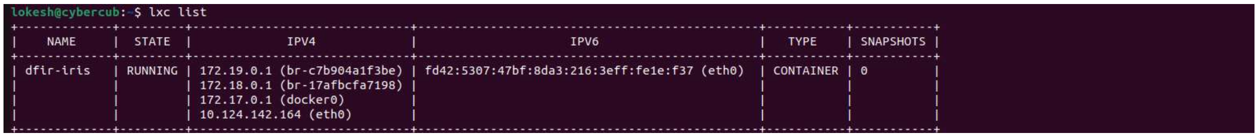
DFIR-IRIS Setup

LXD Container Information:



```
lokesh@cybercub:~$ lxc list
+-------------+---------+------------------------------+----------------------------------------------+-----------+-----------+
|    NAME     |  STATE  |             IPV4             |                     IPV6                     |   TYPE    | SNAPSHOTS |
+-------------+---------+------------------------------+----------------------------------------------+-----------+-----------+
| dfir-iris   | RUNNING | 172.19.0.1 (br-c7b904a1f3be) | fd42:5307:47bf:8da3:216:3eff:fe1e:f37 (eth0) | CONTAINER | 0         |
|             |         | 172.18.0.1 (br-17afbcfa7198) |                                              |           |           |
|             |         | 172.17.0.1 (docker0)         |                                              |           |           |
|             |         | 10.124.142.164 (eth0)        |                                              |           |           |
+-------------+---------+------------------------------+----------------------------------------------+-----------+-----------+
```

Install Docker Engine on Ubuntu LXD Container

Setup Docker's apt repository :

```
root@dfir-iris:~# sudo apt-get update
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:5 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:6 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1854 kB]

root@dfir-iris:~# sudo apt-get install ca-certificates curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ca-certificates is already the newest version (20240203~22.04.1).

root@dfir-iris:~# sudo install -m 0755 -d /etc/apt/keyrings
root@dfir-iris:~# sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o
/etc/apt/keyrings/docker.asc
root@dfir-iris:~# sudo chmod a+r /etc/apt/keyrings/docker.asc

root@dfir-iris:~# echo \
 "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc]
https://download.docker.com/linux/ubuntu \
$(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
sudo tee /etc/apt/sources.list.d/docker.list > /dev/null

root@dfir-iris:~# sudo apt-get update
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
```

Install the Docker packages:

```
root@dfir-iris:~# sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin
docker-compose-plugin -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done

root@dfir-iris:~# sudo docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
c1ec31eb5944: Pull complete
Digest: sha256:d211f485f2dd1dee407a80973c8f129f00d54604d2c90732e8e320e5038a0348
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
 $ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
 https://hub.docker.com/

For more examples and ideas, visit:
 https://docs.docker.com/get-started/
```

Setting Up of Docker Compose

To download and install Compose standalone, run

```
root@dfir-iris:~# sudo curl -SL
https://github.com/docker/compose/releases/download/v2.29.0/docker-compose-linux-x86_64 -o
/usr/local/bin/docker-compose
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
100 60.2M  100 60.2M    0     0  3440k      0  0:00:17  0:00:17 --:--:-- 3814k
```

Apply executable permissions to the standalone binary in the target path for the installation.

```
root@dfir-iris:~# sudo chmod +x /usr/local/bin/docker-compose
```

Test and execute compose commands using docker-compose

```
root@dfir-iris:~# sudo ln -s /usr/local/bin/docker-compose /usr/bin/docker-compose
```

Test the Installation

```
root@dfir-iris:~# docker-compose --version
Docker Compose version v2.29.0
```

```
root@dfir-iris:~# useradd lokesh -m -s /bin/bash
root@dfir-iris:~# usermod lokesh -aG sudo
root@dfir-iris:~# sudo passwd lokesh
New password:
Retype new password:
passwd: password updated successfully
root@dfir-iris:~# su - lokesh
lokesh@dfir-iris:~$
```

Clone the iris-web repository:

```
lokesh@dfir-iris:~$ git clone https://github.com/dfir-iris/iris-web.git
Cloning into 'iris-web'...
remote: Enumerating objects: 41654, done.
remote: Counting objects: 100% (7793/7793), done.
remote: Compressing objects: 100% (1253/1253), done.
```

```
remote: Total 41654 (delta 6833), reused 7359 (delta 6511), pack-reused 33861 (from 1)
Receiving objects: 100% (41654/41654), 30.94 MiB | 3.64 MiB/s, done.
Resolving deltas: 100% (32686/32686), done.
lokesh@dfir-iris:~$ cd iris-web
```

Check out the latest **non-beta** tagged version:

```
lokesh@dfir-iris:~/iris-web$ git checkout v2.3.7
Note: switching to 'v2.3.7'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to false

HEAD is now at 8c355244 Bump version: 2.3.6 → 2.3.7
```

Copy the environment file

```
lokesh@dfir-iris:~/iris-web$ cp .env.model .env
```

Before Running sudo docker-compose build check Errors faced how I debugged

```
lokesh@dfir-iris:~/iris-web/docker/webApp$ sudo docker-compose build
WARN[0000] /home/lokesh/iris-web/docker-compose.yml: the attribute `version` is obsolete, it
will be ignored, please remove it to avoid potential confusion
[+] Building 98.1s (87/87) FINISHED
docker:default
 => [db internal] load build definition from Dockerfile
0.0s
```

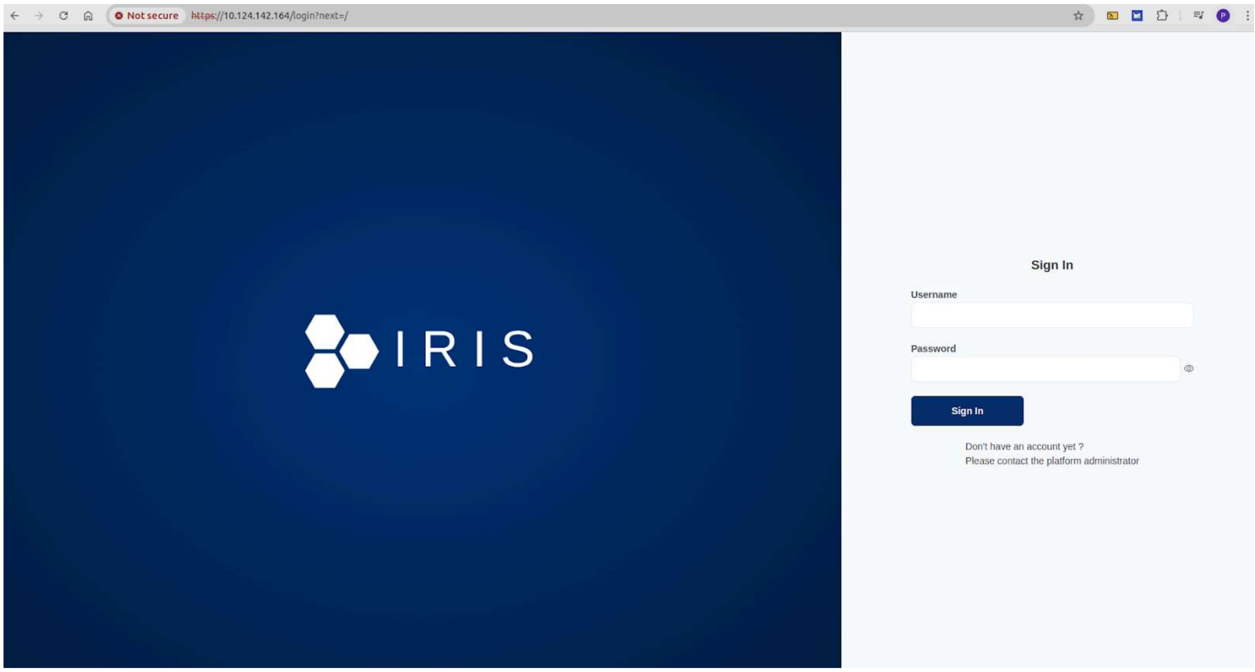
Successful

Start IRIS:

```
lokesh@dfir-iris:~/iris-web$ sudo docker-compose up -d
WARN[0000] /home/lokesh/iris-web/docker-compose.yml: the attribute `version` is obsolete, it
will be ignored, please remove it to avoid potential confusion
[+] Running 5/5
 ✔ Container iriswebapp_db        Running
0.0s
 ✔ Container iriswebapp_rabbitmq  Started
0.1s
 ✔ Container iriswebapp_app       Running
0.0s
 ✔ Container iriswebapp_nginx     Started
0.4s
 ✔ Container iriswebapp_worker    Started
```

IRIS UI

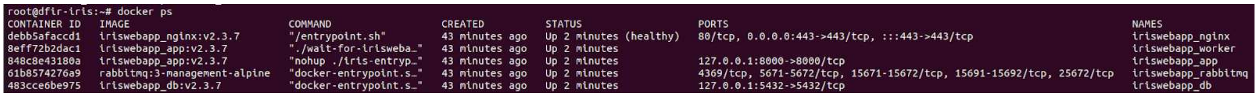
https://IpOfContainer



Not secure https://10.124.142.164/login?next=/

Don't have an account yet ?
Please contact the platform administrator

uname and passwd:

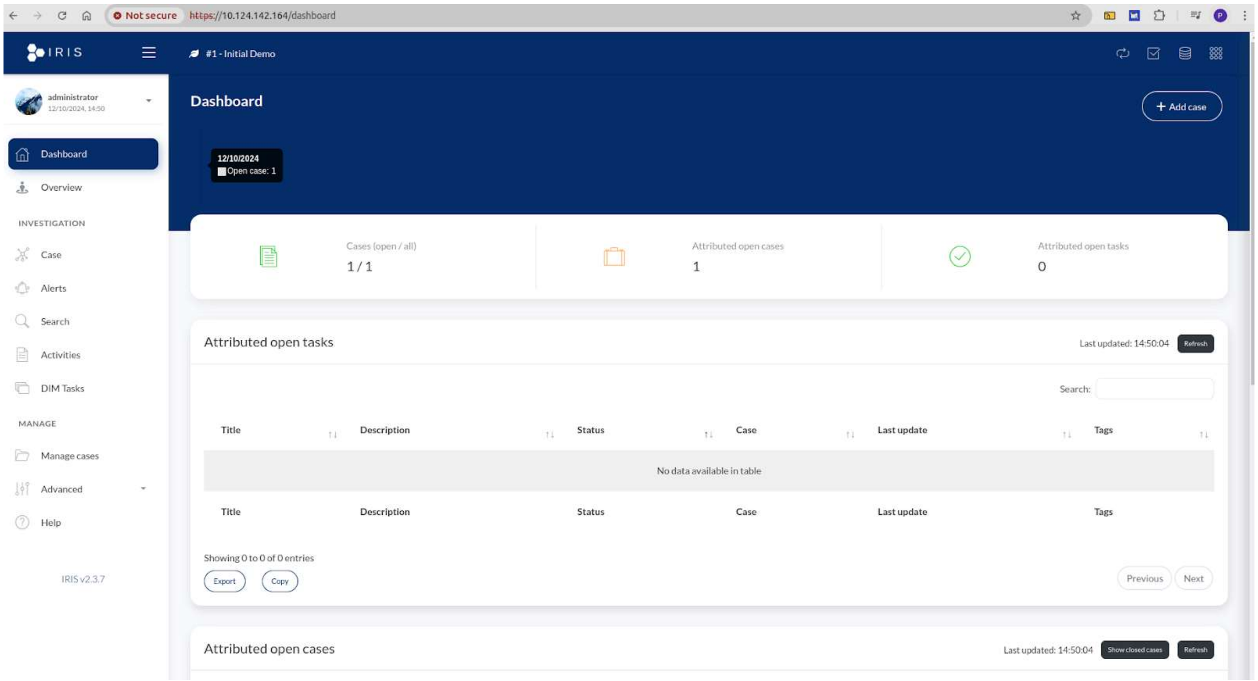


```
root@dfir-iris:~# docker ps
CONTAINER ID   IMAGE                          COMMAND                  CREATED          STATUS                   PORTS                                                                  NAMES
debb5afaccd1   iriswebapp_nginx:v2.3.7        "/entrypoint.sh"         43 minutes ago   Up 2 minutes (healthy)   80/tcp, 0.0.0.0:443->443/tcp, :::443->443/tcp                          iriswebapp_nginx
8eff72b2dac1   iriswebapp_app:v2.3.7          "./wait-for-irisweba…"   43 minutes ago   Up 2 minutes                                                                                    iriswebapp_worker
848c8e43180a   iriswebapp_app:v2.3.7          "nohup ./iris-entryp…"   43 minutes ago   Up 2 minutes             127.0.0.1:8000->8000/tcp                                               iriswebapp_app
61b8574276a9   rabbitmq:3-management-alpine   "docker-entrypoint.s…"   43 minutes ago   Up 2 minutes             4369/tcp, 5671-5672/tcp, 15671-15672/tcp, 15691-15692/tcp, 25672/tcp   iriswebapp_rabbitmq
483cce6be975   iriswebapp_db:v2.3.7           "docker-entrypoint.s…"   43 minutes ago   Up 2 minutes             127.0.0.1:5432->5432/tcp                                               iriswebapp_db
```

you see logs of irisweb_app to get username and password
root@dfir-iris:~# docker logs 848c8e43180a --follow
2024-10-12 08:32:38 :: INFO :: post_init :: run_post_init :: You can now login with user administrator and password >>> n)D;HCOz`<h>x8.[<<< on 443

Username : administrator
Password : n)D;HCOz`<h>x8.[

After Loging in you will get IRIS Administrator UI



Dashboard

12/10/2024
Open case: 1

Cases (open / all) 1 / 1

Attributed open cases 1

Attributed open tasks 0

Attributed open tasks

Last updated: 14:50:04

Search:

Title	Description	Status	Case	Last update	Tags
No data available in table					
Title	Description	Status	Case	Last update	Tags

Showing 0 to 0 of 0 entries

Attributed open cases

Last updated: 14:50:04

Errors and Debugged

```
lokesh@dfir-iris:~/iris-web$ sudo docker-compose build
[sudo] password for lokesh:
WARN[0000] /home/lokesh/iris-web/docker-compose.yml: the attribute `version` is obsolete, it
will be ignored, please remove it to avoid potential confusion
[+] Building 32.6s (10/10) FINISHED
docker:default
 => [db internal] load build definition from Dockerfile
0.0s
 => => transferring dockerfile: 969B
0.0s
 => [db internal] load metadata for docker.io/library/postgres:12-alpine
1.8s
 => [db internal] load .dockerignore
0.0s
 => => transferring context: 2B
0.0s
 => [db internal] load build context
0.0s
 => => transferring context: 36B
0.0s
```

```
 => [db 1/2] FROM
docker.io/library/postgres:12-alpine@sha256:76685db4bc5175623bc5d8fa68d6c9ba548aeccd7
64158709b781ba3c37b8d44                                                    0.0s
 => CACHED [db 2/2] COPY create_user.sh   /docker-entrypoint-initdb.d/10-create_user.sh
0.0s
 => [db] exporting to image
0.0s
 => => exporting layers
0.0s
 => => writing image
sha256:c0311edc3cf677af22d0fe7785219427083ba670cccccc1d4ff9575be5d5f25b
0.0s
 => => naming to docker.io/library/iriswebapp_db:v2.3.7
0.0s
 => [db] resolving provenance for metadata file
0.0s
 => [app internal] load build definition from Dockerfile
0.0s
 => => transferring dockerfile: 2.35kB
0.0s
 => WARN: FromAsCasing: 'as' and 'FROM' keywords' casing do not match (line 38)
0.0s
 => ERROR [app internal] load metadata for docker.io/library/python:3.9
30.7s
------
 > [app internal] load metadata for docker.io/library/python:3.9:
------
failed to solve: DeadlineExceeded: DeadlineExceeded: DeadlineExceeded: python:3.9: failed to
resolve source metadata for docker.io/library/python:3.9: failed to authorize: DeadlineExceeded:
failed to fetch anonymous token: Get
"https://auth.docker.io/token?scope=repository%3Alibrary%2Fpython%3Apull&service=registry.d
ocker.io": dial tcp [2600:1f18:2148:bc01:20a3:9c3e:d4a7:9fb]:443: i/o timeout
```

Solution:

```
lokesh@dfir-iris:~/iris-web$ curl -fsSL get.docker.com | sh
# Executing docker install script, commit: 39040d838e8bcc48c23a0cc4117475dd15189976
Warning: the "docker" command appears to already exist on this system.

If you already have Docker installed, this script can cause trouble, which is
why we're displaying this warning and provide the opportunity to cancel the
installation.

If you installed the current Docker package using this script and are using it
```

```
again to update Docker, you can safely ignore this message.

You may press Ctrl+C now to abort this script.
+ sleep 20
+ sudo -E sh -c apt-get -qq update >/dev/null
```

```
lokesh@dfir-iris:~/iris-web$ sudo docker-compose build
WARN[0000] /home/lokesh/iris-web/docker-compose.yml: the attribute `version` is obsolete, it
will be ignored, please remove it to avoid potential confusion
[+] Building 53.3s (18/37)
docker:default
 => [db internal] load build definition from Dockerfile
0.0s
 => => transferring dockerfile: 969B
0.0s
 => [db internal] load metadata for docker.io/library/postgres:12-alpine
1.7s
 => [db internal] load .dockerignore
0.0s
 => => transferring context: 2B
0.0s
 => [db internal] load build context
0.0s

48.47   × Running setup.py install for splunk-hec did not run successfully.
48.47   │ exit code: 1
48.47   ╰─> [39 lines of output]
48.47       /opt/venv/lib/python3.9/site-packages/setuptools/_distutils/cmd.py:66:
SetuptoolsDeprecationWarning: setup.py install is deprecated.
48.47       !!
48.47
48.47               ********************************************************************************
48.47               Please avoid running ``setup.py`` directly.
48.47               Instead, use pypa/build, pypa/installer or other
48.47               standards-based tools.
48.47
48.47               See https://blog.ganssle.io/articles/2021/10/setup-py-deprecated.html for details.
48.47               ********************************************************************************
```

```
48.47
48.47      !!
48.47        self.initialize_options()
48.47      Traceback (most recent call last):
48.47        File "<string>", line 2, in <module>
48.47        File "<pip-setuptools-caller>", line 34, in <module>
48.47        File
"/tmp/pip-install-7v5tvs9r/splunk-hec_f3cc9301a6cd413d824f7f452bd477af/setup.py", line 13, in
<module>
48.47          setup(name='Splunk-HEC',
48.47        File "/opt/venv/lib/python3.9/site-packages/setuptools/_distutils/core.py", line 183, in
setup
48.47          return run_commands(dist)
48.47        File "/opt/venv/lib/python3.9/site-packages/setuptools/_distutils/core.py", line 199, in
run_commands
48.47          dist.run_commands()
48.47        File "/opt/venv/lib/python3.9/site-packages/setuptools/_distutils/dist.py", line 954, in
run_commands
48.47          self.run_command(cmd)
48.47        File "/opt/venv/lib/python3.9/site-packages/setuptools/dist.py", line 950, in
run_command
48.47          super().run_command(command)
48.47        File "/opt/venv/lib/python3.9/site-packages/setuptools/_distutils/dist.py", line 972, in
run_command
48.47          cmd_obj.ensure_finalized()
48.47        File "/opt/venv/lib/python3.9/site-packages/setuptools/_distutils/cmd.py", line 111, in
ensure_finalized
48.47          self.finalize_options()
48.47        File "/opt/venv/lib/python3.9/site-packages/setuptools/command/install.py", line 67,
in finalize_options
48.47          super().finalize_options()
48.47        File "/opt/venv/lib/python3.9/site-packages/setuptools/_distutils/command/install.py",
line 408, in finalize_options
48.47          'dist_fullname': self.distribution.get_fullname(),
48.47        File "/opt/venv/lib/python3.9/site-packages/setuptools/_core_metadata.py", line 267,
in get_fullname
48.47          return _distribution_fullname(self.get_name(), self.get_version())
48.47        File "/opt/venv/lib/python3.9/site-packages/setuptools/_core_metadata.py", line 285,
in _distribution_fullname
48.47          canonicalize_version(version, strip_trailing_zero=False),
48.47      TypeError: canonicalize_version() got an unexpected keyword argument
'strip_trailing_zero'
48.47      [end of output]
48.47
```

```
48.47   note: This error originates from a subprocess, and is likely not a problem with pip.
48.47 error: legacy-install-failure
48.47


48.47 × Encountered error while trying to install package.
48.47  ╰─> splunk-hec
48.47
48.47 note: This is an issue with the package mentioned above, not pip.
48.47 hint: See above for output from the failure.
48.74
48.74 [notice] A new release of pip is available: 23.0.1 -> 24.2
48.74 [notice] To update, run: pip install --upgrade pip
------
failed to solve: process "/bin/sh -c pip3 install -r requirements.txt" did not complete successfully:
exit code: 1
```

Debugging
Find DockerFile to edit

```
lokesh@dfir-iris:~/iris-web$ ls
CODESTYLE.md  CONFIGURATION.md  CONTRIBUTING.md  LICENSE.txt  README.md
SECURITY.md  certificates  deploy  docker  docker-compose.yml  get-docker.sh  img  scripts
source  upgrades
lokesh@dfir-iris:~/iris-web$ cd docker/

lokesh@dfir-iris:~/iris-web/docker$ cd webApp/
lokesh@dfir-iris:~/iris-web/docker/webApp$ ls
Dockerfile  Dockerfile.k8s  iris-entrypoint.sh  wait-for-iriswebapp.sh

lokesh@dfir-iris:~/iris-web/docker/webApp$ sudo docker-compose build
```

```
FROM python:3.9 AS compile-image
RUN apt-get update

RUN python -m venv /opt/venv
# Make sure we use the virtualenv:
ENV PATH="/opt/venv/bin:$PATH"

COPY source/dependencies /dependencies
COPY source/requirements.txt

RUN pip3 install --upgrade pip setuptools    #Added
RUN pip3 install wheel                        #Added
RUN pip3 install -r requirements.txt
```

```
lokesh@dfir-iris:~/iris-web/docker/webApp$ sudo docker-compose build
WARN[0000] /home/lokesh/iris-web/docker-compose.yml: the attribute `version` is obsolete, it
will be ignored, please remove it to avoid potential confusion
[+] Building 98.1s (87/87) FINISHED
docker:default
 => [db internal] load build definition from Dockerfile
0.0s
```

Successful