greatlearning

Course: Cloud Computing on AWS

By Nirmallya Mukherjee

greatlearning

Introduction

Cloud fundamentals & VERY useful links

Documentation

- Bookmark these
  - https://aws.amazon.com/documentation
  - https://aws.amazon.com/faqs
  - https://aws.amazon.com/blogs/aws
  - https://aws.amazon.com/whitepapers
- Keep this information handy and if necessary download the PDF wherever available

Certification prep

greatlearning

Exam overview

- https://aws.amazon.com/certification/certification-prep/
- https://aws.amazon.com/certification/our-certifications/
- https://aws.amazon.com/certification/certified-solutions-architect-associate/

Study materials

- https://aws.amazon.com/whitepapers/
- https://aws.amazon.com/architecture/
- https://aws.amazon.com/ec2/faqs/

- http://docs.aws.amazon.com/autoscaling/latest/userguide/as-instance-termination.html
- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html
- https://aws.amazon.com/premiumsupport/knowledge-center/snapshot-ebs-raid-array/
- https://aws.amazon.com/ec2/vm-import/
- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html
- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html
- http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html
- http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/LSI.html
- https://aws.amazon.com/devpay/
- http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html
- http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-anatomy.html
- http://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html

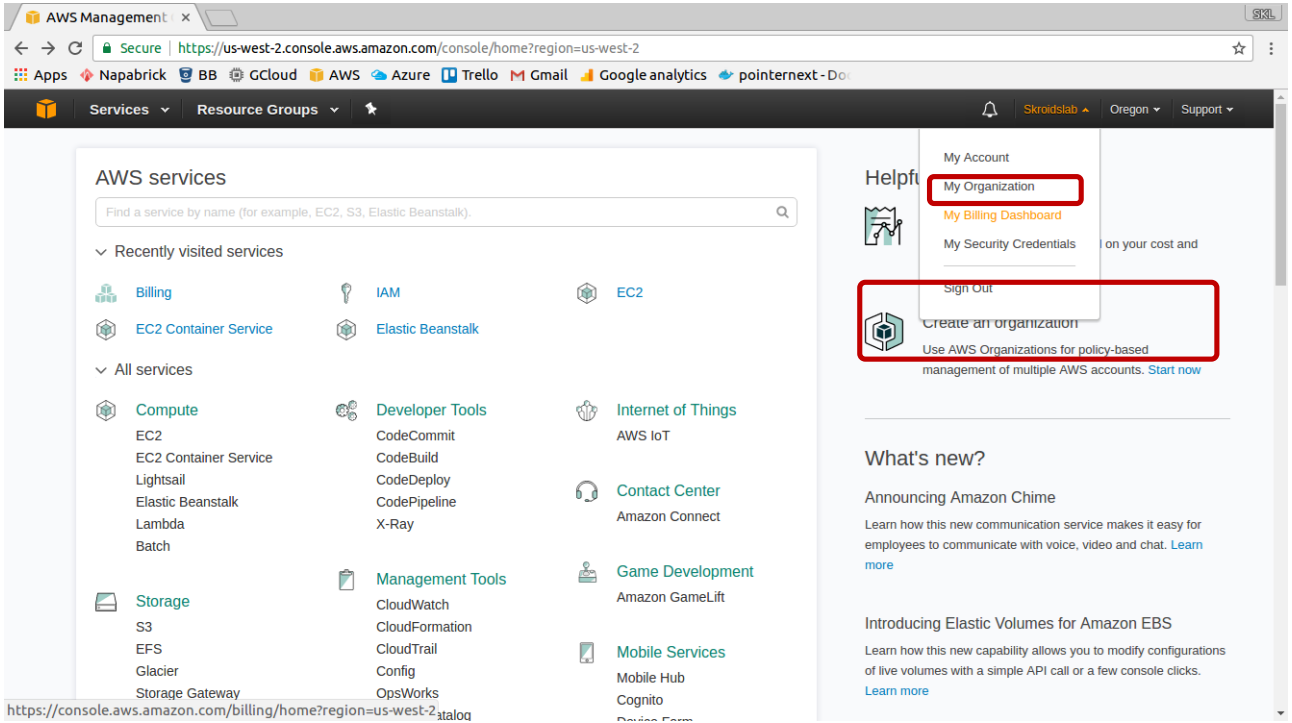
- Interesting-> https://www.awsarchitectureblog.com/2014/04/shuffle-sharding.html
- Free datasets-> https://aws.amazon.com/public-datasets/

greatlearning

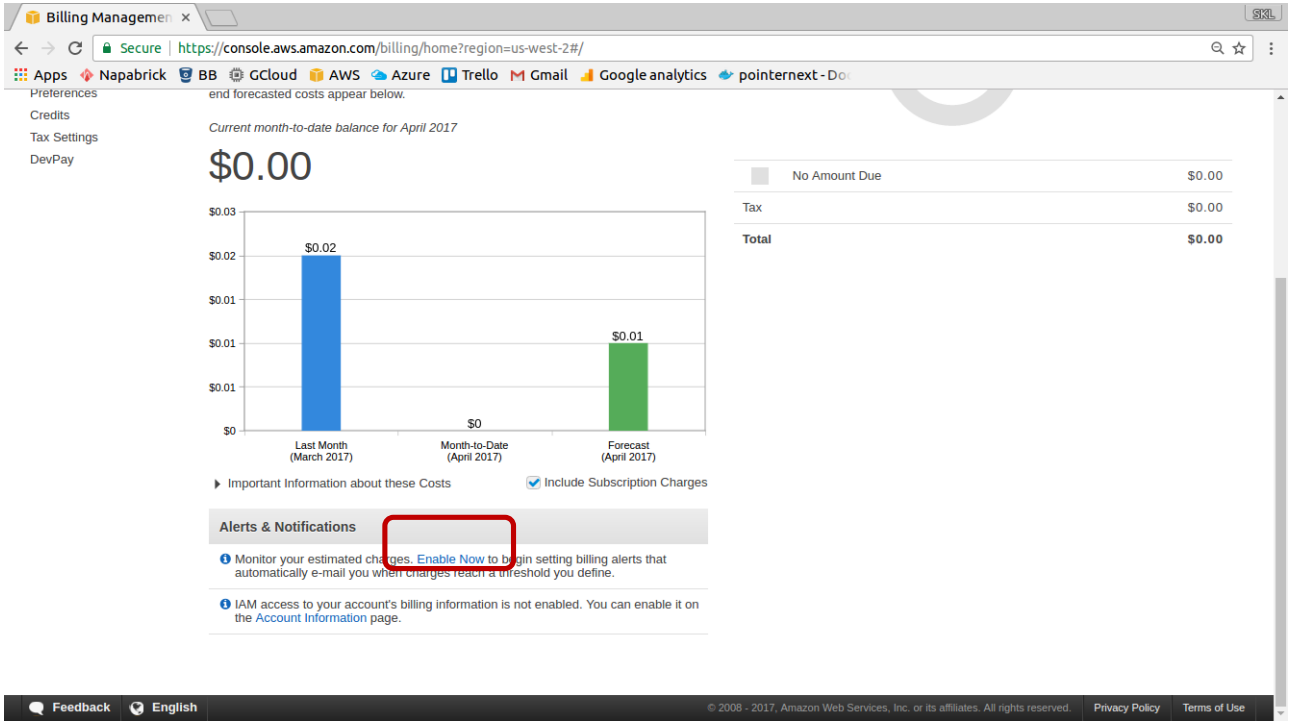
Introduction

Understanding billing and alerts

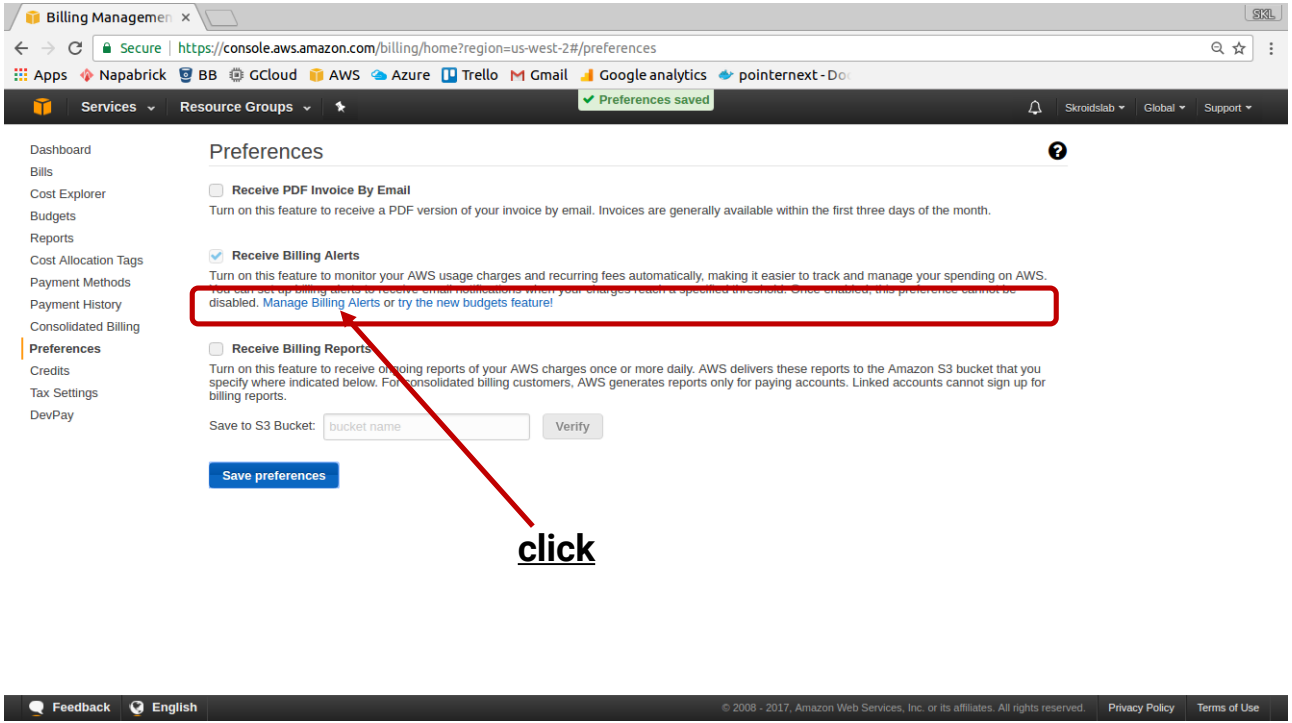
Billing - dashboard



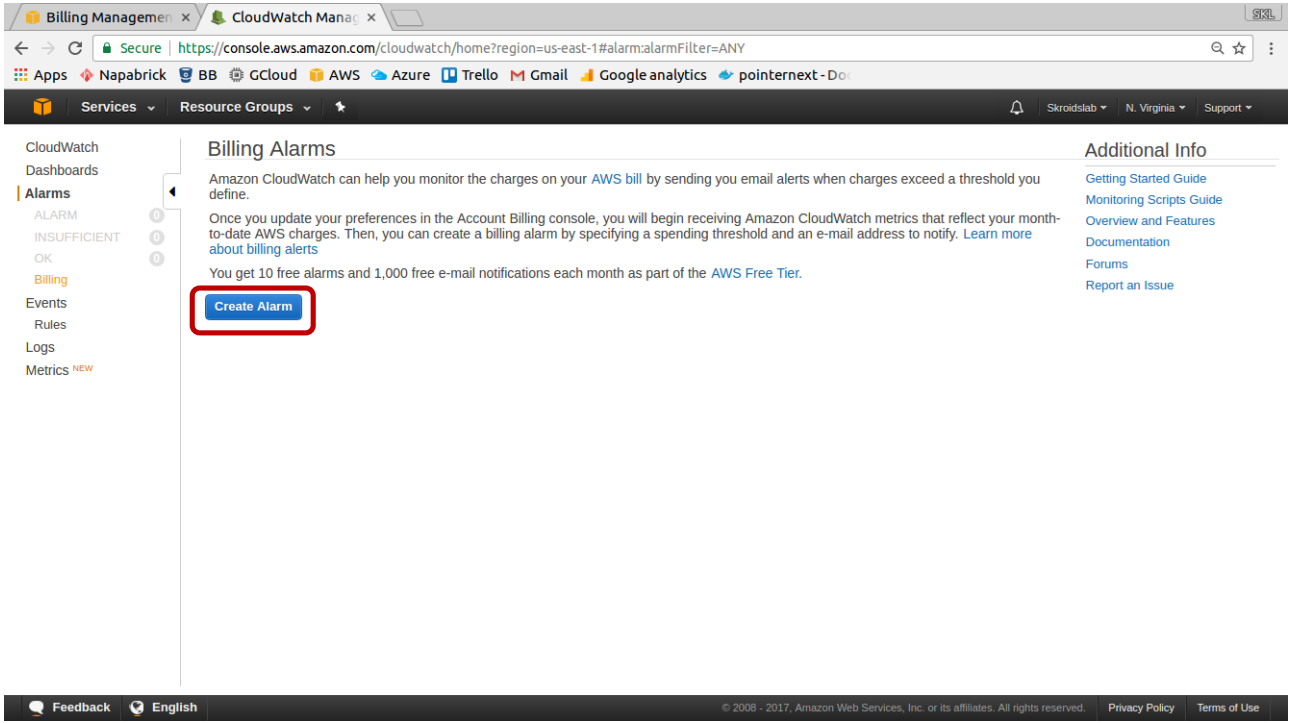
Billing - dashboard



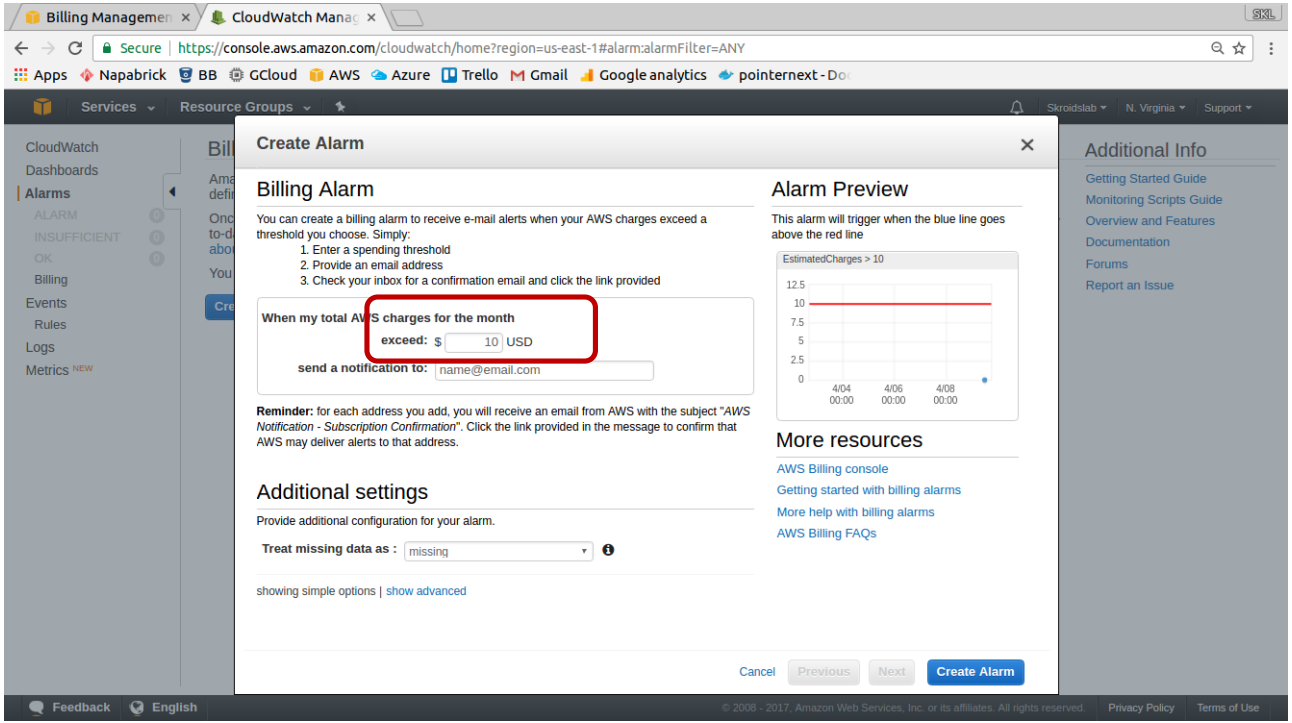
Billing - dashboard



Billing - dashboard

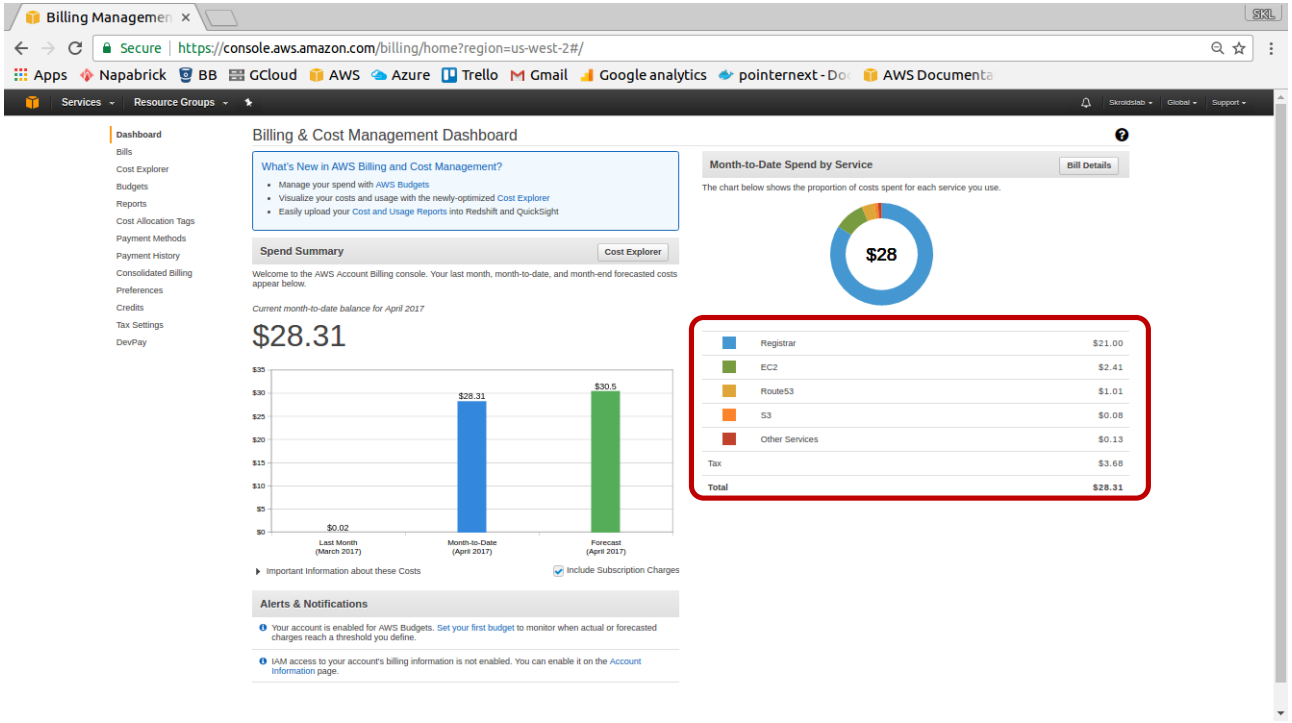


Billing - dashboard



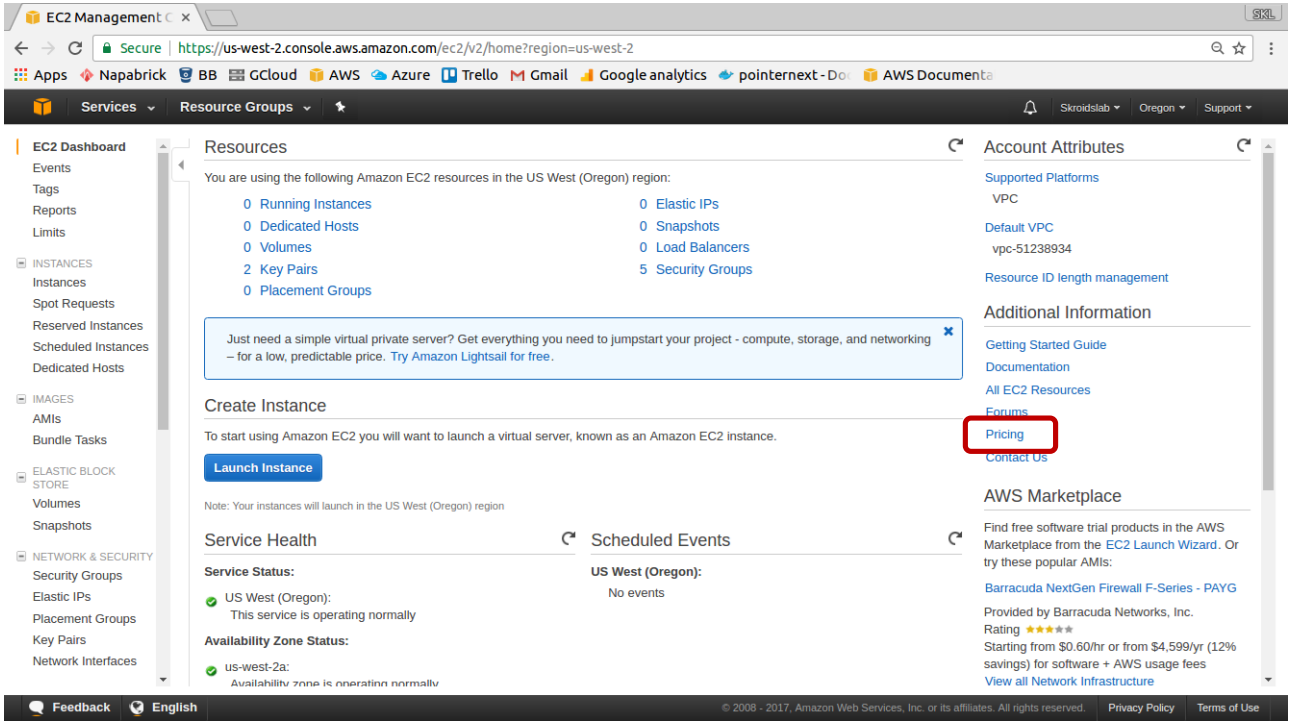
The email needs to be verified in 72hrs.

Billing - dashboard, itemized view

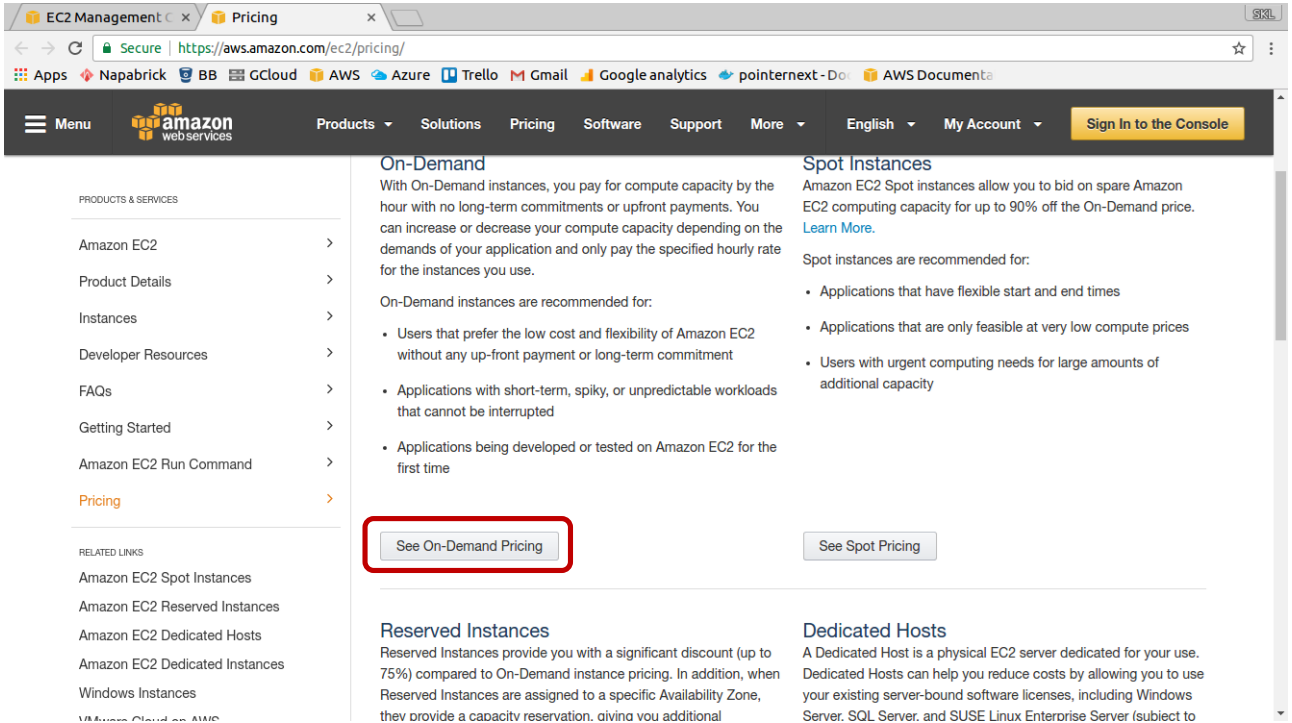


How much are we talking about?

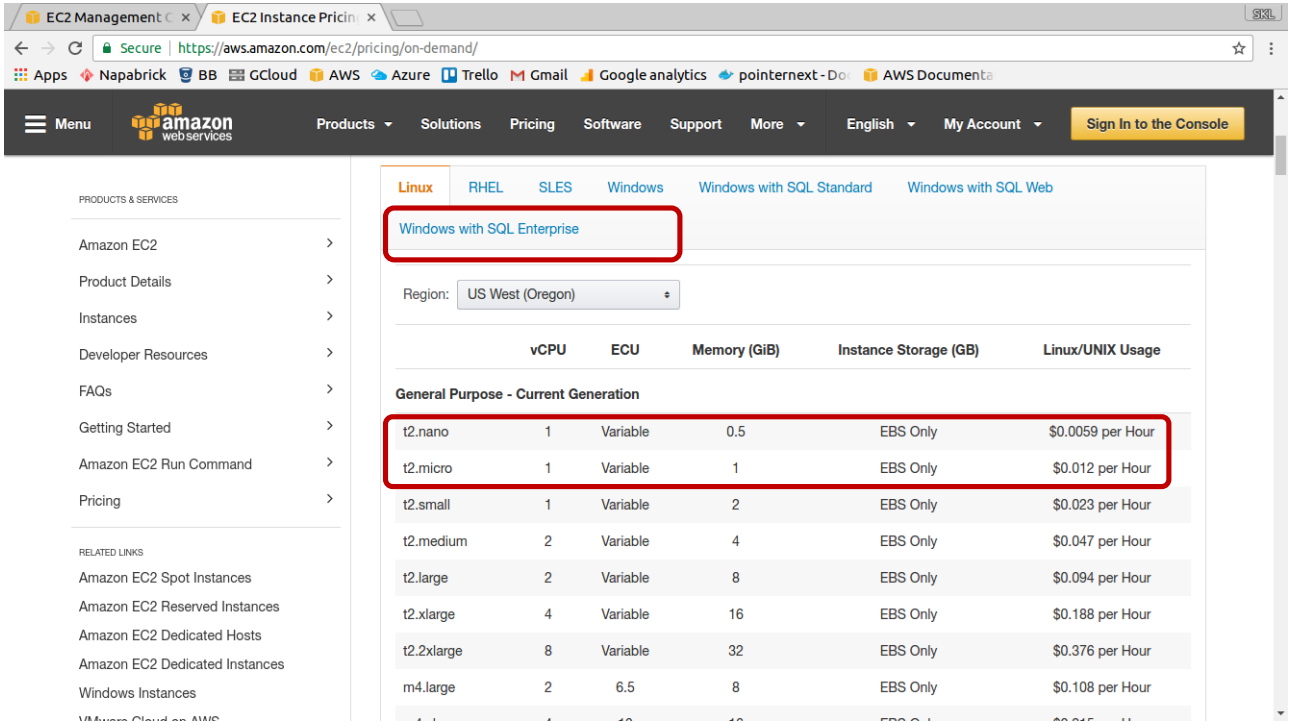
greatlearning



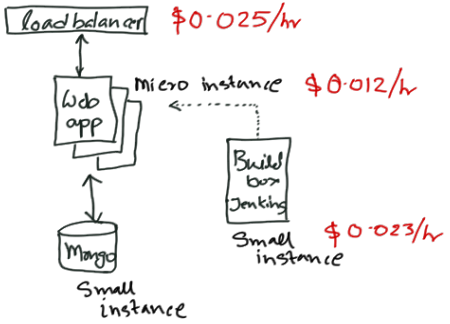
How much are we talking about?



How much are we talking about?

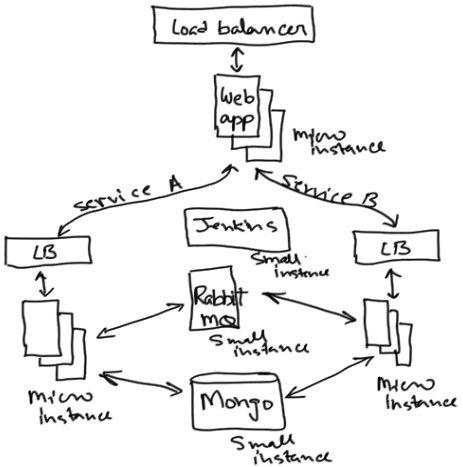


How much are we talking about?



Component	Count	Unit Cost	Price
Load balancer	1	$0.025/hr	$0.025
Micro instance	3	$0.012/hr	$0.036
Small Instance	2	$0.023/hr	$0.046

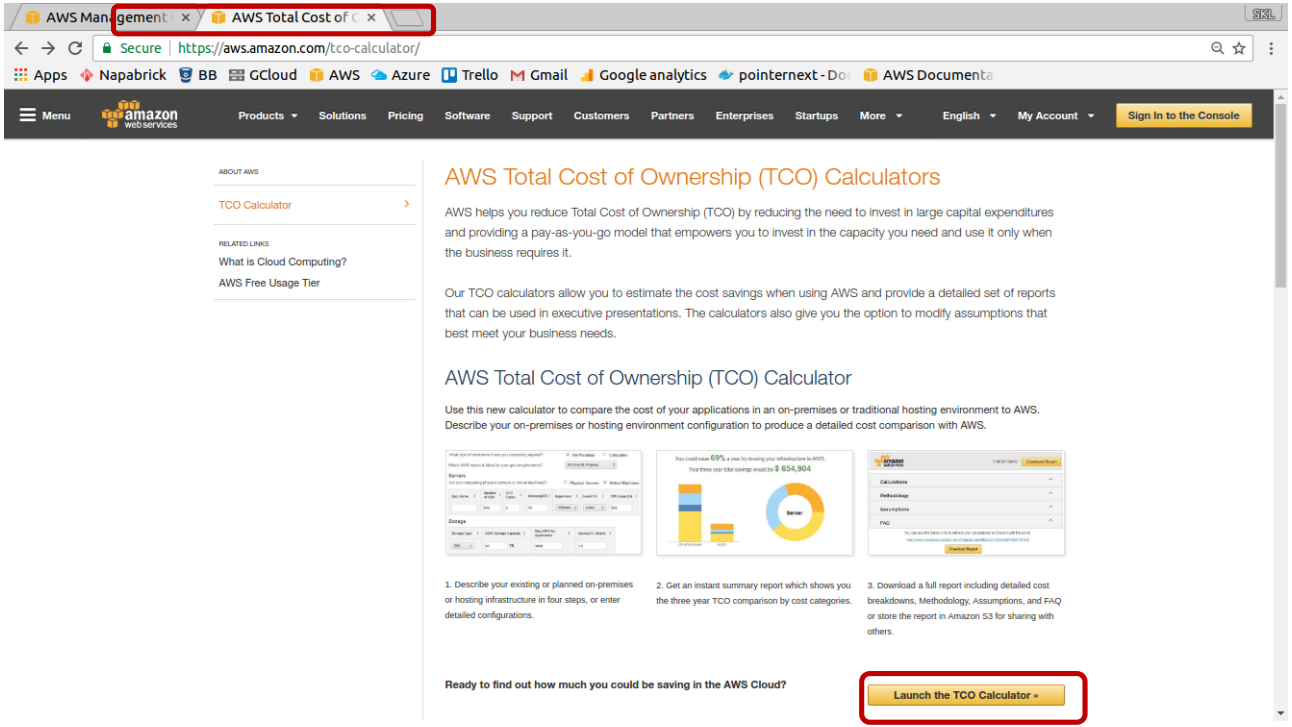
Per hour cost is ~ $0.11



Component	Count	Unit Cost	Price
Load balancer	3	$0.025/hr	$0.075
Micro instance	9	$0.012/hr	$0.108
Small Instance	3	$0.023/hr	$0.069

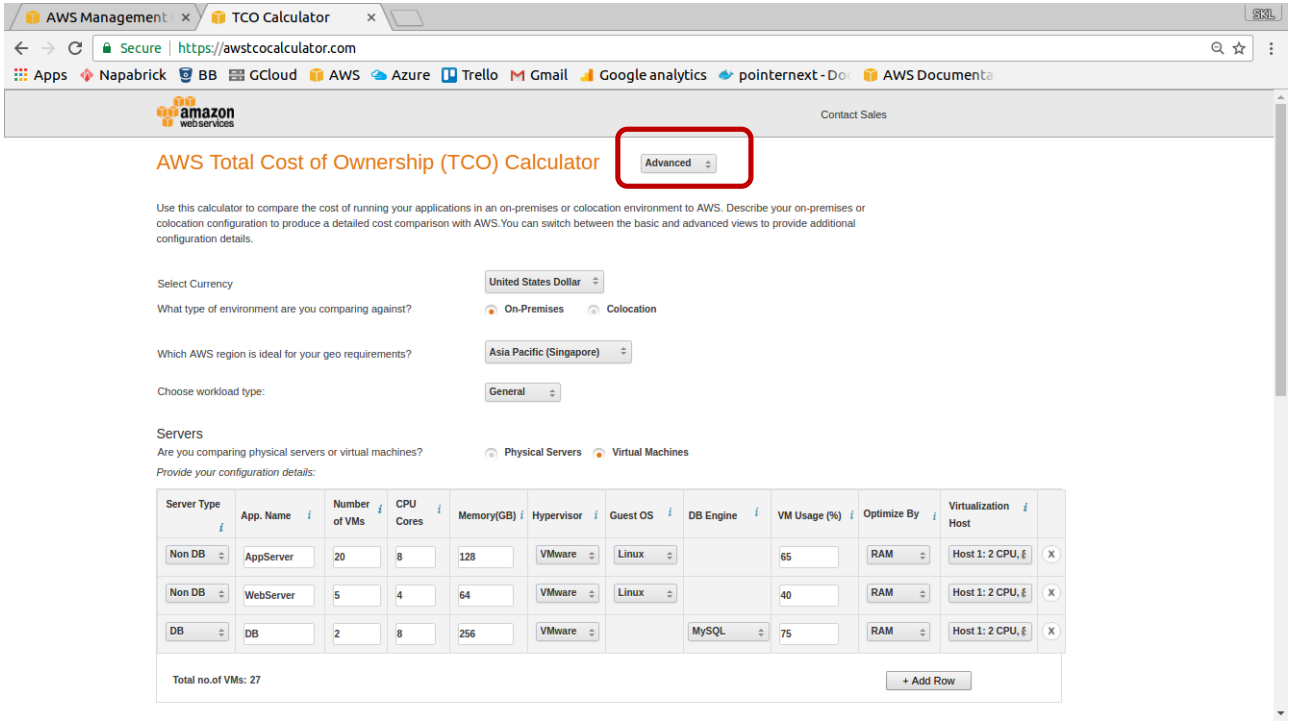
Per hour cost is ~ $0.26

Cost of Ownership

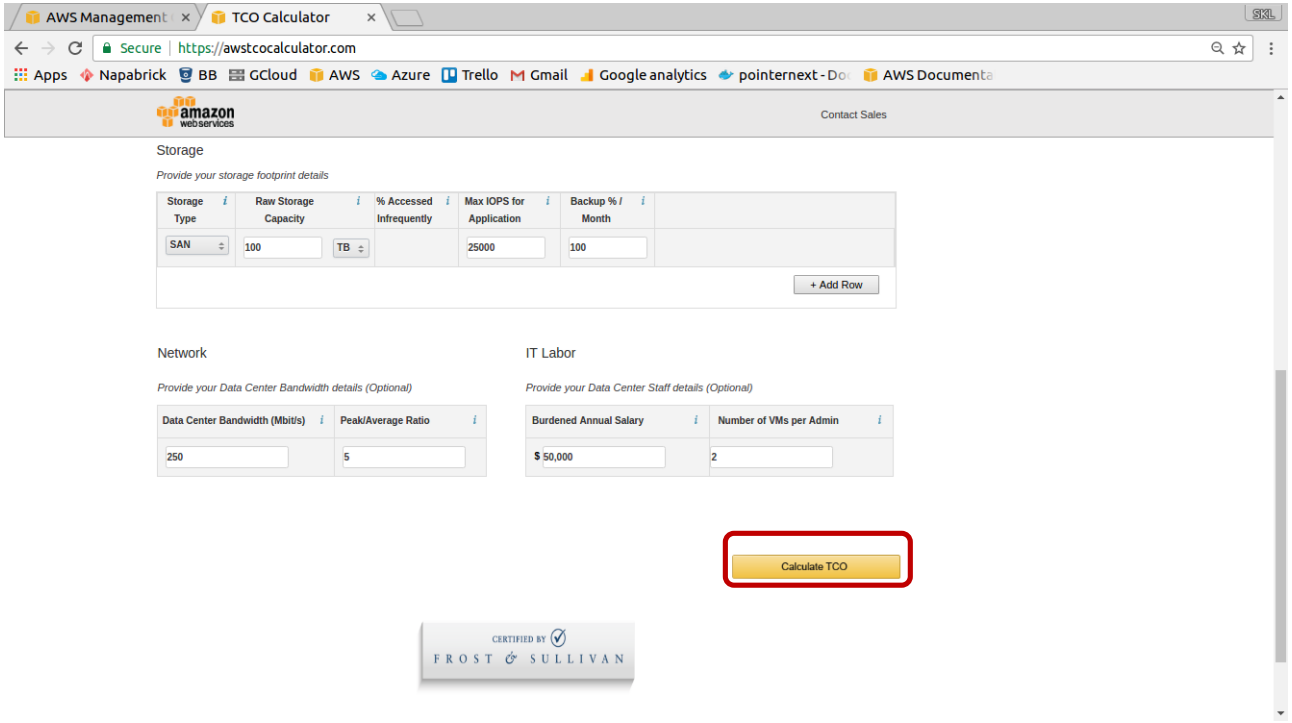


https://aws.amazon.com/tco-calculator/

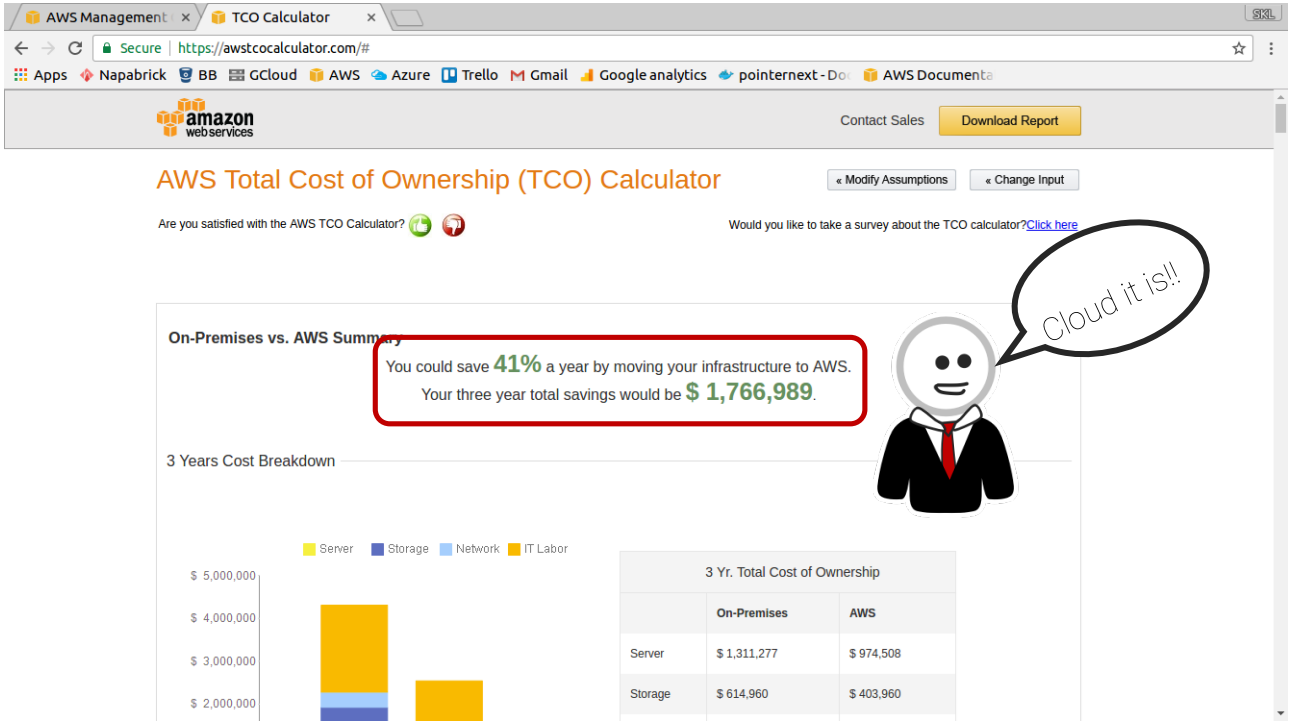
Cost of Ownership



Cost of Ownership



Cost of Ownership



greatlearning

Identity and Access Management (IAM)

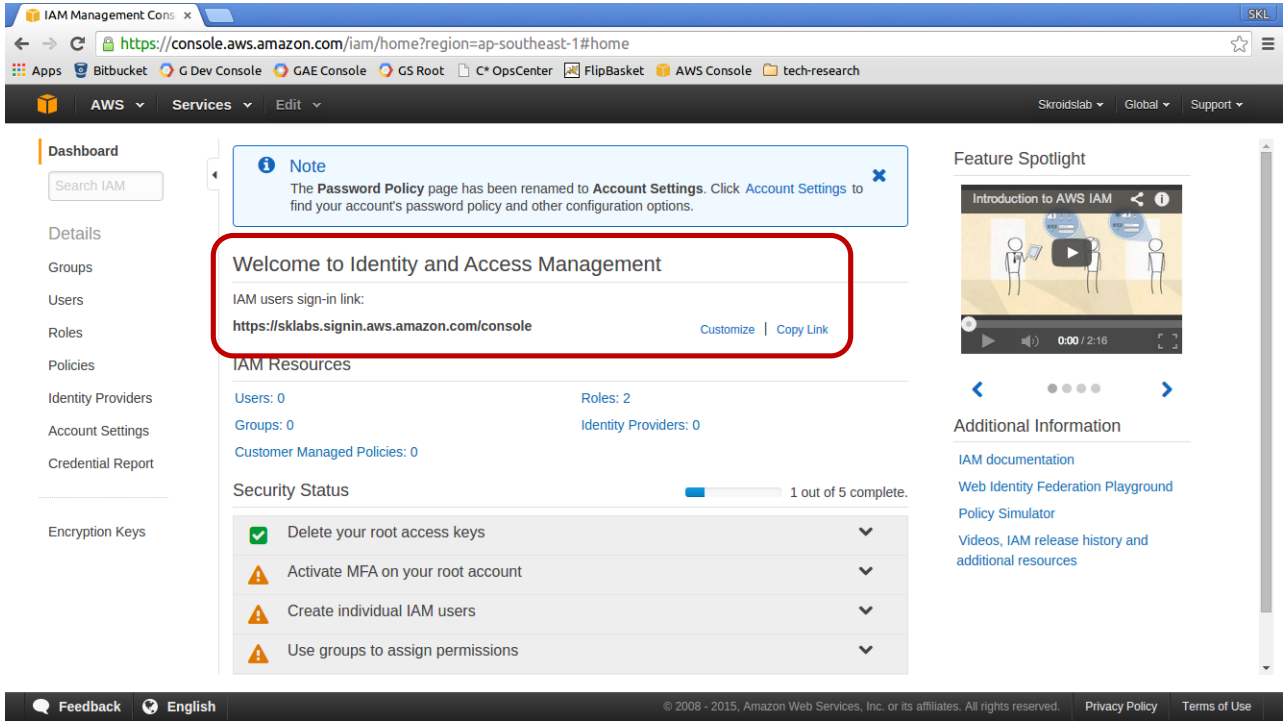
Fundamentals & Multi Factor Authentication setup

Overview - Security services

- This is an important service for maintaining AWS account
- Can integrate with existing active directory allowing SSO
- Federation includes LinkedIn or Facebook
- Fine grained access control for various resources
- Can define various roles
- Multifactor authentication (especially for the root account)
- Temporary access for users to certain areas of AWS
- Password management policies (e.g. rotation and rules)
- Core areas
    - Users - individuals
    - Groups - set of users under one set of permissions
    - Roles - access specifications (can be allocated to users, groups and resources such as EC2)
    - Policies - basically permissions assigned to a User/Group/Role

Activity - Custom AWS signin URL

greatlearning



Change the IAM sign in link, send out to your team. Notice that the IAM settings do not need a region - it will be "Global"

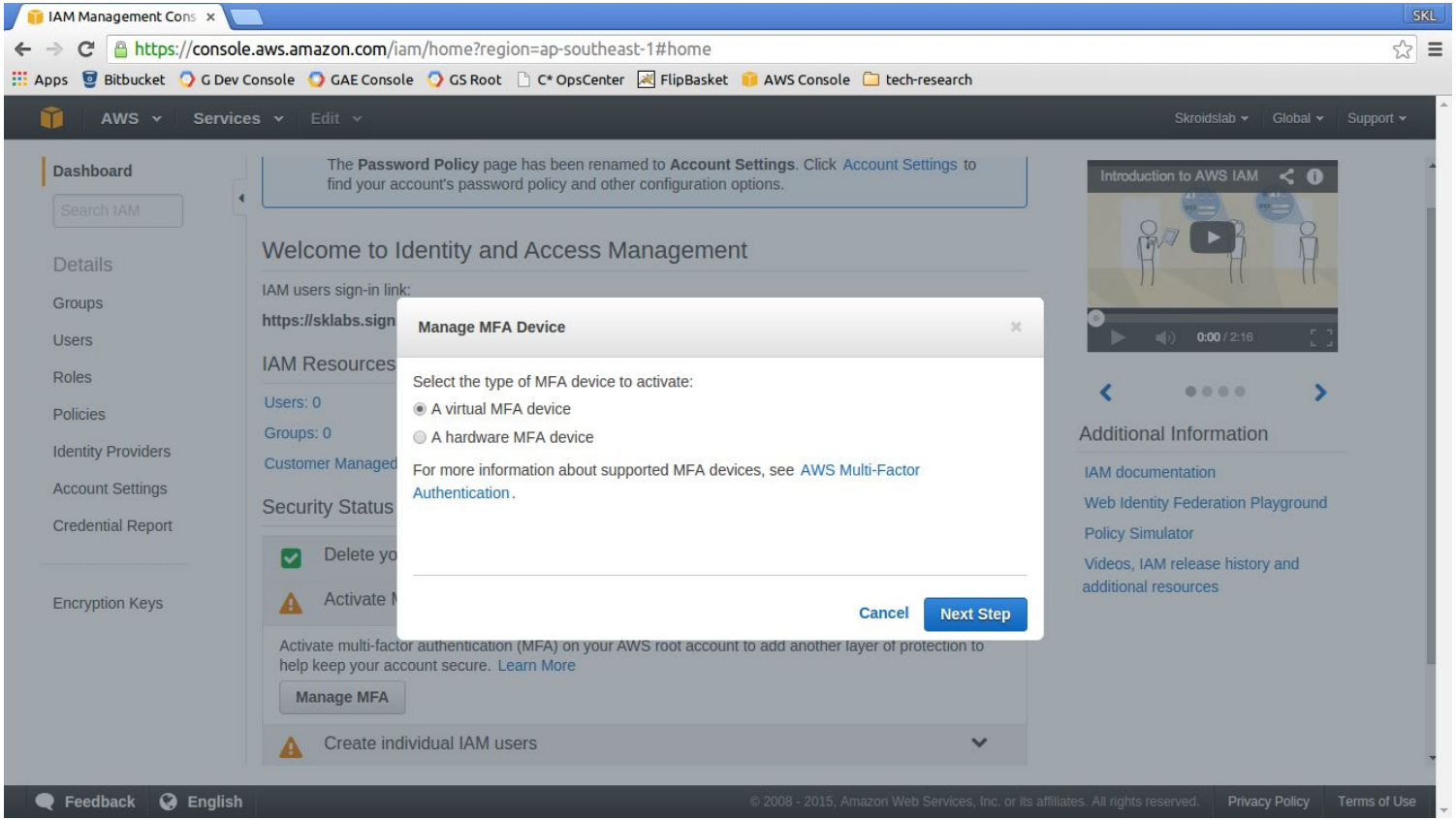
Activity - MFA setup

- Good idea to enable on the root account
  - Root a/c is the email that you used to signup in AWS
  - Can be setup on all accounts

- Install the "AWS Virtual MFA" on your mobile device, choices are
  - Google authenticator app (install this)
  - AWS Virtual MFA app - provided by "AWS Mobile LLC"

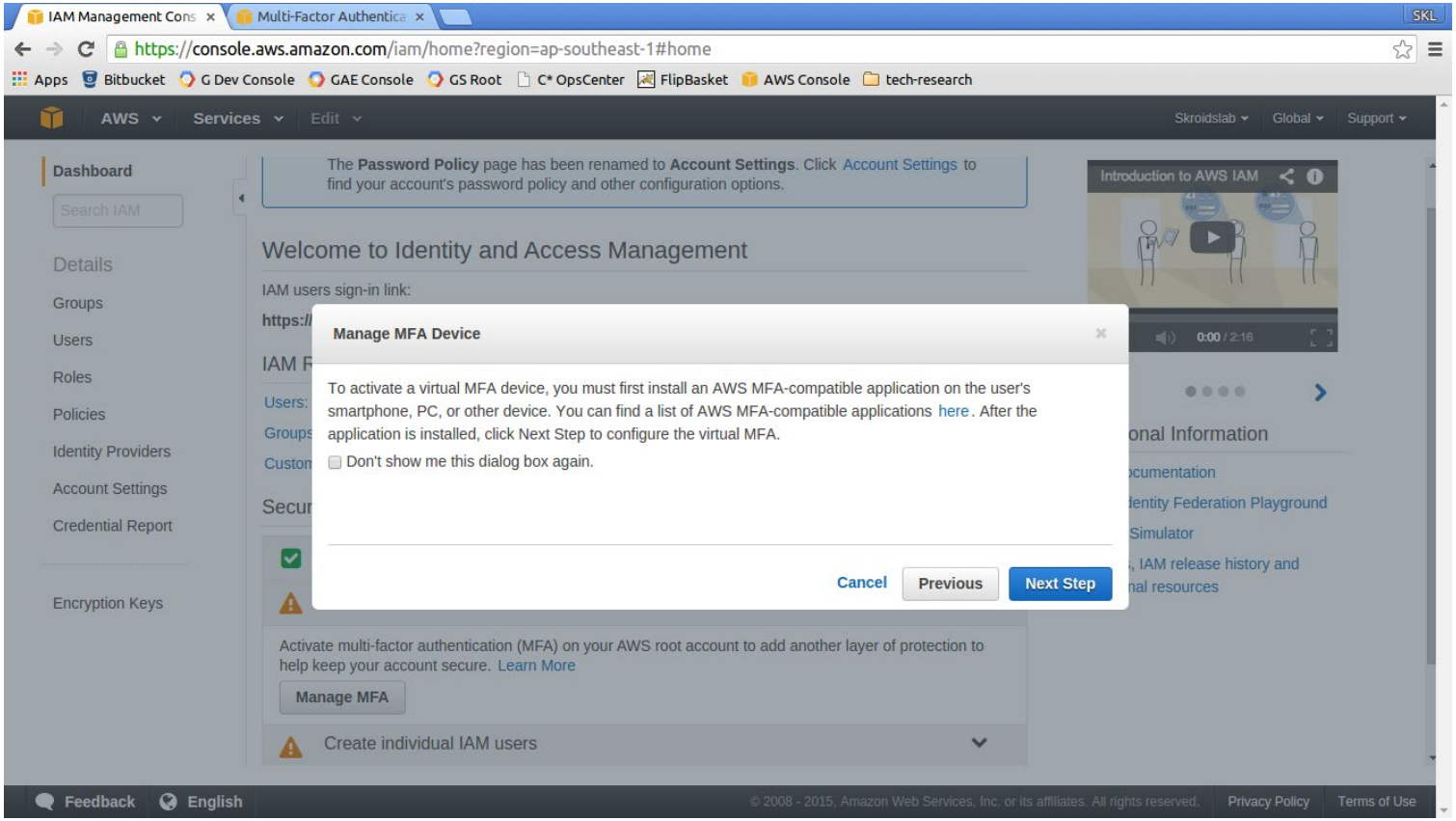
Activity - MFA setup

greatlearning

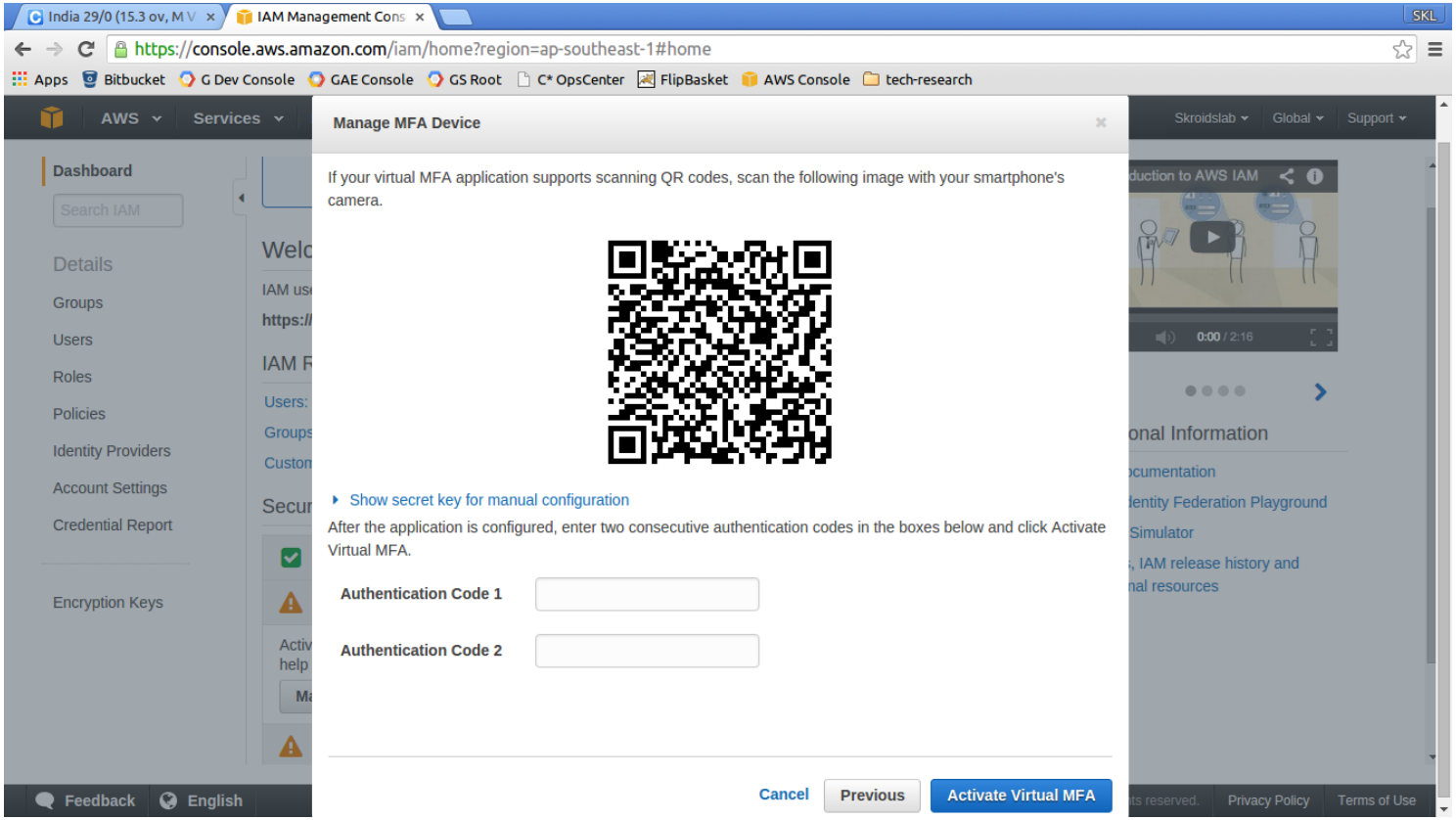


Activity - MFA setup

greatlearning



Activity - MFA setup



Activity - MFA setup

- Open "Google authenticator" in your mobile app
- Scan the QRCode as displayed on the console
- This will access the MFA
- Enter the digits in the first authentication code field, wait for it to change and add the second one
- Logout of the AWS console, log back in and now see it asks for the second authentication

greatlearning

Compute - Part I

EC2 introduction

Overview - Elastic Compute Cloud

greatlearning

- The "backbone"! AKA EC2
- Rent instances/machines/boxes/VMs (pick your choice)
  - https://aws.amazon.com/ec2/instance-types

The Amazon EC2 Service Level Agreement (SLA) commitment is 99.95% availability for each Region

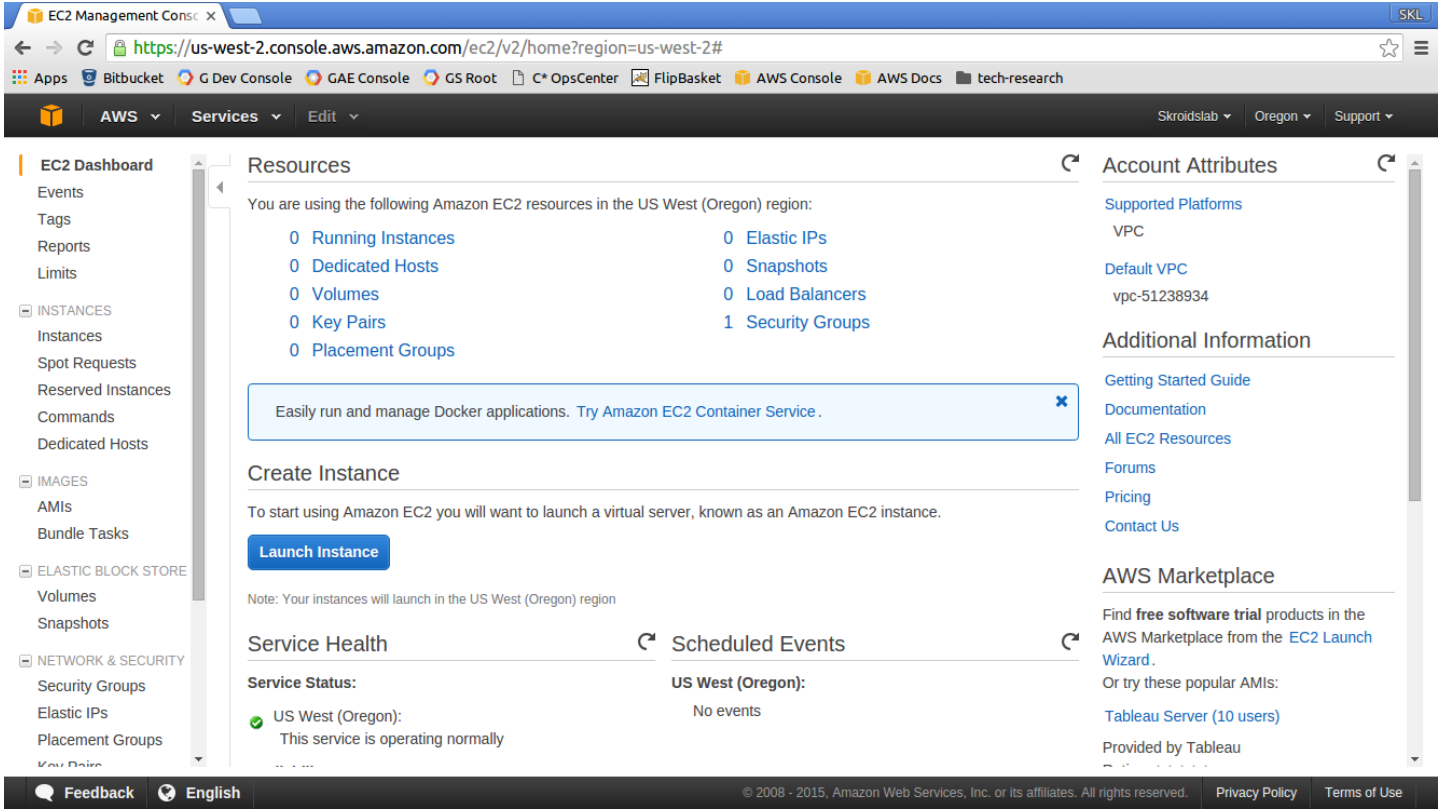
Overview - Elastic Compute Cloud

greatlearning

- Key design aspects
  - Have a few *reserved* instances (discounts are big!) + autoscale with *on-demand* instances
  - *Spot* instances for use-cases that can be interrupted unpredictably
  - Have mounted disks for app data
  - Think microservices
  - Create application feature zones (groups of microservices)
- Pricing tip about spot instance
  - If spot instance is terminated by AWS then you will not be charged for the partial hour of use
  - If you terminate the instance then the whole hour will be chargeable
- EBS which is storage, summary below
  - SSD General purpose - GP2 (upto 10k IOPS)
  - SSD Provisioned iops - IO1 (>10k IOPS)
  - HDD, Throughput optimized - ST1 (frequently accessed, e.g. sequentially updating data workloads), non bootable
  - HDD cold - SC1 - less frequently accessed, non bootable
  - HDD Magnetic - standard, really cheap, bootable
- Cannot mount EBS to multiple instances, use EFS instead
- EFS is like a shared store area

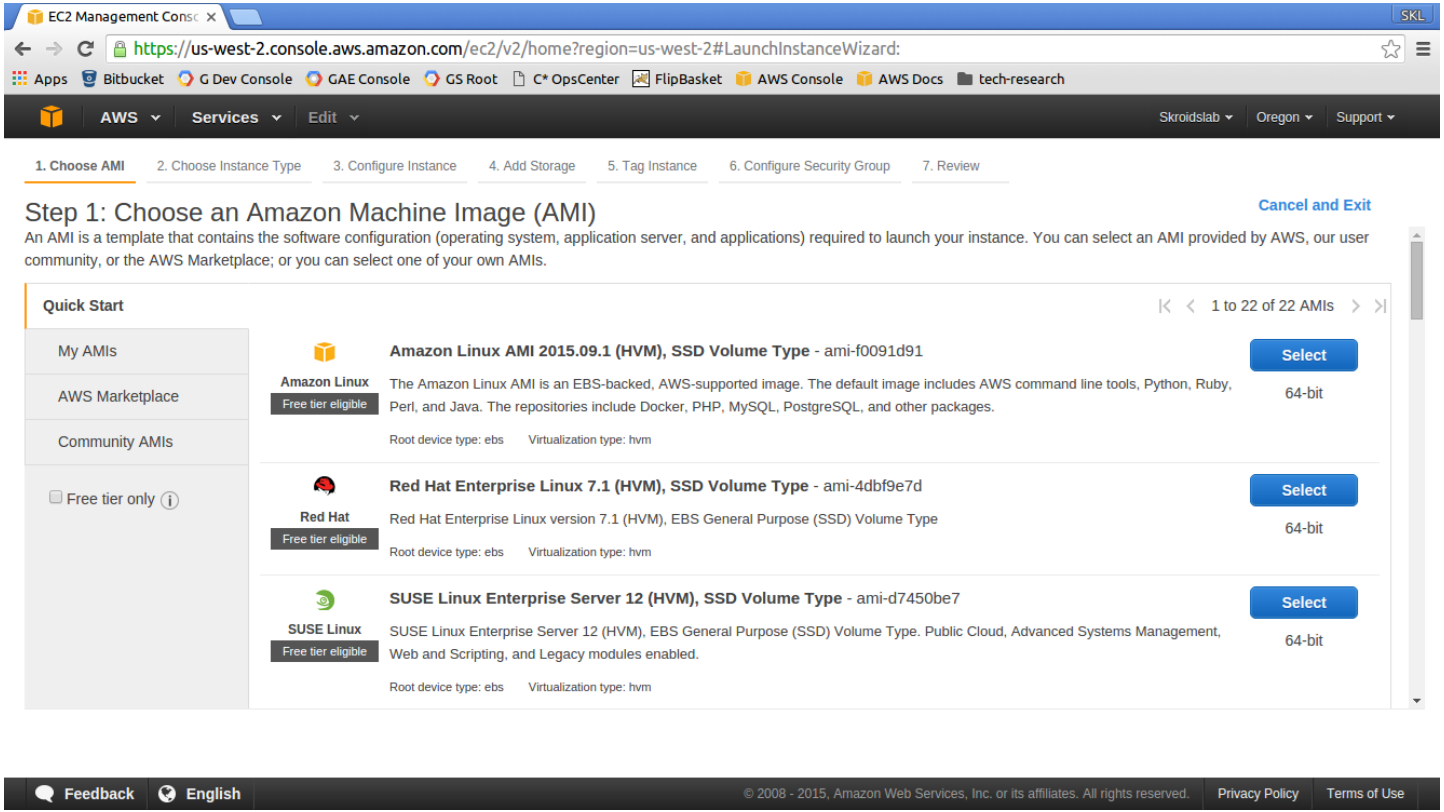
Activity - EC2 Dashboard

greatlearning



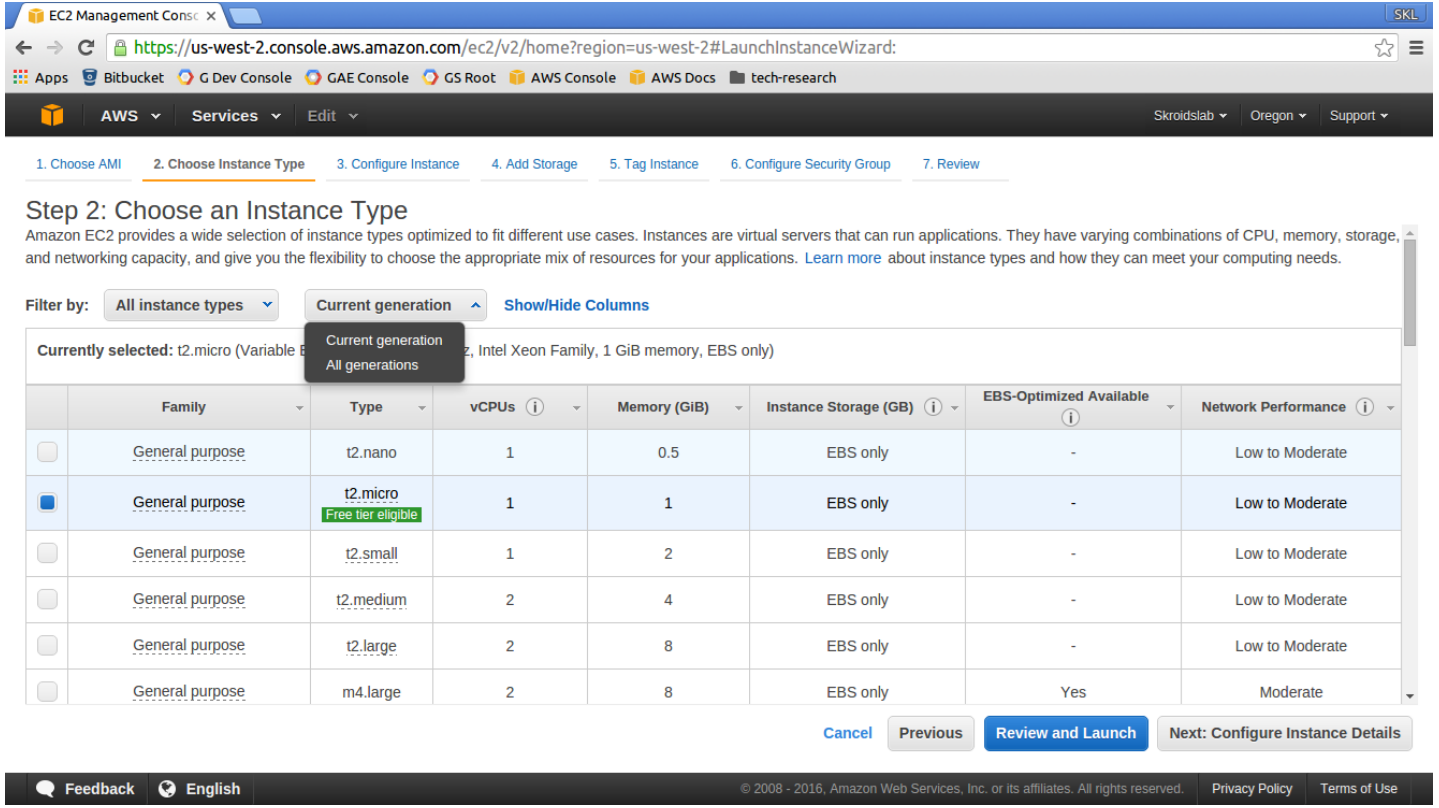
Activity - EC2 launch instance

greatlearning

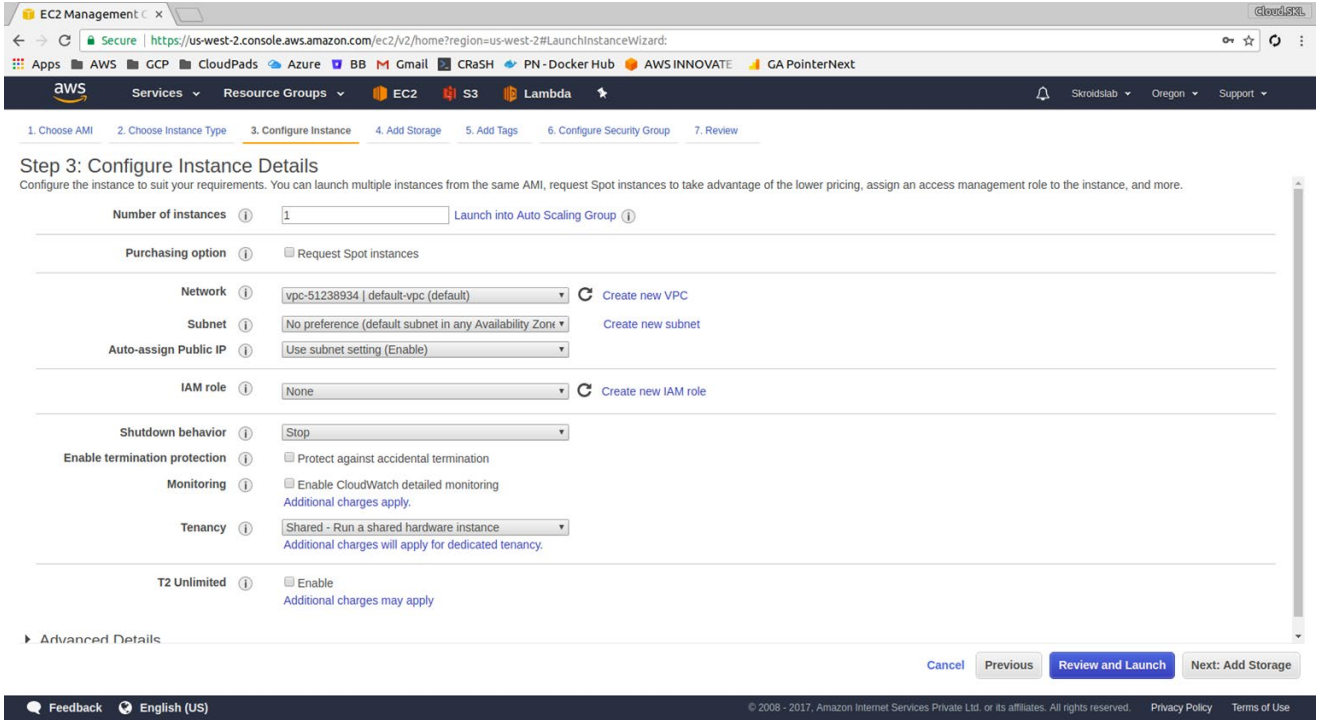


Activity - EC2 launch instance

greatlearning

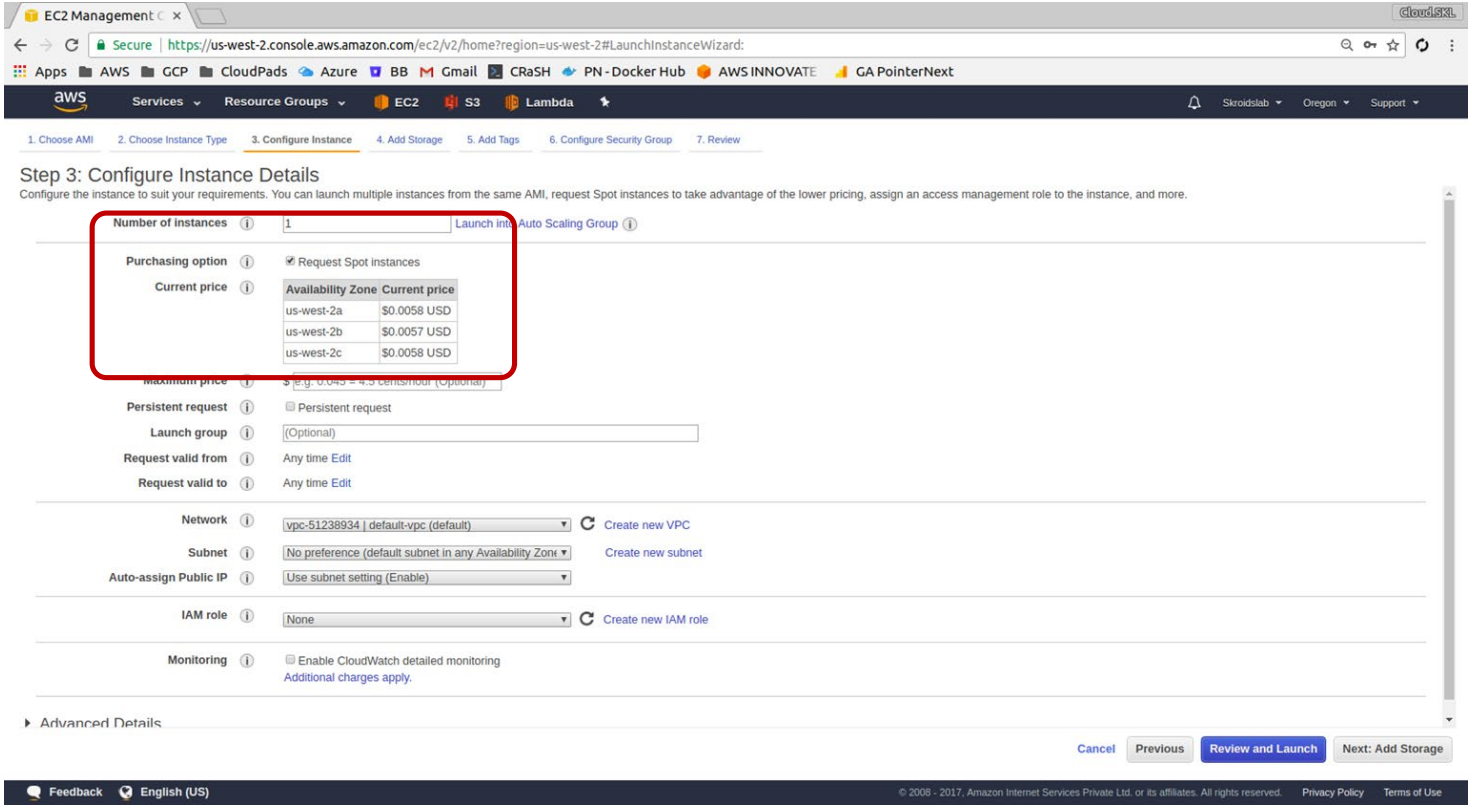


Activity - EC2 launch instance

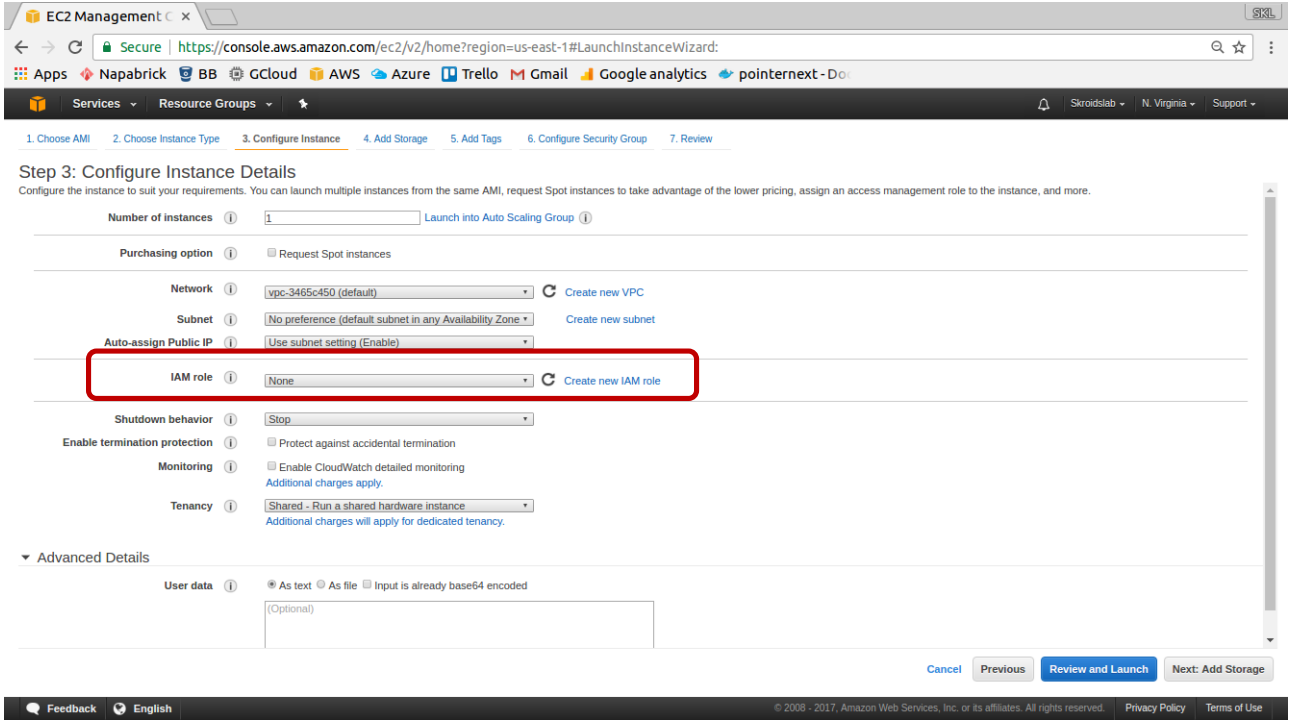


https://aws.amazon.com/blogs/aws/new-t2-unlimited-going-beyond-the-burst-with-high-performance/

Activity - EC2 launch instance



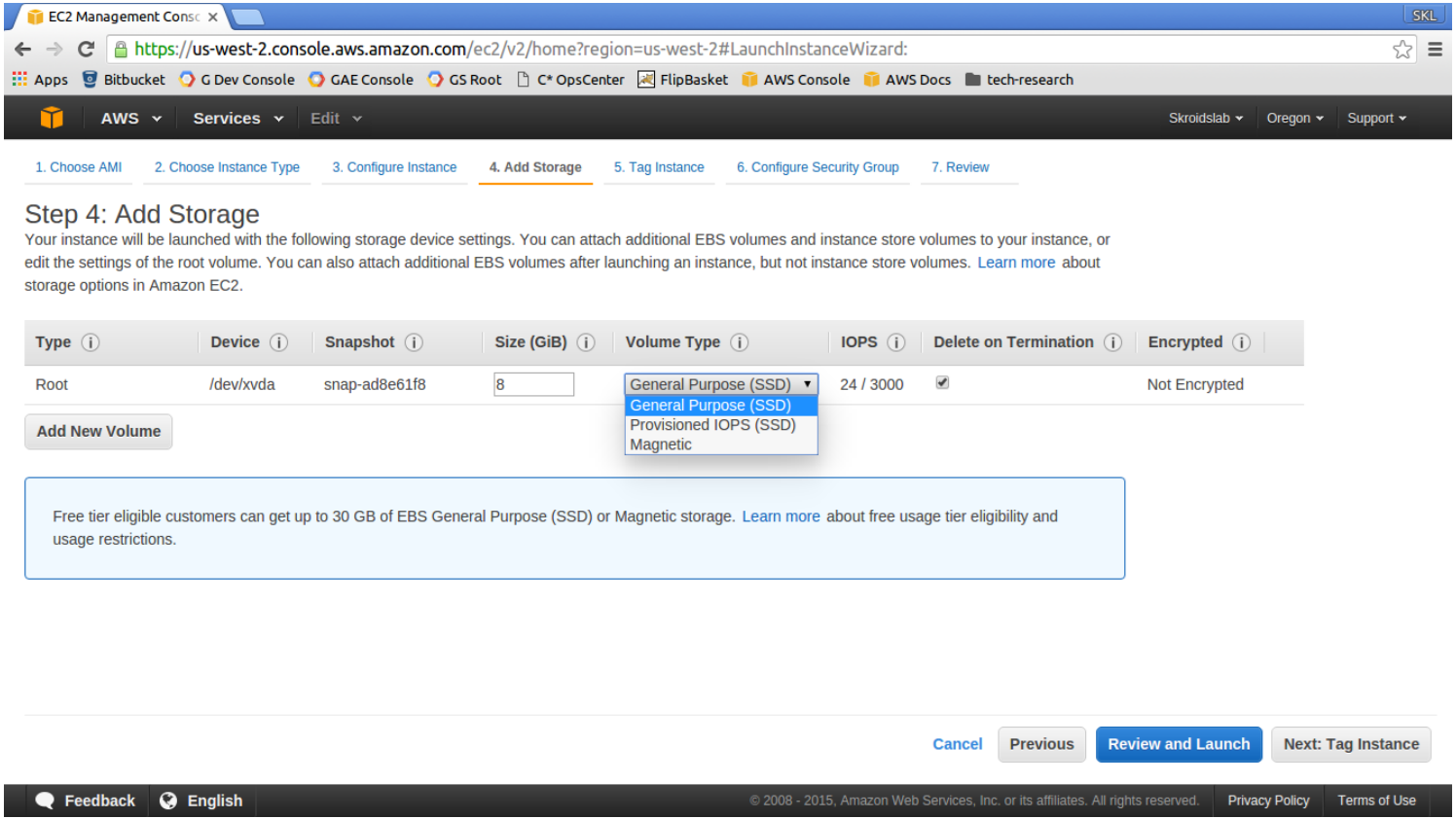
Activity - EC2 launch instance



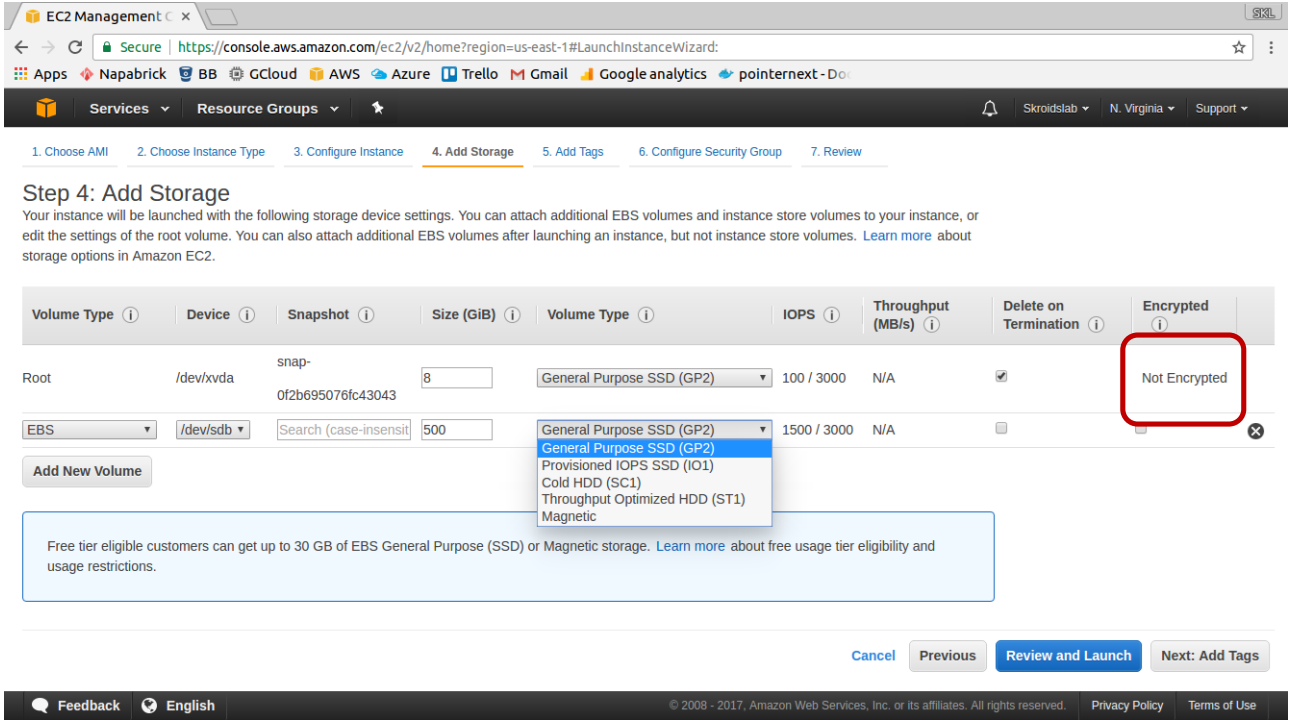
Important! What happens if you miss adding a role?

Activity - EC2 launch instance

greatlearning



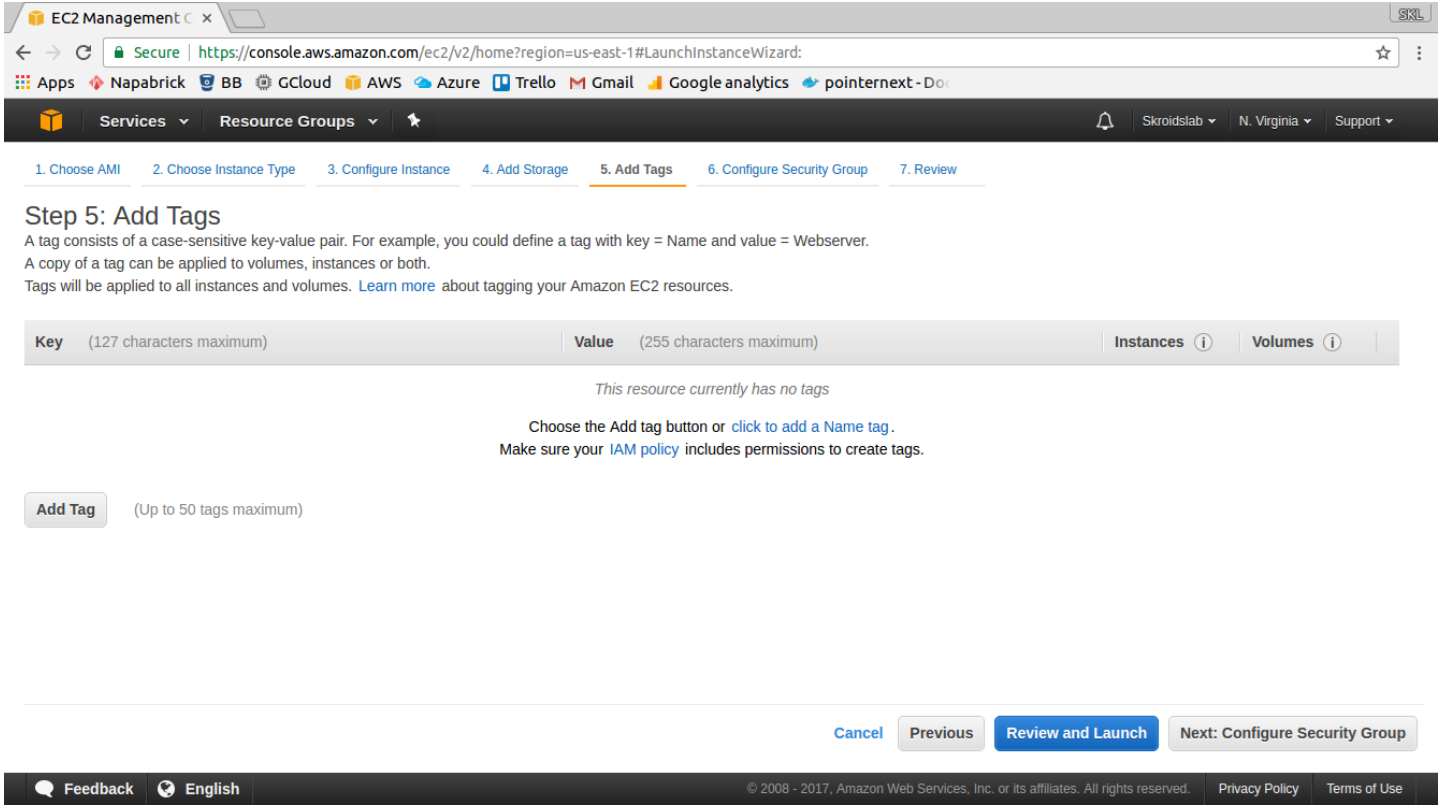
Activity - EC2 launch instance



Cannot encrypt the boot volume BUT any additional EBS you can.
Or create your own AMI and encrypt Or use 3rd party service

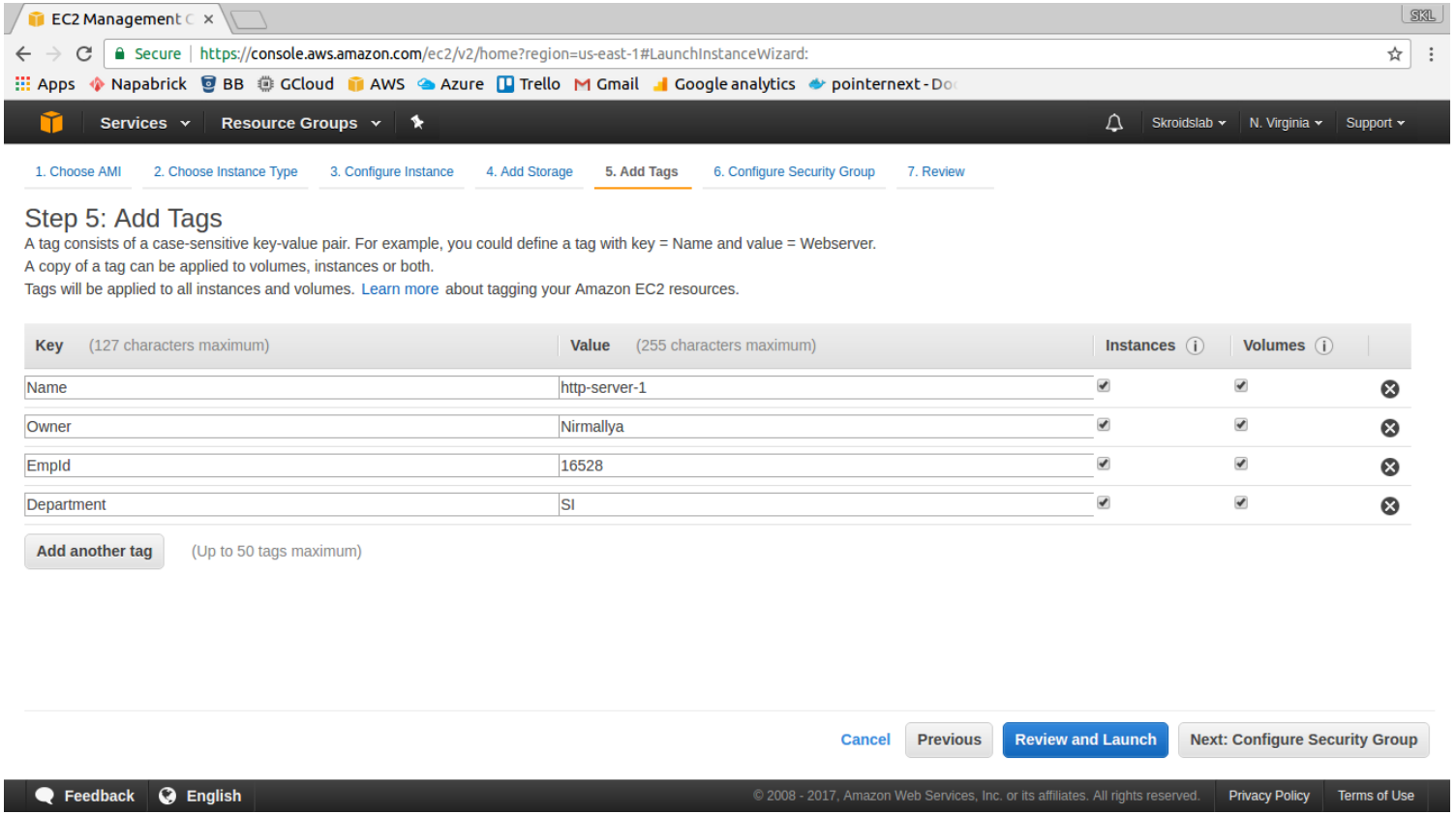
Activity - EC2 launch instance

greatlearning



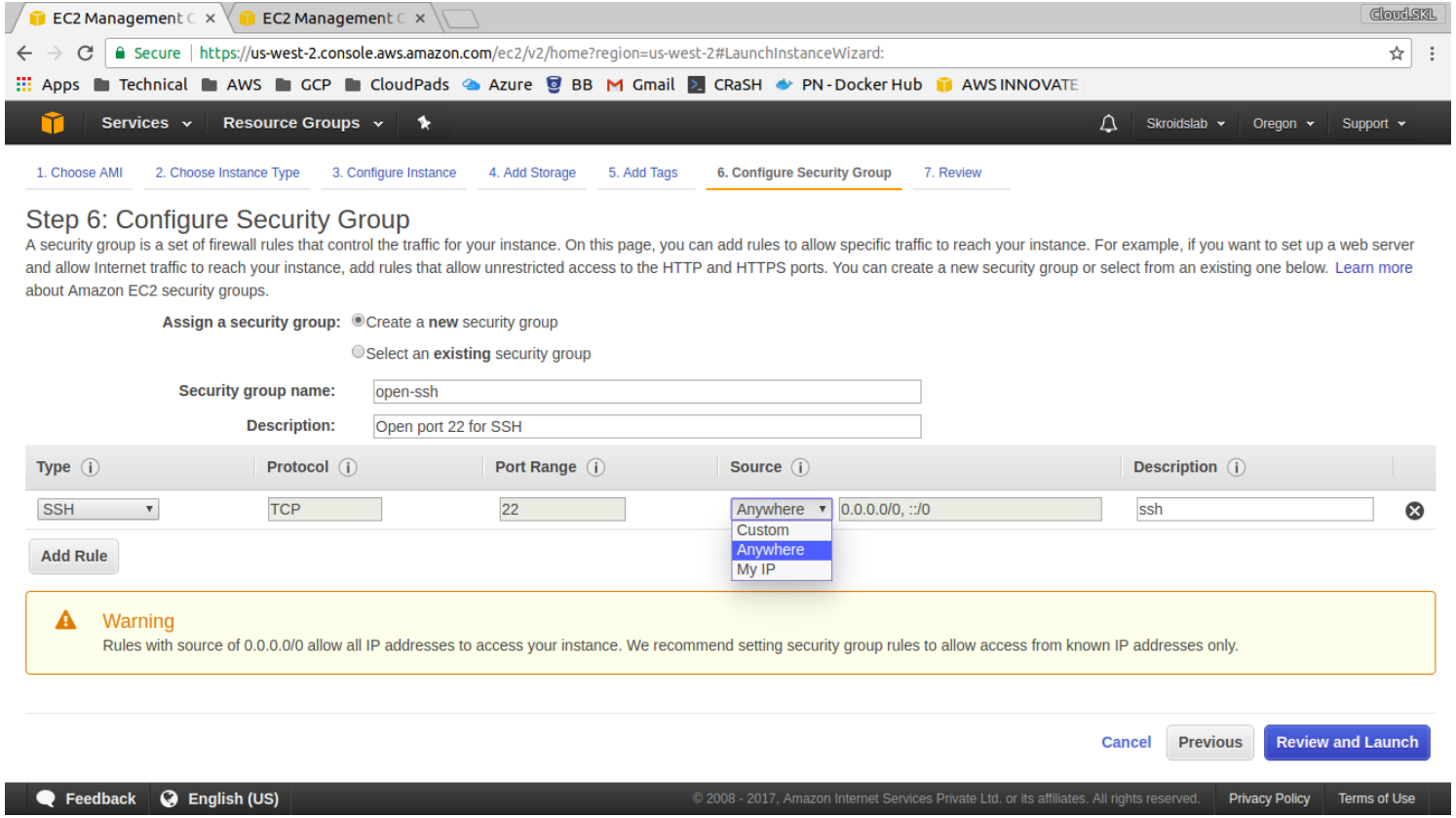
Activity - EC2 launch instance

greatlearning



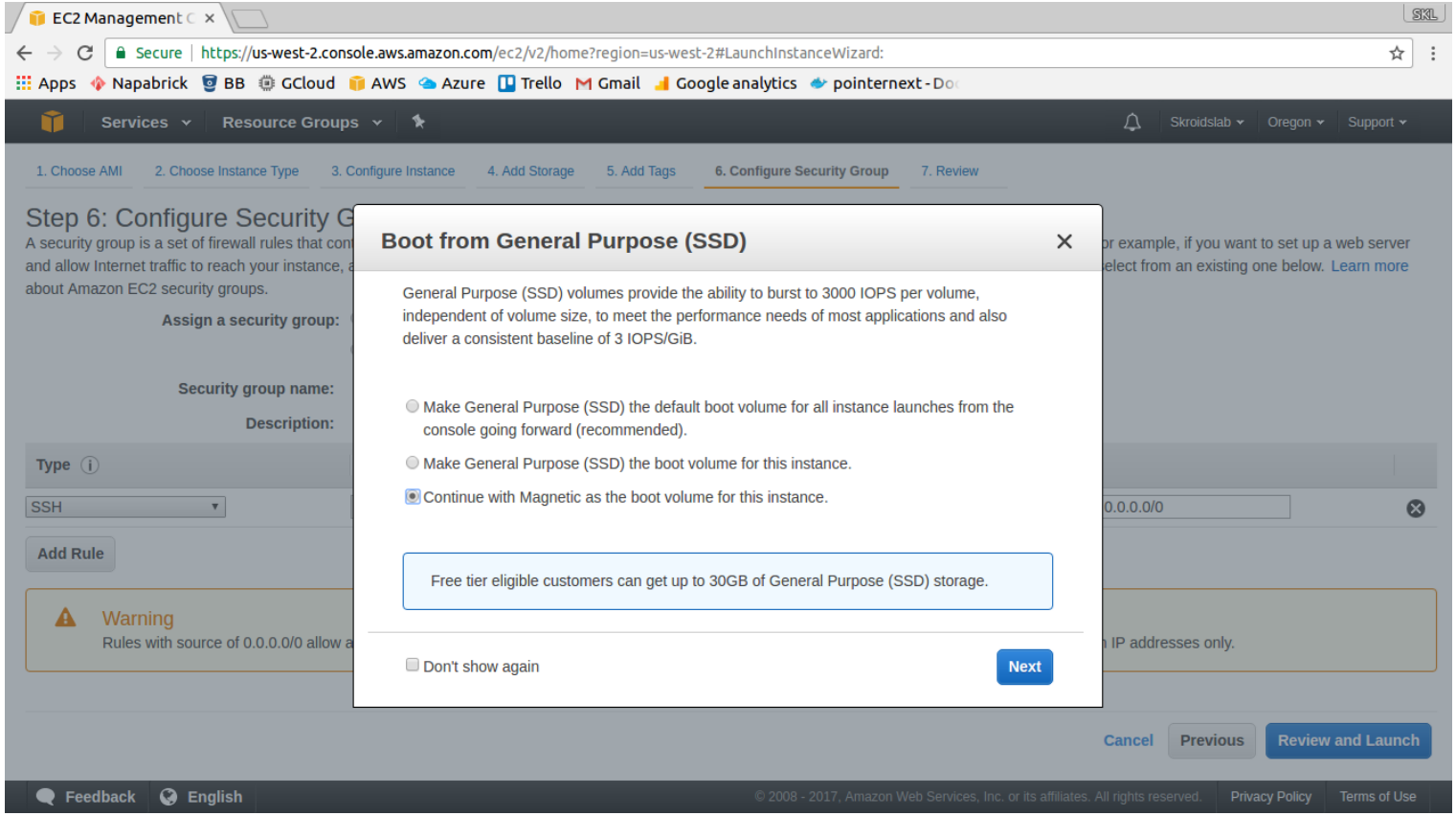
Activity - EC2 launch instance

greatlearning

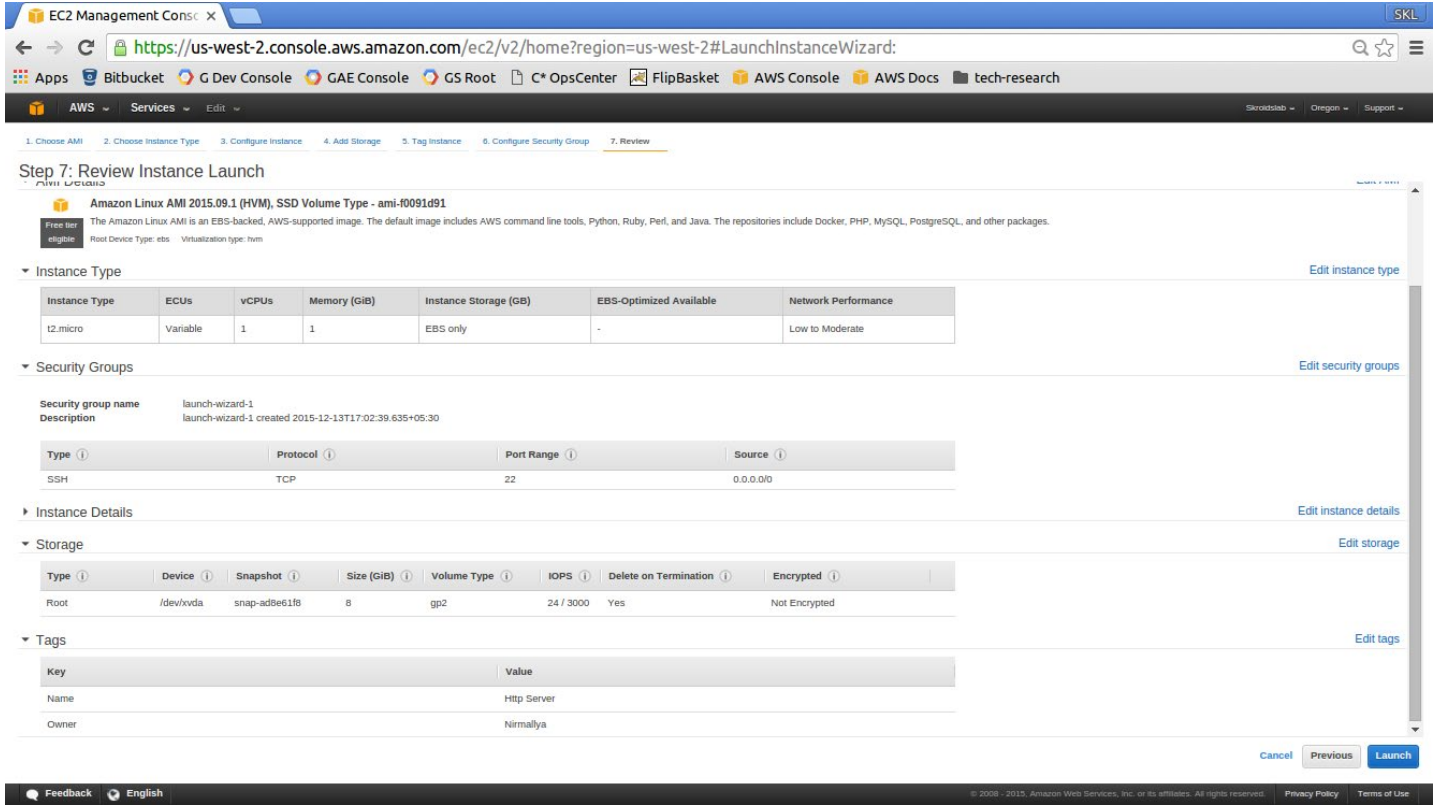


Activity - EC2 launch instance

greatlearning

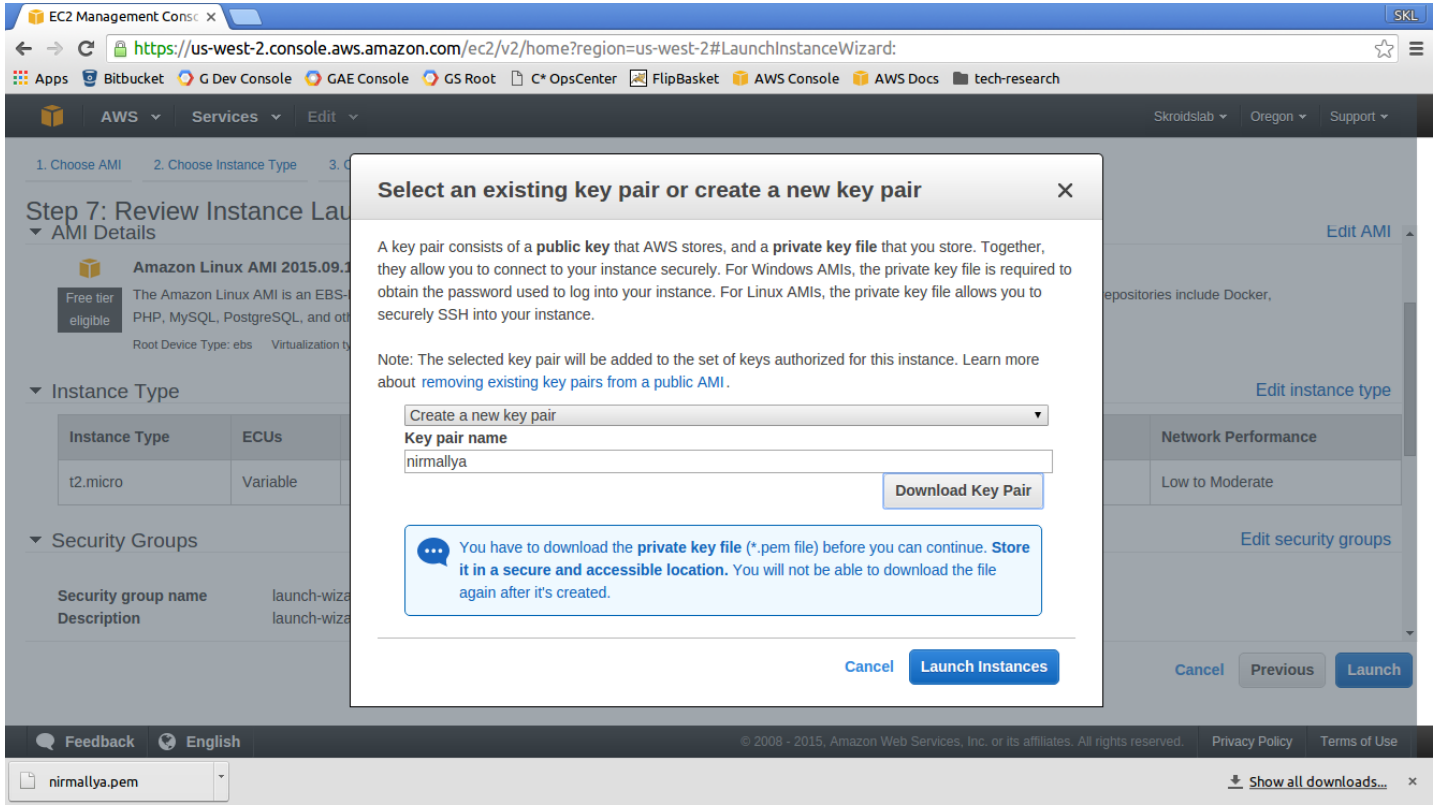


Activity - EC2 launch instance



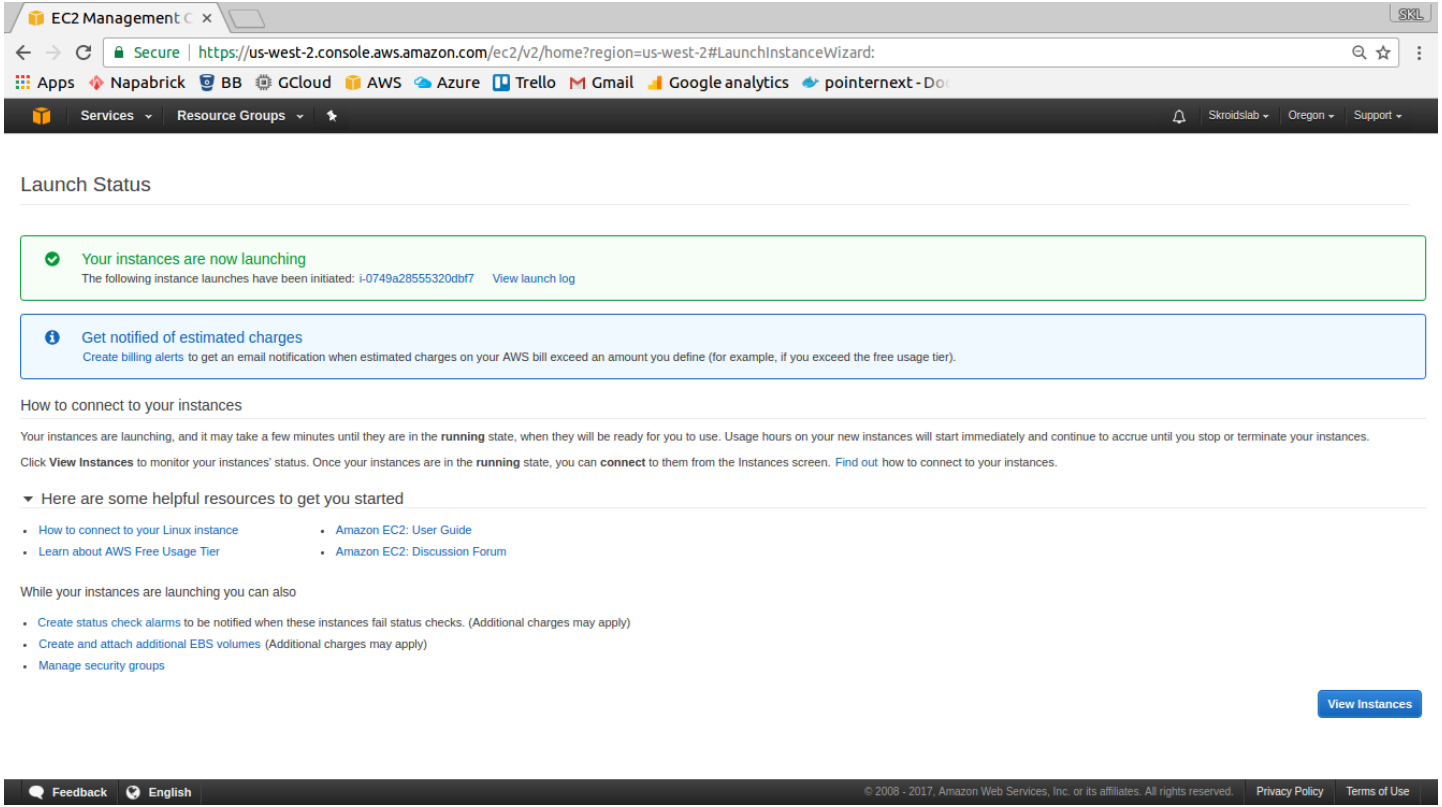
Activity - EC2 launch instance

greatlearning

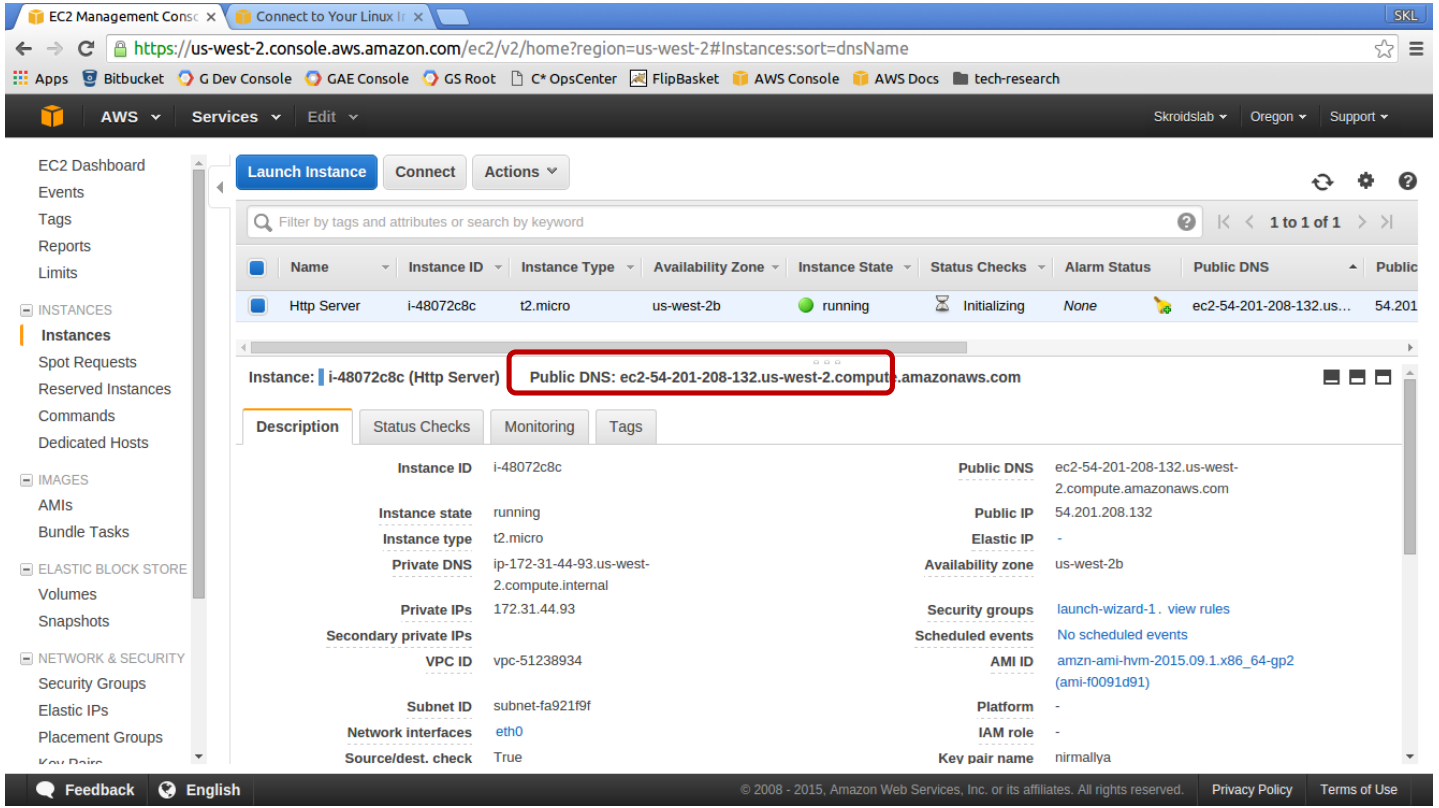


Activity - EC2 launch instance

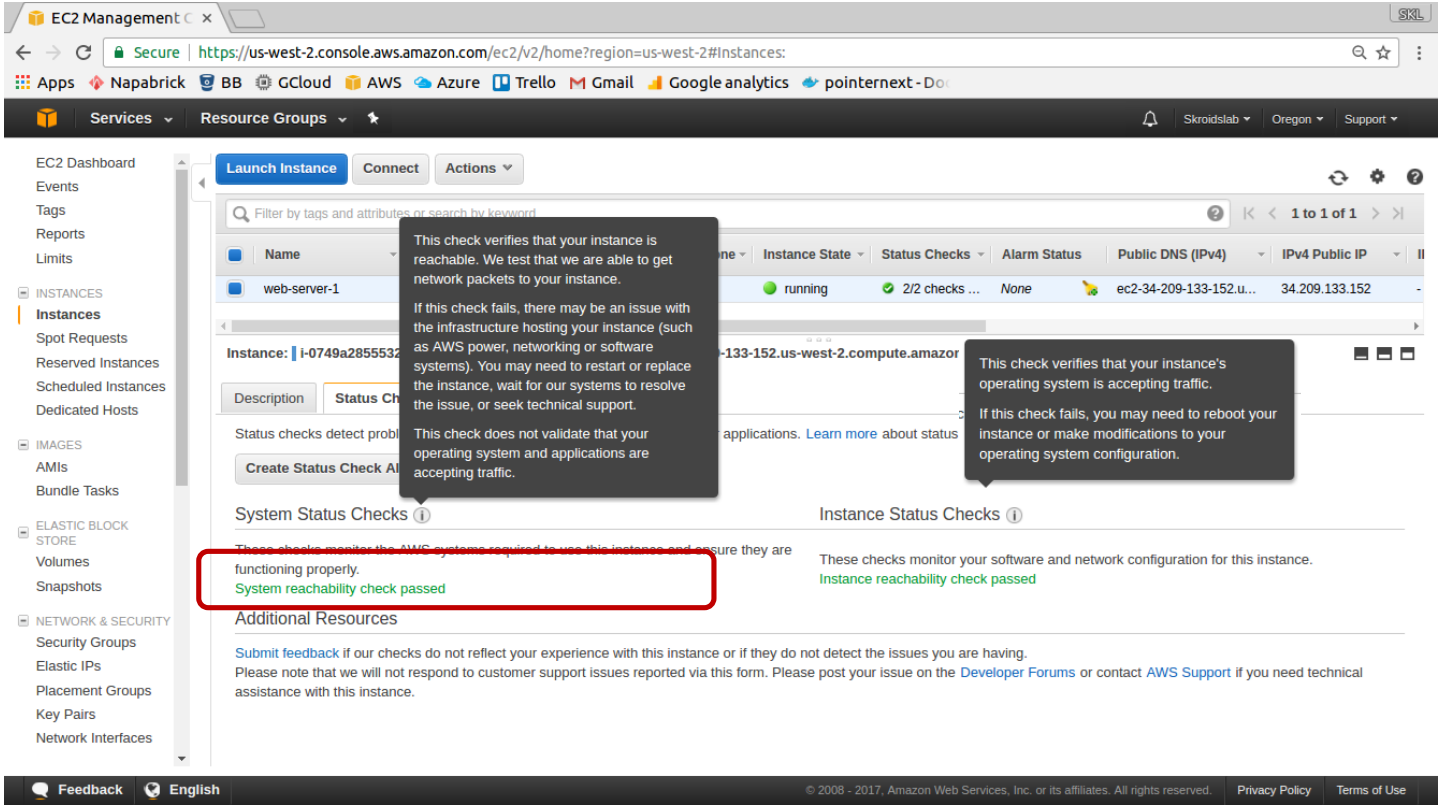
greatlearning



Activity - EC2 launch instance



Activity - EC2 launch instance



Activity - EC2 launch instance

greatlearning

- When you launch an instance in EC2-Classic, we automatically assign a public IP address to the instance. You cannot modify this behavior. When you launch an instance into a VPC, your subnet has an attribute that determines whether instances launched into that subnet receive a public IP address.
- By default, we *don't automatically assign a public IP address* to an instance that you launch in a *non default subnet*.
- You can control whether your instance in a VPC receives a public IP address by doing the following:
    - Modifying the public IP addressing attribute of your subnet. For more information, see Modifying Your Subnet's Public IP Addressing Behavior in the Amazon VPC User Guide.
    - Enabling or disabling the public IP addressing feature during launch, which overrides the subnet's public IP addressing attribute. For more information, see Assigning a Public IP Address.

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html

Activity - EC2 install http server

greatlearning

- Connect to AWS using PUTTY [http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html]
- Protect your PEM file
  - chmod 400 <PEM>
- To login to the instance you can use public DNS or IP
  - ssh -i <PEM> ec2-user@<Public DNS>

  OR
  - ssh <Public IP> -l ec2-user -i <PEM>
- Once you are in, fire up the following commands
  - sudo yum update
  - sudo yum install httpd
  - sudo service httpd start
  - curl localhost
- Go to the browser and access the site using the public IP address
- Are you able to see the default page?

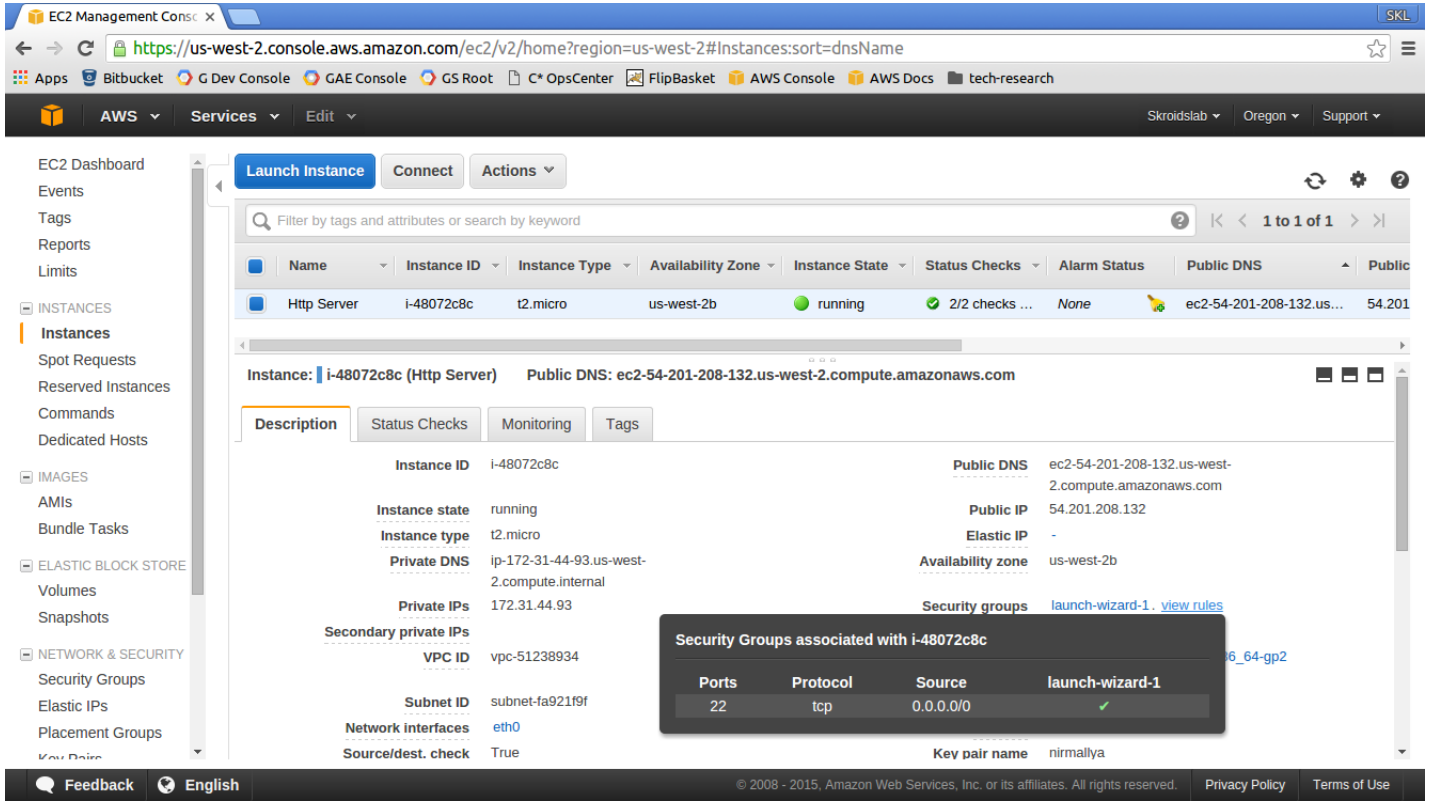
greatlearning

Compute - Part I

Security groups

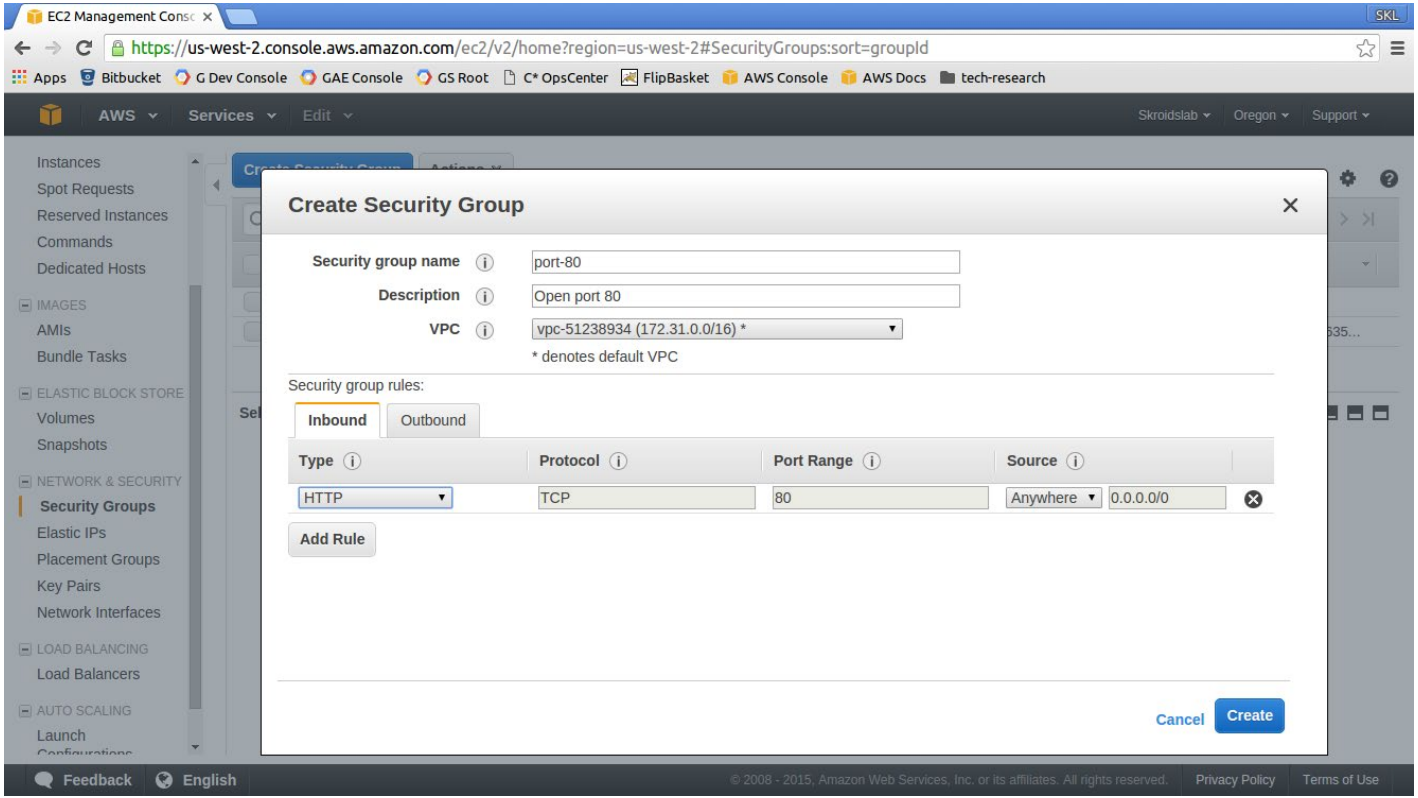
Activity - Security group

greatlearning



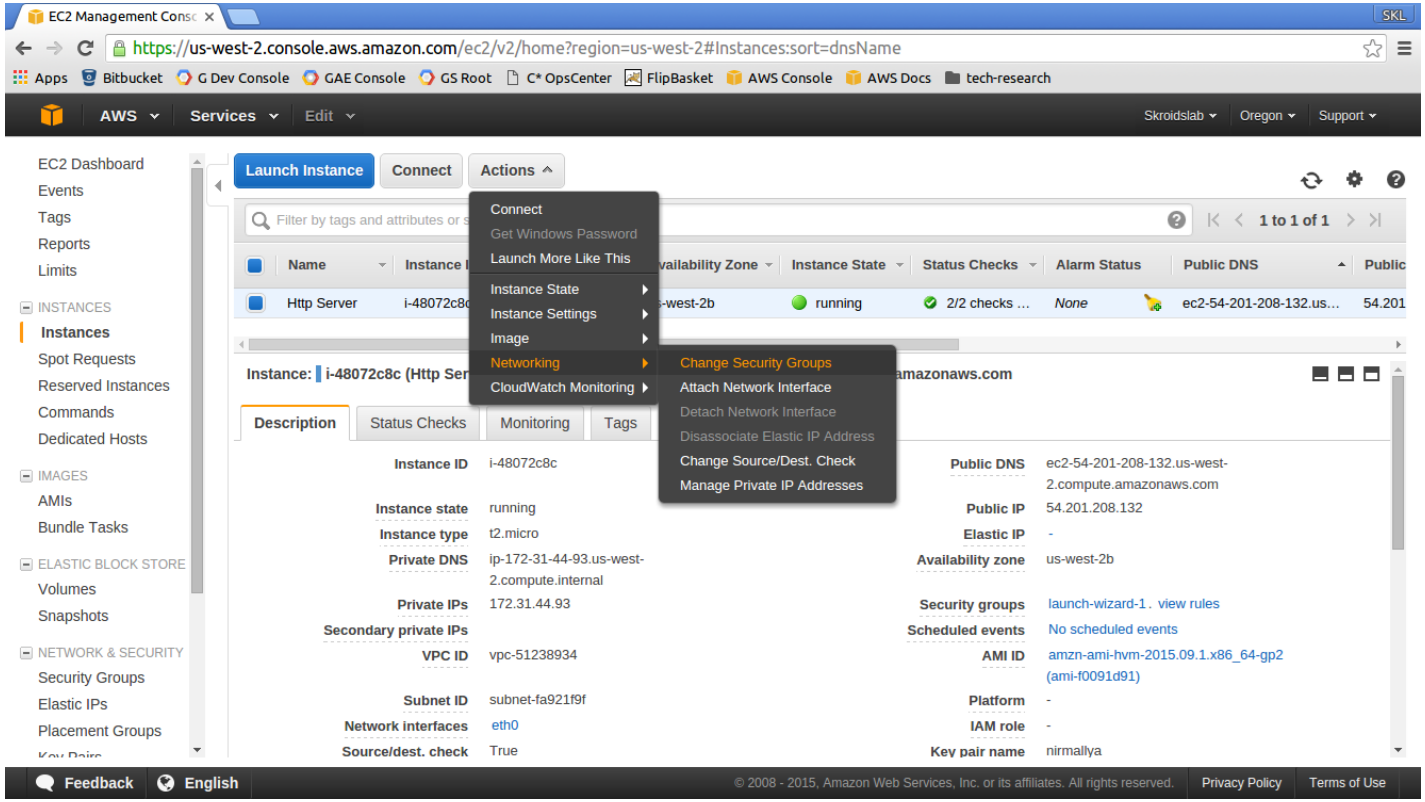
Activity - Security group

greatlearning



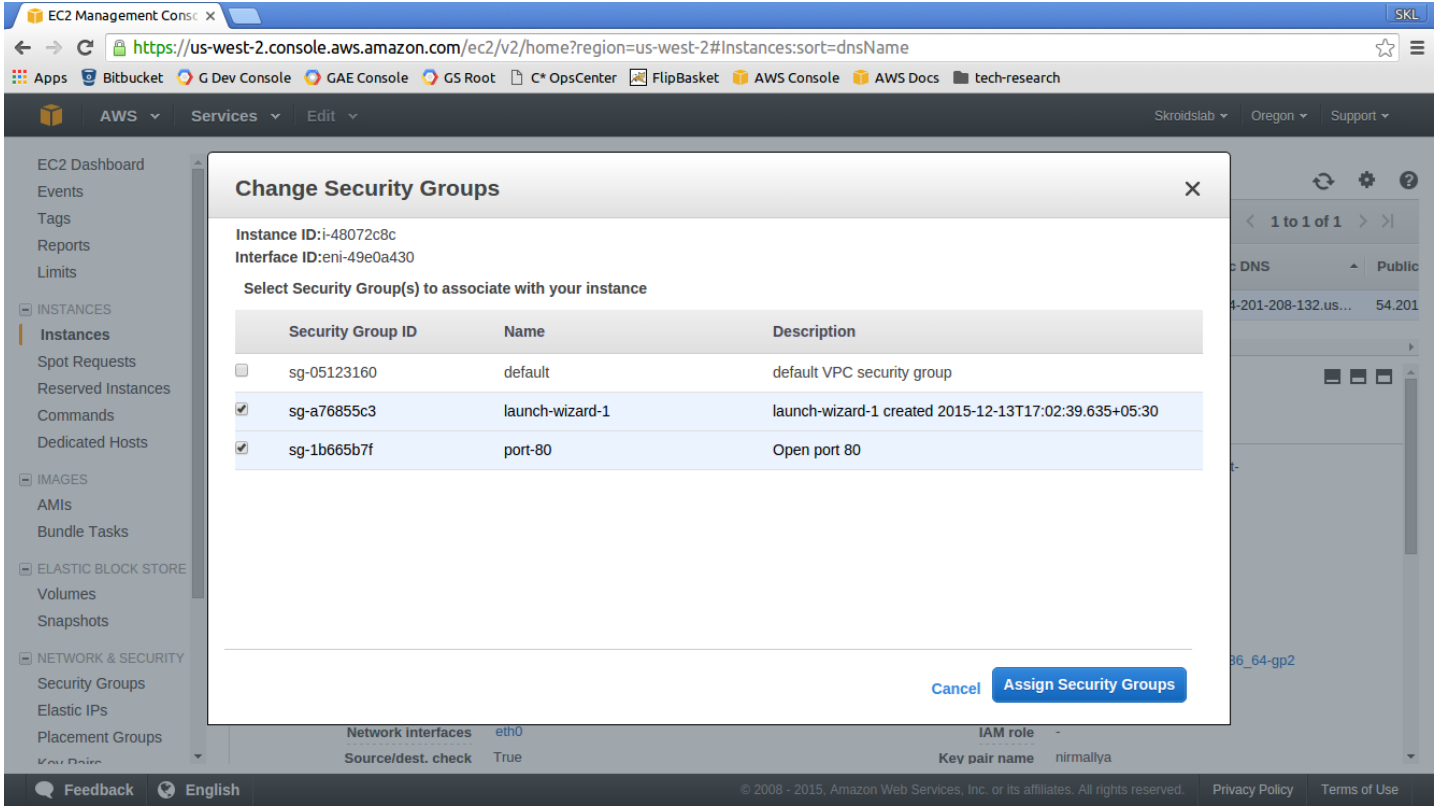
Activity - Security group

greatlearning



Activity - Security group

greatlearning



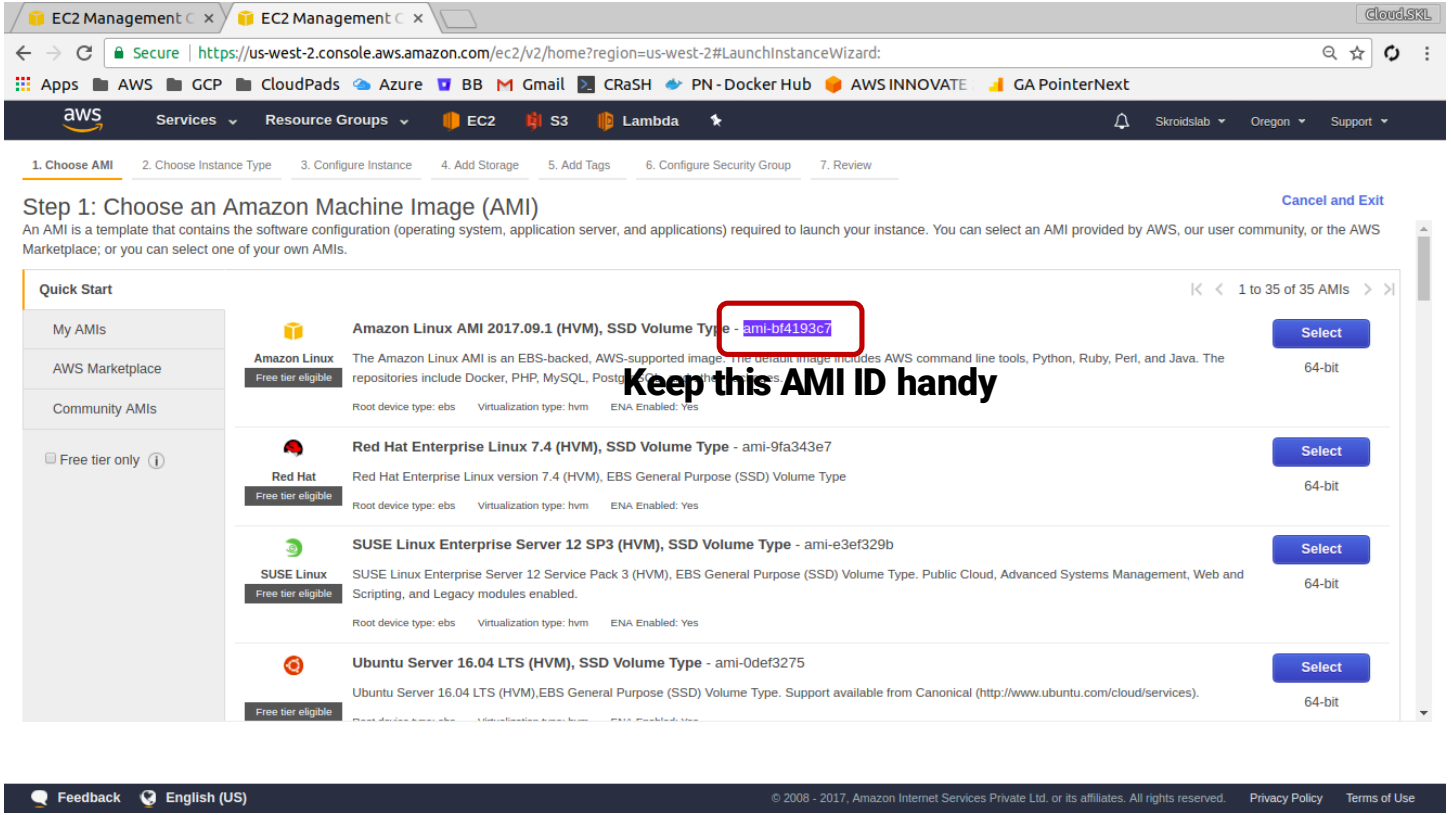
Fleet of EC2 instances

greatlearning

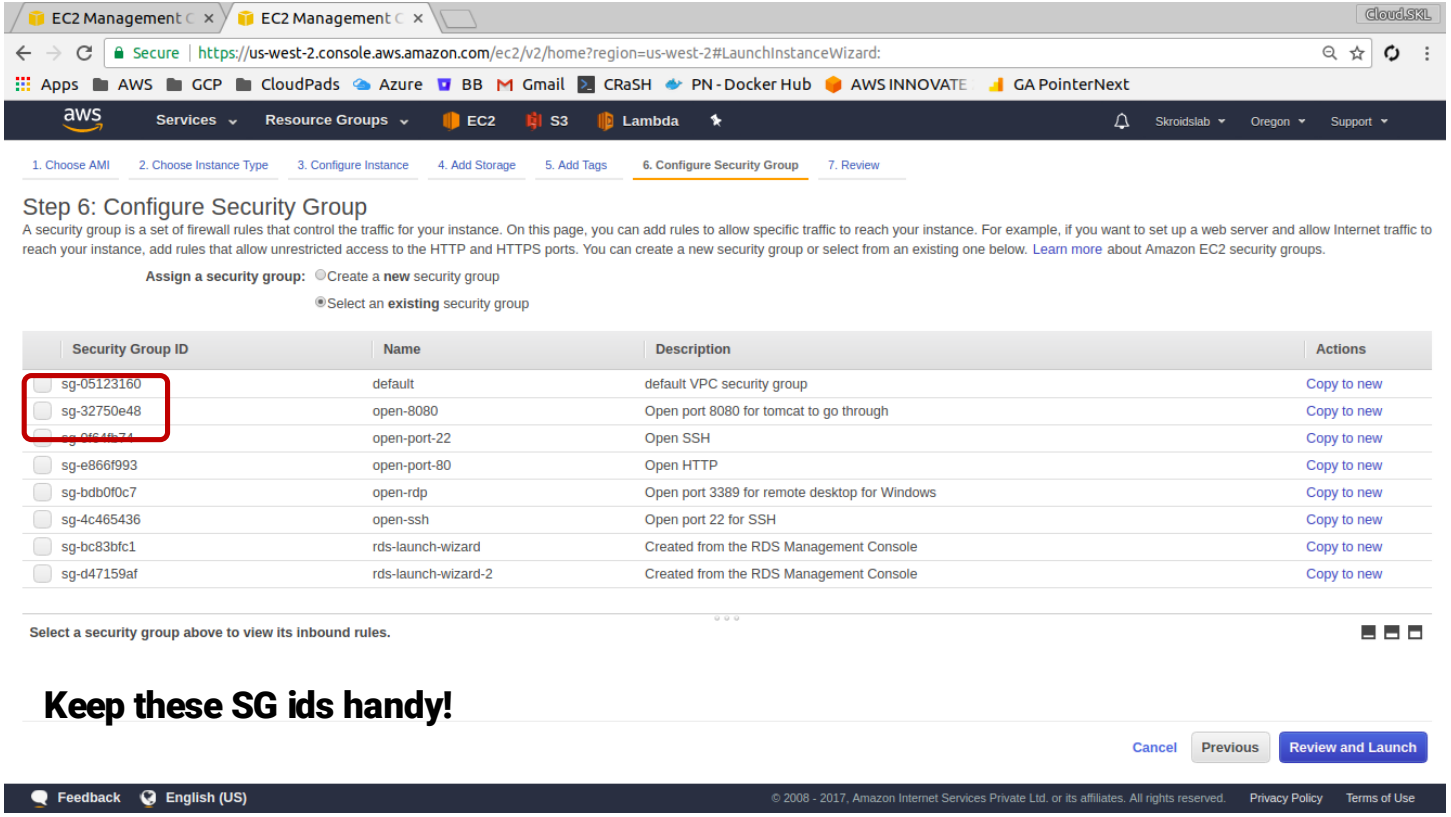
- We have one instance and are able to access the site with the direct IP address
- However, we would like to have a design where we have more than 1 server hiding behind a load balancer(LB)
- Concept
  - Create multiple instances in availability regions defined by the subnets
  - Point the LB to these multiple instances
- Exercise
  - We will use EC2 instance "Launch Templates"
  - Create 2 more EC2 instance in the same VPC but use a different subnet

Activity - Instance template

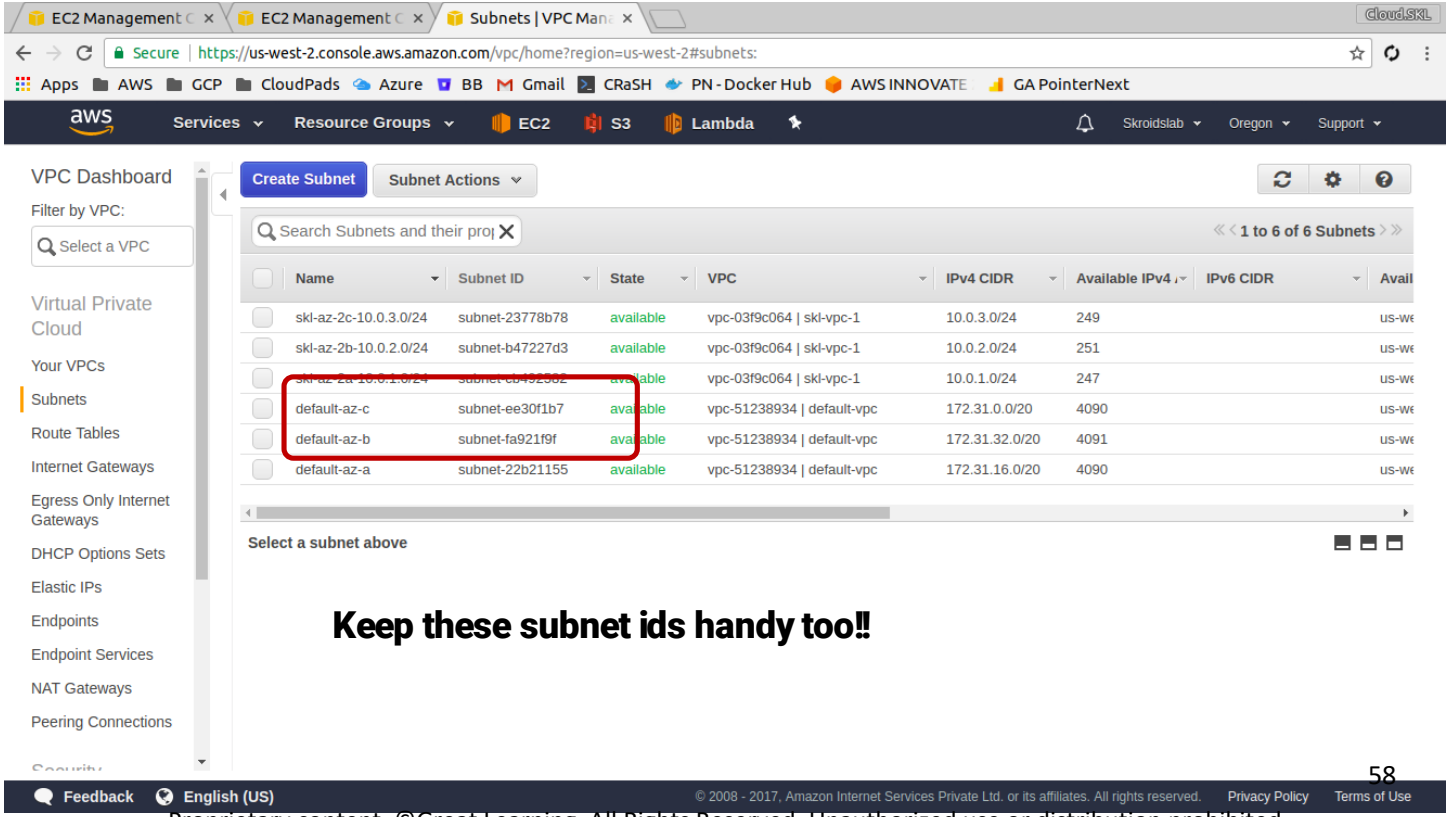
greatlearning



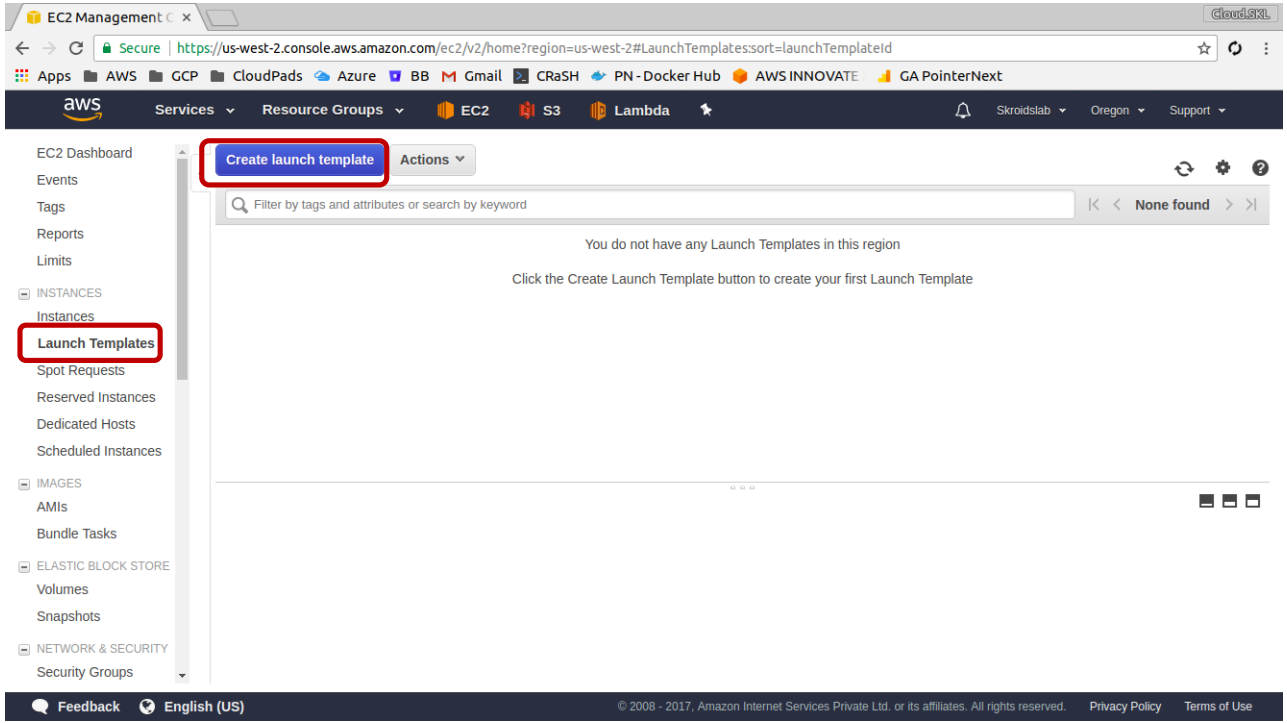
Activity - Instance template



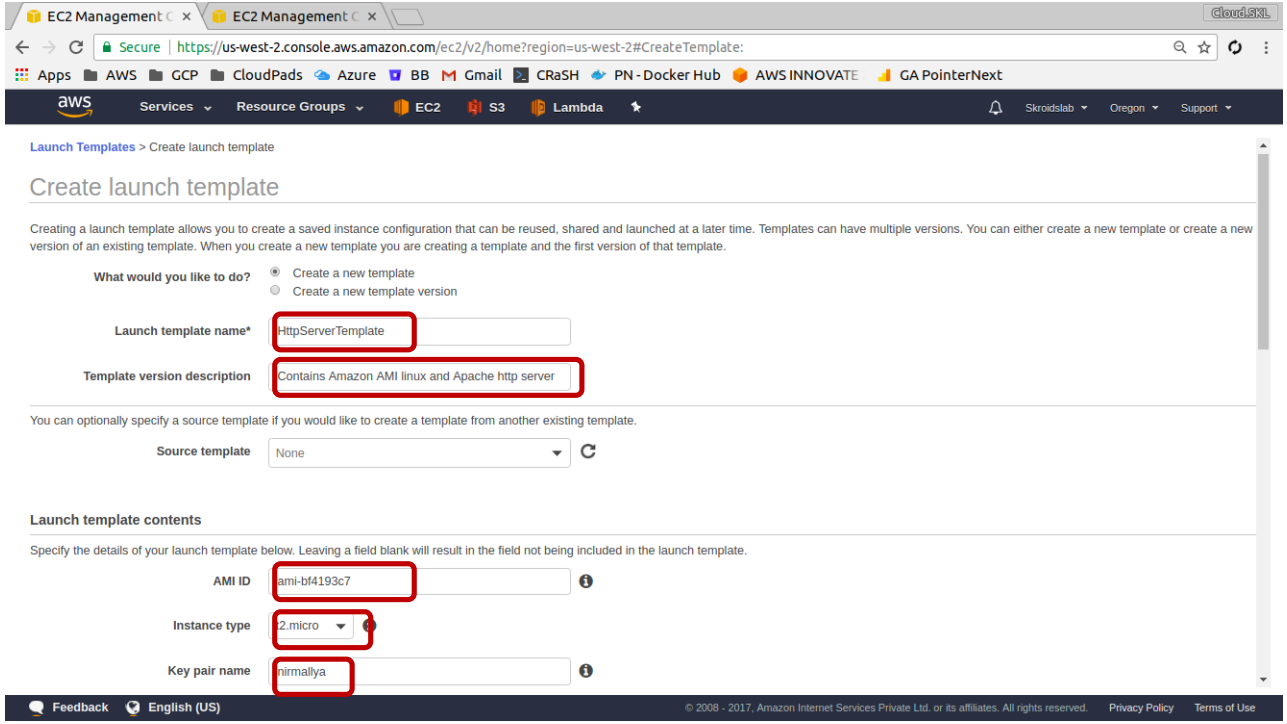
Activity - Instance template



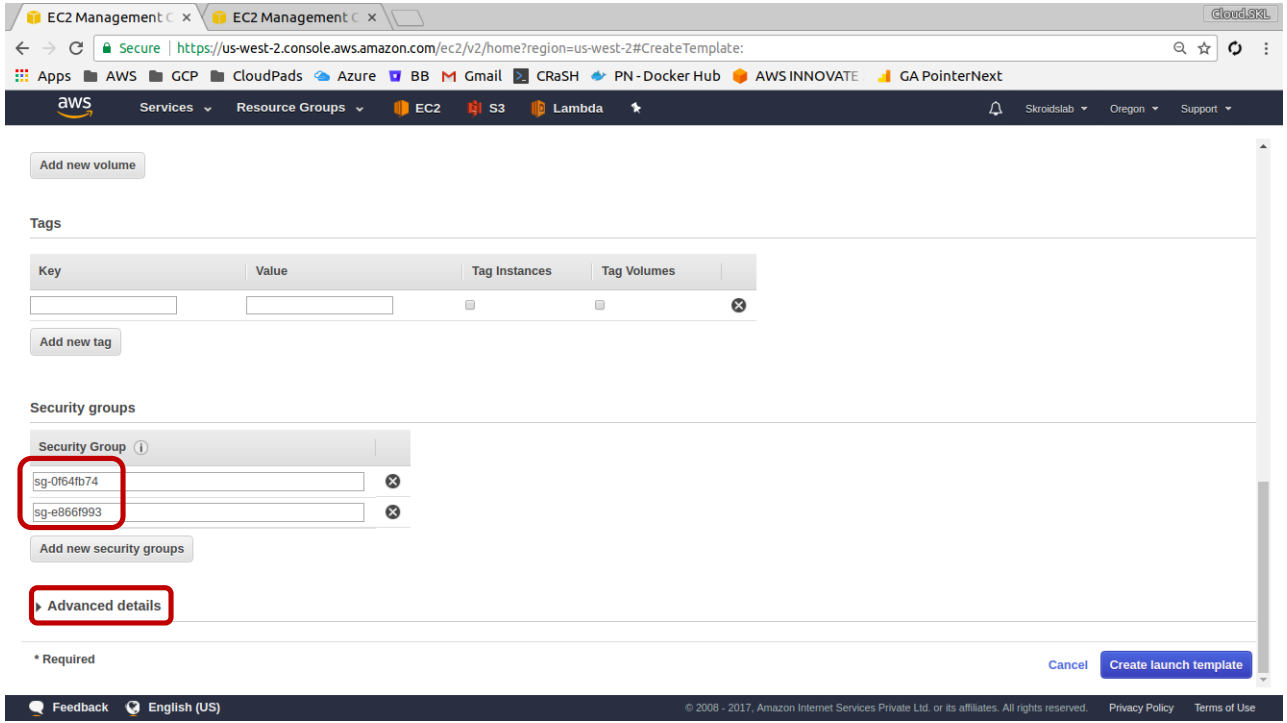
Activity - Instance template



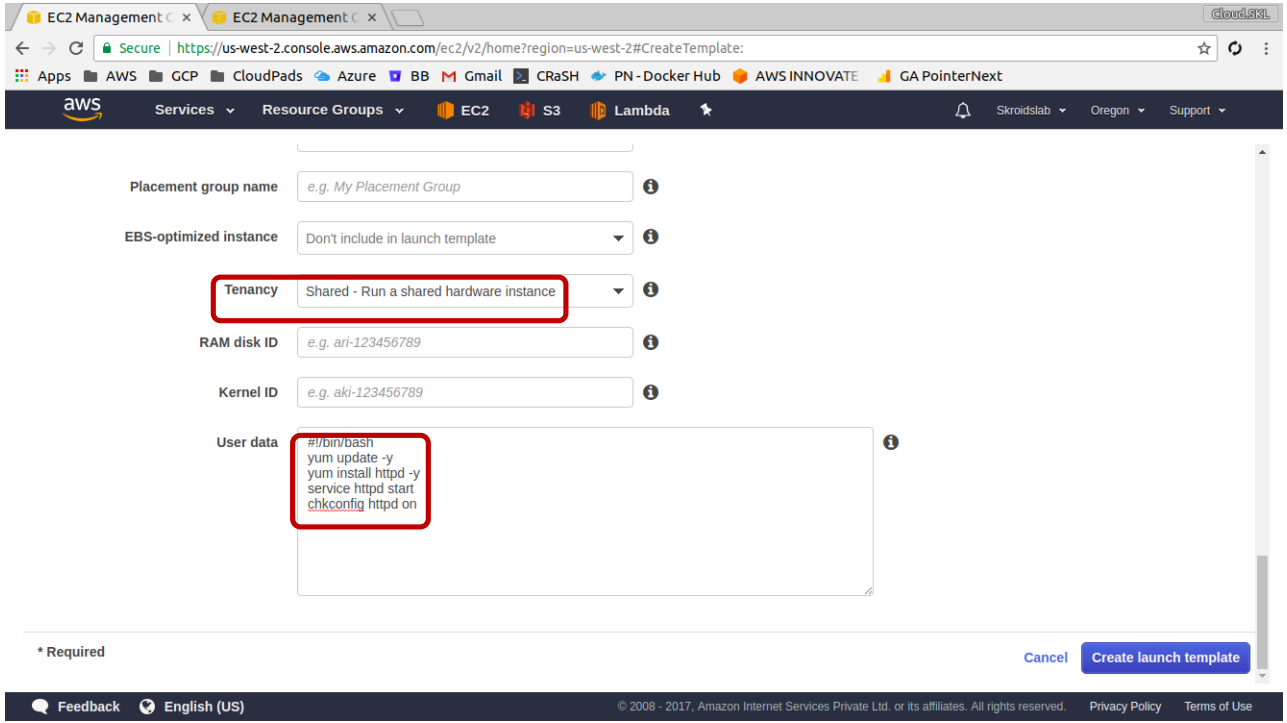
Activity - Instance template



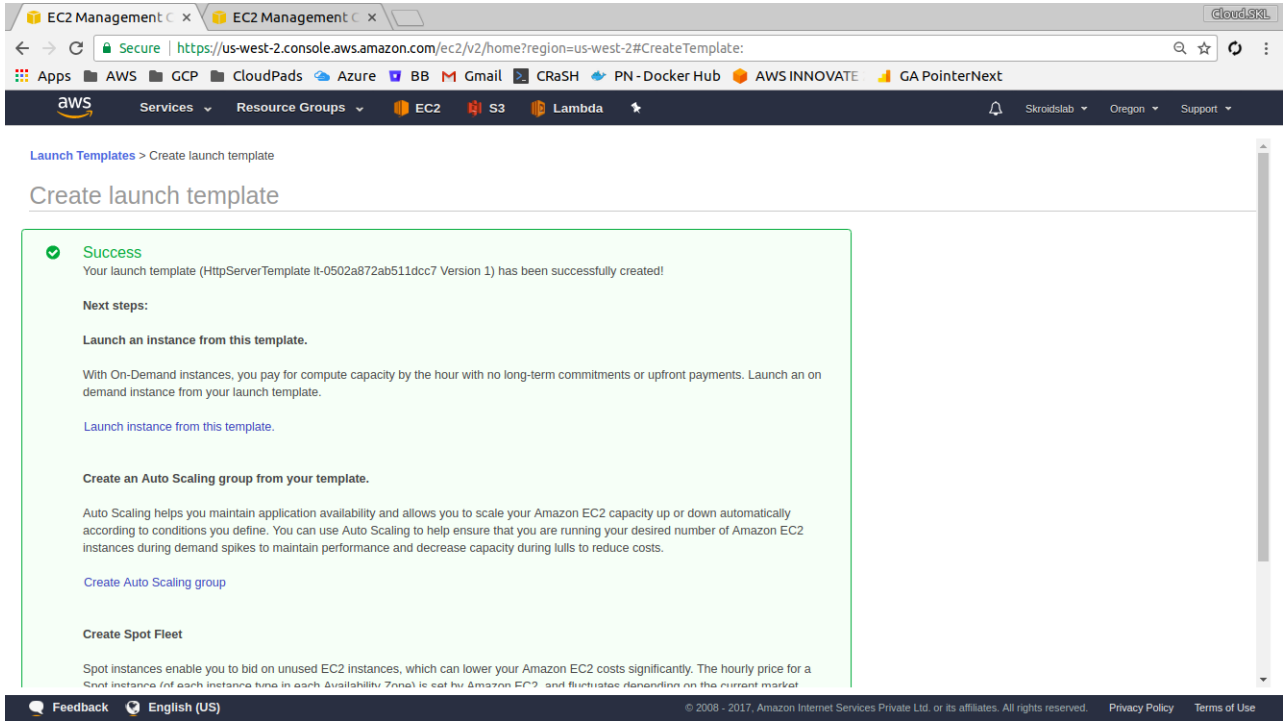
Activity - Instance template



Activity - Instance template

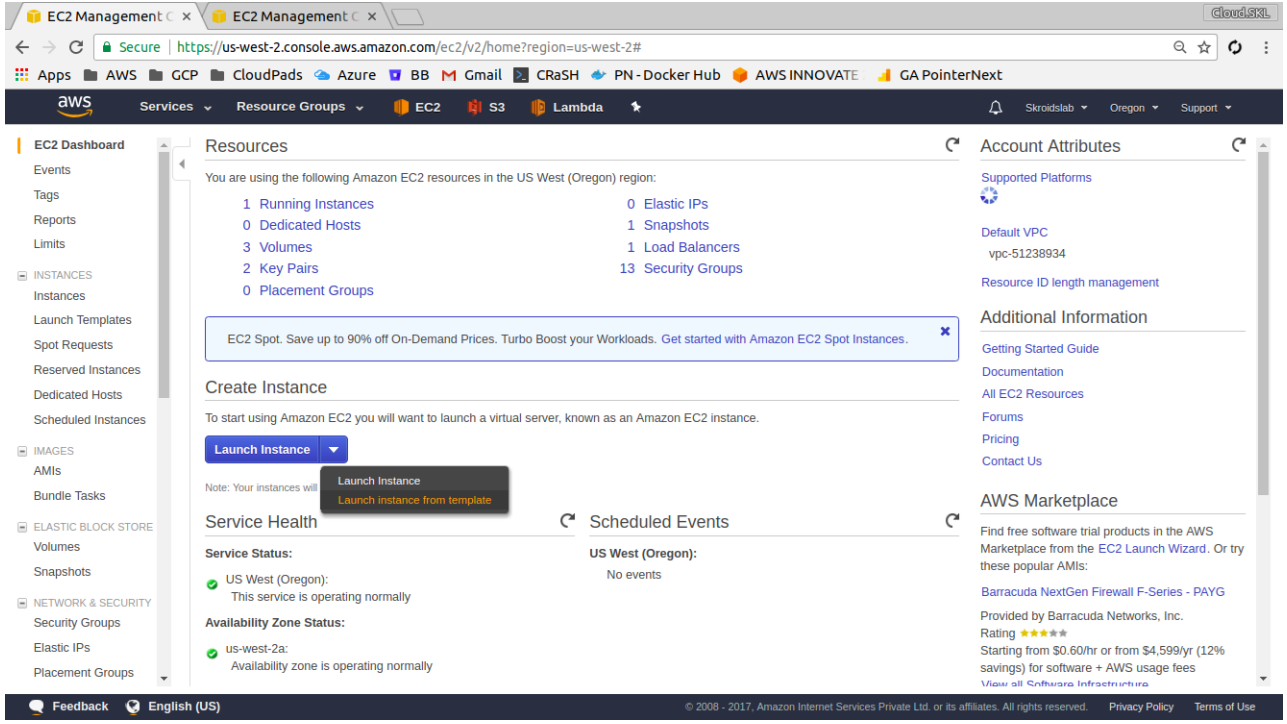


Activity - Instance template



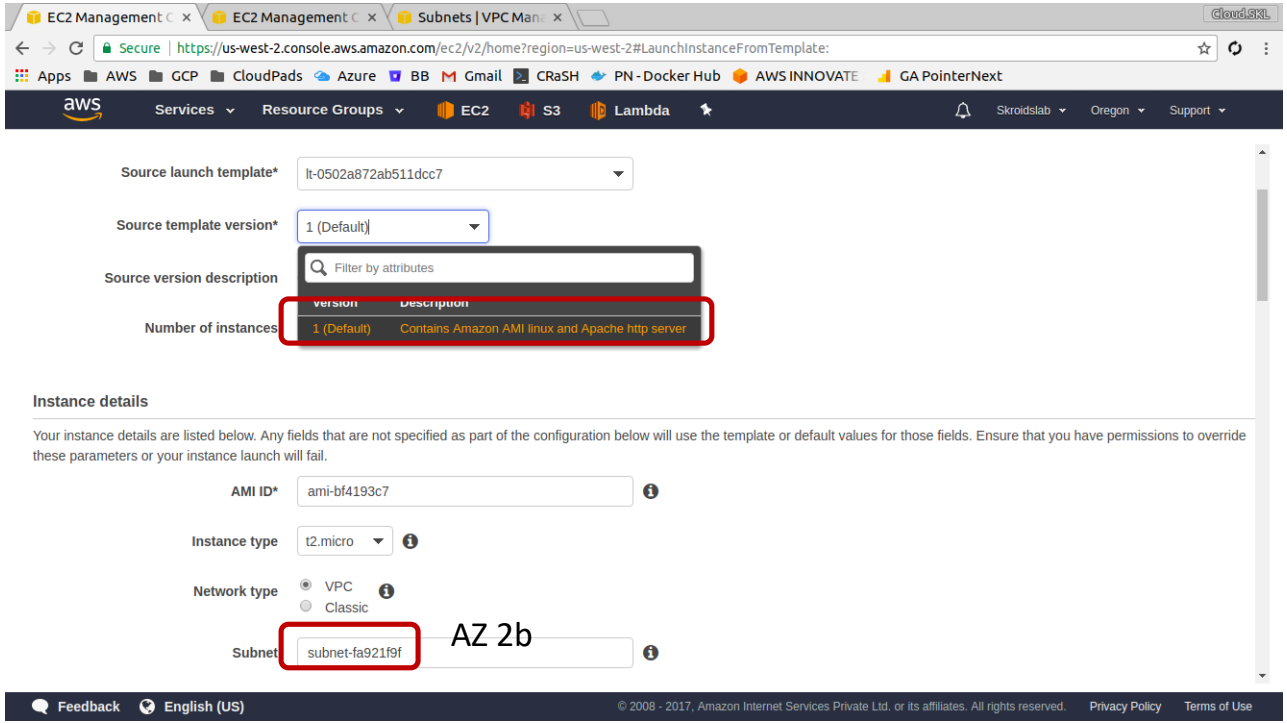
Activity - Instance template

Launch 2 more instances using the instance template



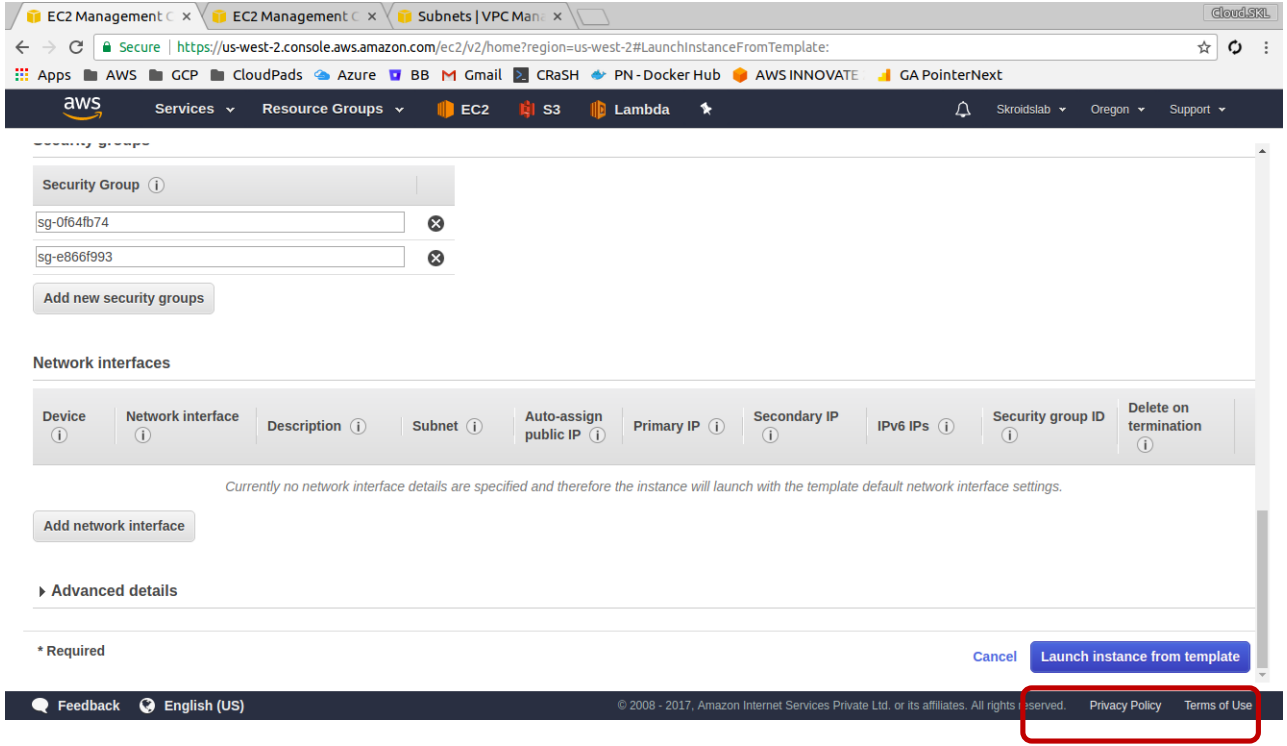
Activity - Instance template

greatlearning



After this add the "tag"

Activity - Instance template



And it says "User Data" needs to be base64 encoded!!!

Activity - Instance template

- Goto https://www.base64encode.org/
  - Click on the "Encode" tab
  - Paste the full user data in the text area
- The encoded string will look like this
  - IyEvYmluL2Jhc2gNCnl1bSB1cGRhdGUgLXkNCnl1bSBpbnN0YWxsIGh0dHBkIC15DQpzZXJ2aWNlIGh0dHBkIHN0YXJ0DQpjaGtjb25maWcgaHR0cGQgb24=

Fleet of EC2 instances

greatlearning

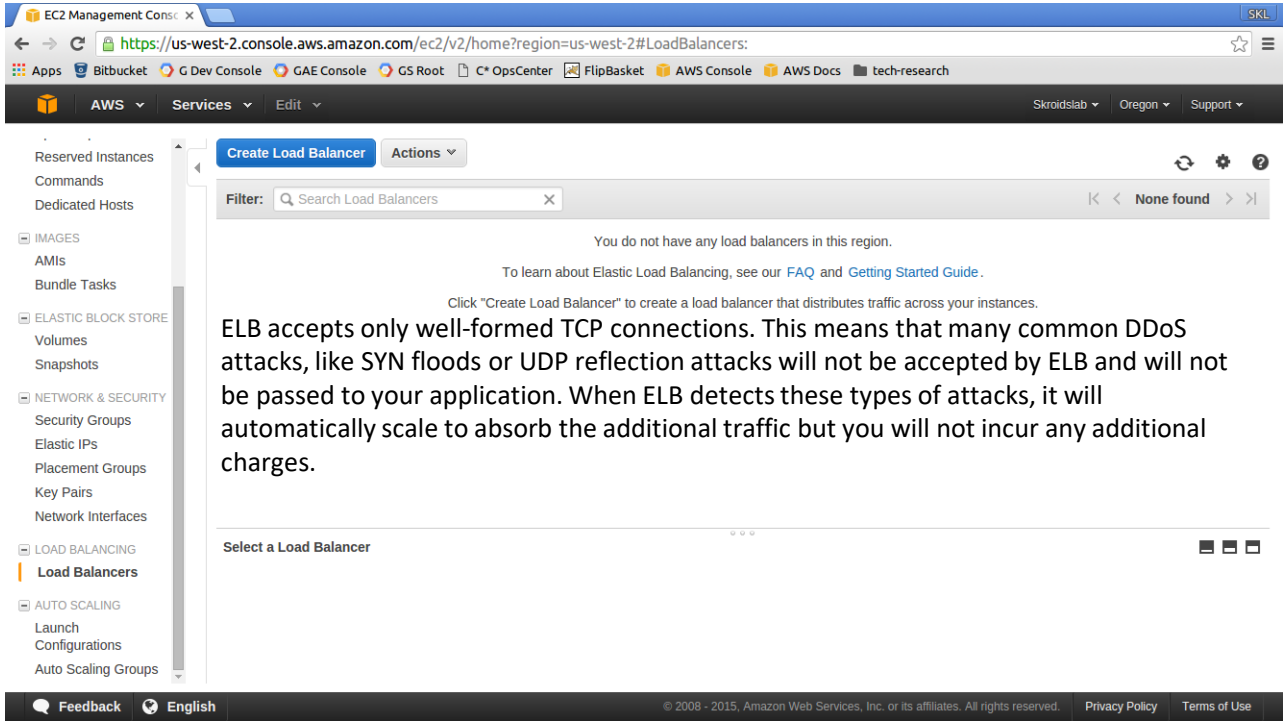
- Install the apache http server
    - $ sudo yum update
    - $ sudo yum install httpd
    - $ sudo service httpd start
    - $ curl localhost
  - Also create files called index.html & health.html
    - $ sudo su [For root access]
    - # cd /var/www/html
    - # echo "Web server 1" > index.html
    - # echo "ok" > health.html
  - Do this in both instances

greatlearning

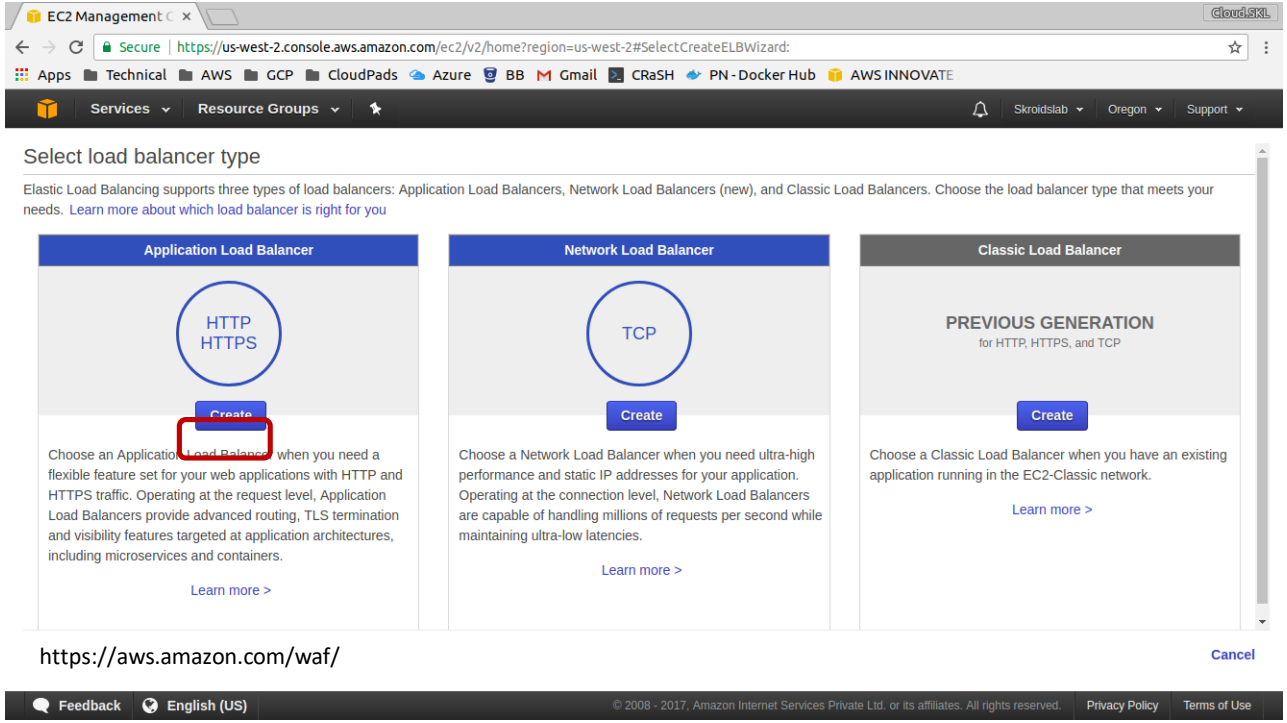
Compute - Part I

Load balancing

Activity - load balancer



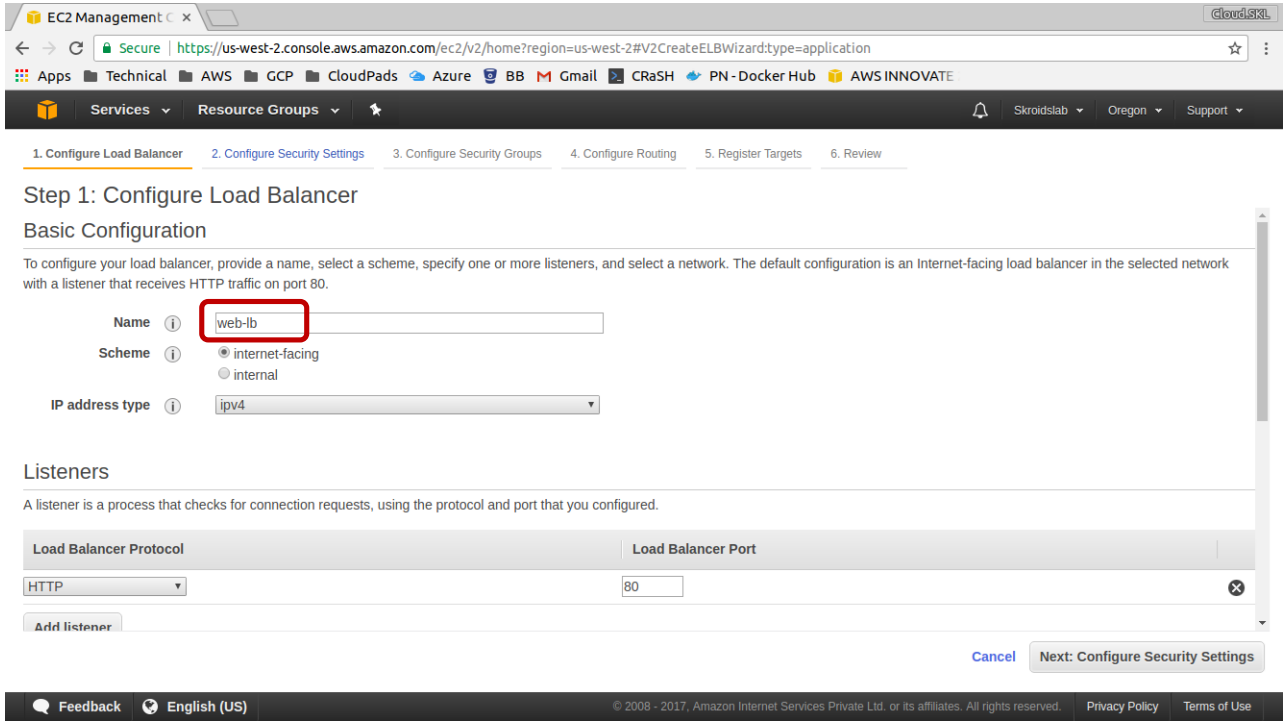
Activity - load balancer



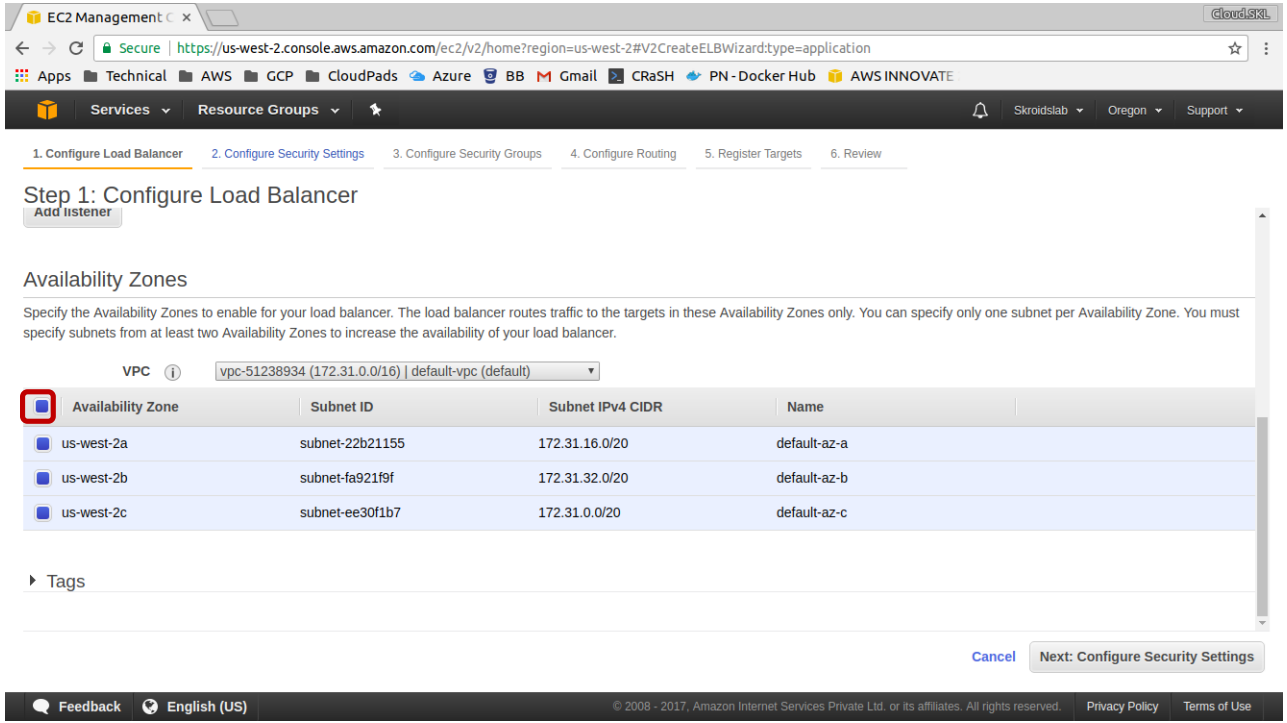
https://aws.amazon.com/waf/

https://aws.amazon.com/blogs/aws/new-application-load-balancing-via-ip-address-to-aws-on-premises-resources

Activity - http load balancer

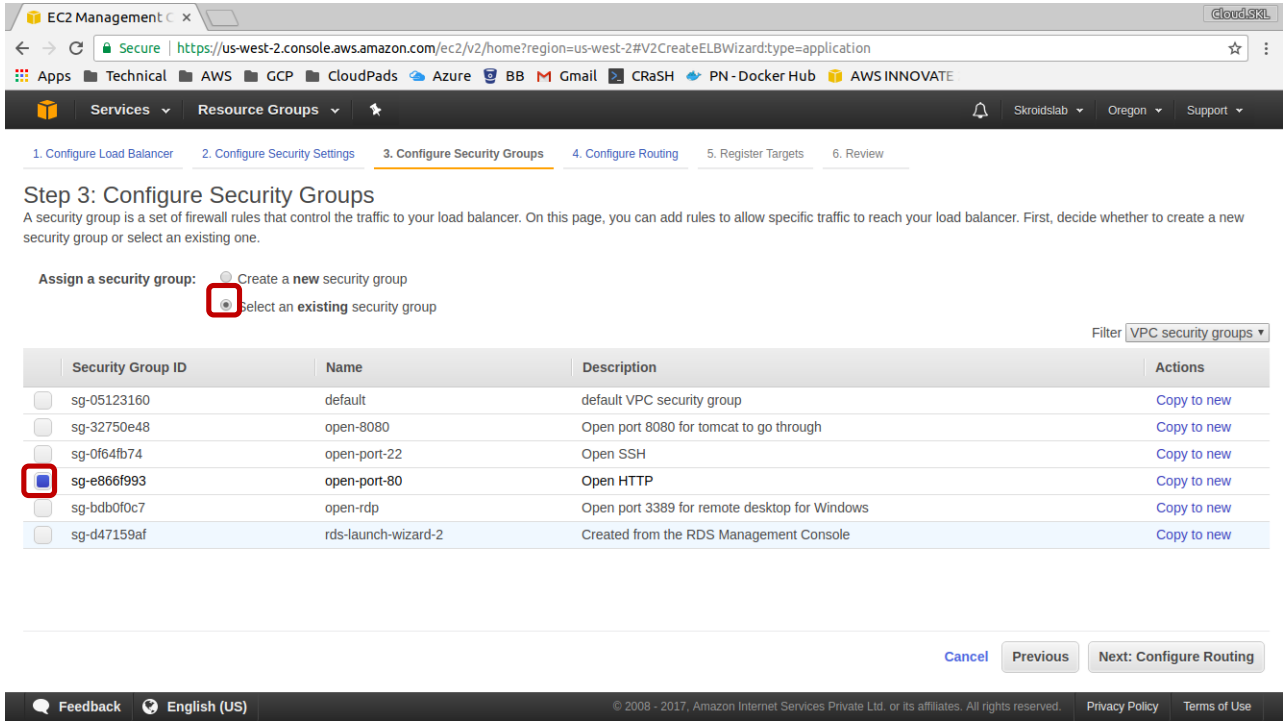


Activity - http load balancer

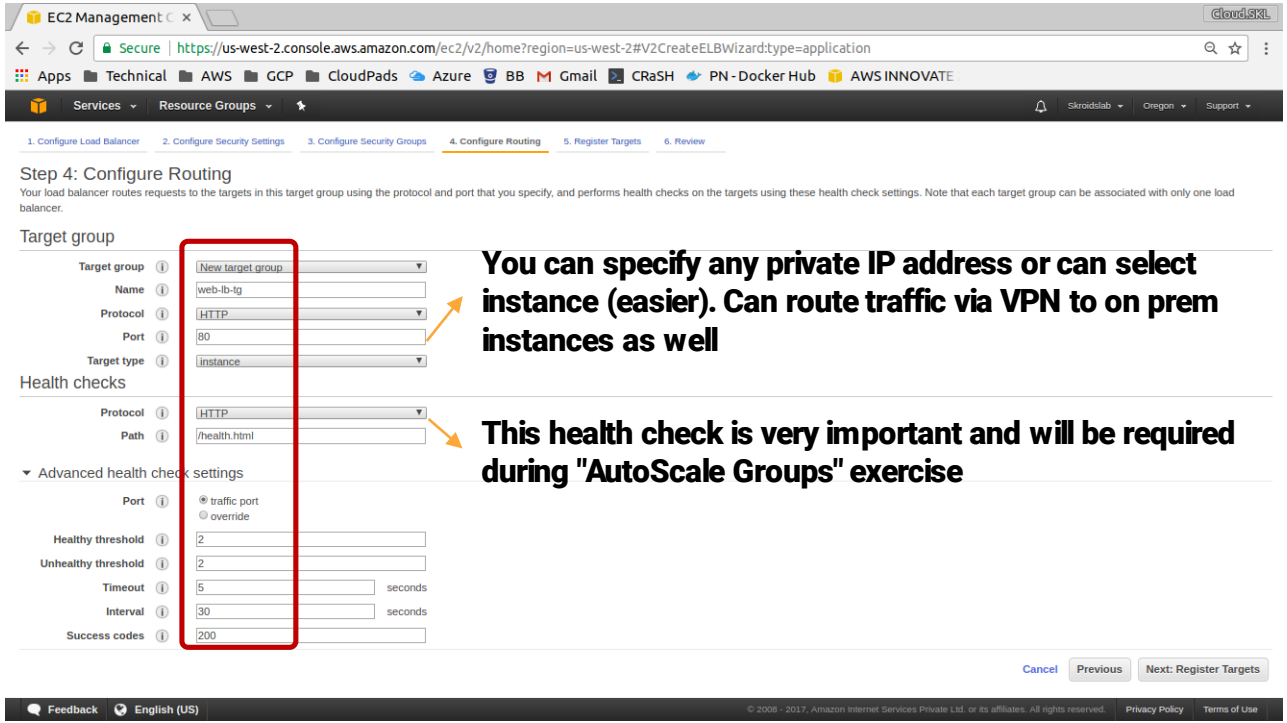


Activity - http load balancer

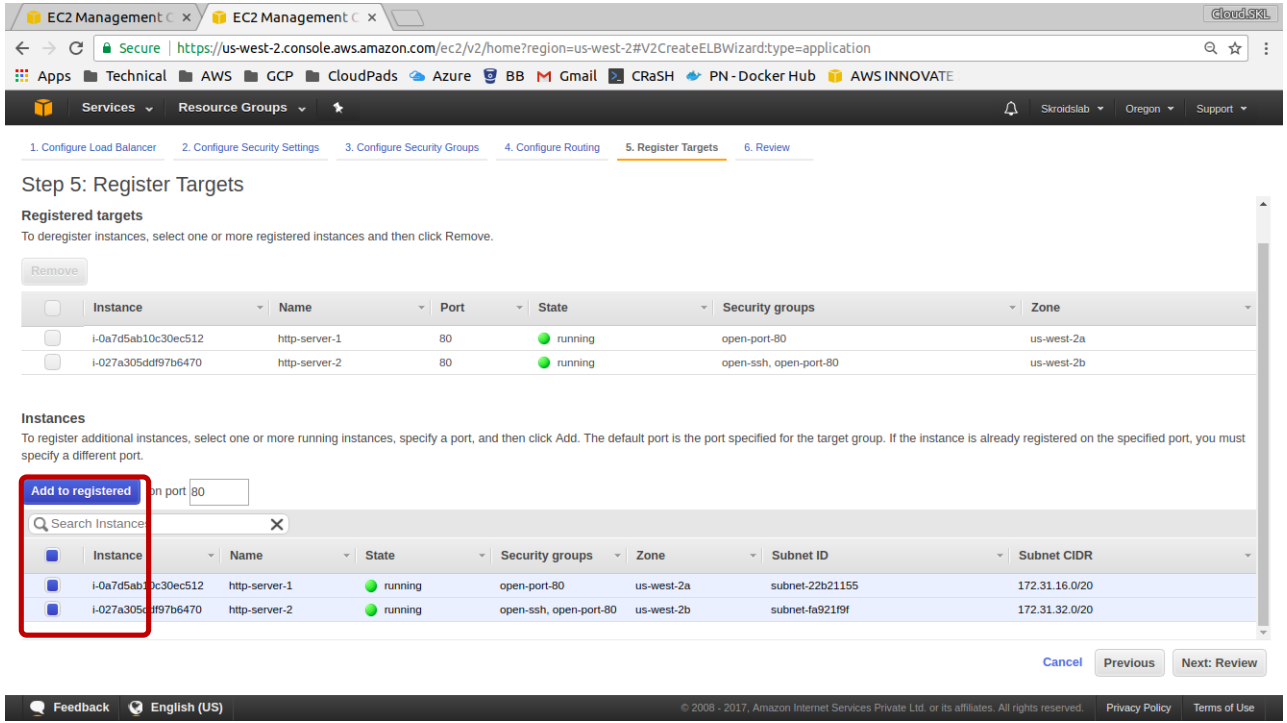
Activity - http load balancer



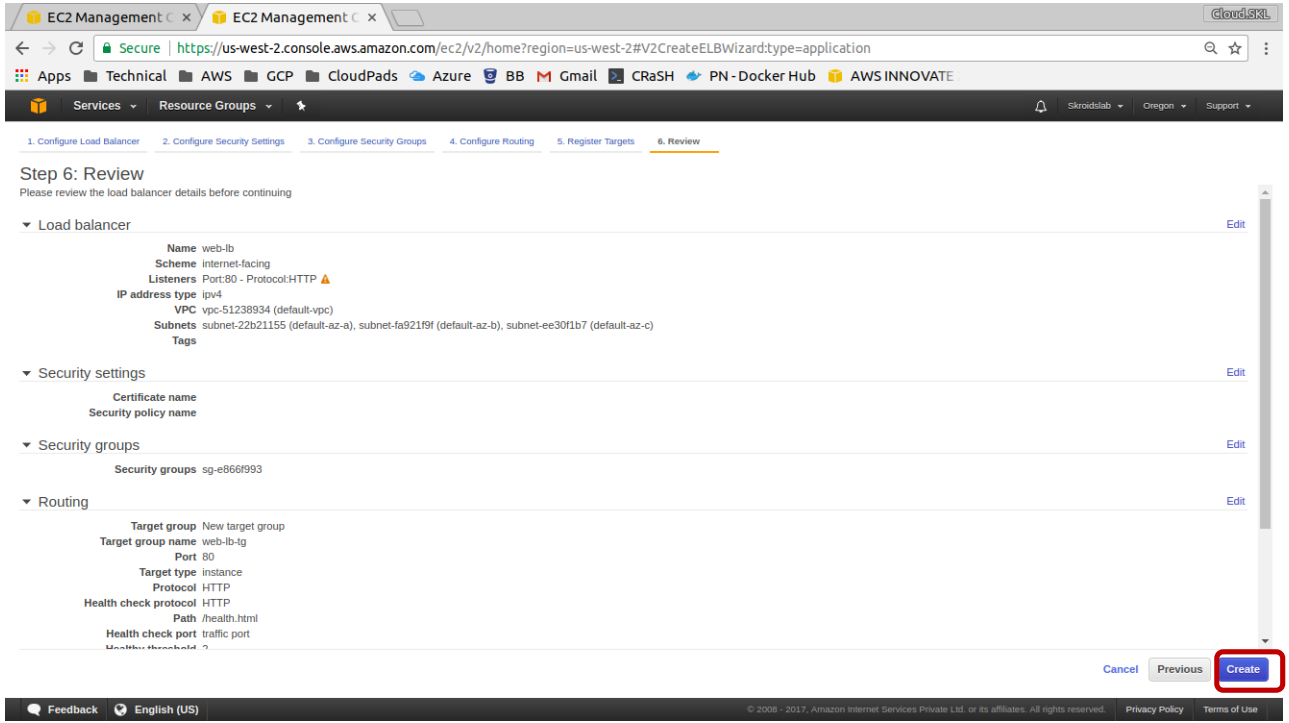
Activity - http load balancer



Activity - http load balancer

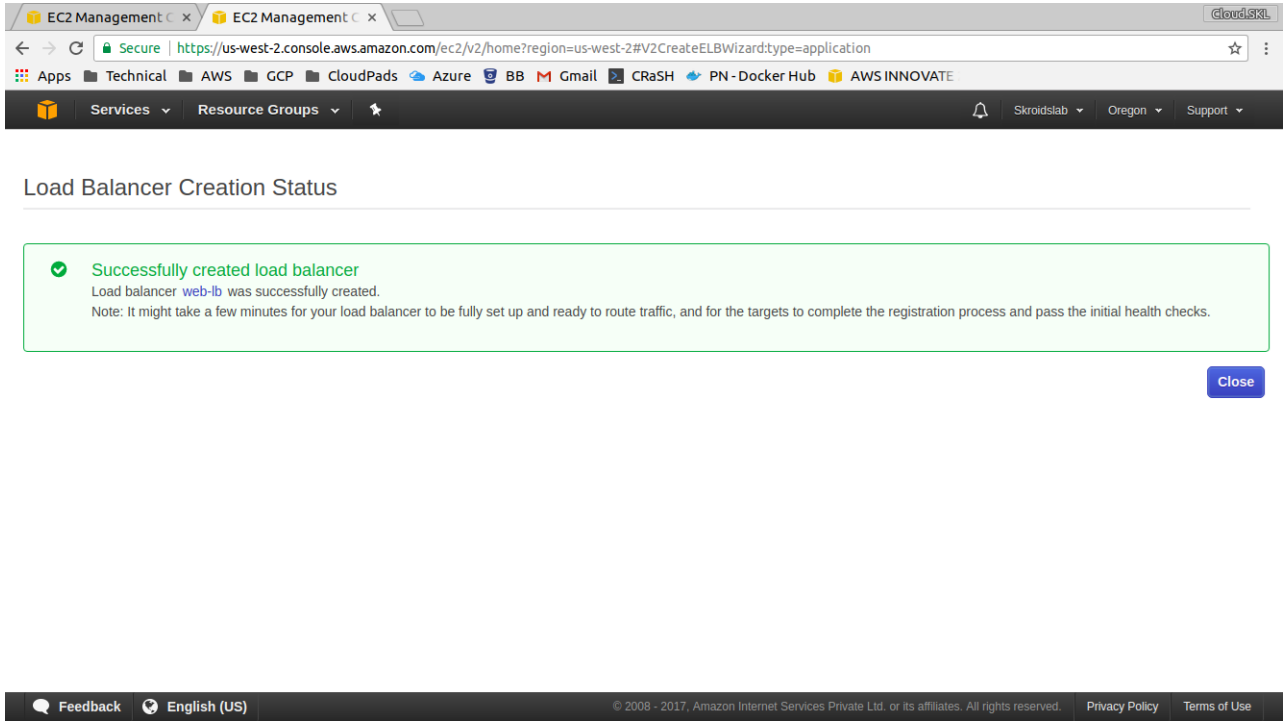


Activity - http load balancer

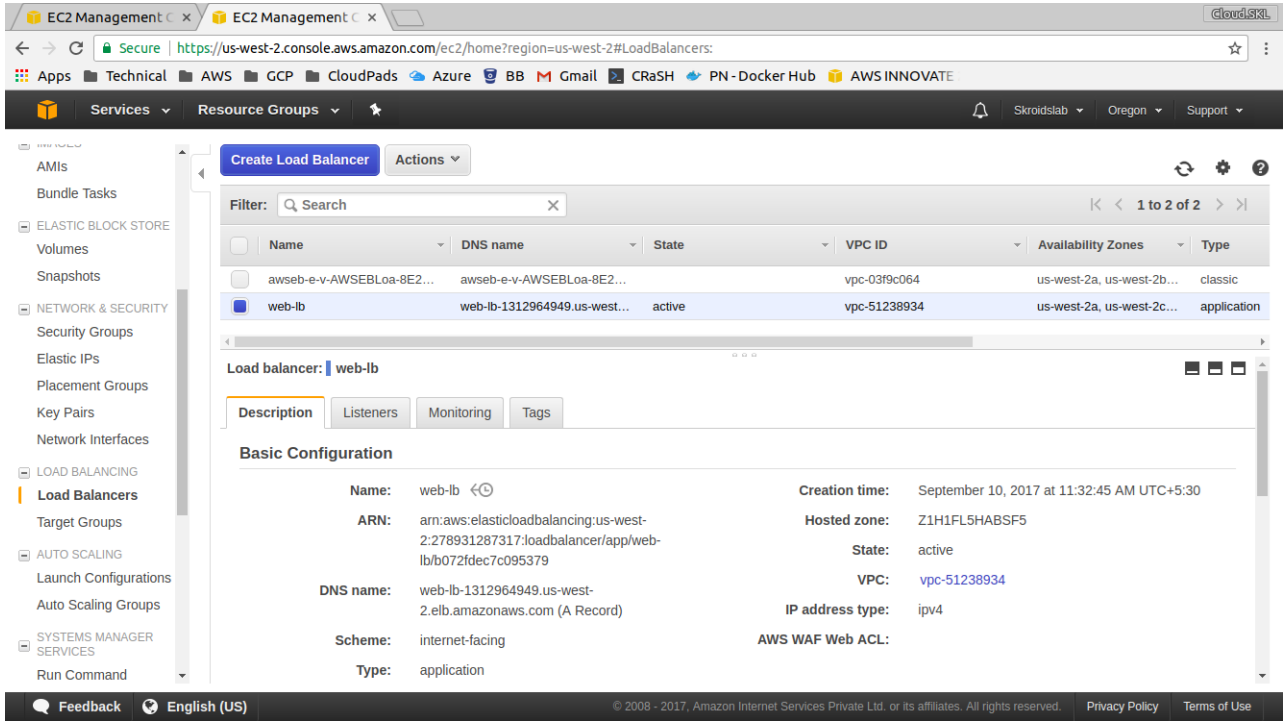


Activity - http load balancer

greatlearning

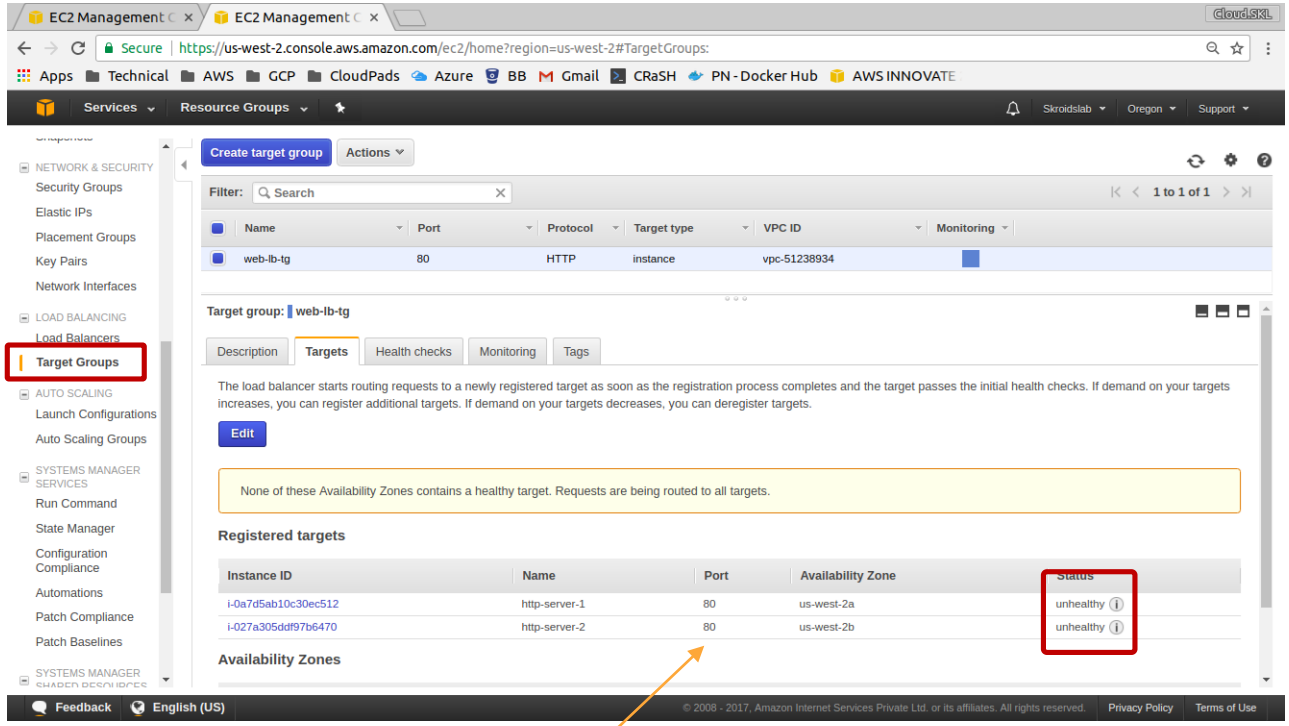


Activity - http load balancer



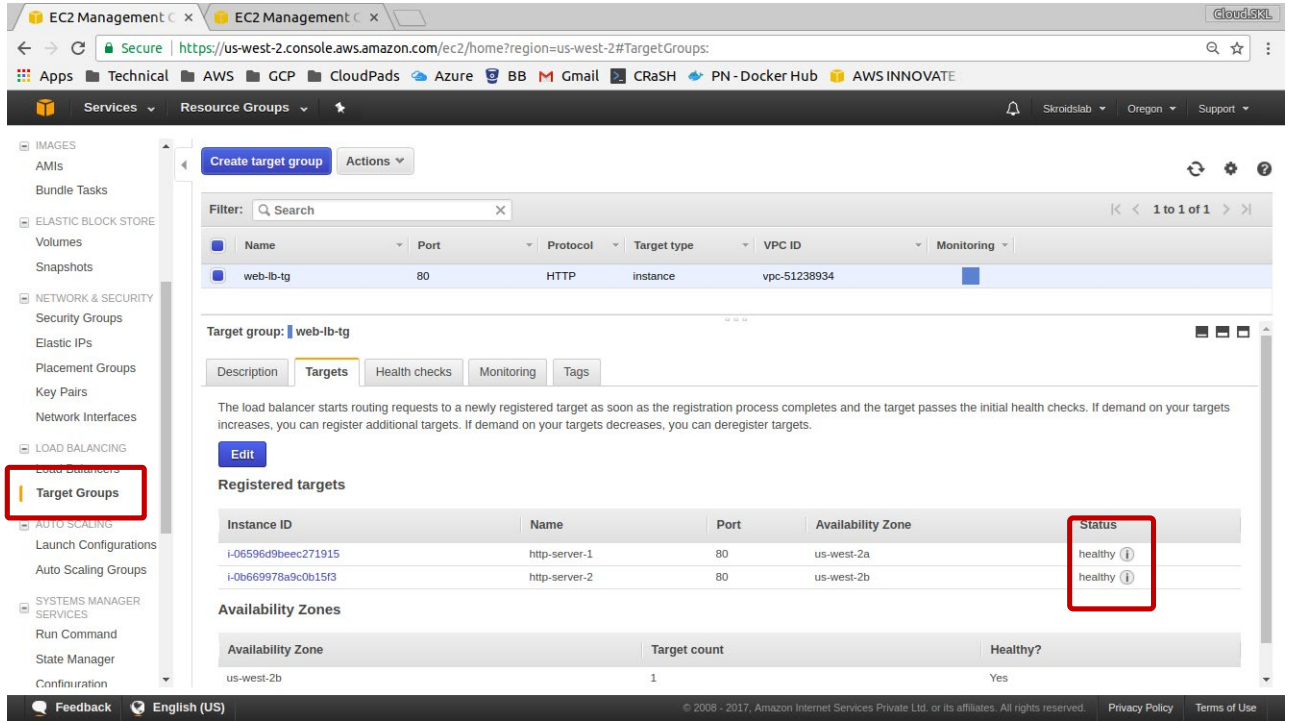
Activity - http load balancer

greatlearning



Port from the http LB is automatically mapped

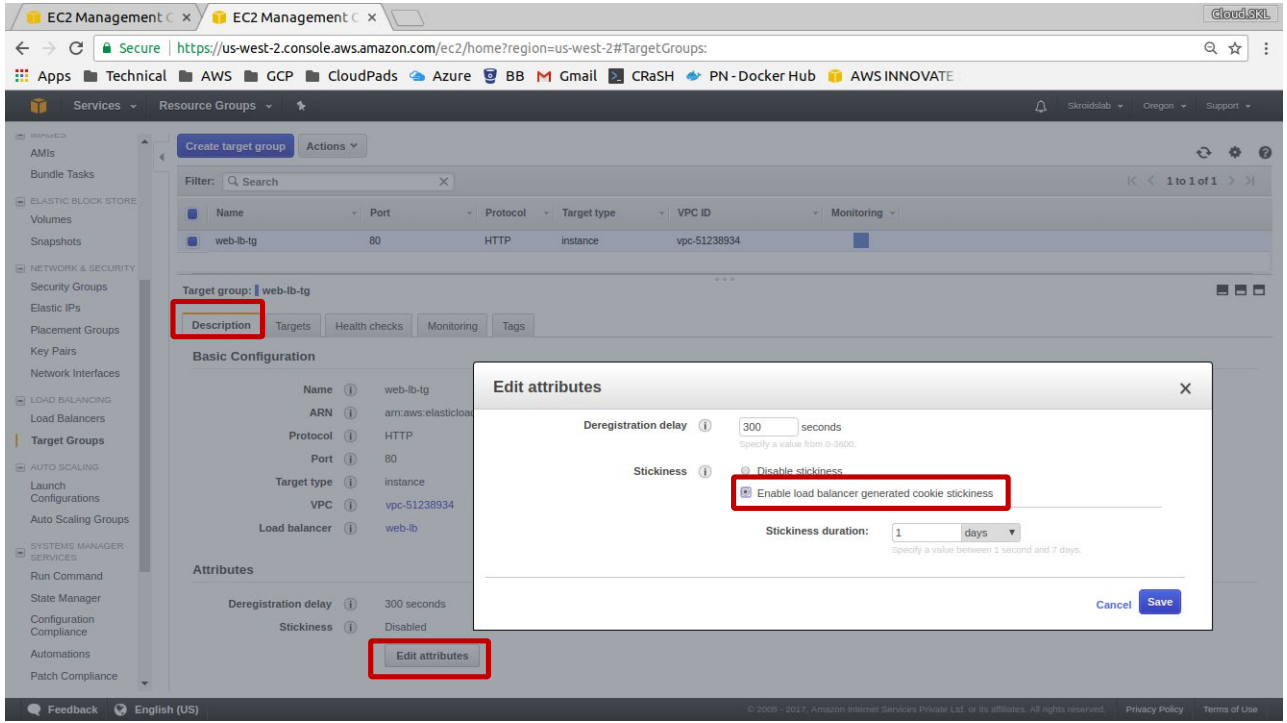
Activity - http load balancer



Activity - load balancer

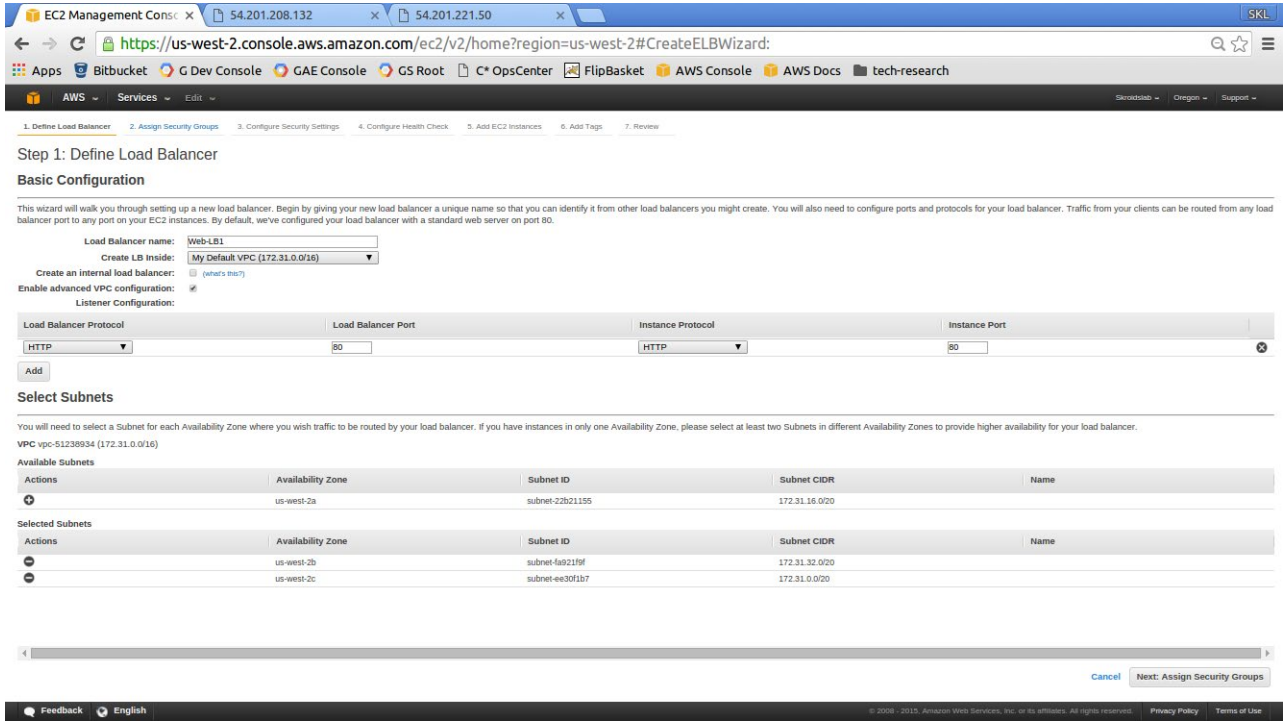
- Hit the load balancer using the DNS name
- No IP address will be provided, it may be changed by AWS
- Not a best practice of accessing LB using IP address
- Hit the DNS a few times and see the content change as the request shifts from one server to the other
- You can configure alarms
- LB always gives you a public DNS and not a public IP
- ACTIVITY -> Simulate a failure by shutting down an instance
- DEBATE -> You can enable LB to "instance stickiness" (next...)

Activity - load balancer

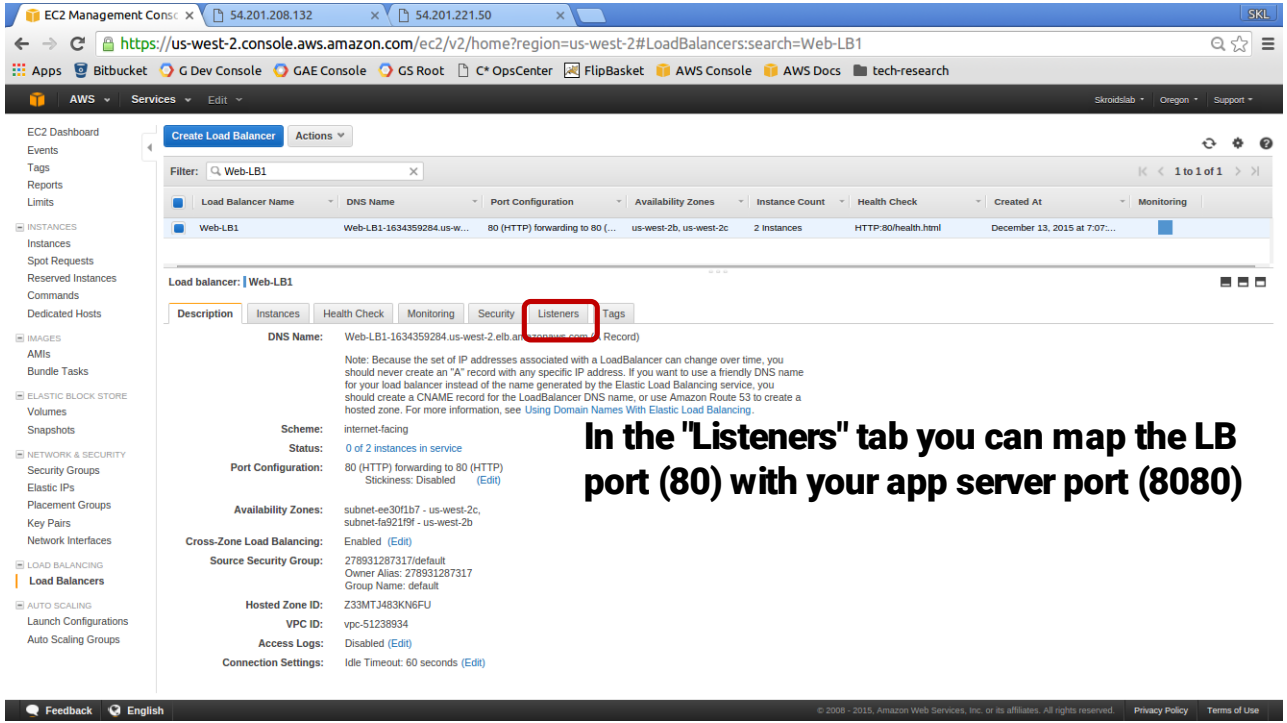


Reference - classic load balancer

greatlearning



Reference - classic load balancer



In the "Listeners" tab you can map the LB port (80) with your app server port (8080)

greatlearning

Compute - Part I

Web Application Firewall (WAF)

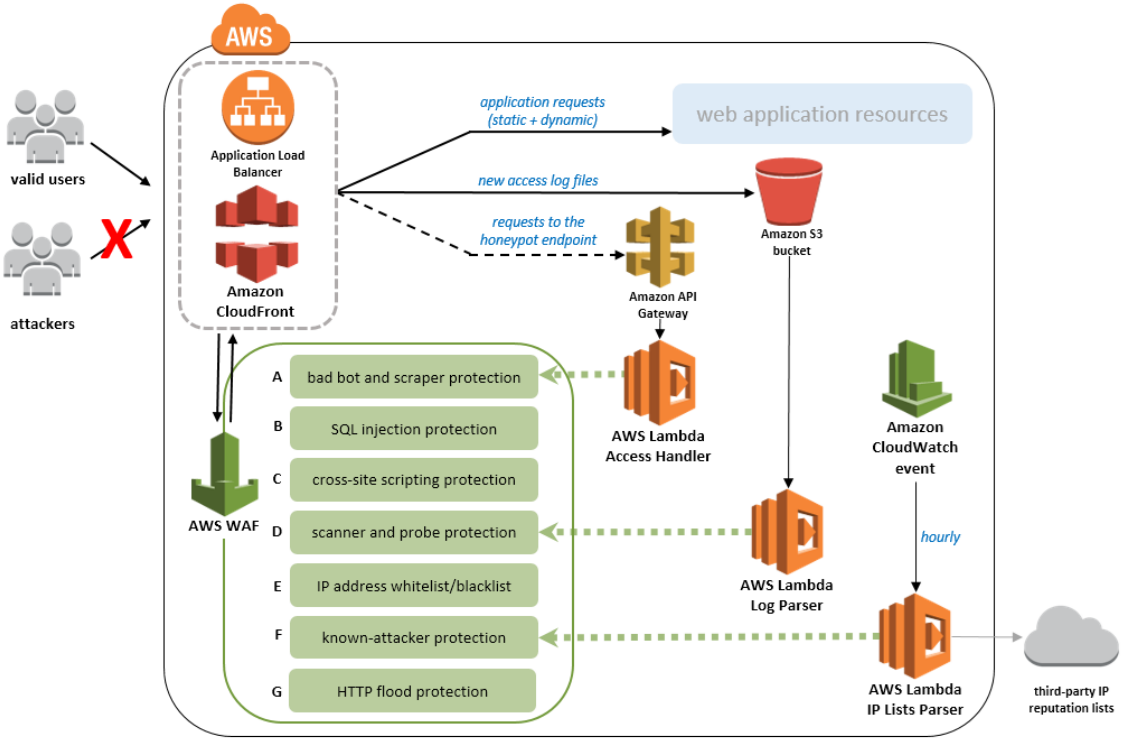
Shield - discussion

WAF exercise prerequisites

greatlearning

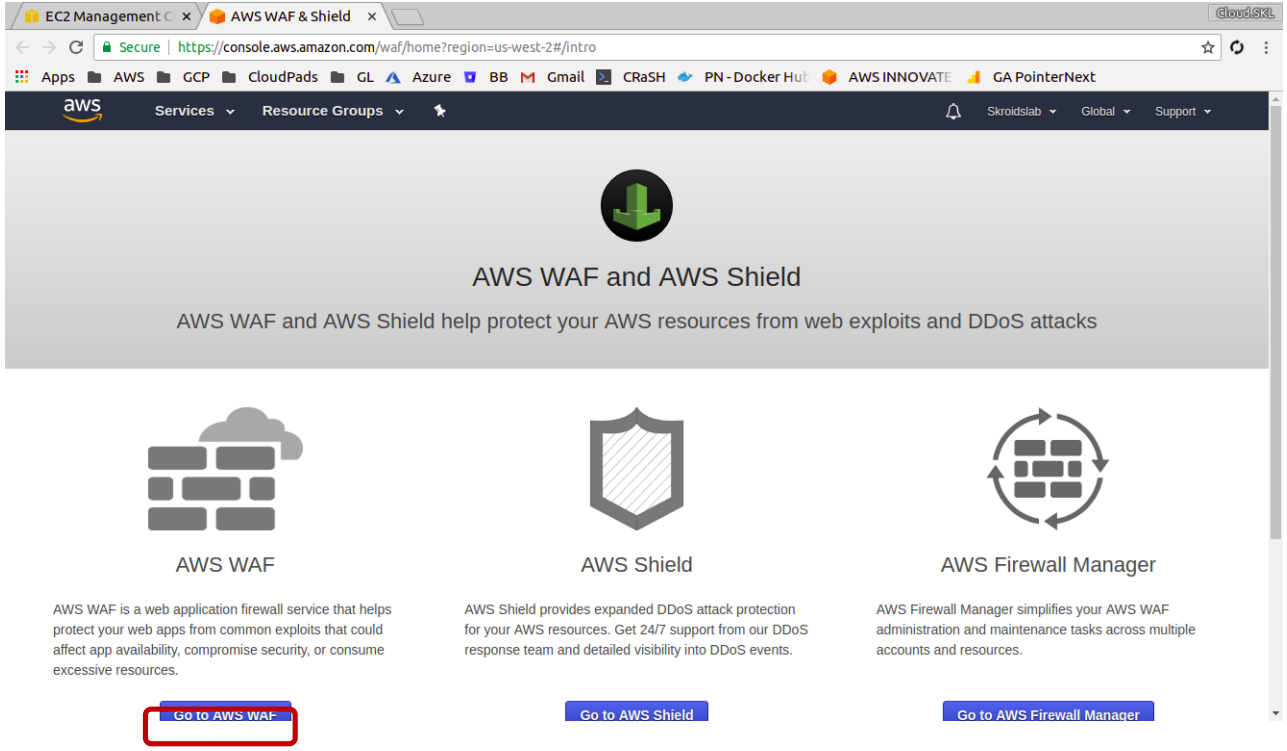
- Any web application hosted on EC2
- Serving traffic on port 80
- Application load balancer with a target group having the EC2 instance
- WAF pricing: https://aws.amazon.com/waf/pricing/
  - $5 per web ACL per month
  - $1 per rule per web ACL per month
  - $0.60 per million web requests
- Shield standard and advanced https://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html
- Tutorials: https://docs.aws.amazon.com/waf/latest/developerguide/tutorials.html
- Popular rules: https://github.com/aws-samples/aws-waf-sample

LB and WAF & other components



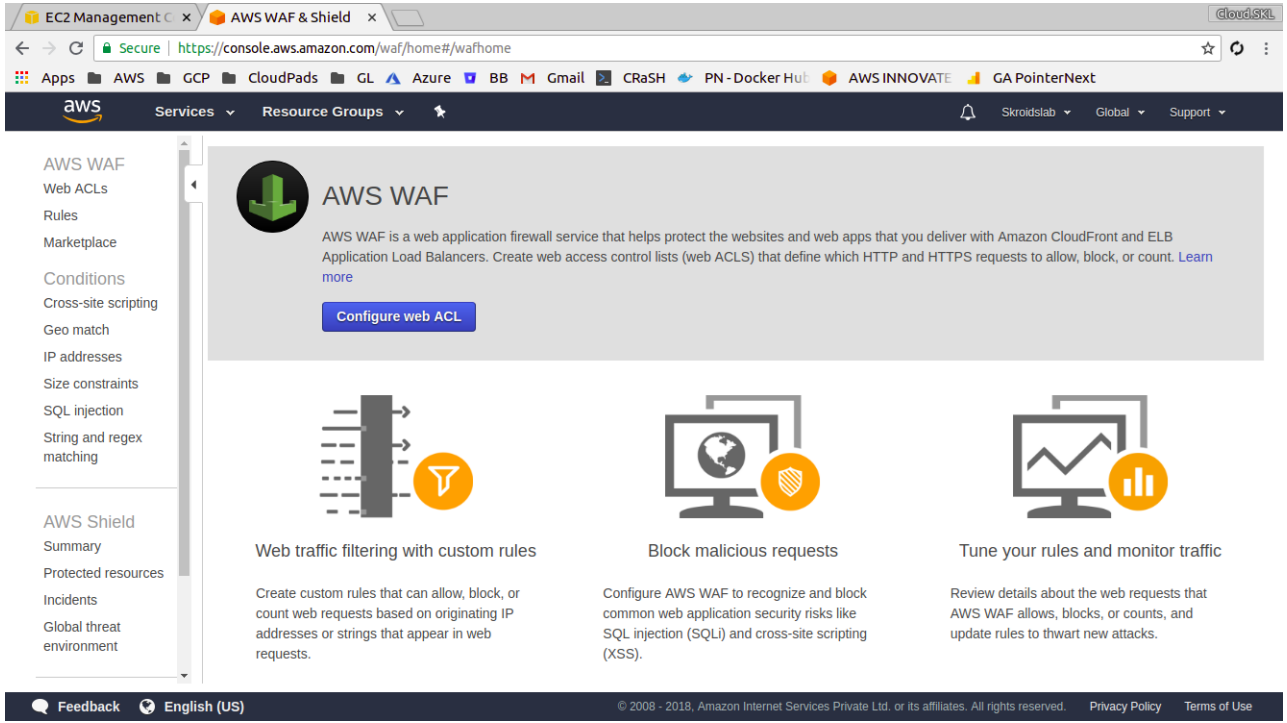
WAF can sit in front of LB or CDN

WAF

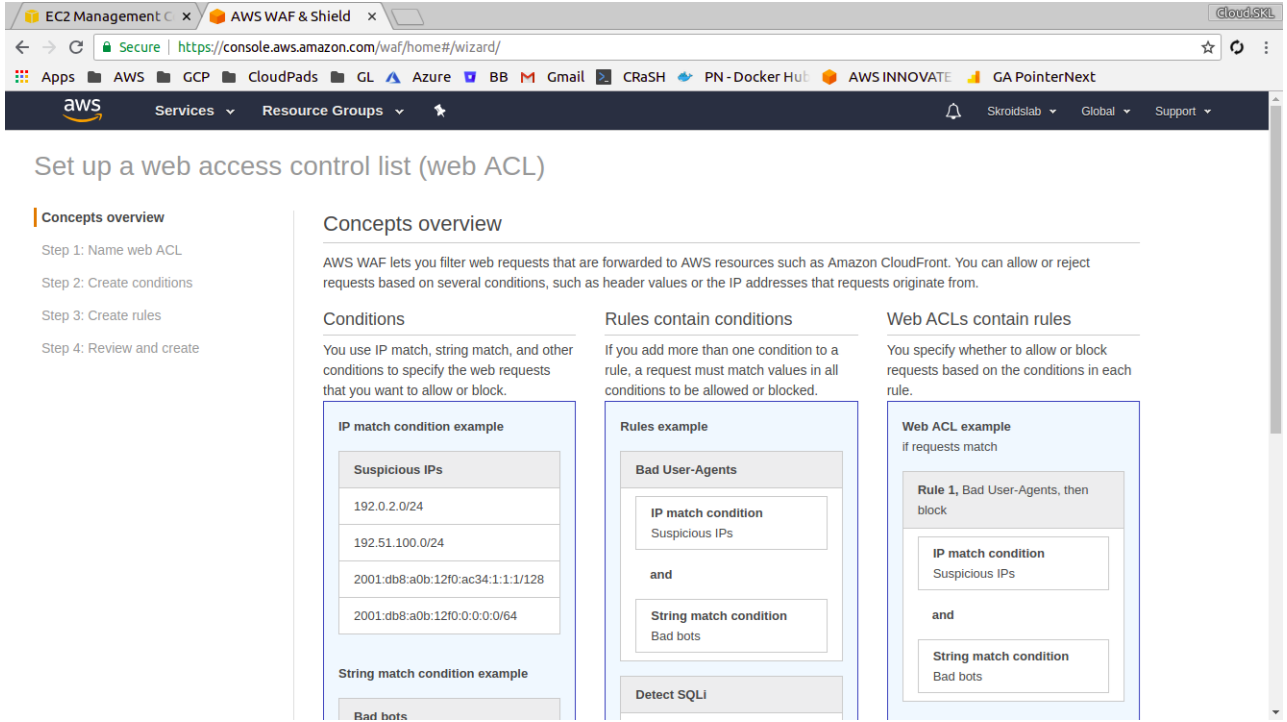


WAF

greatlearning



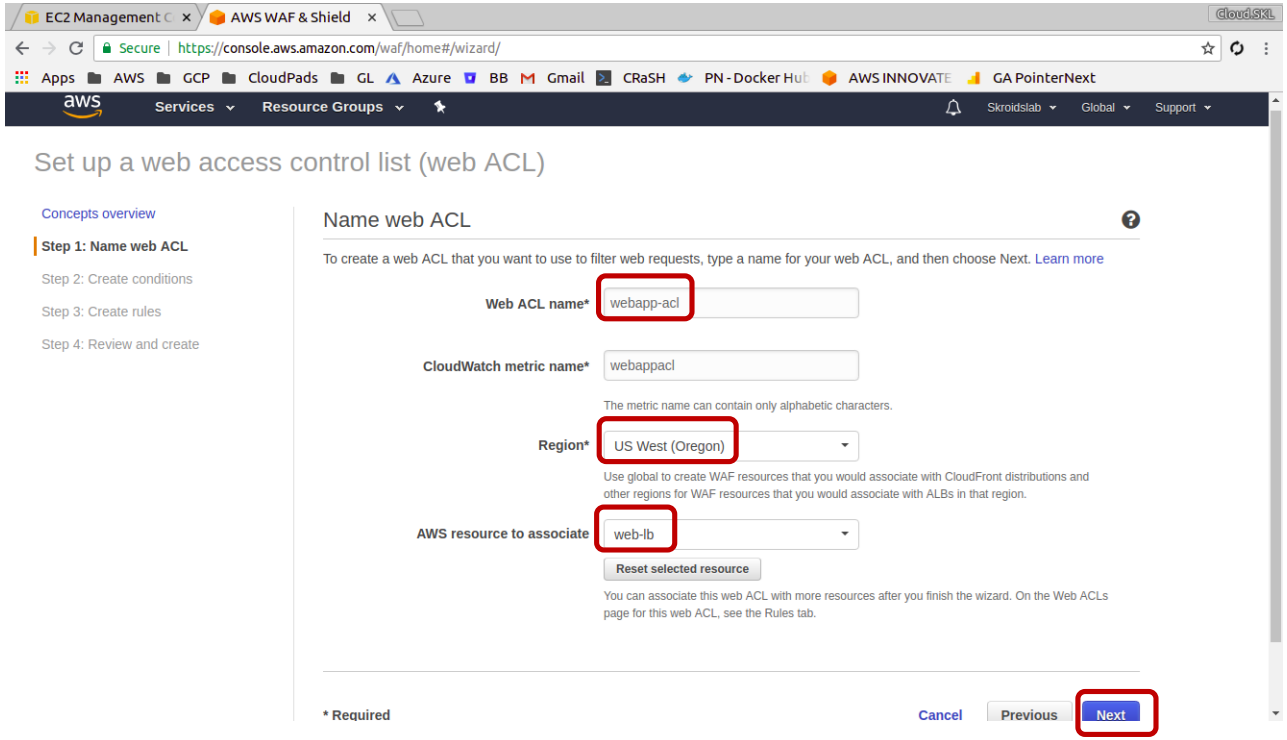
WAF - ACL



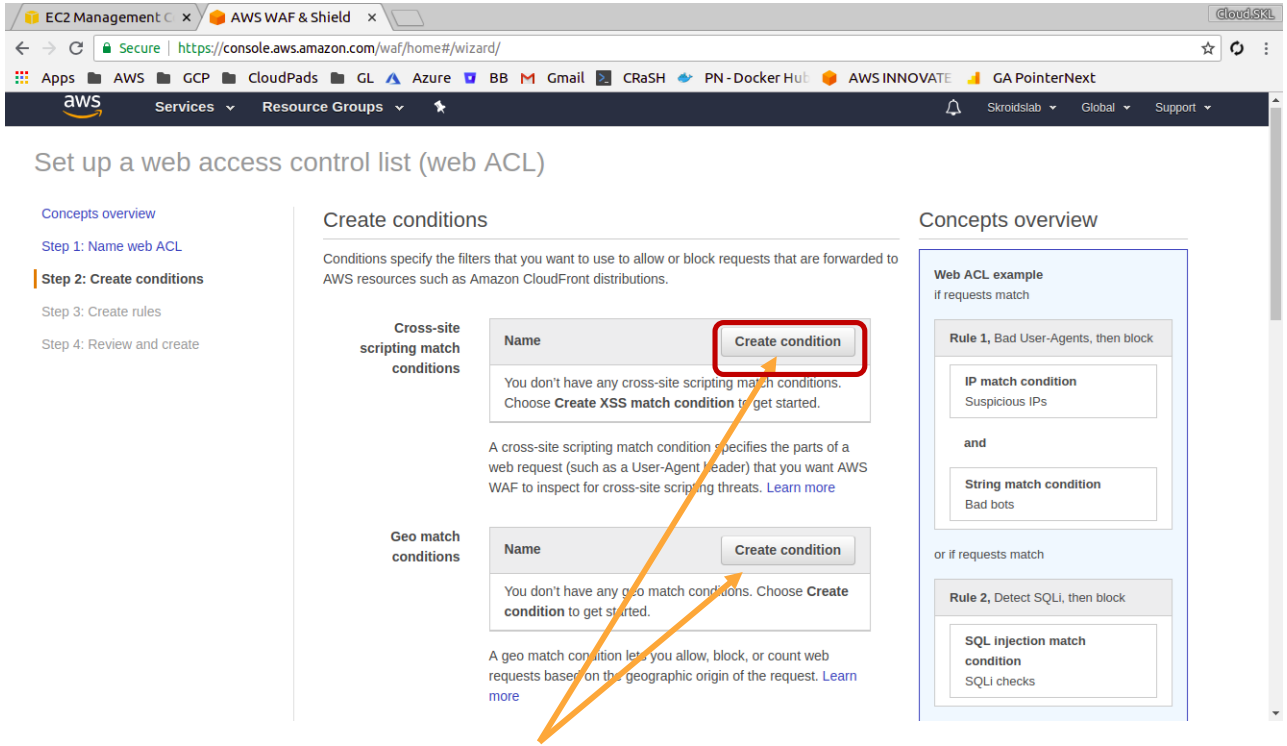
Scroll down and click "Next"

WAF - ACL

greatlearning



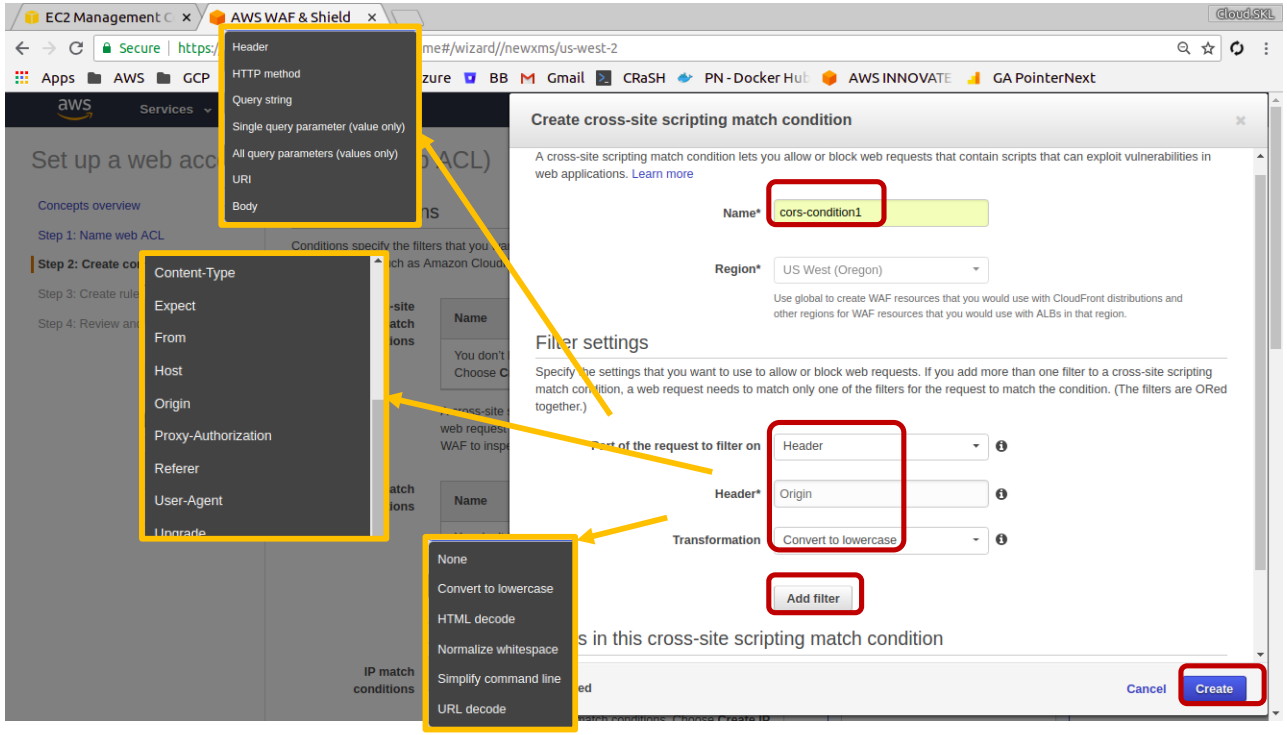
WAF - Conditions



Create multiple conditions by clicking on the appropriate "Create condition" button which will show an "overlay" window

WAF - CORS condition

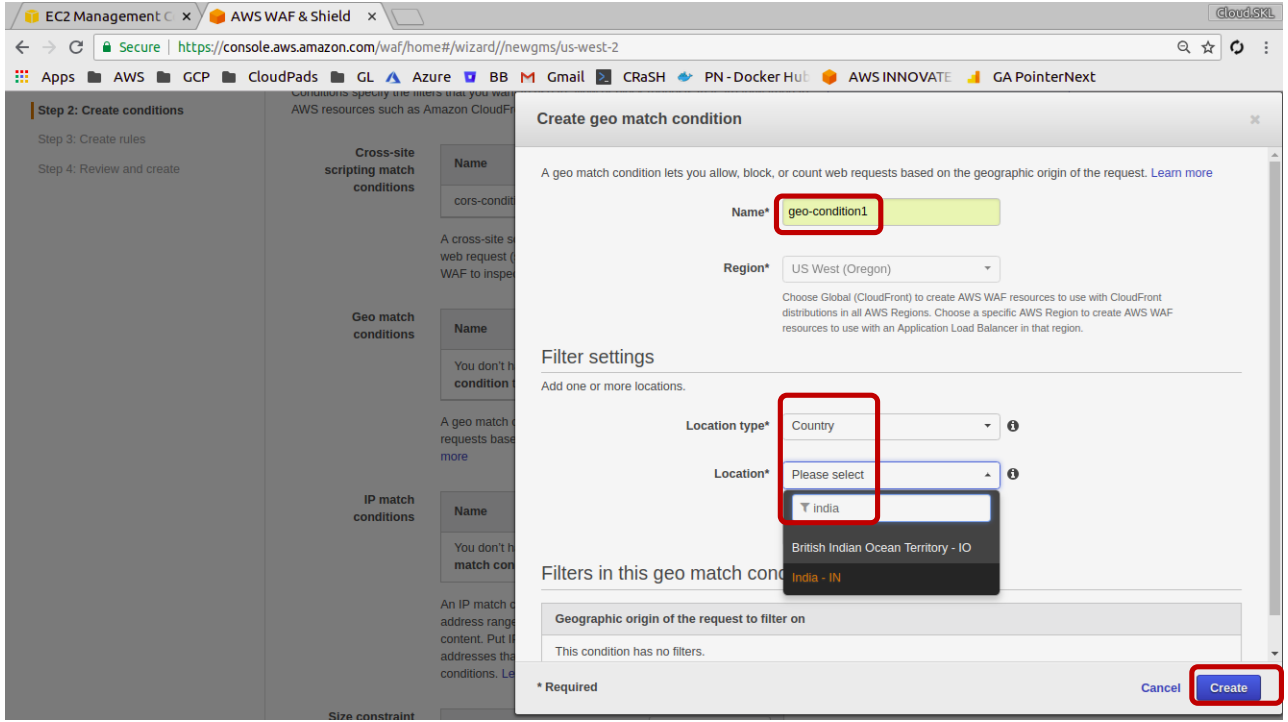
greatlearning



This flow remains the same for all conditions. Multiple filters are ORed together

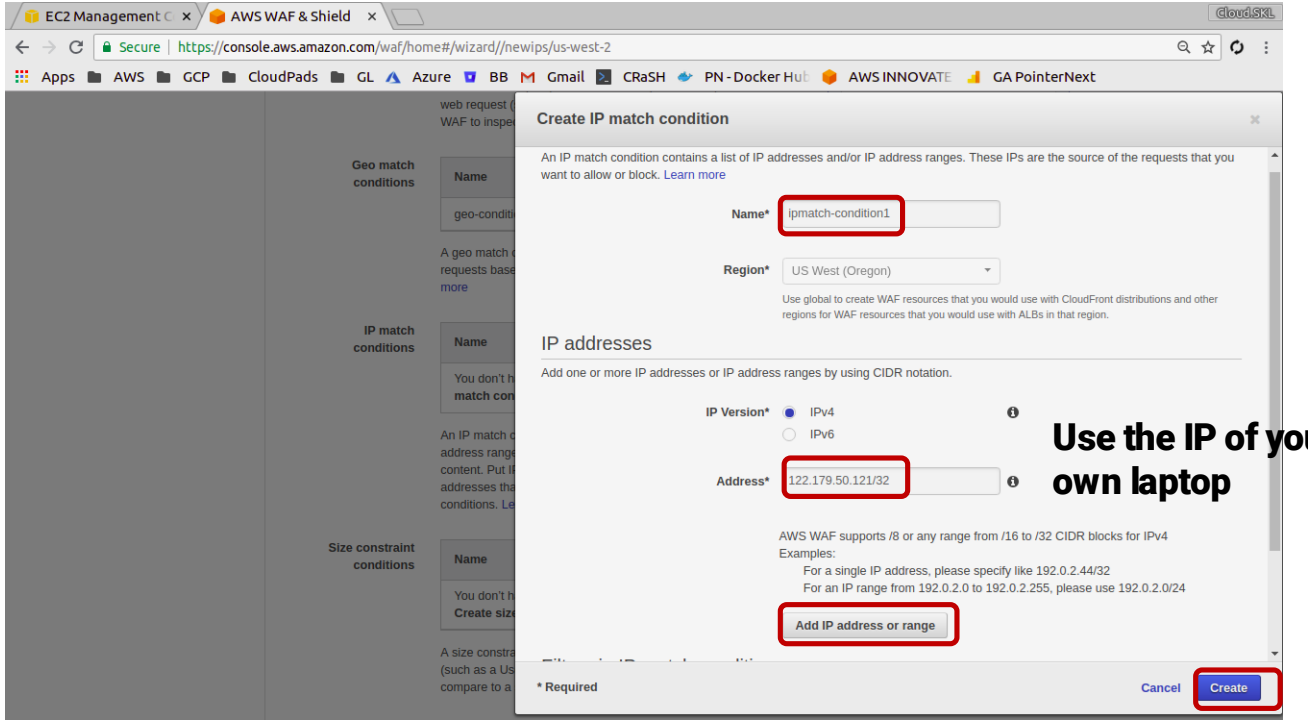
WAF - Geo/country condition

greatlearning



WAF - IP match condition

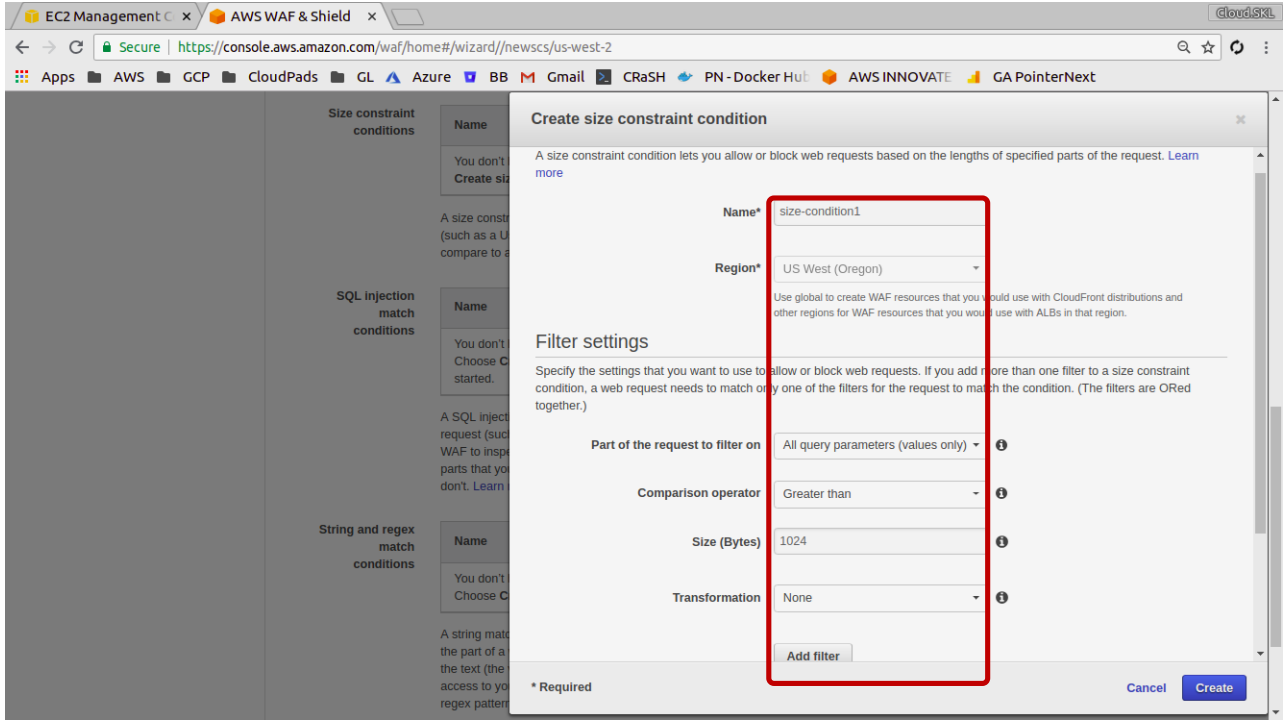
greatlearning



Use the IP of your own laptop

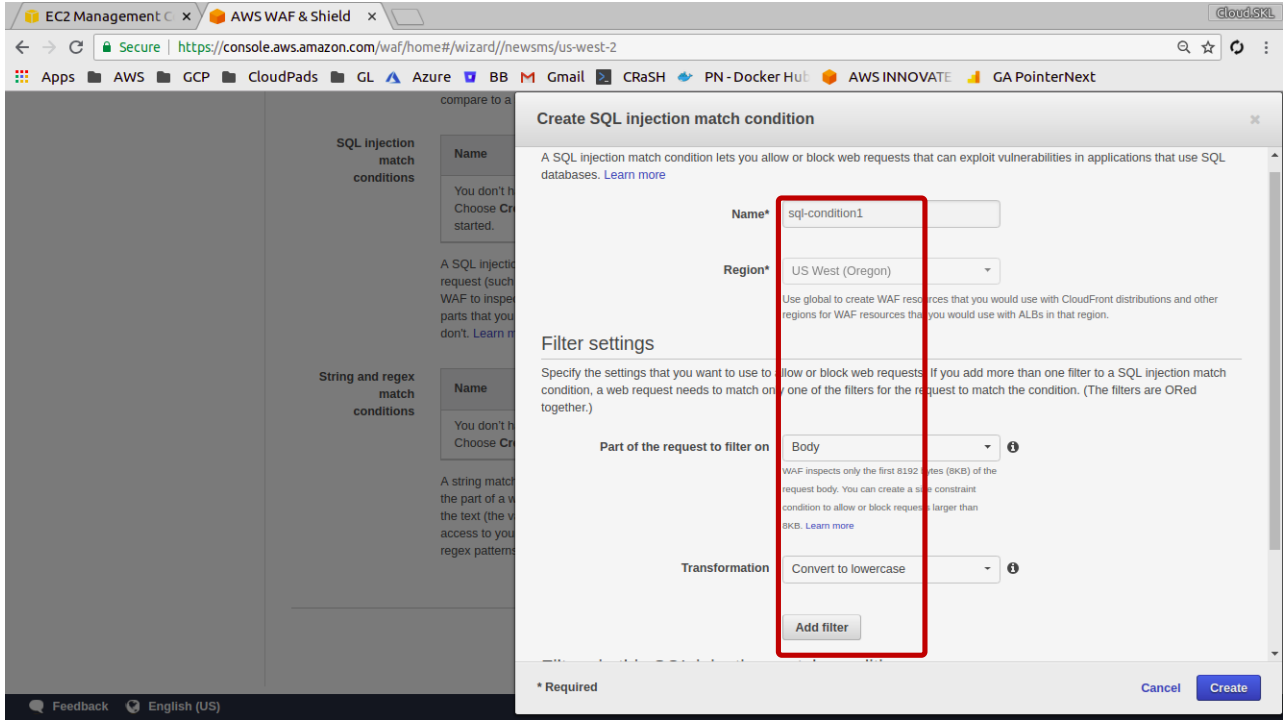
We will use this condition to allow traffic only from this IP

WAF - Size check condition

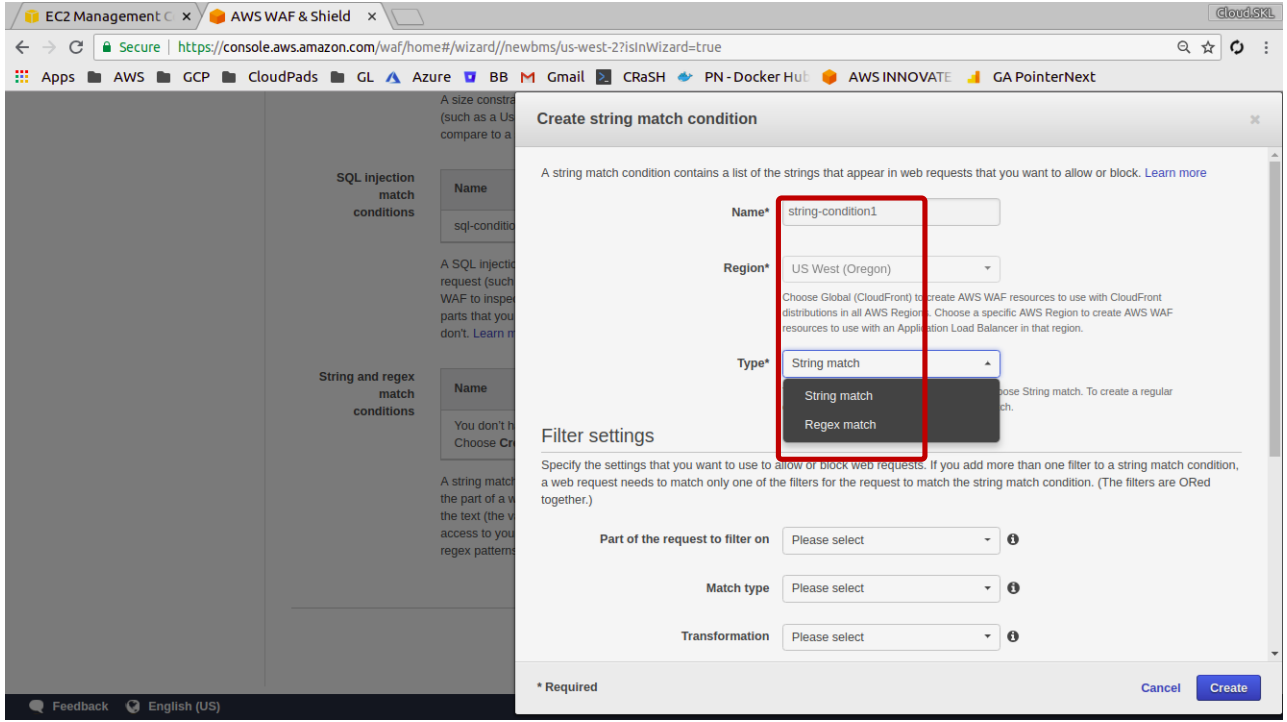


WAF - SQL injection condition

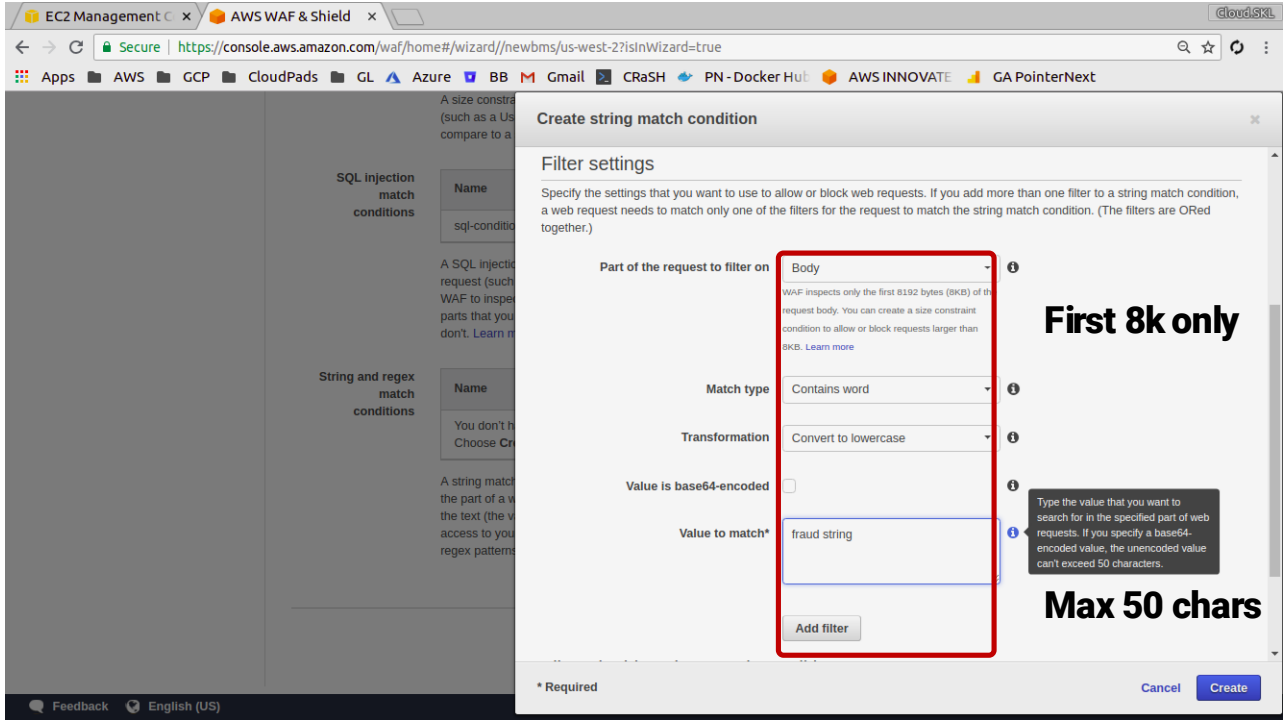
greatlearning



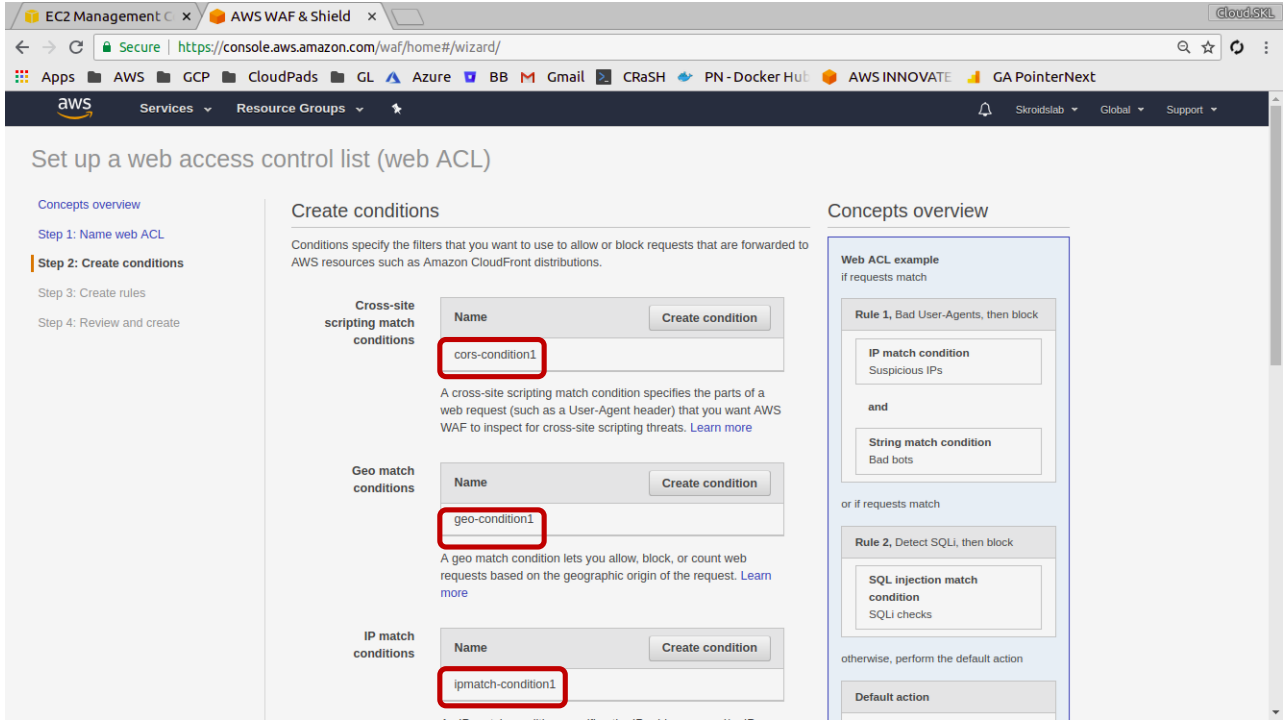
WAF - String match condition



WAF - String match condition

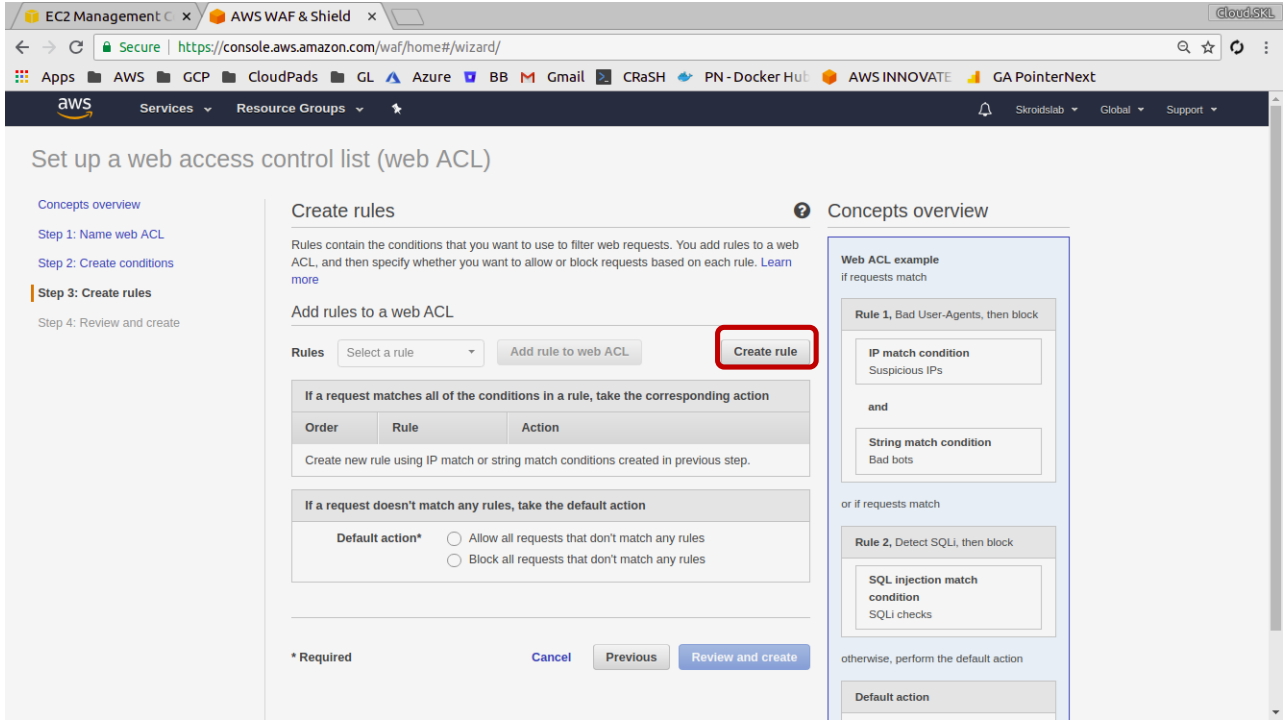


WAF - condition summary



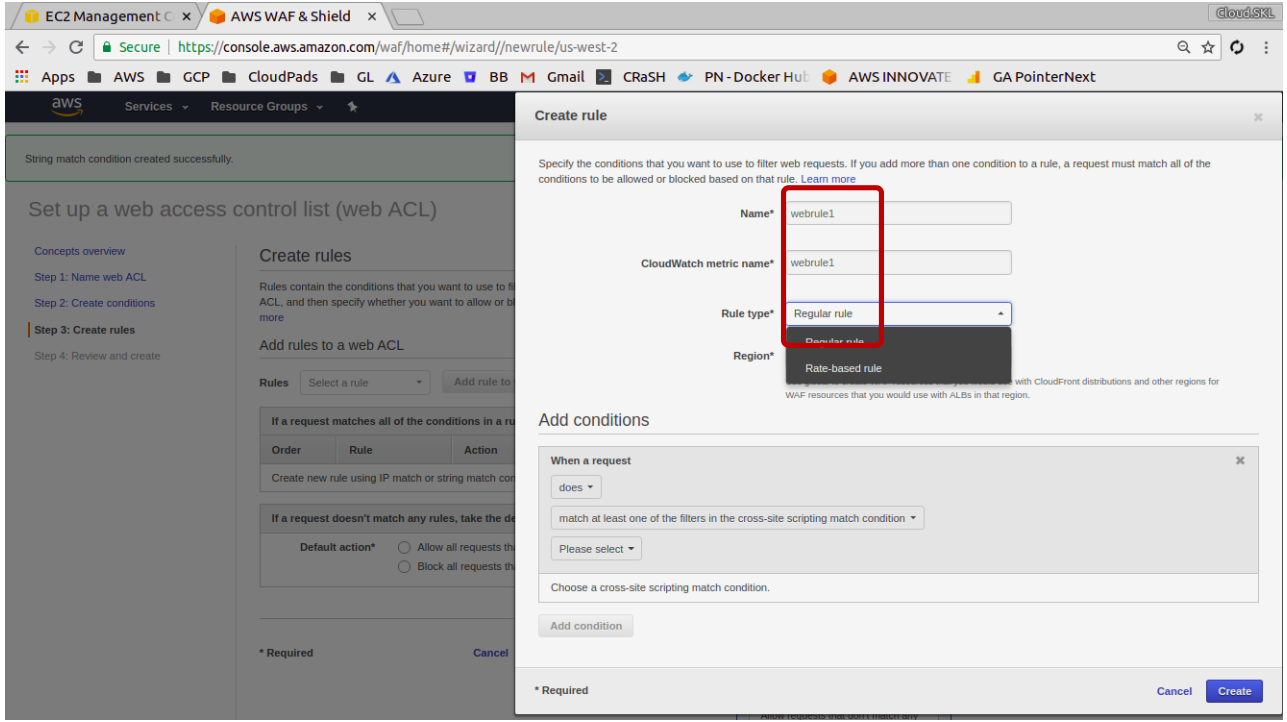
and other conditions. Scroll down and click "Next"

WAF - Rules

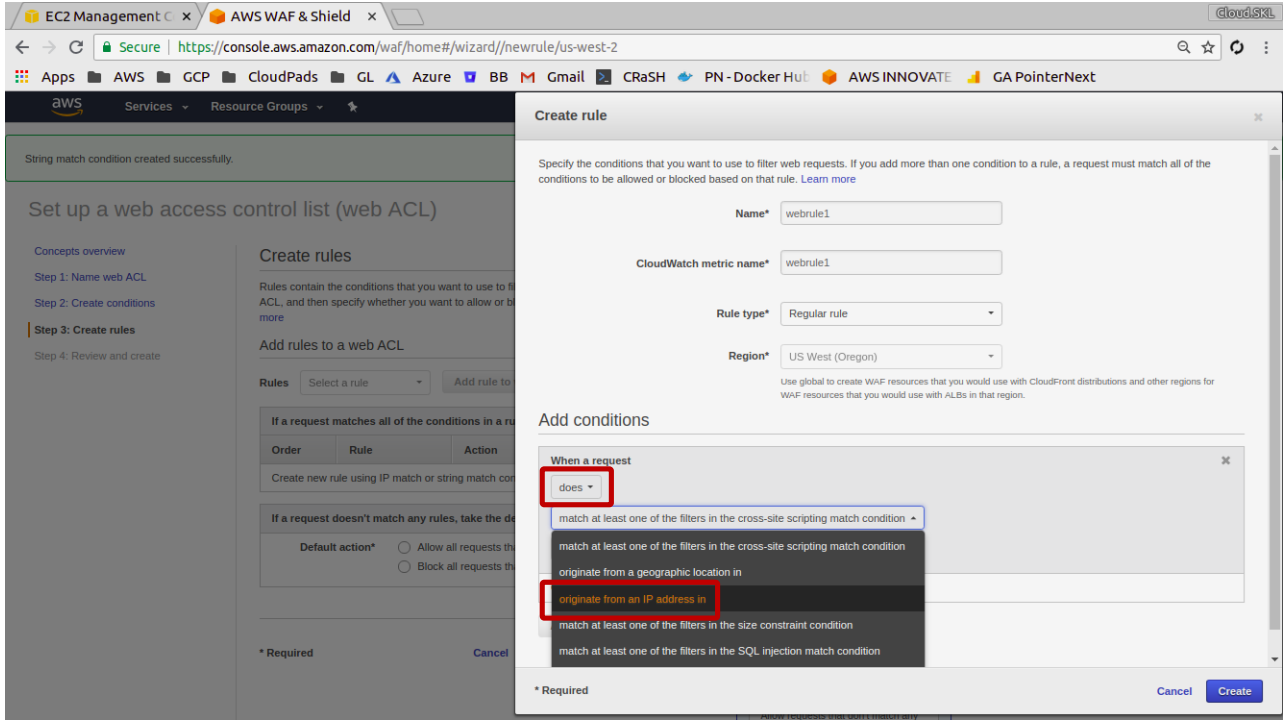


Rules will use the conditions defined earlier

WAF - Rules

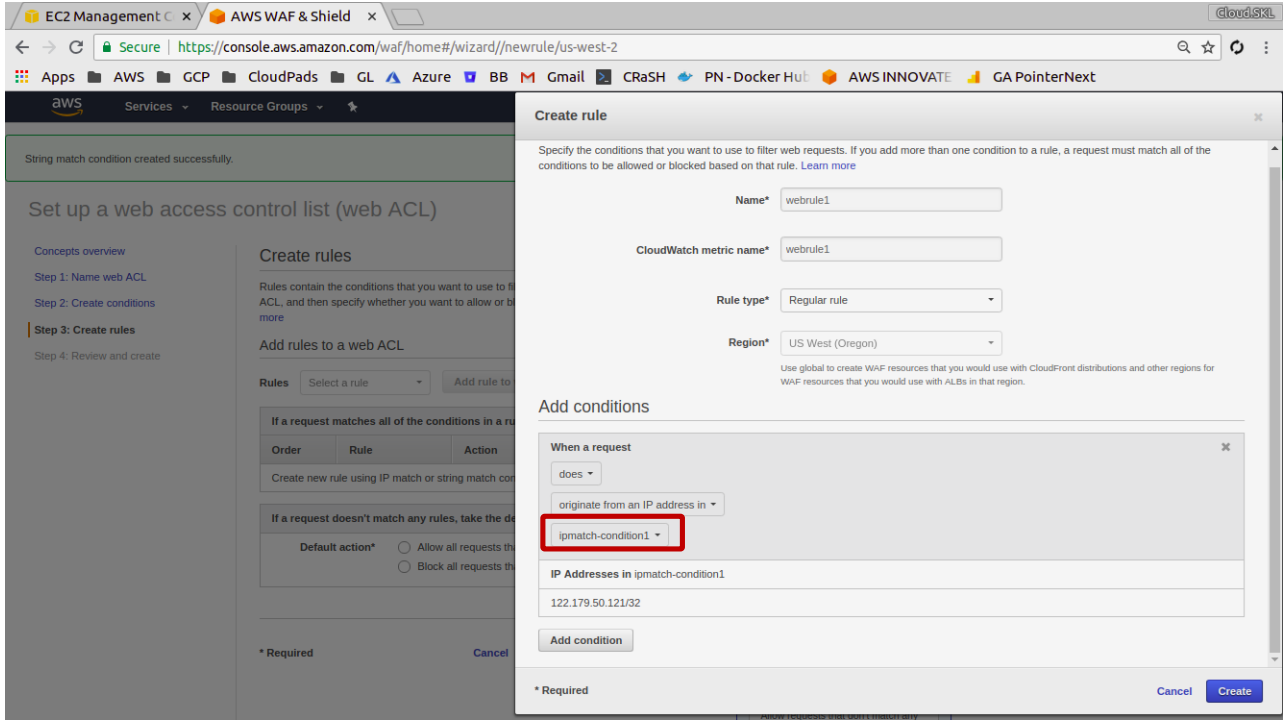


WAF - Rules

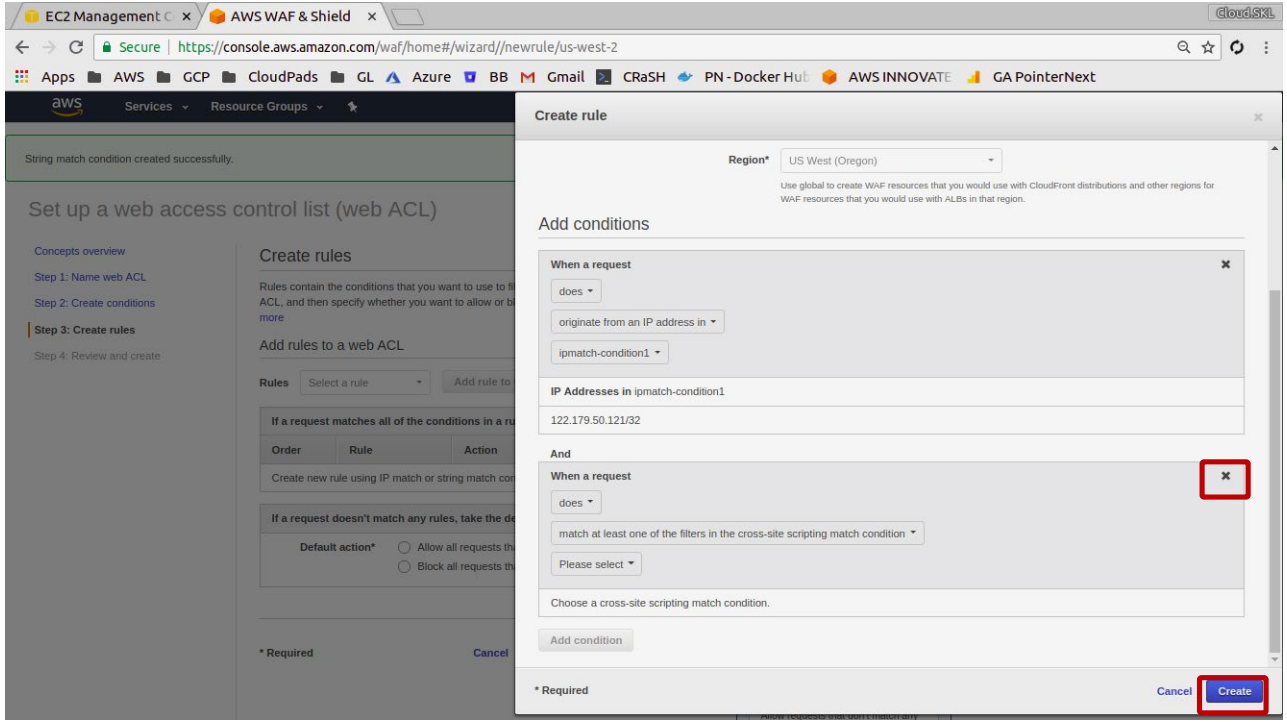


WAF - Rules

greatlearning

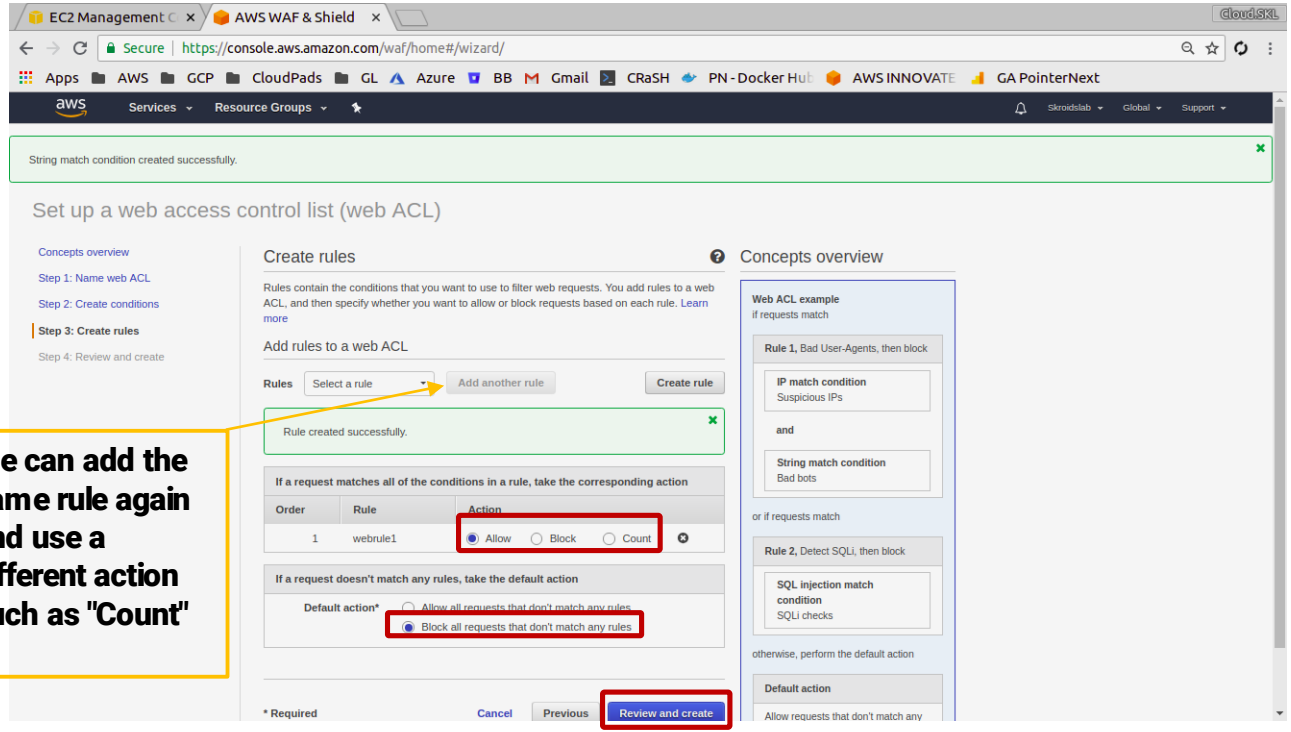


WAF - Rules



Another condition will be ANDed together
Remove the newly added condition!

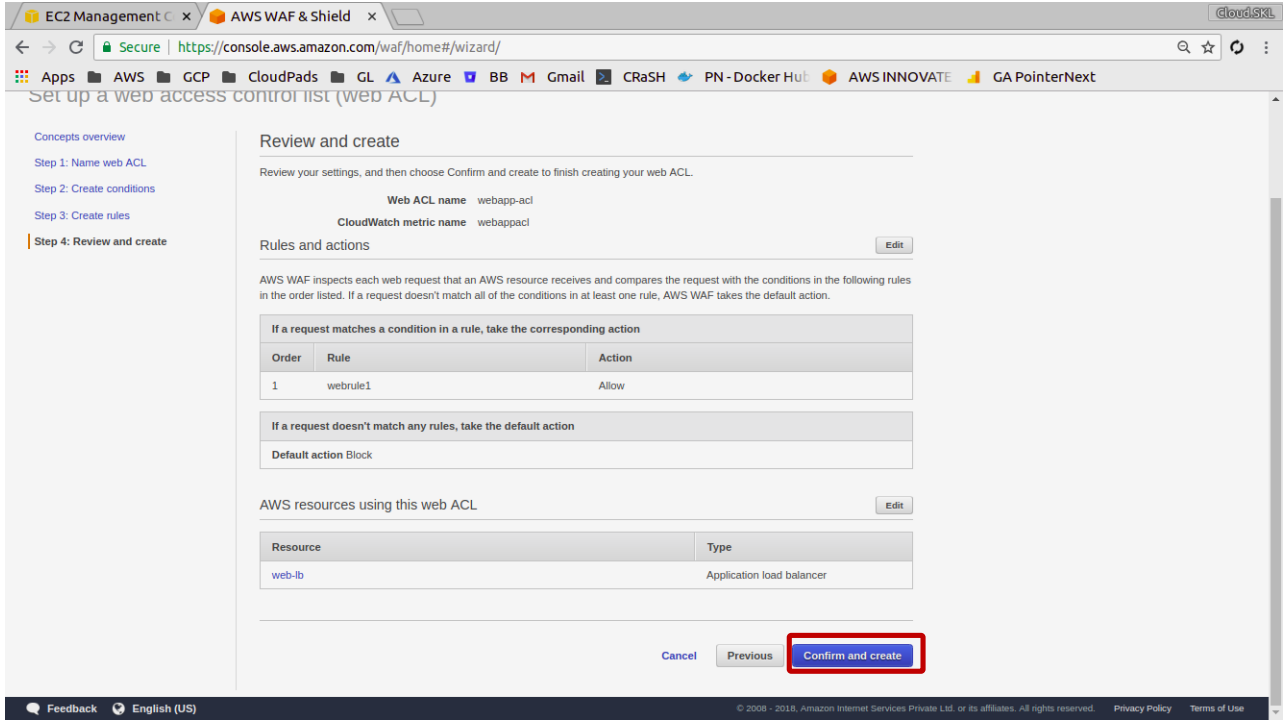
WAF - Rules summary



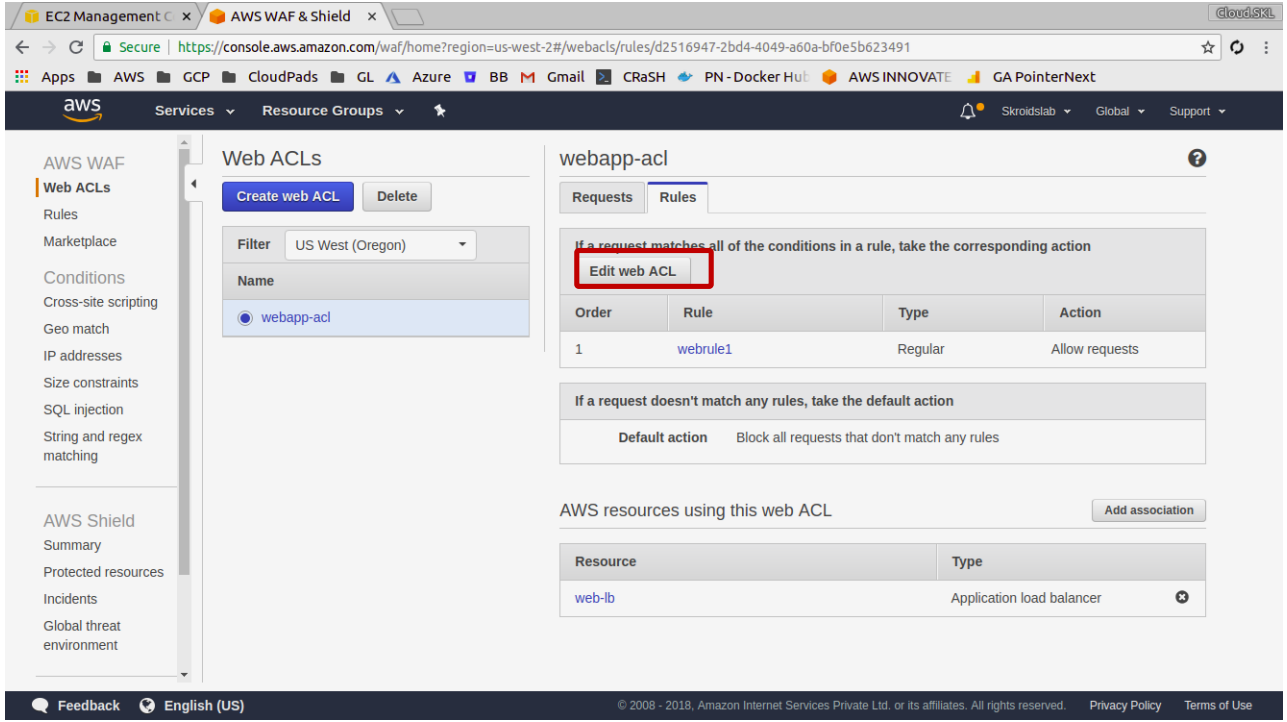
We can add the same rule again and use a different action such as "Count"

Change the action to "Allow" and default action to "Block". This will allow traffic ONLY from your laptop IP

WAF - ACL creation final step

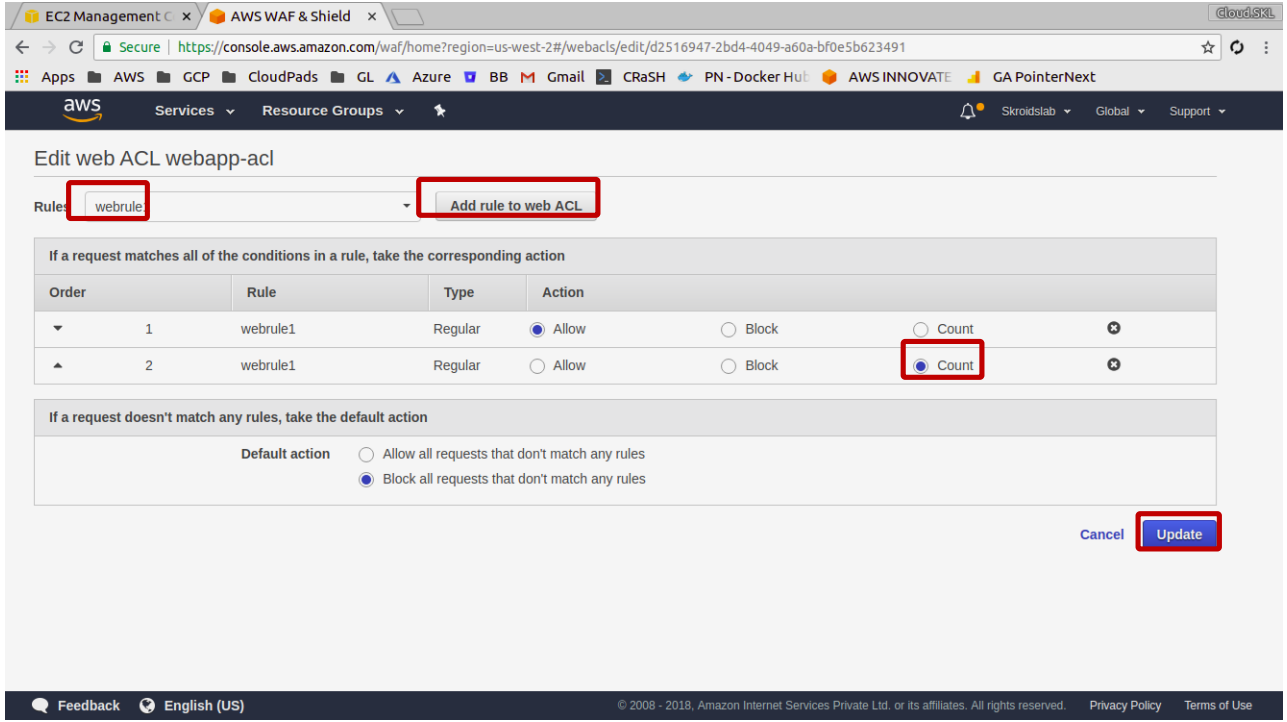


WAF - ACL summary



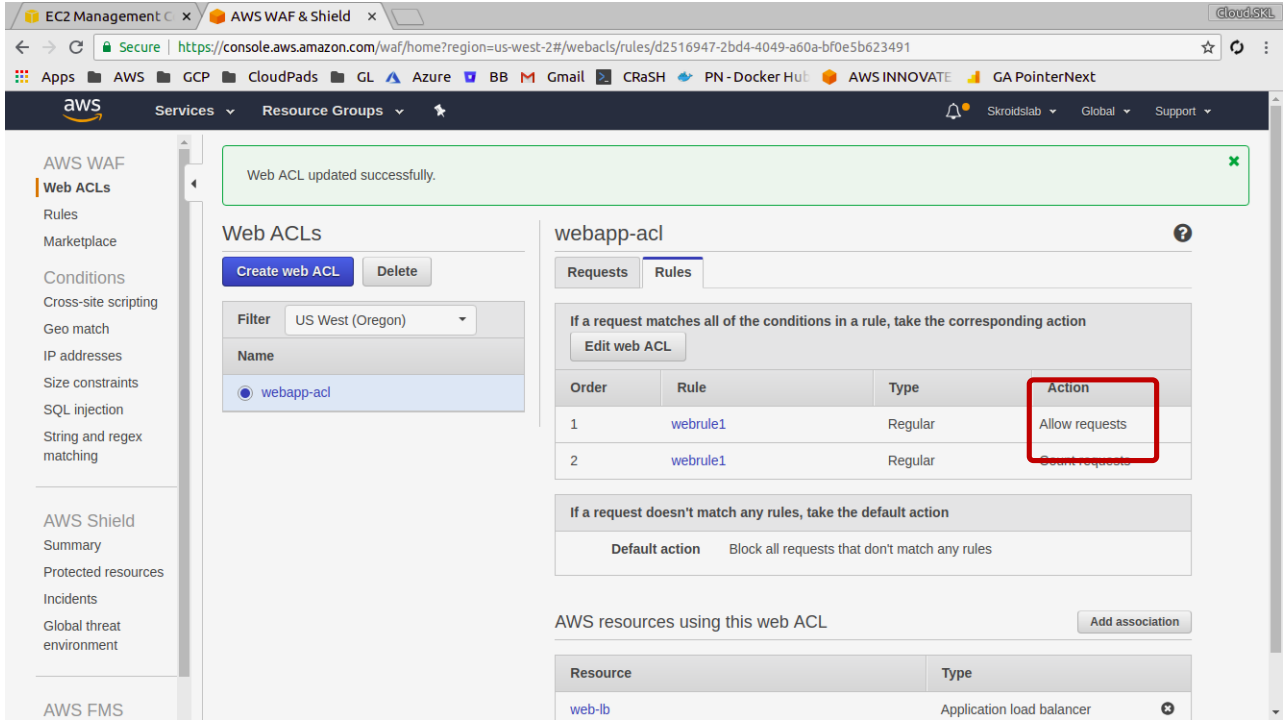
WAF

greatlearning



WAF

greatlearning

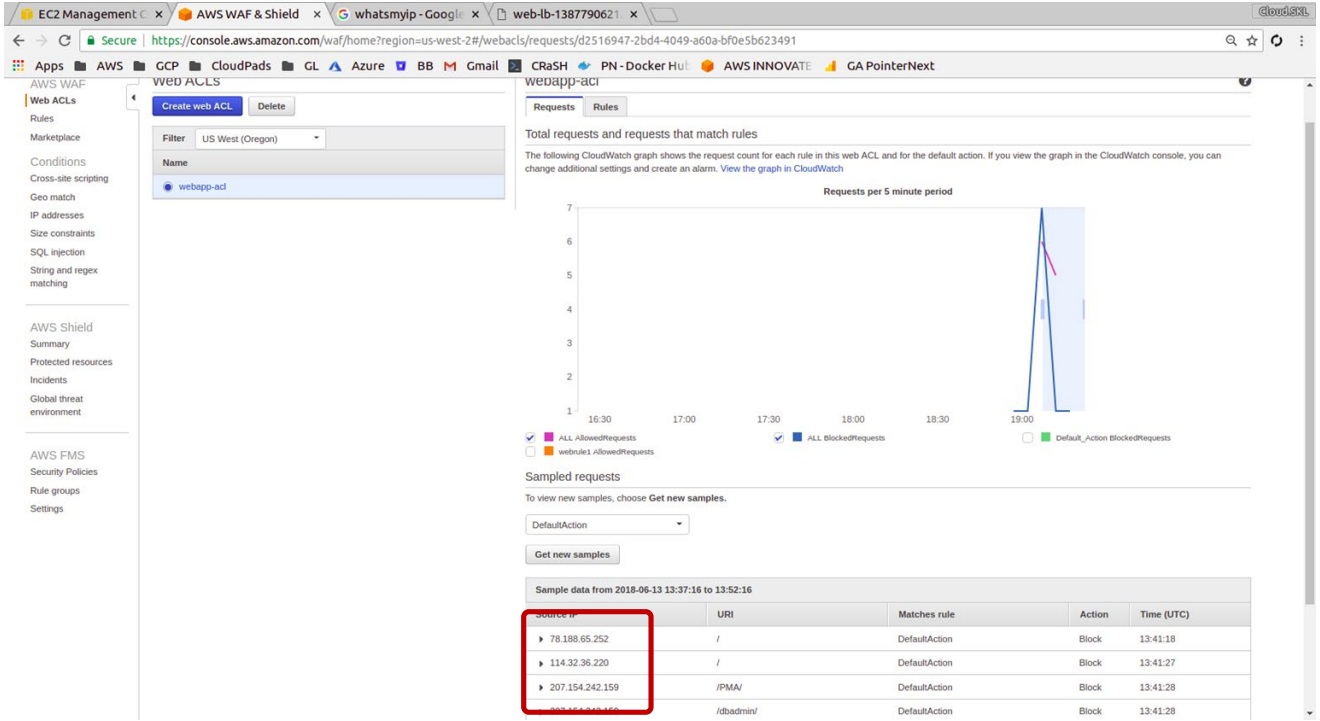


$5 per web ACL per month
$1 per rule per web ACL per month

WAF - Testing

- Hit the LB DNS and you will be able to access the site
- Refresh a few times to increase the count of hits
- Go back to WAF and see the graph and "Get new samples"
- If the screen is not refreshing with data then wait for 10 mins
- Update the rule and change it to block the requests from YOUR laptop IP and see the samples show blocked requests!

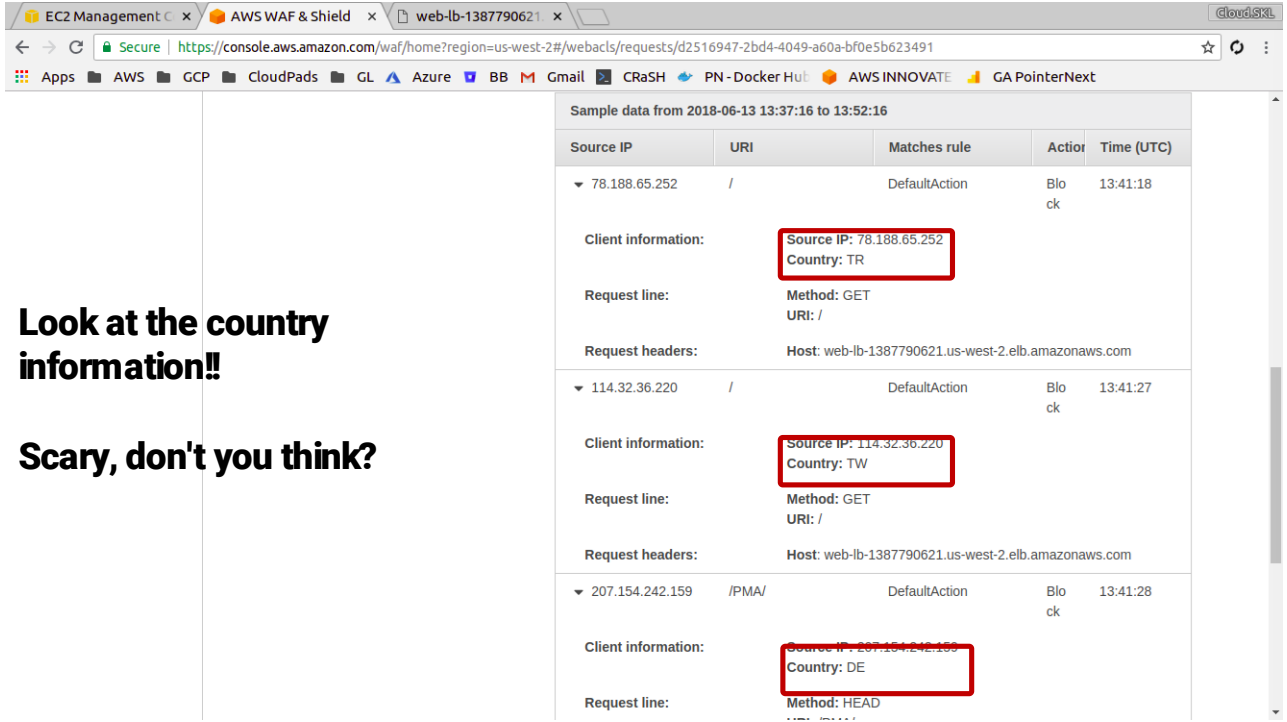
WAF



In a matter of minutes you can see sites being blocked!!!
See next ...

WAF

greatlearning



Look at the country information!!

Scary, don't you think?

WAF - Cleanup

- We have to remove all rules
- Remove conditions
- Delete rules
- Remove the LB association
- Delete the ACL
- Delete the rule condition(s)
- Delete the rule
- Delete the conditions
- Remove the LB,TG and EC2 instance

greatlearning

Compute - Part I

Boot volume and Instance types

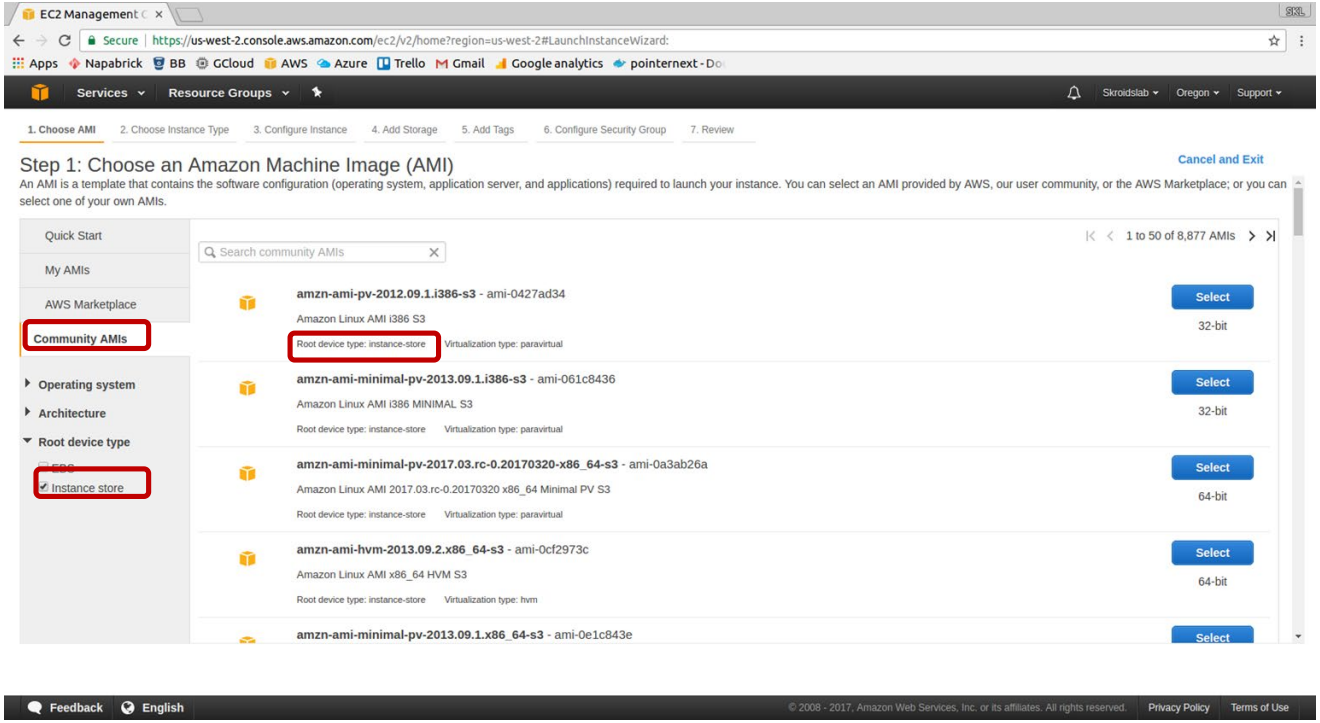
EC2 - Boot volume types

greatlearning

- Type 1 - Backed by EBS (common choice)
  - Can be attached at the time of launching or after launching
  - Can stop the instance
  - Snapshot the disk
  - In case of any AWS failure, stop the instance and start it again, EBS survives and the instance is created on a different VM
  - Can detach and attach to another instance
  - Termination protection is available (delete host retain boot volume)
- Type 2 - Instance store (Ephemeral store)
  - Can attach instance store ONLY at the time of launching
  - Can only reboot or terminate the instance
  - If there is an instance problem then you lose the instance store based volume (less durability than EBS)
  - Cannot detach and attach to another instance
  - No termination protection

EC2 - Boot volume types

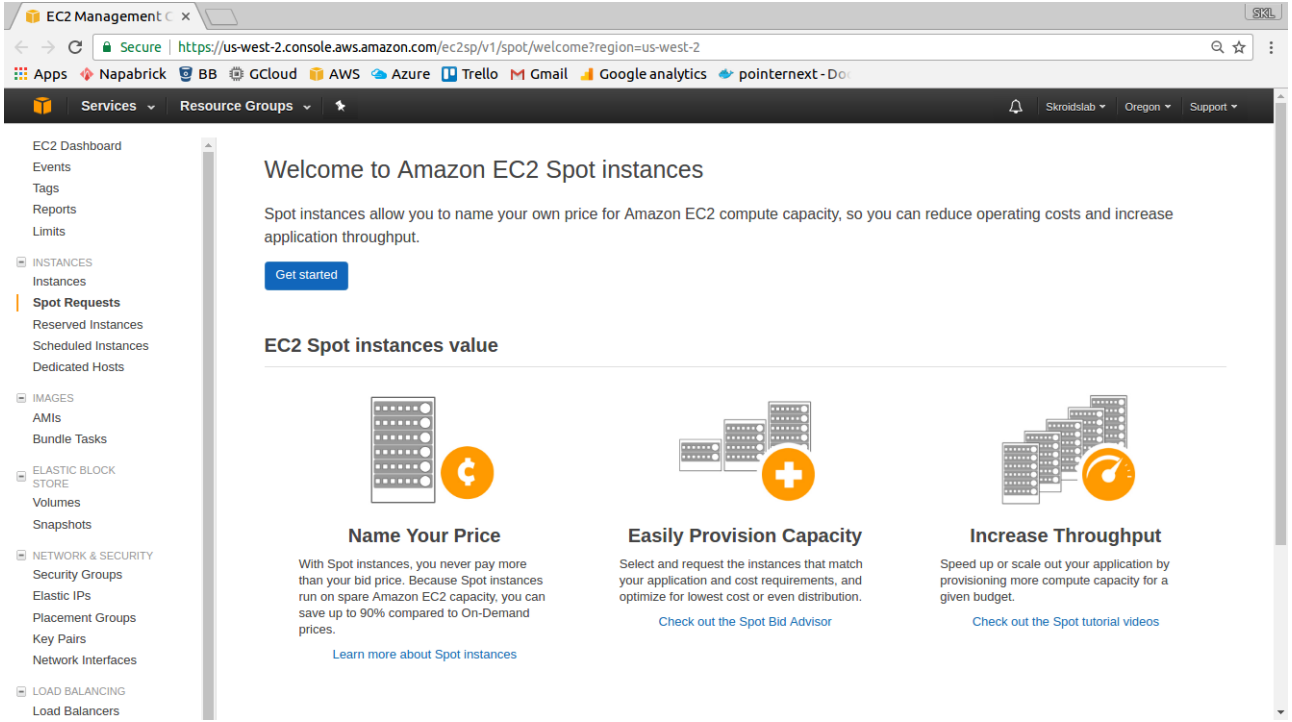
greatlearning



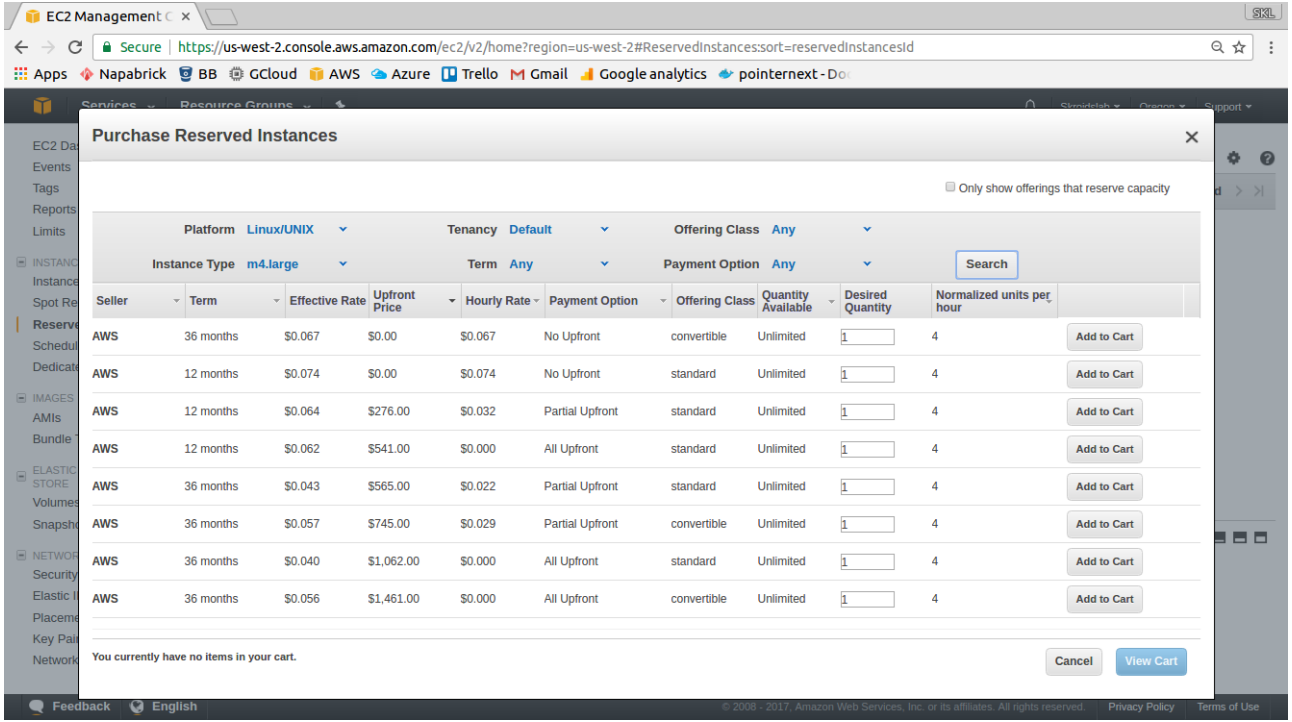
Get an instance store based EC2 instance

EC2 - Other types of instances

greatlearning

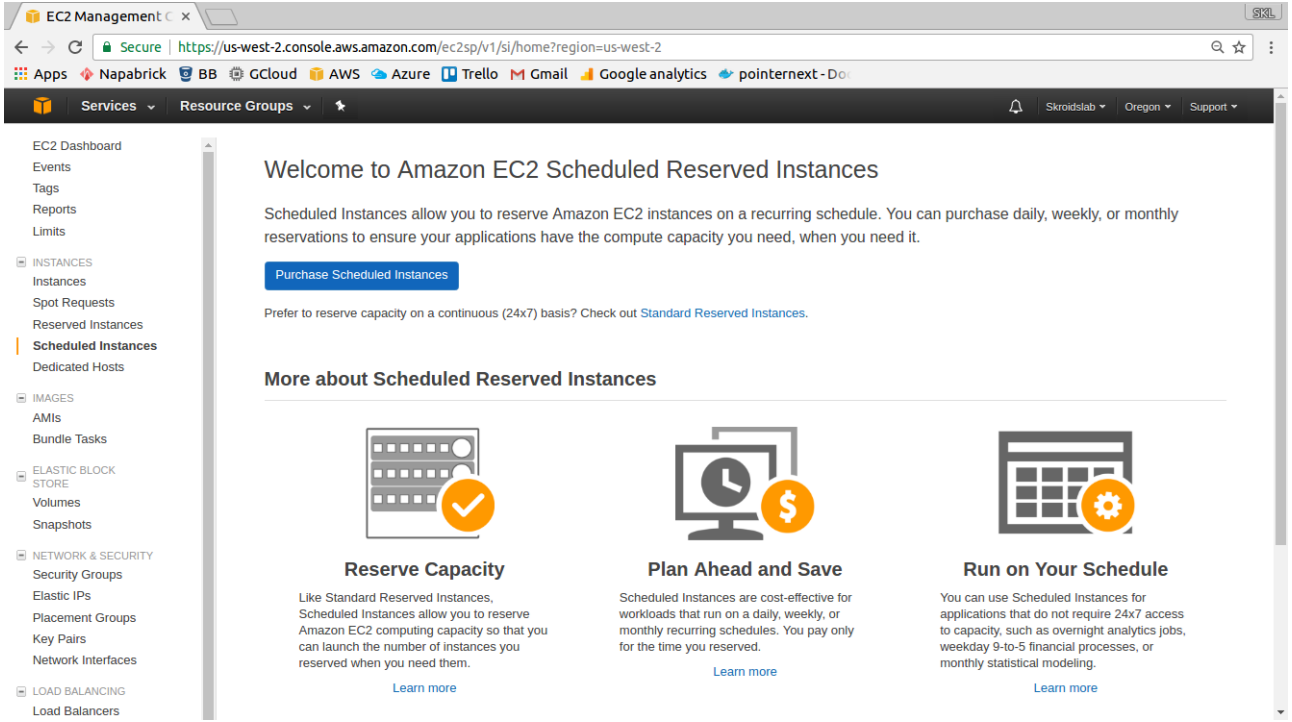


EC2 - Other types of instances

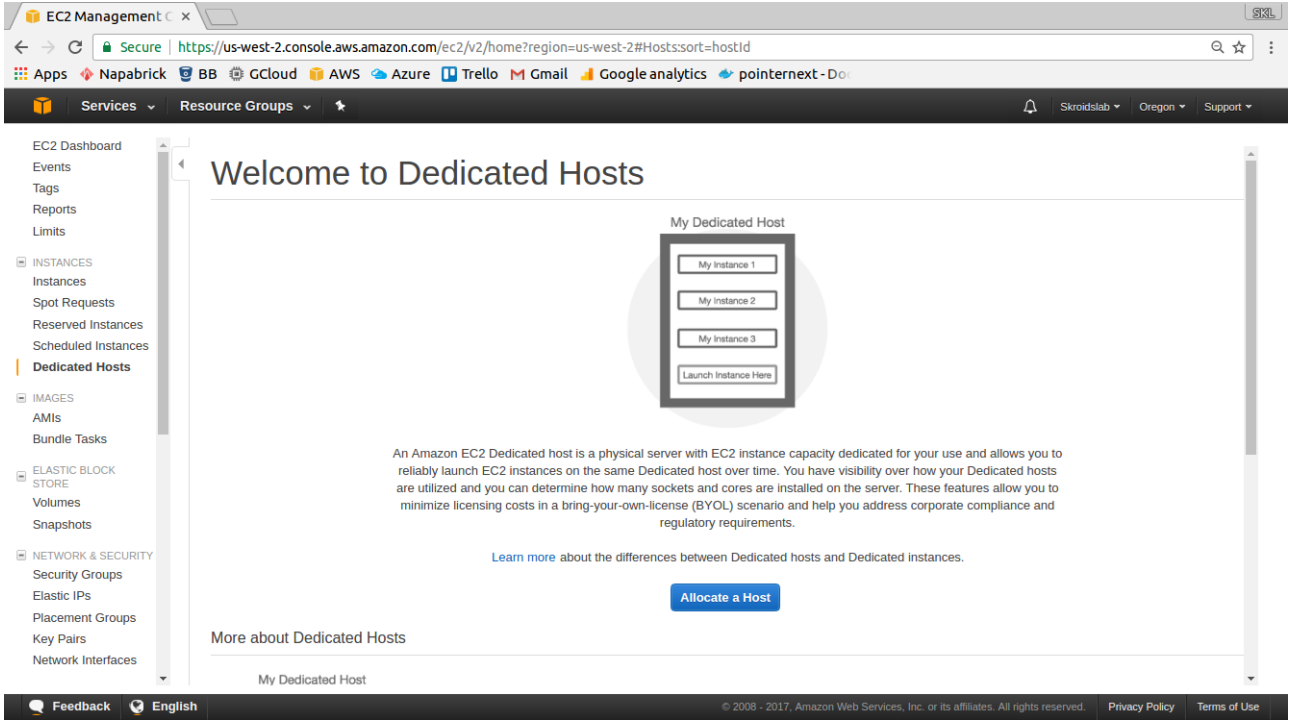


EC2 - Other types of instances

greatlearning



EC2 - Other types of instances

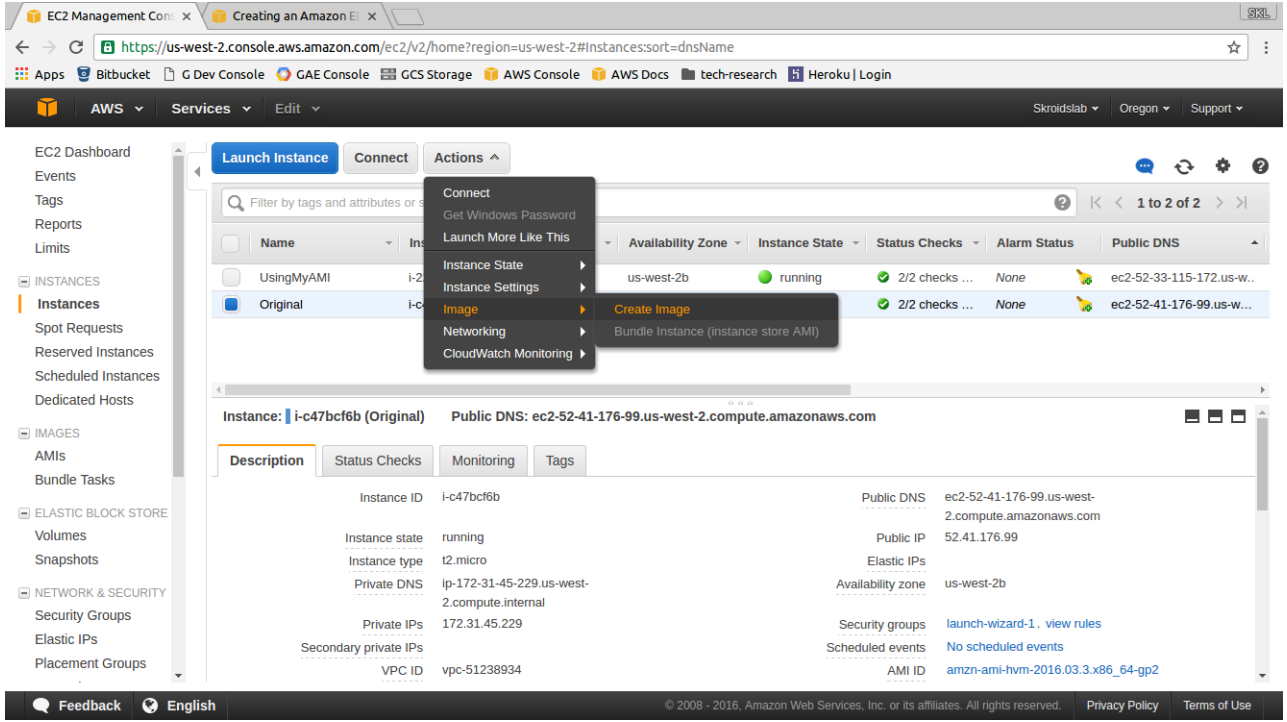


greatlearning

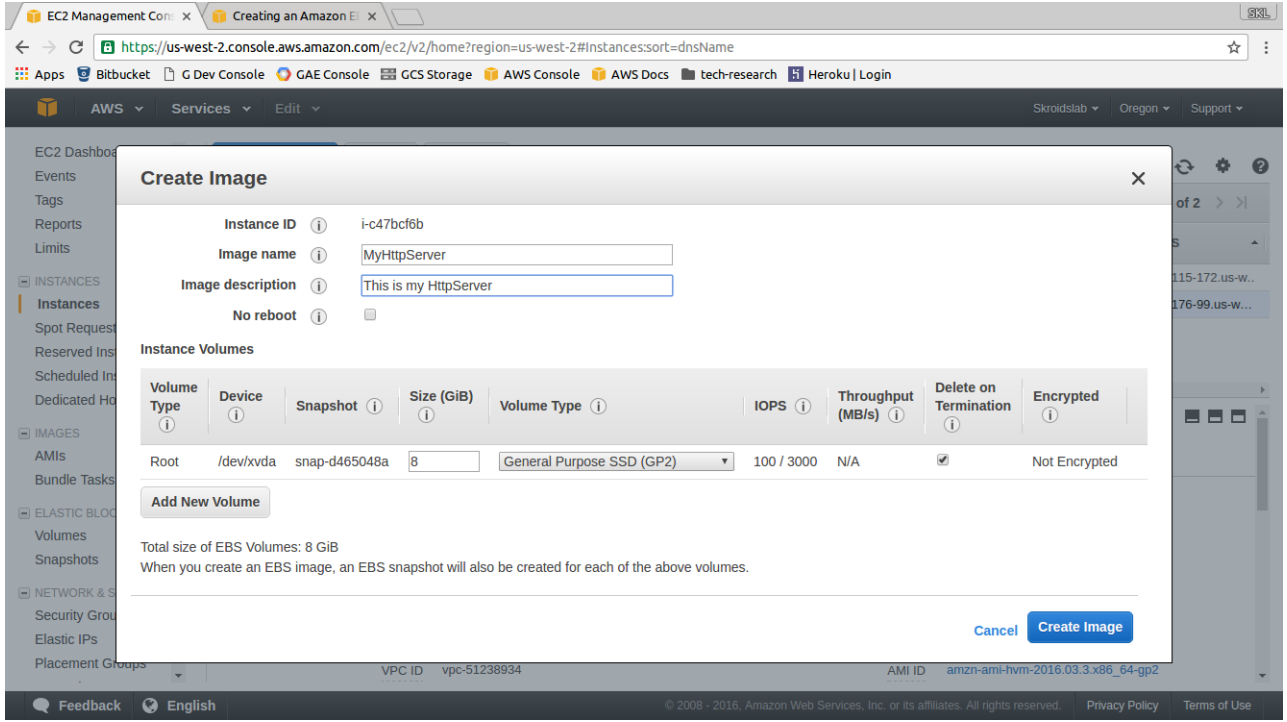
Compute - Part II

AMI

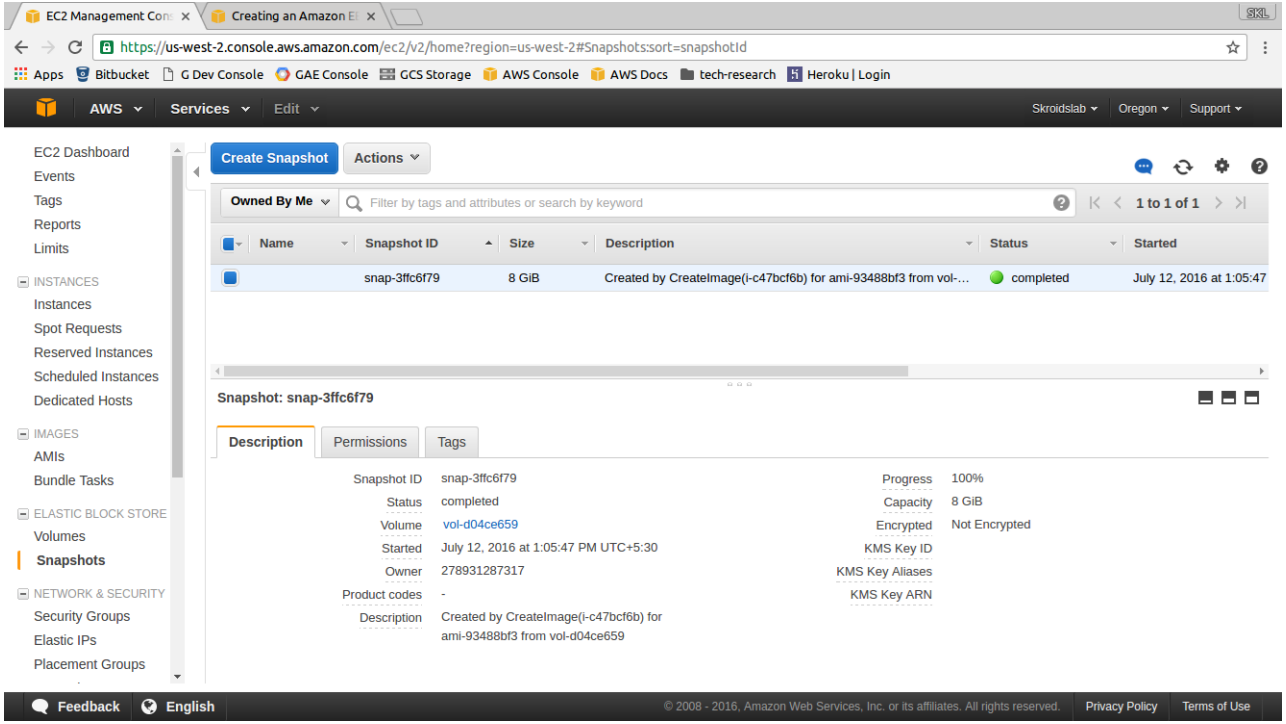
Activity - AMI from an existing instance



Activity - AMI

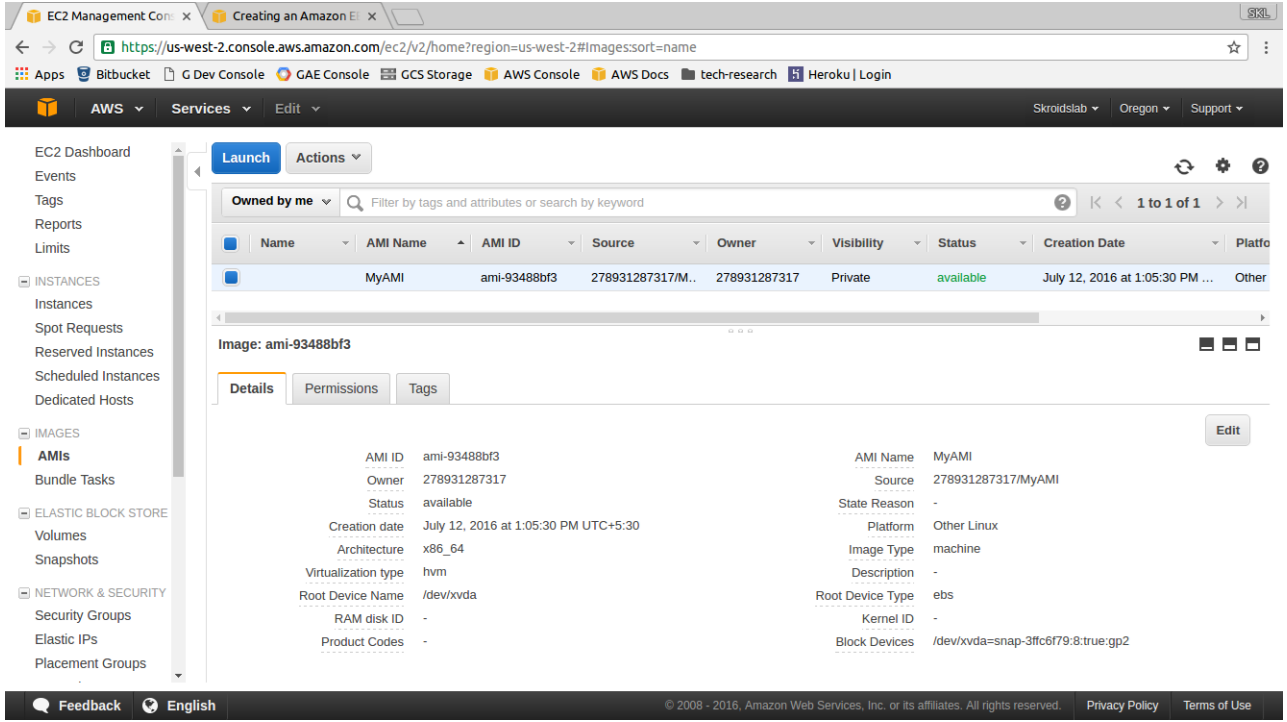


Activity - AMI (auto snapshot created)



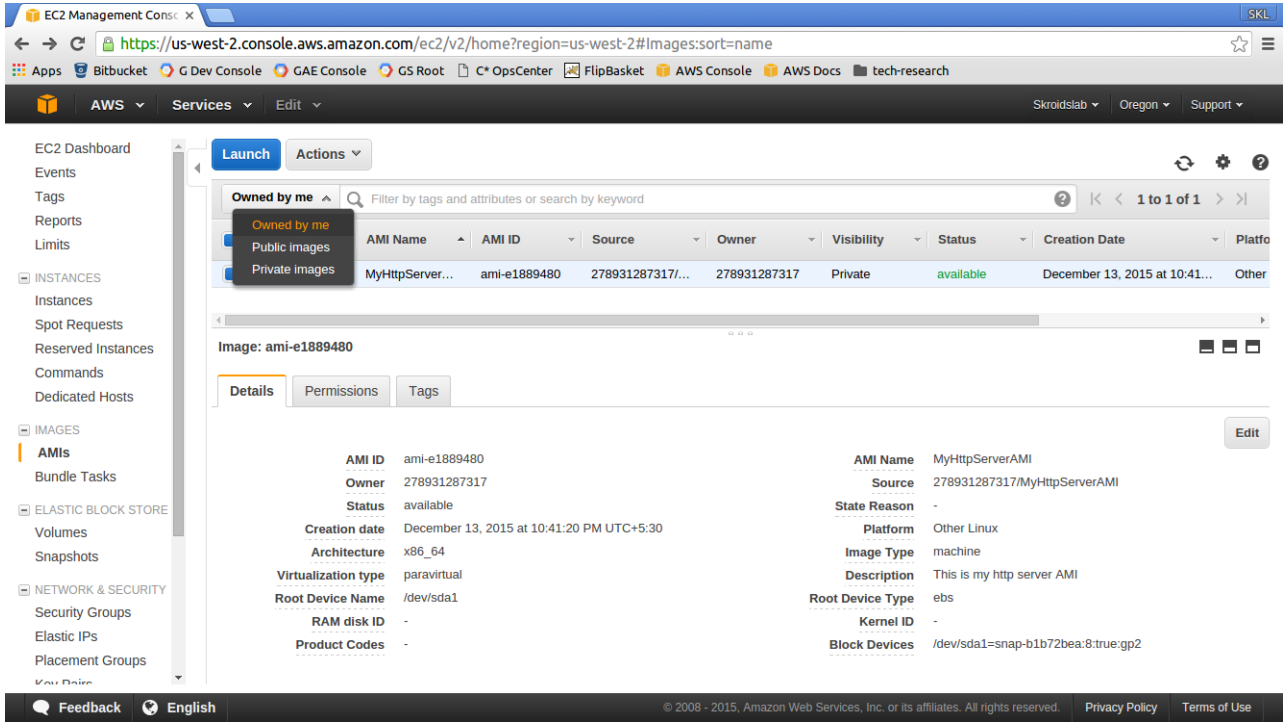
Activity - AMI

greatlearning



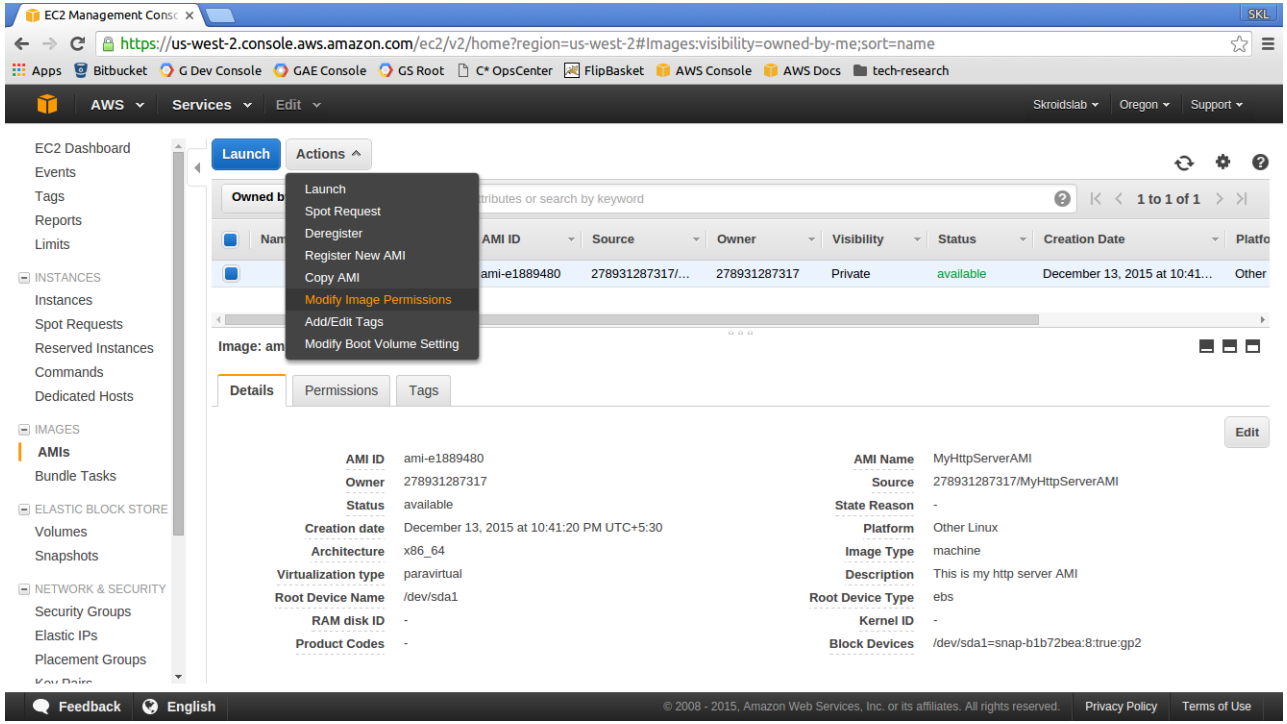
Activity - AMI

greatlearning



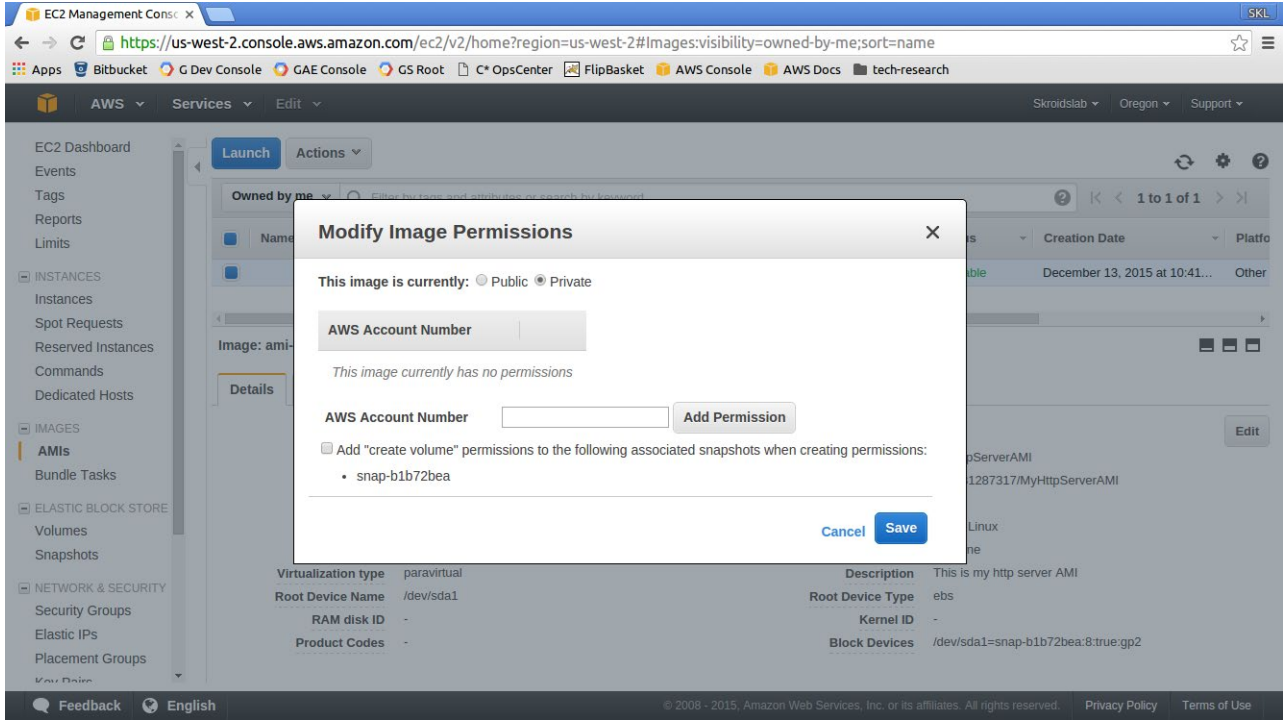
Activity - AMI

greatlearning



Activity - AMI

greatlearning



Activity - AMI

- AMIs are region specific, can only launch instances in the region where the AMI is stored
- Can copy AMIs to other regions via the console
- Can upload your own AMI built from other options such as a virtualization software
    - Have to convert to AMI manually using CLI
- Security precautions in case of public AMIs
- https://aws.amazon.com/articles/public-ami-publishing-hardening-and-clean-up-requirements/
- This for the main part falls in the devops section

greatlearning

Compute - Part II

CLI and bootstrap scripts

Activity - CLI setup

greatlearning

- The CLI works OOB in an instance that has the Amazon Linux AMI OR can be installed on the local machine as follows
  - $ sudo apt update
  - $ sudo apt install python-pip (or python-pip3 optional in case pip is not there)
  - $ sudo pip install awscli *
  - (Mac->) $ sudo easy_install pip
  - (Mac->) $ sudo pip install awscli –upgrade –ignore-installed six
- Login to the instance (ssh -i <pem> ec2-user@<dns>) and

  $ sudo su

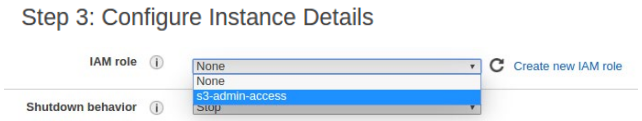
  # aws s3 ls
- The instance will not be able to access the bucket
- Do the following to setup the access (possible on your laptop as well)
  - $ aws configure
  - Create & enter the key etc of the user "CloudRoot" (Administrative policy attached)
  - Use the region as "us-west-2"
  - Inspect the files in the ~ folder under .aws subfolder (created because of aws configure)
  - The file "config" contains the region (In case the region was specified)
  - The file "credentials" contains the keys (huge security risk, also have to change in case the pwd is changed, solution is to use roles)

Activity - CLI

- "$ **aws s3 ls**" and you will be able to see the buckets
- To see the contents of the bucket type "# aws s3 ls s3://<bucket>/folder"
- "$ **aws ec2 describe-instances**" to see the list of instances in your account
- "$ **aws ec2 describe-instances | grep InstanceId**"
- "$ **aws ec2 terminate-instances –instance-ids i-0749a28555320dbf7**" - ec2 instance will be terminated
- "$ **aws rds describe-db-instances**" - will list all the databases in the account

Activity - CLI

- In the previous activity we saw how to set up a user with access using the access key and secret
- If someone hacks into the account then these keys are exposed
- Let's now create a new instance but this time assign a role
- Remember the role comment from the EC2 activity? "What happens if you miss assigning a role?"
  - At the time of launching a new instance select the IAM role that you want to associate in step 3 e.g. "s3-admin-access" that we created during IAM role activity



  - Proceed with the rest of the steps to launch the instance as usual
- Once the instance is launched you now configure the CLI but leave the access key and secret as blank
- You can execute the list commands of S3 as before without the access keys etc. This is more secure!
- You can remove the role all access is revoked immediately

Activity - Bootstrap script

greatlearning

- It is a set of commands that are executed when an instance goes online (provisioned for the first time and at every reboot) as root.
- This is also known as "User Data" (as seen on the AWS EC2 instance creation screen)
- Ex 1: Regular shell script & here's a sample to install http server

```
#!/bin/bash
yum update -y
yum install httpd -y
service httpd start
chkconfig httpd on
IP_ADDR=$(curl http://169.254.169.254/latest/meta-data/public-ipv4)
echo "This is auto scale server $IP_ADDR" > /var/www/html/index.html
echo "ok" > /var/www/html/health.html
mkdir /opt/efs
```

- Ex 2: Copy files from S3
  - aws s3 cp s3://<bucket>/<subfolder>/filelist <target folder in the instance>
- Ex 3: Mount an EFS for file share
- This is very useful during autoscale where a server is provisioned with the software components without manual effort
- Note - it can take several minutes for the script to run
- Exercise - where can this be specified?

User data gets added to the cloud-init which is execute at the time of booting.
Must read -> http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonLinuxAMIBasics.html#CloudInit

greatlearning

Compute - Part II

EC2 Autoscaling

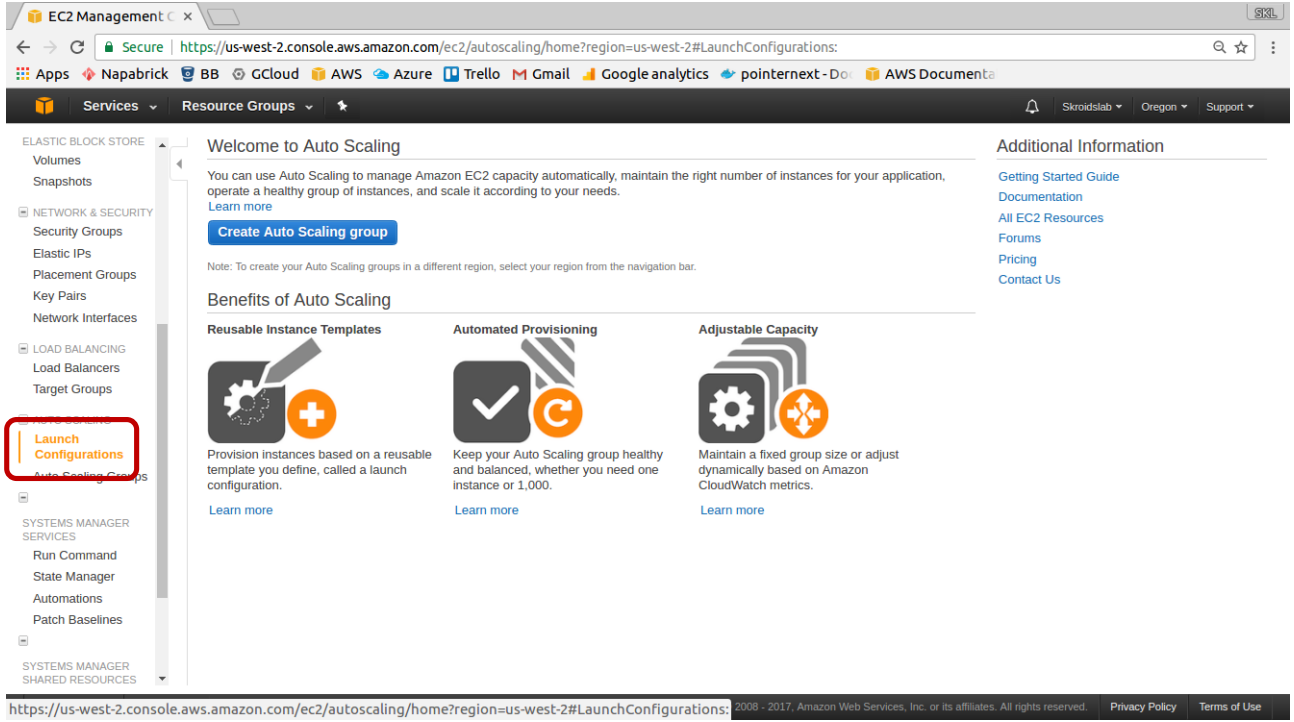
Activity - Config group & Autoscale

- Important to know "Elasticity"
- Core concept is to expand with load and shrink otherwise
- Cost varies accordingly - demand based cost of operations (OPEX)
- IaaS providers will let us configure rules based on which it scales either way
- Good idea for the application tier
- Debate such a model for the data tier and state your observations

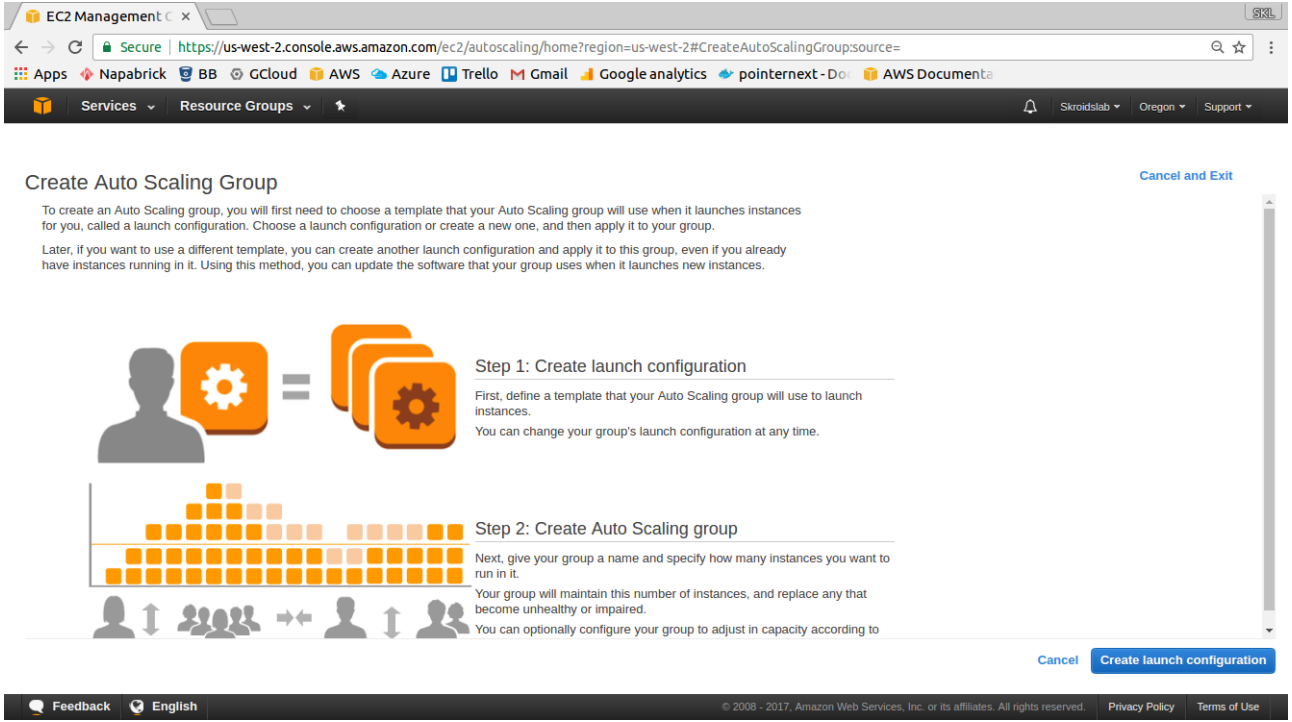
Question

Are you sure the capacity graph will be smooth and as parallel to the utilization graph?

Activity - Launch configuration

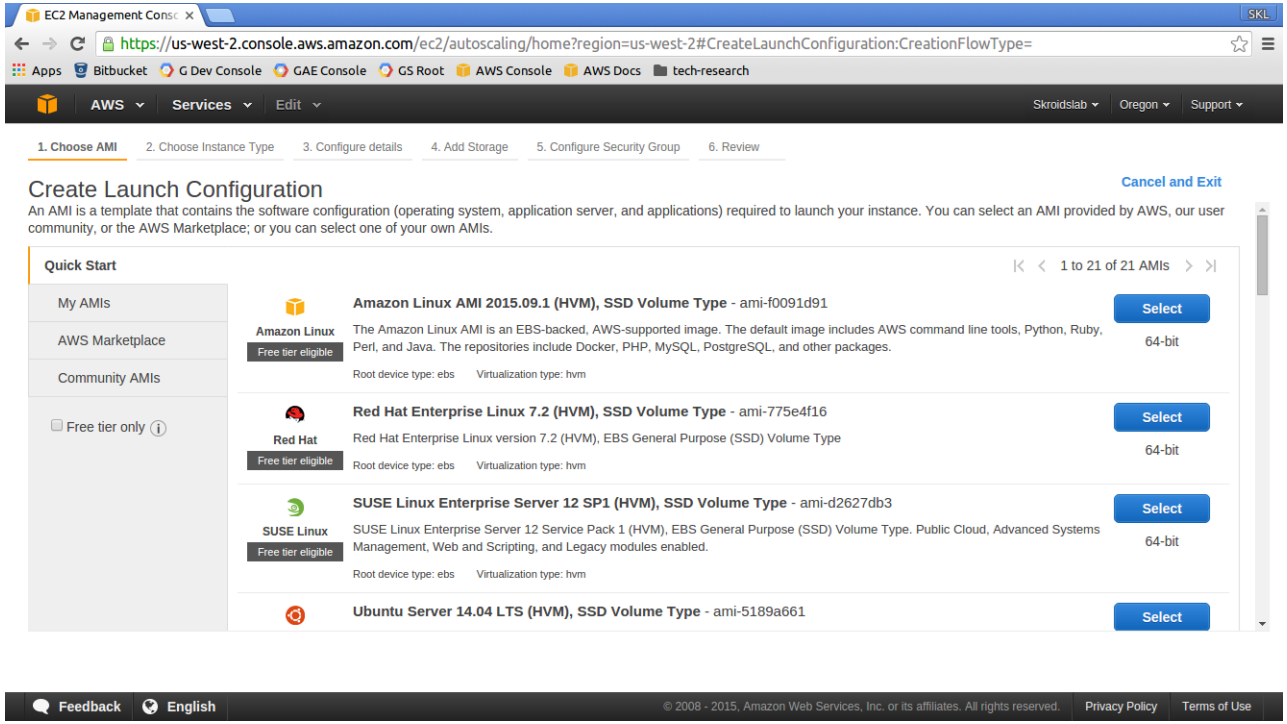


Activity - Launch configuration



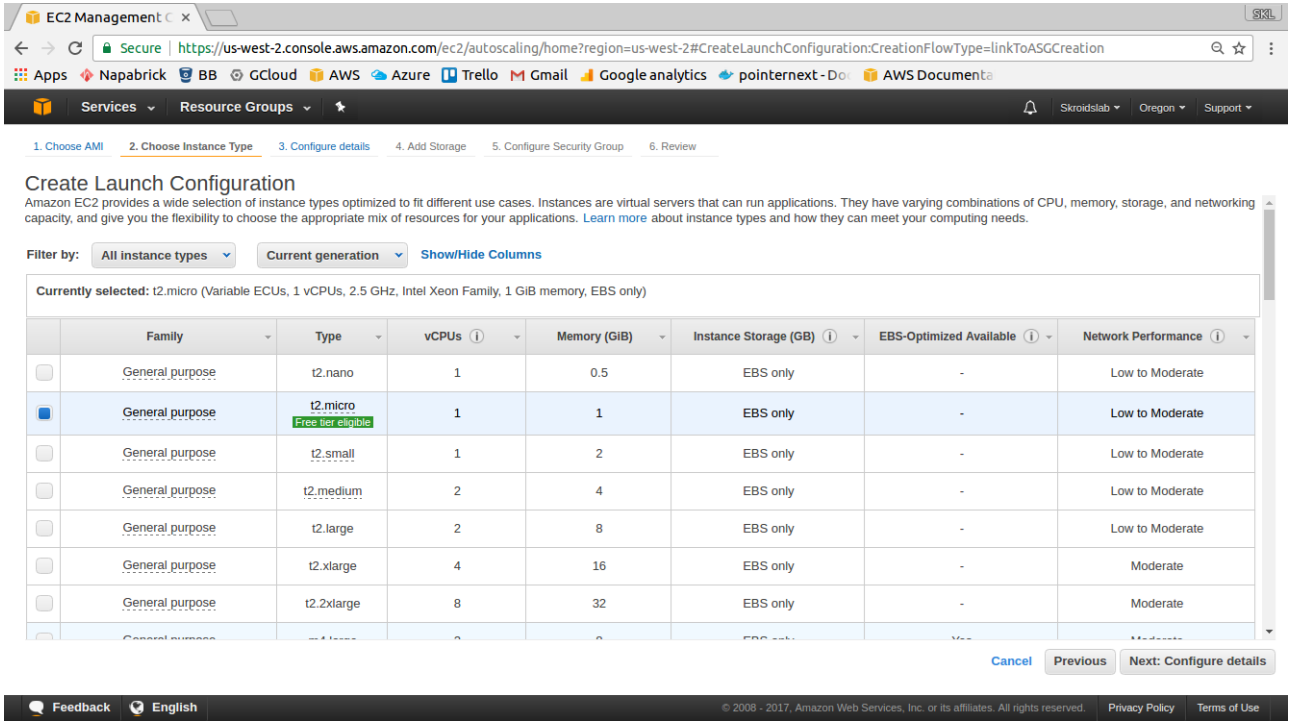
Activity - Launch configuration

greatlearning



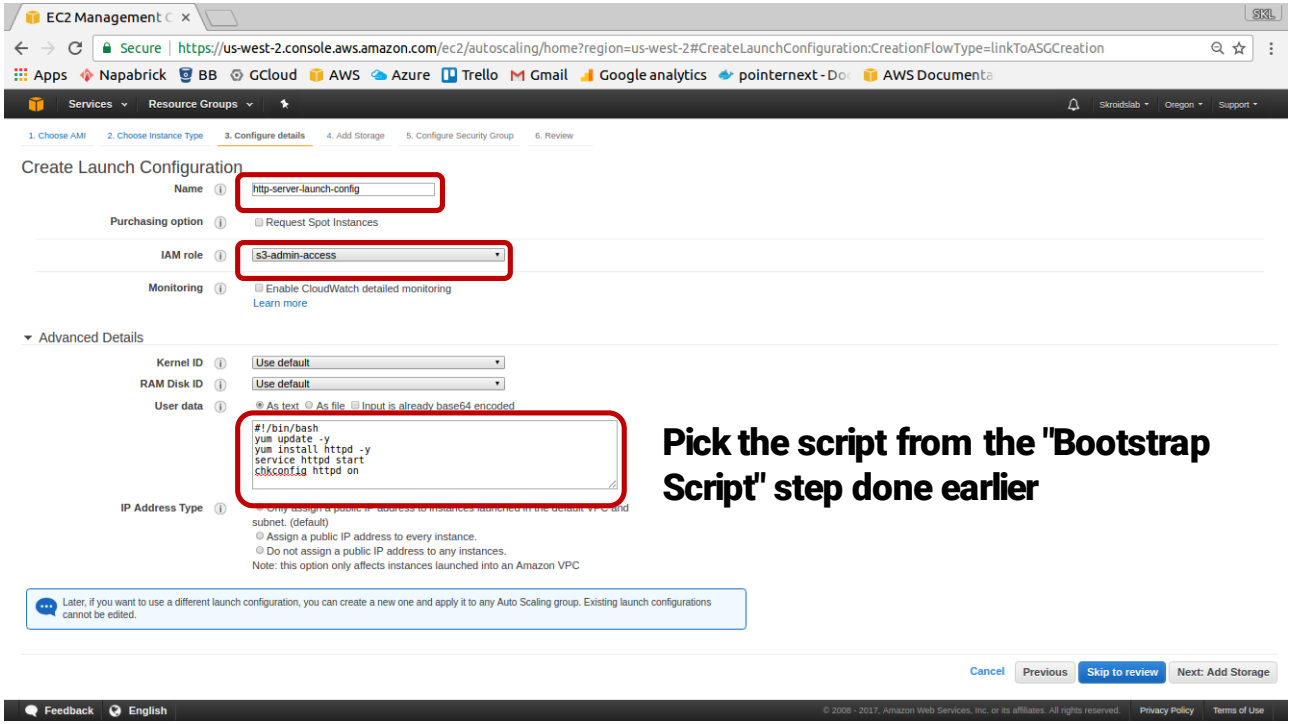
Activity - Launch configuration

greatlearning



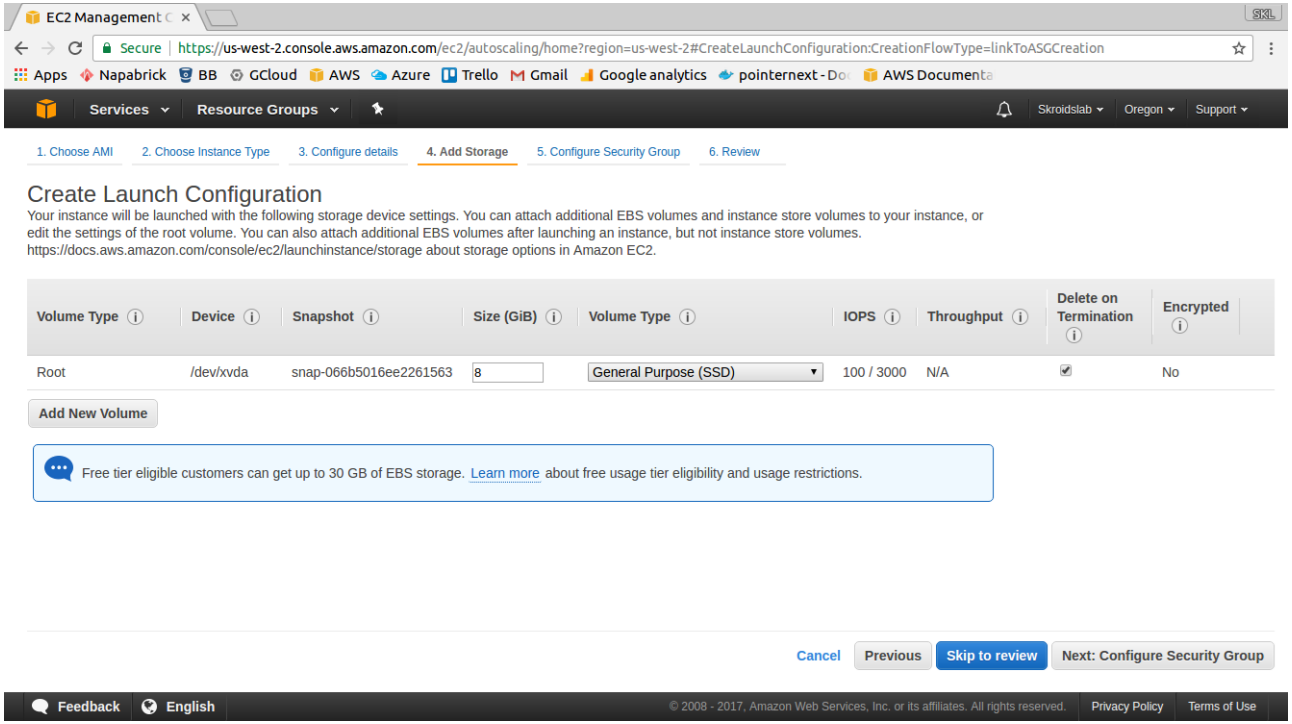
Activity - Launch configuration

greatlearning



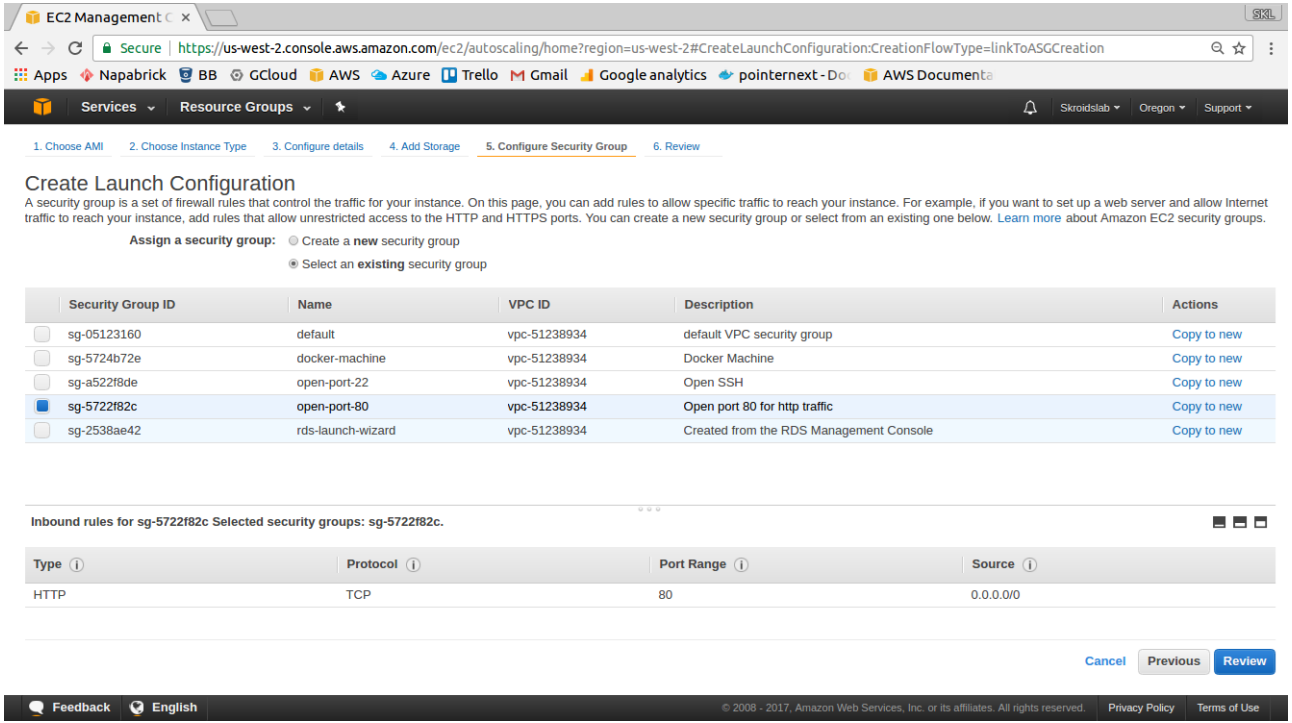
Pick the script from the "Bootstrap Script" step done earlier

Activity - Launch configuration

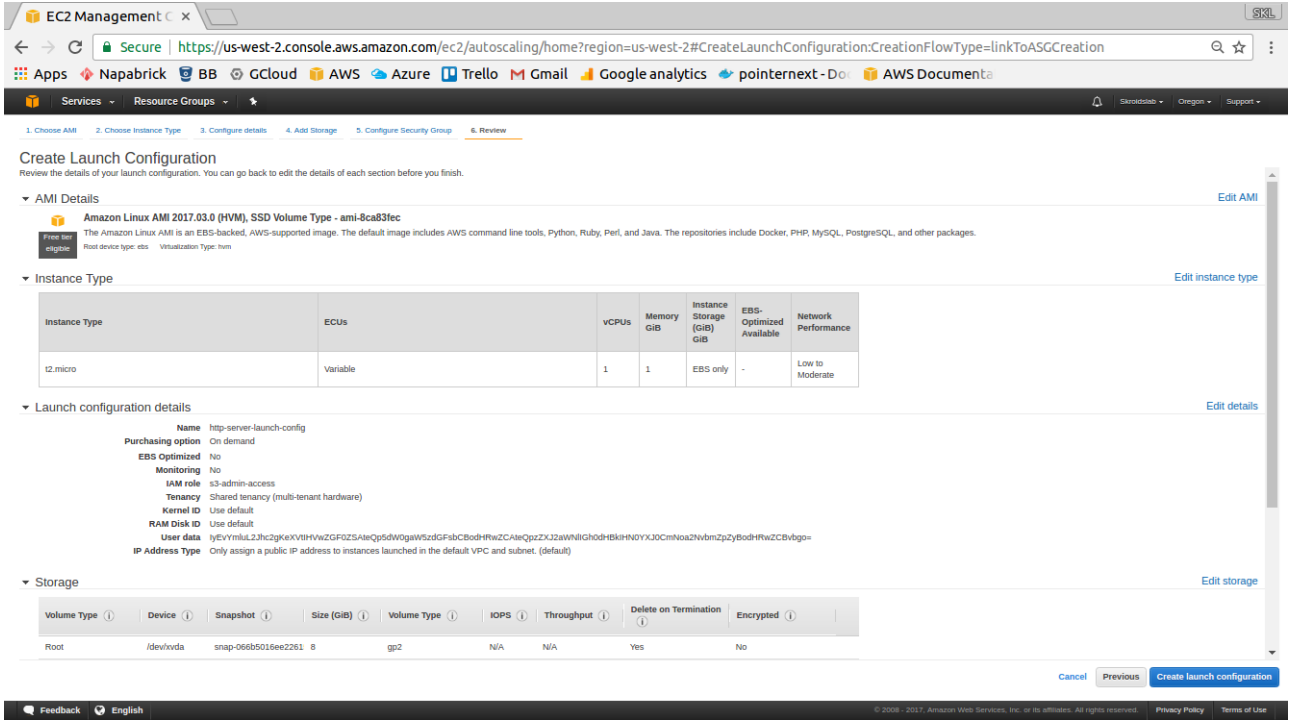


Activity - Launch configuration

greatlearning

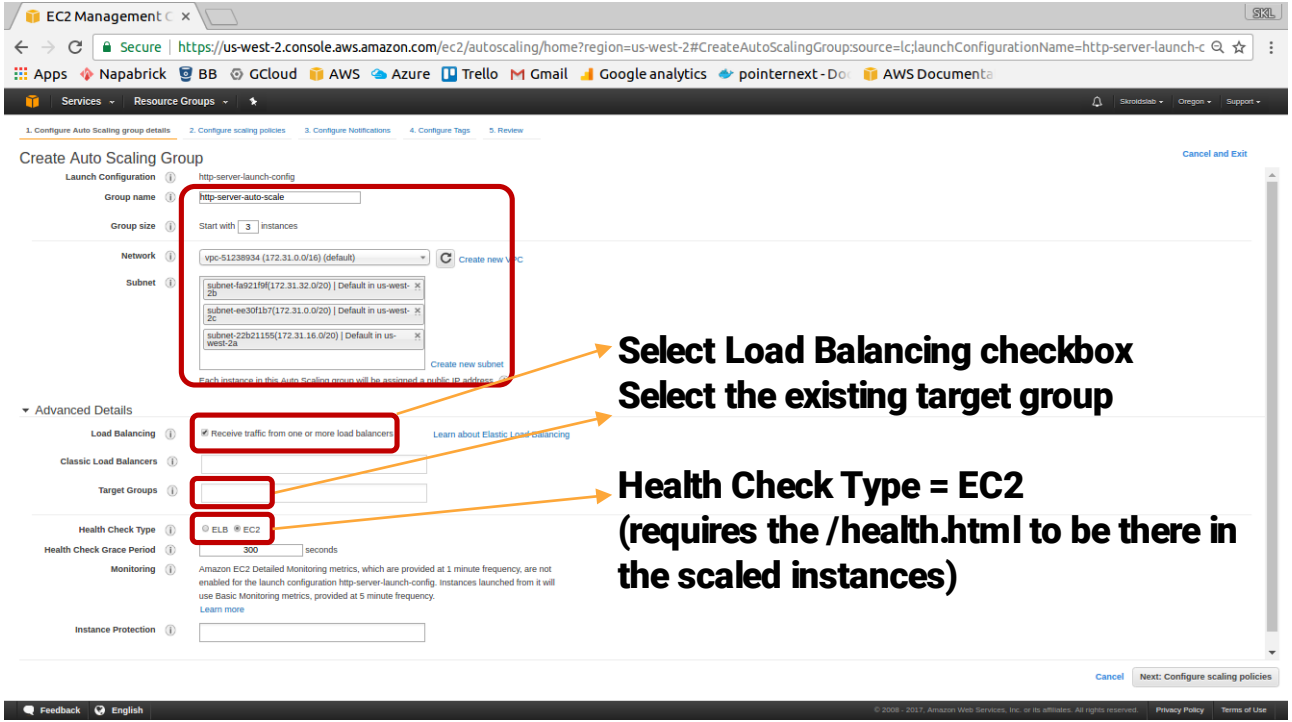


Activity - Launch configuration

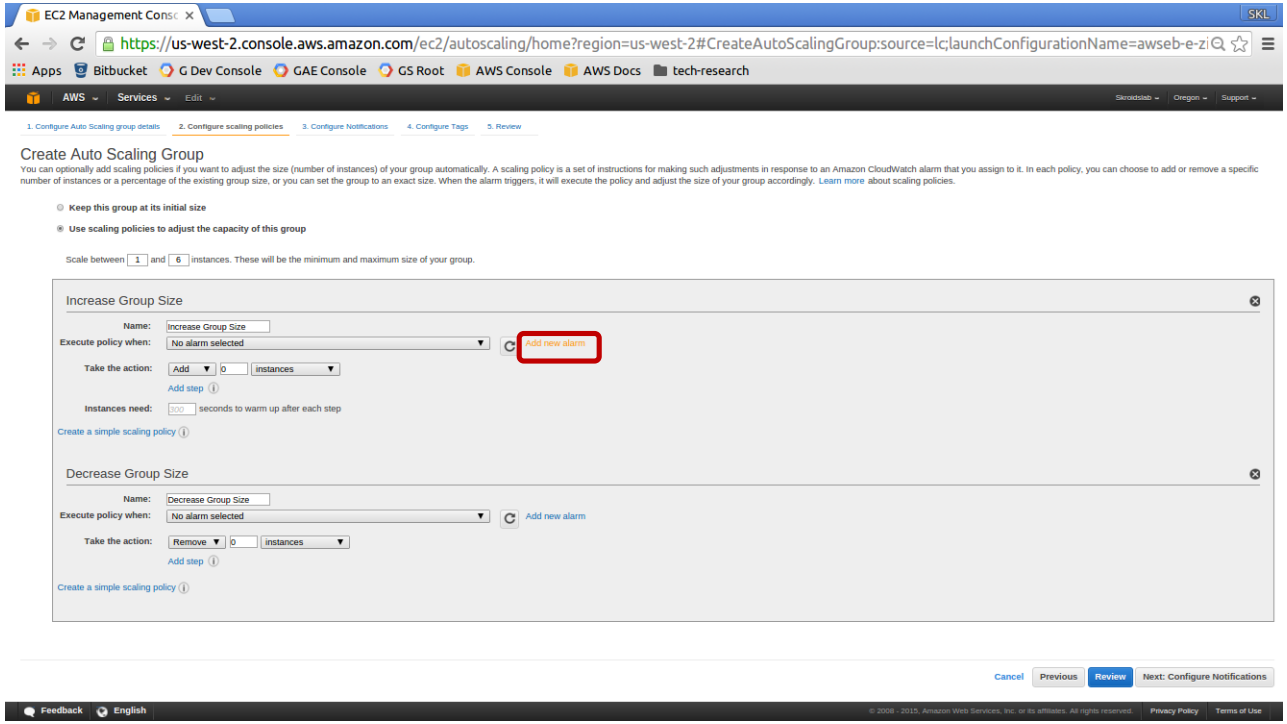


Pick the existing PEM and acknowledge in the next step

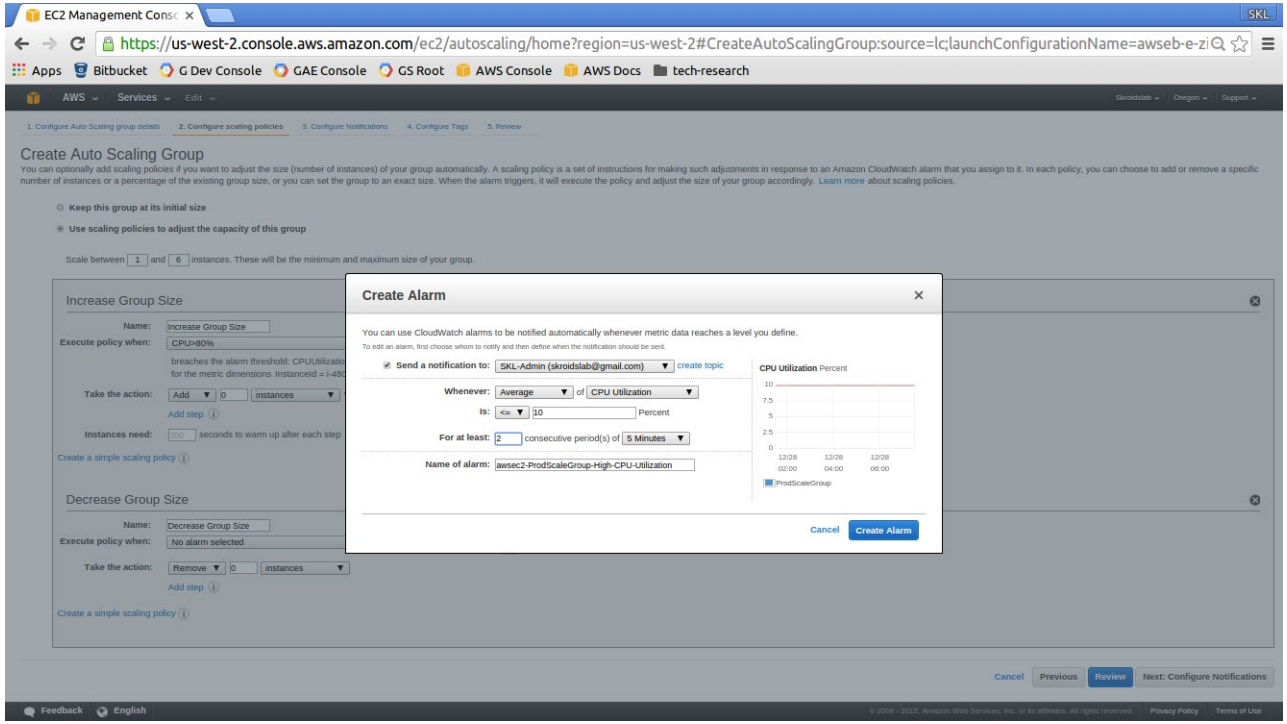
Activity - Auto scale group



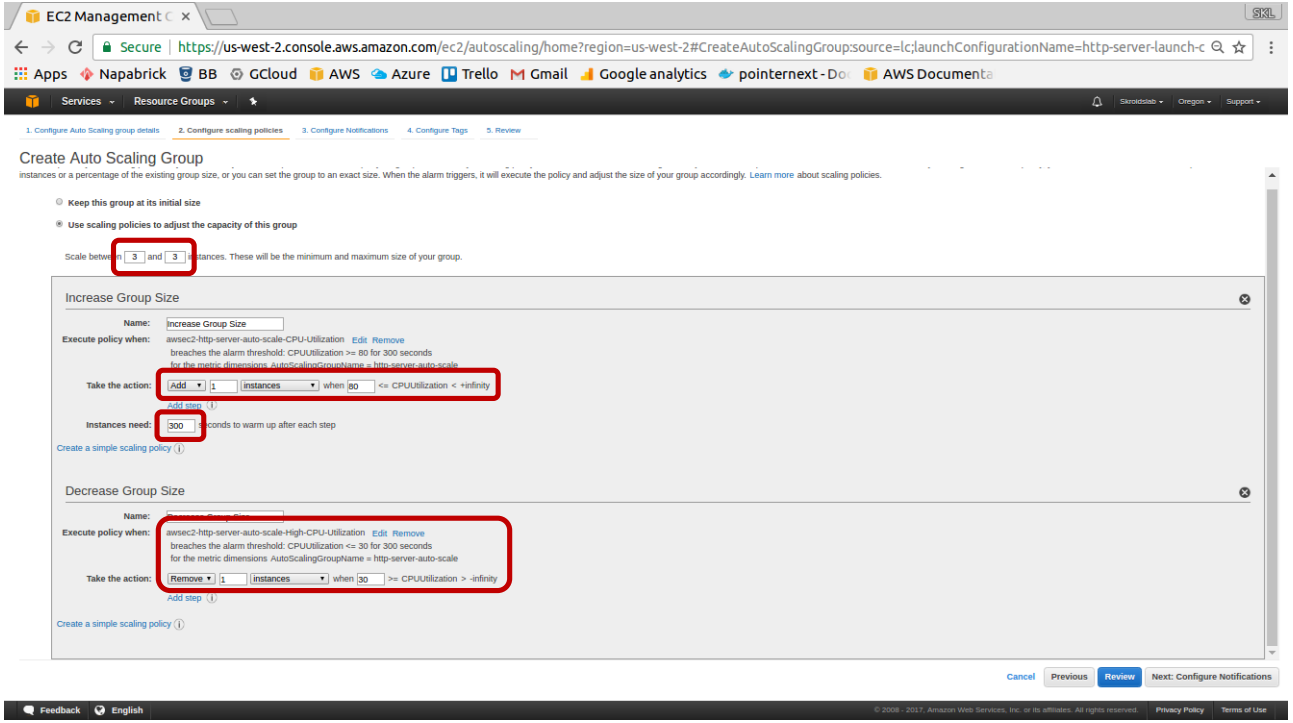
Activity - Auto scale group



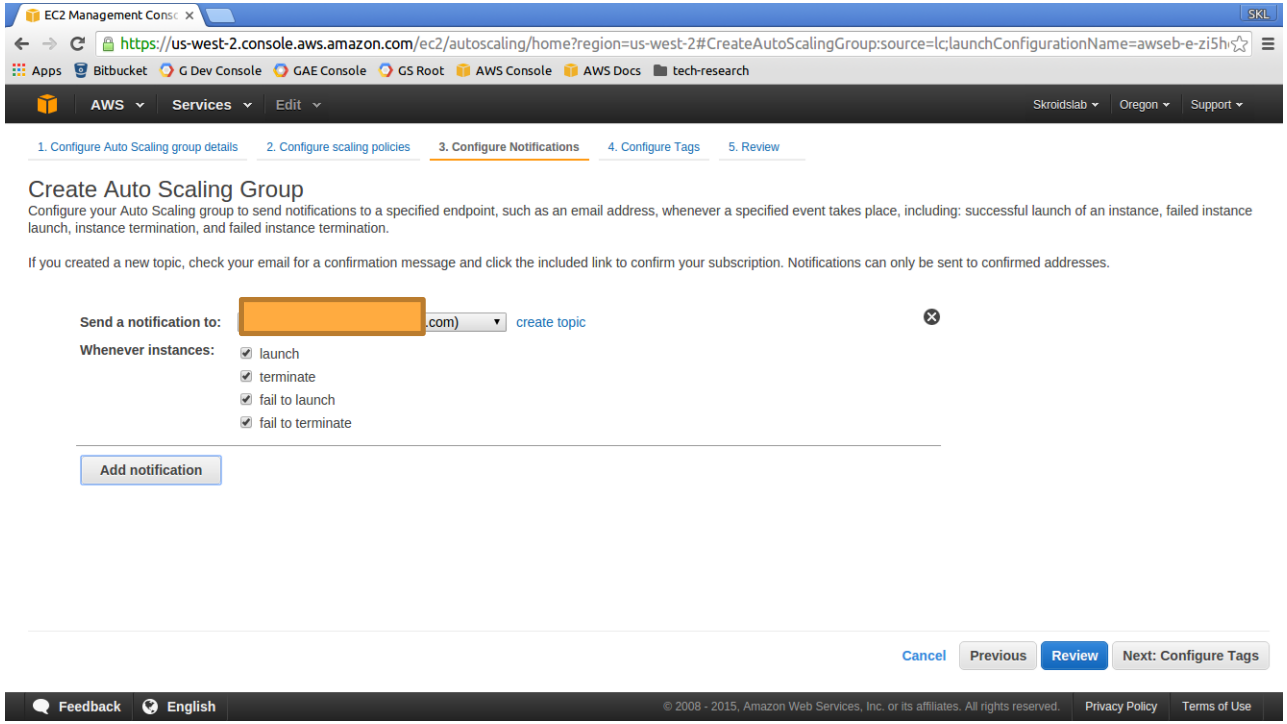
Activity - Auto scale group



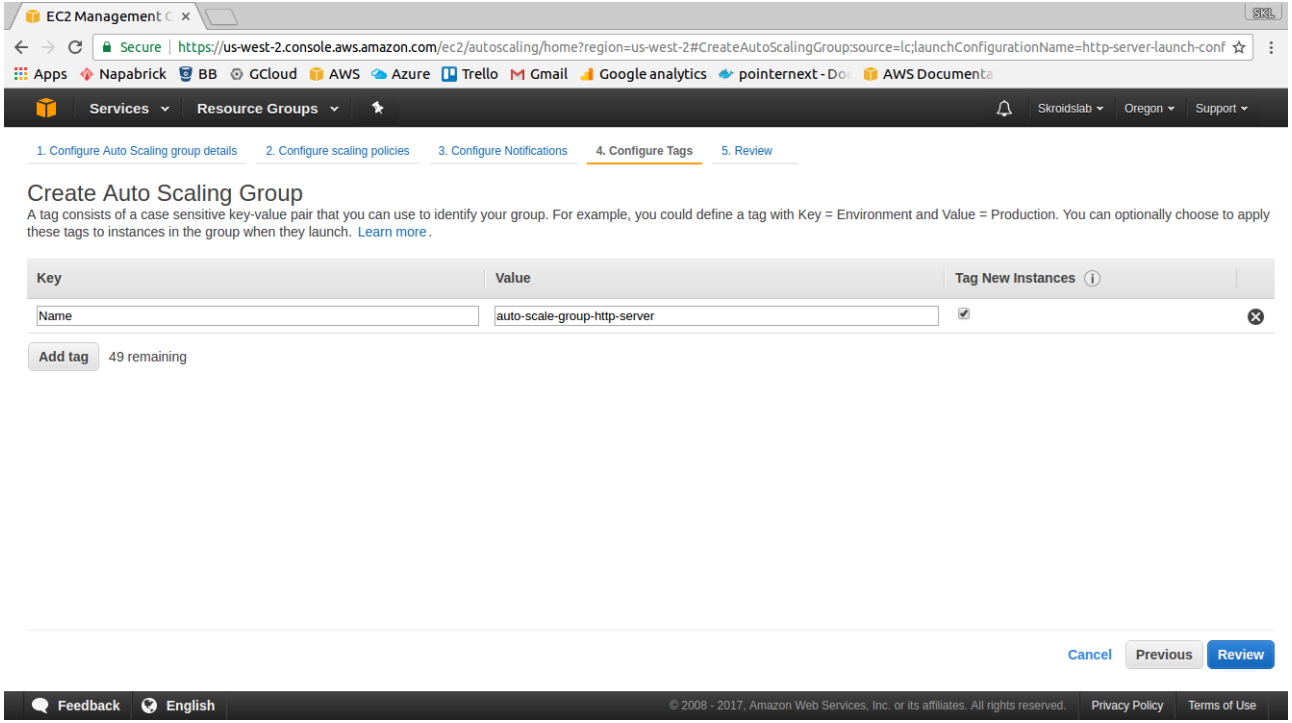
Activity - Auto scale group



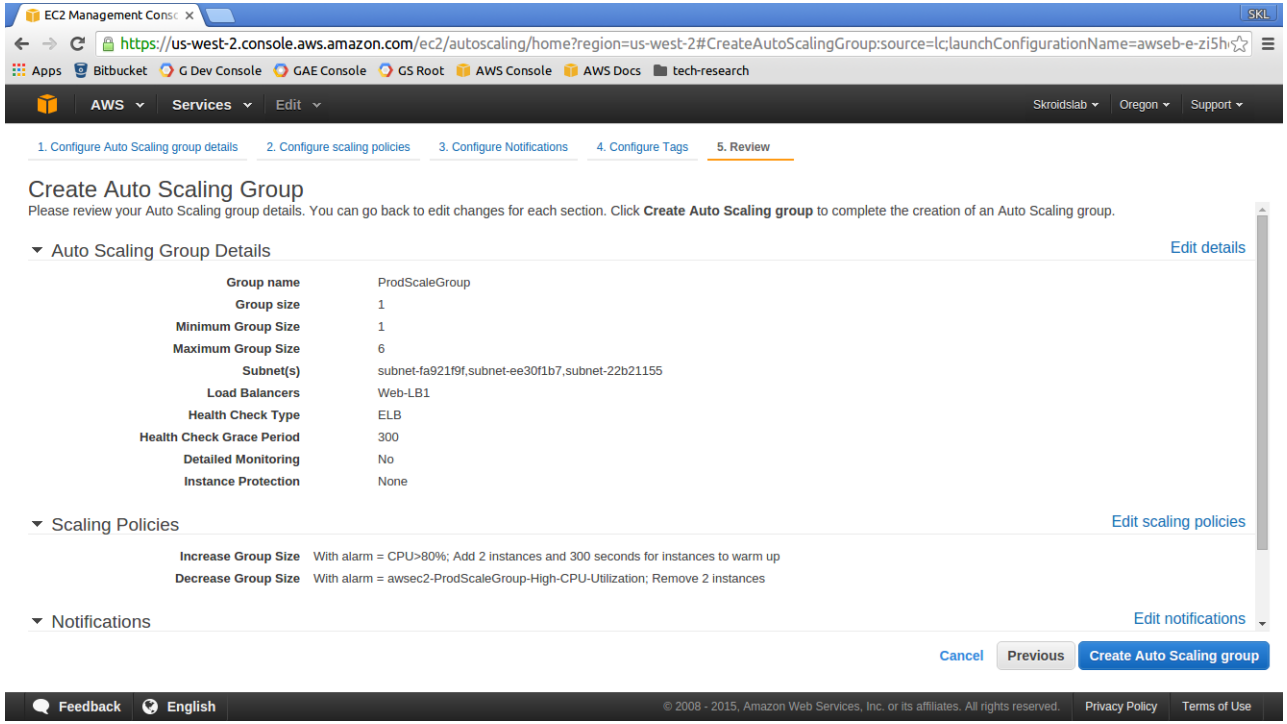
Activity - Auto scale group



Activity - Auto scale group

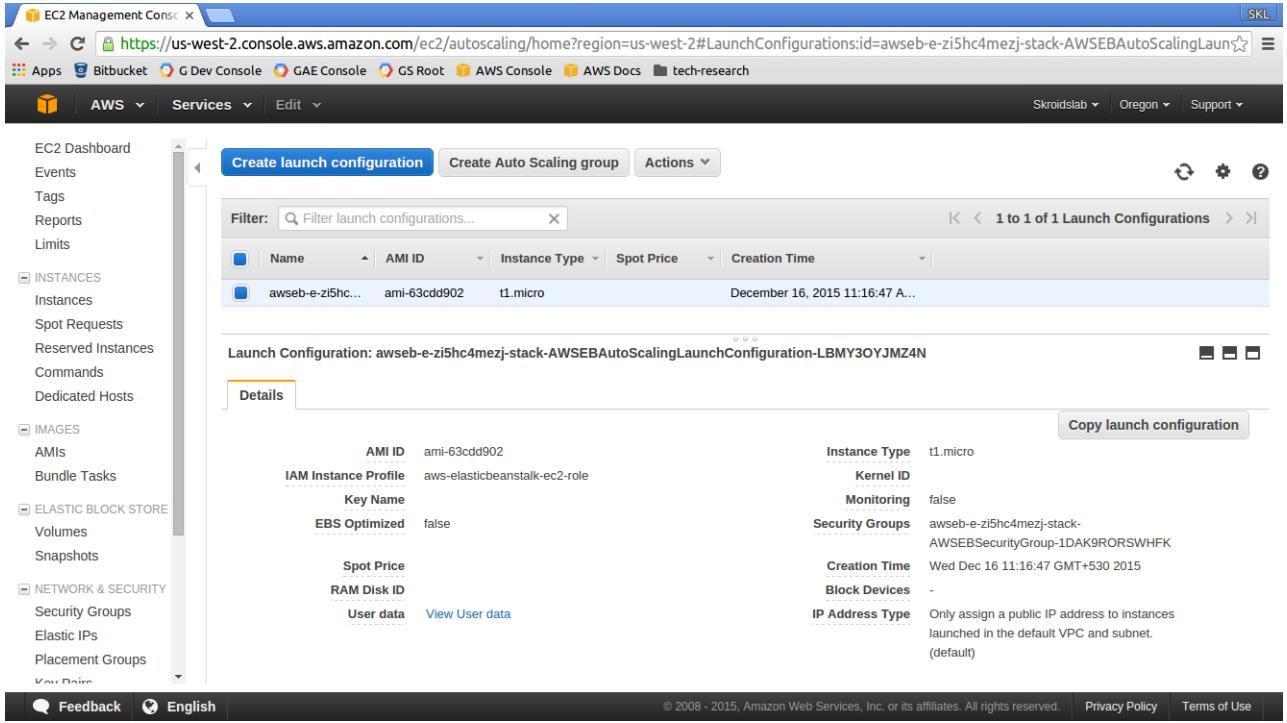


Activity - Auto scale group



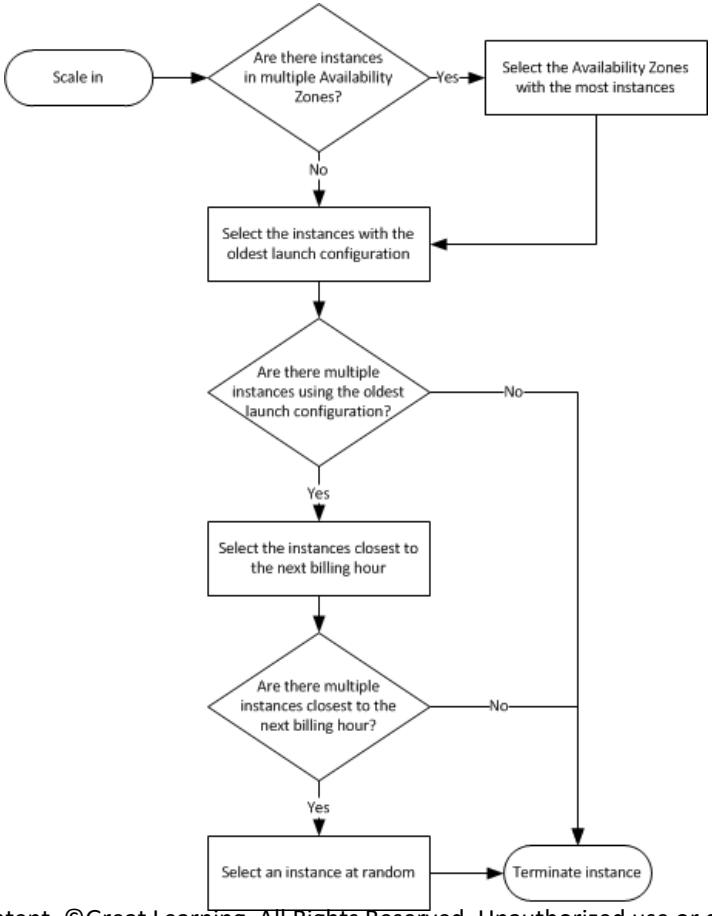
Activity - Auto scale group

greatlearning



Go to the Load Balancer section and see the instances! Kill this newly created instance and state your observations!

Auto scale instance termination



greatlearning

Compute - Part II

Instance metadata & Placement groups

Activity - Instance metadata

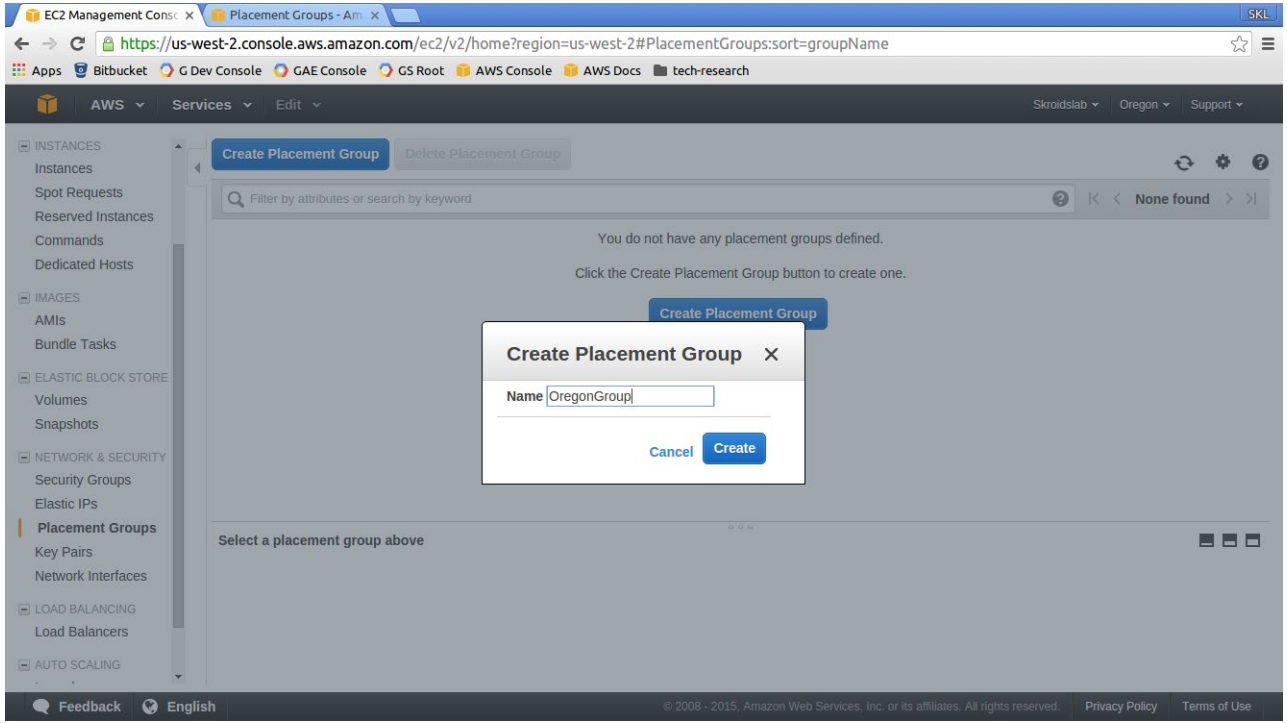
- On any instance using the following URL, gets the metadata
  - curl http://169.254.169.254/latest/meta-data/
  - Above command gives a bunch of options
  - Use any of these options at the end of the URL to get the metadata e.g.
  - curl http://169.254.169.254/latest/meta-data/public-ipv4
  - Notice the output in the following line just before the prompt
  - This URL is not about user data

Activity - Placement groups

greatlearning

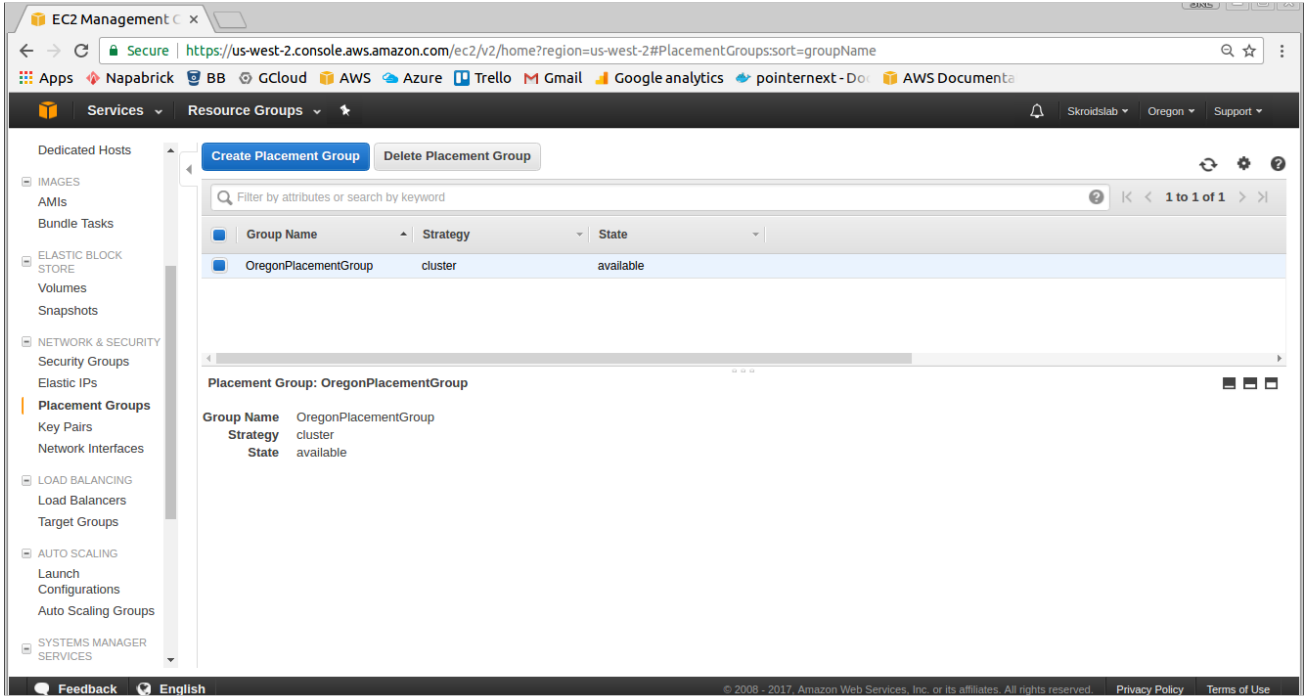
- A placement group is a logical group of EC2 instances in a "single availability zone"
- The objective is to have very high speed connectivity (10gbps) among the instances giving:
  - Low network latency
  - High network throughput
  - Or Both
- Name must be unique within the account
- Only certain type of instances can be launched (optimized for Compute, GPU, Mem, Storage)
- Recommended to have the same type of machines within a given placement group
- Cannot merge 2 placement groups
- Cannot move a placement group from one region to other either in part or full
- Cannot move an existing instance into a placement group

Activity - Placement groups



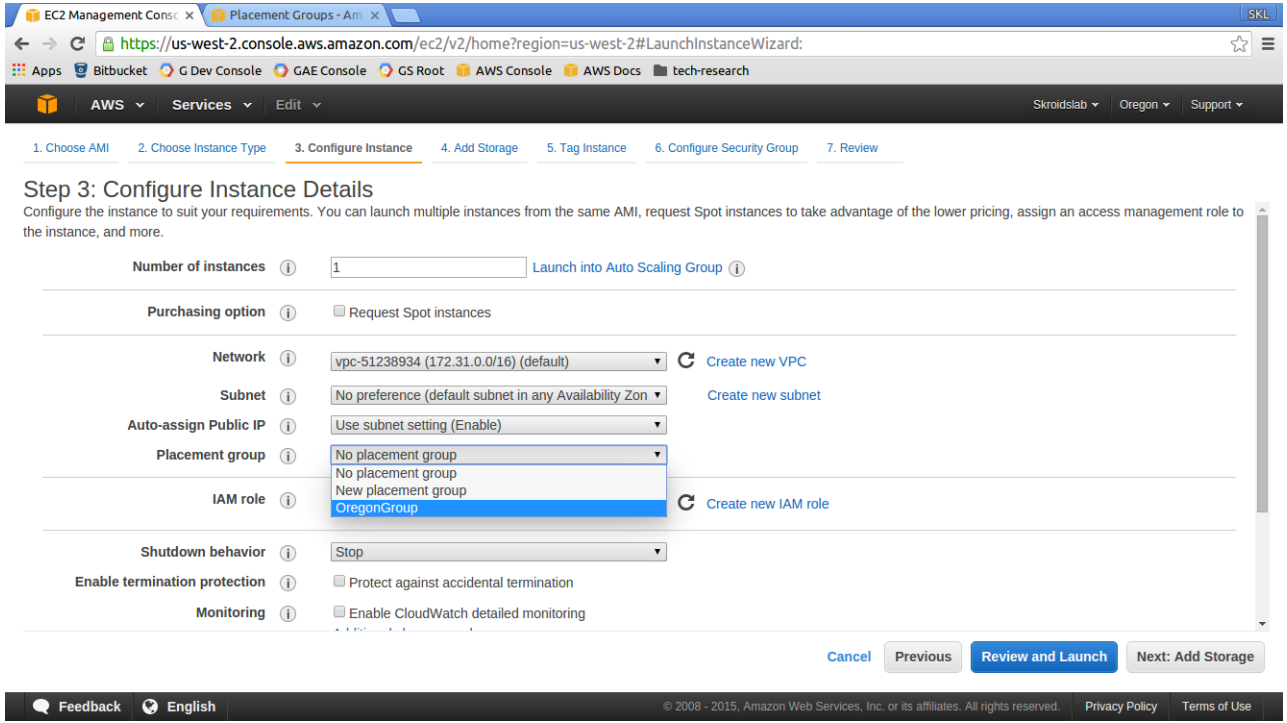
Activity - Placement groups

greatlearning



Activity - Placement groups

greatlearning



Compute - Part II

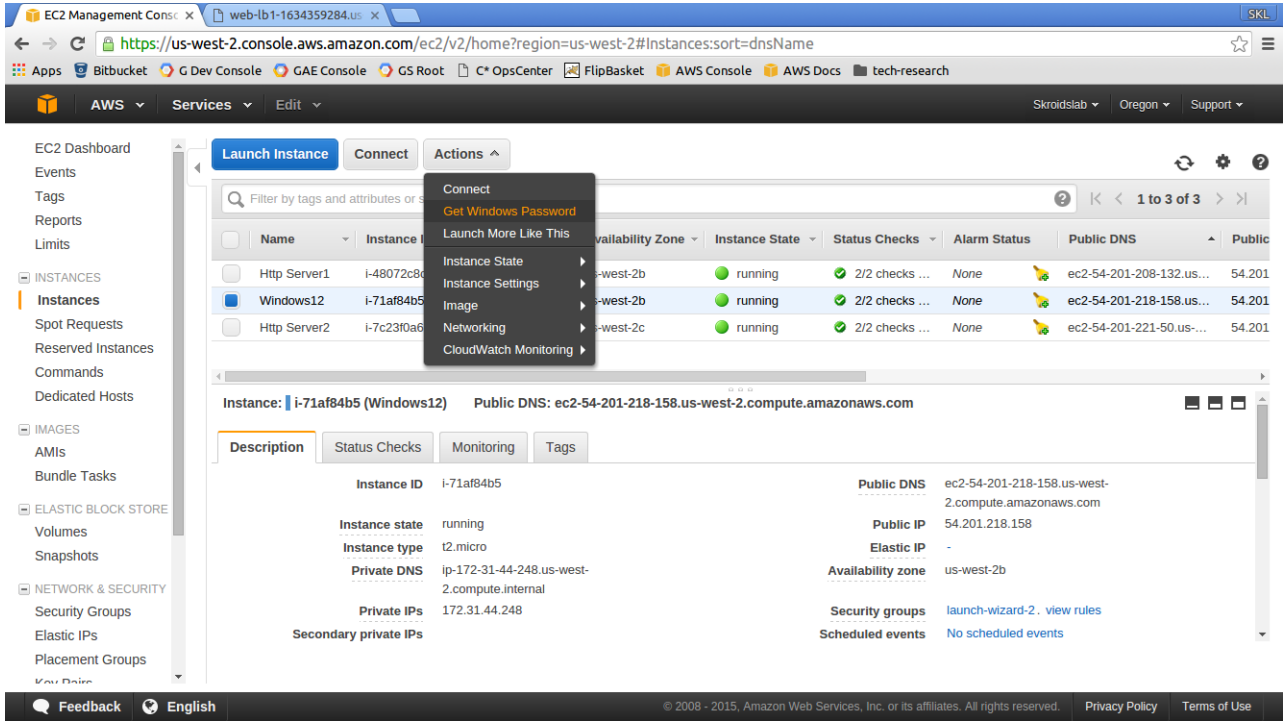
Windows on EC2

Windows EC2 instance

- Let's launch a windows instance
  - "Microsoft Windows Server 2016 Base"
  - m4.xlarge
  - Volume needs to be 30GB minimum
  - Add the RDP (remote desktop protocol) in the security group
  - Create a new PEM file
- Launch the instance (takes slightly longer as compared to linux)
- Next steps are a bit different in windows ...

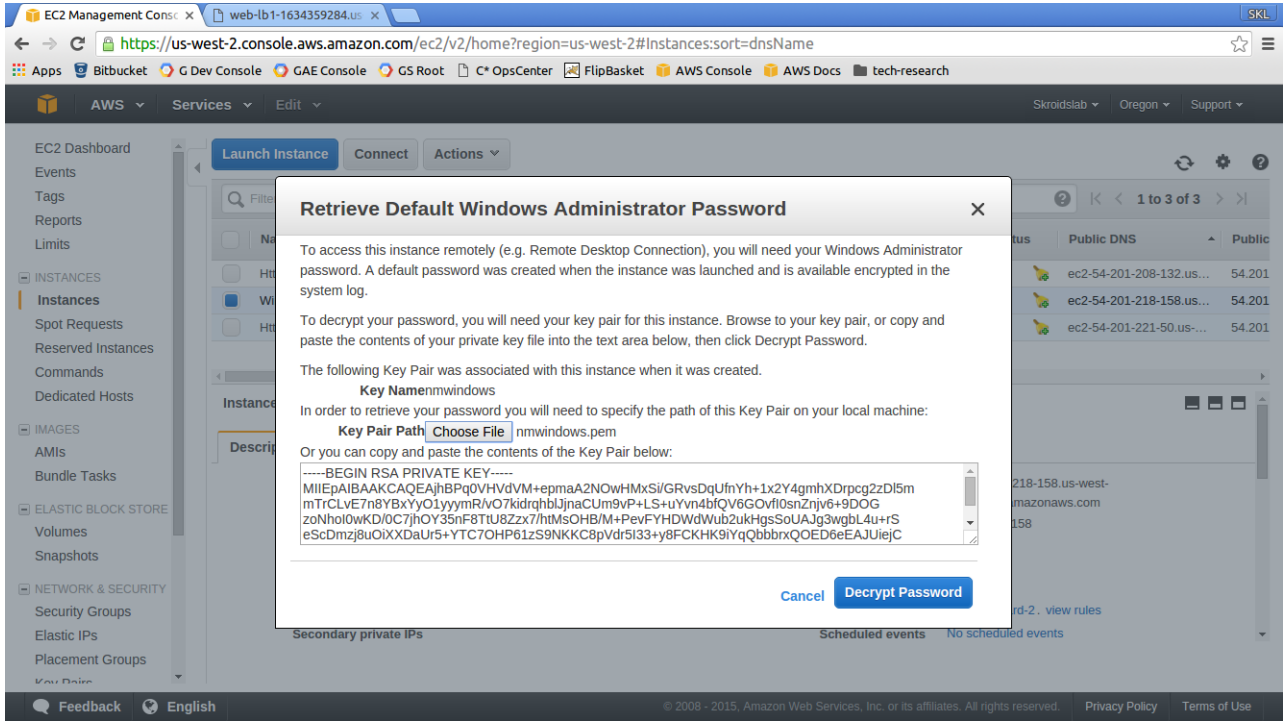
Activity - Windows EC2 instance

greatlearning

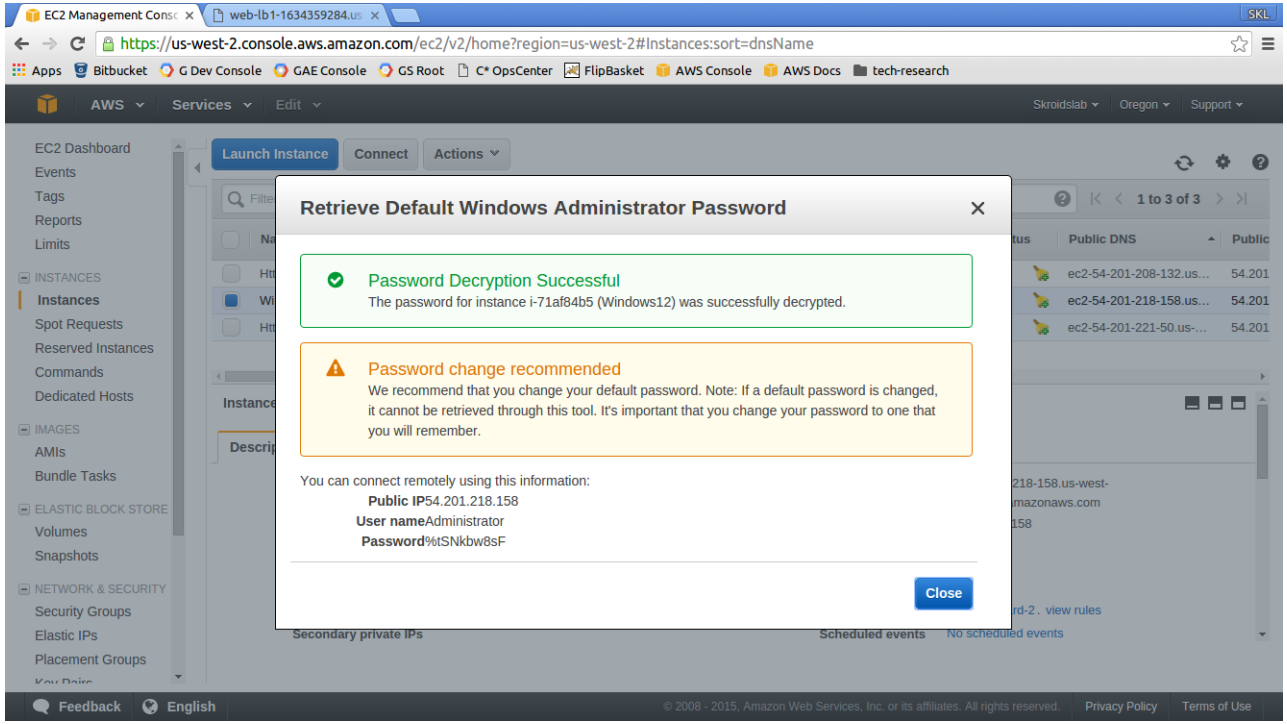


Activity - Windows EC2 instance

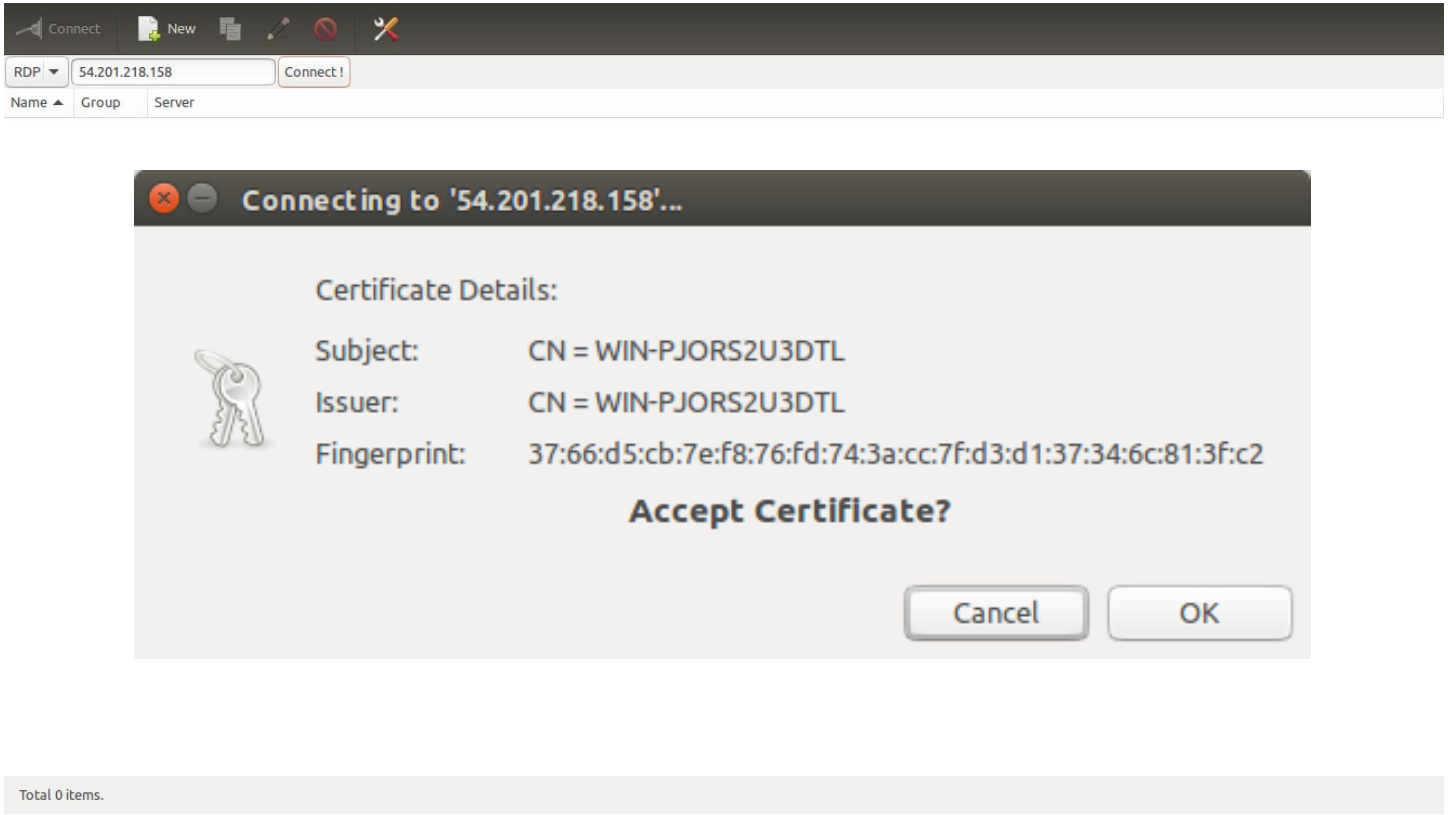
greatlearning



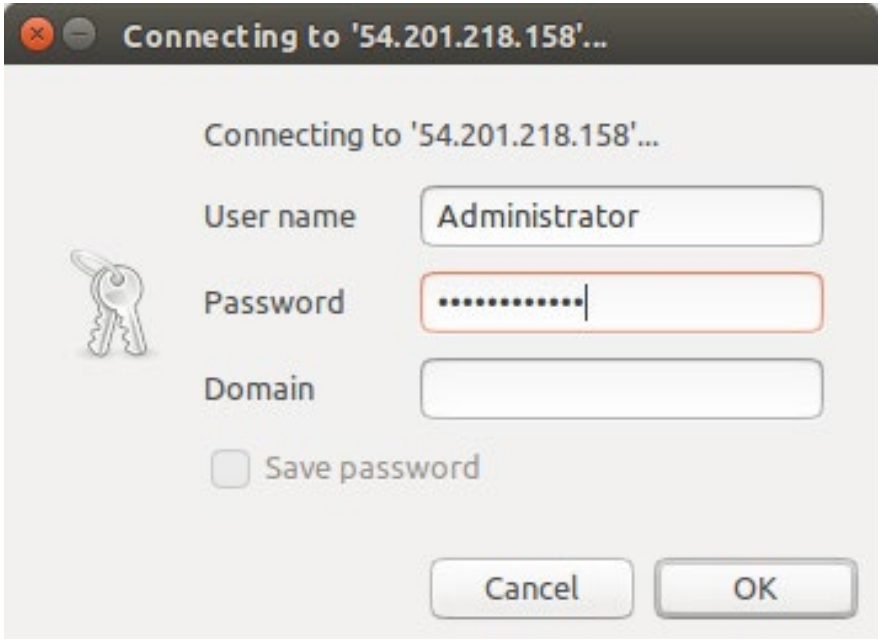
Activity - Windows EC2 instance



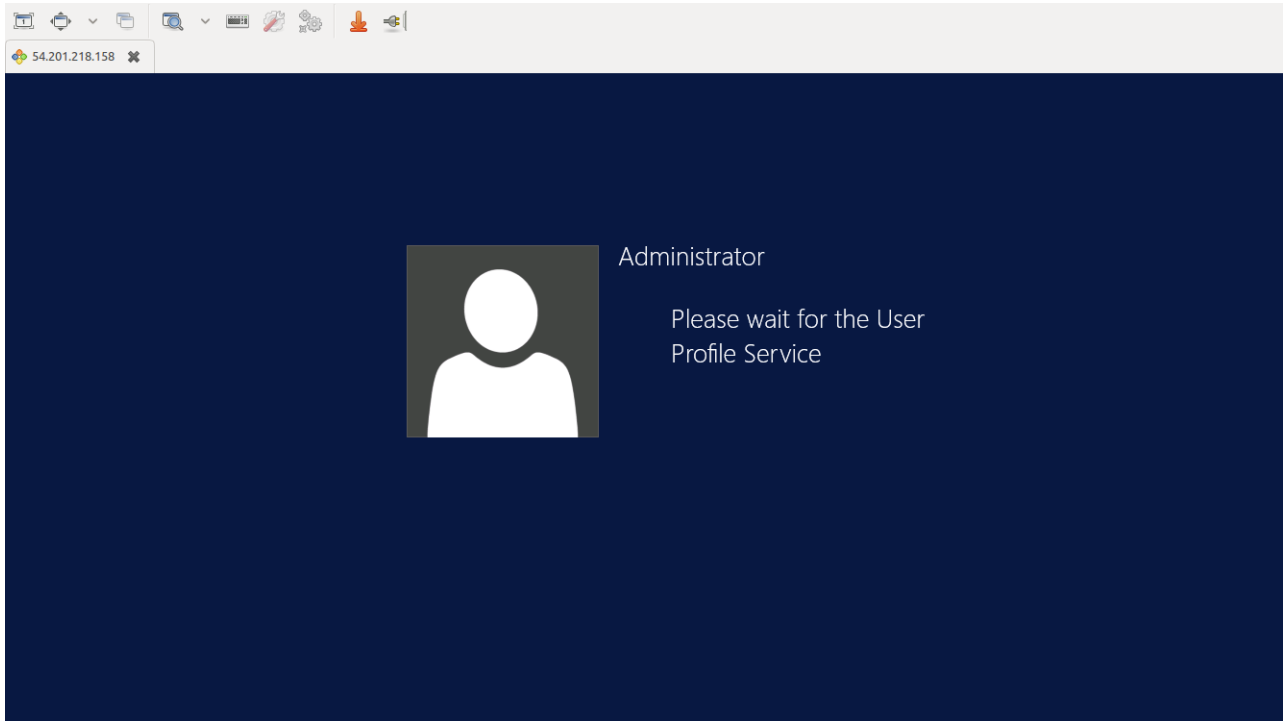
Activity - Windows EC2 instance



Activity - Windows EC2 instance



Activity - Windows EC2 instance



Activity - Windows EC2 instance