

Updating ELK Stack for LME

Updating ELK Stack for LME

If you find you need to update the ELK (Elastic, Logstash, Kibana) Stack for LME you have come to the right place.

At time of writing had just update to 8.15.0 due to Critical Vulnerability with Kibana.. Important point to note, for this all to hang together all 3 components of the ELK stack need to be on the same version

Step 1 Identify Current Version You Are Running

sudo docker ps

```
pbr_admin@pbr-lme-k11:~$ sudo docker ps
[sudo] password for pbr_admin:
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS        PORTS                    NAMES
79d7372a6271   docker.elastic.co/kibana/kibana:8.15.0  "/bin/tini -- /bin/b"    2 minutes ago  Up 2 minutes (healthy)  5601/tcp            lme_kibana.1.8b10i2mj8ruh7z5u2iux2z4k1
58a2ac66c8f8   docker.elastic.co/elasticsearch/elasticsearch:8.15.0  "/bin/tini -- /usr/l"    2 minutes ago  Up 2 minutes (healthy)  9200/tcp, 9300/tcp    lme_elasticsearch.1.7uq0mxyzng4l5dqa16sqa75fp
6d0da701fb2d   docker.elastic.co/logstash/logstash:8.15.0  "/usr/local/bin/dock"    2 minutes ago  Up 2 minutes (healthy)  5044/tcp, 9600/tcp    lme_logstash.1.2pobt0ykc70u890u2ckcz3sq
```

Step 1A Download the New Docker Images

TBH not sure if this step is required, but this is what I did and it worked, so thought I'd document it you need to download the 3 images

before you start view the images currently on the system with command

sudo docker image ls

```
pbr_admin@pbr-lme-k11:~$ sudo docker ps
[sudo] password for pbr_admin:
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS        PORTS                    NAMES
79d7372a6271   docker.elastic.co/kibana/kibana:8.15.0  "/bin/tini -- /bin/b"    2 minutes ago  Up 2 minutes (healthy)  5601/tcp            lme_kibana.1.8b10i2mj8ruh7z5u2iux2z4k1
58a2ac66c8f8   docker.elastic.co/elasticsearch/elasticsearch:8.15.0  "/bin/tini -- /usr/l"    2 minutes ago  Up 2 minutes (healthy)  9200/tcp, 9300/tcp    lme_elasticsearch.1.7uq0mxyzng4l5dqa16sqa75fp
6d0da701fb2d   docker.elastic.co/logstash/logstash:8.15.0  "/usr/local/bin/dock"    2 minutes ago  Up 2 minutes (healthy)  5044/tcp, 9600/tcp    lme_logstash.1.2pobt0ykc70u890u2ckcz3sq
```

To pull images from the repos, you can run the following commands.

Make sure to update the version you require - check Elastic documentation for possible issues first.

```
sudo docker pull docker.elastic.co/elasticsearch/elasticsearch:8.15.0
```

```
pbr_admin@pbr-lme-k11:~$ sudo docker pull docker.elastic.co/elasticsearch/elasticsearch:8.15.0
8.15.0: Pulling from elasticsearch/elasticsearch
bef9b66d64c1: Pull complete
1fd631a7f77b: Pull complete
be0505076ce2: Pull complete
4ca545ee6d5d: Pull complete
dc9db6ea5ff2: Pull complete
dd7fea410473: Pull complete
7aaf9e867095: Pull complete
8c9e11efa7e5: Pull complete
8d0f979b52e8: Pull complete
8cad84c16df: Pull complete
Digest: sha256:84a73ced8390c059e7bc2858595c68dc36e6f8bdb98895dcab0074eda35ac96e
Status: Downloaded newer image for docker.elastic.co/elasticsearch/elasticsearch:8.15.0
docker.elastic.co/elasticsearch/elasticsearch:8.15.0
```

```
sudo docker pull docker.elastic.co/kibana/kibana:8.15.0
```

```
8.15.0: Pulling from kibana/kibana
bef9b66d64c1: Already exists
f6b84247827c: Pull complete
b1a5a823635f: Pull complete
7ff3c1349574: Pull complete
acaf211e68f0: Pull complete
e6482380a03e: Pull complete
4ca545ee6d5d: Pull complete
5d37849b8bfb: Pull complete
38a4f0ace1b9: Pull complete
93469ea36cfe: Pull complete
40d69daa44b4: Pull complete
9bcdcf41232d: Pull complete
50c27f863681: Pull complete
Digest: sha256:ff5f6b9a49f410658b74b337b102c302bbeb52b470efe1f0e3af3c7526fbe0e7
Status: Downloaded newer image for docker.elastic.co/kibana/kibana:8.15.0
docker.elastic.co/kibana/kibana:8.15.0
```

```
sudo docker pull docker.elastic.co/logstash/logstash:8.15.0
```

```
pbr_admin@pbr-lme-k11:~$ sudo docker pull docker.elastic.co/logstash/logstash:8.15.0
8.15.0: Pulling from logstash/logstash
bef9b66d64c1: Already exists
bbe25ee946c: Pull complete
26488eb933d4: Pull complete
45b1fd29c944: Pull complete
4ca545ee6d5d: Pull complete
12a8edbceb65: Pull complete
7d5f2a507bae: Pull complete
6eecd48a52f: Pull complete
46ef65f74cf8: Pull complete
1ebb4dc57ea8: Pull complete
d0fca5b18401: Pull complete
db33482f1e04: Pull complete
Digest: sha256:73a30fb57f305c0a6e0018ef37aeda016b5a3578a95530af13579382938cc3d6
Status: Downloaded newer image for docker.elastic.co/logstash/logstash:8.15.0
docker.elastic.co/logstash/logstash:8.15.0
```

Now if you enter the command **sudo docker image ls** you should see the new images you have acquired listed

Step 2 Edit the Docker Compose file and Pull the Images

Edit the docker compose file, in the case of LME, it can be found at /opt/lme/Chapter 3 Files/docker-compose-stack-live.yml

Copy of this file is attached to this article and can be accessed here [docker-compose-stack.yml](#)

You need to edit the 3 lines that specify the new image you want to use (in this example these are the images before I changed them to be 8.15.0)

```
elasticsearch:
  image: docker.elastic.co/elasticsearch/elasticsearch:8.11.1
```

```
kibana:
  # depends_on:
  # elasticsearch:
  #   condition: service_healthy
  image: docker.elastic.co/kibana/kibana:8.11.1
```

```
logstash:
  image: docker.elastic.co/logstash/logstash:8.11.1
```

the image name needs to be the same name as the image you have downloaded in previous step once updated and saved run the following command

```
sudo docker compose -f /opt/lme/Chapter\ 3\ Files/docker-compose-stack-live.yml pull
```

```
pbr_admin@pbr-lme-k11:~$ sudo docker compose -f /opt/lme/Chapter\ 3\ Files/docker-compose-stack-live.yml pull
WARN[0000] /opt/lme/Chapter 3 Files/docker-compose-stack-live.yml: 'version' is obsolete
[+] Pulling 3/3
✔ elasticsearch Pulled
✔ logstash Pulled
✔ kibana Pulled
```

Step 3 Update the Docker Service with the New Images

sudo docker service ls - will display the services and importantly names & versions running in docker

```
pbr_admin@pbr-lme-k11:~$ sudo docker service ls
ID            NAME                MODE                REPLICAS    IMAGE                                     PORTS
mppts0ige044  lme_elasticsearch   replicated          1/1         docker.elastic.co/elasticsearch/elasticsearch:8.15.0  *:9200->9200/tcp
17avotbhqc55  lme_kibana          replicated          1/1         docker.elastic.co/kibana/kibana:8.15.0  *:443->5601/tcp
ys3oar2or2mo  lme_logstash        replicated          1/1         docker.elastic.co/logstash/logstash:8.15.0  *:5044->5044/tcp
```

sudo docker service update --image docker.elastic.co/elasticsearch/elasticsearch:8.15.0 lme_elasticsearch

where `docker.elastic.co/elasticsearch/elasticsearch:8.15.0` is the new image and `lme_elasticsearch` is the service name

you need to do this for all 3 services

- `lme_elasticsearch`

- ```
sudo docker service update --image docker.elastic.co/elasticsearch/elasticsearch:8.15.0 lme_elasticsearch
```

- `lme_kibana`

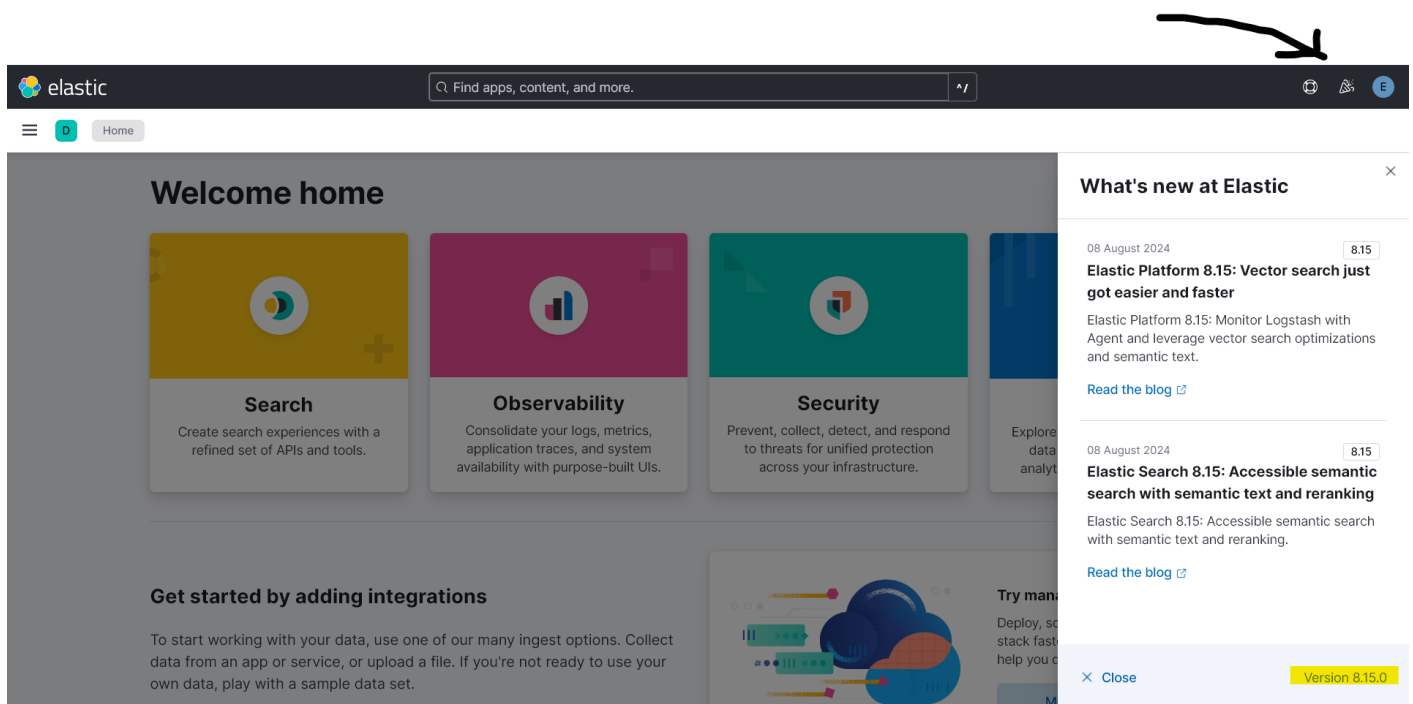
- ```
sudo docker service update --image docker.elastic.co/kibana/kibana:8.15.0 lme_kibana
```

- `lme_logstash`

- ```
sudo docker service update --image docker.elastic.co/logstash/logstash:8.15.0 lme_logstash
```

Now check its all updated and on the correct version with **`sudo docker ps`**

You can also navigate to the web portal `pbr-lme-kl1` and log on , click on pizza icon top right and down the bottom you should see the version listed



---

Revision #5

Created 15 August 2024 03:22:07 by David Diamond

Updated 26 June 2025 11:13:15 by Dylan Healey