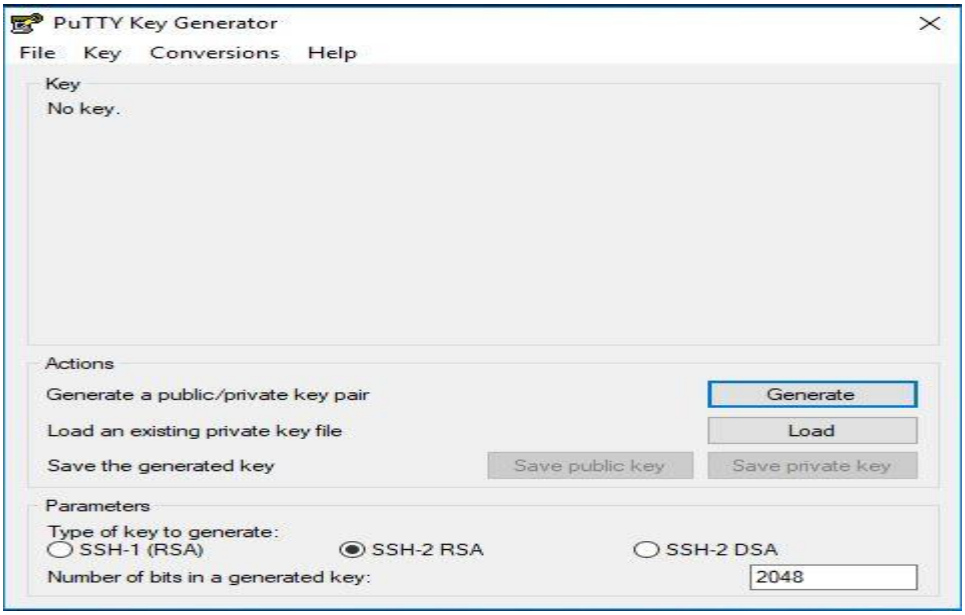
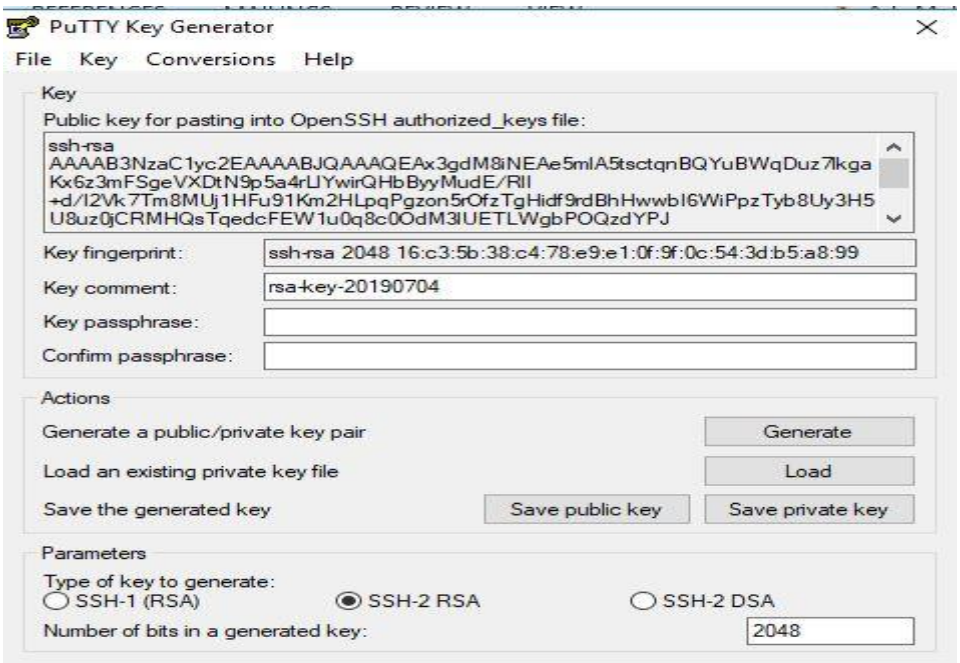
PELATIHAN - PRAKTEK

Membuat Key untuk tujuan remote SSH menggunakan PuttyGent sbb:

1. Buka puttygent



2. Klik: Generate, lalu tunggu beberapa saat sedang proses pembuatan key



3. Klik: Save public key, lalu simpan file ke directory yang di inginkan dan berikan nama, misal: user-public-key => lalu Save
4. Klik: Save private key, lalu simpan file ke directory yang di inginkan dan berikan nama, missal: user-private-key => akan muncul pertanyaan sbb:

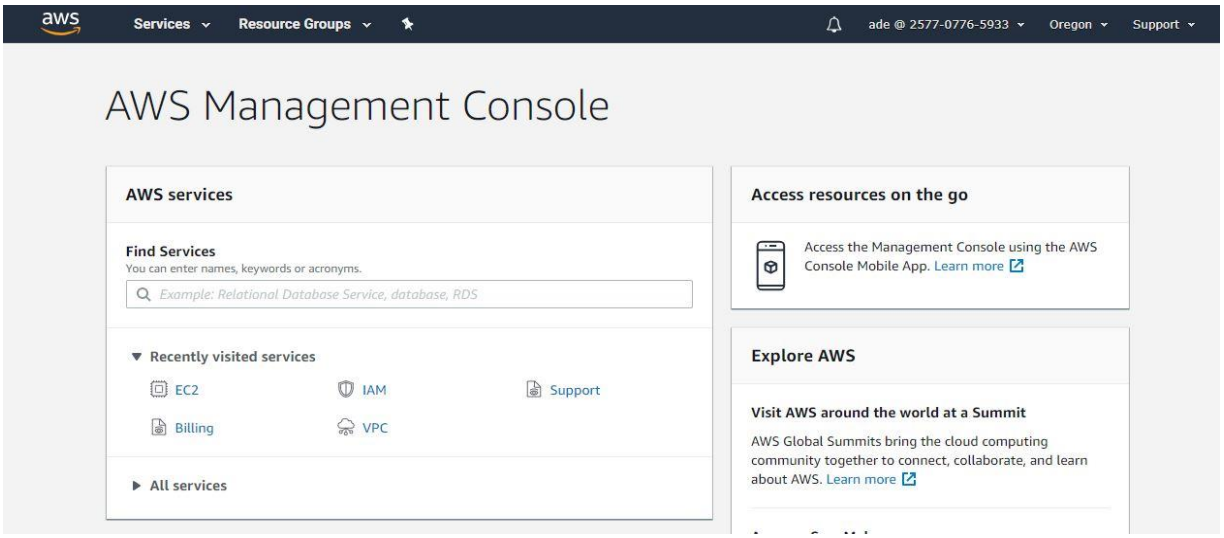
Klik: Yes, lalu arahkan ke directory yang di inginkan dan berikan nama, misal: user-private-key

Login ke dashboard AWS

URL: https://257707765933.signin.aws.amazon.com/console

1. Masukkan IAM username dan Password, dan akan tampil Dashboard AWS
   Note: Pastikan Region menggunakan: N. Virginia

   IAM user name : userlatihan
   Password : @dm1nLatih01



Total: 15 user
- Menggunakan 3 Region: tiap region 5 user
- Total 15 EC2 per Region

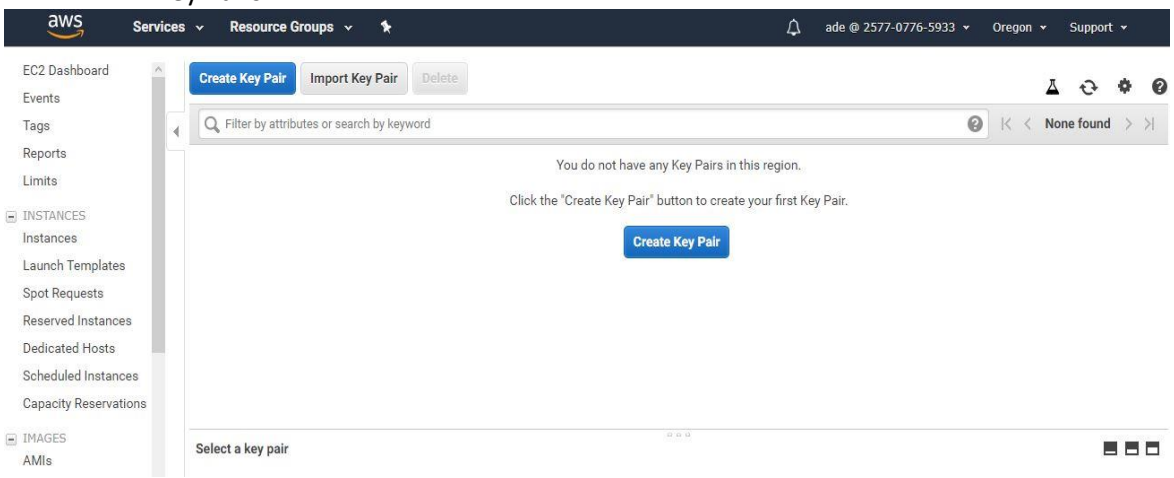
1. N. Virginia => subnet-543fd319|subnet3-default|Default in use-east-1a

2. Ohio => subnet-d8f2fbb0|Default in us-east-2a

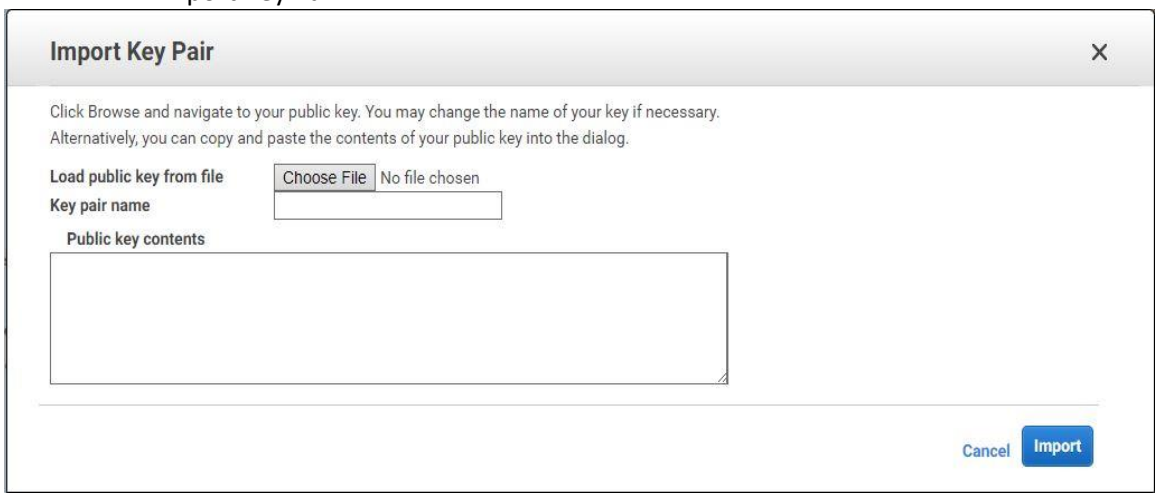
3. N. California => subnet-2b3c3070 | Default in us-west-1b

1.1. Import Key

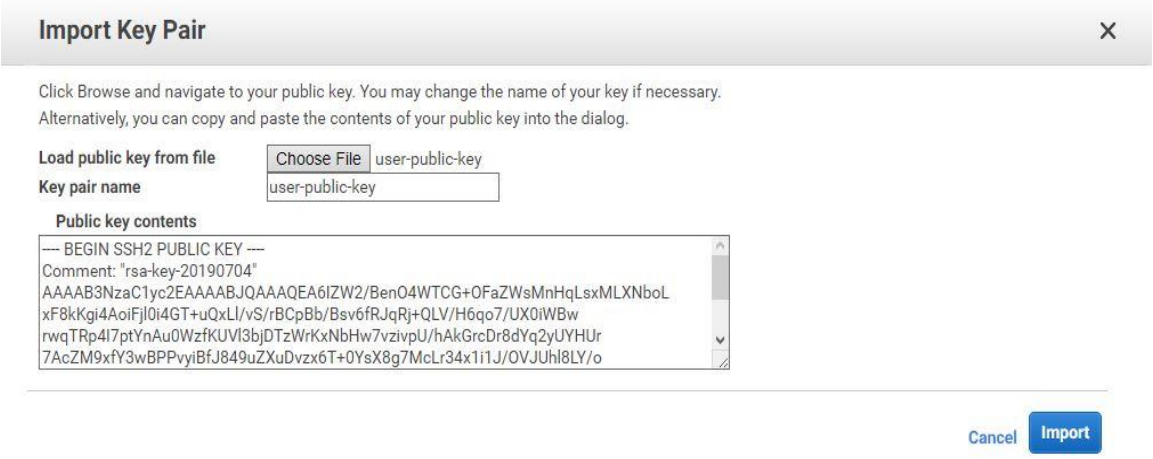
- Klik: Key Pairs



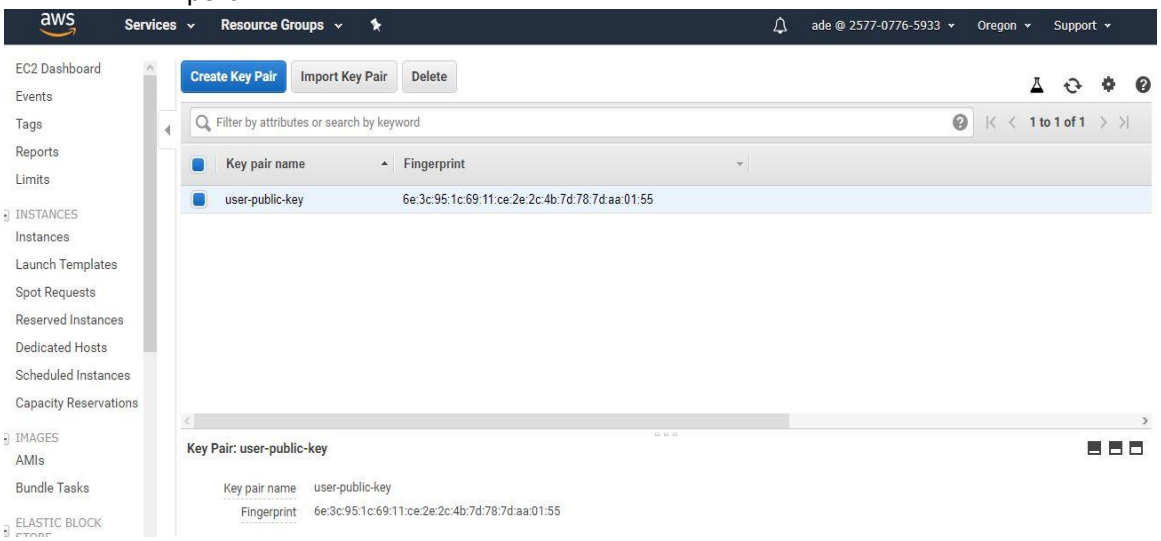
- Klik: Import Key Pair



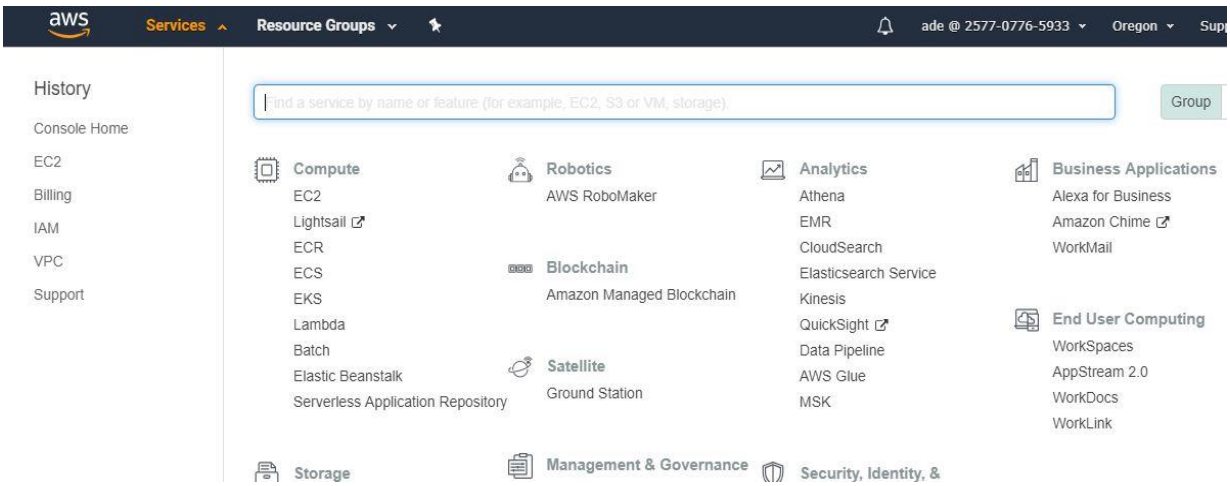
- Klik: Choose File, dan arahkan ke Public Key yang telah dibuat



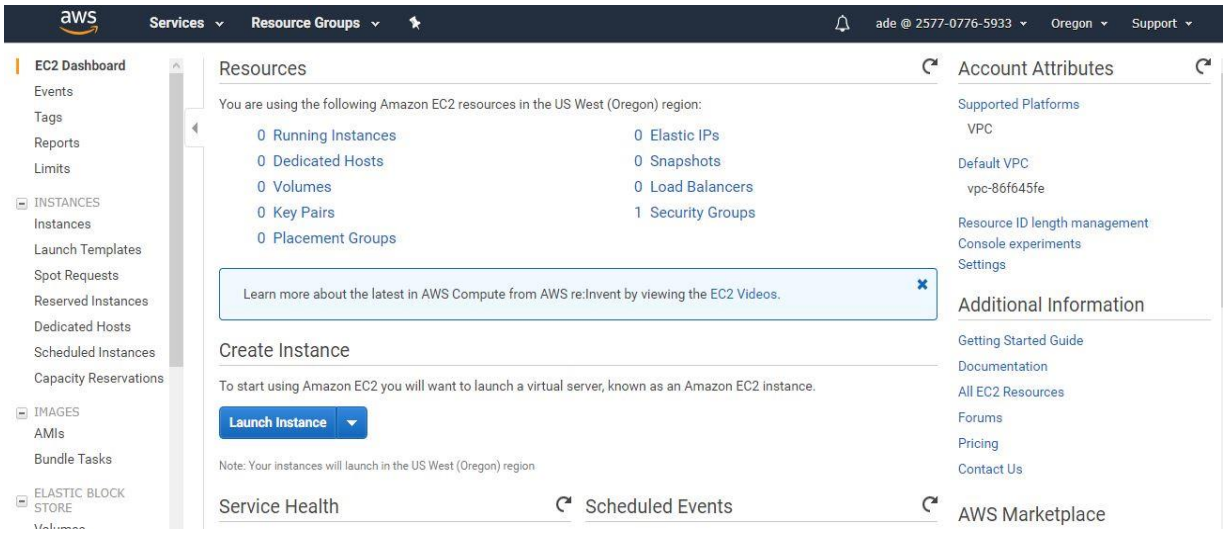
- Klik: Import



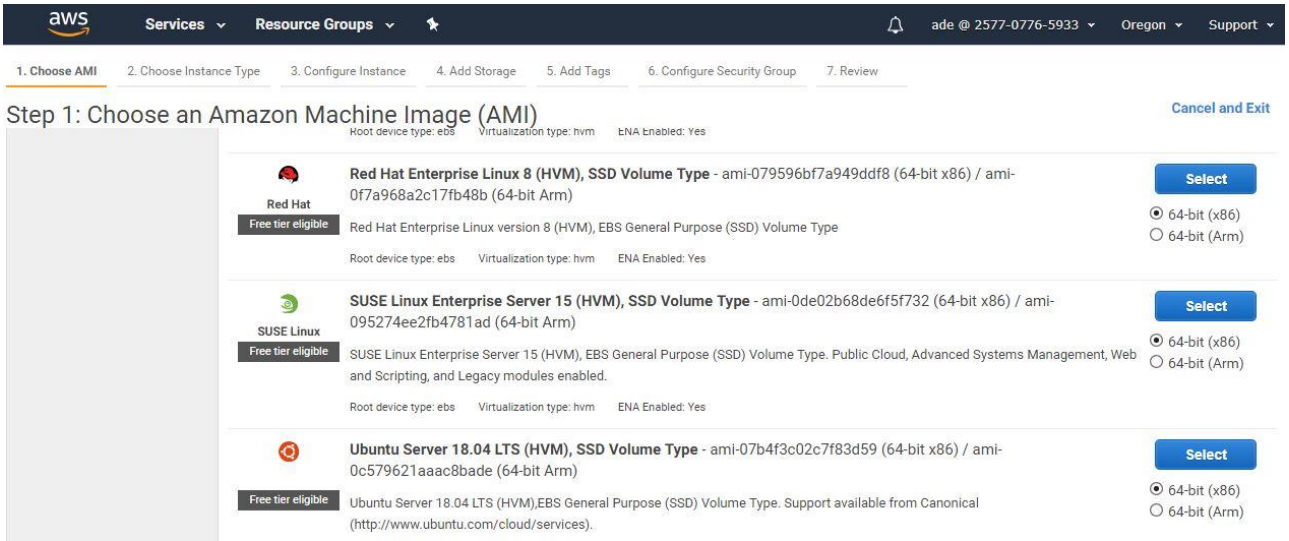
2. Kik tombol : Services di sebelah kiri atas dashboard



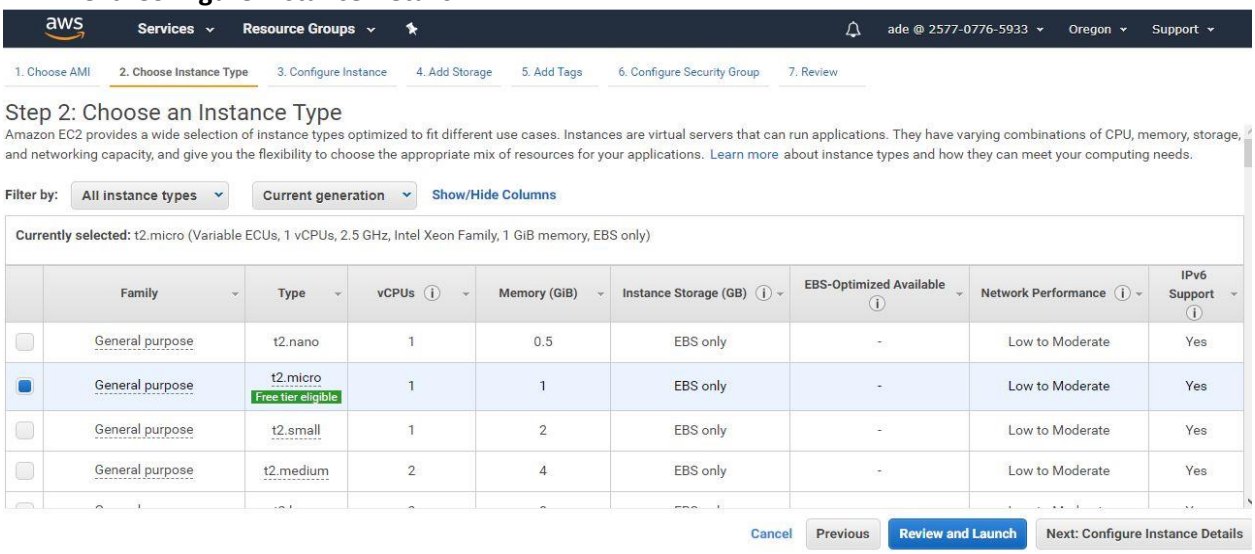
3. **Klik: EC2 yang ada di bagian: Compute**



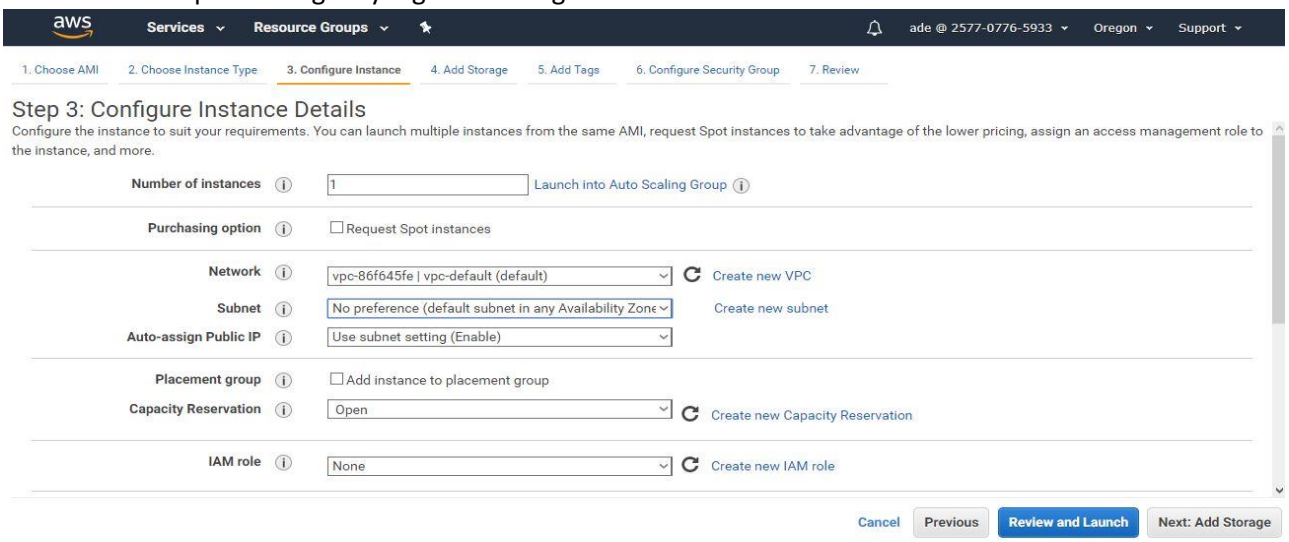
4. Klik: Launch Instance, dan scrool ke bawah ke images OS: Ubuntu Server 18.04 (Free tier eligible), klik: Select



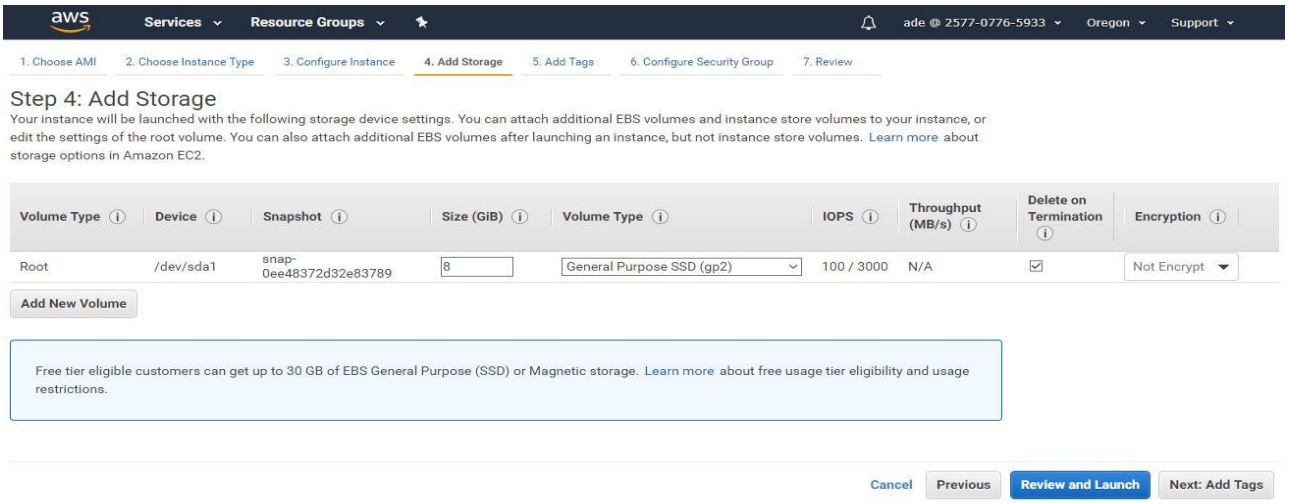
5. **Klik: Next: Configure Instance Details**



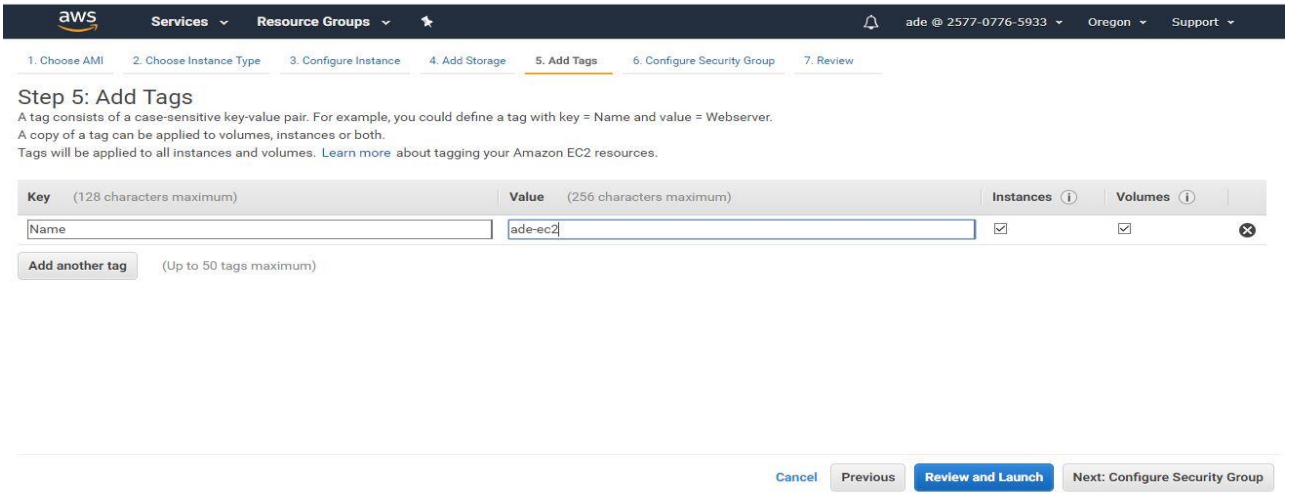
6. Configure Instance sbb:
   - Network => pilih: vpc-default
   - Subnet => pilih: <Region yang telah dibagikan>



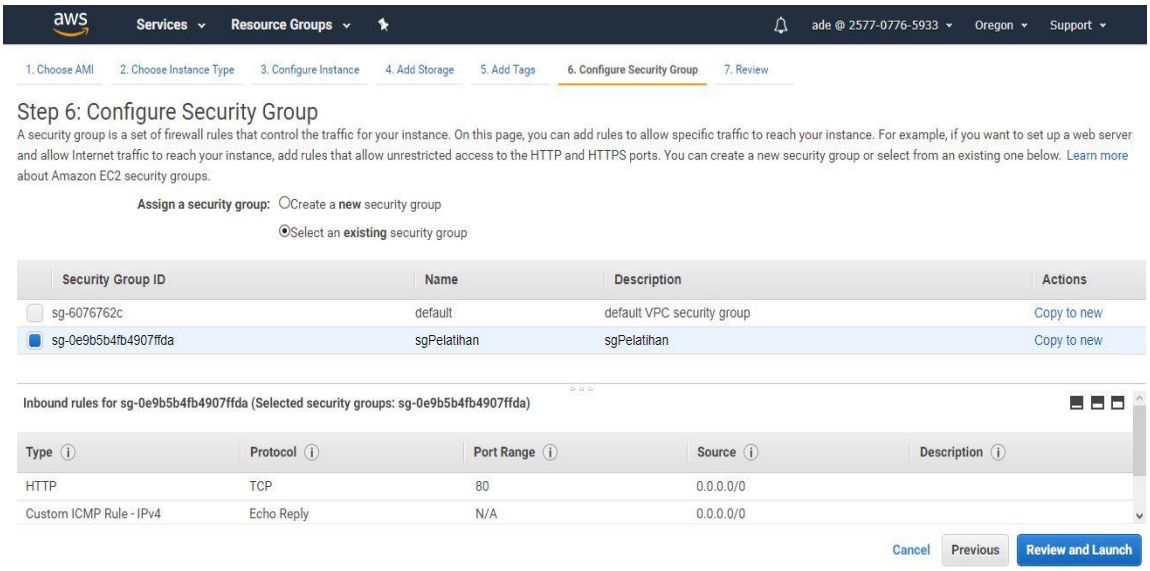
7. Lalu klik => Next: Add Storage



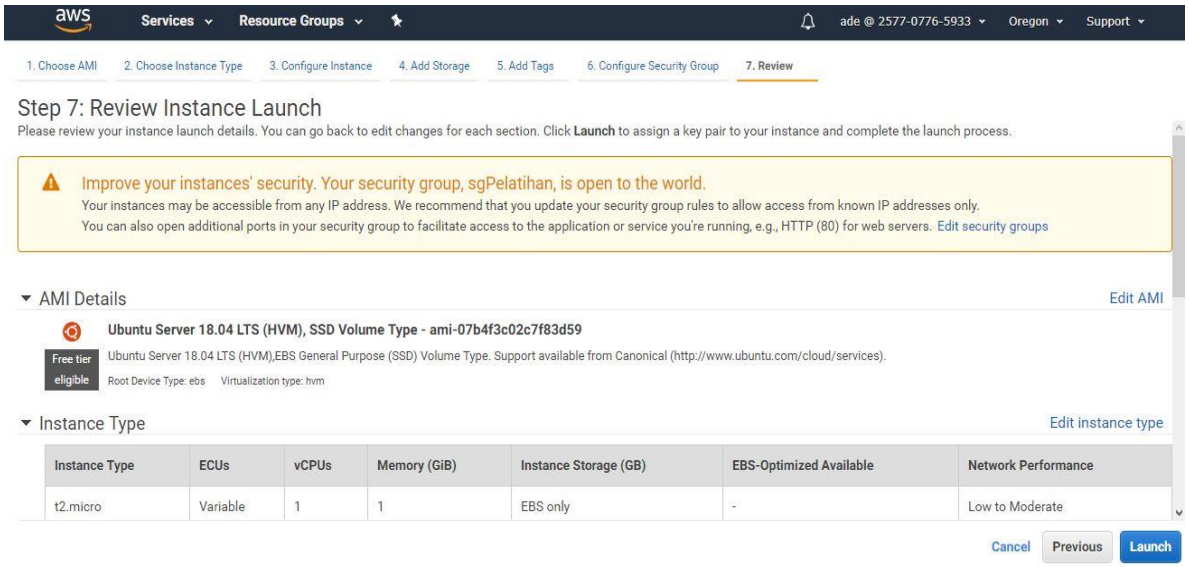
8. **Klik: Next: Add Tags, lalu klik: Add Tag**
   - Pada kolom: Key, ketik: Name
   - Value, ketik missal: lb-namaUser
   - Klik: Next: Configure Security Group



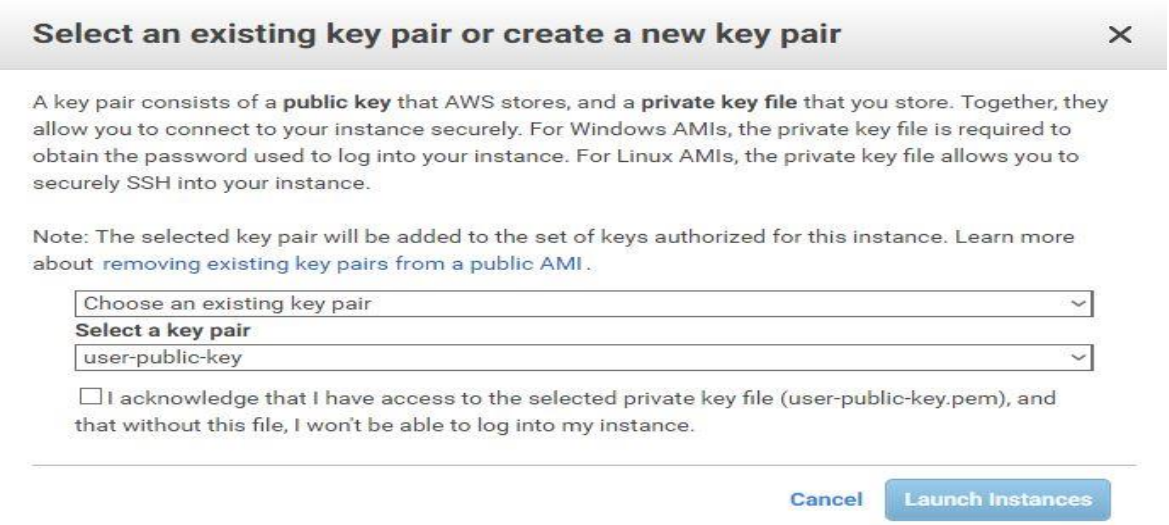
9. **Pada bagian: Assign a security group, pilih: Select an existing security group**
   - Lalu pilih: sgPelatihan



10. Klik: Review and Launch



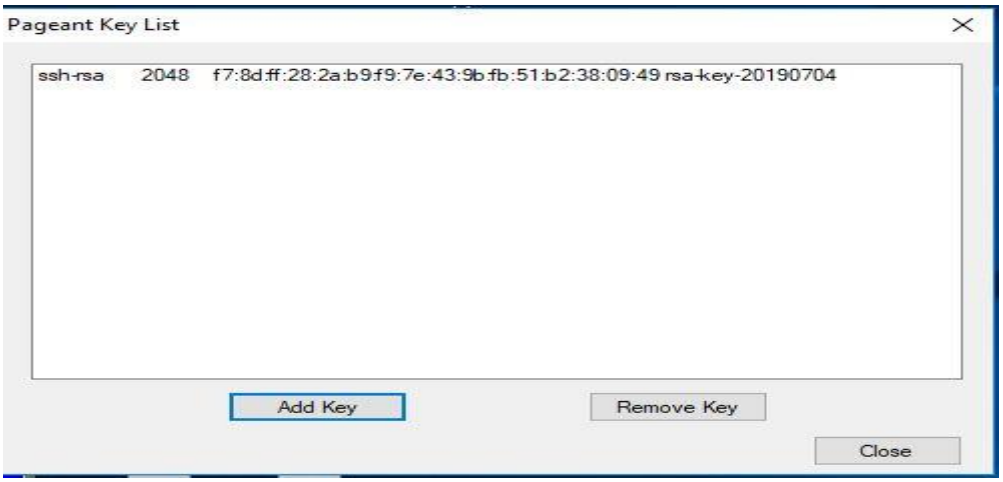
11. **Klik: Launch**



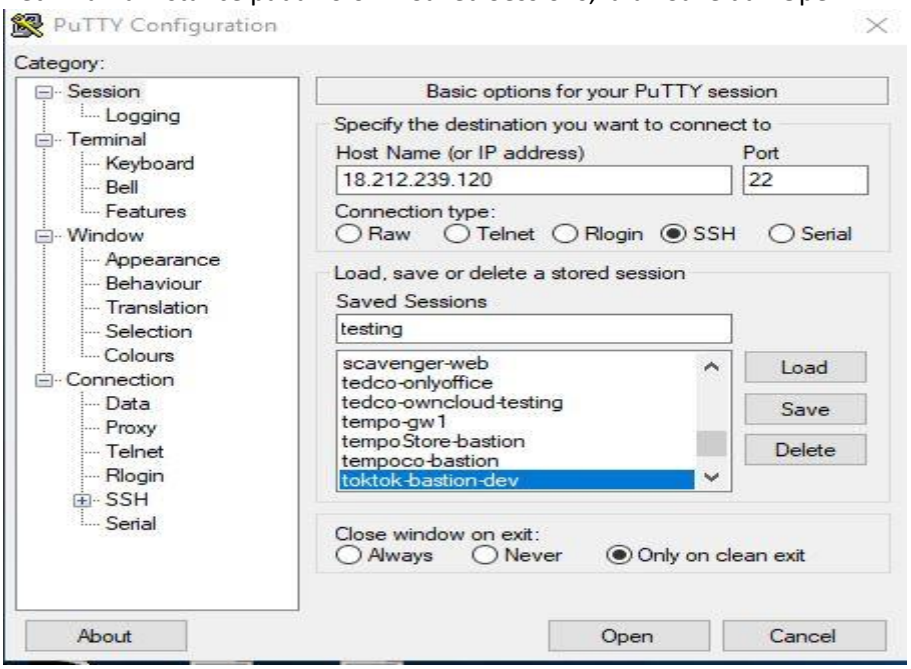
12. **Arahkan Public Key, dan**
    - Klik: I acknowledge that I have access to the selected private key file (user-public-key.pem), and that without this file, I won't be able to log into my instance.
    - Klik: Launch Instances

Install LAMP (Linux Apache MySQL PHP)

1. ssh ke instance menggunakan key yang telah dibuat (private key)
2. Gunakan pageant (double klik), lalu add key dan arahkan ke private key



3. Buka putty dan ketik ip dari instance pada kolom Host Name
4. Ketik nama instance pada kolom: Saved Sessions, lalu: Save dan Open



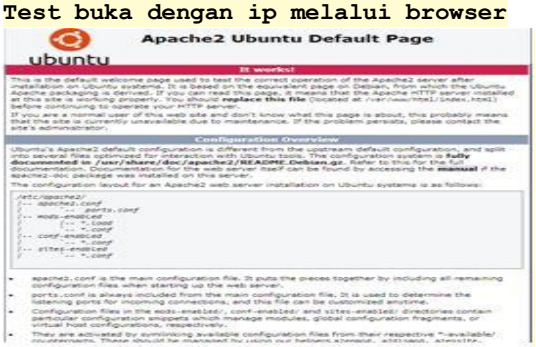
5. **Gunakan login as: Ubuntu**

```
ubuntu@ip-172-31-25-187: ~

  System load:  0.0                Processes:           92
  Usage of /:   16.7% of 7.69GB    Users logged in:     1
  Memory usage: 15%                IP address for eth0: 172.31.25.187
  Swap usage:   0%

 * MicroK8s 1.15 is out! It has already been installed on more
   than 14 different distros. Guess which ones?

     https://snapcraft.io/microk8s

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

14 packages can be updated.
3 updates are security updates.


Last login: Fri Jul  5 15:13:56 2019 from 140.213.8.18
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-25-187:~$
```

6. **Install Apache**

```
$ sudo apt-get install apache2 -y
```

7. **Test buka dengan ip melalui browser**



8. **Install MySQL**

```
$ sudo apt-get install mysql-server -y
```

9. **Secure for MySQL server**

```
$ sudo mysql_secure_installation
```

Ketik: Y

```
ubuntu@ip-172-31-25-187: ~

Setting up libhttp-message-perl (6.14-1) ...
Setting up mysql-client-5.7 (5.7.26-0ubuntu0.18.04.1) ...
Setting up mysql-server-5.7 (5.7.26-0ubuntu0.18.04.1) ...
update-alternatives: using /etc/mysql/mysql.cnf to provide /etc/mysql/my.cnf (my
.cnf) in auto mode
Renaming removed key_buffer and myisam-recover options (if present)
Created symlink /etc/systemd/system/multi-user.target.wants/mysql.service → /lib
/systemd/system/mysql.service.
Setting up mysql-server (5.7.26-0ubuntu0.18.04.1) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for systemd (237-3ubuntu10.23) ...
ubuntu@ip-172-31-25-187:~$  sudo mysql_secure_installation

Securing the MySQL server deployment.

Connecting to MySQL using a blank password.

VALIDATE PASSWORD PLUGIN can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD plugin?

Press y|Y for Yes, any other key for No: y
```

Ketik: 2

```
ubuntu@ip-172-31-25-187: ~
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for systemd (237-3ubuntu10.23) ...
ubuntu@ip-172-31-25-187:~$  sudo mysql_secure_installation

Securing the MySQL server deployment.

Connecting to MySQL using a blank password.

VALIDATE PASSWORD PLUGIN can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD plugin?

Press y|Y for Yes, any other key for No: y

There are three levels of password validation policy:

LOW    Length >= 8
MEDIUM Length >= 8, numeric, mixed case, and special characters
STRONG Length >= 8, numeric, mixed case, special characters and dictionary
            file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 2
```

Masukkan password dan jawab: Y (to continue with the password provided

Jawab: Y (Reload privilege table)

```
ubuntu@ip-172-31-25-187: ~
Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 2
Please set the password for root here.

New password:

Re-enter new password:

Estimated strength of the password: 50
Do you wish to continue with the password provided?(Press y|Y for Yes, any other
 key for No) : y
By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : y
Success.


Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : y
Success.

By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.


Remove test database and access to it? (Press y|Y for Yes, any other key for No)
 : y
```

10. **Testing MySQL server**

$ sudo mysql -u root -p

```
ubuntu@ip-172-31-25-187:~$ sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.26-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Mysql> show databases;

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
4 rows in set (0.00 sec)

mysql>
```

11. **Install PHP**

$ sudo apt-get install php libapache2-mod-php php-mysql php-gd php-xml

12. **Testing PHP**

$ cd /var/www/html
$ sudo nano info.php

Ketikkan ini:
<?php phpinfo(); ?>

Save dengan menggunakan: ctrl-x lalu: Y dan tekan tombol: Enter

13. **Test buka file info.php melalui browser**

Contoh: http://18.212.239.120/info.php

14. **Install phpMyAdmin**

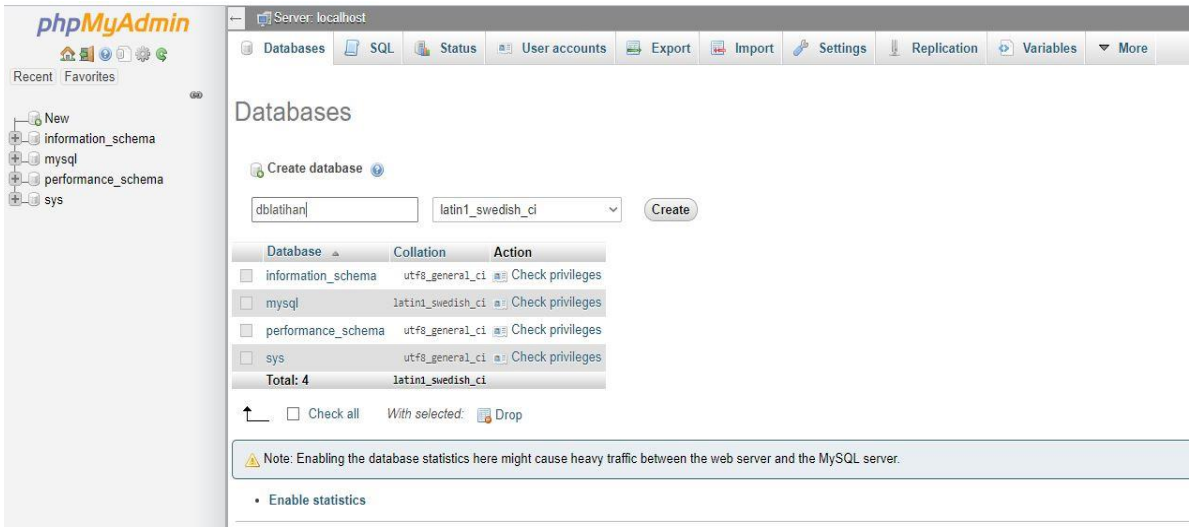
$ cd /var/www/html
$ sudo wget https://files.phpmyadmin.net/phpMyAdmin/4.9.0.1/phpMyAdmin-4.9.0.1-all-languages.zip
$ sudo apt-get install unzip
$ sudo unzip phpMyAdmin-4.9.0.1-all-languages.zip
$ sudo mv phpMyAdmin-4.9.0.1-all-languages phpmyadmin
$ cd phpmyadmin
$ sudo cp config.sample.inc.php config.inc.php
$ sudo mysql -u root -p

```
mysql> CREATE USER 'userlatihan'@'%' IDENTIFIED BY '@dm1nLatih01';
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON *.* TO 'userlatihan'@'%' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)

mysql> exit;
```

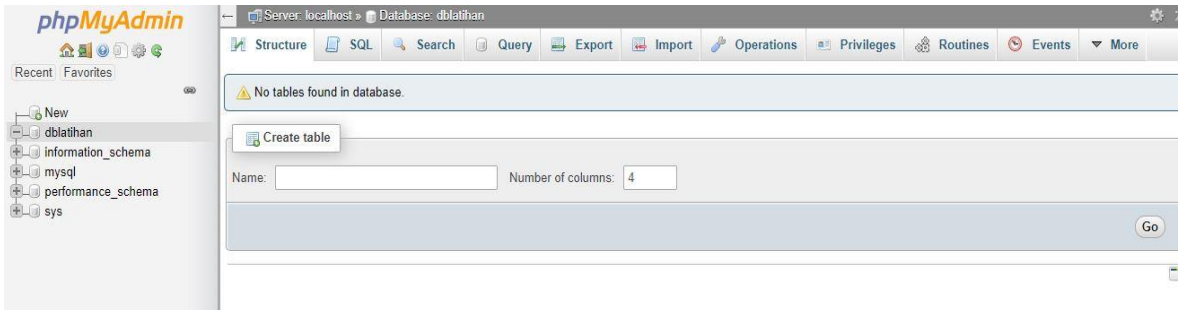
15. **Buka phpMyAdmin melalui browser**
    Misal: http://18.212.239.120/phpmyadmin/

Username: userlatihan
Password: @dm1nLatih01

16. **Test membuat database dari phpMyAdmin**
    Pada kolom: Create database, ketik nama database: dblatihan



Lalu klik tombol: Create



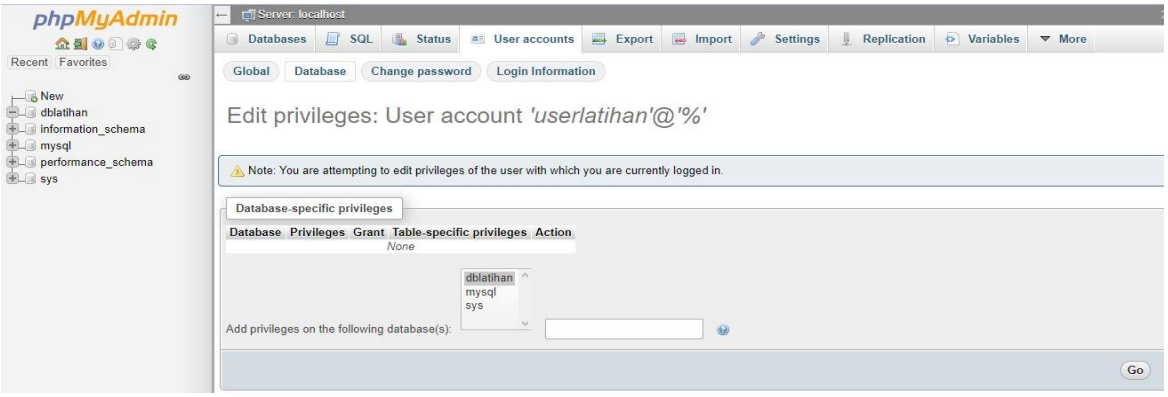
17. Mengarahkan dan memberikan permit user ke database

17.1. Kembali ke Home phpMyAdmin dan klik: User accounts

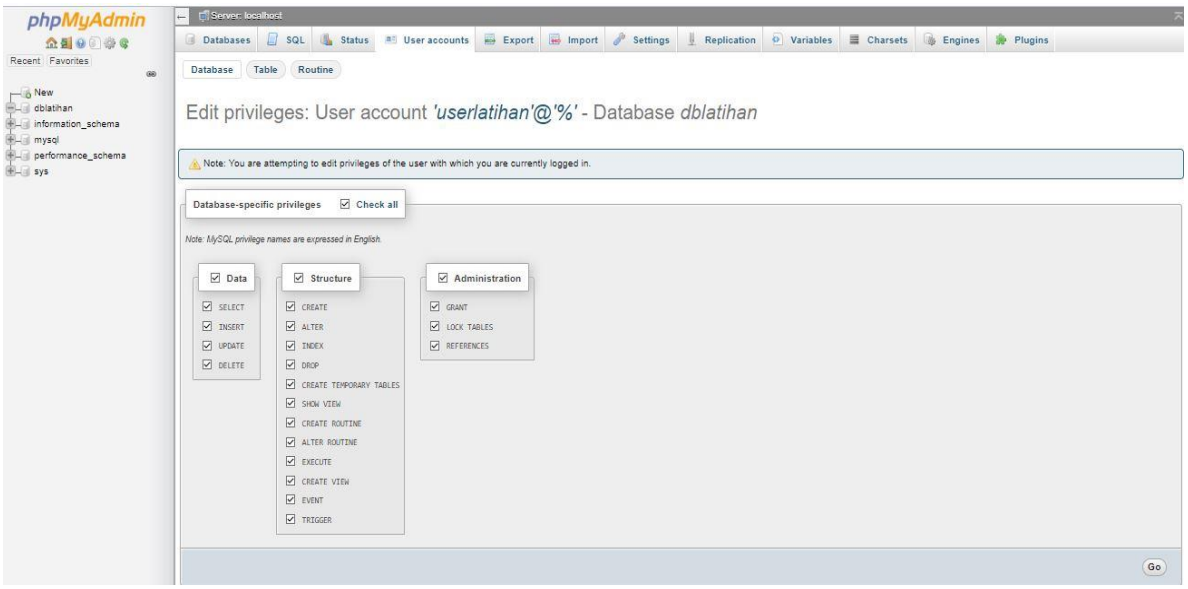
17.2. Klik: Edit privileges

17.3. Klik: Database, dan pilih nama database, yaitu: dblatihan

17.4. Klik: Go



17.5. Klik: Check all pada kolom: Database-specific privileges



Note: Disarankan jangan menggunakan account root pada saat menggunakan phpMyAdmin atau pada script web untuk alasan keamanan

SSL/HTTPS (Generat private key dan certificate .crt)

```
$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/ssl/private/pelatihan.com.key -out /etc/ssl/certs/pelatihan.com.crt

139956474339776:error:2406F079:random number generator:RAND_load_file:Cannot open
file:../crypto/rand/randfile.c
:88:Filename=/home/ubuntu/.rnd
Generating a RSA private key
.....................................................................+++++
..+++++
writing new private key to '/etc/ssl/private/pelatihan.com.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:Jawa Tengah
Locality Name (eg, city) []:Batang
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Kominfo
Organizational Unit Name (eg, section) []:IT Divisi
Common Name (e.g. server FQDN or YOUR name) []:pelatihan.com
Email Address []:training@pelatihan.com

$ cd /etc/apache2/sites-available
$ cp default-ssl.conf default-ssl.conf-backup
$ sudo default-ssl.conf
```

```
<IfModule mod_ssl.c>
 <VirtualHost _default_:443>
                ServerAdmin webmaster@localhost
                ServerName pelatihan.com
                ServerAlias www.pelatihan.com
                DocumentRoot /var/www/html
                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined
                #Include conf-available/serve-cgi-bin.conf
                #   SSL Engine Switch:
                #   Enable/Disable SSL for this virtual host.
                SSLEngine on
                SSLCertificateFile      /etc/ssl/certs/pelatihan.com.crt
                SSLCertificateKeyFile   /etcd c/ssl/private/pelatihan.com.key
                #
                #SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
                #SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
 </VirtualHost>
</IfModule>
```

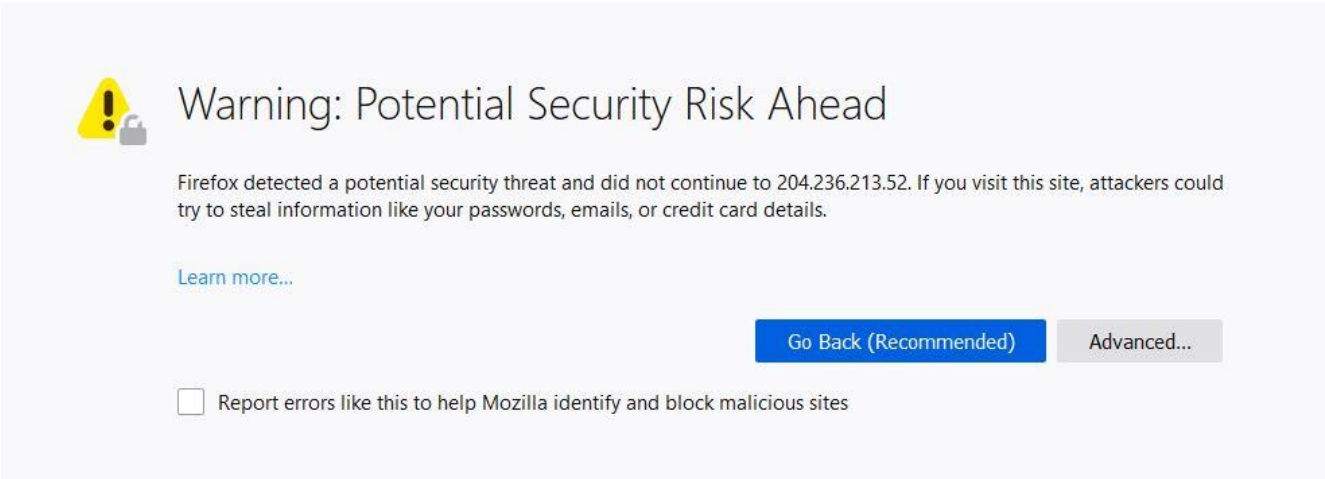
```
$ cd /etc/apache2/sites-available/
$ sudo cp 000-default.conf 000-default.conf-backup
$ sudo nano 000-default.conf
```

```
<VirtualHost *:80>
 # The ServerName directive sets the request scheme, hostname and port that
 # value is not decisive as it is used as a last resort host regardless.
 # However, you must set it for any further virtual host explicitly.

 ServerName pelatihan.com
 ServerAlias www.pelatihan.com
 DocumentRoot /var/www/html
</VirtualHost>
```

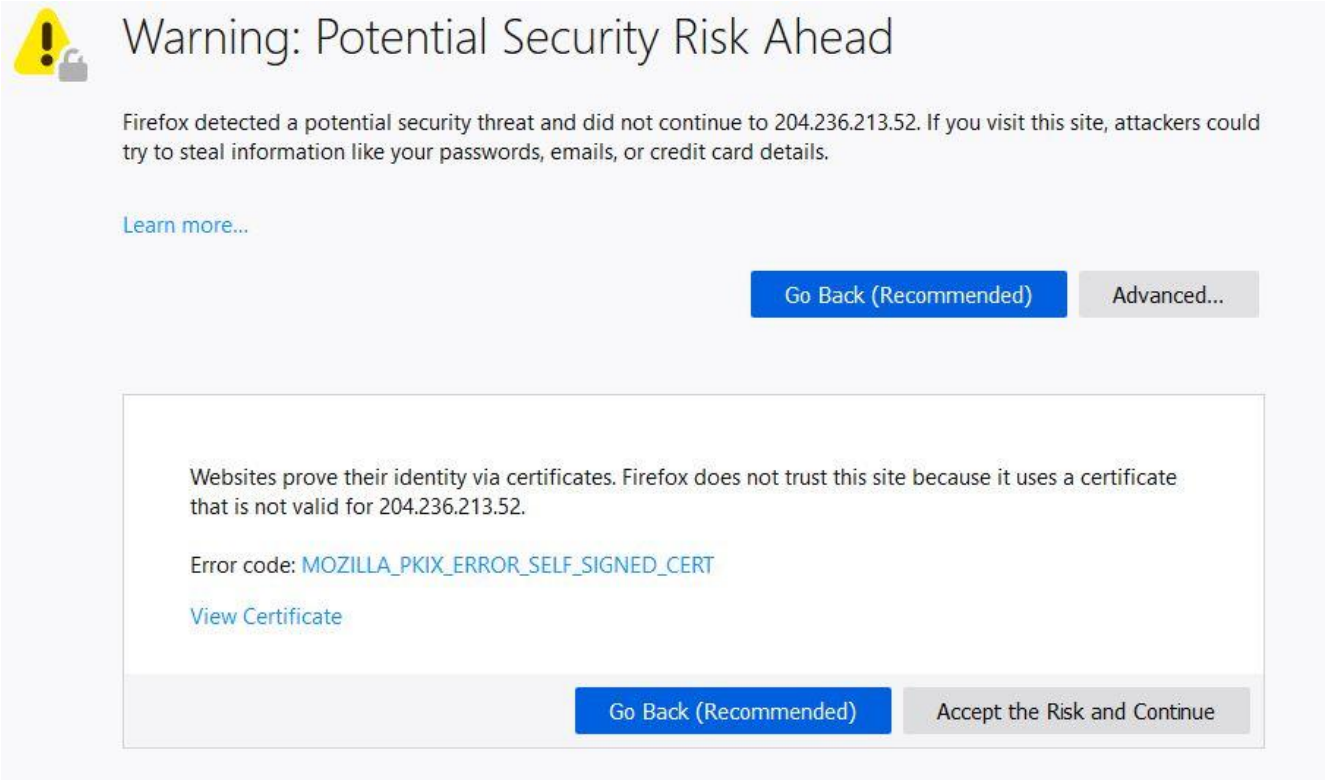
```
$ sudo apachectl configtest
$ sudo a2enmod ssl
$ sudo a2ensite default-ssl
$ sudo systemctl restart apache2.service

or
$ sudo service apache2 restart
```

Test Buka halaman web
Contoh: https://204.236.213.52/

Akan muncul sbb:



Lalu klik: Advanced dan Accept the Risk and Continue



Redirect web ke https

```
$ sudo vim /etc/apache2/sites-available/000-default.conf

    <VirtualHost *:80>
            . . .
            Redirect permanent "/" "https://pelatihan.com/"
            . . .
    </VirtualHost>

Save dengan command: ctrl-x (lalu jawab: Y)

$ sudo systemctl restart apache2
```

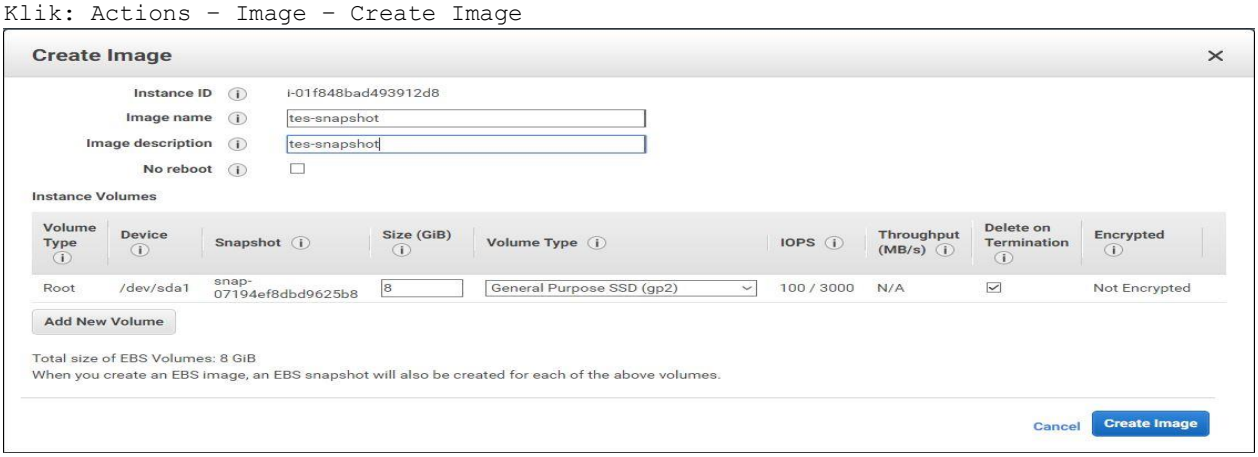
LOAD BALANCING

1. Membuat key di instance-1 agar dapat ssh ke instance-2 dan instance-3

```
$ ssh-keygen -b 2048
$ cd /home/ubuntu/.ssh
$ cat id_rsa.pub >> authorized_keys
```

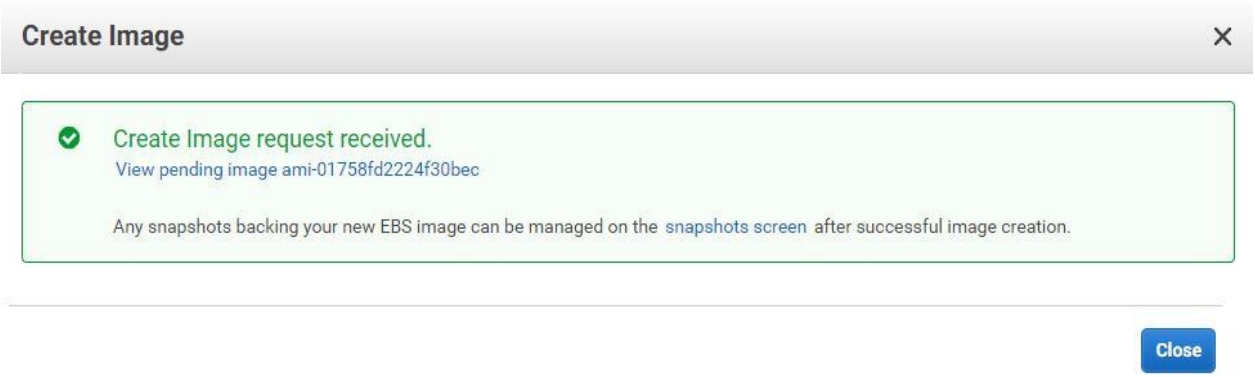
2. Membuat Snapshot instance/vm

Klik: Actions – Image – Create Image



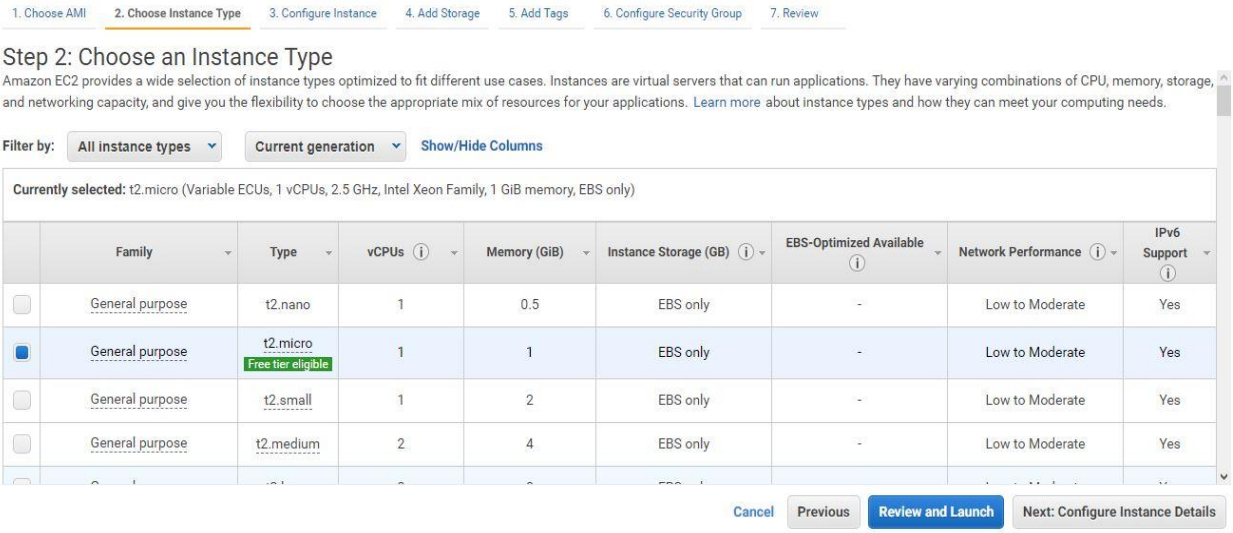
Imange name : (misal: test-snapshot)
Image description : (misal:test-snapshot)

Klik: Create Image – Close

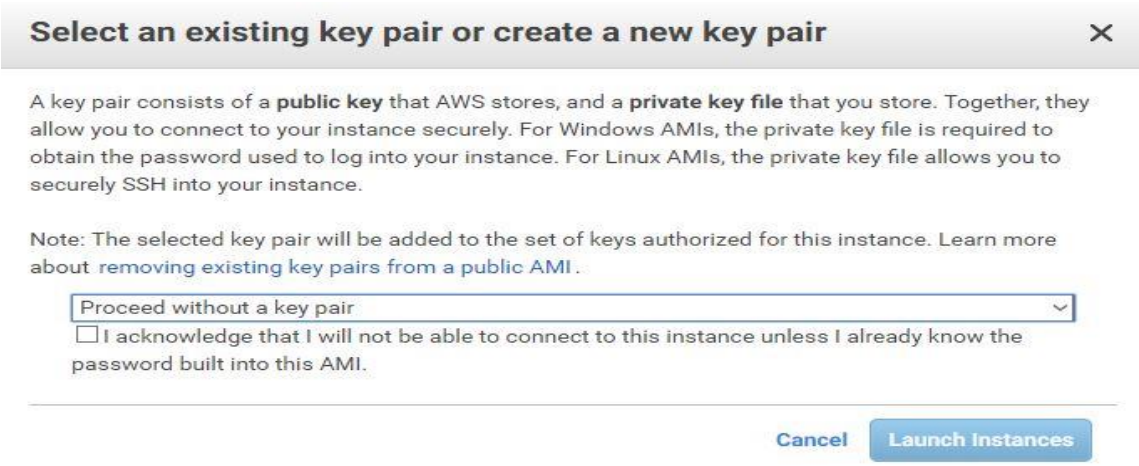


Membuar Instance dari Image Snapshot

1. Ke dashboard: Instance
   Klik: Launch Instance
   Klik: My AMIs (Pilih Image Snapshot yang telah dibuat)
   Klik: Select => Next: Configure Instance Details



2. Configure Instance Detail
   2.1. Subnet: subnet3-default | Default in us-east-1a
   2.2. Auto-assign Public IP : Disable
   2.3. Klik => Next: Add Storage
   2.4. Klik => Next: Add Tags
   2.5. Klik => Add tag
   2.6. Pada kolom: Key, ketik: Name
   2.7. Pada kolom: Value, ketik: (misal: test2)
   2.8. Klik: Next: Configure Security Group
   2.9. Assign a security group, pilih: Select an existing security group
   2.10. Pilih: sgPelatihan
   2.11. Klik: Review and Lauch
   2.12. Klik: Launch
   2.13. PIlih: Proceed without a key pair
   Dan klik: I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.



   2.14. KLik: View Instances

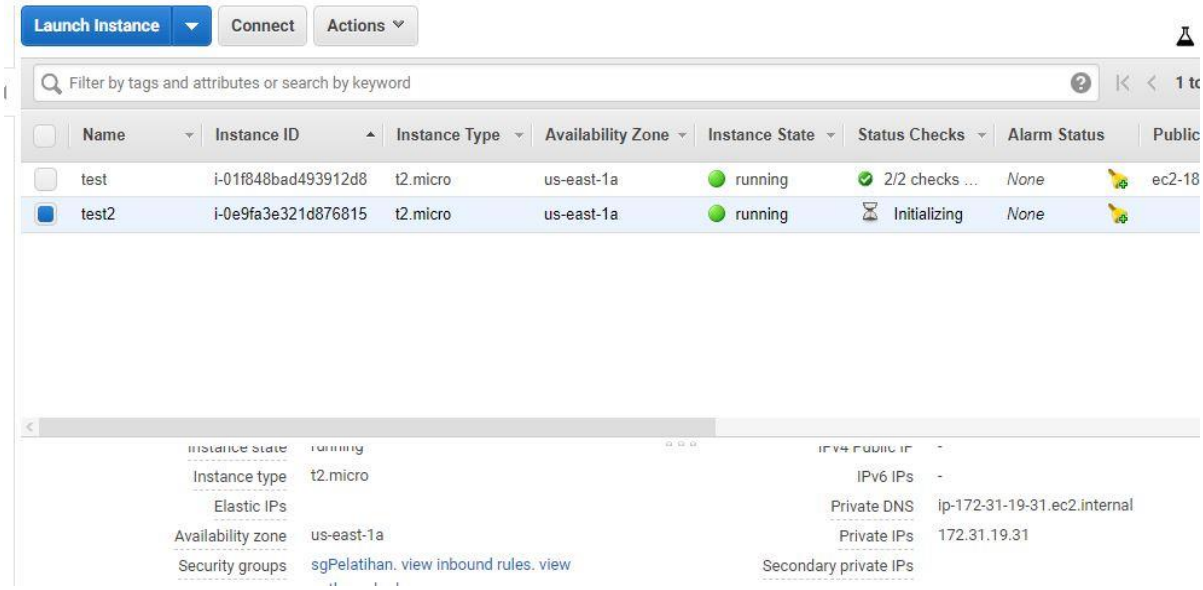
3. Membuat insntance-3 dimana proses sama seperti pada point 1 hingga 2 diatas

4. SSH ke instance pertama

5. Buka file hosts di instance ke-1, dan tambahkan ip instance ke-2 dan instance k3-3 dengan ip private-nya
   $ sudo nano /etc/hosts

   Misal:
   172.31.19.31 web1
   172.31.22.231 web2

   Lalu save dengan tombol: ctrl-X lalu jawab: y dan Enter



6. Test ssh dari instance-1 ke instance-2 dan instance-3
   $ ssh ubuntu@test2

   Muncul pertanyaan: Are you sure you want to continue connecting (yes/no)?
   Jawab: yes, Lalu: Enter

   Jika telah berhasil ssh ke instance-2 dan instance-3, lalu keluar kembali dengan mengetik: **Exit**

INSTALL LOAD BALANCING

```
$ sudo apt-get install software-properties-common
$ sudo add-apt-repository ppa:vbernat/haproxy-2.0
```

```
 HAProxy is a free, very fast and reliable solution offering high availability, load balancing, and proxying for TC
 and HTTP-based applications. It is particularly suited for web sites crawling under very high loads while needing
ersistence or Layer7 processing. Supporting tens of thousands of connections is clearly realistic with todays hardw
re. Its mode of operation makes its integration into existing architectures very easy and riskless, while still off
ring the possibility not to expose fragile web servers to the Net.

This PPA contains packages for HAProxy 2.0.
 More info: https://launchpad.net/~vbernat/+archive/ubuntu/haproxy-2.0
Press [ENTER] to continue or Ctrl-c to cancel adding it.
```

Tekan: Enter

```
$ sudo apt-get update
$ sudo apt-get install haproxy
```

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  liblua5.3-0 libpcre2-8-0
Suggested packages:
  vim-haproxy haproxy-doc
The following NEW packages will be installed:
  haproxy liblua5.3-0 libpcre2-8-0
0 upgraded, 3 newly installed, 0 to remove and 20 not upgraded.
Need to get 1786 kB of archives.
After this operation, 4177 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Tekan: y lalu: Enter

```
$ cd /etc/haproxy.cfg
$ sudo cp haproxy.cfg haproxy.cfg-backup
$ sudo nano haproxy.cfg
```

Tambahkan di baris paling akhir sbb:

```
       listen stats
           bind 172.31.19.31:80
           mode http
           default_backend My_Web_Servers
           stats enable
           stats hide-version
           stats refresh 30s
           stats show-node
           stats auth admin:@dm1nLatih01
           stats uri  /stats

       backend My_Web_Servers
           mode http
           balance roundrobin
           option forwardfor
           option httpchk OPTIONS /
           server web1 172.31.25.23:80 check
           server web2 172.31.16.194:80 check
```

Lalu: **Save**

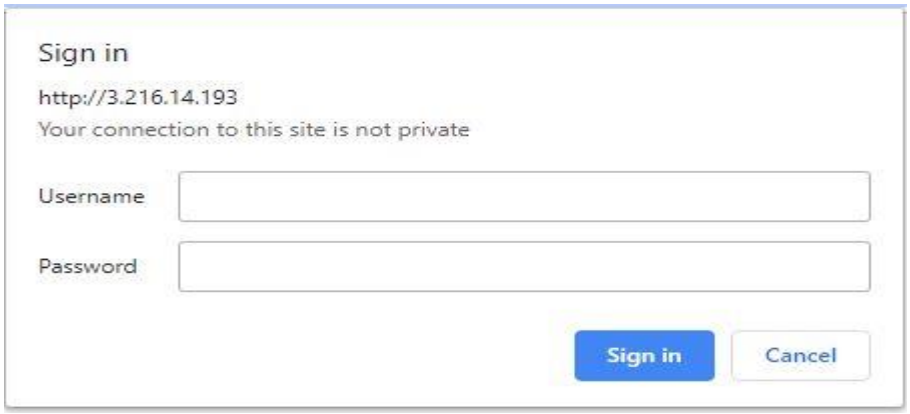
NOTE:
Pada bagian: stats auth ➔ ketik password admin sesuai yang diinginkan

```
$ sudo /etc/init.d/haproxy restart
```

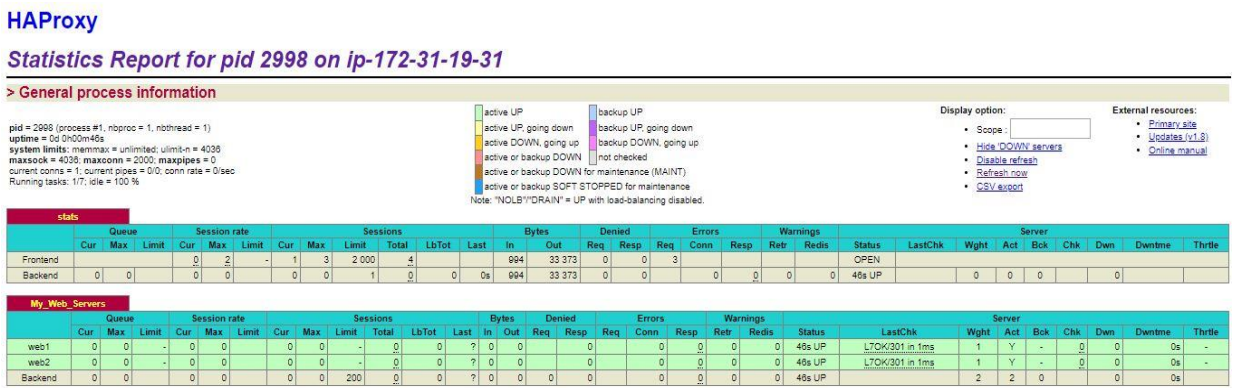
Buka browser dan ketikkan ip dari Instance/VM Load Balancing

Contoh: http://3.216.14.193/stats

Masukkan Login dan Password Load Balancing



Tampilan Load Balancing HAProxy sbb:



HAProxy

Statistics Report for pid 2998 on ip-172-31-19-31

> General process information

pid = 2998 (process #1, nbproc = 1, nbthread = 1)
uptime = 0d 0h00m46s
system limits: memmax = unlimited; ulimit-n = 4036
maxsock = 4036; **maxconn** = 2000; **maxpipes** = 0
current conns = 1; current pipes = 0/0; conn rate = 0/sec
Running tasks: 1/7; idle = 100 %

active UP
active UP, going down
active DOWN, going up
active or backup DOWN
active or backup DOWN for maintenance (MAINT)
active or backup SOFT STOPPED for maintenance
backup UP
backup UP, going down
backup DOWN, going up
not checked
Note: "NOLB"/"DRAIN" = UP with load-balancing disabled.

Display option:
- Scope :
- Hide 'DOWN' servers
- Disable refresh
- Refresh now
- CSV export

External resources:
- Primary site
- Updates (v1.8)
- Online manual

stats

	Queue			Session rate			Sessions						Bytes		Denied		Errors			Warnings		Server								
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
Frontend				0	2	-	1	3	2 000	4			994	33 373	0	0	3					OPEN								
Backend	0	0		0	0		0	0	1	0	0	0s	994	33 373	0	0		0	0	0	0	46s UP		0	0	0		0		

My_Web_Servers

	Queue			Session rate			Sessions						Bytes		Denied		Errors			Warnings		Server								
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
web1	0	0	-	0	0		0	0	-	0	0	?	0	0		0		0	0	0	0	46s UP	L7OK/301 in 1ms	1	Y	-	0	0	0s	-
web2	0	0	-	0	0		0	0	-	0	0	?	0	0		0		0	0	0	0	46s UP	L7OK/301 in 1ms	1	Y	-	0	0	0s	-
Backend	0	0		0	0		0	0	200	0	0	?	0	0	0	0		0	0	0	0	46s UP		2	2	0		0	0s	

SSH ke Web1

```
$ ssh ubuntu@web1
$ cd /var/www/html
$ sudo cp index.html index.html-backup
$ sudo su
# cat /dev/null > index.html
# exit
$ sudo nano /var/www/html/index.html

  Ketik:  Ini adalah Web Server 1

  Lalu: Save
```

$ sudo nano /etc/apache2/sites-available/000-default.conf

Ketik tanda pagar (*) di depan tulisan: Redirect permanent "/" https://pelatihan.com/

```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerName pelatihan.com
        ServerAlias www.pelatihan.com
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        #Redirect permanent "/" "https://pelatihan.com/"
```

Lalu: Save

$ sudo /etc/init.d/apache2 restart
$ exit

SSH ke Web2

$ ssh ubuntu@web2
$ cd /var/www/html
$ sudo cp index.html index.html-backup
$ sudo su
# cat /dev/null > index.html
# exit
$ sudo nano /var/www/html/index.html

Ketik: Ini adalah Web Server 2

Lalu: Save

$ sudo nano /etc/apache2/sites-available/000-default.conf

Ketik tanda pagar (*) di depan tulisan: Redirect permanent "/" https://pelatihan.com/

```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerName pelatihan.com
        ServerAlias www.pelatihan.com
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        #Redirect permanent "/" "https://pelatihan.com/"
```

Lalu: Save

$ sudo /etc/init.d/apache2 restart
$ exit

INSTALL BASTION SERVER MENGGUNAKAN IPTABLES

SSH ke instance LB

```
$ sudo /etc/init.d/ufw stop
$ sudo /etc/init.d/ufw status
```

Check status ufw dan pastikan sudah disable

```
● ufw.service - Uncomplicated Firewall
   Loaded: loaded (/lib/systemd/system/ufw.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Wed 2019-07-10 11:36:03 UTC; 2min 42s ago
     Docs: man:ufw(8)
  Process: 4006 ExecStop=/lib/ufw/ufw-init stop (code=exited, status=0/SUCCESS)
 Main PID: 387 (code=exited, status=0/SUCCESS)

Jul 10 11:36:03 ip-172-31-19-31 systemd[1]: Stopping Uncomplicated firewall...
Jul 10 11:36:03 ip-172-31-19-31 ufw-init[4006]: Skip stopping firewall: ufw (not enabled)
Jul 10 11:36:03 ip-172-31-19-31 systemd[1]: Stopped Uncomplicated firewall.
Warning: Journal has been rotated since unit was started. Log output is incomplete or unavailable.
ubuntu@ip-172-31-19-31:~$
```

Copy iptables default

```
$ sudo iptables-save > iptables-baru
$ sudo iptables -L
```

```
ubuntu@ip-172-31-19-31:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ubuntu@ip-172-31-19-31:~$
```

Skenarionya kita akan coba ssh ke instance web1 dan web2 dari luar melalui server bastion dengan cara Forwarding Port

Buat file untuk menandakan posisi ssh ada di server mana

```
$ ssh ubuntu@web1
$ sudo nano ssh-ke-web1

  Isi dengan:
    ssh key web1
```

Lalu: **Save**

```
$ ll
$ exit
$ ssh ubuntu@web2
$ sudo nano ssh-ke-web2

  Isi dengan:
    ssh ke web2
```

Lalu: **Save**

```
$ ll
$ exit
```

Check ip forward apakah dalam kondisi Enable atau Disable

Note:

$ cat /proc/sys/net/ipv4/ip_forward

0 = Disable

1 = Enable

Enable ip forward:

$ sudo sysctl net.ipv4.ip_forward=1

$ cat /proc/sys/net/ipv4/ip_forward

$ cat /etc/hosts

Catat ip web1 dan web2 untuk dimasukkan ke iptables

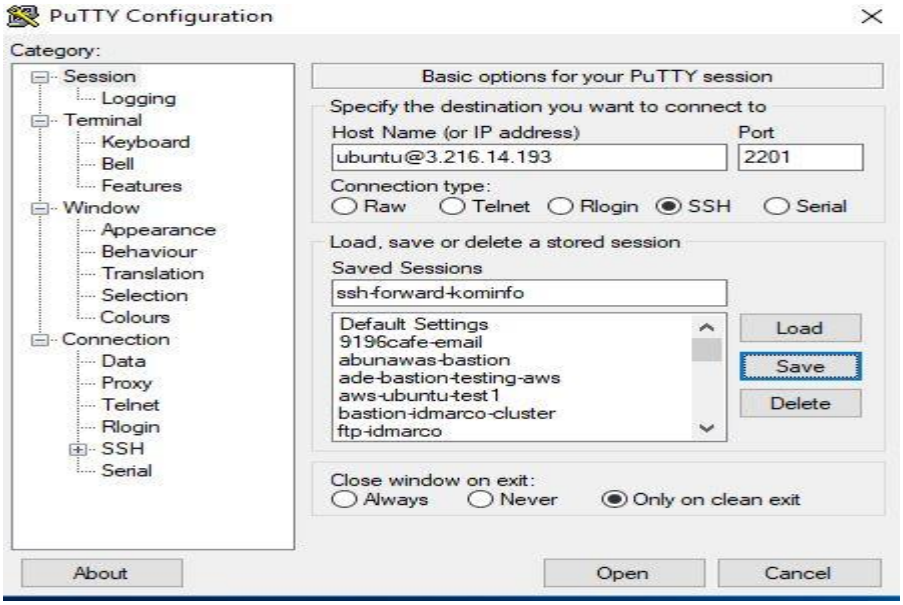
$ sudo nano iptables-baru

$ sudo iptables-restore < iptables-baru

$ sudo iptables -L

TEST SSH KE WEB1 DAN WEB2 MELALUI BASTION SERVER

1. Buka putty



SSH ke Web1
Host Name : ubuntu@3.216.14.193
Port : 2201
Saved Sessions : ssh-forward-kominfo

$ ll

Note:
- Cek apakah ada file ssh-ke-web1 (jika ada berarti benar ssh ke web1)
- Lalu coba ssh ke web2, dengan mengganti portnya ke port 2202