## Python 3 Installation:

sudo yum install yum-utils make wget

sudo yum-builddep python

wget https://www.python.org/ftp/python/3.5.1/Python-3.5.1.tgz

tar xzf Python-3.5.1.tgz

cd Python-3.5.1

./configure

make

sudo make altinstall

python3.5 –V

Python 3.5.1 (means python 3.5 is installed)

Few aliases, which helps in the long run. Add these to your .bashrc

Add these to .bashrc

nano ~/.bashrc

>>and enter the below content over there.

alias python3='/usr/local/bin/python3.5'

alias pip3='/usr/local/bin/pip3.5'

# (without this sudo does not see aliases)

alias sudo='sudo '

Website I followed: https://janikarhunen.fi/how-to-install-python-3-5-1-on-centos-7

## Postfix Installation:

yum -y install postfix cyrus-sasl-plain mailx

systemctl restart postfix

systemctl enable postfix

Open the /etc/postfix/main.cf and add the following lines to the end of the file.

myhostname = hostname.example.com

relayhost = [smtp.gmail.com]:587

smtp\_use\_tls = yes

smtp\_sasl\_auth\_enable = yes

smtp\_sasl\_password\_maps = hash:/etc/postfix/sasl\_passwd

smtp\_tls\_CAfile = /etc/ssl/certs/ca-bundle.crt

smtp\_sasl\_security\_options = noanonymous

smtp\_sasl\_tls\_security\_options = noanonymous

Myhostname is optional

Create a /etc/postfix/sasl\_passwd file and add following line

[smtp.gmail.com]:587 username:password

postmap /etc/postfix/sasl\_passwd

chown root:postfix /etc/postfix/sasl\_passwd\*

chmod 640 /etc/postfix/sasl\_passwd\*

systemctl reload postfix

To test the email server:

*echo "This is a test." | mail -s "test message" user@example.net*

In different window use the below command to check the status:

*tail -f /var/log/maillog*

If there are not enough details in the maillog to determine the problem, then the debug level can be increased by adding the following lines to the /etc/postfix/main.cf.

debug\_peer\_list=smtp.gmail.com

debug\_peer\_level=3

*Restart Postfix:*

systemctl reload postfix

*I followed the below website to install postfix:*

[*https://devops.ionos.com/tutorials/configure-a-postfix-relay-through-gmail-on-centos-7/*](https://devops.ionos.com/tutorials/configure-a-postfix-relay-through-gmail-on-centos-7/)

## Elastalert Installation:

yum install -y epel-release python36 python36-setuptools python36-devel python36-pip gcc

Get the .zip file from <https://github.com/Yelp/elastalert>

Download and using bitwise copy to any folder

Then using the below command:

sudo yum install unzip

unzip elastalert-master.zip -d /etc/ElasAlert/

Locate the Requirement.txt file in elast-master folder

python3.9 -m pip download -r requirements.txt

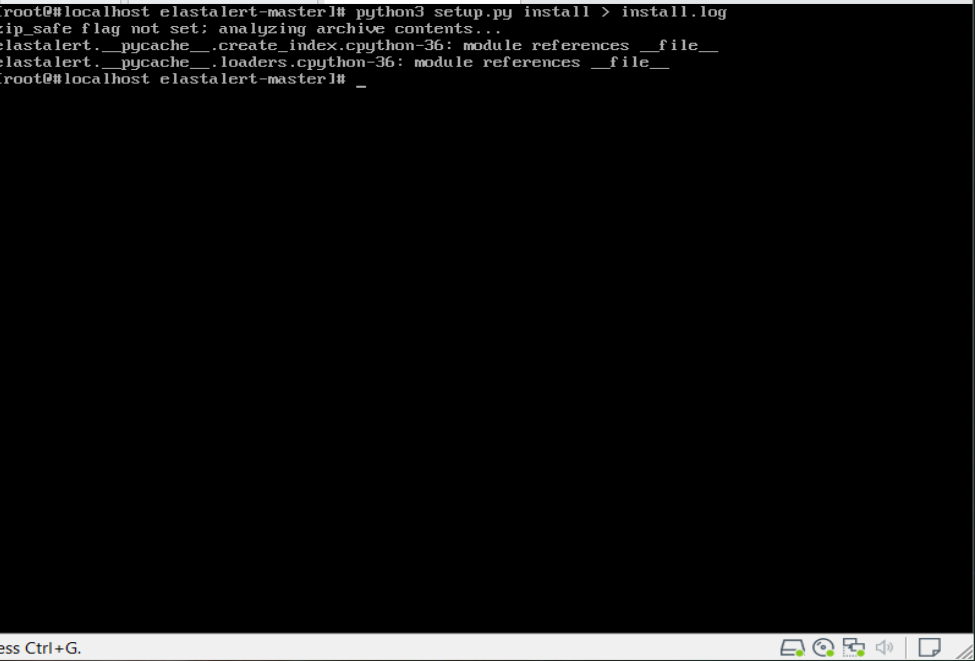
python3.9 -m pip install . --find-links file:/path/to/files --no-index

Edit setup.py:

And comment (#) aws,boto3, jirs,stomp and twilio

python3.9 setup.py install > install.log

You will see something like this, that’s a good sign



elastalert-create-index

Now edit example\_rules/example\_frequency.yaml file

*# From example\_rules/example\_frequency.yaml*

es\_host: elasticsearch.example.com

es\_port: 14900

name: Example rule

type: frequency

index: logstash-\*

num\_events: 50

timeframe:

hours: 4

filter:

- term:

some\_field: "some\_value"

alert:

- "email"

email:

- "elastalert@example.com"

To Test the rule:

elastalert-test-rule example\_rules/example\_frequency.yaml

To run the config file:

elastalert-test-rule --config <path-to-config-file> example\_rules/example\_frequency.yaml

To run ElasAlert

python -m elastalert.elastalert --verbose --rule example\_frequency.yaml

Websites I used for installing ESATAlert:

<https://elastalert.readthedocs.io/en/latest/running_elastalert.html#downloading-and-configuring>

http://shadowtrackers.net/blog/installing-elastalert-on-a-stand-alone-networksystem

## All the comments I used for the above Installation:

1016 sudo apt-get install python-minimal

1017 yum install python-minimal

1018 python --version

1019 yum install -y epel-release python36 python36-setuptools python36-devel python36-pip gcc

1020 mv /home/gadmin/elastalert-master

1021 mv /home/gadmin/elastalert-master/\*.\*

1022 mv /home/gadmin/elastalert-master

1023 pwd

1024 mv /home/gadmin/elastalert-master /root/Elastalert/elastalert/deeESAlert

1025 yum install yum-utils make wget

1026 yum-builddep python

1027 wget https://www.python.org/ftp/python/3.5.1/Python-3.5.1.tgz

1028 tar xzf Python-3.5.1.tgz

1029 cd Python-3.5.1

1030 ./configure

1031 make

1032 nano ~/.bashrc

1033 pwd

1034 nano ~/.bashrc

1035 cd ..

1036 ls

1037 cd python-3.5.1

1038 cd Python-3.5.1

1039 ls

1040 cd ..

1041 ls

1042 cd elastalert-master/

1043 ls

1044 pip3 download -r requirements.txt

1045 pwd

1046 python3 -m pip install . --find-links file:/root/Elastalert/elastalert/deeESAlert/elastalert-master

1047 ls

1048 nano setup.py

1049 python3 setup.py install > install.log

1050 ls

1051 cp config.yaml.example config.yaml

1052 nano config.yaml

1053 elastalert-create-index

1054 nano example\_rules/example\_frequency.yaml

1055 elastalert-test-rule example\_rules/example\_frequency.yaml

1056 pwd

1057 elastalert-test-rule --config /root/Elastalert/elastalert/deeESAlert/elastalert-master

1058 elastalert-test-rule --config /root/Elastalert/elastalert/deeESAlert/elastalert-master example\_rules/example\_frequency.yaml

1059 elastalert-test-rule --config /root/Elastalert/elastalert/deeESAlert/elastalert-master/ example\_rules/example\_frequency.yaml

1060 elastalert-test-rule --config config.yaml example\_rules/example\_frequency.yaml

1061 python -m elastalert.elastalert --verbose --rule example\_frequency.yaml

1062 python3.5 -m elastalert.elastalert --verbose --rule example\_frequency.yaml

1063 python3 -m elastalert.elastalert --verbose --rule example\_frequency.yaml

1064 history

**To test (in 192.168.175.71):**

Su -

cd /root/Elastalert/elastalert/deeESAlert/elastalert-master

python3 -m elastalert.elastalert --verbose --rule example\_frequency.yaml