

COMP 4632

Practicing Cybersecurity: Attacks and Counter-measures

Week 13 Lab Exercise

Topic: Cloud Security

Lab Objective

Cloud computing is a hot technology trend in IT industry. Many businesses have started adopting cloud service in order to gain benefit from it. However, cloud security is always a concern among all cloud users. This cloud security related lab aims at achieving the following objectives:

- Understand what security measures can be adopted on cloud service
- Experience how to setup a two tier architecture on public cloud
- Understand the importance of identity and access management (IAM) on cloud service

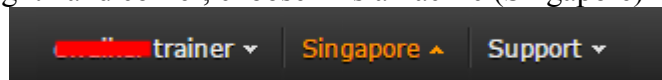
**This lab mainly relies on Amazon Web Service (AWS), an IaaS cloud provider. Students are required to register an AWS account by following instructions in pre-class setup lab sheet.*

Task 1 – Network Architecture Design on Cloud

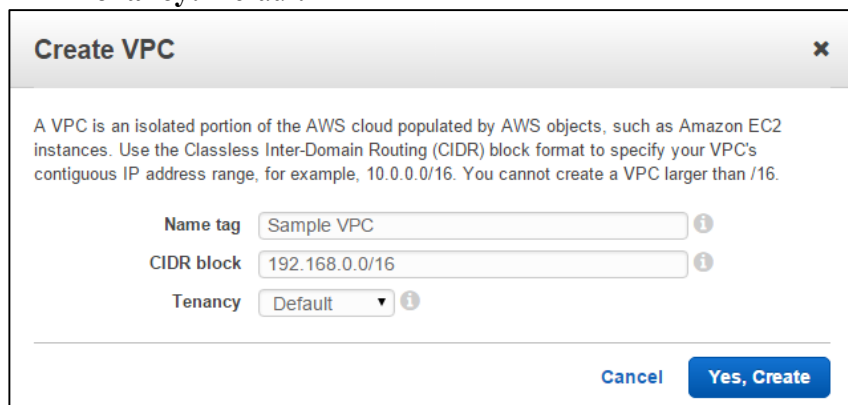
Although cloud service provider is responsible for providing network service to cloud user, implementation of secure network architecture for application is still the responsibility of cloud users. In this task, we are going to design a two tier architecture on AWS.

Task 1.1 Setup Virtual Private Cloud (VPC)

- Login the AWS in the following link and access the management console
 - <https://console.aws.amazon.com/>
- On top right hand corner, choose “Asia Pacific (Singapore)”



- On top left hand corner, choose Services => Networking => VPC
- On left navigation panel, select “Your VPCs”
- On right view, select “Create VPC”, type below value, click “Yes, Create”
 - **Name tag:** [Any]
 - **CIDR block:** 192.168.0.0/16
 - **Tenancy:** Default



Create VPC [X]

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. Use the Classless Inter-Domain Routing (CIDR) block format to specify your VPC's contiguous IP address range, for example, 10.0.0.0/16. You cannot create a VPC larger than /16.

Name tag: ⓘ

CIDR block: ⓘ

Tenancy: ⓘ

[Cancel](#) [Yes, Create](#)

- The newly created VPC network is displayed on dashboard as follows

Create VPCActions

Search VPCs and their properties

<input type="checkbox"/>	Name	VPC ID	State	VPC CIDR	DHCP options set	Route table	Network ACL	Tenancy	Default VPC
<input type="checkbox"/>		vpc-0e4fc66b	available	172.31.0.0/16	dopt-457cbc20	rtb-1fe5877a	acl-77caae12	Default	Yes
<input checked="" type="checkbox"/>	Sample VPC	vpc-2440c941	available	192.168.0.0/16	dopt-457cbc20	rtb-8ce88ae9	acl-13d5b176	Default	No

Task 1.2 Configure Subnet and Associate to VPC

- On left navigation panel, select “Subnets”
- On right view, select “Create Subnet”, type below value, click “Yes, Create”
 - Name tag:** Application Subnet
 - VPC:** [Choose the one you created]
 - Availability Zone:** ap-southeast-1a
 - CIDR block:** 192.168.100.0/24

Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC.

Name tag

VPC

Availability Zone

CIDR block

- Setup one more subnet with the following information
 - Name tag:** Database Subnet
 - VPC:** [Choose the one you created]
 - Availability Zone:** ap-southeast-1a
 - CIDR block:** 192.168.200.0/24
- The newly created subnets are displayed on dashboard as follows

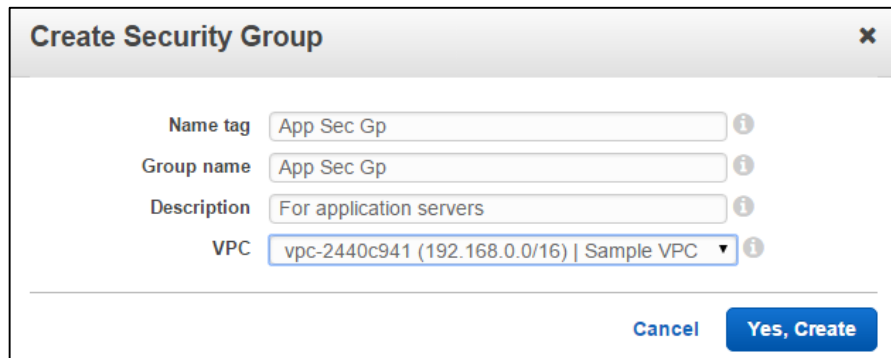
<input type="checkbox"/>	Name	Subnet ID	State	VPC	CIDR	Available IPs	Availability Zone	Route Table	Network ACL	Default Subnet	Auto-assign Public IP
<input type="checkbox"/>		subnet-c52157b2	available	vpc-0e4fc66b (172.31.0.0/16)	172.31.16.0/20	4091	ap-southeast-1b	rtb-1fe5877a	acl-77caae12	Yes	Yes
<input type="checkbox"/>		subnet-06b4ce63	available	vpc-0e4fc66b (172.31.0.0/16)	172.31.0.0/20	4091	ap-southeast-1a	rtb-1fe5877a	acl-77caae12	Yes	Yes
<input checked="" type="checkbox"/>	Application Subnet	subnet-9eabd11b	available	vpc-2440c941 (192.168.0.0/16) ...	192.168.100.0/24	251	ap-southeast-1a	rtb-8ce88ae9	acl-13d5b176	No	No
<input checked="" type="checkbox"/>	Database Subnet	subnet-6da8d208	available	vpc-2440c941 (192.168.0.0/16) ...	192.168.200.0/24	251	ap-southeast-1a	rtb-8ce88ae9	acl-13d5b176	No	No

- Right click the subnet => select “Modify Auto-Assign Public IP”
- Check the box “Enable auto-assign Public IP” => click “Save”
- Do the same setting on another subnet

<input type="checkbox"/>	Name	Subnet ID	State	VPC	CIDR	Available IPs	Availability Zone	Route Table	Network ACL	Default Subnet	Auto-assign Public IP
<input type="checkbox"/>	Application Subnet	subnet-9eabd11b	available	vpc-2440c941 (192.168.0.0/16) ...	192.168.100.0/24	251	ap-southeast-1a	rtb-8ce88ae9	acl-13d5b176	No	Yes
<input checked="" type="checkbox"/>	Database Subnet	subnet-6da8d208	available	vpc-2440c941 (192.168.0.0/16) ...	192.168.200.0/24	251	ap-southeast-1a	rtb-8ce88ae9	acl-13d5b176	No	Yes

Task 1.3 Security Configuration on VPC

- On left navigation panel, select “Security Groups”
- On right view, select “Create Security Group”, type below value, click “Yes, Create”
 - Name tag:** App Sec Gp
 - Group Name:** App Sec Gp
 - Description:** For application servers
 - VPC:** [Choose the one you created]



Create Security Group

Name tag: App Sec Gp

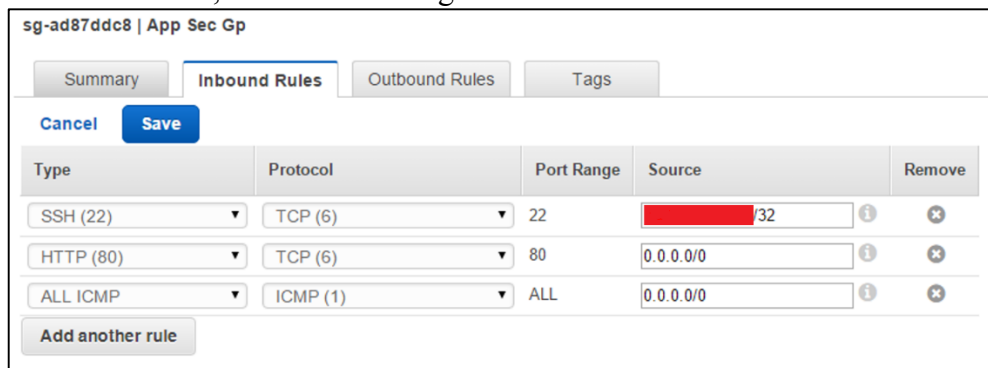
Group name: App Sec Gp

Description: For application servers

VPC: vpc-2440c941 (192.168.0.0/16) | Sample VPC

Buttons: Cancel, Yes, Create

- Click the new security group, select “**Inbound Rules**” at bottom right panel
- Click “**Edit**”, add the following rules and click “**Save**”



sg-ad87ddc8 | App Sec Gp

Summary Inbound Rules Outbound Rules Tags

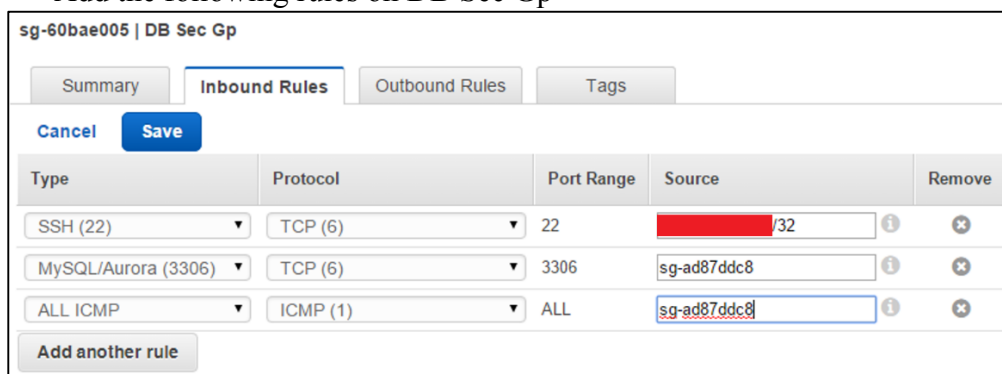
Cancel Save

Type	Protocol	Port Range	Source	Remove
SSH (22)	TCP (6)	22	[Redacted] /32	[Info] [Remove]
HTTP (80)	TCP (6)	80	0.0.0.0/0	[Info] [Remove]
ALL ICMP	ICMP (1)	ALL	0.0.0.0/0	[Info] [Remove]

Add another rule

**Note: Only your own IP address is allowed to connect to SSH port*

- Create one more security group for database servers with the following setting
 - **Name tag:** DB Sec Gp
 - **Group Name:** DB Sec Gp
 - **Description:** For database servers
 - **VPC:** [Choose the one you created]
- Add the following rules on DB Sec Gp



sg-60bae005 | DB Sec Gp

Summary Inbound Rules Outbound Rules Tags

Cancel Save

Type	Protocol	Port Range	Source	Remove
SSH (22)	TCP (6)	22	[Redacted] /32	[Info] [Remove]
MySQL/Aurora (3306)	TCP (6)	3306	sg-ad87ddc8	[Info] [Remove]
ALL ICMP	ICMP (1)	ALL	sg-ad87ddc8	[Info] [Remove]

Add another rule

**Note: Only open MySQL port and ICMP for App Sec Gp*

In this task, we would not touch “Network ACLs” for simplicity. Network ACLs in AWS acts as firewall at subnet level while Security Groups acts as firewall at instance level. For details, please see the following reference:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html

##Question 1

What is the difference on ruleset between “stateful” firewall (i.e. Security Group) and “stateless” firewall (i.e. Network ACL)? (0.5 mark)

Task 1.4 Internet Gateway and Route Table Configuration

- On left navigation panel, select “**Internet Gateways**”
- On right view, select “**Create Internet Gateway**”, type below value, click “**Yes, Create**”

Create Internet Gateway

An Internet gateway is a virtual router that connects a VPC to the Internet.

Name tag

- On left navigation panel, select “**Route Tables**”
- On right view, select the route table of your own VPC
- At bottom right panel, select “**Routes**” tab and click “**Edit**”
- Add the route with the target of internet gateway that just created

<input type="checkbox"/>	Name	Route Table ID	Explicitly Associat	Main	VPC
<input checked="" type="checkbox"/>		rtb-8ce88ae9	0 Subnets	Yes	vpc-2440c941 (192.168.0.0/16) Sample VPC
<input type="checkbox"/>		rtb-1fe5877a	0 Subnets	Yes	vpc-0e4fc66b (172.31.0.0/16)

rtb-8ce88ae9

Destination	Target	Status	Propagated	Remove
192.168.0.0/16	local	Active	No	
0.0.0.0/0	igw-6075d105	Active	No	<input type="button" value="x"/>

Task 2 – Instances on Cloud

After designing the network architecture on the public cloud, it is time to launch instances and put them into appropriate network segment for protection.

Task 2.1 Instance Launching (Application Server)

- On top left hand corner, choose Services => Compute => EC2
- On left navigation panel, select “**Instances**”
- On right view, select “**Launch Instance**”
- Step 1: Choose an Amazon Machine Image (AMI)
 - Select “**Ubuntu Server 14.04 LTS (HVM), SSD Volume Type**”



Ubuntu Server 14.04 LTS (HVM), SSD Volume Type - ami-96f1c1c4

Free tier eligible

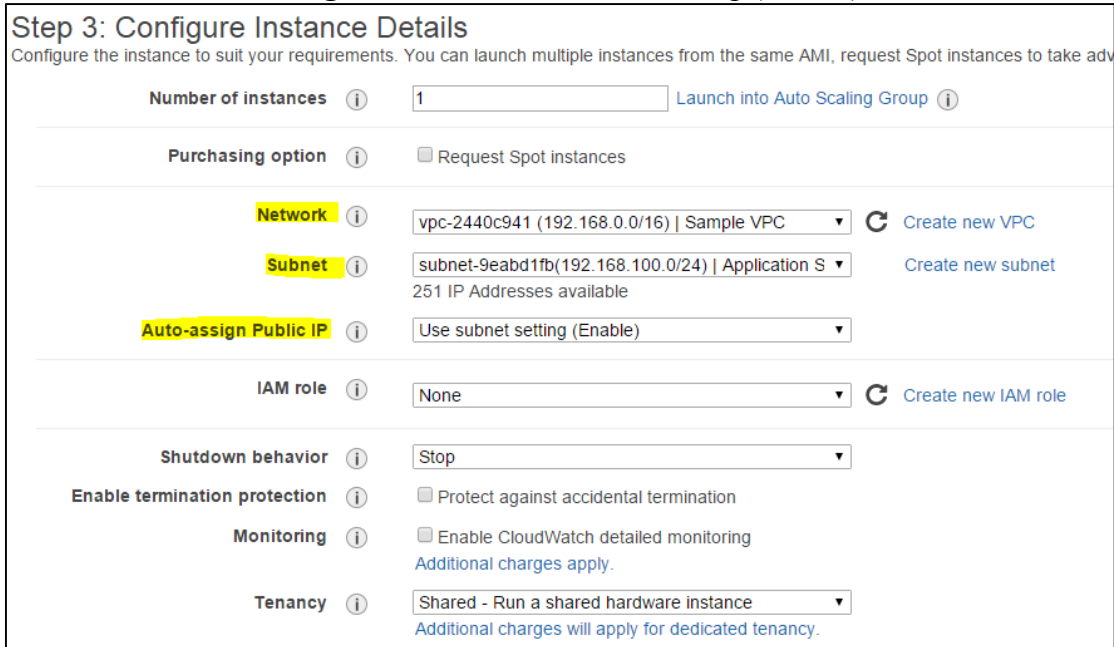
Root device type: ebs Virtualization type: hvm

- Step 2: Choose an Instance Type
 - Select “**t2.micro**” and click “**Next: configure Instance Details**”

Family	Type	vCPUs	Memory (GiB)
General purpose	t2.micro Free tier eligible	1	1

Note: If you choose other instance types, charge will be resulted as they are **NOT free tier eligible.*

- Step 3: Configure Instance Details
 - Keep all default values except the following settings:
 - **Network**: [Choose the VPC you created]
 - **Subnet**: [Choose the application subnet]
 - **Auto-assign Public IP**: Use subnet setting (Enable)



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of lower prices.

Number of instances: 1 [Launch into Auto Scaling Group](#)

Purchasing option: ☐ Request Spot instances

Network: vpc-2440c941 (192.168.0.0/16) | Sample VPC [Create new VPC](#)

Subnet: subnet-9eabd1fb (192.168.100.0/24) | Application S [Create new subnet](#)
251 IP Addresses available

Auto-assign Public IP: Use subnet setting (Enable)

IAM role: None [Create new IAM role](#)

Shutdown behavior: Stop

Enable termination protection: ☐ Protect against accidental termination

Monitoring: ☐ Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

Tenancy: Shared - Run a shared hardware instance
[Additional charges will apply for dedicated tenancy.](#)

- Step 4: Add Storage
 - Keep default values and click “**Next: Tag Instance**”
- Step 5: Tag Instance
 - Input the following tag and click “**Next: Configure Security Group**”
 - **Key:** Name => **Value:** Application Server

Step 5: Tag Instance
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)
Name	Application Server

- Step 6: Configure Security Group
 - Choose “**Select an existing security group**”
 - Select “**App Sec Gp**” and Click “**Review and Launch**”

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 allow specific traffic to reach your instance. For example, if you want to set up the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [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	Description
<input checked="" type="checkbox"/> sg-ad87ddc8	App Sec Gp	For application servers
<input type="checkbox"/> sg-60bae005	DB Sec Gp	For database servers
<input type="checkbox"/> sg-a180dac4	default	default VPC security group

- Step 7: Review Instance Launch
 - Choose “**Launch**” after ensuring all configurations are correct
 - Select “**Create a new key pair**”
 - Type in key pair name and click “**Download Key Pair**”
 - Click “**Launch Instances**”

Save As

This PC > Desktop > temp

Search temp

New folder

Name	Date modified	Type
No items match your search.		

SampleKeys.pem

PEM File (.pem)

Save Cancel

Select an existing key pair or create a new key pair

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.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

Key pair name

Sample Keys

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 “**View Instance**” and return to Dashboard

Launch Instance

Connect

Actions

Filter by tags and attributes or search by keyword

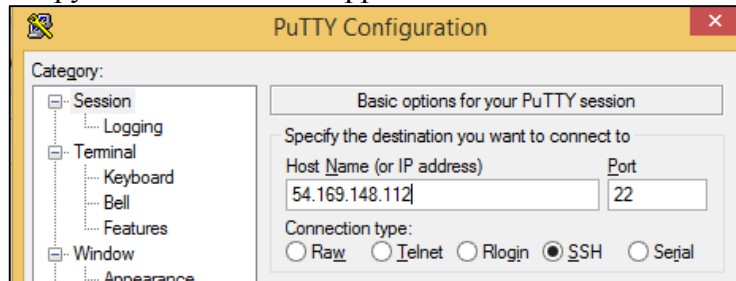
	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS	Public IP	Key Name
	Application ...	i-42cfbae6	t2 micro	ap-southeast-1a	running	Initializing	None		54.169.148.112	Sample Keys

Task 2.2 Instance Launching (Database Server)

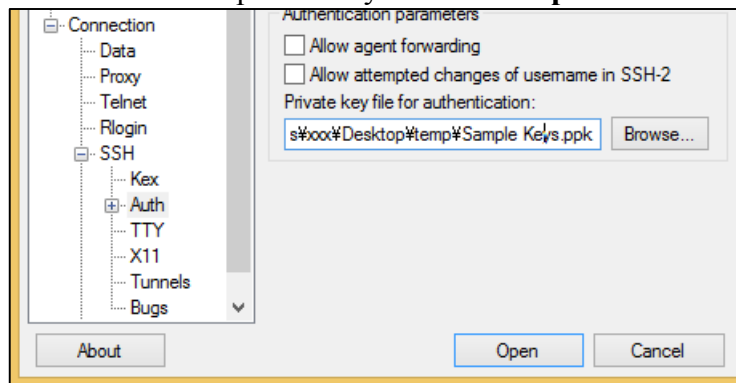
- Repeat the steps in task 2.1 and launch an instance for database server
- Please pay attention to the following setting
 - Place it into correct **SUBNET**
 - Choose correct **SECURITY GROUP**
 - Use the same **Key Pair**

Task 2.3 Connect to Application Instance via SSH

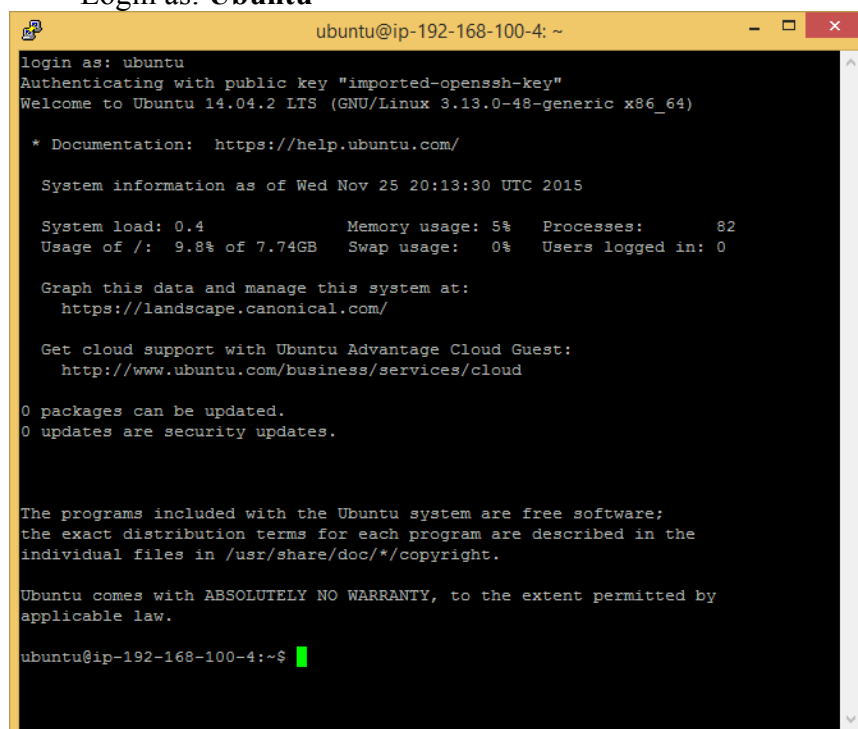
- Use PuttyGen to convert the PEM key to PPK key
 - Load the PEM Key
 - Click “Save private key”
- Use “Putty” to connect to the instance
 - Copy the “Public IP” of application server



- On left panel, expand “SSH” => select “Auth”
- Browse the PPK private key and click “Open”



- Click “Yes” for PuTTY Security Alert
- Browse the PPK private key and click “Open”
- Login as: **Ubuntu**



##Question 2

Try to perform PING from Application server to public IP and private IP of Database server. Describe the observation and briefly explain why. (1 mark)

Hint: Security Group and Route Table

##Question 3

Sketch a simple network diagram with ruleset information of this lab. (1.5 marks)

Task 3 – IAM on Cloud

Identity and Access Management always plays an important role in various prospective whatever physical level, OS level, application level or even singular API calling. The same theory applies to cloud service too. Typical application of IAM is on securing the management console.

Task 3.1 Group Creation

- On top left hand corner, choose Services => Security and Identity => IAM
- On left navigation panel, select “**Groups**”
- On right view, select “**Create New Group**”
- Step 1: Group Name
 - Provide “**Group Name**” and click “**Next Step**”
- Step 2: Attach Policy
 - Type “**EC2**” in filter
 - Select “**AmazonEC2ReadOnlyAccess**”
 - Click “**Next Step**”
- Step 3: Review
 - Review the setting and click “**Create Group**”

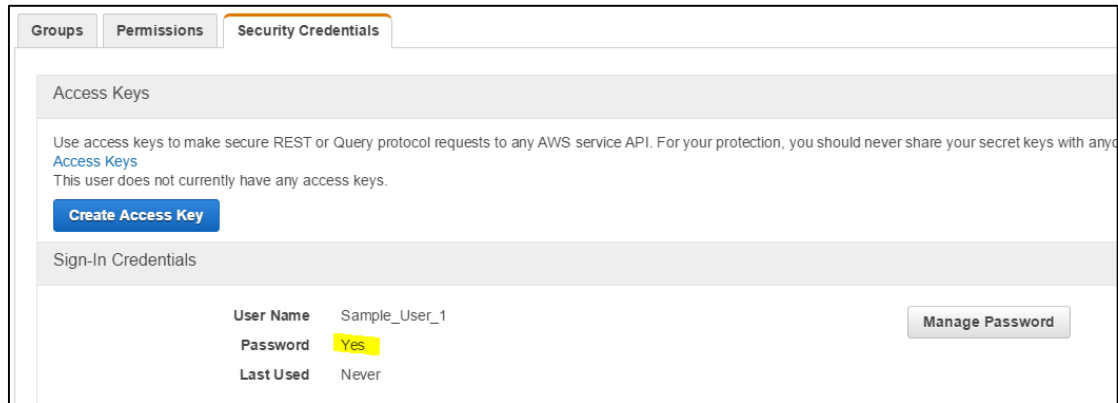
<input type="checkbox"/>	Group Name ↕	Users	Inline Policy
<input type="checkbox"/>	Sample_Group	0	

Task 3.2 User Creation and Group Assignment

- On left navigation panel, select “**Users**”
- On right view, select “**Create New Users**”
- Enter User Name(s)
- Uncheck “**Generate an access key for each user**”

<input type="checkbox"/>	User Name ↕	Groups	Password	Password Last Used ↕	Access Keys
<input type="checkbox"/>	Sample_User_1	0		N/A	None
<input type="checkbox"/>	Sample_User_2	0		N/A	None

- Click the user
- Select “**Security Credentials**” tab => “**Manage Password**”
- Choose “**Assign a custom password**” and set a password



Groups Permissions **Security Credentials**

Access Keys

Use access keys to make secure REST or Query protocol requests to any AWS service API. For your protection, you should never share your secret keys with anyone.

[Access Keys](#)

This user does not currently have any access keys.

[Create Access Key](#)

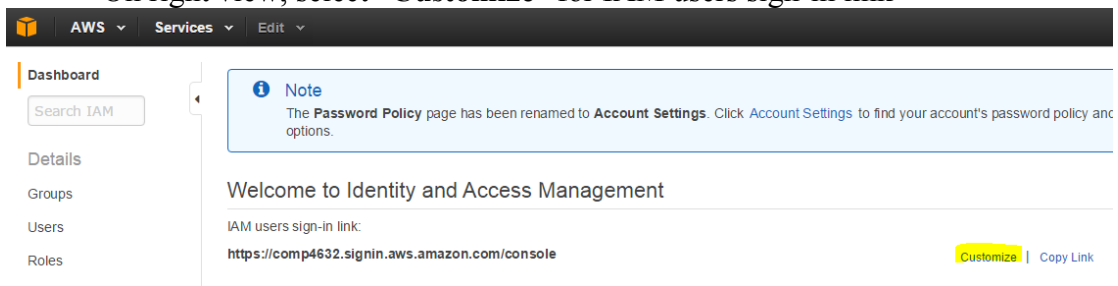
Sign-In Credentials

User Name	Sample_User_1	Manage Password
Password	Yes	
Last Used	Never	

- Select “**Groups**” tab => “**Add User to Groups**”
- Select the group created previously => “**Add to Groups**”

Task 3.3 Test on User Access Right

- On left navigation panel, select “**Dashboard**”
- On right view, select “**Customize**” for IAM users sign-in link



AWS Services Edit

Dashboard

Search IAM

Details

Groups

Users

Roles

Note

The **Password Policy** page has been renamed to **Account Settings**. Click [Account Settings](#) to find your account's password policy and options.

Welcome to Identity and Access Management

IAM users sign-in link:

<https://comp4632.signin.aws.amazon.com/console> [Customize](#) | [Copy Link](#)

- Set a name for the alias
- Open another type of browser and go to the link
- Login as the user you created
- Try to launch an instance and see what happens.

##Bonus Question 1

What is your observation in task 3.3? Please explain why and provide screenshot to support (1 mark)

##Bonus Question 2

What is the use of access key of users in IAM? (0.5 mark)

##Bonus Question 3

List out THREE security measures that you learnt from this lab and lecture which can adopt on cloud service and briefly explain how they work. (1.5 marks)

End of Lab