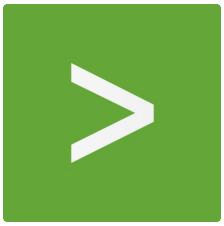
Product Overview



Splunk Enterprise Free (for docker)

By Splunk Inc

Copy and paste to pull this image

```
docker pull store/splunk/enterprise:6.5.2
```

Free Details

This is a fully featured single instance of Splunk Enterprise with Alerts.

SETUP INSTRUCTIONS

Supported tags

- `6.5.2` - Splunk Enterprise base image Dockerfile
- `6.5.2-monitor` , `latest` - Splunk Enterprise with Docker Monitoring Dockerfile

What is Splunk Enterprise?

Splunk Enterprise is the platform for operational intelligence. The software lets you collect, analyze, and act upon the untapped value of big data that your technology infrastructure, security systems, and business applications generate. It gives you insights to drive operational performance and business results.

This repository contains Dockerfiles that you can use to build Splunk Docker images.

Get started with the Splunk Enterprise Docker Image

If you have not used Docker before, see the Getting started tutorial for Docker.

1. (Optional) Sign up for a Docker ID at Docker Hub.
2. Download and install Docker on your system.
3. Open a shell prompt or Terminal window.
4. Enter the following command to pull the Splunk Enterprise version 6.5.2 image.

```
docker pull store/splunk/enterprise
```

5. Run the Docker image.

```
docker run -d -e "SPLUNK_START_ARGS=--accept-license" -e "SPLUNK_USER=root" -p "8000:8000" sto
```

6. Access the Splunk instance with a browser by using the Docker machine IP address and Splunk Web port. For example, `` `http://localhost:8000 ``

See How to use the Splunk Enterprise Docker image for additional example commands.

How to use the Splunk Enterprise Docker image

The following commands can be run from a shell prompt or Docker QuickStart Terminal (on Mac OS X).

Pull an image for version 6.5.2 of Splunk Enterprise from this repository

```
docker pull store/splunk/enterprise:6.5.2
```

Pull an image that uses the latest version of Splunk Enterprise from this repository

```
docker pull store/splunk/enterprise:latest
```

Start a Splunk Enterprise container and automatically accept the license agreement

This command starts a Splunk Enterprise instance from the Docker container in this repository, accepts the license agreement, and opens TCP port 8000 so that you can access the Splunk instance from your local machine.

```
docker run --name splunk --hostname splunk -p 8000:8000 -d -e "SPLUNK_START_ARGS=--accept-license" st
```

Start a Splunk Enterprise container and mount the necessary container volumes

```
docker run --name vsplunk -v /opt/splunk/etc -v /opt/splunk/var busybox
docker run --hostname splunk --name splunk --volumes-from=vsplunk -p 8000:8000 -d -e "SPLUNK_START_AR
```

Use entrypoint.sh to execute Splunk commands

You can execute commands in the container by typing in the following command, for example:

```
docker exec splunk entrypoint.sh splunk version
```

To learn about the commands you can use with entrypoint.sh, see Administrative CLI commands in the Splunk documentation.

You can also use entrypoint.sh to configure Splunk services with environment variables. See Basic configuration with environment variables.

Configure the Splunk Enterprise Docker container with docker-compose

1. At a shell prompt, create a text file `docker-compose.yml` if it does not already exist.
2. Open `docker-compose.yml` for editing.
3. Insert the following block of text into the file.

```
version: '2'
services:
 vsplunk:
```

```
image: busybox
volumes:
 - /opt/splunk/etc
 - /opt/splunk/var
splunk:
 image: store/splunk/enterprise:6.5.2-monitor
 hostname: splunkenterprise
 environment:
  SPLUNK_START_ARGS: --accept-license --answer-yes
  SPLUNK_ENABLE_LISTEN: 9997
  SPLUNK_ADD: tcp 1514
  SPLUNK_USER: root
 volumes_from:
  - vsplunk
 volumes:
  - /var/lib/docker/containers:/host/containers:ro
  - /var/run/docker.sock:/var/run/docker.sock:ro
 ports:
  - "8000:8000"
  - "9997:9997"
  - "8088:8088"
  - "1514:1514"
```

4. Save the file and close it.
5. Run the `docker-compose` utility in the same directory.

```
docker-compose up
```

Configuration

Image Variants

The `store/splunk/enterprise` image comes in several variants:

`store/splunk/enterprise:6.5.2` This is the default Splunk Enterprise image.

`store/splunk/enterprise:6.5.2-monitor` This image comes with some data inputs activated (e.g., file monitor of docker host JSON logs, HTTP Event Collector, Syslog, etc.). It also includes the Docker app which has dashboards to help you analyze collected logs and docker information such as stats, events, tops, and inspect from your running images.

Data Store

This Docker image has two data volumes:

- `/opt/splunk/etc` - stores Splunk configurations, including applications and lookups
- `/opt/splunk/var` - stores indexed data, logs and internal Splunk data

User

All Splunk processes by default runs as the `splunk` user. The user can be changed by setting the SPLUNK_USER env variable.

Ports

This Docker container exposes the following network ports:

- `8000/tcp` - Splunk Web interface
- `8088/tcp` - HTTP Event Collector
- `8088/tcp` - Splunk Services
- `8191/tcp` - Application Key Value Store
- `9997/tcp` - Splunk receiving Port (not used by default) typically used by the Splunk Universal Forwarder
- `1514/tcp` - Network Input (not used by default) typically used to collect syslog TCP data

This Docker image uses port 1514 instead of the standard port 514 for the syslog port because network ports below 1024 require root access. See Run Splunk Enterprise as a different or non-root user.

Hostname

When you use this Docker image, set a `hostname` for it. If you recreate the instance later, the image retains the hostname.

Basic configuration with Environment Variables

You can use environment variables for basic configuration of the indexer and forwarder. For more advanced configuration, create configuration files within the container or use a Splunk deployment server to deliver configurations to the instance.

- `SPLUNK_ENABLE_DEPLOY_SERVER='true'` - Enables deployment server on Indexer.
- `SPLUNK_DEPLOYMENT_SERVER='<servername>:<port>` - configure deployment client. Set deployment server url.
    - Example: `--env SPLUNK_DEPLOYMENT_SERVER='splunkdeploymentserver:8089'` .
- `SPLUNK_ENABLE_LISTEN=<port>` - enable receiving.

    - Additional configuration is available using `SPLUNK_ENABLE_LISTEN_ARGS` environment variable.

- `SPLUNK_FORWARD_SERVER=<servername>:<port>` - forward data to indexer.
    - Additional configuration is available using `SPLUNK_FORWARD_SERVER_ARGS` environment variable.
    - Additional forwarders can be set up using `SPLUNK_FORWARD_SERVER_<1..30>` and `SPLUNK_FORWARD_SERVER_<1..30>_ARGS` .
    - Example: `--env SPLUNK_FORWARD_SERVER='splunkindexer:9997' --env SPLUNK_FORWARD_SERVER_ARGS='method clone' --env SPLUNK_FORWARD_SERVER_1='splunkindexer2:9997' --env SPLUNK_FORWARD_SERVER_1_ARGS='-method clone'` .
- `SPLUNK_ADD='<monitor|add> <what_to_monitor|what_to_add>'` - execute add command, for example to monitor files or listen on specific ports.
    - Additional add commands can be executed (up to 30) using `SPLUNK_ADD_<1..30>` .
    - Example `--env SPLUNK_ADD='udp 1514' --env SPLUNK_ADD_1='monitor /var/log/*'` .
- `SPLUNK_CMD='any splunk command'` - execute any splunk command.
    - Additional commands can be executed (up to 30) using `SPLUNK_CMD_<1..30>` .
    - Example `--env SPLUNK_CMD='edit user admin -password random_password -role admin -auth admin:changeme'` .

Example

Following is an example of how to configure Splunk Enterprise and the Splunk universal forwarder in Docker.

```
> echo "Creating docker network, so all containers will see each other"
> docker network create splunk
> echo "Starting deployment server for forwarders"
> docker run -d --net splunk \
    --hostname splunkdeploymentserver \
    --name splunkdeploymentserver \
    --publish 8000 \
    --env SPLUNK_ENABLE_DEPLOY_SERVER=true \
    store/splunk/enterprise
> echo "Starting Splunk Enterprise"
> docker run -d --net splunk \
    --hostname splunkenterprise \
    --name splunkenterprise \
    --publish 8000 \
```

```
    --env SPLUNK_ENABLE_LISTEN=9997 \
    store/splunk/enterprise
> echo "Starting forwarder, which forwards data to Splunk"
> docker run -d --net splunk \
    --name forwarder \
    --hostname forwarder \
    --env SPLUNK_FORWARD_SERVER='splunkenterprise:9997' \
    --env SPLUNK_FORWARD_SERVER_ARGS='-method clone' \
    --env SPLUNK_ADD='udp 1514' \
    --env SPLUNK_DEPLOYMENT_SERVER='splunkdeploymentserver:8089' \
    splunk/universalforwarder
```

After this script executes, you can forward syslog data to the *udp* port of container *forwarder* (for internal containers only, as Splunk does not publish the port). Data should arrive in Splunk Enterprise and you should see the forwarder registered with the deployment server.

Troubleshoot problems with the image

Basic troubleshooting

If you do not see data when you load the Docker Overview app in the Docker app, confirm that:

- You have started the container with the right environment variables. In particular, you must have the proper access control to the mount points to read the default JSON log files that the docker host collects. See Required Permissions for more detail.
- You have included the necessary volumes for the Docker image.
- Your Docker container has the correct filesystem permissions.

Required Permisssions

The following mount points require special permissions:

- `/var/lib/docker/containers` : By default, the Docker host only exposes read access to the root user. Read access to the volume could be changed for any users that start the Splunk process.
- `/var/run/docker.sock` - Requires access to the Docker Remote API to collect information such as docker stats, tops, events, and inspect.

Overriding the SPLUNK_USER envrionment variable to an authorized user (such as "root") gives you the required access to the mount points that the Docker app needs to analyze the collected Docker information.

Troubleshoot upgrade problems with docker-compose

If you use `docker-compose` (or reference an existing volume with `docker run`) to configure and run your Docker image and the Splunk Enterprise Docker container detects an upgrade after you make a change to `docker-compose.yml`, complete the following procedure to make the image ignore the upgrade prompt:

1. Open `docker-compose.yml` for editing.
2. In the `Environment:` section for the Splunk Enterprise image, add the following line:

```
SPLUNK_START_ARGS: --accept-license --answer-yes
```

3. Save `docker-compose.yml` and close it.
4. Run `docker-compose up` again.

If you still need help

If you still have trouble collecting or analyzing data with the Splunk Enterprise Docker image, use one of the following options:

- Post a question to Splunk Answers
- Join the Splunk Slack channel
- Visit the #splunk channel on EFNet Internet Relay Chat
- Send an email to docker-maint@splunk.com