

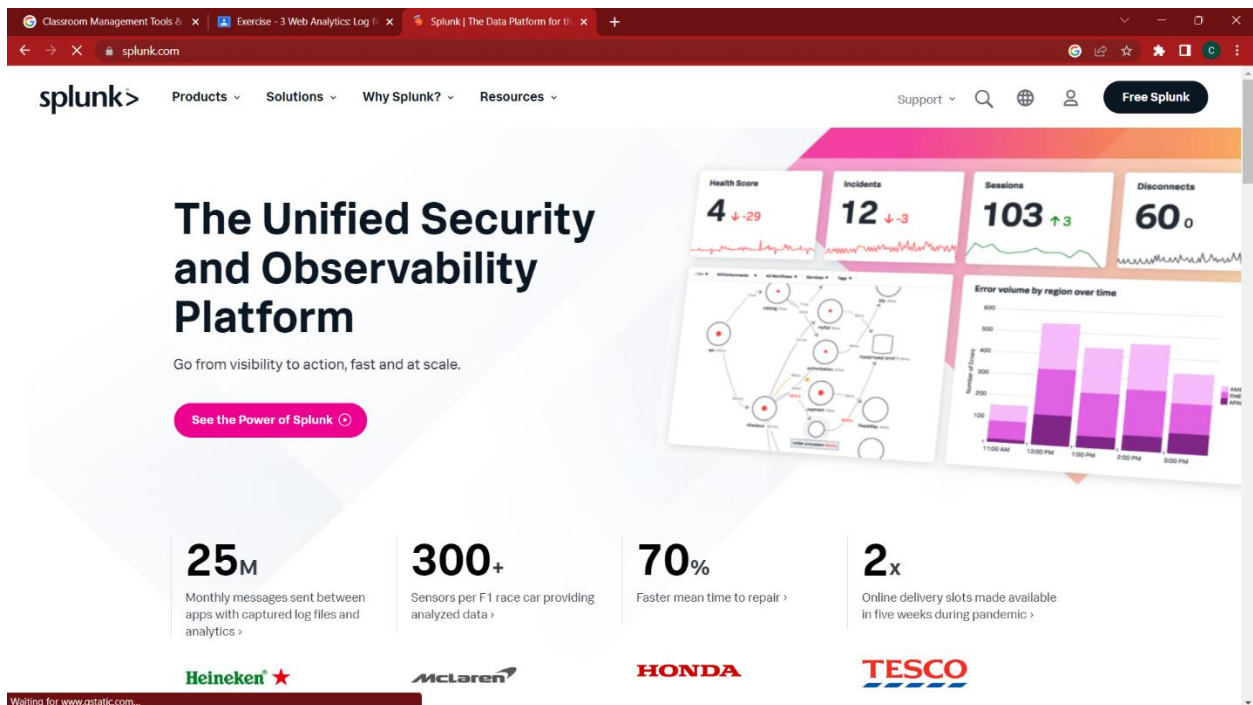
CHARAN N

Log File Analysis

What is Splunk?

About Splunk Enterprise

Splunk Enterprise is a software product that enables you to search, analyze, and visualize the data gathered from the components of your IT infrastructure or business. Splunk Enterprise takes in data from websites, applications, sensors, devices, and so on. After you define the data source, Splunk Enterprise indexes the data stream and parses it into a series of individual events that you can view and search.



STEP-1: Creating account in splunk

Classroom Management Tools | Exercise - 3 Web Analytics: Log | Splunk Cloud Platform Free Trial | +

splunk.com/en_us/download/splunk-cloud.html

Products Solutions Why Splunk? Resources Support

Splunk Cloud Platform Trial

Try Splunk Cloud free for 14 days. No credit card required.

- Keep it simple with SaaS — no installation required to start getting data in.
- Ingest up to 5GB/day of your own data in a Splunk-hosted cloud environment.
- Start searching, analyzing and visualizing your data on powerful, easy-to-understand dashboards.
- Keep your data safe in a highly secure environment that is SOC 2 Type I Attestation, ISO 27001 certification, HIPAA and PCI DSS compliant.

Once you sign up for the Splunk Cloud Platform trial, you'll see how it helps you to:

- ✓ Tackle your hardest security and observability use cases.
- ✓ Stream, collect and index any data at any scale.
- ✓ Set up real-time alerts so you can act fast.
- ✓ Customize for your unique business needs with free, pre-built apps from Splunkbase.

Start Your Cloud Platform Trial

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

Business Email

Password

First Name

Last Name

Job Title

Phone Number

Company

India

Zip / Postal Code

STEP-2: Login To Splunk

Classroom Management Tools | Exercise - 3 Web Analytics: Log | Log into Splunk | +

login.splunk.com/?redirecturl=https%3A%2F%2Fwww.splunk.com%2Fen_us%2Fdownload%2Fsplunk-cloud.html&ga=2.252166921.1462590615.1675185028-1979815582.1675185...

Splunk Account Login

Email or Username
charan.n@msds.christuniversity.in

Password

Forgot your [Password](#) or [username](#)?

Need to [sign up](#) for a Splunk account?

Splunk Cloud Services

[Product Login](#)

Splunk Observability Cloud

Splunk Infrastructure Monitoring, APM, Log Observer and RUM

[Product Login](#)

Splunk On-Call (formerly VictorOps)

[Product Login](#)

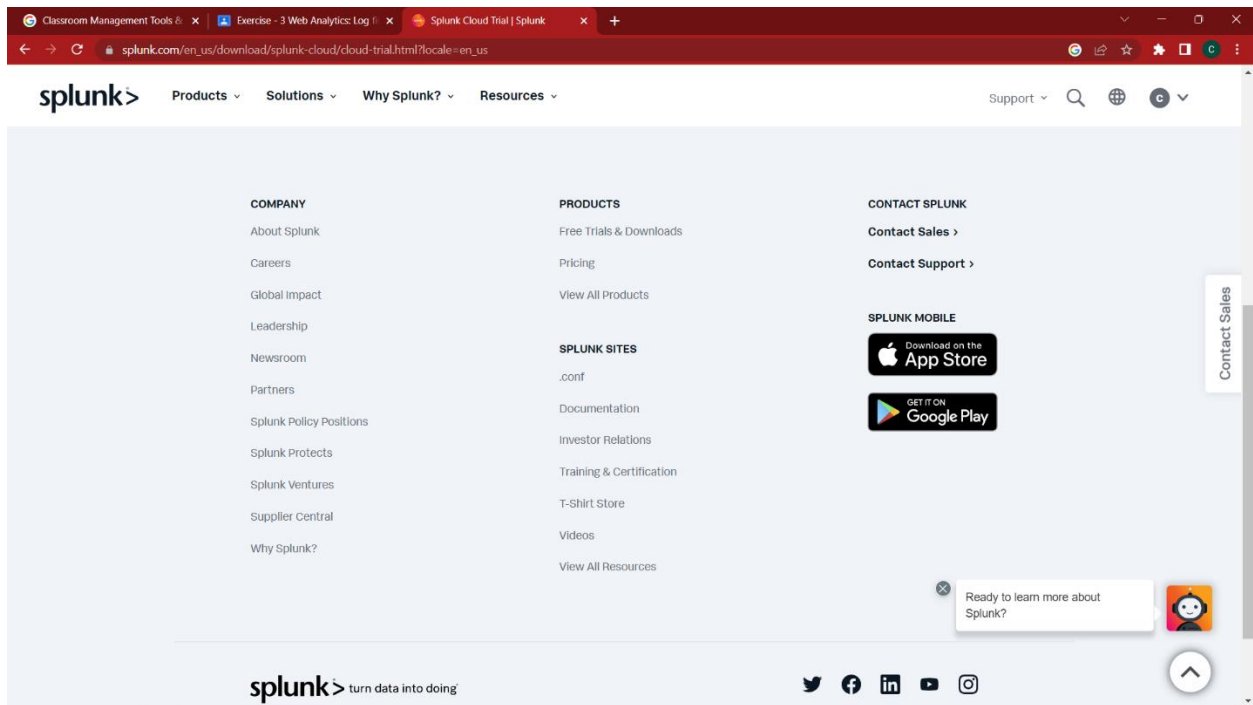
Splunk Synthetic Monitoring & Web Optimization (formerly Rigor)

[Synthetic Monitoring Product Login](#)

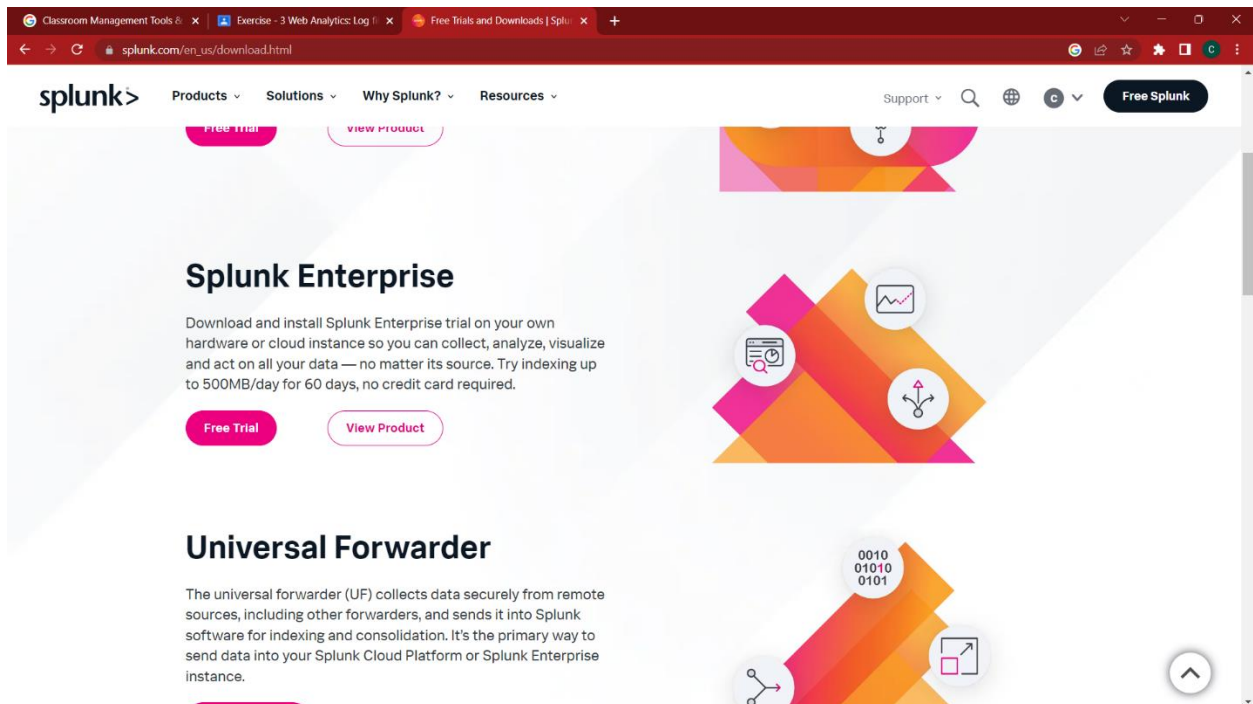
[Web Optimization Product Login](#)

Privacy Website Terms of Use Splunk Licensing Terms Export Control

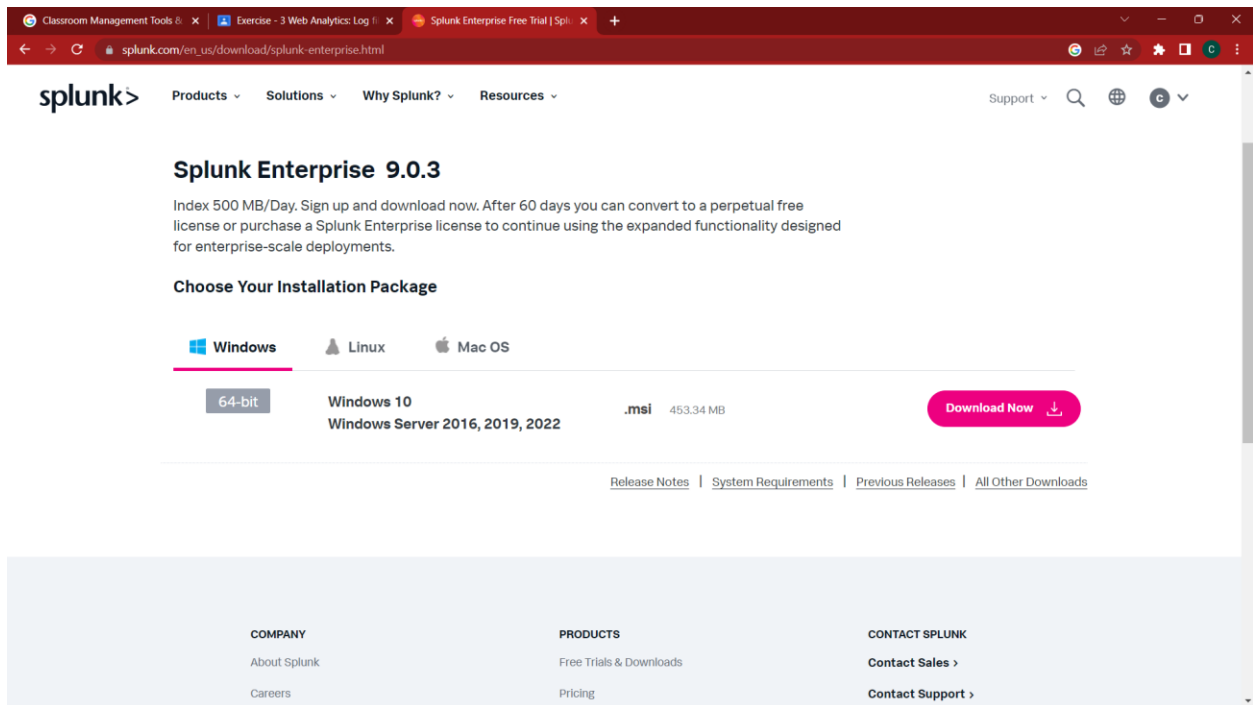
STEP-3: At the bottom of the page, under the products, click free trial and downloads



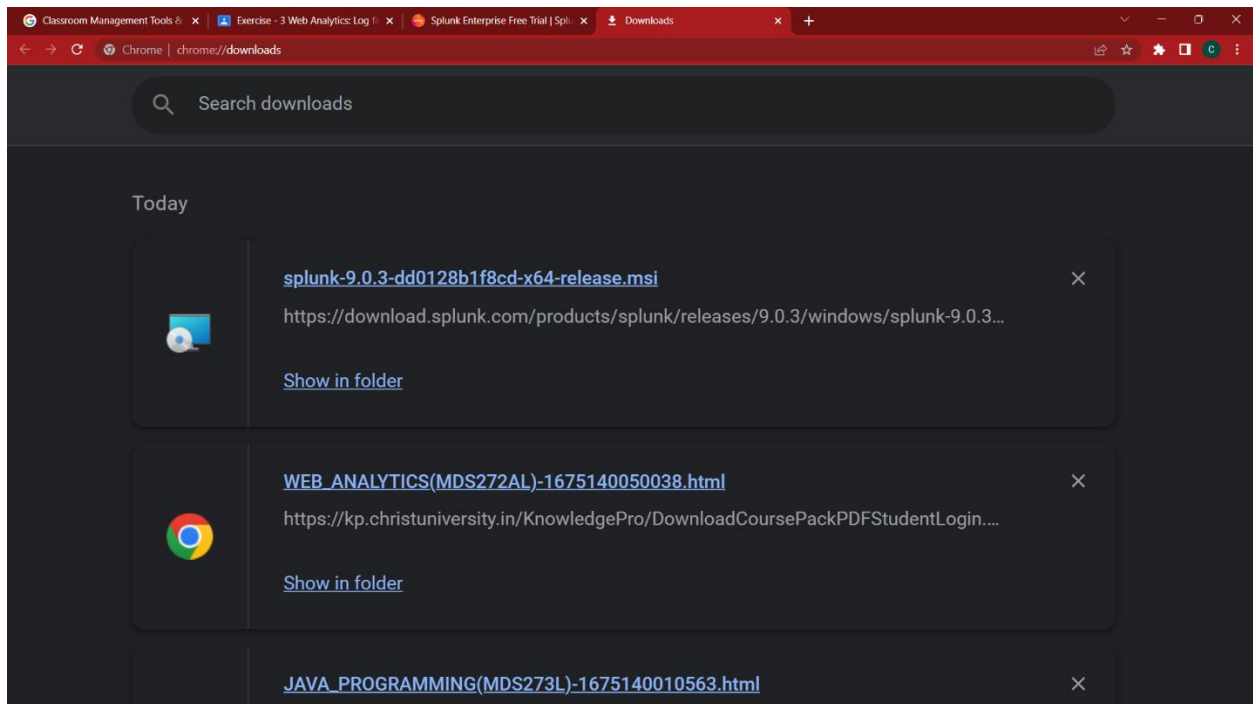
STEP-4: Scroll down and search for Splunk Enterprise and click free trial.



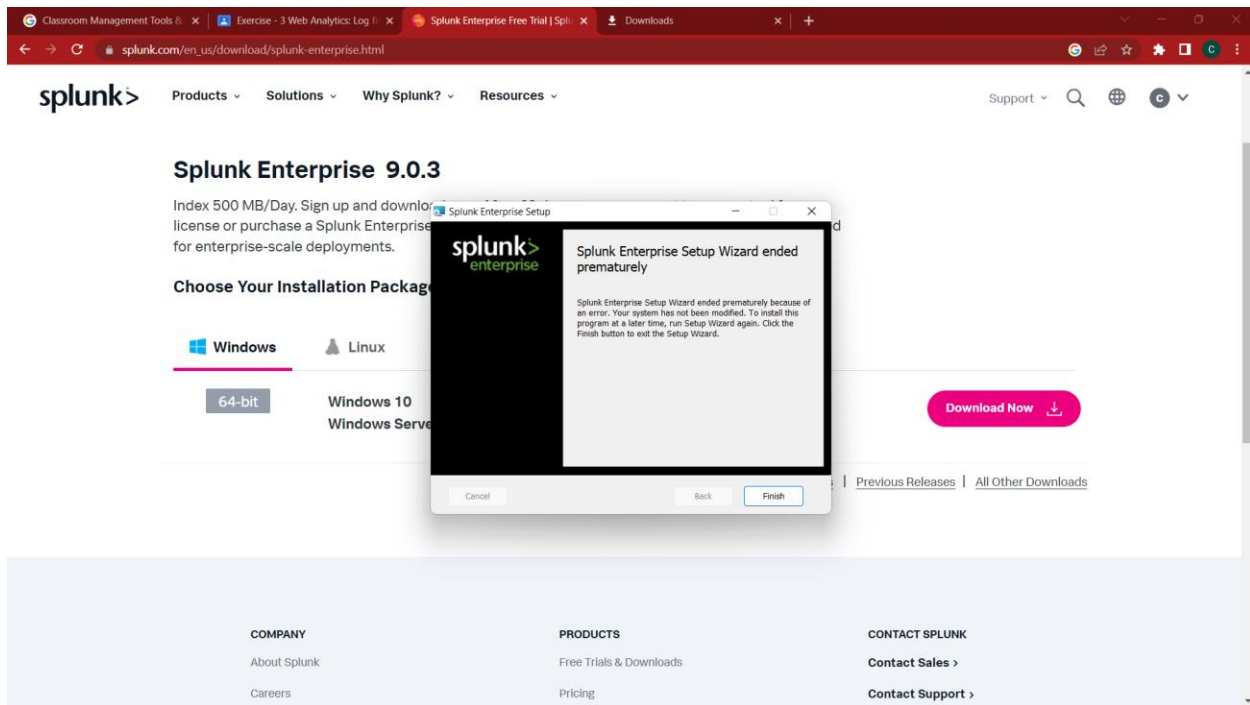
STEP-5: Download the appropriate version for your device



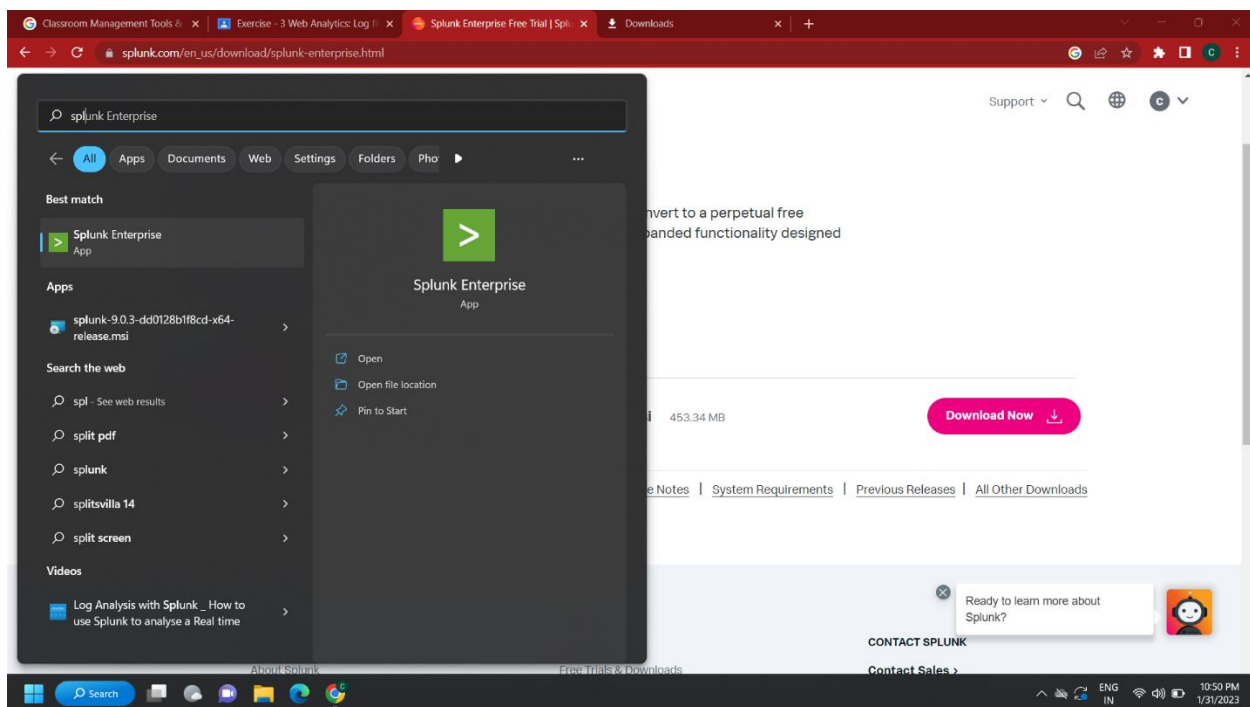
STEP-6: Select the downloaded file and click install



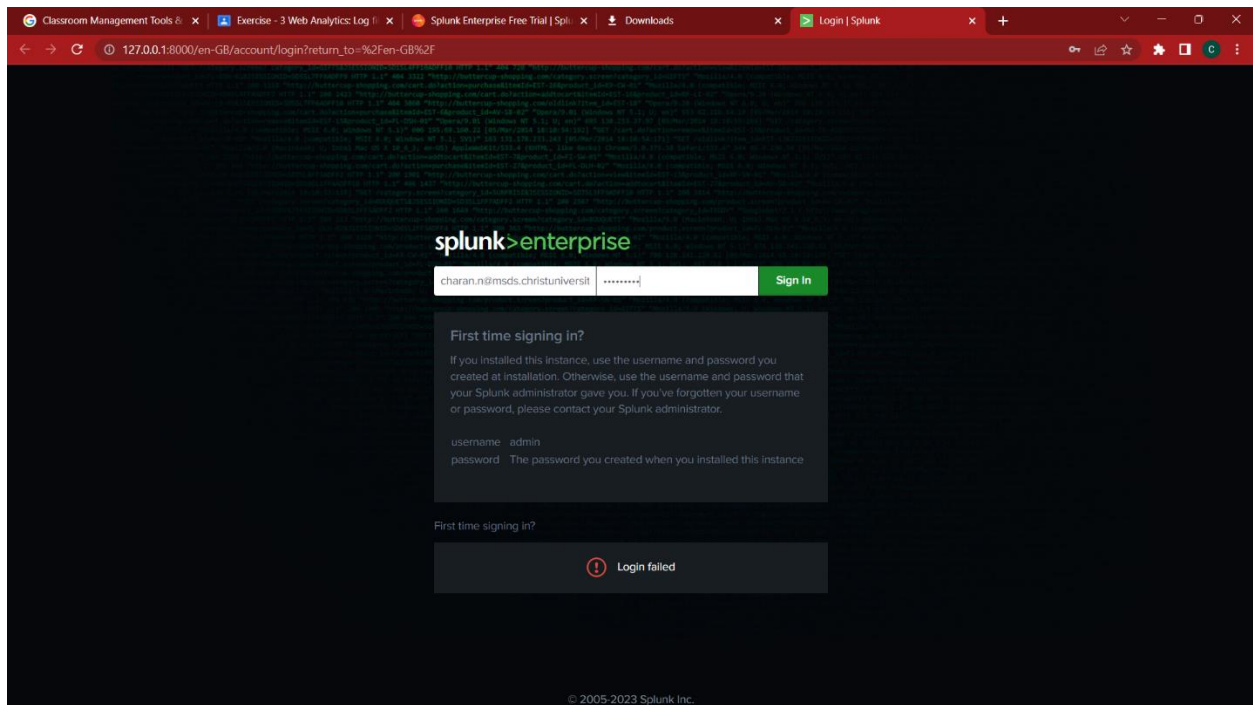
STEP-7: After few steps of installation, a dialogue box appears as this



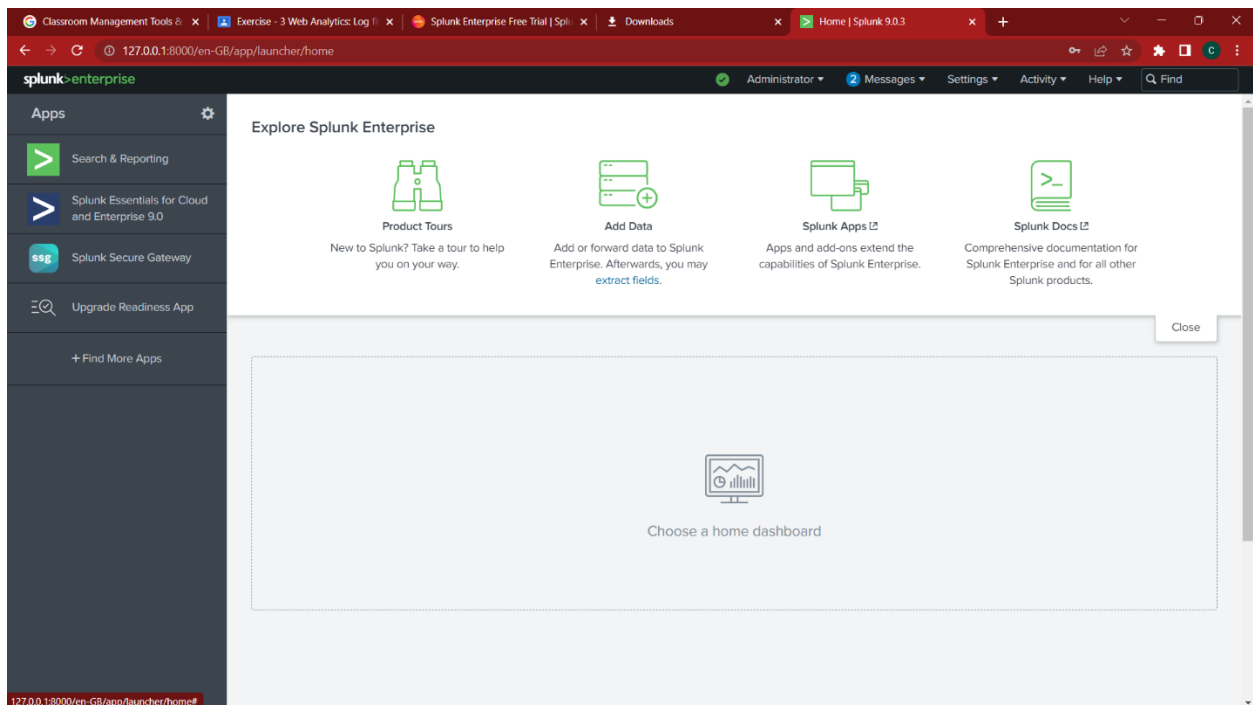
STEP-8: Open the splunk enterprise application



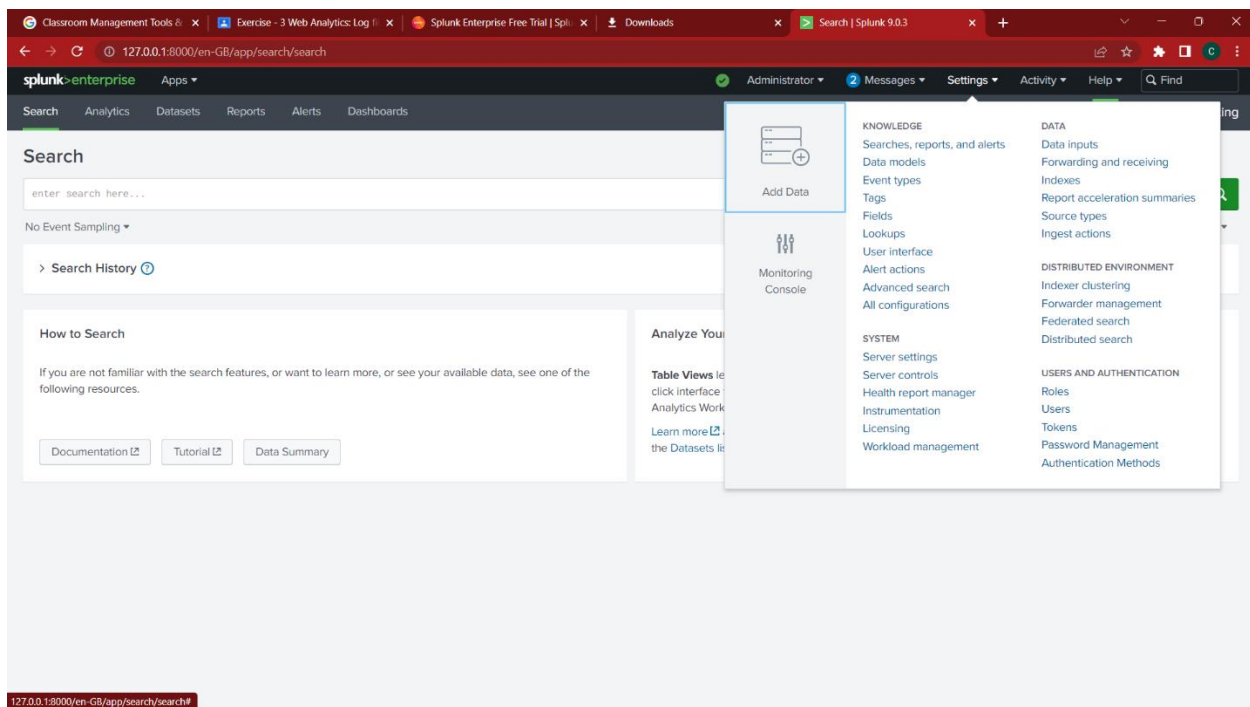
STEP-9: Sign in using the user id and password which you have given on the time of installation



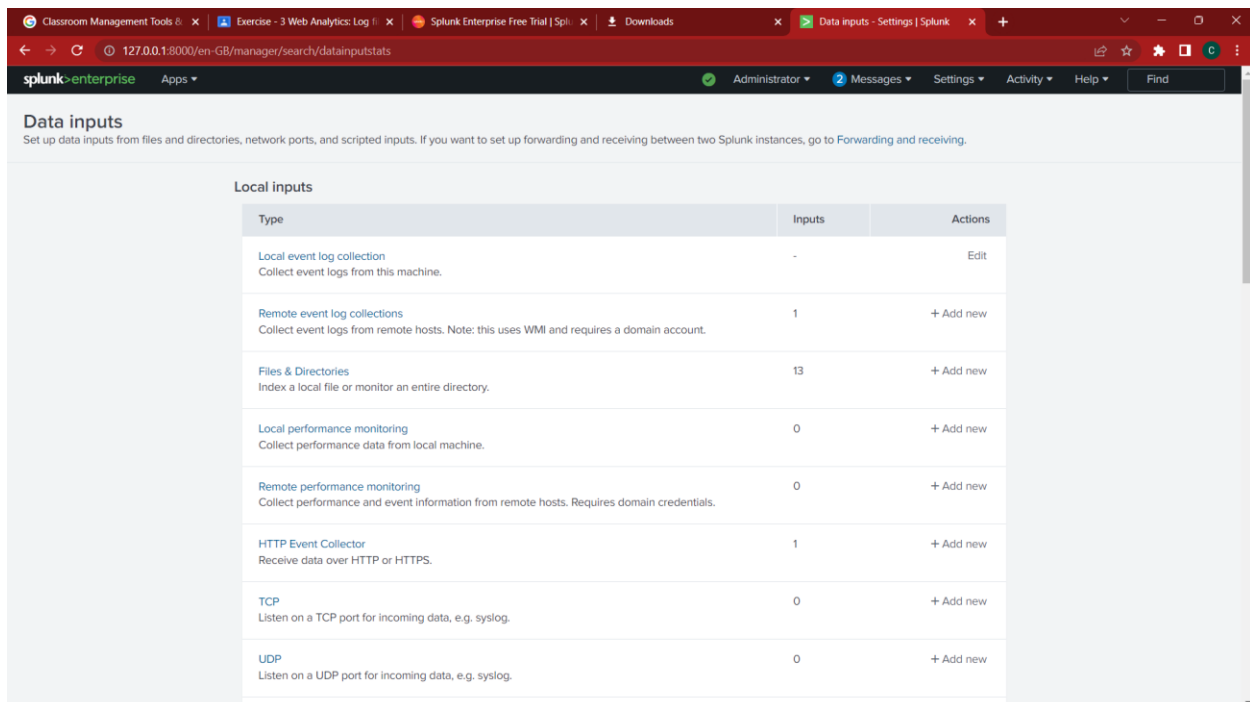
STEP-10: Splunk enterprise looks like this



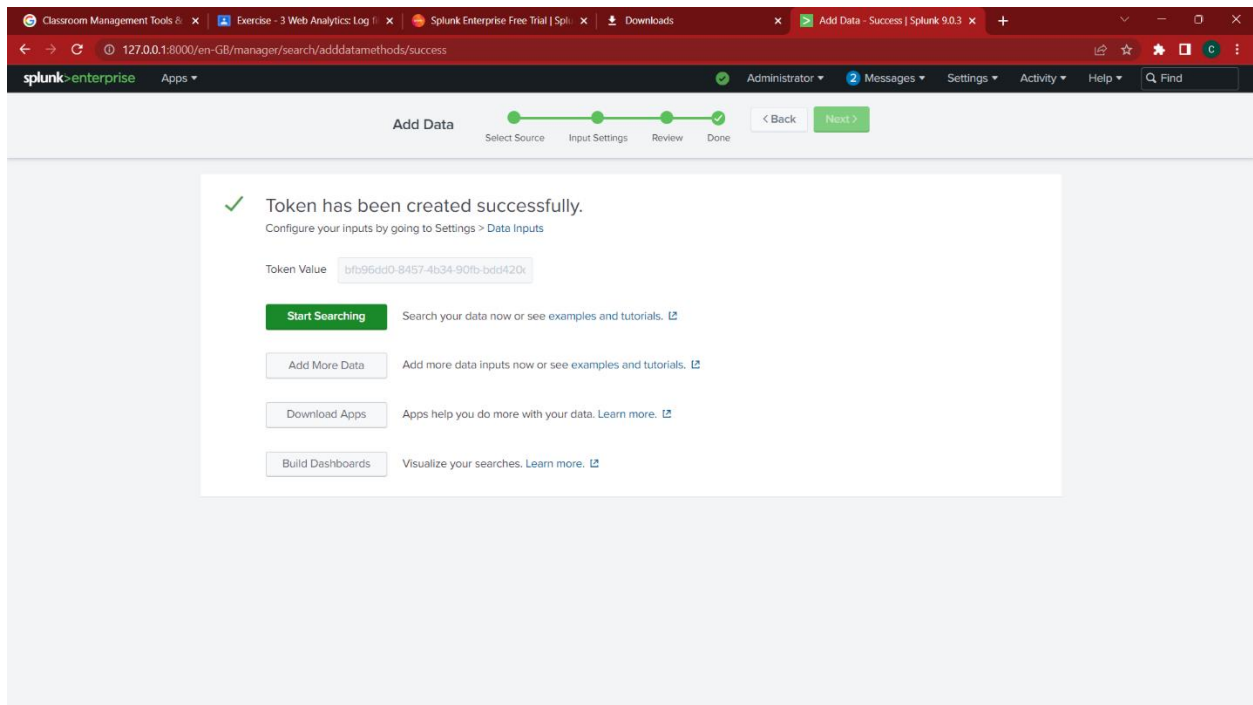
STEP-11: In the settings menu, under data, click data inputs, to see the inputs



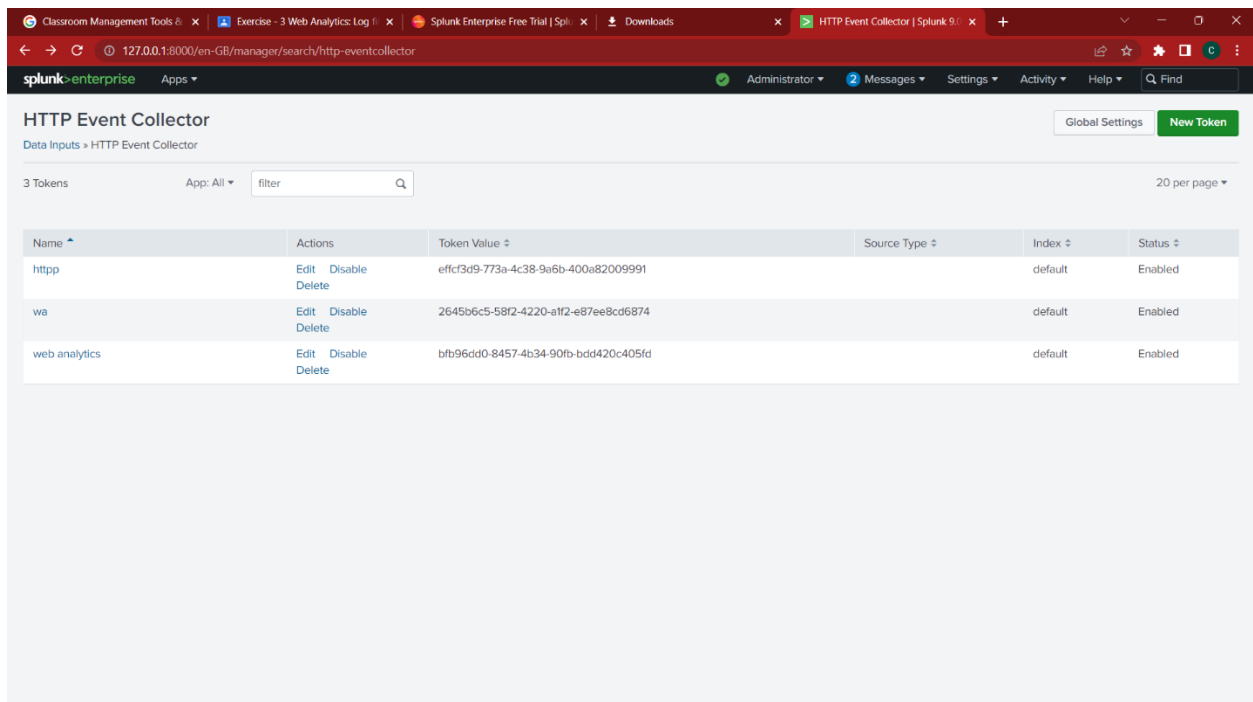
STEP-12: You can see the data inputs in the next page



STEP-13: After few steps, Your token will be created.



STEP-14: You can see the data available in HTTP event collector



STEP-15: In the local performance mentoring, create the details which you have to see.

Add Data

Select Source Input Settings Review Done

< Back Submit >

Review

Input Type Local Performance Monitor
Collection Name Task1
Selected Object Bluetooth Device
Selected Counters N/A
Selected Instances N/A
Polling Interval 300
App Context search
Host DESKTOP-2T09KEP
Index default

Add Data

Select Source Input Settings Review Done

< Back Next >

✓ Local performance monitoring 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. [🔗](#)
- [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. 🔗](#)

STEP-16: You can see the first task we have created in the collection name

The screenshot shows the Splunk Enterprise web interface. The browser address bar displays the URL: `127.0.0.1:8000/en-GB/manager/search/data/inputs/win-perfmon`. The page title is "Local performance monitoring". Below the title, there is a "Data inputs > Local performance monitoring" breadcrumb. A "Showing 1-1 of 1 item" message is displayed above a table. The table has columns: "Collection name", "Counters", "Instances", "Polling interval", "Index", "Status", and "Actions". The table contains one row with the following data: "Task1", "None", "*", "300", "default", "Enabled | Disable", and "Clone | Delete". A "filter" input field is located above the table. A "25 per page" dropdown is also visible. A green button labeled "New Local Performance Monitoring" is located in the top right corner.

Collection name	Counters	Instances	Polling interval	Index	Status	Actions
Task1	None	*	300	default	Enabled Disable	Clone Delete

STEP-17: Repeat the process to create another collection

The screenshot shows the "Add Data" wizard in the Splunk Enterprise web interface. The browser address bar displays the URL: `127.0.0.1:8000/en-GB/manager/search/adddatamethods/selectsource?input_mode=1&input_type=perfmom_local`. The wizard has a progress bar with four steps: "Select Source", "Input Settings", "Review", and "Done". The "Select Source" step is currently active. On the left, there is a list of data sources: "Local Event Logs", "Remote Event Logs", "Files & Directories", "HTTP Event Collector", "TCP / UDP", "Local Performance Monitoring" (selected), "Remote Performance Monitoring", "Registry monitoring", and "Active Directory monitoring". The "Local Performance Monitoring" source is highlighted. On the right, there is a configuration form. The "Collection name" field is set to "Task2". The "Available objects" dropdown menu is open, showing a list of performance objects: "GPU Engine", "GPU Local Adapter Memory", "GPU Non Local Adapter Memory", "GPU Process Memory", "Generic IKEv1, AuthIP, and IKEv2", "HTTP Service", "HTTP Service Request Queues", "HTTP Service Uri Groups", "Hyper-V Dynamic Memory", and "Integration Service". The "Polling interval" is set to "300" seconds. A "FAQ" section is visible below the configuration form.

Collection name: Task2

Available objects: -- Select object --

Polling interval: 300 sec

FAQ

- > What Windows performance metrics can I monitor?
- > What is the best method for monitoring performance?

Classroom Management Tools | Exercise - 3 Web Analytics: Log | Splunk Enterprise Free Trial | Downloads | Add Data - Select Source | Splunk

127.0.0.1:8000/en-GB/manager/search/adddatamethods/selectsource?input_mode=1&input_type=perfmom_local

splunk enterprise Apps Administrator Messages Settings Activity Help Find

Add Data

Select Source Input Settings Review Done

< Back Next >

Local Event Logs
Collect event logs from this machine.

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

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

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

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

Local Performance Monitoring
Collect performance data from this machine.

Remote Performance Monitoring
Collect performance and event information from remote hosts. Requires domain credentials.

Registry monitoring
Have the Splunk platform index the local Windows Registry, and monitor it for changes.

Active Directory monitoring
Index and monitor Active Directory.

Local Windows host monitoring

Configure this instance to monitor Windows performance counters. The performance objects available for monitoring depend on the system libraries installed. Microsoft and third-party vendors provide performance libraries. [Learn More](#)

Collection name Task2

Available objects HTTP Service

Select Counters

Available counter(s)	add all	Selected counter(s)	remove all
CurrentUriCached			
TotalFlushedUri			
TotalUriCached			
UriCacheFlushes			
UriCacheHits			

Select Instances

Available instance(s)	add all	Selected instance(s)	remove all
-----------------------	---------	----------------------	------------

Polling interval 300 sec

FAQ

> What Windows performance metrics can the Splunk platform collect?

Classroom Management Tools | Exercise - 3 Web Analytics: Log | Splunk Enterprise Free Trial | Downloads | Add Data - Input Settings | Splunk

127.0.0.1:8000/en-GB/manager/search/adddatamethods/inputsettings

splunk enterprise Apps Administrator Messages Settings Activity Help Find

Add Data

Select Source Input Settings Review Done

< Back Review >

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](#)

Host field value DESKTOP-2T09KEP

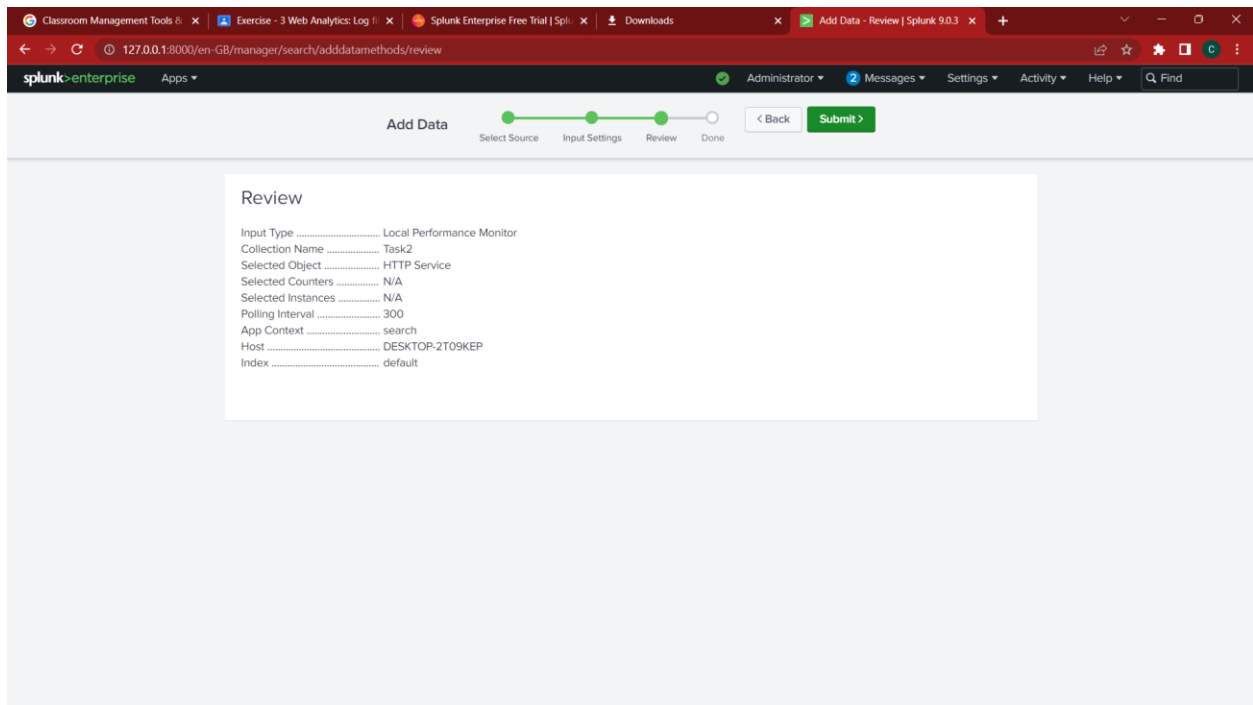
Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

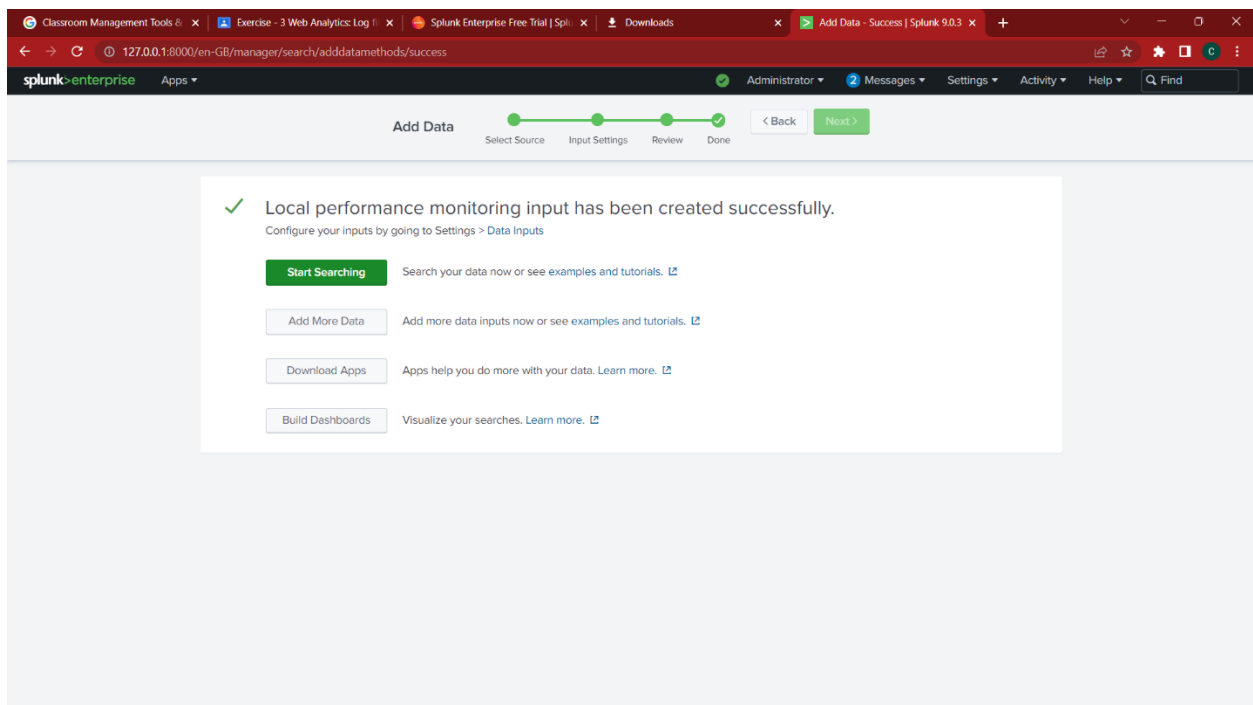
Index Default Create a new index

FAQ

> How do indexes work?



STEP-18: This page shows the local performance monitoring input is created



STEP-19: Next click on to the forwarding and receiving menu

The screenshot shows a web browser window with multiple tabs. The active tab is 'Settings | Splunk'. The address bar shows the URL '127.0.0.1:8000/en-GB/manager/search/forwardreceive'. The Splunk Enterprise logo and 'Apps' dropdown are in the top left. The top navigation bar includes 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' search bar.

Forwarding and receiving

Forward data
Set up forwarding between two or more Splunk instances.

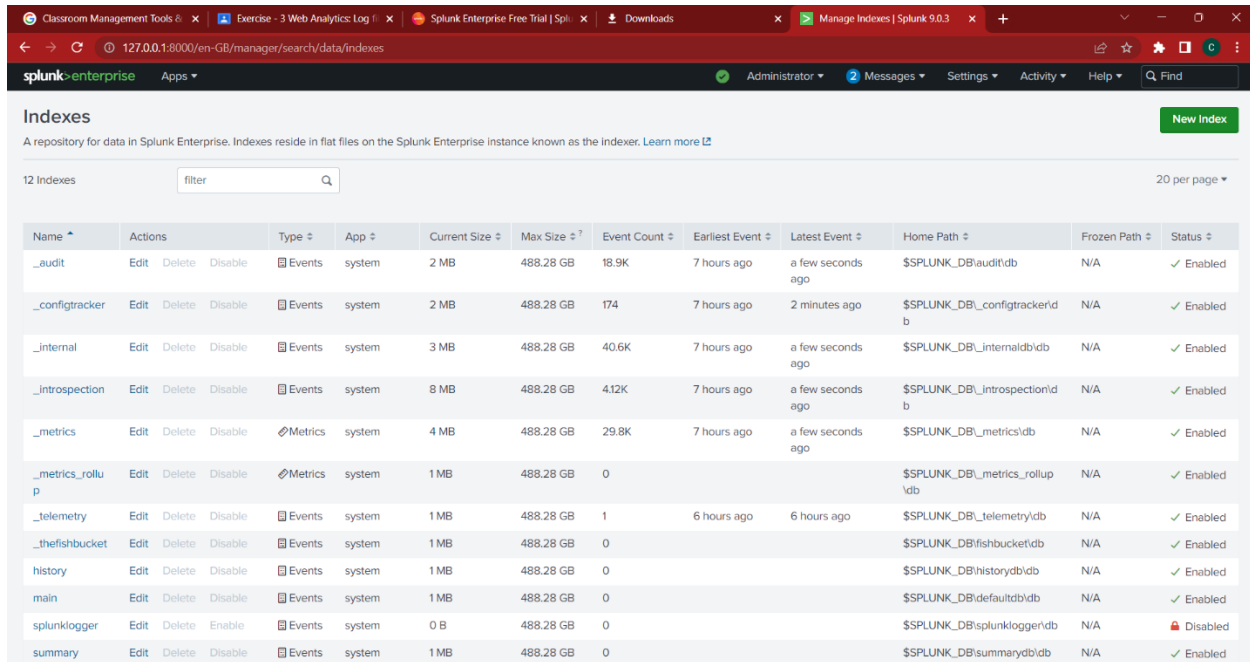
[Forwarding defaults](#)

[Configure forwarding](#) [+ Add new](#)

Receive data
Configure this instance to receive data forwarded from other instances.

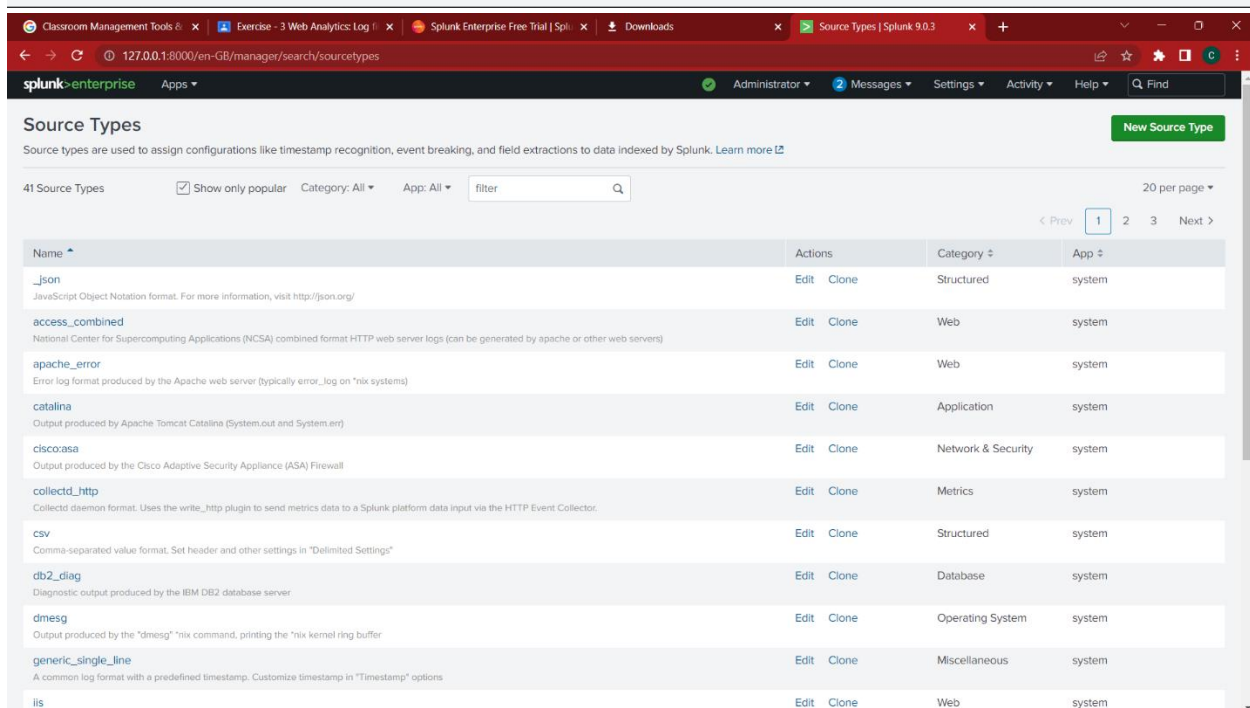
[Configure receiving](#) [+ Add new](#)

STEP-20: In next pages you can see the indexes and source types. This explains some process in splunk



The screenshot shows the Splunk Enterprise web interface. The browser tabs include 'Classroom Management Tools', 'Exercise - 3 Web Analytics Log', 'Splunk Enterprise Free Trial | Spl...', 'Downloads', and 'Manage Indexes | Splunk 9.0.3'. The address bar shows '127.0.0.1:8000/en-GB/manager/search/data/indexes'. The page title is 'splunk enterprise' with a navigation bar containing 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. The main heading is 'Indexes' with a 'New Index' button. Below the heading is a description: 'A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. Learn more'. There are 12 indexes listed, with a filter input and '20 per page' dropdown. The table has columns: Name, Actions, Type, App, Current Size, Max Size, Event Count, Earliest Event, Latest Event, Home Path, Frozen Path, and Status.

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path	Status
_audit	Edit Delete Disable	Events	system	2 MB	488.28 GB	18.9K	7 hours ago	a few seconds ago	\$SPLUNK_DB\audit\db	N/A	Enabled
_configtracker	Edit Delete Disable	Events	system	2 MB	488.28 GB	174	7 hours ago	2 minutes ago	\$SPLUNK_DB_configtracker\db	N/A	Enabled
_internal	Edit Delete Disable	Events	system	3 MB	488.28 GB	40.6K	7 hours ago	a few seconds ago	\$SPLUNK_DB_internal\db	N/A	Enabled
_introspection	Edit Delete Disable	Events	system	8 MB	488.28 GB	4.12K	7 hours ago	a few seconds ago	\$SPLUNK_DB_introspection\db	N/A	Enabled
_metrics	Edit Delete Disable	Metrics	system	4 MB	488.28 GB	29.8K	7 hours ago	a few seconds ago	\$SPLUNK_DB_metrics\db	N/A	Enabled
_metrics_rollup	Edit Delete Disable	Metrics	system	1 MB	488.28 GB	0			\$SPLUNK_DB_metrics_rollup\db	N/A	Enabled
_telemetry	Edit Delete Disable	Events	system	1 MB	488.28 GB	1	6 hours ago	6 hours ago	\$SPLUNK_DB_telemetry\db	N/A	Enabled
_thefishbucket	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB_fishbucket\db	N/A	Enabled
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB_history\db	N/A	Enabled
main	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB_default\db	N/A	Enabled
splunklogger	Edit Delete Enable	Events	system	0 B	488.28 GB	0			\$SPLUNK_DB_splunklogger\db	N/A	Disabled
summary	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB_summary\db	N/A	Enabled



The screenshot shows the Splunk Enterprise web interface for Source Types. The browser tabs include 'Classroom Management Tools', 'Exercise - 3 Web Analytics Log', 'Splunk Enterprise Free Trial | Spl...', 'Downloads', and 'Source Types | Splunk 9.0.3'. The address bar shows '127.0.0.1:8000/en-GB/manager/search/sourcetypes'. The page title is 'splunk enterprise' with a navigation bar containing 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. The main heading is 'Source Types' with a 'New Source Type' button. Below the heading is a description: 'Source types are used to assign configurations like timestamp recognition, event breaking, and field extractions to data indexed by Splunk. Learn more'. There are 41 source types listed, with a 'Show only popular' checkbox, 'Category: All', 'App: All', a filter input, and '20 per page' dropdown. The table has columns: Name, Actions, Category, and App.

Name	Actions	Category	App
_json JavaScript Object Notation format. For more information, visit http://json.org/	Edit Clone	Structured	system
access_combined National Center for Supercomputing Applications (NCSA) combined format HTTP web server logs (can be generated by apache or other web servers)	Edit Clone	Web	system
apache_error Error log format produced by the Apache web server (typically error_log on *nix systems)	Edit Clone	Web	system
catalina Output produced by Apache Tomcat Catalina (System.out and System.err)	Edit Clone	Application	system
cisco:asa Output produced by the Cisco Adaptive Security Appliance (ASA) Firewall	Edit Clone	Network & Security	system
collectd_http Collectd daemon format. Uses the write_http plugin to send metrics data to a Splunk platform data input via the HTTP Event Collector.	Edit Clone	Metrics	system
csv Comma-separated value format. Set header and other settings in "Delimited Settings"	Edit Clone	Structured	system
db2_diag Diagnostic output produced by the IBM DB2 database server	Edit Clone	Database	system
dmesg Output produced by the "dmesg" *nix command, printing the *nix kernel ring buffer	Edit Clone	Operating System	system
generic_single_line A common log format with a predefined timestamp. Customize timestamp in "Timestamp" options	Edit Clone	Miscellaneous	system
iis	Edit Clone	Web	system

After this using some stats and visualization technique,

- Now go to Search & Reporting in the home.
- In the search bar search any pipeline and then save as ☐ new dashboard ☐ create new dashboard
- It can be visualised in bar graph/column graph/pie-chart and so on.
- We can edit the dashboard and add a new panel or a report to the existing dashboard.
- Edit ☐ Add Panel ☐ (select the required dashboard or report to be cloned to the existing). Having a centralized logging system makes life easy for developers especially when there is a need to troubleshoot the application, detect issues, secure the application due to unexpected hits on services or review the performance of the application, etc. Some of the great features of a centralized logging system are its low-cost maintenance, easy logs searching, graphical UI etc.
- A dashboard is used to represent tables or charts which are related to some business meaning. It is done through panels. The panels in a dashboard hold the chart or summarized data in a visually appealing manner. We can add multiple panels, and hence multiple reports and charts to the same dashboard.

