

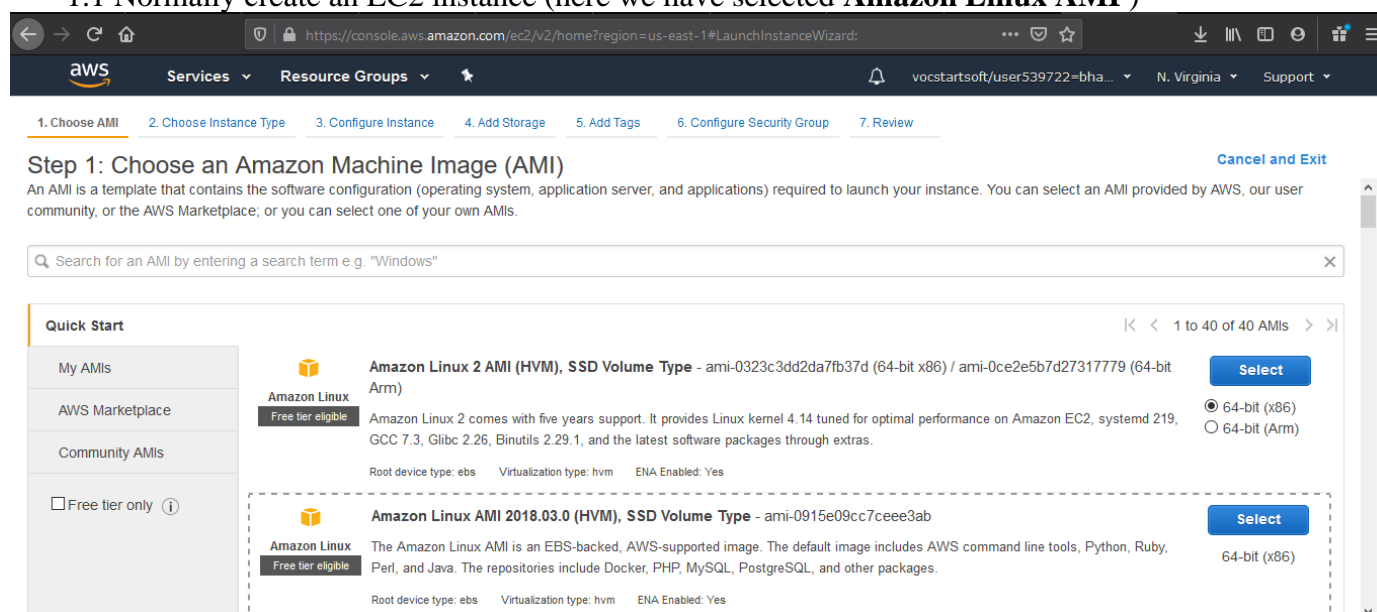
Practical 10: Launching EC2 Spot Instances with Auto Scaling and Amazon CloudWatch

Solution:

Step 1: Create an AMI instance for multiple Spot instances

We need to create an AMI image so that we can copy that same instance and make multiple instances of the same EC2 instances to work with spot instances.

1.1 Normally create an EC2 instance (here we have selected **Amazon Linux AMI**)



1.2 In instance type select basic (free tier)

1.3 In configure Instance details got to **Advance Details** and type the following bash script

```
#!/bin/bash
yum install httpd -y
echo '<h1>Welcome to my AMI </h1>>'>/var/www/html/index.html
chkconfig httpd on
service httpd start
```

This script runs on startup of the instance which download's apache server to run a simple **index.html** file with **Welcome to Ami**

aws Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Additional charges apply.

T2/T3 Unlimited ☐ Enable
Additional charges may apply

File systems

▼ Advanced Details

Metadata accessible

Metadata version

Metadata token response hop limit

User data ☒ As text ☐ As file ☐ Input is already base64 encoded

```
#!/bin/bash
yum install httpd -y
echo '<h1>Welcome to my AMI </h1>>'>/var/www/html/index.html
chkconfig httpd on
service httpd start
```

1.4 Keep storage pre defined

1.5 Add tags:

Key: Name

Value: ASG

aws Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

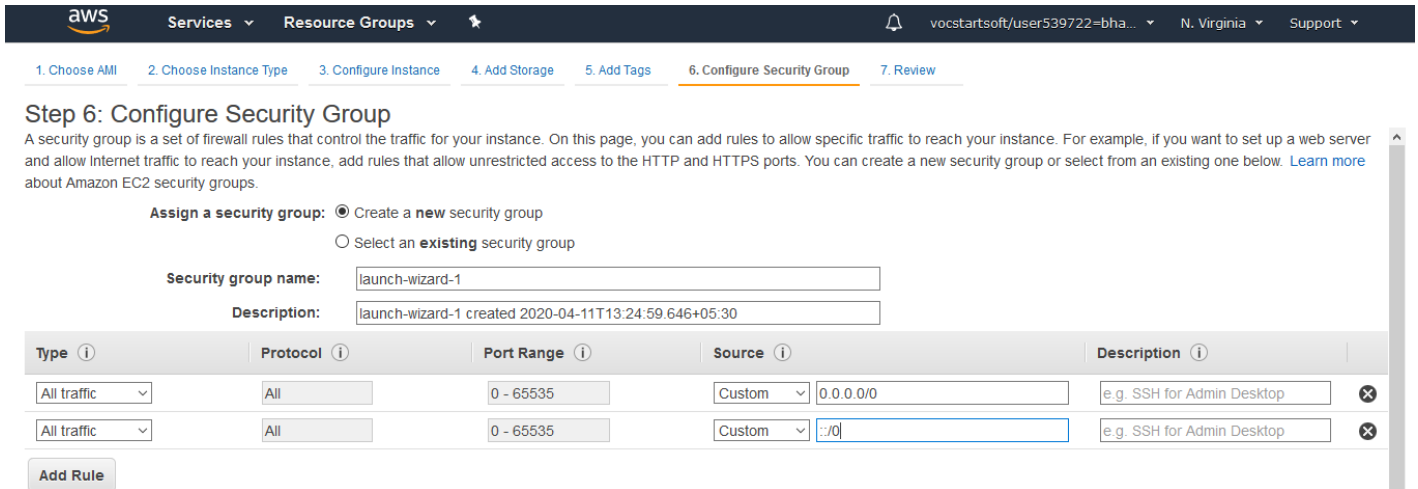
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances <input type="checkbox"/>	Volumes <input type="checkbox"/>
Name	ASG	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

(Up to 50 tags maximum)

1.6 In Configure Security Group

Create a new security group and define 2 rules as below mentioned screenshot



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 a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to 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 name:

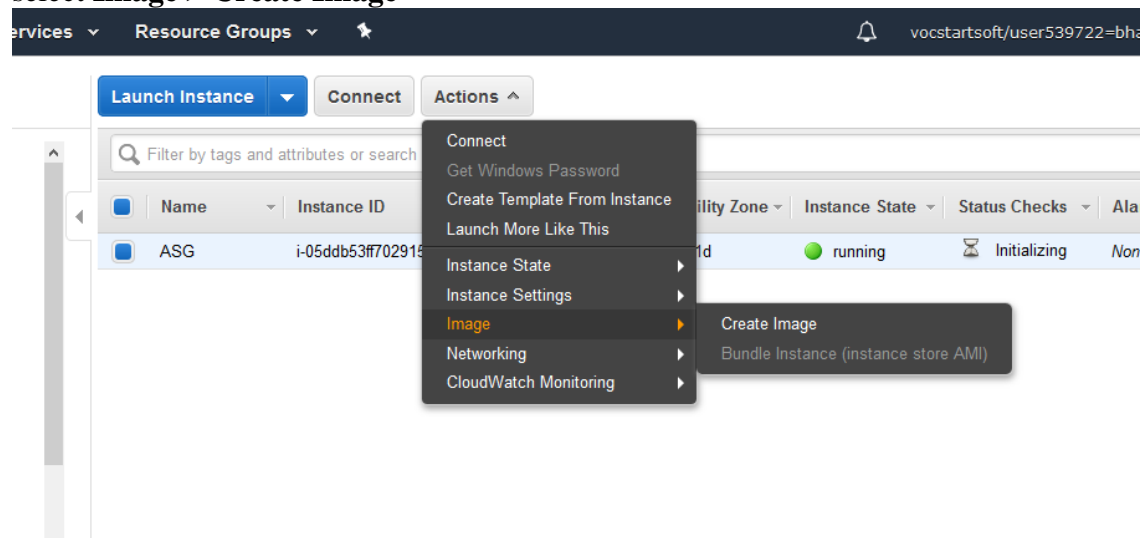
Description:

Type	Protocol	Port Range	Source	Description
All traffic	All	0 - 65535	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
All traffic	All	0 - 65535	Custom ::/0	e.g. SSH for Admin Desktop

[Add Rule](#)

1.7 Review the instance and launch it

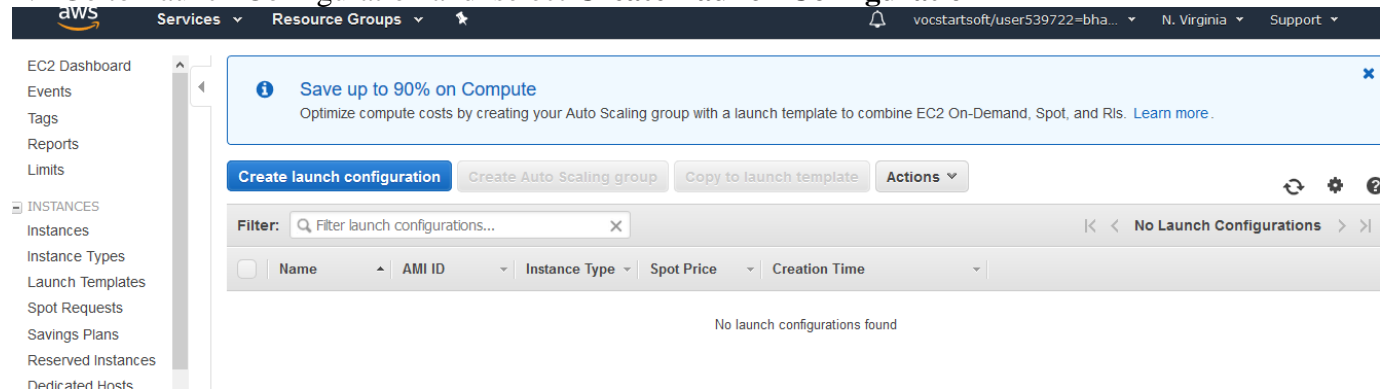
1.8 Now go to the EC2 Dashboard and select the instance which you just created and in **Action** select **Image > Create Image**



1.9 In the Create Image sub menu give whatever name you want and whatever Image Description you want and select Create Image.

Step 2 : Creating Launch Configuration

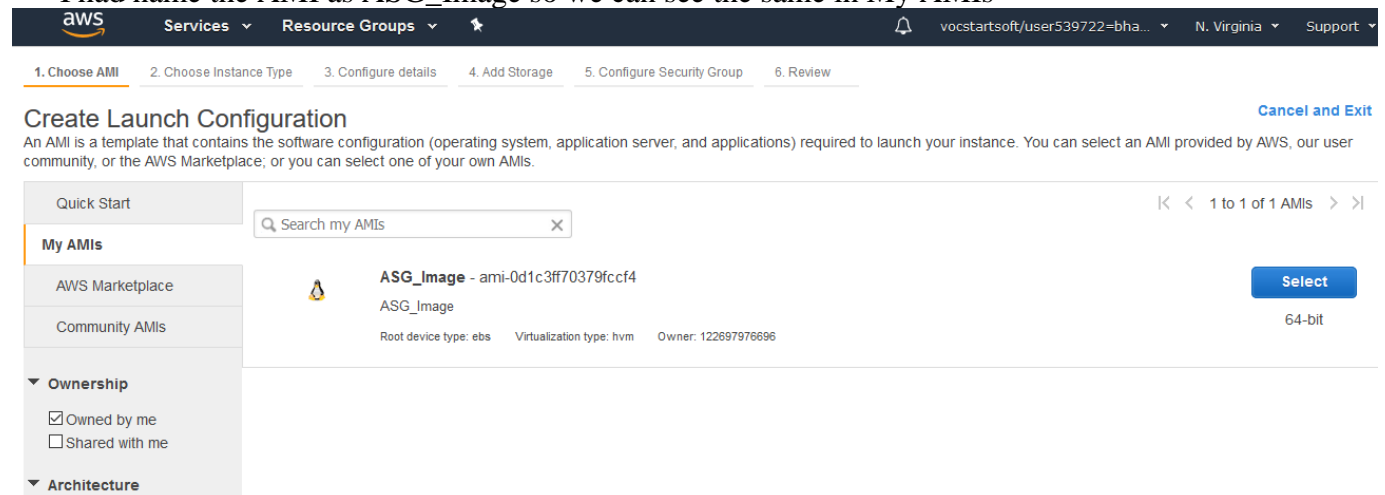
2.1 Go to Launch Configuration and select **Create Launch Configuration**



2.2 Select the option **MyAMI**.

Since we have an Image of AMI we just created we should be able to get the AMI reference here.

I had name the AMI as ASG_Image so we can see the same in My AMIs



2.3 Since we are creating multiple instance of the same AMI we will the same menu as we get while creating an EC2 instance.

2.4 Go with default Configure Details.

2.5 Go with default Storage.

2.6 In Configure Security Group Select an Existing Security Group and select the security group the same for the AMI reference we just created.

1. Choose AMI 2. Choose Instance Type 3. Configure details 4. Add Storage 5. Configure Security Group 6. Review

Create Launch Configuration

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 a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to 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	VPC ID	Description	Actions
<input type="checkbox"/>	sg-01ac5b700948ff8a3	default	vpc-0d7a4c2d61b15b2d4	default VPC security group	Copy to new
<input type="checkbox"/>	sg-f6c34eac	default	vpc-95cea1ef	default VPC security group	Copy to new
<input checked="" type="checkbox"/>	sg-0983f76c2f411c9e5	launch-wizard-1	vpc-95cea1ef	launch-wizard-1 created 2020-04-11T13:24:59.646+05:30	Copy to new

Inbound rules for sg-0983f76c2f411c9e5 Selected security groups: sg-0983f76c2f411c9e5.

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
All traffic	All	All	0.0.0.0/0

2.7 Review and launch

Step 3 : Auto Scaling the instances

3.1 After instances are created the last screen will be appear where it will have an option of **Create an Auto Scaling Group using Launch Configuration**. Select that option.

Launch configuration creation status

✓ **Successfully created launch configuration: Test**
[View creation log](#)

View

[View your launch configurations](#)
[View your Auto Scaling groups](#)

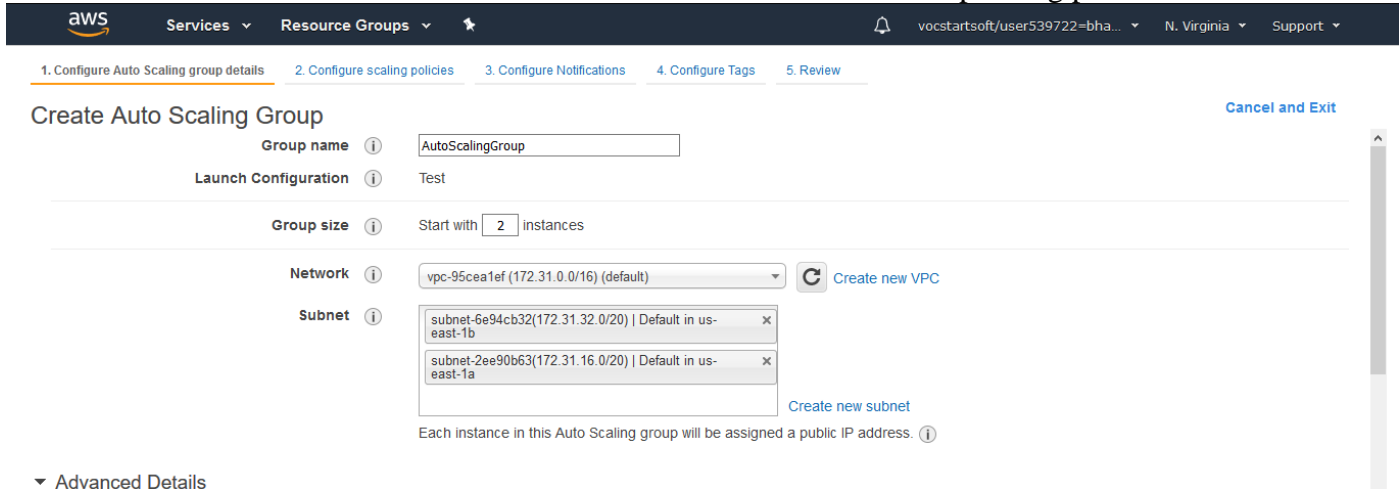
► Here are some helpful resources to get you started

[Create an Auto Scaling group using this launch configuration](#) [Close](#)

3.2 Name the Group Name : AutoScalingGroup(whatever name you prefer)

Start with group Size of : 2 (can be any)

Network : Created VPC network in Practical 2 and in Subnet the corresponding public subnet.



1. Configure Auto Scaling group details 2. Configure scaling policies 3. Configure Notifications 4. Configure Tags 5. Review

Create Auto Scaling Group [Cancel and Exit](#)

Group name

Launch Configuration

Group size

Network [Create new VPC](#)

Subnet [Create new subnet](#)

Each instance in this Auto Scaling group will be assigned a public IP address.

▼ Advanced Details

3.2 Advanced Details

▼ Advanced Details

Load Balancing ☒ Receive traffic from one or more load balancers [Learn about Elastic Load Balancing](#)

Classic Load Balancers

Target Groups

Health Check Type ☒ ELB ☐ EC2

Health Check Grace Period seconds

Monitoring Amazon EC2 Detailed Monitoring metrics, which are provided at 1 minute frequency, are not enabled for the launch configuration javahome-cloud-ic. Instances launched from it will use Basic Monitoring metrics, provided at 5 minute frequency. [Learn more](#)

Instance Protection

Service-Linked Role [View Role in IAM](#)

[Cancel](#) [Next: Configure scaling policy](#)

3.3 Create and save it

Step 4 : After you done with step 3 will have an option of setting an alarm
Set Alarm for increase Group Size and Decrease Group size. Set Rules for the same

Create Alarm ✕

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.
To edit an alarm, first choose whom to notify and then define when the notification should be sent.

☒ **Send a notification to:** [create topic](#) CPU Utilization Percent

Whenever: Average of CPU Utilization

Is: >= 50 Percent ✖ Server Error 0

For at least: 1 consecutive period(s) of 5 Minutes

Name of alarm: awsec2-AutoScalingGroup-High-CPU-Utilizatio

Cancel
Create Alarm

Similarly do the same for what to do when load is less.

Decrease Group Size

Name: Decrease Group Size

Execute policy when: awsec2-AutoScalingGroup-High-CPU-Utilization [Edit](#) [Remove](#)
breaches the alarm threshold: CPUUtilization < 50 for 60 seconds
for the metric dimensions AutoScalingGroupName = AutoScalingGroup

Take the action: Remove 2 capacity units when 50 >= CPUUtilization > -infinity

Add step ⓘ

Create a simple scaling policy ⓘ