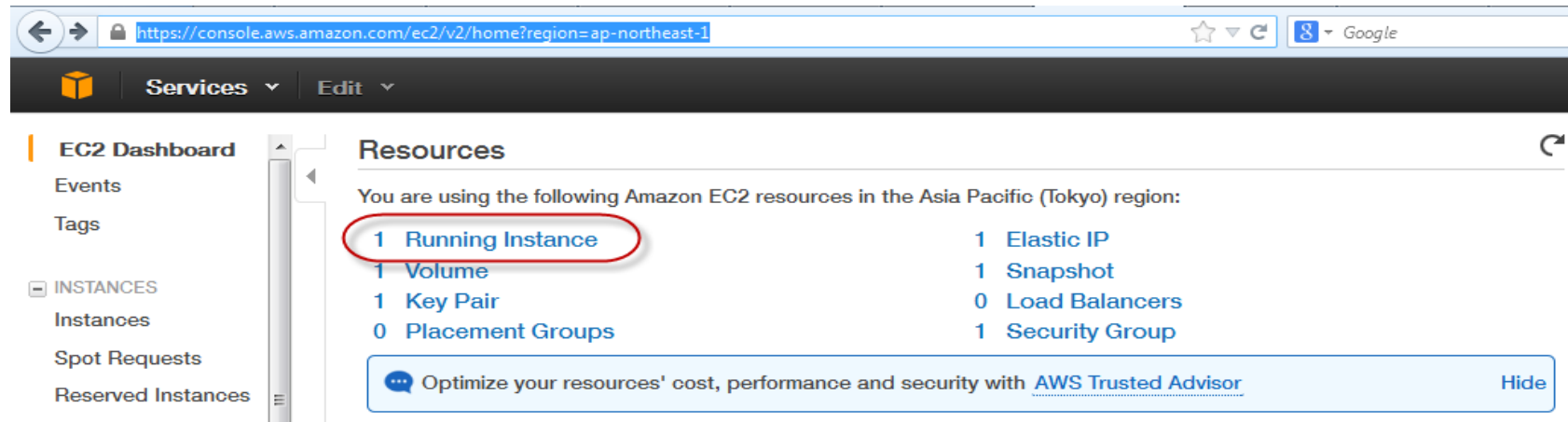


## 1. Create a instance server on console of AWS

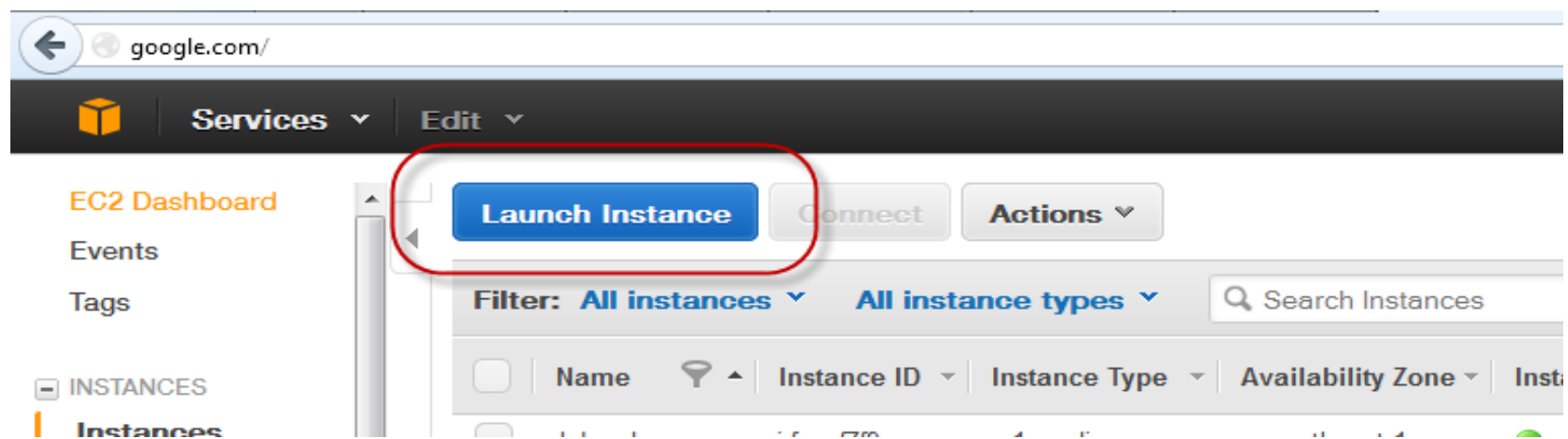
### 1.1 Go to console link of AWS

<https://console.aws.amazon.com/ec2/v2/home?region=ap-northeast-1>

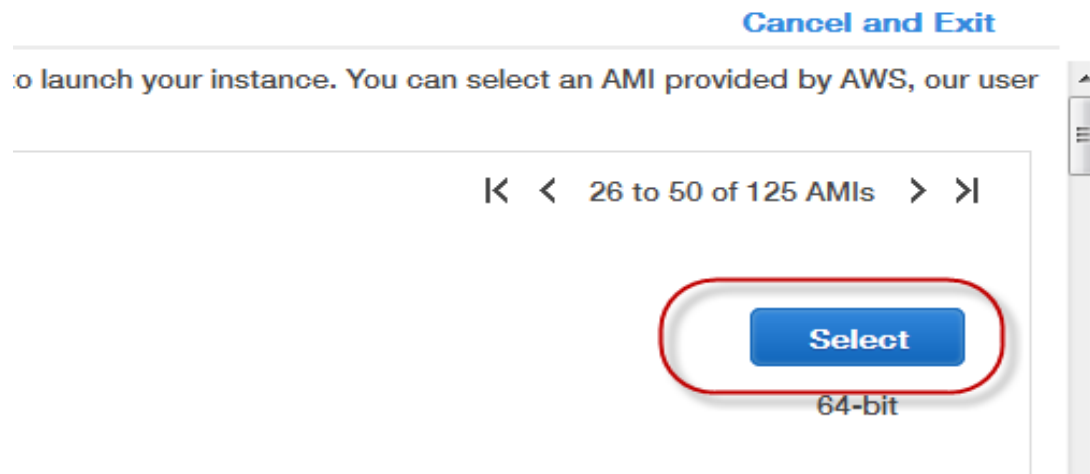
### 1.2 Click Running Instance



### 1.3 Click Launch Instance



1.4 Choose AMI: Select Community AMIs tab, Cent OS checkbox, 64-bit checkbox, EBS checkbox, CentOS6.3\_01-02-13 - ami-....



1.5 Choose Instance Type, Chọn General purpose, m1.medium, Next: Config Instance Detail

x 160	-	Low
x 410	-	Moderate
x 420	Yes	Moderate
x 420	Yes	High
BS only	Yes	Moderate
BS only	Yes	High

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

1.6 Configure Instance Details. Next: Add Storage

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

1.7 Add Storage. Next: Tag Instance

ty and usage restrictions.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Tag Instance](#)

### 1.8 Tag Instance.

Select Key: Jobpad, Value: Jobpad. Next: Configure Security Group

Kinoshita Yoshihiko ▾Tokyo ▾Help ▾

Instance

6. Configure Security Group

7. Review

key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Value (255 characters maximum)

Jobpad

Jobpad

✕

Cancel


Previous

Review and Launch

Next: Configure Security Group

### 1.9 Security Group

Select an existing security Group, sg-bde9e0df. Review and Launch

 **Services** ▾ **Edit** ▾

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. **Configure**

## Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to the security group, add rules that allow unrestricted access to the HTTP and HTTPS ports, or add rules that allow Internet traffic to reach your instance. [Learn more](#) about Amazon EC2 security groups.

**Assign a security group:** ☐ Create a **new** security group  
☒ Select an **existing** security group

Security Group ID	Name
<input checked="" type="checkbox"/> sg-bde9e0df	default

Inbound rules for sg-bde9e0df

Protocol ⓘ	Type ⓘ	Port Range
SSH	TCP	22
HTTP	TCP	80

1.10 Launch

Kinoshita YoshihikoTokyoHelp

[Configure Security Group](#)

7. Review

Click to assign a key pair to your instance and complete the launch process.

×

pe, configuration options, or storage devices. Learn more about [free usage tier](#) eligibility and

[Don't show me this again](#)

[Edit AMI](#)

[Edit instance type](#)

(GiB)	EBS-Optimized Available	Network Performance
		...

Cancel

Previous

Launch

### 1.11 Select Keypair

Select Create new Keypair.

Input Keypair name

Download Keypair for remote login (Example Jobpad1.pem)

**Select an existing key pair or create a new key pair** X

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Create a new key pair ▼

**Key pair name**  
Jobpad1

Download Key Pair

You have to download the **private key file** (\*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

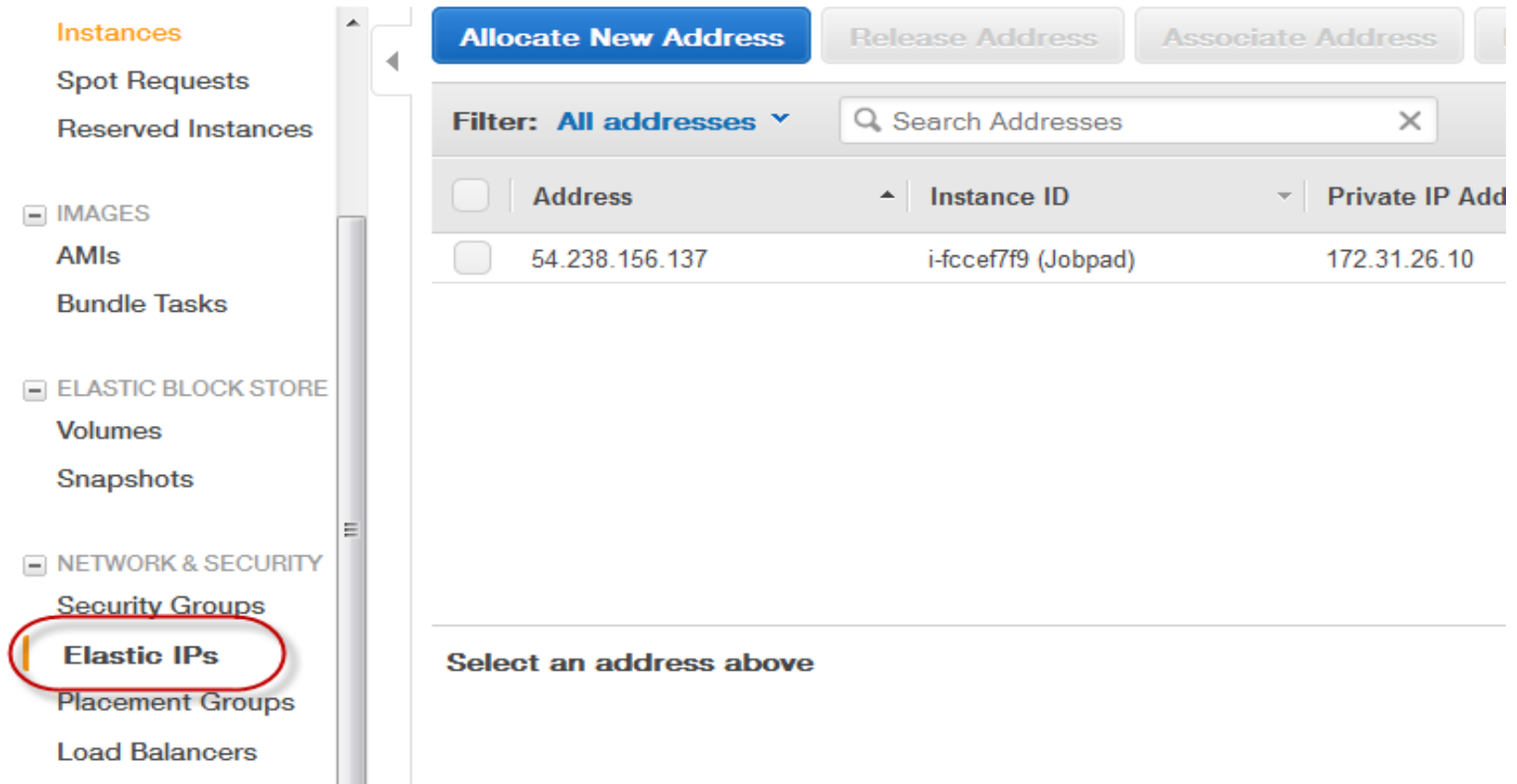
Cancel Launch Instances

Click Launch Instance

## 2. Create static IP for registered Instance

### 2.1 Access Elastic Ips

<https://console.aws.amazon.com/ec2/v2/home?region=ap-northeast-1#Addresses:>



The screenshot displays the AWS Management Console interface for Elastic IP addresses. The left-hand navigation pane is visible, with the 'Elastic IPs' option selected and highlighted by a red circle. The main content area features a header with three buttons: 'Allocate New Address' (in blue), 'Release Address', and 'Associate Address'. Below the buttons is a filter section showing 'Filter: All addresses' and a search bar labeled 'Search Addresses'. A table lists the allocated addresses with columns for a selection checkbox, the public 'Address', the associated 'Instance ID', and the 'Private IP Address'. One address is listed: 54.238.156.137, associated with instance i-fccef7f9 (Jobpad), with a private IP of 172.31.26.10. At the bottom of the table area, the text 'Select an address above' is displayed.

<input type="checkbox"/>	Address	Instance ID	Private IP Address
<input type="checkbox"/>	54.238.156.137	i-fccef7f9 (Jobpad)	172.31.26.10



Key Pairs

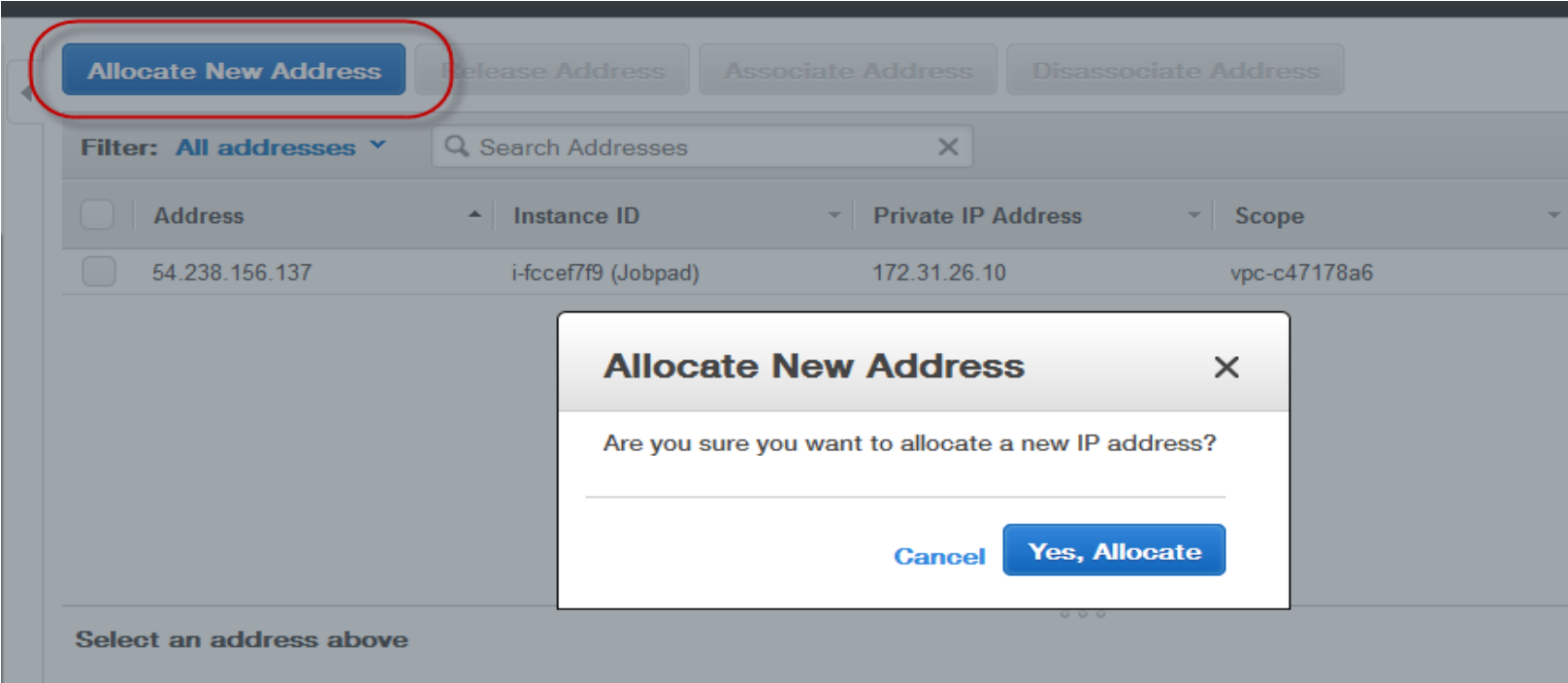
Network Interfaces

© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved.

[Privacy Policy](#)

[Terms of Use](#)

## 2.2 Allocate new Address



The screenshot shows the AWS Management Console interface for managing IP addresses. At the top, there are buttons for 'Allocate New Address', 'Release Address', 'Associate Address', and 'Disassociate Address'. The 'Allocate New Address' button is highlighted with a red circle. Below these buttons is a filter dropdown set to 'All addresses' and a search bar labeled 'Search Addresses'. A table lists available addresses with columns for 'Address', 'Instance ID', 'Private IP Address', and 'Scope'. One address is listed: 54.238.156.137, associated with instance i-fccef7f9 (Jobpad), with private IP 172.31.26.10, and scope vpc-c47178a6. A modal dialog titled 'Allocate New Address' is open, asking 'Are you sure you want to allocate a new IP address?' with 'Cancel' and 'Yes, Allocate' buttons. At the bottom left, there is a text prompt 'Select an address above'.

Address	Instance ID	Private IP Address	Scope
54.238.156.137	i-fccef7f9 (Jobpad)	172.31.26.10	vpc-c47178a6

## 2.3 Connect IP with instance

Allocate New Address

Release Address

Associate Address

Disassociate Address

Filter: All addresses

Search Addresses

<input type="checkbox"/>	Address	Instance ID	Private IP Address	Scope
<input type="checkbox"/>	54.238.156.137	i-fccef7f9 (Jobpad)	172.31.26.10	vpc-c47178a6

Associate Address

Select the instance OR network interface to which you wish to associate this IP address (54.238.156.137)

Instance

i-fccef7f9 - Jobpad

Or

Network Interface

Select Network Interface

Private IP Address

172.31.26.10

Allow Reassociation

☐

Cancel

Associate

Instance ID

i-fccef7f9

Private IP address

172.31.26.10

### 3. Update Security Group for external access

#### 3.1 Access into Security Group

<https://console.aws.amazon.com/ec2/home?region=ap-northeast-1#s=SecurityGroups>

Services Edit

Instances  
Spot Requests  
Reserved Instance

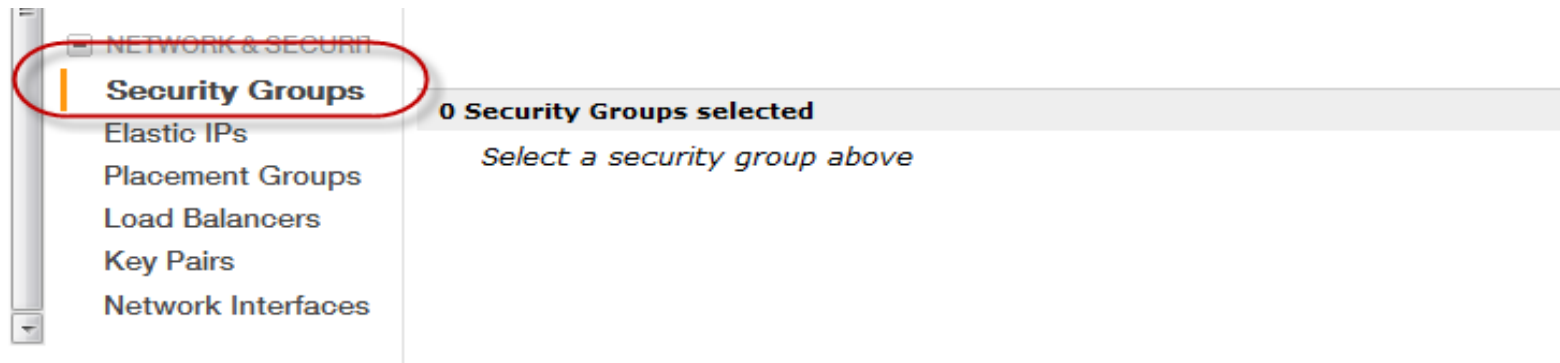
IMAGES  
AMIs  
Bundle Tasks

ELASTIC BLOCK STO  
Volumes  
Snapshots

Create Security Group Delete

Viewing: All Security Groups Search

	Group ID	Name	VPC ID	Description
<input type="checkbox"/>	sg-bde9e0df	default	vpc-c47178a6	default VPC secu



### 3.2 Select Group ID, add Inbound Rule

Kinoshita YoshihikoTokyoHelp

Create Security GroupDelete

All Security GroupsSearch

1 to 1 of 1 Items

Group ID	Name	VPC ID	Description
sg-bde9e0df	default	vpc-c47178a6	default VPC security group

InboundOutbound

Create a rule: Custom TCP rule

Port range: (e.g., 80 or 49152-65535)

Source: 0.0.0.0/0 (e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

Add Rule

Apply Rule Changes

Port (Service)	Source	Action
ALL	sg-bde9e0df	Delete
TCP		
Port (Service)	Source	Action
22 (SSH)	118.70.67.54/32	Delete
22 (SSH)	14.160.64.122/32	Delete
80 (HTTP)	0.0.0.0/0	Delete
3306 (MYSQL)	118.70.67.54/32	Delete
3389 (RDP)	118.70.67.54/32	Delete

Inc. or its affiliates. All rights reserved. Privacy PolicyTerms of UseFeedback

22 (SSH) **118.70.67.54**/32  
80 (HTTP) 0.0.0.0/0  
3306 (MYSQL) **118.70.67.54**/32  
3389 (RDP) **118.70.67.54**/32

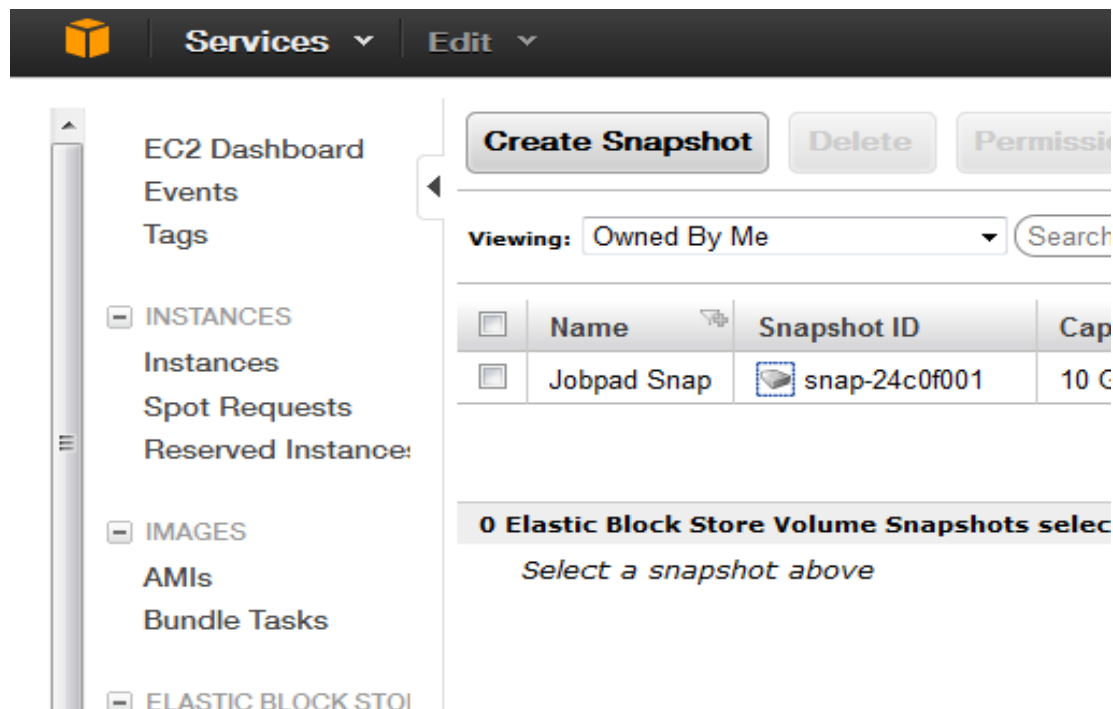
**RED IP** is local IP can remote access to server

Select new rule (ex. SSH), Source (ex. 118.70.67.54/32), Add Rule, Apply Rule Change


80 (HTTP) 0.0.0.0/0 : Allow all user public access on port 80

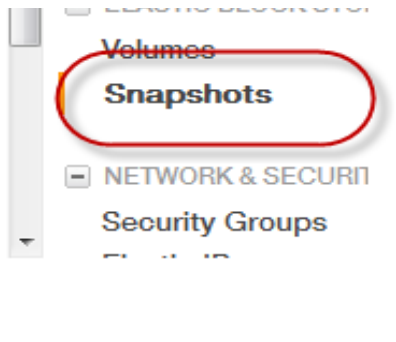
#### 4. Create Snapshot back-up

##### 4.1 Access into Snapshop

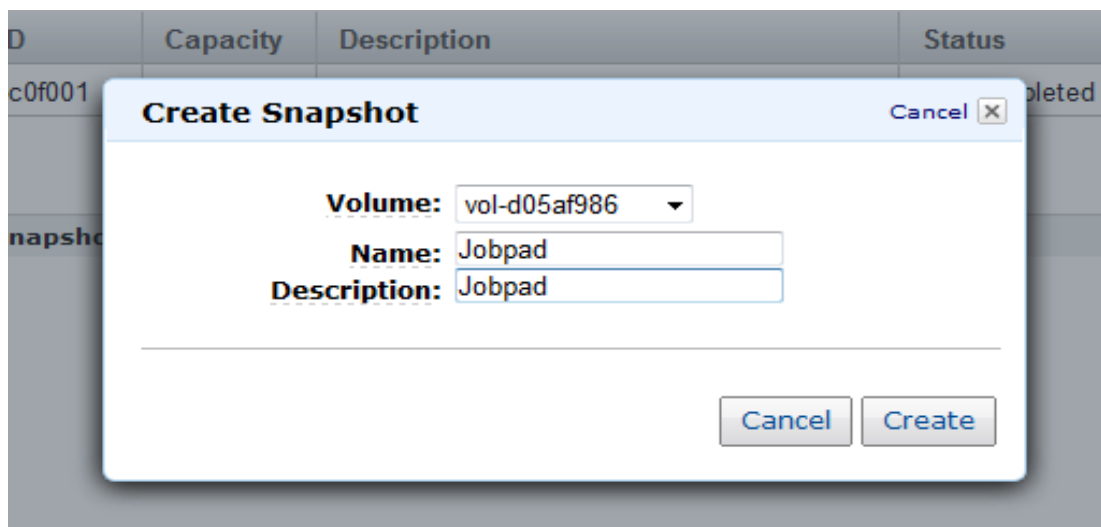


The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with 'Services' and 'Edit' dropdowns. The left sidebar contains a navigation menu with 'EC2 Dashboard', 'Events', 'Tags', 'INSTANCES' (with sub-items: Instances, Spot Requests, Reserved Instance:), 'IMAGES' (with sub-items: AMIs, Bundle Tasks), and 'ELASTIC BLOCK STO'. The main content area is titled 'Snapshots' and features buttons for 'Create Snapshot', 'Delete', and 'Permissions'. Below these buttons is a 'Viewing:' dropdown set to 'Owned By Me' and a 'Search' button. A table lists snapshots with columns for 'Name', 'Snapshot ID', and 'Cap'. One snapshot is listed: 'Jobpad Snap' with ID 'snap-24c0f001' and capacity '10 C'. At the bottom, a message states '0 Elastic Block Store Volume Snapshots selected' and 'Select a snapshot above'.

	Name	Snapshot ID	Cap
<input type="checkbox"/>	Jobpad Snap	 snap-24c0f001	10 C



#### 4.2 Create Snapshot

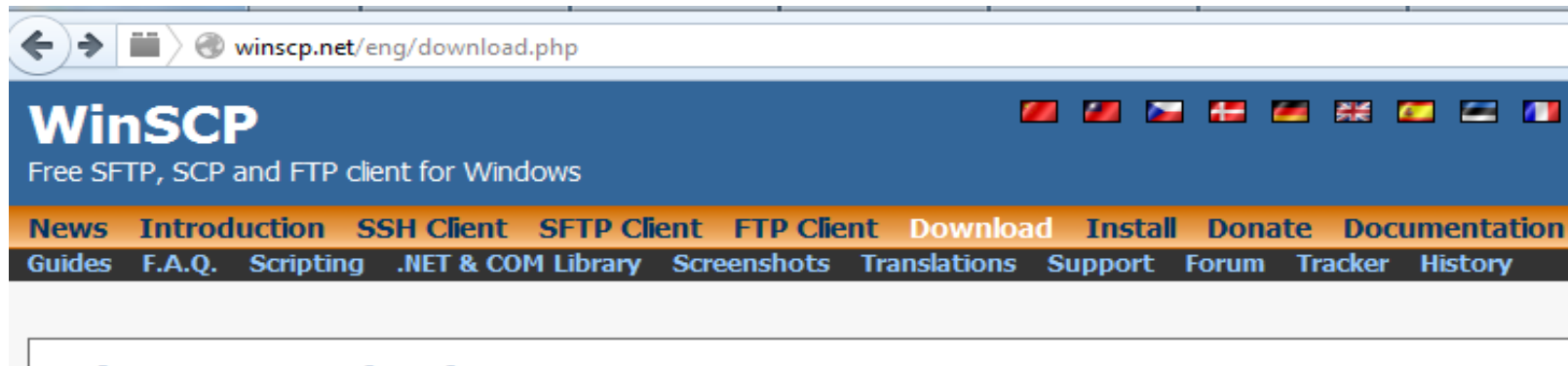


#### 5. Connect Server from Putty

##### 5.1 Download and setup WinSCP, Putty

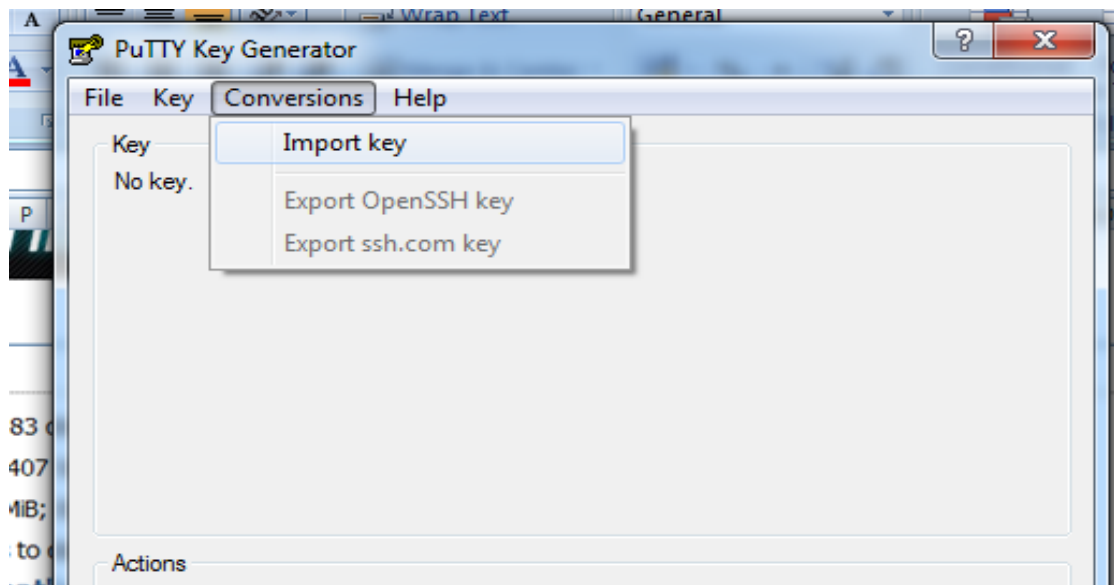
Download link

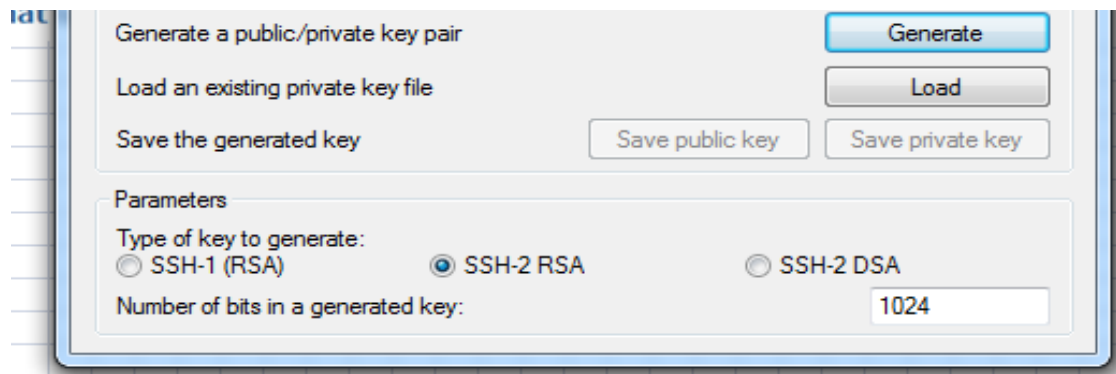
<http://winscp.net/eng/download.php>



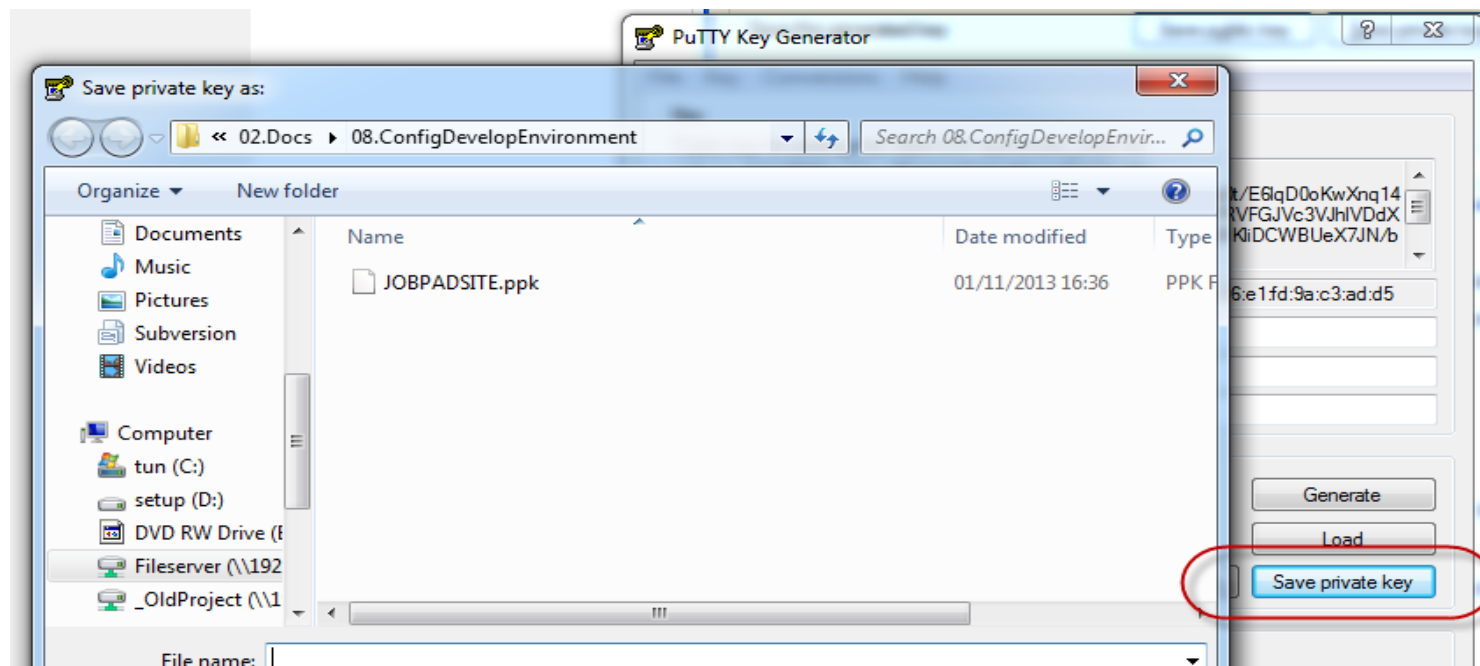
## 5.2 Create PPK from PEM

Open Putty Key, **DONOT CLICK GENERATE**

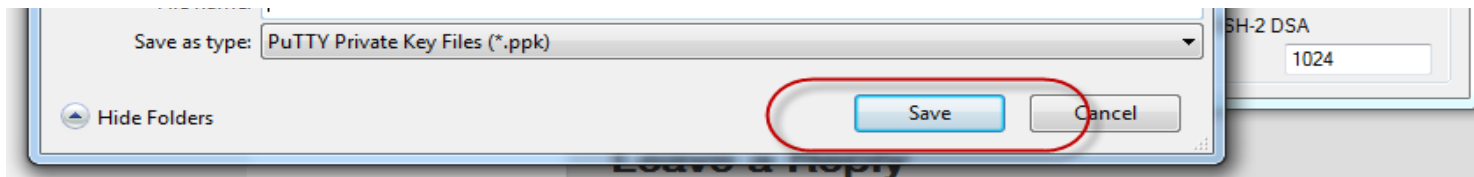




Save Private Key

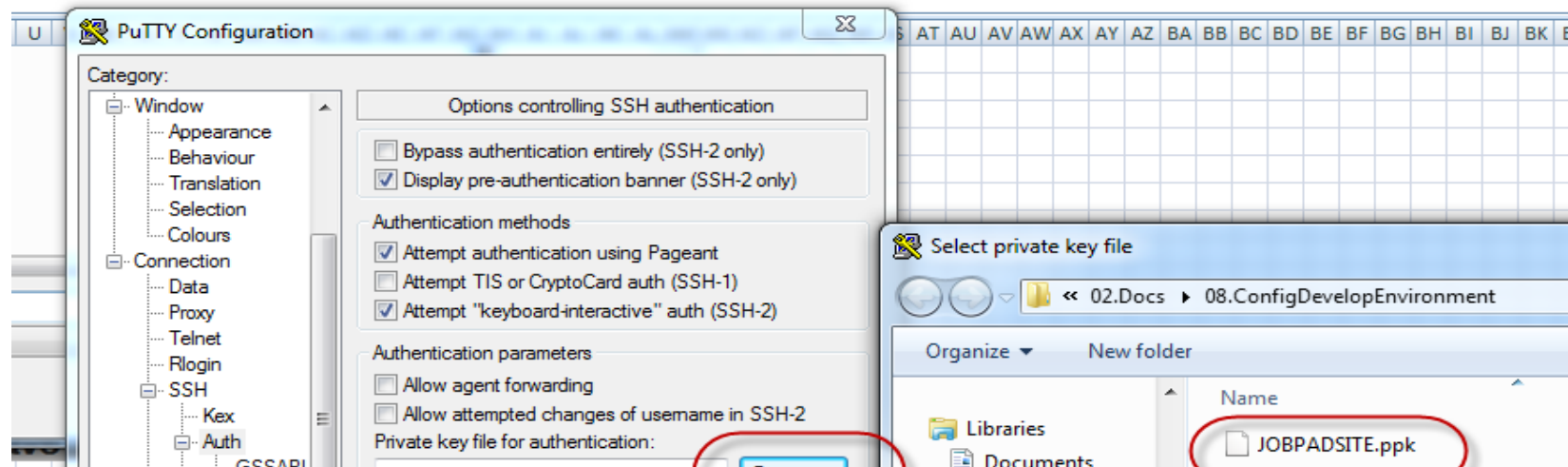


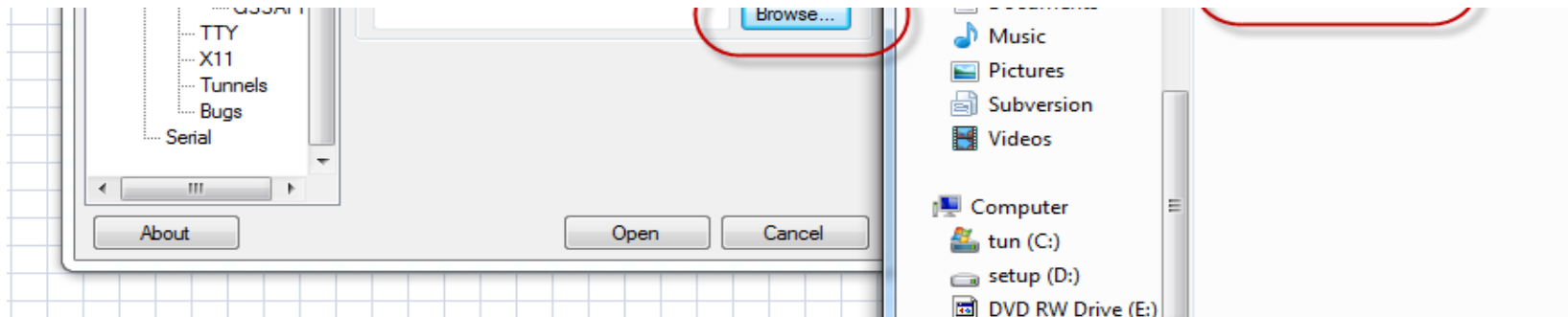




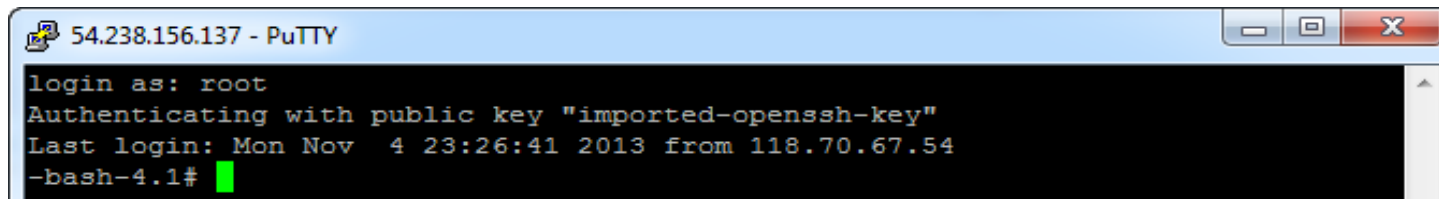
## 6. Setup server

6.1 Use PPK file, open Putty to connect to server. Use **ROOT** account  
Use registered static IP on AWS (Ex. 54.238.156.137)





## 6.2 Login via root user



## 6.3 Upgrade system

yum update

## 6.4 Add repo for new source code

rpm -Uvh http://repo.webtatic.com/yum/el6/latest.rpm

## 6.5 Install Apache 2.2.15, PHP 5.4.19, MySQL 5.5.30

<https://www.digitalocean.com/community/articles/how-to-install-linux-apache-mysql-php-lamp-stack-on-centos-6>

yum --enablerepo=remi install httpd

service httpd start

yum --enablerepo=remi install mysql-server

service mysqld start

/usr/bin/mysql\_secure\_installation

*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? [Y/n] 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? [Y/n] n*  
*... 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? [Y/n] y*  
*- Dropping test database...*  
*... Success!*  
*- Removing privileges on test database...*  
*... Success!*

*Reloading the privilege tables will ensure that all changes made so far will take effect immediately.*

*Reload privilege tables now? [Y/n] y*  
*... Success!*

*Cleaning up...*

*All done! If you've completed all of the above steps, your MySQL installation should now be secure.*

*Thanks for using MySQL!*

Set password for root user is **[jobpajobpa]**

```
yum --enablerepo=remi install php php-mysql
```

```
yum --enablerepo=remi install php-gd
```

```
yum --enablerepo=remi install php-xml
```

```
yum --enablerepo=remi install php-soap
```







```
yum --enablerepo=remi install php-mbstring
```














```
yum --enablerepo=remi install php-mysqli
```

#### 6.6 Install phpmyadmin

<http://www.tecmint.com/install-phpmyadmin-for-apache-or-nginx-on-rhelcentos-6-3-5-8-fedora-17-12/>

#### 6.7 Use WINSXP to copy all source code to /var/www/html

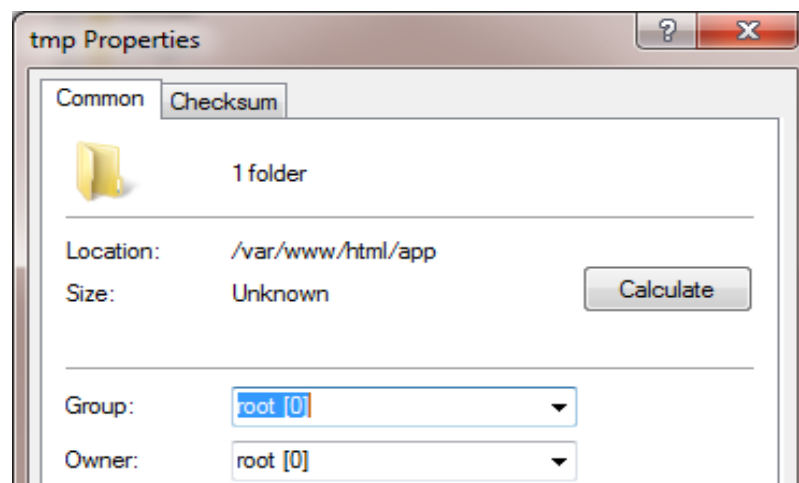
Name	Ext	Size	Changed	Rights	Owner
			01/11/2013 17:40:39	rwxr-xr-x	root
 .settings			05/11/2013 09:30:07	rwxr-xr-x	root
 app			05/11/2013 09:32:52	rwxr-xr-x	root
 lib			05/11/2013 09:41:33	rwxr-xr-x	root
 plugins			05/11/2013 09:47:50	rwxr-xr-x	root
 script			05/11/2013 09:47:50	rwxr-xr-x	root

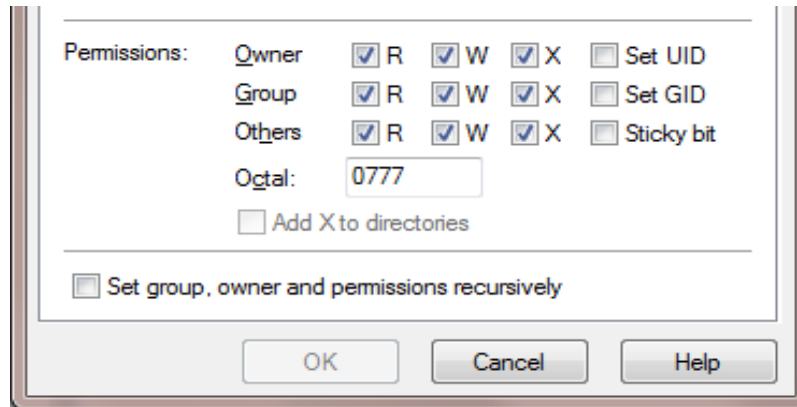
 vendors		05/11/2013 09:47:51	rw-r--r--	root
 .buildpath	174 B	01/04/2013 15:16:12	rw-r--r--	root
 .editorconfig	265 B	01/04/2013 15:16:12	rw-r--r--	root
 .gitignore	333 B	01/04/2013 15:15:36	rw-r--r--	root
 .htaccess	139 B	03/06/2013 09:36:46	rw-r--r--	root
 .project	520 B	27/08/2013 13:10:01	rw-r--r--	root
 .travis.yml	3,588 B	01/04/2013 15:15:36	rw-r--r--	root
 build.properties	174 B	01/04/2013 15:16:12	rw-r--r--	root
 build.xml	9,907 B	01/04/2013 15:16:12	rw-r--r--	root
 index.php	1,466 B	01/04/2013 15:16:12	rw-r--r--	root
 info.php	21 B	01/11/2013 17:49:39	rw-r--r--	root
 README.md	1,665 B	01/04/2013 15:16:12	rw-r--r--	root
 test.php	22 B	22/03/2013 13:44:38	rw-r--r--	root

Change access right to 0777 for the following folders:

/var/www/html/app/tmp

/var/www/html/app/webroot/img





6.8 Use WINSXP, duplicate source code from /usr/share/phpMyAdmin to /app/webroot/phpMyAdmin

6.7 Create Database

Access <http://54.238.156.137/app/webroot/phpMyAdmin/index.php>

Create DB jobpad, Charset [utf8 -- UTF-8 Unicode], Collation [utf8\_general\_ci]

Run matomesite\_sql để create table, view, data

6.8 Use putty to restart httpd, mysqld

service httpd restart

service mysqld restart

6.9 Use putty to setup Cron Job for BATCH

Change access right of file /var/www/html/app/Console/cake to 755

crontab -e

0 1 \* \* \* cd /var/www/html/app && Console/cake batch

(Insert to input data, Shift-ZZ to exit crontab editor)

6.10 Update file etc/httpd/conf/httpd.conf, from [AllowOverride none] to [AllowOverride All]

```
<Directory />
```

```
Options FollowSymLinks
```

```
AllowOverride All
```

```
</Directory>
```

```
AllowOverride All
```

```
<Directory "/var/www/icons">
```

```
Options Indexes MultiViews FollowSymLinks
```

```
AllowOverride All
```

```
Order allow,deny
```

```
Allow from all
```

```
</Directory>
```

6.11 Update file etc/php.ini

```
Set time zone
```

```
date.timezone = Asia/Tokyo
```

```
Set upload max size to 10Mb
```

```
upload_max_filesize = 10M
```

```
Set data post max size to 10Mb
```

```
post_max_size = 10M
```

6.12 Installing Clam AntiVirus

```
http://datlinux.blogspot.com/2013/03/how-to-install-clamav-on-linux-centos.html
```

```
wget http://pkgs.repoforge.org/clamav/clamav-0.97.2-1.el5.rf.x86\_64.rpm
```

```
wget http://pkgs.repoforge.org/clamav/clamav-db-0.97.2-1.el5.rf.x86\_64.rpm
```

```
rpm -ivh clamav-0.97.2-1.el5.rf.x86_64.rpm
```

```
rpm -ivh clamav-db-0.97.2-1.el5.rf.x86_64.rpm
```

```
crontab -e
```

```
05 2 * * * root clamscan -R /var/www
```

```
00 10 * * * * root freshclam
```