AIL Installation
(Sample Configuration)

AIL = **A**nalysis of **I**nformation **L**eaks

This document is not guaranteed for your system.

2021 March 7

AIL OVA File Download & Import

Get the AIL OVA file
https://www.circl.lu/ail-images/latest/
(AIL_master@5cc4da2.ova [2.5G] (As of 2021 March 7))

Import AIL OVA file on VirtualBos

Change Network Adapter
[NAT] -> [Bridge Adapter]
（If you can, increase Main Memory, CPUs and Video Memory）

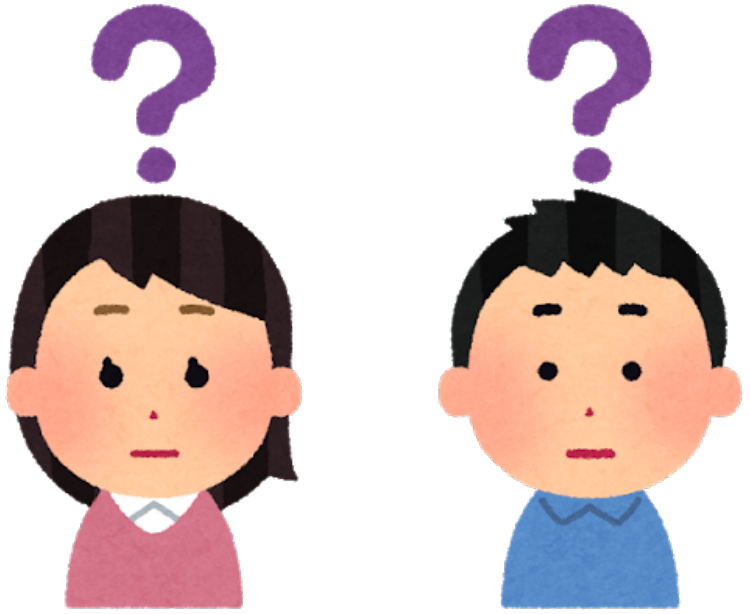
Login OS and change some configurations

Login OS（Ubuntu 18.04）
ID/Password = ail/ail

```
localectl status
sudo localectl set-keymap jp106
sudo localectl status
date
sudo timedatectl set-timezone Asia/Tokyo
date
sudo reboot
```

Verify IP Address

ifconfig



Change SSH Configuration

```
sudo vim /etc/ssh/sshd_config

(Before)
#PasswordAuthentication yes
#PermitEmptyPasswords no
->
(After)
PasswordAuthentication yes
PermitEmptyPasswords no
```

```
sudo service ssh status
sudo service ssh restart
sudo service ssh status
```

Change core.cfg Configuration

```
sudo vim /home/ail/AIL-framework/configs/core.cfg

(Before)
pystemonpath = /home/pystemon/pystemon/
->
(After)
pystemonpath = /home/ail/pystemon/

(Before)
activate_crawler = False
->
(After)
activate_crawler = True
```

Install pystemon

```
cd /home/ail/
mv pystemon pystemon_old
git clone https://github.com/cvandeplas/pystemon
cd pystemon
sudo pip3 install -r requirements.txt
```

Change pystemon.yaml Configuration (1/4)

```
sudo vim /home/ail/pystemon/pystemon.yaml

(Before)
  mongo:
    storage-classname:    MongoStorage
    save: no              # Keep a copy of pasties that triggered alerts
    save-all: no          # Keep a copy of all pasties
    (略)
    user:
    password:
->
(After)
  mongo:
    storage-classname:    MongoStorage
    save: yes             # Keep a copy of pasties that triggered alerts
    save-all: yes         # Keep a copy of all pasties
    (略)
     user: "pystemon"
     password: "pystemon”
```

Change pystemon.yaml Configuration (2/4)

```
(Before)
  redis:
    storage-classname:    RedisStorage
    save: no              # Keep a copy of pasties that triggered alerts
    save-all: no          # Keep a copy of all pasties
->
(After)
  redis:
    storage-classname:    RedisStorage
    save: yes             # Keep a copy of pasties that triggered alerts
    save-all: yes         # Keep a copy of all pasties

(Before)
  pastebin.com:
    enable: no
->
(After)
  pastebin.com:
    enable: yes
```

Change pystemon.yaml Configuration (3/4)

```
(Before)
  gist.github.com:
    enable: no
->
(After)
  gist.github.com:
    enable: yes

(Before)
  kpaste.net:
    enable: no
->
(After)
  kpaste.net:
    enable: yes
```

Change pystemon.yaml Configuration (4/4)

```
(Before)
  ideone.com:
    enable: no
->
(After)
  ideone.com:
    enable: yes
```

Change LAUNCH.sh Configuration

```
sudo vim /home/ail/AIL-framework/bin/LAUNCH.sh
(Before)
    ENV_PY="${DIR}/AILENV/bin/python"
    export AIL_VENV=${AIL_HOME}/AILENV/
->
(After)
    ENV_PY="${DIR}AILENV/bin/python"
    export AIL_VENV=${AIL_HOME}AILENV/
```

Change Flask_server.py Configuration

```
sudo vim /home/ail/AIL-framework/var/www/Flask_server.py
(Before)
    app.run(host=host, port=FLASK_PORT, threaded=True,
ssl_context=ssl_context)
->
(After)
    app.run(host="0.0.0.0", port=FLASK_PORT, threaded=True,
ssl_context=ssl_context)
```

Change mongostorage.py Configuration

vim /home/ail/pystemon/pystemon/storage/mongostorage.py
(Before)
import os
->
(After)
import os,sys
sys.path.append('/usr/local/lib/python3.6/dist-packages')
sys.path.append('/home/ail/pystemon/pystemon')
sys.path.append('/home/ail/pystemon')

Change rc.local Configuration

```
sudo vim /etc/rc.local
(Before)
#!/bin/sh -e
sudo -u ail bash /home/ail/AIL-framework/bin/LAUNCH.sh -l
sudo -u ail bash /home/ail/AIL-framework/bin/LAUNCH.sh -f
exit 0
->
(After)
#!/bin/sh -e
sudo -u ail bash /home/ail/AIL-framework/bin/LAUNCH.sh -l
sudo -u ail bash /home/ail/AIL-framework/bin/LAUNCH.sh -f
sudo -u ail bash /home/ail/AIL-framework/bin/LAUNCH.sh -c
exit 0
```

Install MongoDB

```
sudo apt update
sudo apt install mongodb-server
sudo service mongodb status
sudo systemctl enable mongodb
```

Ninja - a covert agent or mercenary in feudal Japan
https://en.wikipedia.org/wiki/Ninja

MongoDB Configuration

```
ail@ail:~$ mongo
 (略)
> use paste
switched to db paste
> db
paste
> db.createUser({
    user: 'pystemon',
    pwd: 'pystemon',
    roles: [
        { role: 'readWrite', db: 'paste' }
    ]
})
Successfully added user: {
        "user" : "pystemon",
        "roles" : [
         {
          "role" : "readWrite",
          "db" : "paste"
         }
        ]
}

> exit
bye
```

Blue letters mean are what I typed/input.

Install pymongo & Reboot OS

```
sudo pip3 install pymongo

sudo reboot
```

Yoshida Shōin: The Revolutionary and Teacher
https://www.nippon.com/en/features/c01801/

Reset Credentials for AIL

```
/home/ail/AIL-framework/bin/LAUNCH.sh –rp

Write down User/Password
   new user created: admin@admin.test
   password: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
   token: yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
```

Login AIL & Set New Password

Access the following AIL from Host OS
https://<AIL IP Address>:7000/

Set New Password
(e.g.: Password1234)

(Supplement) Some command for Troubleshooting

```
screen -r Script_AIL

screen -r Feeder_Pystemon
```

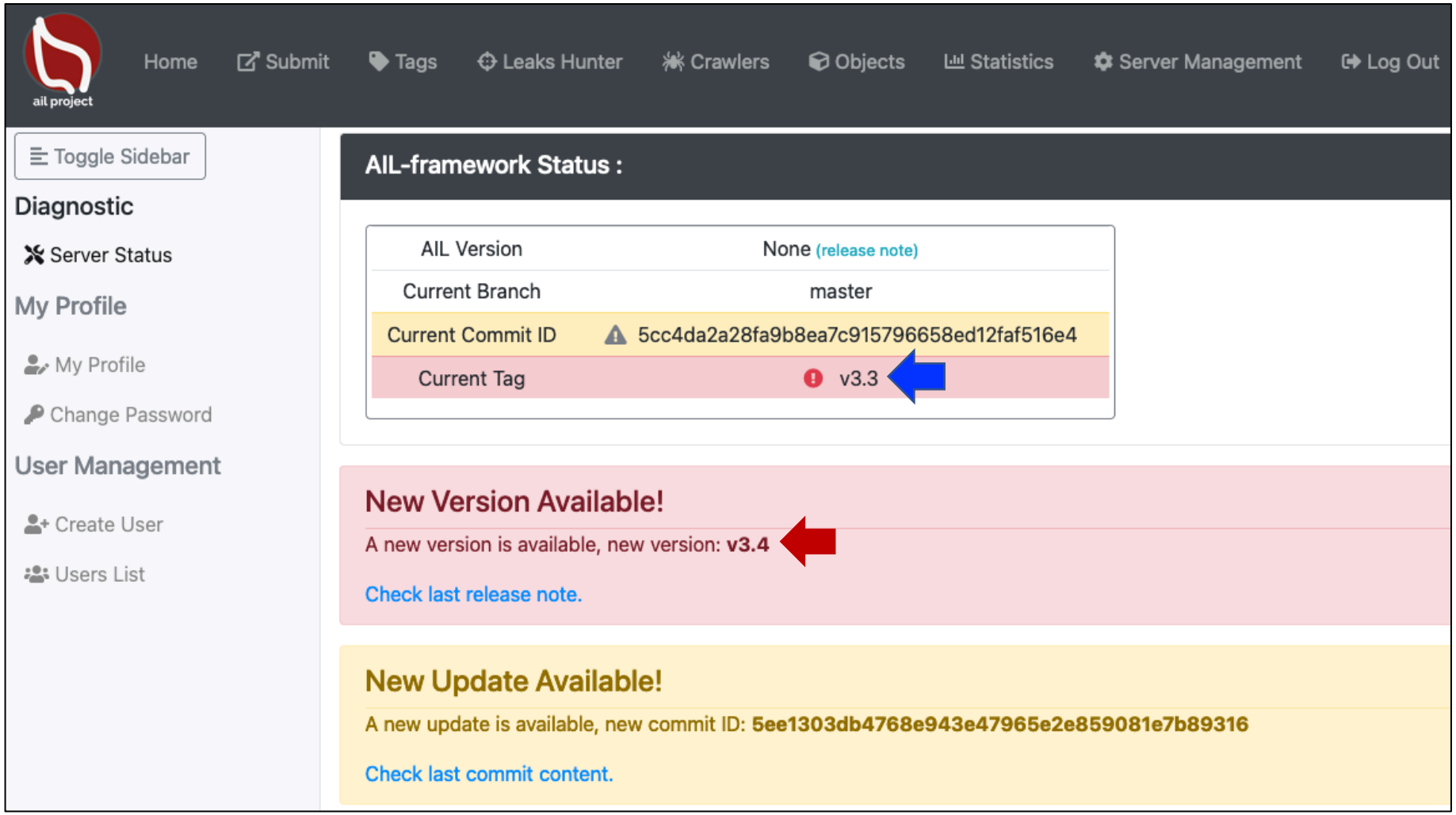
Here is a list of shortcuts to manage/navigate in the screen:

- `Ctrl-a` + `d` detach screen
- `Ctrl-a` + `c` Create new window
- `Ctrl-a` + `n` next window screen
- `Ctrl-a` + `p` previous window screen
- `Ctrl-a` + `"` get a list of all terminal/ select a terminal by name

Feeder_Pystemon not importing · Issue #461 · CIRCL/AIL-framework · GitHub
https://github.com/CIRCL/AIL-framework/issues/461

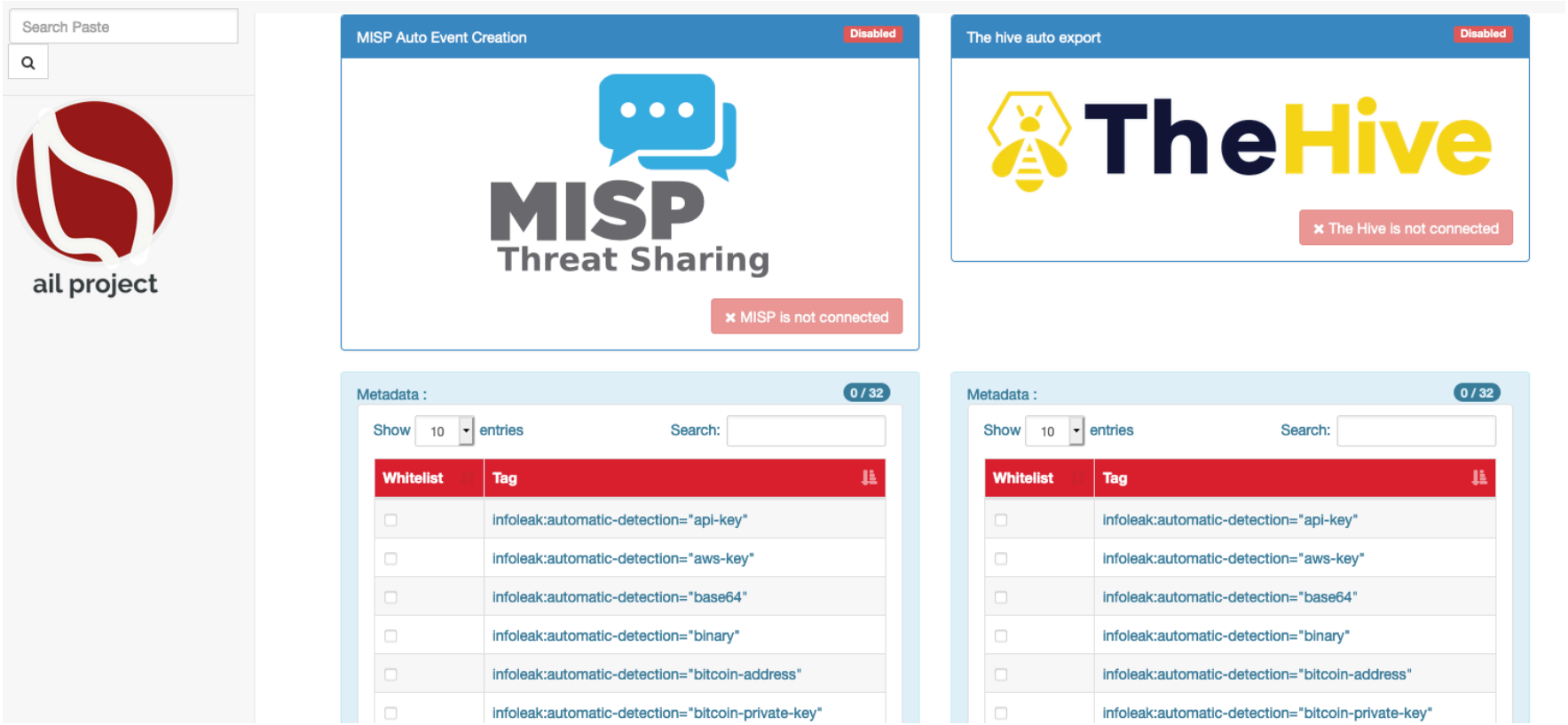
(Supplement) AIL Version

Installed AIL Version is v3.3. Current Latest version is v.3.4.



(Supplement) Collaboration with MISP and TheHive

Seems to be able to collaborated with MISP and TheHive.



MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing
https://www.misp-project.org/
TheHive Project
https://thehive-project.org/

References

AIL Training Materials
https://www.circl.lu/services/ail-training-materials/

CIRCL AIL Training - PeerTube Luxembourg
https://peertube.opencloud.lu/videos/watch/b8cf2c67-df7b-4abc-a81c-a5b381144a20
(CIRCL AIL Framework Movies)

AIL framework - Analysis Information Leak framework
https://github.com/CIRCL/AIL-framework

AIL information leaks analysis and the GDPR in the context of collection, analysis and sharing information leaks
http://www.circl.lu/assets/files/information-leaks-analysis-and-gdpr.pdf