 🔍 Smart Mode ▾

Events Patterns Statistics (300,024) Visualization

20 Per Page ▾ 1 2 3 4 5 6 7 8 ... Next >

emp_no	hire_date	experience
499999	1997-11-30	26
499998	1993-10-13	31
499997	1986-04-21	38
499996	1990-09-27	34
499995	1993-01-12	31
499994	1990-04-24	34
499993	1997-04-07	27
499992	1987-05-10	37
499991	1989-01-12	35
499990	1985-10-10	39

Creating new field in table using eval

New Search

Save As ▾ Create Table View Close

```
index="employee_index" | eval gender="M" | eval filterdate = strftime(hire_date,"%Y-%m-%d")
| eval today = strftime("1987-01-01","%Y-%m-%d")
| where filterdate <= today | table emp_no hire_date gender
```

All time ▾ 

✓ 71,548 events (before 15/04/2024 22:45:47.000) No Event Sampling ▾ Job ▾  Smart Mode ▾

Events Patterns Statistics (71,548) Visualization

20 Per Page ▾  Preview ▾  1 2 3 4 5 6 7 8 ... Next > 

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

Splunk > enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾

Search Analytics Datasets Reports Alerts Dashboards

CountryApp

New Search

Save As ▾ Create Table View Close

index="employee_index" | eval NameMatcher = if(like(first_name, "%"), "True", "False") | table first_name NameMatcher

All time ▾

✓ 300,024 events (before 15/04/2024 22:51:10.000) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events Patterns Statistics (300,024) Visualization

20 Per Page ▾ Format Preview ▾ 1 2 3 4 5 6 7 8 ... Next >

first_name	NameMatcher
Mong	False
Uta	False
Jianhui	False
Mechthild	False
Lihong	False
Adas	False
Magy	False
Kaijung	False
Shalesh	True
Jeong	False
Cedric	False

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

New Search

Save As ▾ Create Table View Close

index="training_prices_index" | sort Code | reverse All time ▾

✓ 16 events (before 15/04/2024 21:23:38.000) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events (16) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 millisecond per column

16 12 8 4

21:11:54.000 21:11:54.000 21:11:54.000 21:11:54.000 21:11:54.000 21:11:54.000 21:11:54.000 21:11:54.000 21:11:54.000 21:11:54.000

Mon Apr 15 2024

List ▾ 20 Per Page ▾

Time	Event
15/04/2024 21:11:54.000	SF-BVS-01,Pony Run,49.99,41.99,P Code = P price = 49.99 productId = SF-BVS-01 product_name = Pony Run sale_price = 41.99
15/04/2024 21:11:54.000	SF-BVS-G01,Grand Theft Scooter,26.99,21.99,O Code = O price = 26.99 productId = SF-BVS-G01 product_name = Grand Theft Scooter sale_price = 21.99
15/04/2024 21:11:54.000	WC-SH-A02,Fire Resistance Suit of Provolone,3.99,1.99,N Code = N price = 3.99 productId = WC-SH-A02 product_name = Fire Resistance Suit of Provolone sale_price = 1.99

< Hide Fields SELECTED FIELDS
a Code 16
price 9
a product_name 16
a productId 16
sale_price 8

Dedup commands

Splunk Enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards CountryApp

New Search

index="employee_index" | dedup gender

2 events (before 15/04/2024 23:03:52.000) No Event Sampling ▾

Events (2) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 millisecond per column

Time	Event
22:03:28.000 Mon Apr 15 2024	15/04/2024 22:03:28.000 499999, 1958-05-01, Sachin, Tsukuda, M, 1997-11-30 birth_date = 1958-05-01 emp_no = 499999 first_name = Sachin gender = M hire_date = 1997-11-30 last_name = Tsukuda
22:03:28.000	15/04/2024 22:03:28.000 499995, 1958-09-24, Dekang, Lichtner, F, 1993-01-12 birth_date = 1958-09-24 emp_no = 499995 first_name = Dekang gender = F hire_date = 1993-01-12 last_name = Lichtner

List ▾ Format 20 Per Page ▾

◀ Hide Fields :≡ All Fields i Time Event

SELECTED FIELDS
a birth_date 2
emp_no 2
a first_name 2
a gender 2
a hire_date 2
~ last_name 2

Stats distinct count commands

The screenshot shows the Splunk Enterprise search interface. At the top, the navigation bar includes the 'splunk>enterprise' logo and a 'Apps ▾' dropdown. Below the bar, the main menu has tabs for 'Search' (which is highlighted with a green underline), 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main content area is titled 'New Search'. In the search bar, the command `index="employee_index" | stats dc(gender) as GenderCount` is entered. Below the search bar, it says there are **300,024 events** (before 15/04/2024 23:11:41.000) and 'No Event Sampling ▾'. Under the search results, there are tabs for 'Events', 'Patterns', 'Statistics (1)' (which is underlined in blue), and 'Visualization'. Below these tabs, there are filters: '20 Per Page ▾', 'Format', and 'Preview ▾'. The search results table shows one row with the title 'GenderCount'. At the bottom left, the number '2' is displayed.

Stats distinct count commands

The screenshot shows the Splunk Enterprise search interface. At the top, the navigation bar includes the 'splunk>enterprise' logo and a 'Apps ▾' dropdown. Below the bar, the main menu has tabs for 'Search' (which is highlighted with a green underline), 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main content area is titled 'New Search'. In the search bar, the command `index="employee_index" | stats dc(gender) as GenderCount` is entered. Below the search bar, it says there are **300,024 events** (before 15/04/2024 23:11:41.000) and 'No Event Sampling ▾'. Under the search results, there are tabs for 'Events', 'Patterns', 'Statistics (1)' (which is underlined in blue), and 'Visualization'. Below these tabs, there are filters: '20 Per Page ▾', 'Format', and 'Preview ▾'. The search results table shows one row with the title 'GenderCount'. At the bottom left, there is a page number '2'.

Stats sum commands

The screenshot shows a search interface with the following details:

- New Search** button
- Search query: `index="price_index" | stats sum(sale_price) as Total_Sales_Price`
- Results summary: **✓ 16 events** (before 15/04/2024 23:14:01.000) | No Event Sampling
- Navigation tabs: Events, Patterns, **Statistics (1)**, Visualization
- List settings: 20 Per Page ▾, Format, Preview ▾
- Selected statistic: **Total_Sales_Price** (with a dropdown arrow)
- Value displayed: **270.84**

Stats sum commands

New Search

```
index="price_index" | stats avg(sale_price) as Average_Sales_Price
```

✓ 16 events (before 15/04/2024 23:14:50.000) No Event Sampling ▾

Events Patterns Statistics (1) Visualization

20 Per Page ▾ ✓ Format Preview ▾

Average_Sales_Price ▾

16.9275

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

Splunk > enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾

Search Analytics Datasets Reports Alerts Dashboards

CountryApp

New Search

Save As ▾ Create Table View Close

index="price_index" | head 10

All time ▾

✓ 10 events (before 15/04/2024 23:24:35.000) No Event Sampling ▾ Job ▾ 1 millisecond per column

Events (10) Patterns Statistics Visualization

Format Timeline ▾ 14 Apr 2024 20:51:18.001 10:00:00 0.001 seconds Sun Apr 14 2024

10 events at 20:51:18.000 on Sunday, April 14, 2024

List ▾ Format 20 Per Page ▾

Time	Event
14/04/2024 20:51:18.000	SF-BVS-01,Pony Run,49.99,41.99,P Code = P price = 49.99 productId = SF-BVS-01 product_name = Pony Run sale_price = 41.99
14/04/2024 20:51:18.000	SF-BVS-G01,Grand Theft Scooter,26.99,21.99,0 Code = O price = 26.99 productId = SF-BVS-G01 product_name = Grand Theft Scooter sale_price = 21.99

< Hide Fields SELECTED FIELDS
a Code 10
price 8
a product_name 10
a productId 10

Head Tail commands

Search Analytics Datasets Reports Alerts Dashboards App CountryApp

New Search Save As ▾ Create Table View Close

index="price_index" | tail 5 All time ▾ Smart Mode ▾

✓ 5 events (before 15/04/2024 23:25:12.000) No Event Sampling ▾ Job ▾ Zoom Out Zoom to Selection Deselect 1 millisecond per column

Events (5) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect

5
3
20:51:18.000 20:51:18.000 20:51:18.000 20:51:18.000 20:51:18.000 20:51:18.000 20:51:18.000 20:51:18.000 20:51:18.000 20:51:18.000 Sun Apr 14 2024

List ▾ Format 20 Per Page ▾

Hide Fields	All Fields	i Time	Event
SELECTED FIELDS a Code 5 # price 3 a product_name 5 a productId 5 # sale_price 4		> 14/04/2024 20:51:18.000	DB-SG-G01,Mediocre Kingdoms,24.99,19.99,A Code = A price = 24.99 productId = DB-SG-G01 product_name = Mediocre Kingdoms sale_price = 19.99
		> 14/04/2024 20:51:18.000	DC-SG-G02,Dream Crusher,39.99,24.99,B Code = B price = 39.99 productId = DC-SG-G02 product_name = Dream Crusher sale_price = 24.99
		> 14/04/2024 20:51:18.000	FS-SG-G03,Final Sequel,24.99,16.99,C Code = C price = 24.99 productId = FS-SG-G03 product_name = Final Sequel sale_price = 16.99

Regex commands

Splunk > enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾

Search Analytics Datasets Reports Alerts Dashboards

CountryApp

New Search

Save As ▾ Create Table View Close

index="employee_index" | regex first_name="^[A-Z][a-z]{8}" Last 24 hours 

✓ 27,173 events (14/04/2024 23:30:00.000 to 15/04/2024 23:53:08.000) No Event Sampling ▾ Job ▾  Smart Mode ▾

Events (27,173) Patterns Statistics Visualization

Format Timeline ▾    1 hour per column

30,000 20,000 10,000

00:00 Mon Apr 15 2024 06:00 12:00 18:00 30,000 20,000 10,000

00:00 Mon Apr 15 2024 06:00 12:00 18:00

List ▾  20 Per Page ▾          

Time	Event
15/04/2024 22:03:28.000	499989,1954-05-26,Keiichiro,Lindqvist,M,1993-10-28 birth_date = 1954-05-26 emp_no = 499989 first_name = Keiichiro gender = M hire_date = 1993-10-28 last_name = Lindqvist
15/04/2024 22:03:28.000	499979,1962-10-29,Prasadram,Waleschkowski,M,1994-01-04 birth_date = 1962-10-29 emp_no = 499979 first_name = Prasadram gender = M hire_date = 1994-01-04 last_name = Waleschkowski
15/04/2024	499978,1960-03-29,Chiranjit,Kuzuoka,M,1990-05-24

< Hide Fields  Time Event

SELECTED FIELDS
a birth_date 100+
emp_no 100+
a first_name 100+
a gender 2
a hire_date 100+

Regex commands

Search Analytics Datasets Reports Alerts Dashboards  CountryApp

New Search

index="employee_index" | regex emp_no="^[0-9]{5}\$"

Last 24 hours 

✓ 89,999 events (14/04/2024 23:30:00.000 to 15/04/2024 23:56:28.000) No Event Sampling ▾ Job 

Events (89,999) Patterns Statistics Visualization

Format Timeline ▾    1 hour per column

90,000
60,000
30,000

00:00 Mon Apr 15 2024 06:00 0 events at 08:00 on Monday, April 15, 2024 12:00 18:00

90,000
60,000
30,000

List  20 Per Page ▾ 1 Prev 2 3 4 5 6 7 8 ... Next >

< Hide Fields  Time Event

SELECTED FIELDS
a birth_date 100+
emp_no 100+
a first_name 100+
a gender 2
a hire_date 100+
a last_name 100+

Time	Event
15/04/2024 22:03:25.000	99999,1959-10-09,Gila,Lammel,M,1992-04-20 birth_date = 1959-10-09 emp_no = 99999 first_name = Gila gender = M hire_date = 1992-04-20 last_name = Lammel
15/04/2024 22:03:25.000	99998,1961-10-31,Parto,Lally,F,1995-03-03 birth_date = 1961-10-31 emp_no = 99998 first_name = Parto gender = F hire_date = 1995-03-03 last_name = Lally
15/04/2024 22:03:25.000	99997,1963-04-30,Mack,Morris,M,1995-01-08 birth_date = 1963-04-30 emp_no = 99997 first_name = Mack gender = M hire_date = 1995-01-08 last_name = Morris

Where commands

Splunk > enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾

Search Analytics Datasets Reports Alerts Dashboards

CountryApp

New Search

index="employee_index" | where first_name = "Sachin"

Last 24 hours ▾

232 events (14/04/2024 23:30:00.000 to 15/04/2024 23:58:30.000) No Event Sampling ▾

Events (232) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per column

00:00 Mon Apr 15 2024 06:00 12:00 18:00 250 150

00:00 15/04/2024 23:58:30.000 250

List ▾ Format 20 Per Page ▾ 1 2 3 4 5 6 7 8 ... Next >

Time	Event
15/04/2024 22:03:28.000	499999, 1958-05-01, Sachin, Tsukuda, M, 1997-11-30 birth_date = 1958-05-01 emp_no = 499999 first_name = Sachin gender = M hire_date = 1997-11-30 last_name = Tsukuda
15/04/2024 22:03:27.000	499452, 1962-03-08, Sachin, Baja, F, 1990-01-14 birth_date = 1962-03-08 emp_no = 499452 first_name = Sachin gender = F hire_date = 1990-01-14 last_name = Baja
15/04/2024 22:03:27.000	498737, 1953-06-27, Sachin, Schaap, F, 1988-07-11 birth_date = 1953-06-27 emp_no = 498737 first_name = Sachin gender = F hire_date = 1988-07-11 last_name = Schaap
15/04/2024 22:03:27.000	494048, 1964-06-25, Sachin, Decler, F, 1989-09-02

◀ Hide Fields ⌂ All Fields i Time Event

SELECTED FIELDS
a birth_date 100+
emp_no 100+
a first_name 1
a gender 2
a hire_date 100+
a last_name 100+

INTERESTING FIELDS

Delete commands (Refer can_delete)

Splunk > enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾

Search Analytics Datasets Reports Alerts Dashboards

CountryApp

New Search

index="employee_index" | where first_name = "Sachin" | delete

Last 24 hours ▾

232 events (14/04/2024 23:30:00.000 to 15/04/2024 23:59:14.000) No Event Sampling ▾

Job ▾

Events Patterns Statistics (2) Visualization

20 Per Page ▾ Format Preview ▾

splunk_server	index	deleted	errors
DESKTOP-B08BAAN	_ALL_	232	0
DESKTOP-B08BAAN	employee_index	232	0

Where commands

New Search

index="employee_index" | where first_name = "Sachin"

Save As ▾ Create Table View Close

Last 24 hours ▾

✓ 0 events (14/04/2024 23:30:00.000 to 16/04/2024 00:00:03.000) No Event Sampling ▾

Job ▾ Smart Mode ▾

Events (0) Patterns Statistics Visualization

No results found. Try expanding the time range.

Lookup

Lookup table files

New Lookup Table File

Lookups » Lookup table files

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	Search	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 ▾

1

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

New Search

```
source="dept_emp.csv" host="DESKTOP-B08BAAN" index="dept_emp_index" sourcetype="csv"
```

✓ 331,603 events (before 17/04/2024 06:38:45.000)

No Event Sampling ▾

Join

Events (331,603)

Patterns

Statistics

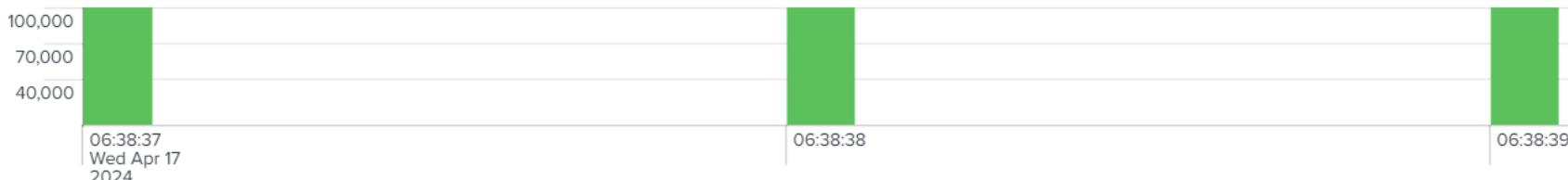
Visualization

Format Timeline ▾

– Zoom Out

+ Zoom to Selection

✖ Deselect



List ▾

✓ Format

20 Per Page ▾

◀ Prev

1

◀ Hide Fields

☰ All Fields



Time

Event

SELECTED FIELDS
a dept_no 9
emp_no 100+
a from_date 100+
a to_date 100+



17/04/2024

06:38:40.000

499999,d004,1997-11-30,9999-01-01

dept_no = d004 | emp_no = 499999 | from_date = 1997-11-30 | to_date = 9999-01-01



17/04/2024

06:38:40.000

499998,d002,1993-12-27,9999-01-01

dept_no = d002 | emp_no = 499998 | from_date = 1993-12-27 | to_date = 9999-01-01

Lookup Definition

deptnamelookup

Lookups » Lookup definitions » deptnamelookup

Type	<input type="text" value="File-based"/>	<input type="button" value="▼"/>
Lookup file *	<input type="text" value="departments.csv"/>	<input type="button" value="▼"/>
Create and manage lookup table files.		
<input type="checkbox"/> Configure time-based lookup		
<input checked="" type="checkbox"/> Advanced options		
Minimum matches	<input type="text" value="1"/>	
The minimum number of matches for each input lookup value. Default is 0.		
Maximum matches	<input type="text" value="1000"/>	
Enter a number from 1-1000 to specify the maximum number of matches for each lookup value. If time-based, default is 1; otherwise, default is 100.		
Default matches	<input type="text" value="NoInputMatches"/>	
When fewer than the minimum number of matches are present for any given input, the Splunk software provides this value one or more times until the minimum is reached.		
<input checked="" type="checkbox"/> Case sensitive match		
Perform case sensitive matching for all lookup table fields.		
<input type="checkbox"/> Batch index query		
If you are working with a large lookup file, select this to improve search performance by grouping index queries.		

Lookup Definition

Lookup definitions			
Lookups » Lookup definitions			
Showing 1-1 of 1 item			
App	CountryApp (CountryA... ▾)	Configuration Source	Visible in the App ▾
Owner	Any		
Name ▾	Type ▾	Supported fields ▾	Lookup file ▾
deptnamelookup	file	dept_no,dept_name	departments.csv

Lookup command

splunk>enterprise Apps ▾ Administrator ▾

Search Analytics Datasets Reports Alerts Dashboards

New Search

```
index="dept_emp_index" | lookup deptname lookup dept_no OUTPUT dept_name
```

✓ 331,603 events (before 17/04/2024 06:51:58.000) No Event Sampling ▾

Events (331,603) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

100,000
70,000
40,000

06:38:37
Wed Apr 17
2024

06:38:38

06:38:39

List ▾ Format 20 Per Page ▾

< Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS a dept_no 9 # emp_no 100+ a from_date 100+ a to_date 100+		>	17/04/2024 06:38:40.000	499999, d004, 1997-11-30, 9999-01-01 dept_no = d004 emp_no = 499999 from_date = 1997-11-30 to_date = 9999-01-01
		>	17/04/2024 06:38:40.000	499998, d002, 1993-12-27, 9999-01-01 dept_no = d002 emp_no = 499998 from_date = 1993-12-27 to_date = 9999-01-01
		>	17/04/2024 06:38:40.000	499997, d005, 1987-08-30, 9999-01-01 dept_no = d005 emp_no = 499997 from_date = 1987-08-30 to_date = 9999-01-01

INTERESTING FIELDS
a dept_name 9

Lookup command

Splunk > enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾

Search Analytics Datasets Reports Alerts Dashboards

New Search Save As ▾

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

✓ 331,603 events (before 17/04/2024 06:51:58.000) No Event Sampling ▾ Job ▾

Events (331,603) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect

100,000
70,000
40,000

06:38:37 Wed Apr 17 2024 06:38:38 06:38:39

List ▾ Format 20 Per Page ▾

◀ Hide Fields ▶ All Fields

i	Time	Event
>	17/04/2024 06:38:40.000	499999, d004, 1997-11-30, 9999-01-01 dept_name = Production dept_no = d004 emp_no = 499999 from_date = 1997-11-30 to_date = 9999-01-01
>	17/04/2024 06:38:40.000	499998, d002, 1993-12-27, 9999-01-01 dept_name = Finance dept_no = d002 emp_no = 499998 from_date = 1993-12-27 to_date = 9999-01-01
>	17/04/2024 06:38:40.000	499997, d005, 1987-08-30, 9999-01-01 dept_name = Development dept_no = d005 emp_no = 499997 from_date = 1987-08-30 to_date = 9999-01-01

SELECTED FIELDS
a dept_name 9
a dept_no 9
emp_no 100+
a from_date 100+
a to_date 100+

INDETECTING FIELDS

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

splunkbase™

Collections

Apps

Find an app

Submit an App

PB



Enterprise Security Configuration Explorer

This App makes it easy to get an overview of all the critical pieces of your Enterprise Security installation such as Correlation Searches, Risk, Risk Factors, etc.

Built by [Arcus Data](#)



Download



Correlation Search

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Correlation Search Explorer Risk ▾ Other ▾ ES Configuration Explorer

Correlation Search Explorer

Author App Exclude ESCU Risk Rules Only Status Real-Time

All All True False All All

Search produced no results.

Uses MLTK Name Search Search Search

All * * Hide Filters

Enabled Correlation Searches Disabled Correlation Searches Enabled Real-Time Correlation Searches Disabled Real-Time Correlation Searches

0 0 0 0

Correlation Searches (Click to Edit)

EventStats

splunk>enterprise Apps ▾

Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾

Search Analytics Datasets Reports Alerts Dashboards

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 ▾ II ⌂ ⌂ ⌂ ⌂ Smart Mode ▾

Events Patterns Statistics (10,000) Visualization

20 Per Page ▾ Format Preview ▾

hire_date ▾  emp_count ▾ 

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

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| streamstats count(emp_no) as emp_count by hire_date | table hire_date emp_count

All time ▾

✓ 10,000 events (before 16/04/2024 07:58:32.000) No Event Sampling ▾ Job ▾ II ⌂ ↗ ↘ Smart Mode ▾

Events Patterns Statistics (10,000) Visualization

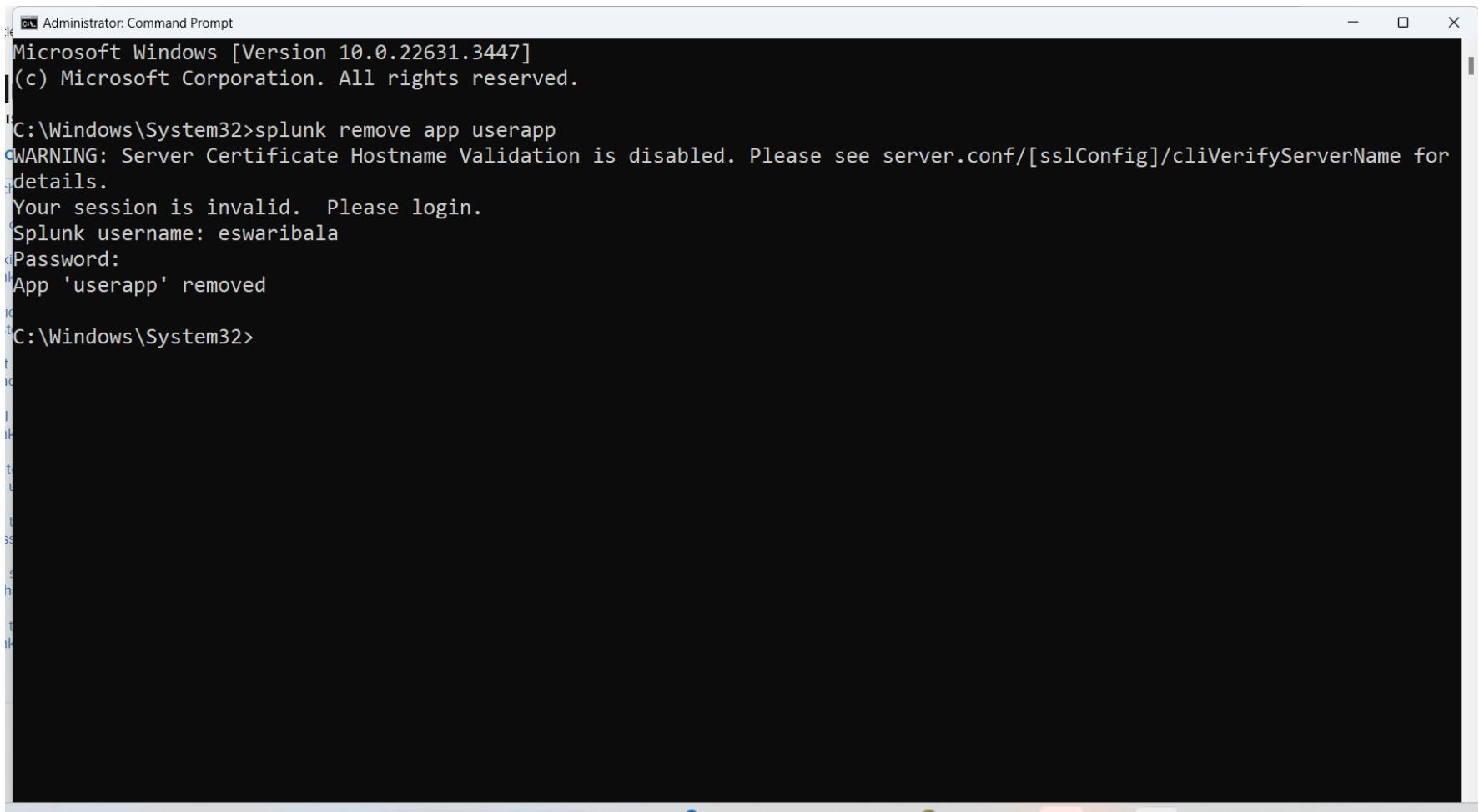
20 Per Page ▾ Format Preview ▾

hire_date ↴ emp_count ↴

hire_date	emp_count
1985-01-01	1
1985-01-01	2
1985-01-01	3
1985-01-01	4
1985-01-01	5
1985-01-01	6
1985-01-01	7
1985-01-01	8
1985-01-01	9
1985-01-14	1
1985-02-01	1

localhost:8000/en-GB

Delete App



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The window displays the following command-line session:

```
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 > enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards TrainingApp

New Search

index="access_big_index" IpAddress=178.115.128.71 | streamstats count as newcount |

58 events (before 15/04/2024 20:54:08.000) No Event Sampling Save As ▾ Create Table View Close All time ▾

Events (58) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 second per column

16 12 8 4

02:28:10 Wed Feb 21 2024

02:28:20 02:28:30 02:28:40 02:28:50

List ▾ Format 20 Per Page ▾ 1 2 3 Next >

16 12 8 4

02:28:10 Wed Feb 21 2024

02:28:20 02:28:30 02:28:40 02:28:50

1 2 3 Next >

Splunk Http Event Collector

HTTP Event Collector					
Data Inputs x HTTP Event Collector				Global Settings	New Token
3 Tokens	App: All ▾	filter	Actions	Source Type	Index
db-connect-http-input	Edit Disable Delete	a550375e-4a49-46d1-a3e1-16e36267f9f6		Default	Enabled
httpdemo	Edit Disable Delete	57b8ce6b-ce8b-4007-94f7-7f96ae6993c8		main	Enabled
HttpEventCollector	Edit Disable Delete	6383193b-2e4d-4e9c-b5e3-ca0802c3e42e	_json	inventoryapi_index	Enabled

Splunk Http Event Collector

Edit Token: HttpEventCollector



Description	optional	
Source	optional	
Set Source Type	Entered sourcetype ▾	
Source Type	_json ▾	
Select Allowed Indexes (optional)	Available indexes <input type="checkbox"/> access <input type="checkbox"/> access_index <input type="checkbox"/> cim_modactions <input type="checkbox"/> country_index <input type="checkbox"/> countryv1_index	Selected indexes « remove all <input checked="" type="checkbox"/> inventoryapi_index
	Select indexes that clients will be able to select from.	
Default Index	<input checked="" type="checkbox"/> inventoryapi_index ▾	
Output Group (optional)	None ▾	
Enable indexer acknowledgement	<input type="checkbox"/>	

Cancel

Save

Splunk Http Event Collector

HTTP <http://localhost:8088/services/collector> Save

POST [▼](#) http://localhost:8088/services/collector

Params	Authorization	Headers (10)	Body	Pre-request Script	Tests	Settings
<input checked="" type="checkbox"/>	Accept-Encoding			gzip, deflate, br		
<input checked="" type="checkbox"/>	Connection			keep-alive		
<input checked="" type="checkbox"/>	Authorization			Splunk 6383193b-2e4d-4e9c-b5e3-ca0802c3e42e		
<input checked="" type="checkbox"/>	Content-Type			application/json		
	Key		Value		Description	

Splunk Http Event Collector

The screenshot shows the Postman application interface. At the top, there is a header bar with tabs for 'GET http://localhost:7074/pa...', 'POST http://localhost:8088C...', 'POST http://localhost:8088/...', and a '+' button. To the right of the tabs, it shows the IP address '172.19.48.1'. Below the header, the URL 'http://localhost:8088/services/collector' is selected in the 'HTTP' dropdown.

The main area is a POST request configuration. The method is set to 'POST' and the URL is 'http://localhost:8088/services/collector'. The 'Body' tab is selected, showing the following JSON payload:

```
1 {  
2   ... "event": "hi",  
3   ... "sourcetype": "manual"  
4 }
```

Below the body, there are tabs for 'Params', 'Authorization', 'Headers (10)', 'Pre-request Script', 'Tests', 'Settings', 'Cookies', and 'Beautify'. The 'Body' tab is currently active. The 'JSON' dropdown at the bottom of the body section is also set to 'Pretty'.

At the bottom of the interface, there are tabs for 'Body', 'Cookies', 'Headers (8)', and 'Test Results'. The 'Body' tab is active. On the right side, there is status information: 'Status: 200 OK', 'Time: 3 ms', 'Size: 274 B', and a 'Save as example' button. There are also icons for 'Pretty', 'Raw', 'Preview', 'Visualize', and a search bar.

Splunk Http Event Collector

New Search

index="inventoryapi_index"

236 events (before 16/04/2024 21:30:26.000) No Event Sampling ▾

Events (236) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 1 hour per column

17:00 18:00 19:00 20:00 21:00

Tue Apr 16 2024

List ▾ ✎ Format 20 Per Page ▾ 1 2 3 4 5 6 7 8 ... Next >

Time	Event
16/04/2024 21:30:19.902	{ [-] Level: Information MessageTemplate: Request finished {Protocol} {Method} {Scheme}://{Host}{PathBase}{Path}{QueryString} - {StatusCode} {ContentLength} {ContentType} {ElapsedMilliseconds}ms Properties: { [+]} } RenderedMessage: Request finished "HTTP/2" "GET" "https://localhost:44322"""/api/v1/Products"" - 200 null "application/json; charset=utf-8; x-api-version=1" 4803.2928ms } Show as raw text index = inventoryapi_index

< Hide Fields :≡ All Fields

SELECTED FIELDS
a index 1

INTERESTING FIELDS
a host 1
a Level 2
linecount 1
a MessageTemplate 68
a Properties.ActionId 2
a Properties.ActionName 1
Properties.EventId.Id 40

Splunk clean dispatch – too many queries

```
Administrator: Command Prompt
C:\Program Files\Splunk\bin>splunk cmd splunkd clean-dispatch C:\Users\Dell\AppData\Local\Temp\splunkdispatch -2d
Using logging configuration at C:\Program Files\Splunk\etc\log-cmdline.cfg.
dispatch dir:      C:\Program Files\Splunk\var\run\splunk\dispatch
destination dir:   C:\Users\Dell\AppData\Local\Temp\splunkdispatch
earliest mod time: 2024-04-16T05:26:44.000+05:30

total: 6396, moved: 2, failed: 0, remaining: 6394 job directories from C:\Program Files\Splunk\var\run\splunk\dispatch to C:\Users\Dell\AppData\Local\Temp\splunkdispatch

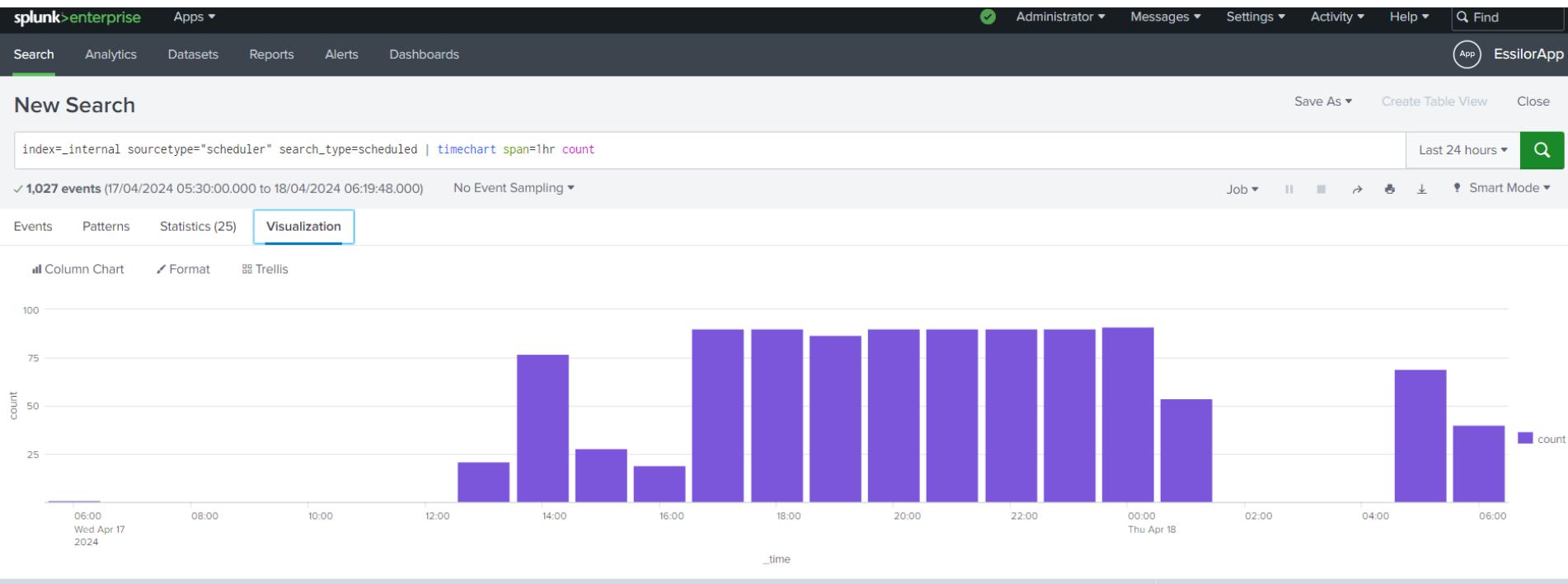
C:\Program Files\Splunk\bin>
```

Splunk clean dispatch – too many queries

File Explorer View				
	Name	Date modified	Type	Size
	1713401141.11	18-04-2024 06:15	File folder	
	1713401154.13	18-04-2024 06:16	File folder	
	alertsmanager_1713400983.1	18-04-2024 06:13	File folder	
	rt_md_1713401085.3	18-04-2024 06:16	File folder	
	rt_md_1713401115.9	18-04-2024 06:16	File folder	
	rt_md_1713401165.14	18-04-2024 06:17	File folder	
	rt_md_1713401183.15	18-04-2024 06:18	File folder	
	scheduler_eswaribala_EssilorApp_QtyA...	18-04-2024 06:15	File folder	
	subsearch_scheduler_nobody_c3BsdW5r...	18-04-2024 06:13	File folder	

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]

The screenshot shows the Splunk Enterprise search interface. The search bar contains the command: `index="employee_index" | table emp_no hire_date | join type=inner emp_no [| search index="dept_emp_index" | fields emp_no dept_no]`. Below the search bar, it says "299,792 events (before 18/04/2024 06:37:10.000) No Event Sampling". The results table has columns: emp_no, hire_date, and dept_no. The data is as follows:

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

