RUNNING SPLUNK ON WINDOWS 11 USING DOCKER *(Total Time: 15 mins)*

Prerequisites:

1. Make sure Docker Desktop is installed

   ```
   MAC: https://docs.docker.com/desktop/setup/install/mac-install/

   WINDOWS: https://docs.docker.com/desktop/setup/install/windows-install/

   LINUX: https://docs.docker.com/desktop/setup/install/linux/
   ```

2. If you are using Windows , make sure WSL (Subsystem for Linux) is installed.

   ```
   Documentation: https://learn.microsoft.com/en-us/windows/wsl/install
   ```

Docker Image:

Docker Image is available for Splunk on Docker hub (1.2 GB Size).

```
Image Link and Documentation: https://hub.docker.com/r/splunk/splunk
```

Use the following command to pull the docker image from Docker Hub:

```
    docker pull splunk/splunk:latest

    Terminal:
    $ docker pull splunk/splunk:latest
    latest: Pulling from splunk/splunk
    b2abe6be4acb: Pull complete
    fc3a2183f4da: Pull complete
    bd61a0d532eb: Pull complete
    c82e132ce5fc: Pull complete
    8c513b00ce36: Pull complete
    133cfad7d9ef: Pull complete
    b7768c8f6aa6: Pull complete
    5f5b632e6750: Pull complete
    83a01b254263: Pull complete
    4f4fb700ef54: Pull complete
    0922b98ea72b: Pull complete
    Digest:
```

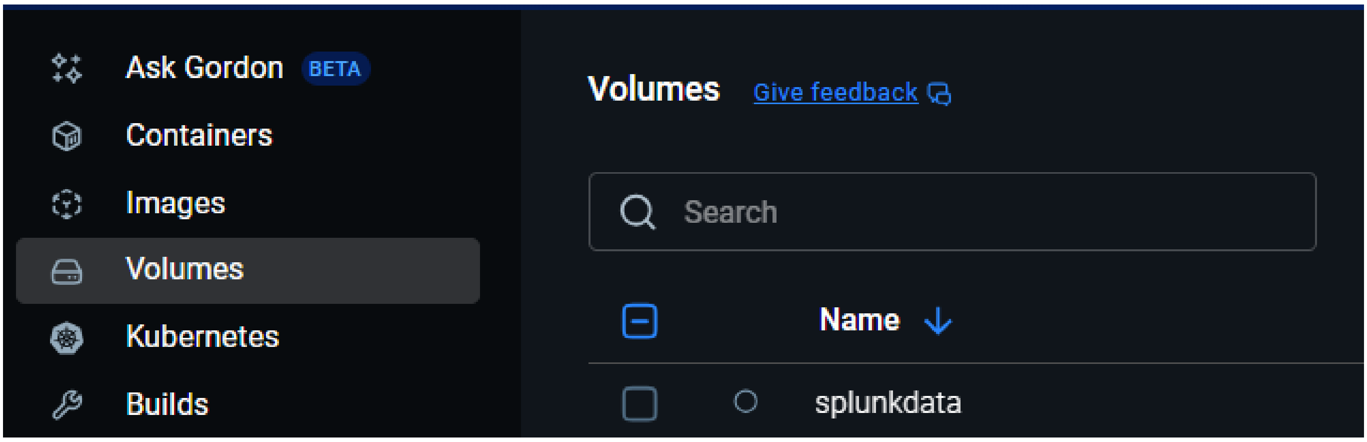
```
sha256:8adbca4db55be5a962ef7897cfe60d3cf64ef02715b0723d2140ddd945d48522
    Status: Downloaded newer image for splunk/splunk:latest
    docker.io/splunk/splunk:latest
```

Create a Volume for Persistant Data for Splunk

The following command is used to create a persistant volume:

```
docker volume create splunkdata
```

```
Terminal:
$ docker volume create splunkdata
splunkdata
```



Create a local directory to mount the volume:

```
mkdir splunkdata
```

Why are we creating a volume and attaching it with the container?

Answer - Because Docker Volumes exists independently from the life of a container. Even if Container gets removed. Thus all the data will be reserved.

Command to run the container:

We are running the following command that performs the following:

- Run container using the latest splunk image.
- Setting a volume to a mount point for the data to persist.
- The docker has been mapped to a host port of 8000 and port 8000 of the container.
- We are accepting the license agreement.
- We are setting the admin password as per Splunk password standards.

Command:

```
docker run -d -p 8000:8000 -v splunkdata:<path of the directory> -e
"SPLUNK_START_ARGS=--accept-license" -e "SPLUNK_GENERAL_TERMS=--accept-sgt-
current-at-splunk-com" -e "SPLUNK_PASSWORD=<your password>" --name splunk
splunk/splunk:latest
```

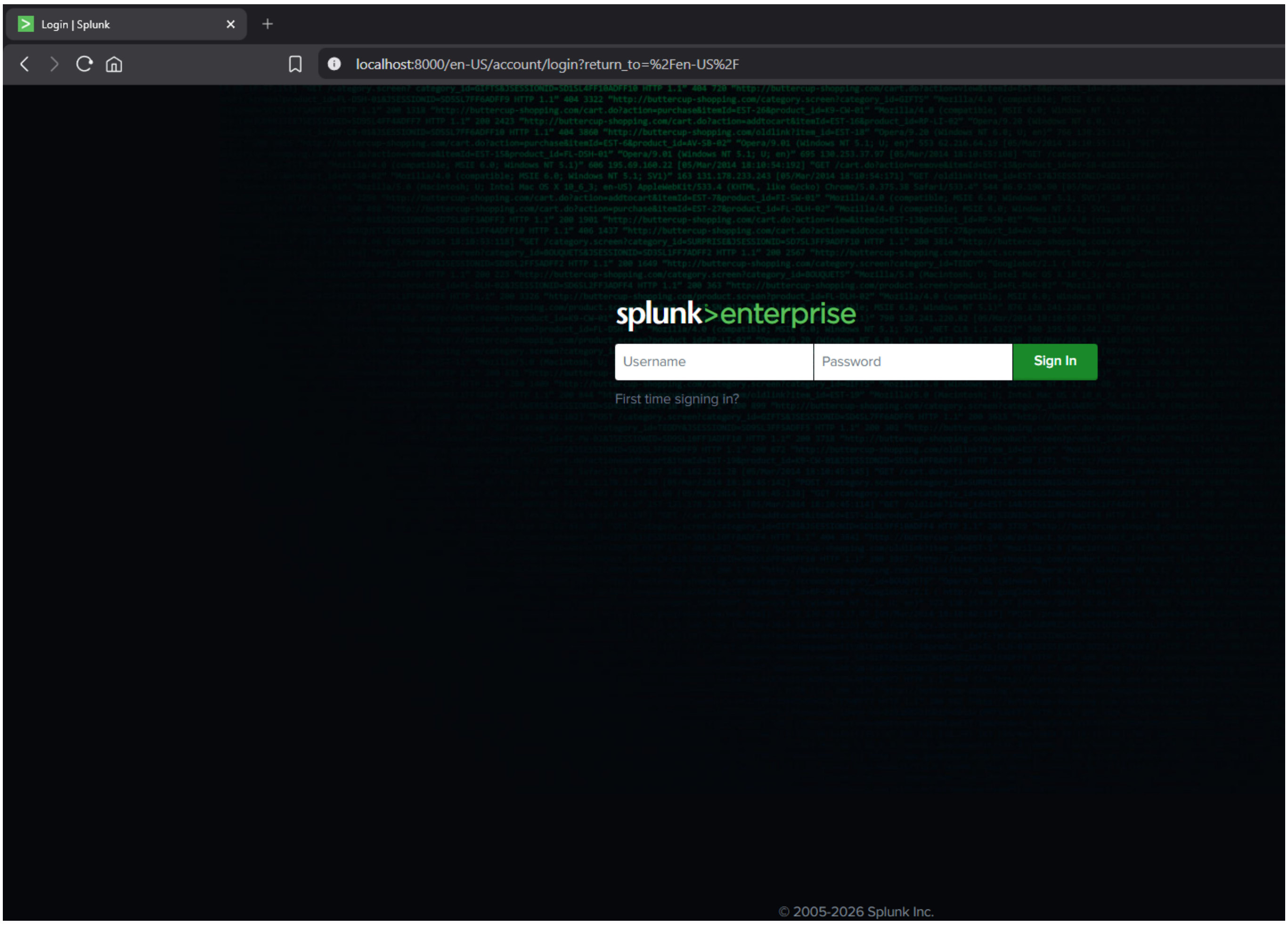
Check and confirm that the docker container is running:

```
Terminal:
docker ps
```

```
CONTAINER ID   IMAGE                  COMMAND                  CREATED
STATUS                  PORTS                                        NAMES
d2b387b319e5   splunk/splunk:latest   "/sbin/entrypoint.sh…"   2 minutes ago   Up
2 minutes (healthy)   0.0.0.0:8000->8000/tcp, [::]:8000->8000/tcp   splunk
```

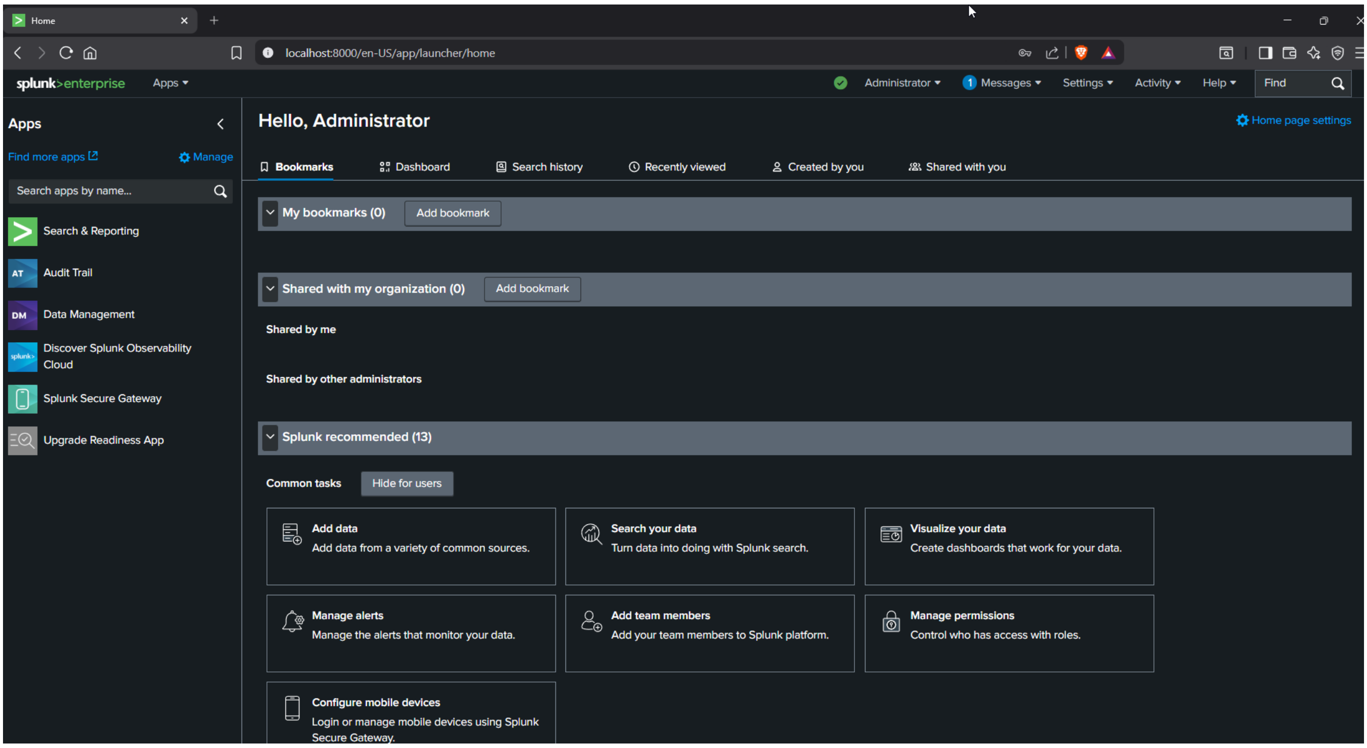
Validation

Splunk Interface on localhost:



localhost:8000/en-US/account/login?return_to=%2Fen-US%2F

Splunk Adminstrator Interface after login and ready for POC:



Hello, Administrator

My bookmarks (0)

Shared with my organization (0)

Shared by me

Shared by other administrators

Splunk recommended (13)

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.

Manage alerts
Manage the alerts that monitor 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.