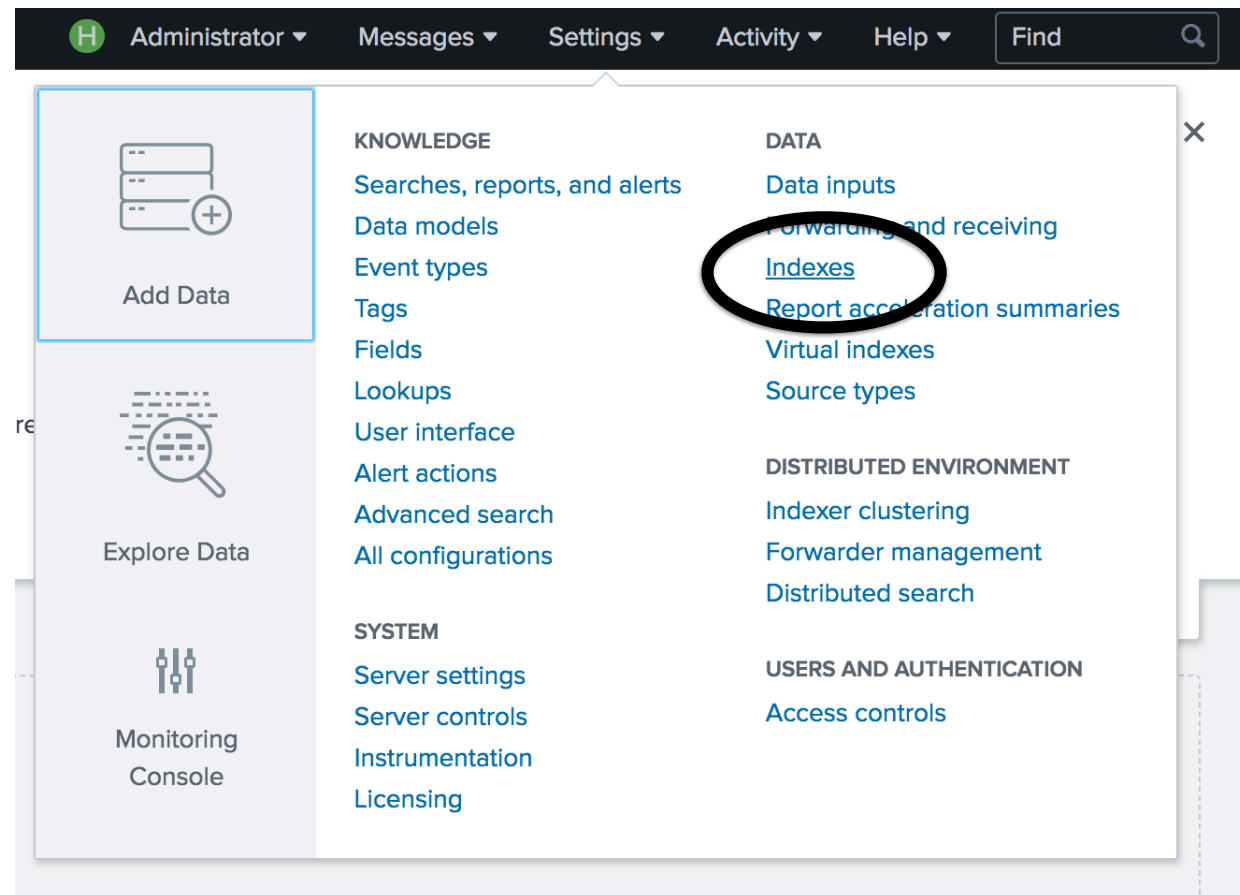


Start by Creating an Index

- For the lab, this can be done in the WebUI
- In a distributed environment, this is typically managed in an app



Creating an Index

splunk>enterprise

Apps ▾

Indexes

A repository for data in Splunk Enterprise. Indexes reside in files.

11 Indexes

filter

Name ▲	Actions	Type ▾
_audit	Edit Delete Disable	Events
_internal	Edit Delete Disable	Events
_introspection	Edit Delete Disable	Events
_telemetry	Edit Delete Disable	Events
_thefishbucket	Edit Delete Disable	Events
firedalerts	Edit Delete Disable	Events
history	Edit Delete Disable	Events
main	Edit Delete Disable	Events
os	Edit Delete Disable	Events
splunklogger	Edit Delete Enable	Events
summary	Edit Delete Disable	Events

New Index

General Settings

Index Name

os

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.

Max Size of Hot/Warm/Cold Bucket

auto

GB ▾

Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path

optional

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

App

Search & Reporting ▾

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

Days ▾

Cancel

Save

Messages ▾

Settings ▾

Activity ▾

Help ▾

Find



New Index

20 per page ▾

Home Path ▾	Frozen Path ▾	Status ▾
\$SPLUNK_DB/audit/db	N/A	✓ Enabled
\$SPLUNK_DB/_internaldb/db	N/A	✓ Enabled
\$SPLUNK_DB/_introspection/db	N/A	✓ Enabled
\$SPLUNK_DB/_telemetry/db	N/A	✓ Enabled
\$SPLUNK_DB/fishbucket/db	N/A	✓ Enabled
\$SPLUNK_DB/firedalerts/db	N/A	✓ Enabled
\$SPLUNK_DB/historydb/db	N/A	✓ Enabled
\$SPLUNK_DB/defaultdb/db	N/A	✓ Enabled
\$SPLUNK_DB/os/db	N/A	✓ Enabled
\$SPLUNK_DB/splunklogger/db	N/A	🔴 Disabled
\$SPLUNK_DB/summarydb/db	N/A	✓ Enabled

Import Data

- Let's tell Splunk to monitor data on our system

The screenshot displays the Splunk web interface. At the top is a navigation bar with links for Administrator, Messages, Settings, Activity, and Help, along with a search bar. The left sidebar contains three main sections: 'Add Data' (highlighted with a blue border), 'Explore Data', and 'Monitoring Console'. The 'Add Data' section is further divided into 'KNOWLEDGE' (Searches, reports, and alerts; Data models; Event types; Tags; Fields; Lookups; User interface; Alert actions; Advanced search; All configurations) and 'SYSTEM' (Server settings; Server controls; Instrumentation; Licensing). The main content area is titled 'Add Data' and asks 'How do you want to add data?'. It features three options: 'Upload' (files from my computer), 'Monitor' (files and ports on this Splunk indexer, highlighted with a grey border), and 'Forward' (data from Splunk forwarder). The 'Monitor' option is selected, showing details for adding data from local files or external sources.

Add Data

How do you want to add data?

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 - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources

Forward
data from Splunk forwarder
Files - TCP/UDP - Scripts

Import Data From File

- Select “Files & Directories”, and locate the file

The screenshot displays the Splunk Enterprise 'Add Data' configuration page. The top navigation bar includes the Splunk logo, 'enterprise' branding, and various menu items like 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below the navigation bar, a progress bar indicates the current step is 'Select Source'. The left sidebar lists three data source categories: 'Files & Directories' (highlighted with a grey box), 'HTTP Event Collector', and 'TCP / UDP'. The 'Files & Directories' section is expanded, showing a description: 'Upload a file, index a local file, or monitor an entire directory.' The main content area contains instructions for configuring file monitoring and a form to specify the file or directory. The 'File or Directory ?' field is populated with '/var/log/auth.log', and the 'Browse' button next to it is highlighted with a grey box. Below this, the 'Continuously Monitor' radio button is selected and highlighted with a grey box, while the 'Index Once' button is unselected. Further down, there are input fields for 'Whitelist ?' and 'Blacklist ?'. At the bottom, a 'FAQ' section is partially visible with the question '> What kinds of files can Splunk index?'. On the right side of the interface, a 'Select source' panel is open, showing a list of system paths. The 'log' directory is expanded, and 'auth.log' is highlighted in blue. Below this list, the path '/var/log/auth.log' is entered into a text field.

Select source

- ☒ siv
- ☐ sys
- ☐ tmp
- ☐ usr
- ☒ var
 - ☐ backups
 - ☐ cache
 - ☐ crash
 - ☐ lib
 - ☐ local
 - ☐ lock
 - ☒ log
 - ☐ apt
 - ☐ dist-upgrade
 - ☐ fsck
 - ☐ lxd
 - ☒ unattended-upgrades
 - alternatives.log
 - alternatives.log.1
 - auth.log**
 - auth.log.1
 - btmpt
 - btmpt.1
 - cloud-init-output.log
 - cloud-init.log
 - dpkg.log
 - dpkg.log.1
 - kern.log
 - kern.log.1
 - lastlog
 - syslog
 - syslog.1
 - syslog.2.gz

Add Data

Select Source Set Source Type Input Settings Review Done

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 Splunk to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. Splunk 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 ?

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

☒ Continuously Monitor ☐ Index Once

Whitelist ?

Blacklist ?

FAQ

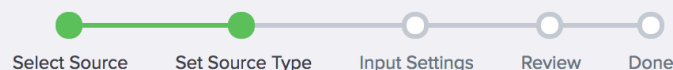
> What kinds of files can Splunk index?

var

- ☐ backups
- ☐ cache
- ☐ crash
- ☐ lib
- ☐ local
- ☐ lock
- ☒ log
 - ☐ apt
 - ☐ dist-upgrade
 - ☐ fsck
 - ☐ lxd
 - ☒ unattended-upgrades
 - alternatives.log
 - alternatives.log.1
 - auth.log**
 - auth.log.1
 - btmpt
 - btmpt.1
 - cloud-init-output.log
 - cloud-init.log
 - dpkg.log
 - dpkg.log.1
 - kern.log
 - kern.log.1
 - lastlog
 - syslog
 - syslog.1
 - syslog.2.gz

/var/log/auth.log

- ## Add Data

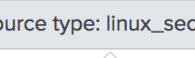


[← Back](#)

Next >

This page lets you see how Splunk sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: /var/log/auth.log

[View Event Summary](#)

Source type: linux_secure ▼

linux_secure ✕

✓ linux_secure
Format for the /var/log/secure file containing all security related messages on a Linux machine

List ▾

Format

20 Per Page ▾

< Prev

1

2

3

4

5

6

7

8

...

Next >

	Time	Event
1	4/29/18 6:25:01.000 AM	Apr 29 06:25:01 ip-10-129-0-145 CRON[19458]: pam_unix(cron:session): session closed for user root
2	4/29/18 6:25:02.000 AM	Apr 29 06:25:02 ip-10-129-0-145 sshd[19456]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=123.183.209.133 user=root
3	4/29/18 6:25:04.000 AM	Apr 29 06:25:04 ip-10-129-0-145 sshd[19456]: Failed password for root from 123.183.209.133 port 11900 ssh2
4	4/29/18 6:25:09.000 AM	Apr 29 06:25:09 ip-10-129-0-145 sshd[19456]: message repeated 2 times: [Failed password for root from 123.183.209.133 port 11900 ssh2]
5	4/29/18	Apr 29 06:25:10 ip-10-129-0-145 sshd[19456]: Received disconnect from 123.183.209.133 port 1

Set Host and Index

- On a production system, we would typically configure this in an inputs app (I'll show you this in a bit)

Add Data

< Back

Review >

Input Settings

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

App context

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

App Context

Search & Reporting (search) ▼

Host

When Splunk 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

my_hostname

Index

Splunk stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting

Index

os ▼

Create a new index

Yay! You're Almost Done

- Click submit to finish, then start searching!

Add Data

Select SourceSet Source TypeInput SettingsReviewDone

< Back

Submit >

Review

Input Type File Monitor
Source Path /var/log/auth.log
Continuously Monitor Yes
Source Type linux_secure
App Context search
Host my_hostname
Index os

✓

File input has been created successfully.
Configure your inputs by going to Settings > [Data Inputs](#)

Start Searching

Search your data now or see [examples and tutorials](#). [🔗](#)

Extract Fields

Create search-time field extractions. [Learn more about fields](#). [🔗](#)

Add More Data

Add more data inputs now or see [examples and tutorials](#). [🔗](#)

Download Apps

Apps help you do more with your data. [Learn more](#). [🔗](#)

Build Dashboards

Visualize your searches. [Learn more](#). [🔗](#)

Your First Search (of this data)

- What do you see?

splunk>enterprise App: Search & Reporting

Search Datasets Reports Alerts Dashboards

Search & Reporting

New Search Save As Close

source="/var/log/auth.log" host="my_hostname" index="os" sourcetype="linux_secure" All time

✓ 151 events (before 5/2/18 7:10:38.000 PM) No Event Sampling

Events (151) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

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 1

a sourcetype 1

INTERESTING FIELDS

date_hour 1

date_mday 1

date_minute 6

a date_month 1

date_second 48

a date_wday 1

date_year 1

a date_zone 1

euid 1

a index 1

linecount 1

pid 32

a process 2

a punct 10

5/2/18 7:10:33.000 PM

May 2 19:10:33 ip-10-129-0-145 sshd[25607]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=123.183.209.133 user=root

Event Actions

Type	Field	Value	Actions
Selected	host	my_hostname	
	source	/var/log/auth.log	
	sourcetype	linux_secure	
Event	euid	0	
	pid	25607	
	process	sshd	
	rhost	123.183.209.133	
	tty	ssh	
	uid	0	
	user	root	
Time	_time	2018-05-02T19:10:33.000+00:00	
Default	index	os	