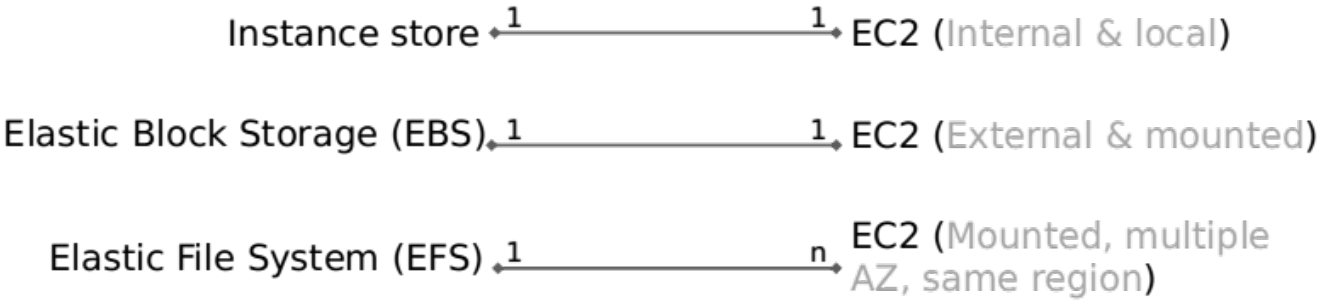
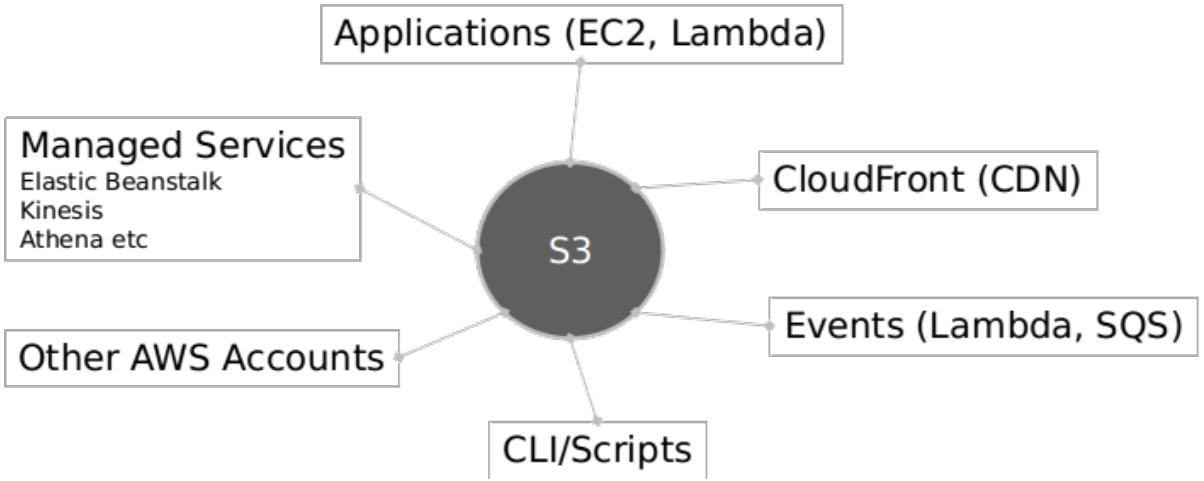
greatlearning

Storage and Content Delivery

Volume > Snapshot > Volume

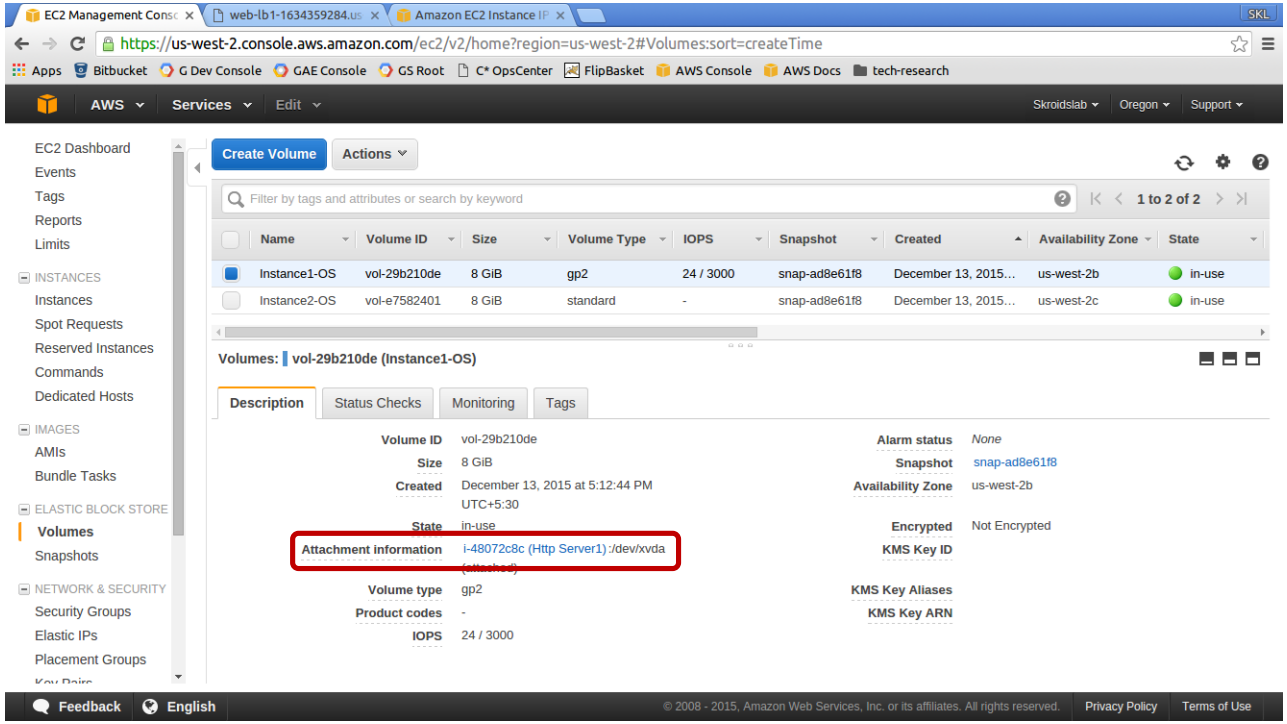
Storage overview





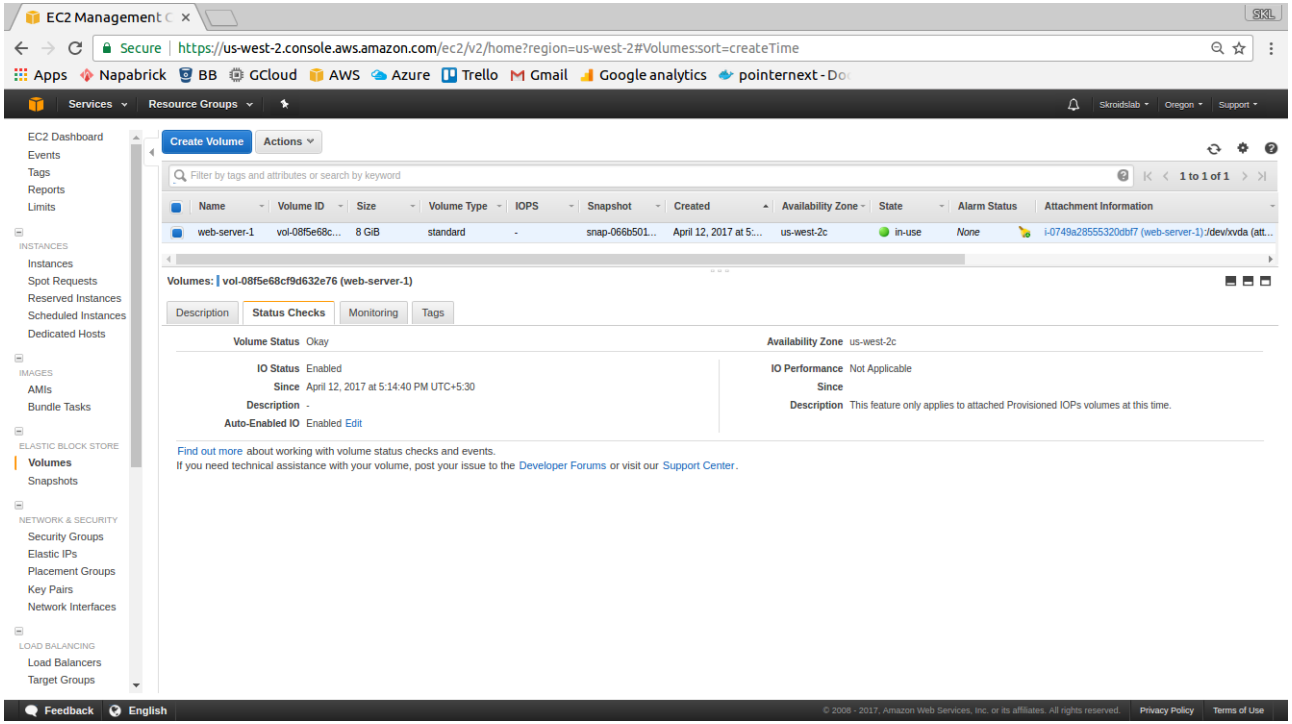
Activity - Volumes

greatlearning

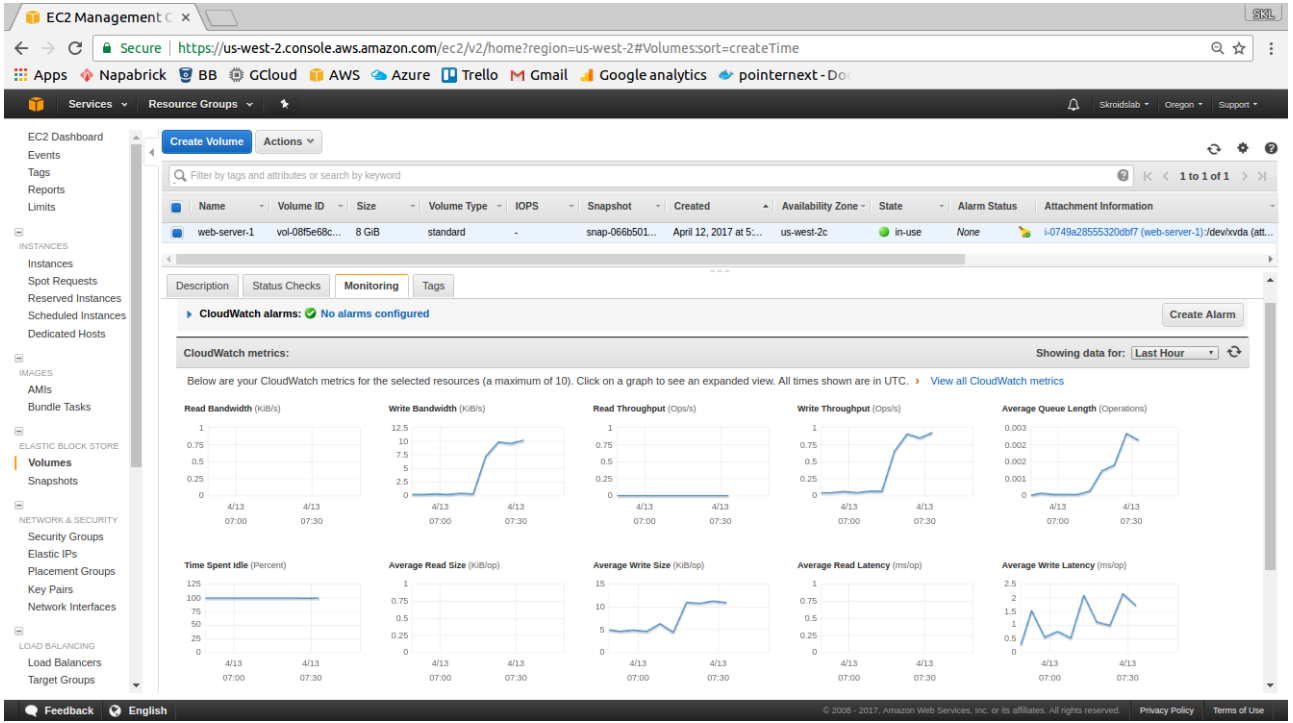


Activity - Volumes

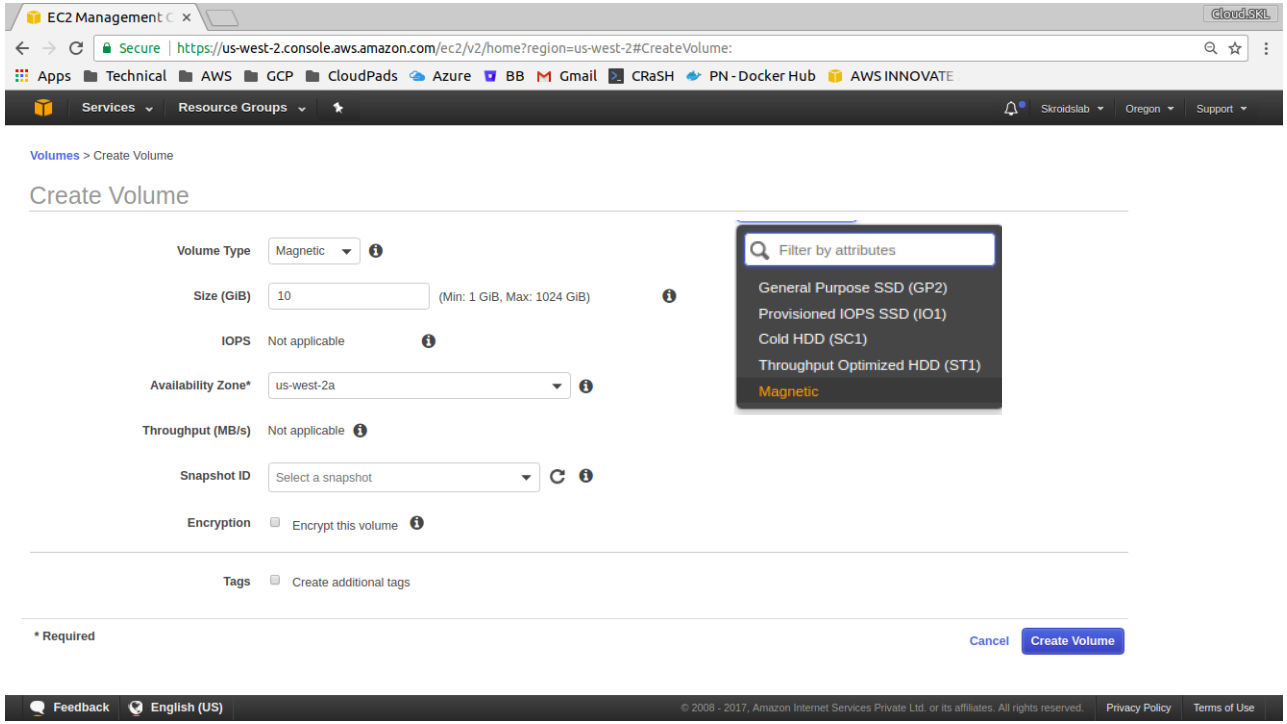
greatlearning



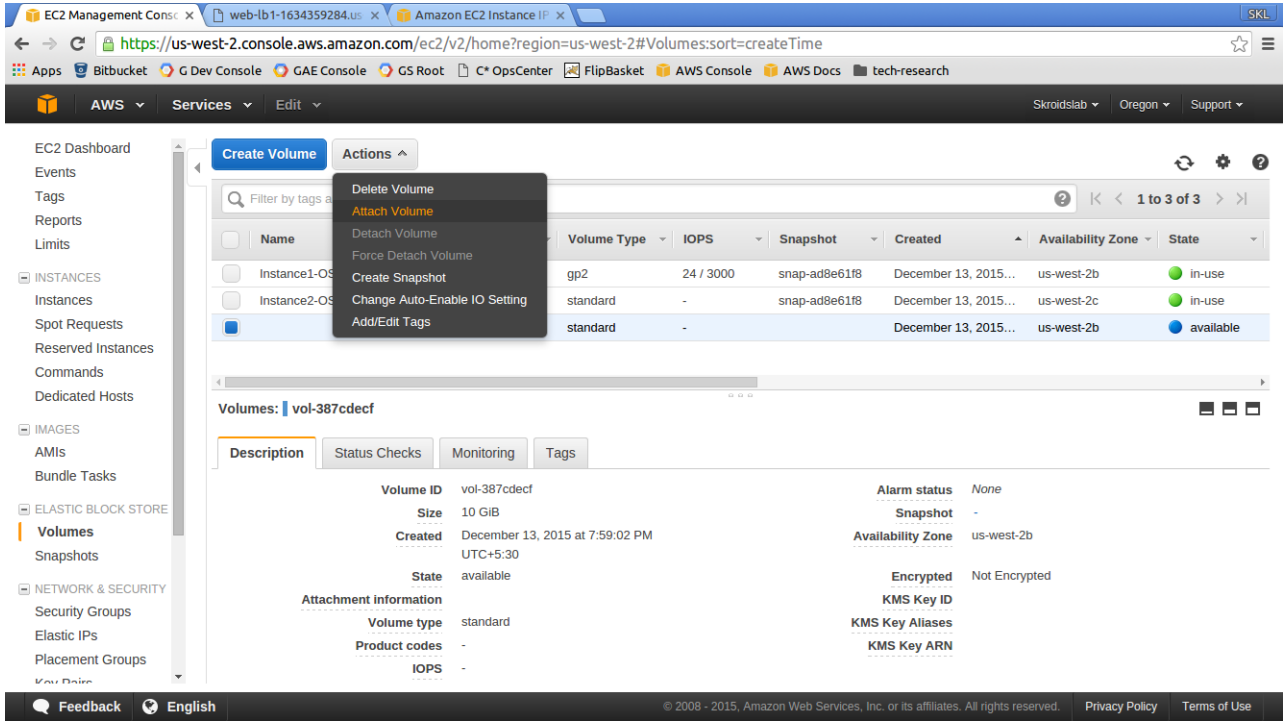
Activity - Volumes



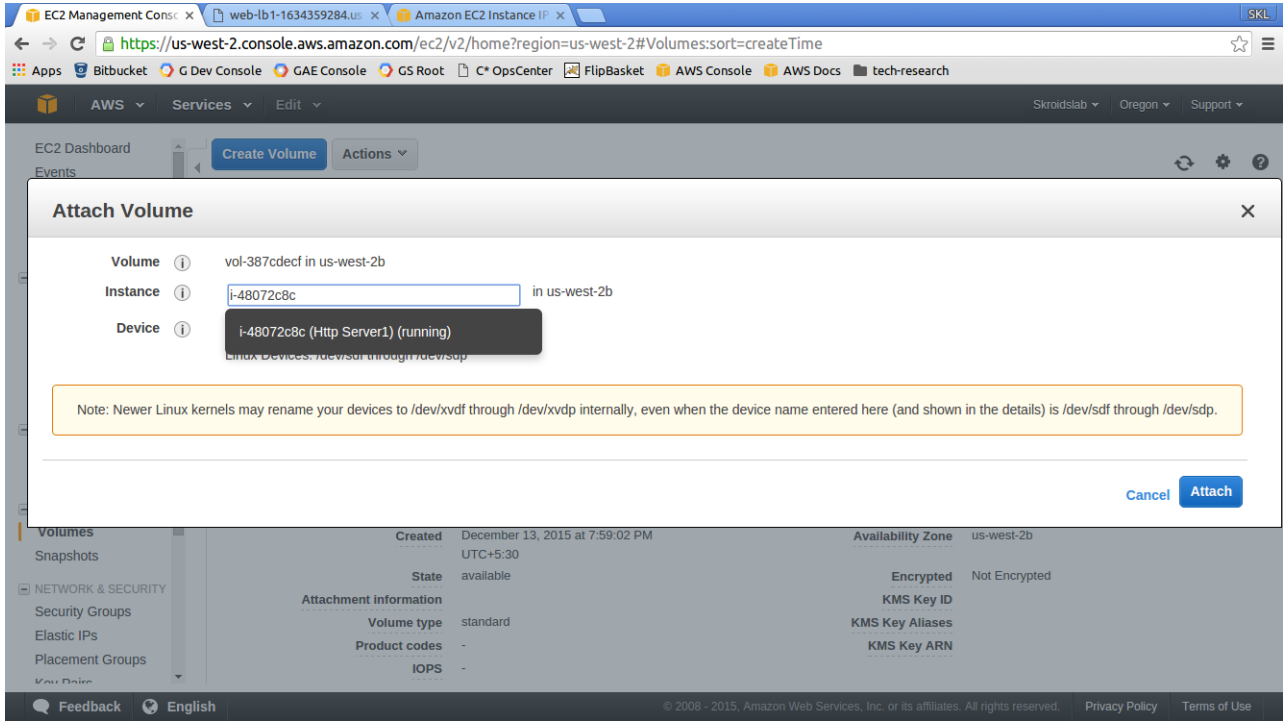
Activity - Volumes



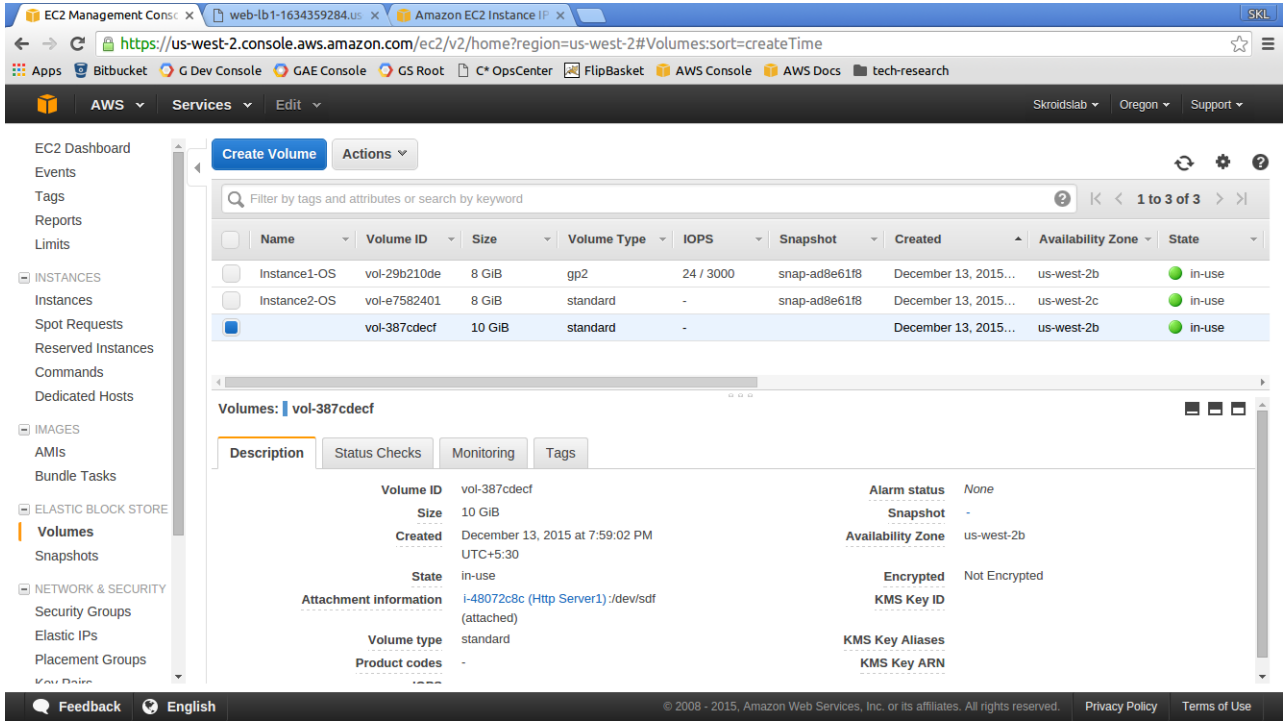
Activity - Volumes



Activity - Volumes



Activity - Volumes



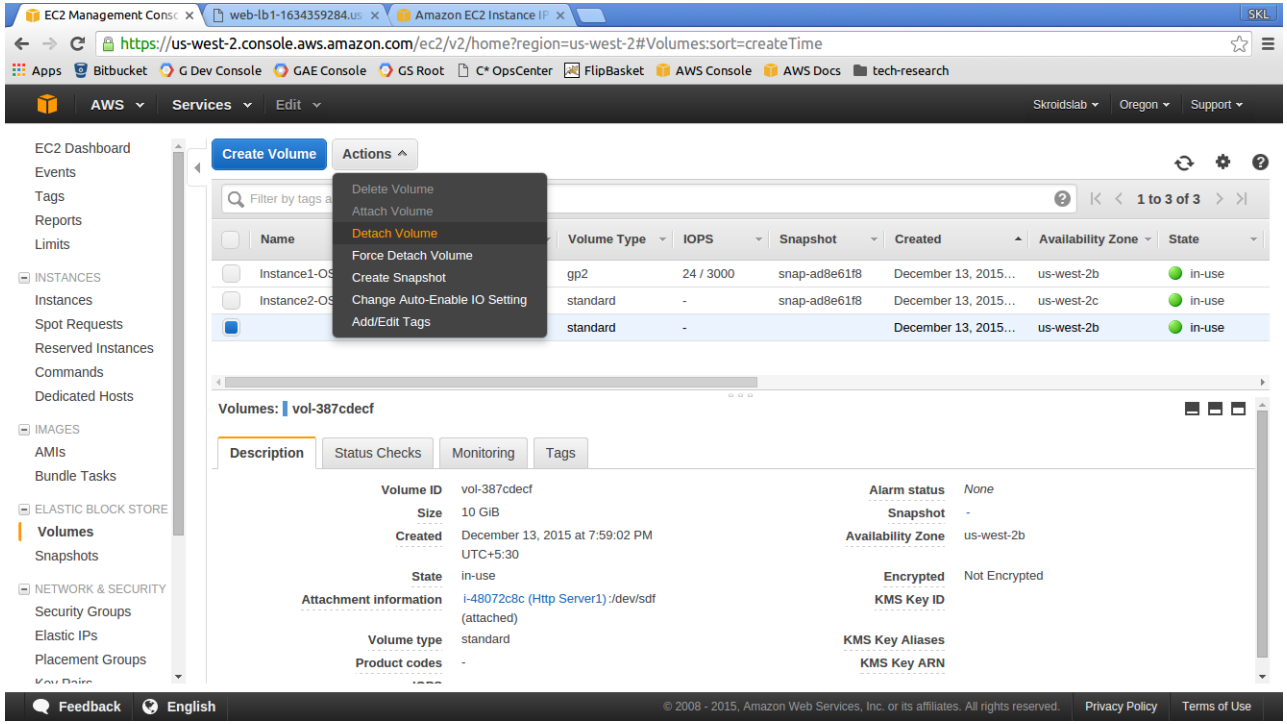
Activity - Volumes

- Login to the ec2 instance
- Fire the command
  - #lsblk
- Notice the volume attached to this instance
- Check if it has any data or not
  - #file -s /dev/xvdf
  - Comes back with "data" means its a raw volume
- Need to format the volume
  - #mkfs -t ext4 /dev/xvdf
  - In windows we will do NTFS instead of ext4
- Now to mount
  - #mkdir /appdata
  - #mount /dev/xvdf /appdata
- Change to the folder /appdata and create a sample.txt file using nano
- To unmount (optional step)
  - #umount /dev/xvdf

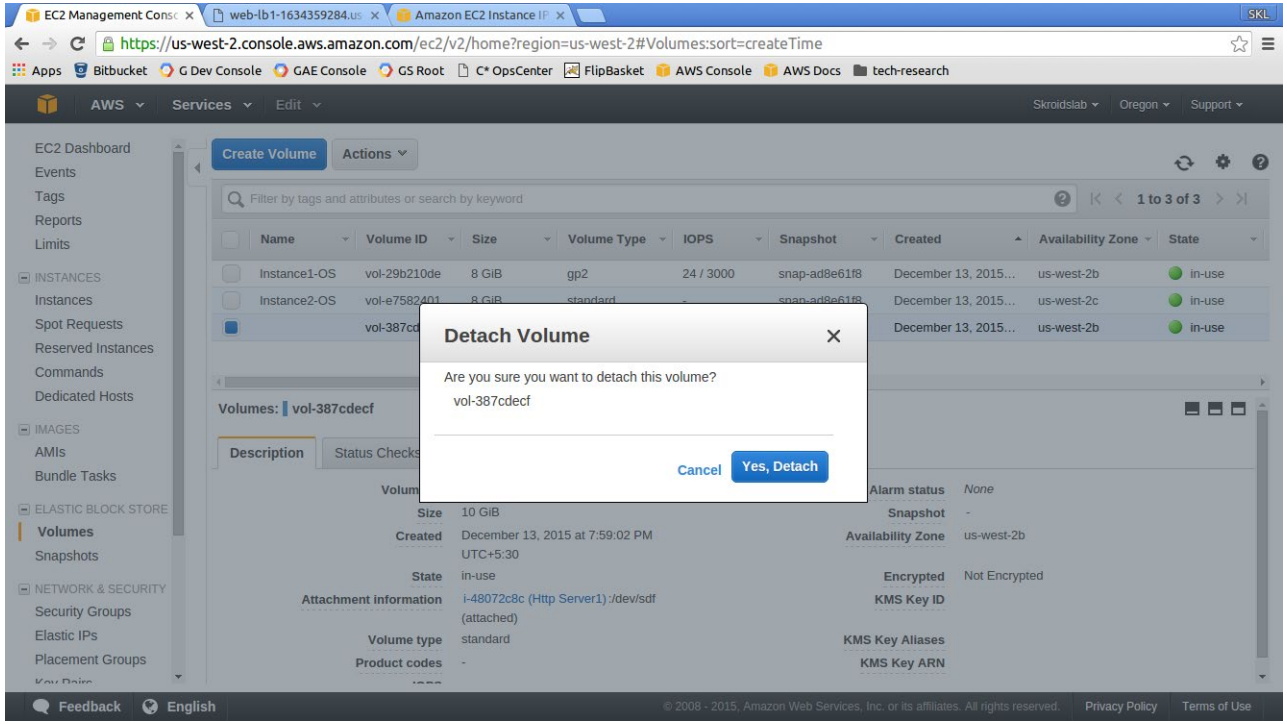
```
[root@ip-172-31-44-93 html]# lsblk
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda    202:0    0   8G  0 disk
└─xvda1 202:1    0   8G  0 part /
xvdf    202:80   0  10G  0 disk
[root@ip-172-31-44-93 html]# mkfs -t ext4 /dev/xvdf
mke2fs 1.42.12 (29-Aug-2014)
Creating filesystem with 2621440 4k blocks and 655360 inodes
Filesystem UUID: 34978822-7044-45c8-9b79-fa3fe2f4da24
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

[root@ip-172-31-44-93 html]# mkdir /appdata
[root@ip-172-31-44-93 html]# mount /dev/xvdf /appdata
[root@ip-172-31-44-93 html]# cd /appdata/
[root@ip-172-31-44-93 appdata]# ls -al
total 24
drwxr-xr-x  3 root root  4096 Dec 13 14:42 .
dr-xr-xr-x 26 root root  4096 Dec 13 14:44 ..
drwx------  2 root root 16384 Dec 13 14:42 lost+found
[root@ip-172-31-44-93 appdata]# df -m
Filesystem     1M-blocks  Used Available Use% Mounted on
/dev/xvda1          7934  1186      6650  16% /
devtmpfs             489     1       489   1% /dev
tmpfs                498     0       498   0% /dev/shm
/dev/xvdf           9952    23      9401   1% /appdata
[root@ip-172-31-44-93 appdata]#
```

Activity - Volumes

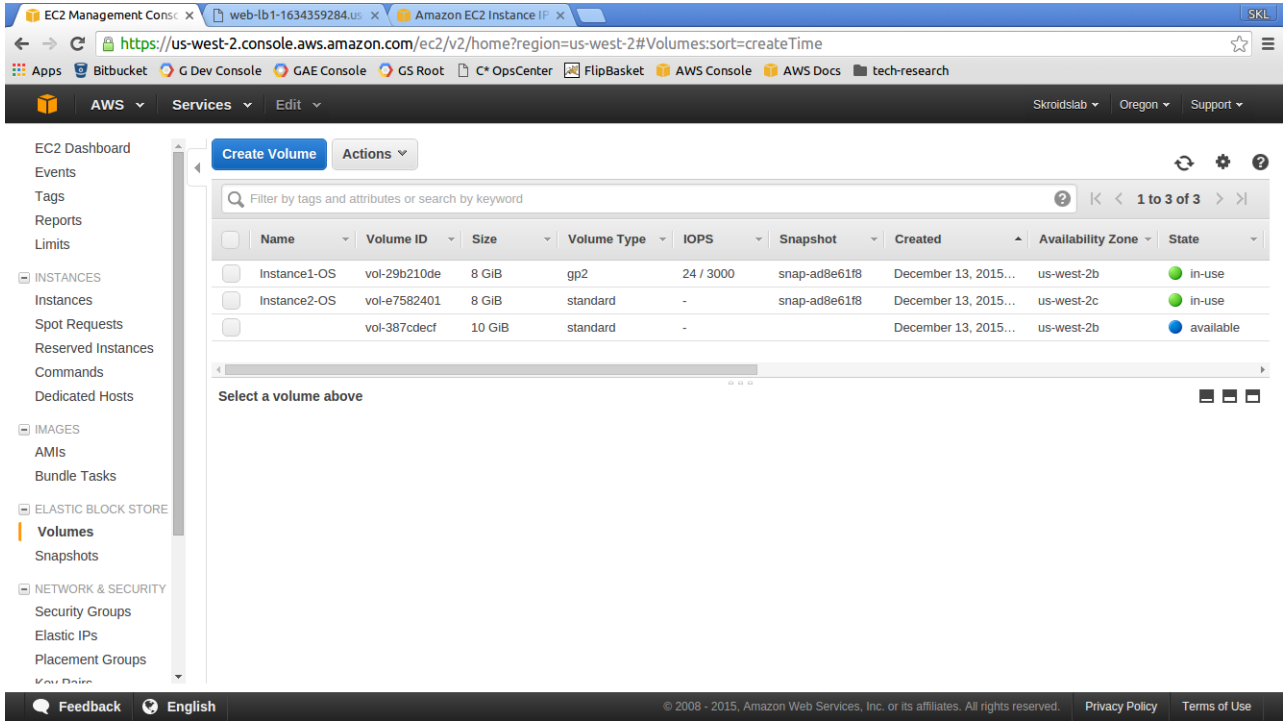
greatlearning



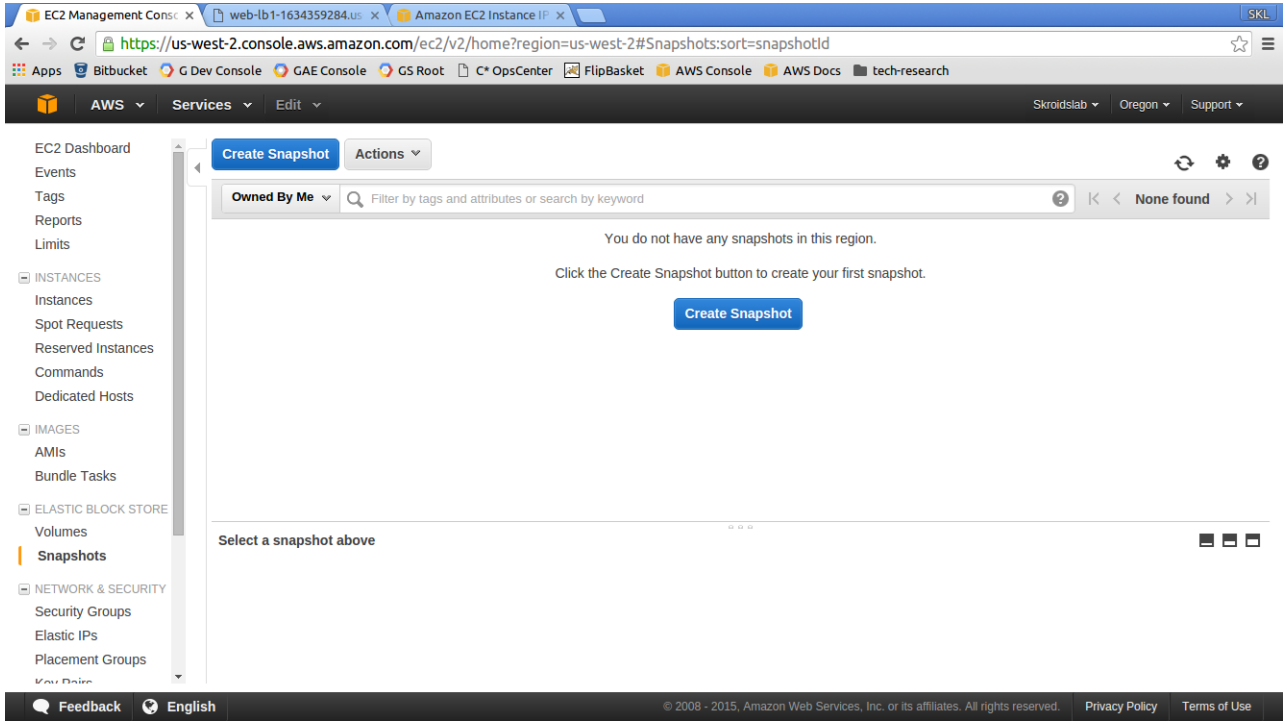
Activity - Volumes



Activity - Volumes

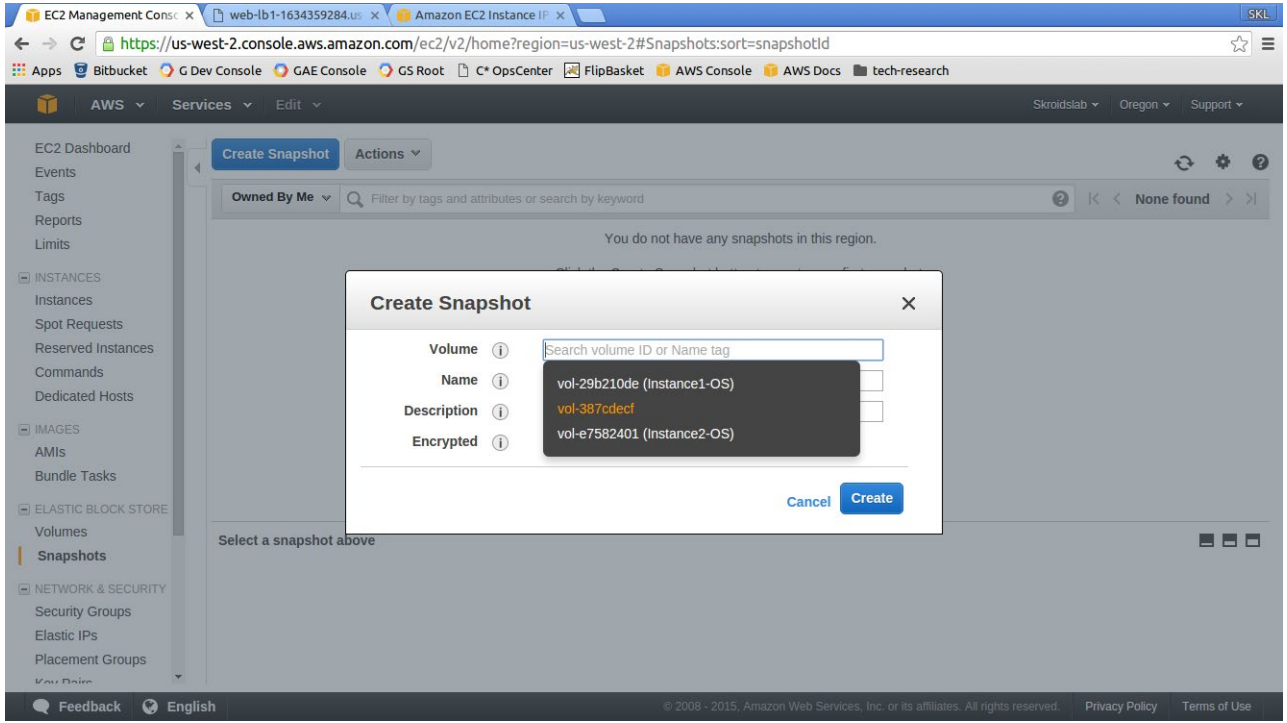


Activity - Snapshot from Volume

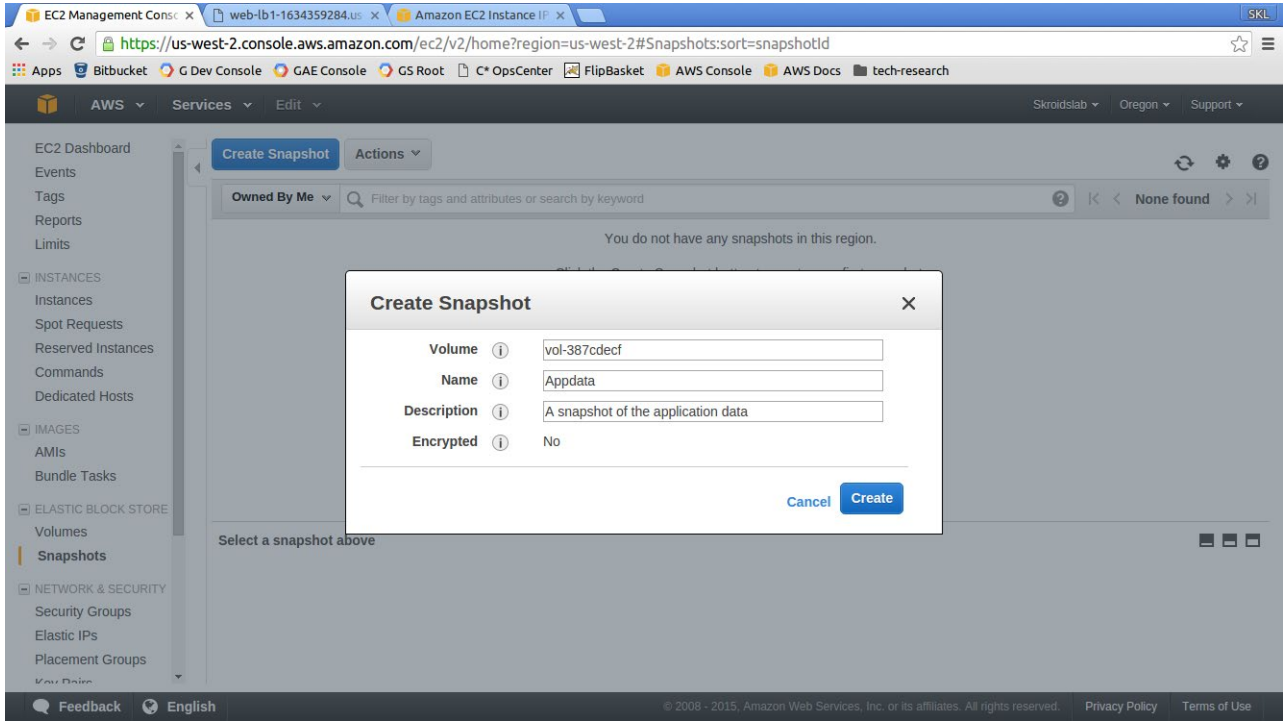


Activity - Snapshot from Volume

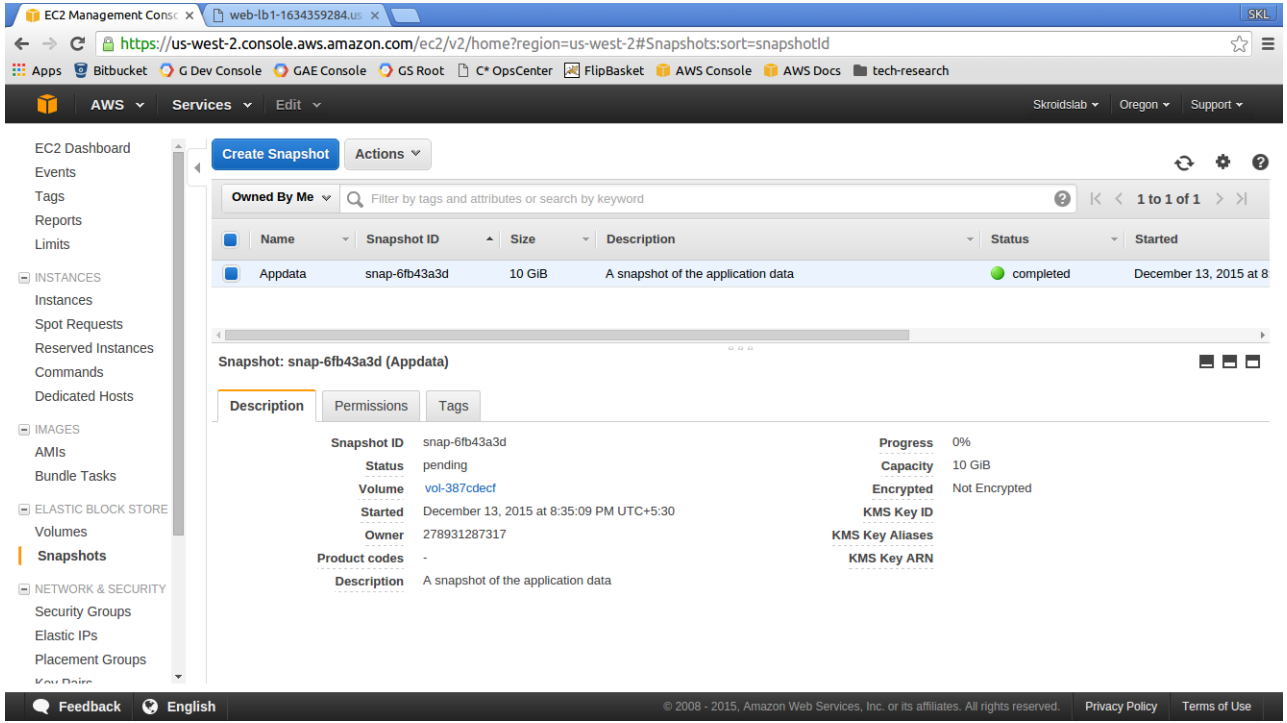
greatlearning



Activity - Snapshot from Volume

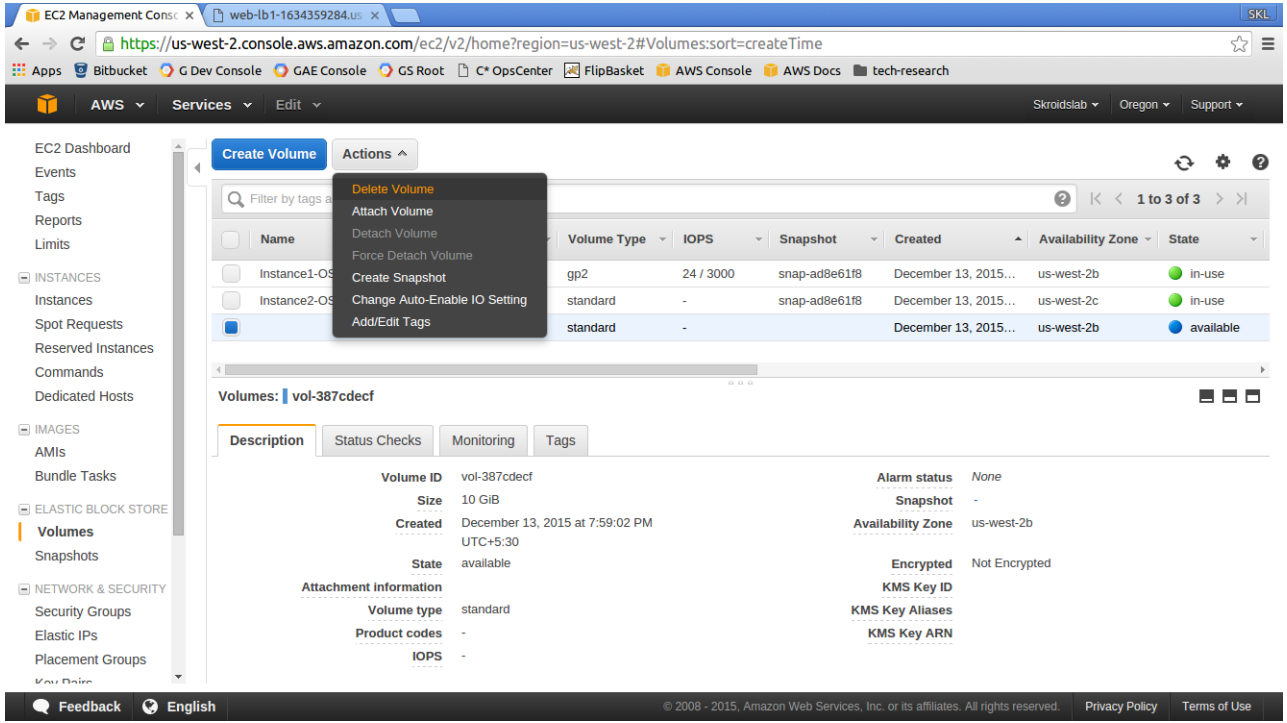


Activity - Snapshot from Volume

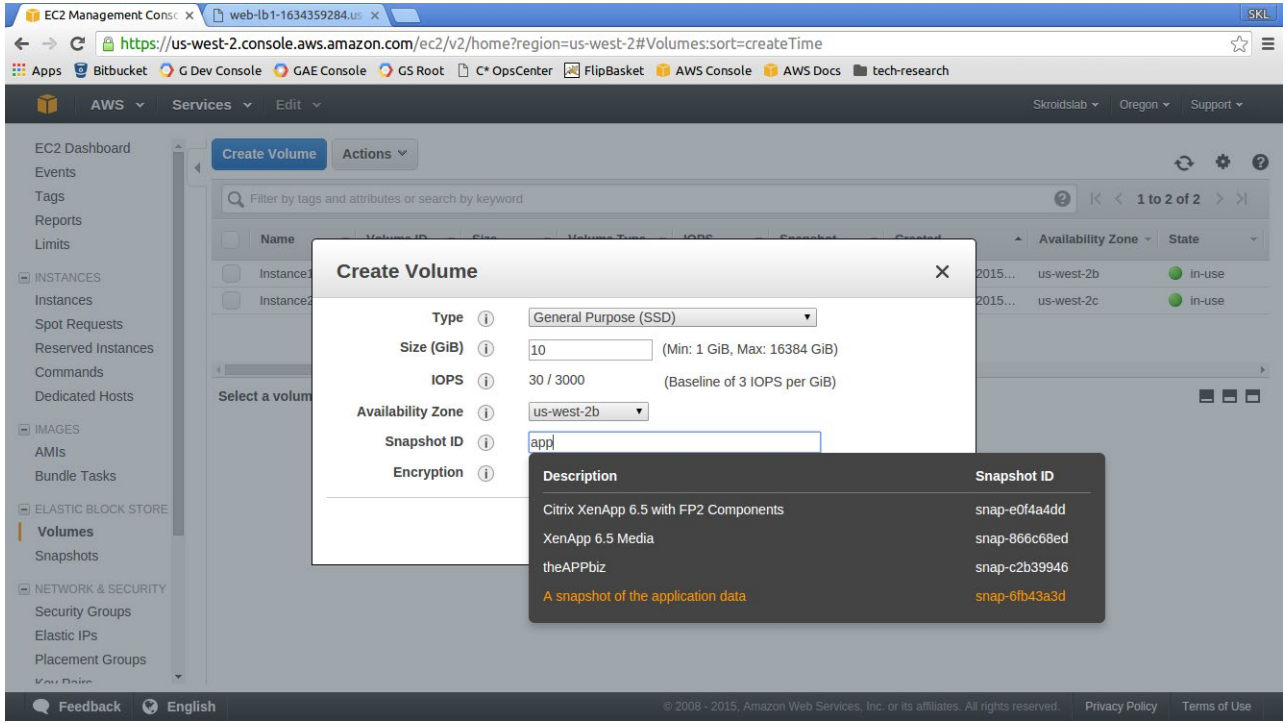


Activity - Volume from Snapshot

greatlearning



Activity - Volume from Snapshot



Activity - Volume from Snapshot

- This is also a way we can migrate data from magnetic drives to SSD
- Can use magnetic drives in stage which is cheaper but use this method to bring over some application lookup data to prod which is on SSD
- Exercise
  - Once the volume is available mount the drive to the instance
  - Verify that the data is still there!

Volumes - need more disk I/O

greatlearning

- Have the max possible EBS volume size with max I/O, but we need more! E.g. vertically scaling a DB server
- Add multiple EBS volumes and create a RAID
- RAID is Redundant Array of Independent Disks
  - 0 = Striped, no redundancy, good performance
  - 1 = Mirrored, redundancy
  - 5 = good reads, bad write performance, AWS does not recommend
  - 10 (1+0) = Striped Mirrored, Good redundancy and performance
  - http://www.thegeekstuff.com/2010/08/raid-levels-tutorial
- How to do RAID on EBS in AWS linux?
  - http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html
- Alternatively if possible consider horizontal elasticity instead of vertical
- Snapshot from a RAID options
  - Shutdown the EC2 instance and then snapshot the RAID array (common option)
  - Freeze the file system (stop the app from writing), unmount the array and then snapshot

greatlearning

Storage and Content Delivery

Elastic File System - EFS

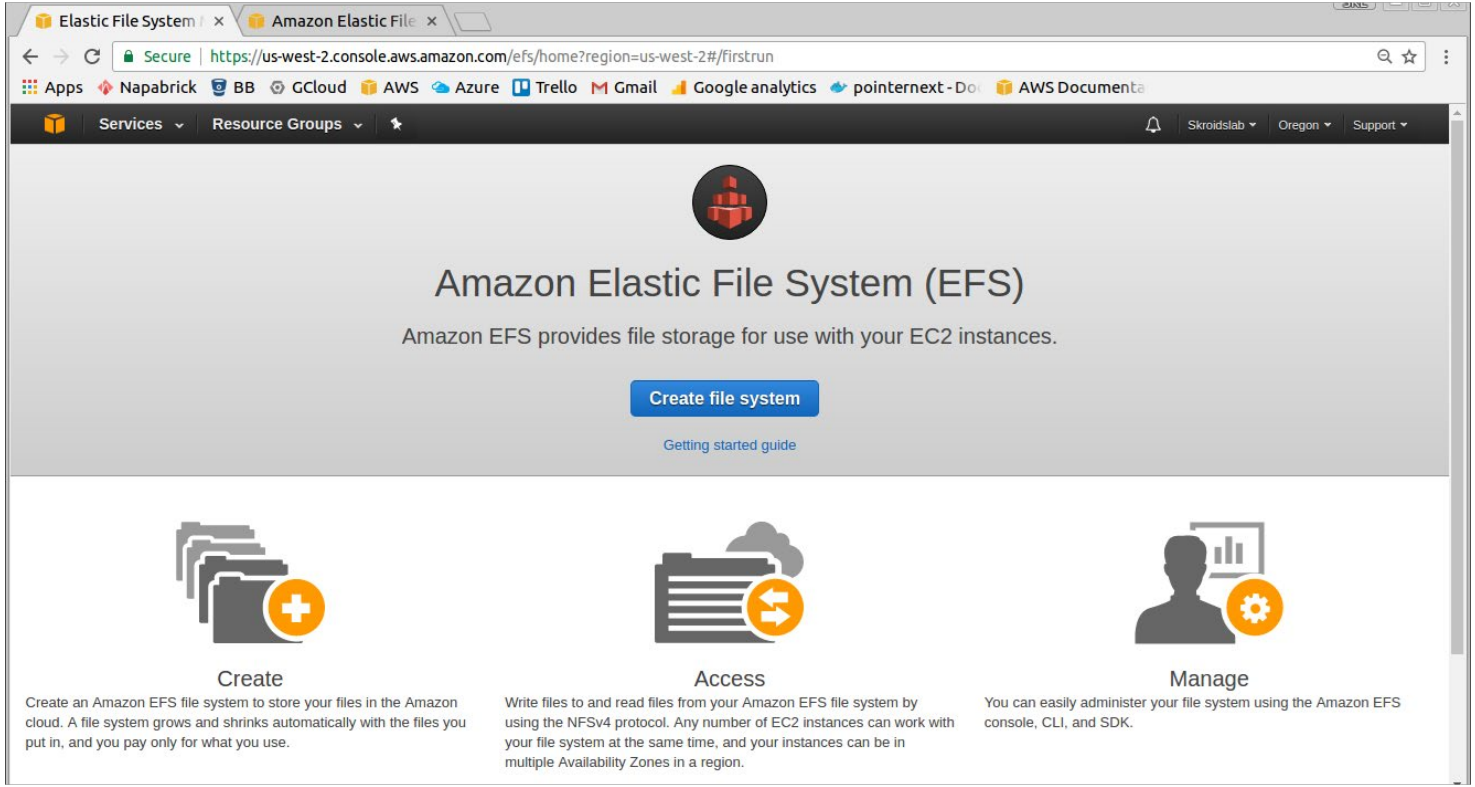
Activity - EFS

greatlearning

- Elastic file system - storage capacity is elastic, growing and shrinking automatically as you add and remove files online EBS which is of a fixed capacity
- EBS cannot be mounted to multiple EC2 instances while EFS can be
- Supports NFSv4 (Network File System)
- Block based storage (S3 is object based storage)
- Read after write consistency (eventual for overwrites of existing data)
- To be used as a file server, scale to petabytes
- Common repo of files for different EC2 instances
- Create access rules at the folder or file level

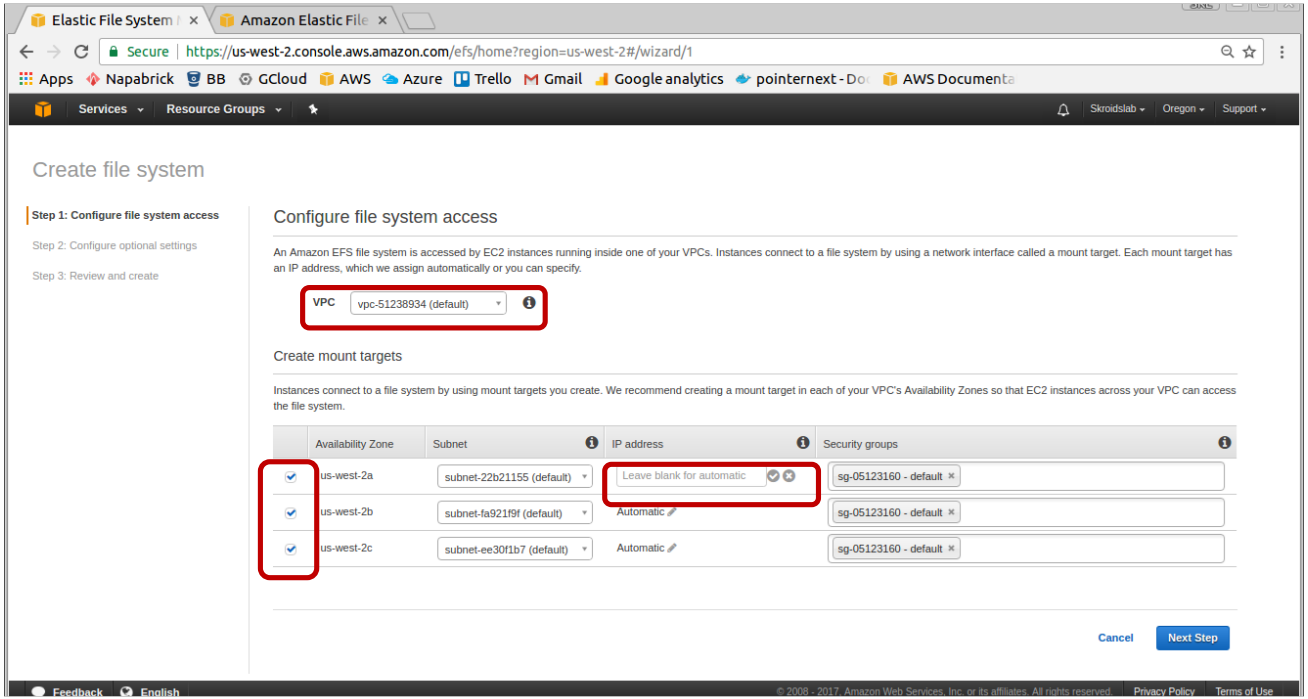
Activity - EFS

greatlearning

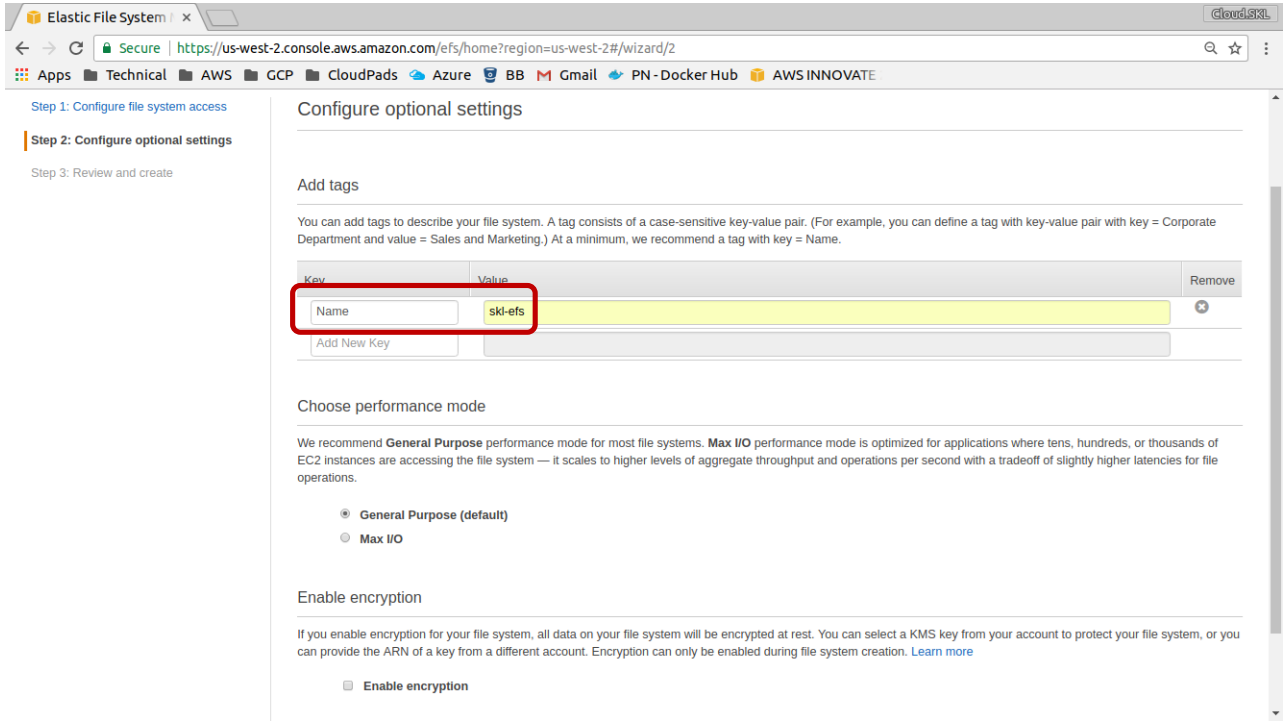


Activity - EFS

greatlearning

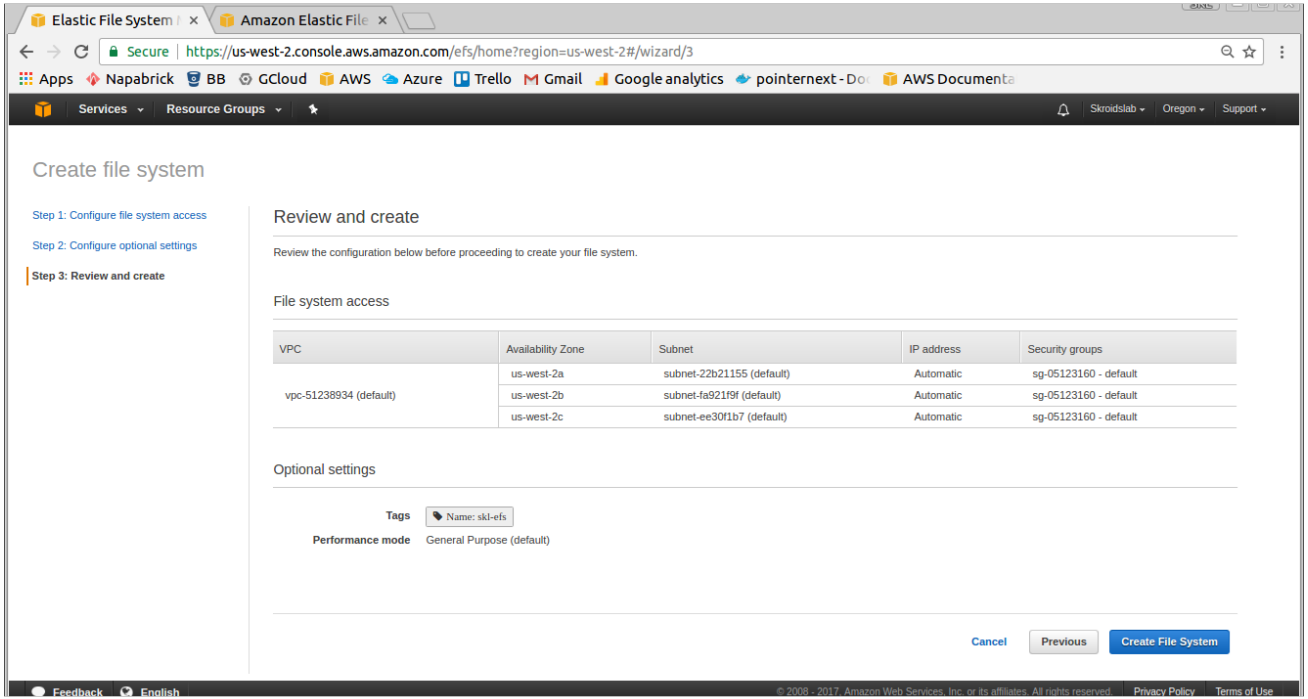


Activity - EFS



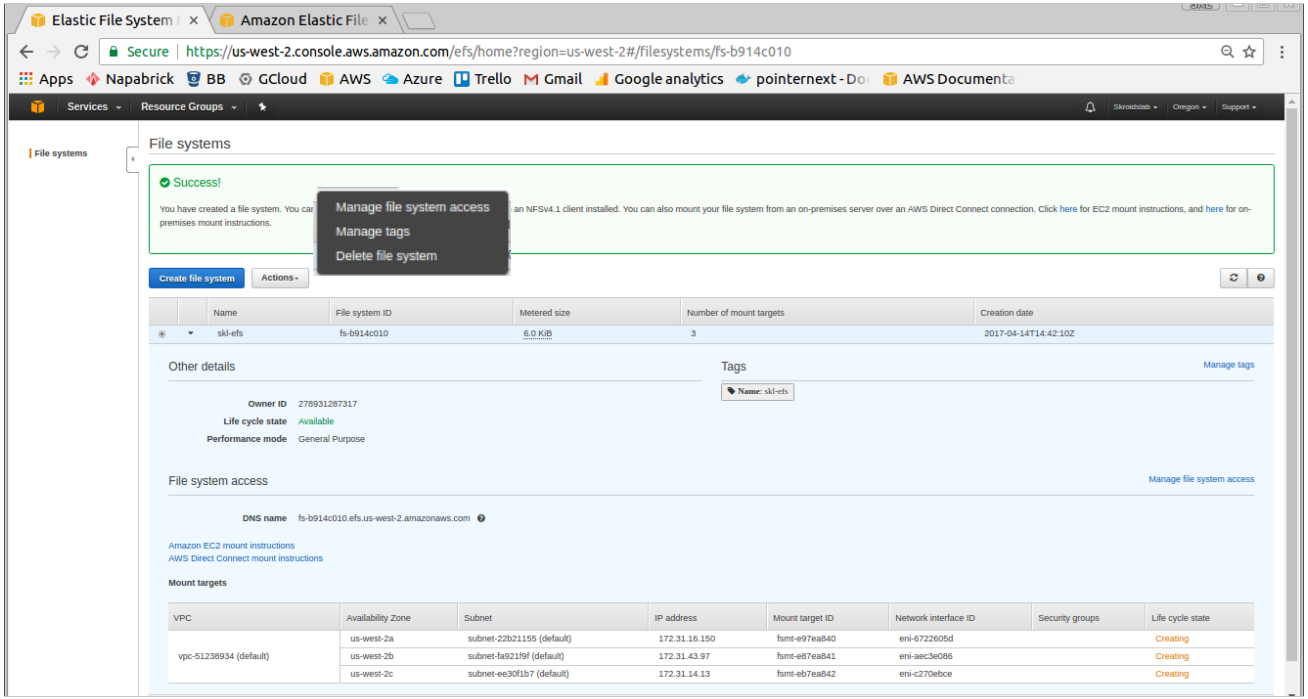
Activity - EFS

greatlearning

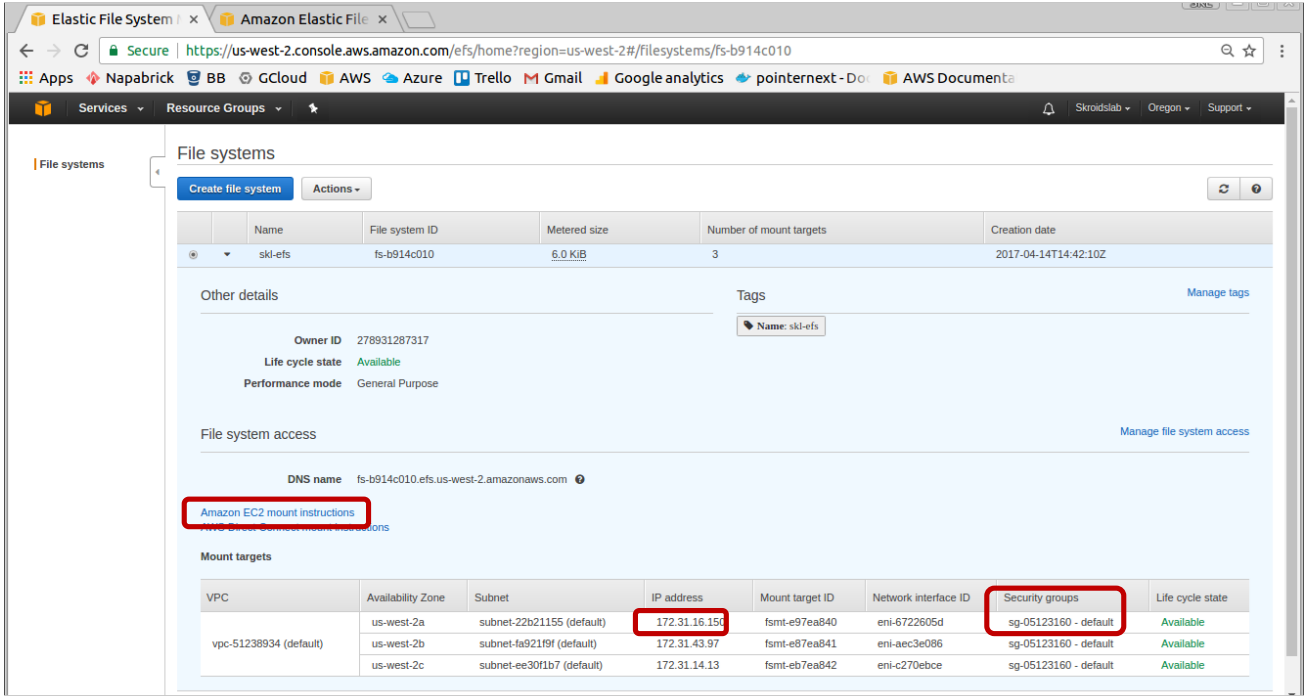


Activity - EFS

greatlearning

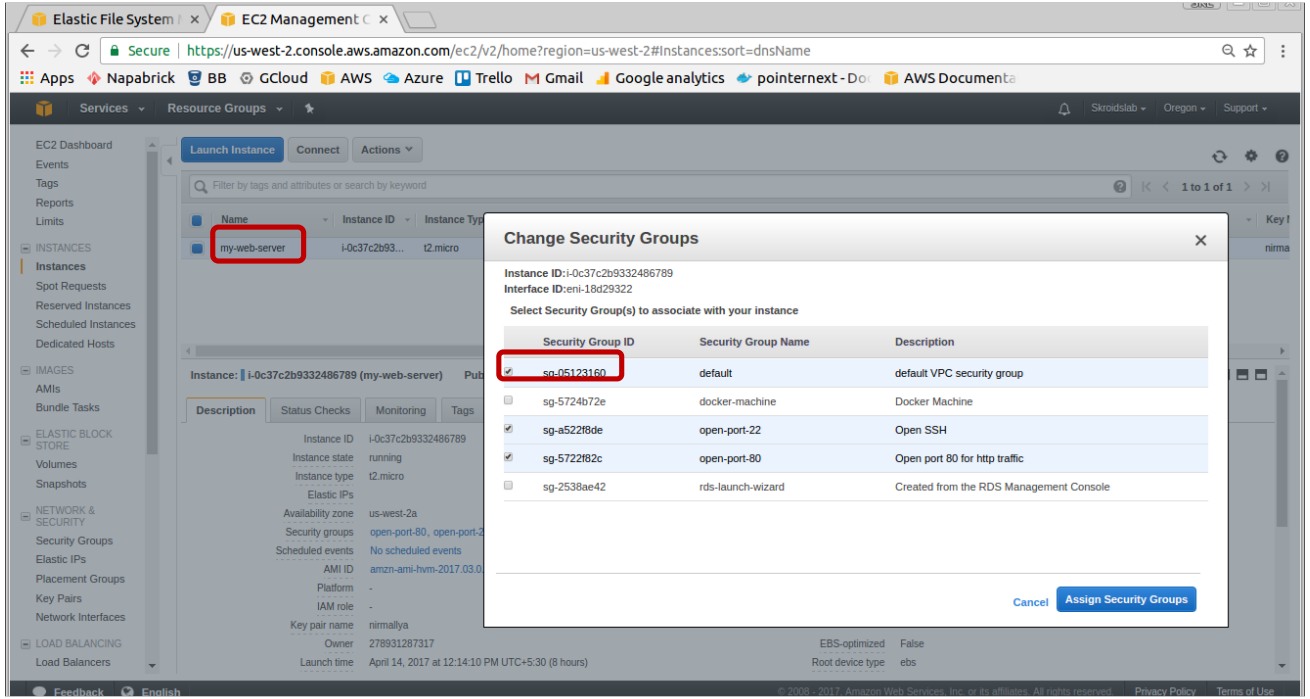


Activity - EFS



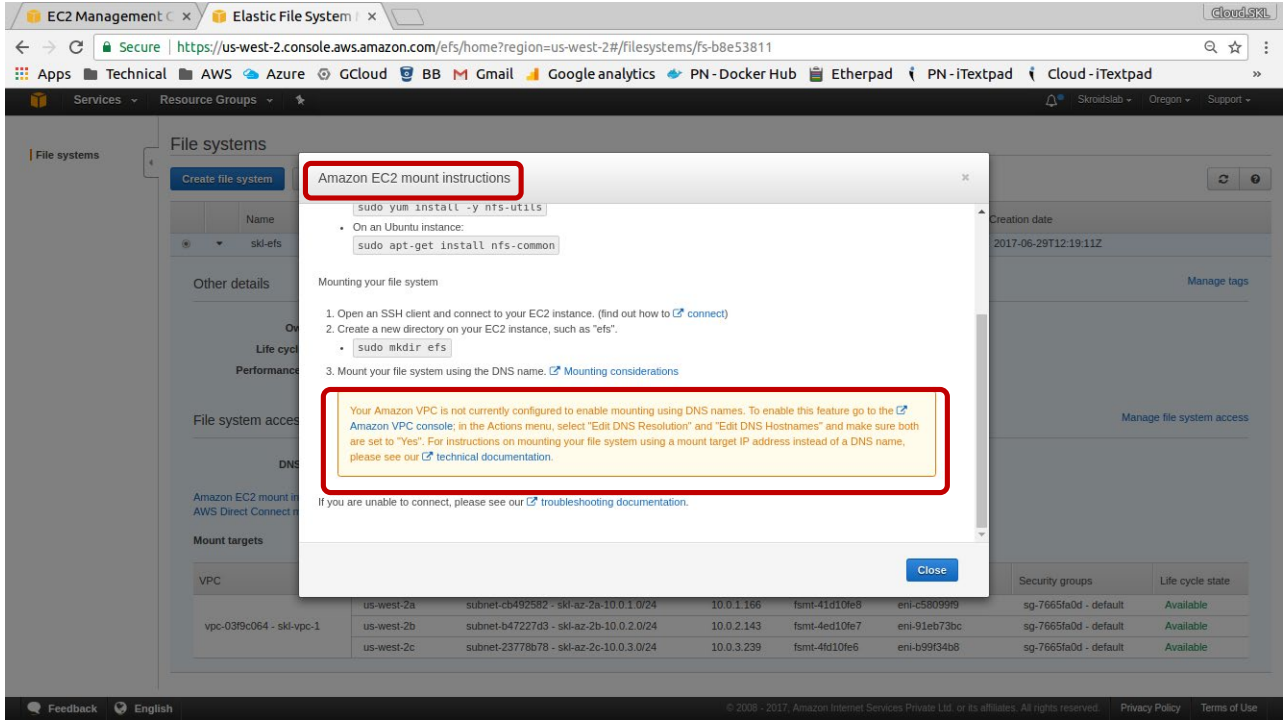
Note - EC2 instance must have this default VPC security group added. Also note the public IP address which you can use to mount using AWS Direct Connect in your own DC

Activity - EC2 instance SG change



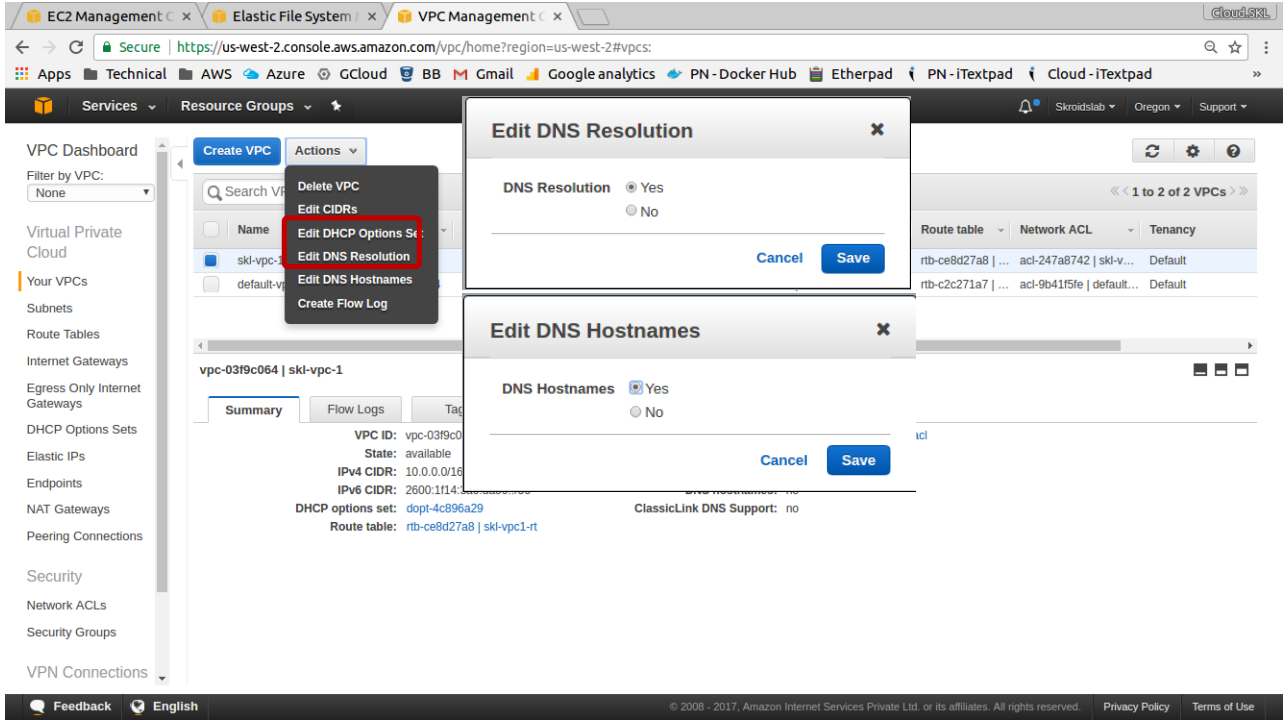
Activity - EFS

greatlearning



In case you have the EC2 instance on a custom VPC and get the error then follow along else skip the VPC setting

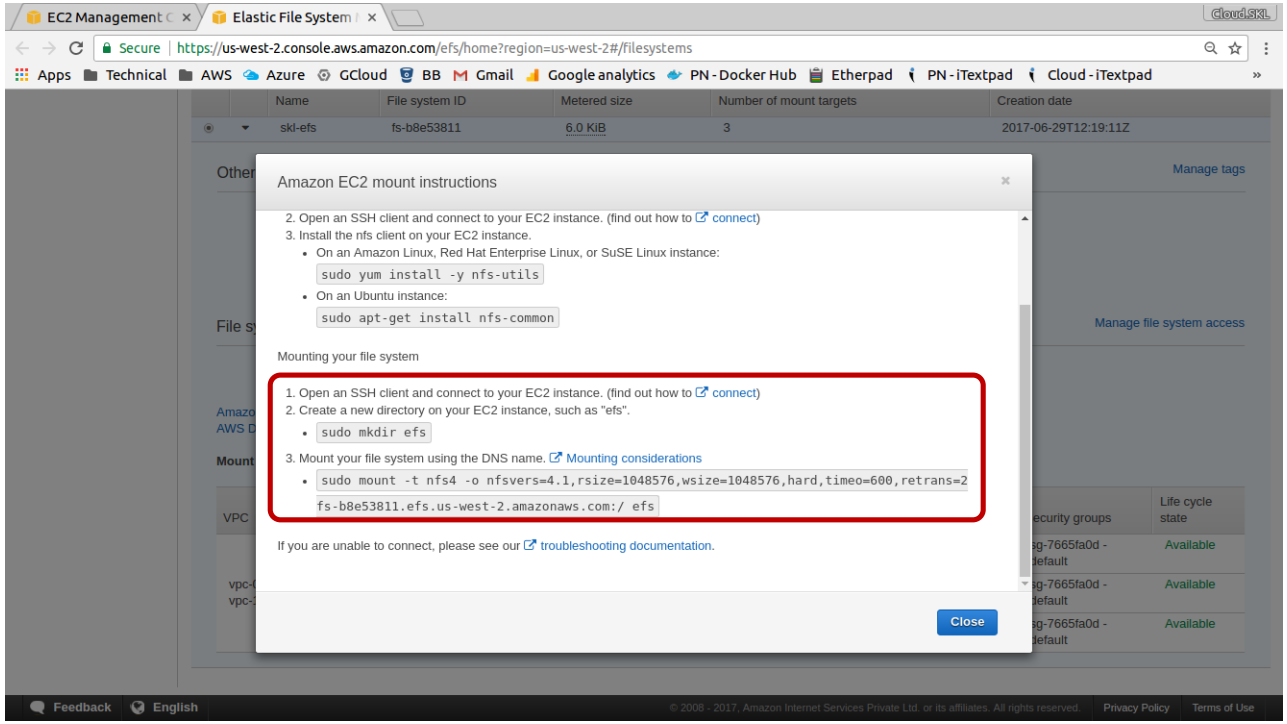
Activity - VPC setup



Select the custom VPC and enable both DNS resolution and hostnames.

Activity - EFS

greatlearning



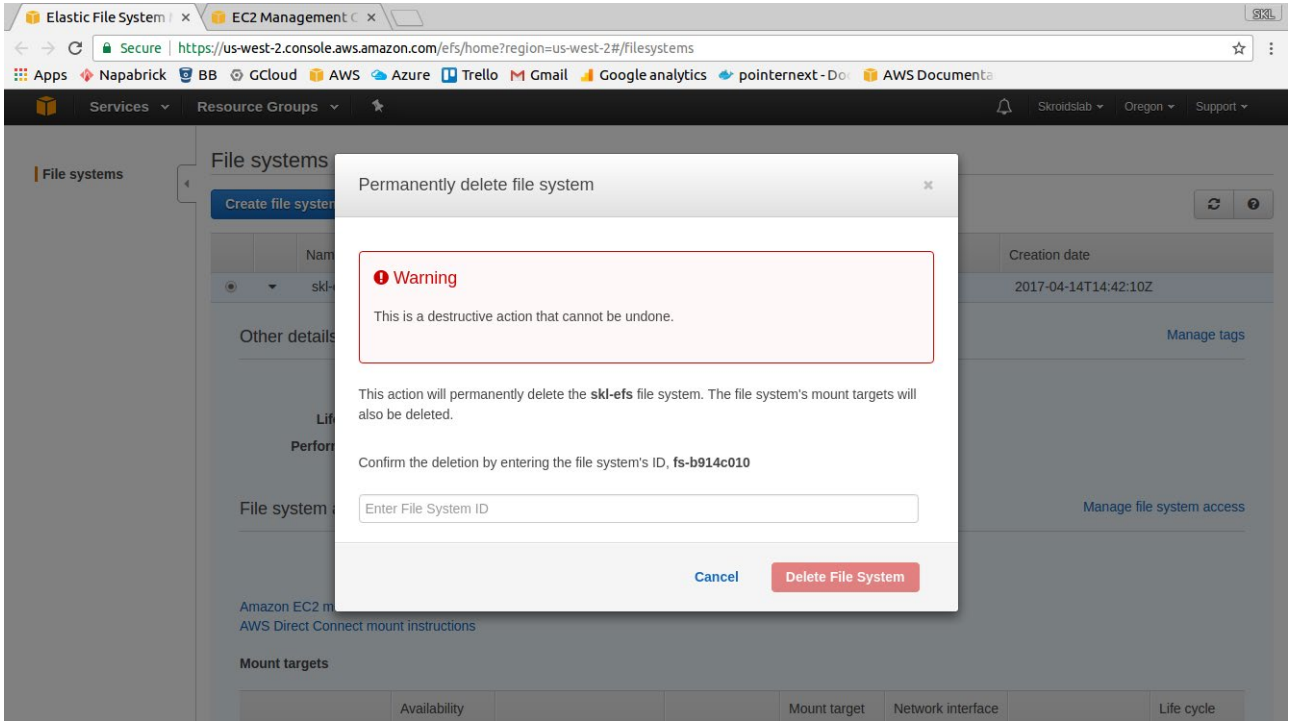
Popup after clicking on "EC2 mount instructions" link

Activity - EFS

greatlearning

- SSH to the EC2 instance
- $ sudo mkdir /opt/efs
- Copy & paste the full mount command and run
- Now the EFS is mounted on /opt/efs
- Create a file in this folder
  - sudo su then use nano to create a sample file
  - Alternatively use chown ubuntu:ubuntu /opt/efs (if on ubuntu)
- You will be charged upto the file size
- Good option for common files like HTML powering websites, store once and let all web servers access the same
- **Exercise** - Create another EC2 instance in a different AZ and follow the same process as above to mount the EFS and you can start sharing files
- To unmount use #umount /opt/efs

Activity - EFS



greatlearning

Storage and Content Delivery

S3

Simple storage service - S3

greatlearning

- Object based, allows file based storage (fyi ... Dropbox is powered by S3)
- At the root there are buckets
- A bucket is like a namespace, so it is globally unique in the given region
  - E.g. if you name a bucket "MySpace", no one else in that region can use it
- Files can be 0 bytes up to 5TB
- 100 buckets per account limit (raise a service request if you need more)
- You get a http 200 code if the upload was good
- Key value metadata is allowed
- Versioning
  - Versioning cannot be disabled if enabled, can be suspended
- Life cycle management
  - Can be used in connection with versioning
  - Can be applied to current and older versions
  - Options - Archive only, Permanent Delete only, Archive and then Perm delete
- 99.9% guarantee availability but built for 99.99% availability for "standard" S3
- Types
  - Standard storage (eleven 9's durability), very low probability of data loss
  - Infrequently accessed but rapid access when needed, low save fee but costs to retrieve (min size 128kb and 30 days after creation date)
  - Reduced redundancy storage (RRS, 99.99% durability), may lose data, eg storing thumbnails etc
  - Glacier - really cheap, but takes hours to fetch (good for archival only, 30 days after IA if applicable)

Simple storage service - S3

greatlearning

- Encryption
  - Upload to S3 via SSL endpoints
  - Encrypt data at rest
  - Manage keys - AWS key management, S3 manages keys, provide your own
  - Good read http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html
- Security
  - All buckets are private by default
  - ACL can be defined at the user level along with privileges of read only etc
  - Can integrate with IAM with roles
  - End points are encrypted by SSL
- Static websites can be easily hosted, no web server is needed
  - Scales automatically
  - Can use route 53 and point to a custom domain
- Integrates with CloudFront (CDN)
- Supports multi-part files (any file > 5GB needs to be broken in parts)
- Stop and resume uploads

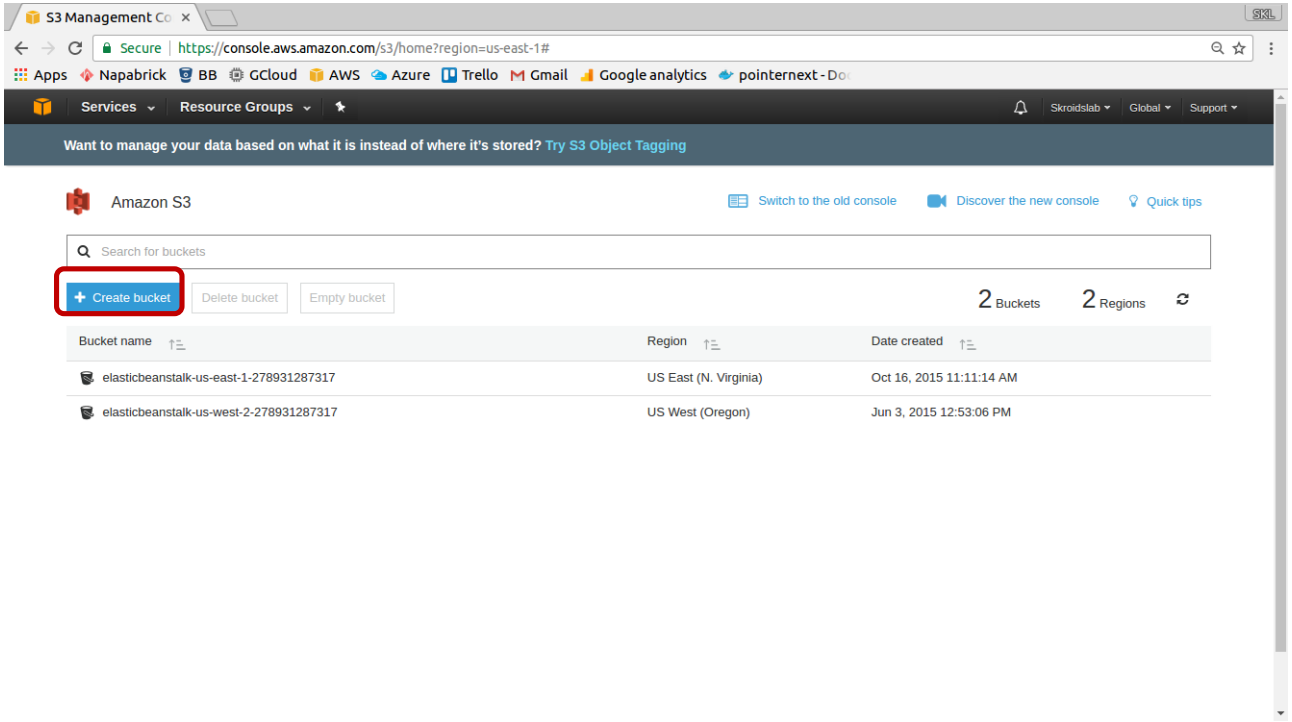
Simple storage service - S3

greatlearning

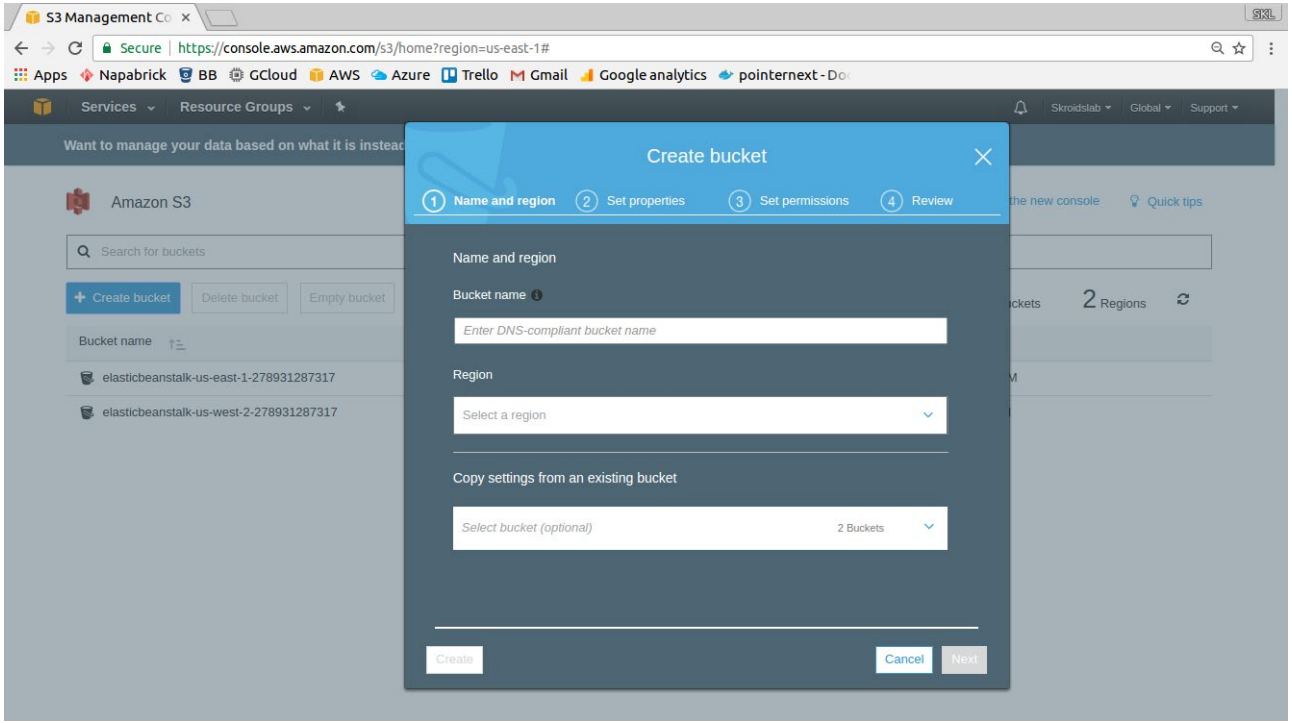
- Consistency
  - Read after write consistency for PUTS of new objects (insert a new object and it is immediately consistent)
  - Eventual consistency for overwrites across all the availability zones (also depends on file size)
- Atomic operation
  - Either new data or old data but no corruption by partial writes
- Object based storage, has the following components-
  - Key (name of the object, sorted by this field)
  - Value (actual data, sequence of bytes)
  - Version ID
  - Metadata
  - Subresources (contains access control lists)
- Charged for
  - Requests
  - Storage management including managing tags
  - Data transfer (in free, move around and serving is not)
  - Transfer acceleration (acceleration via edge location)

Activity - S3

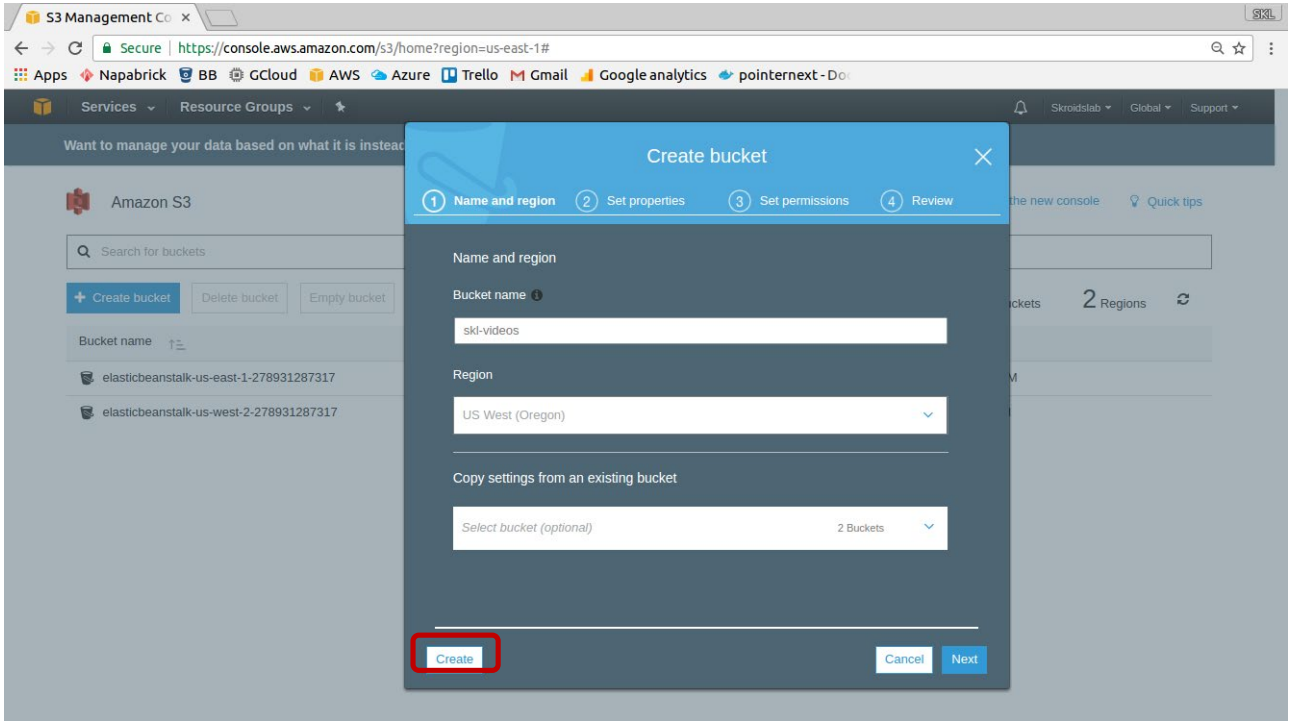
greatlearning



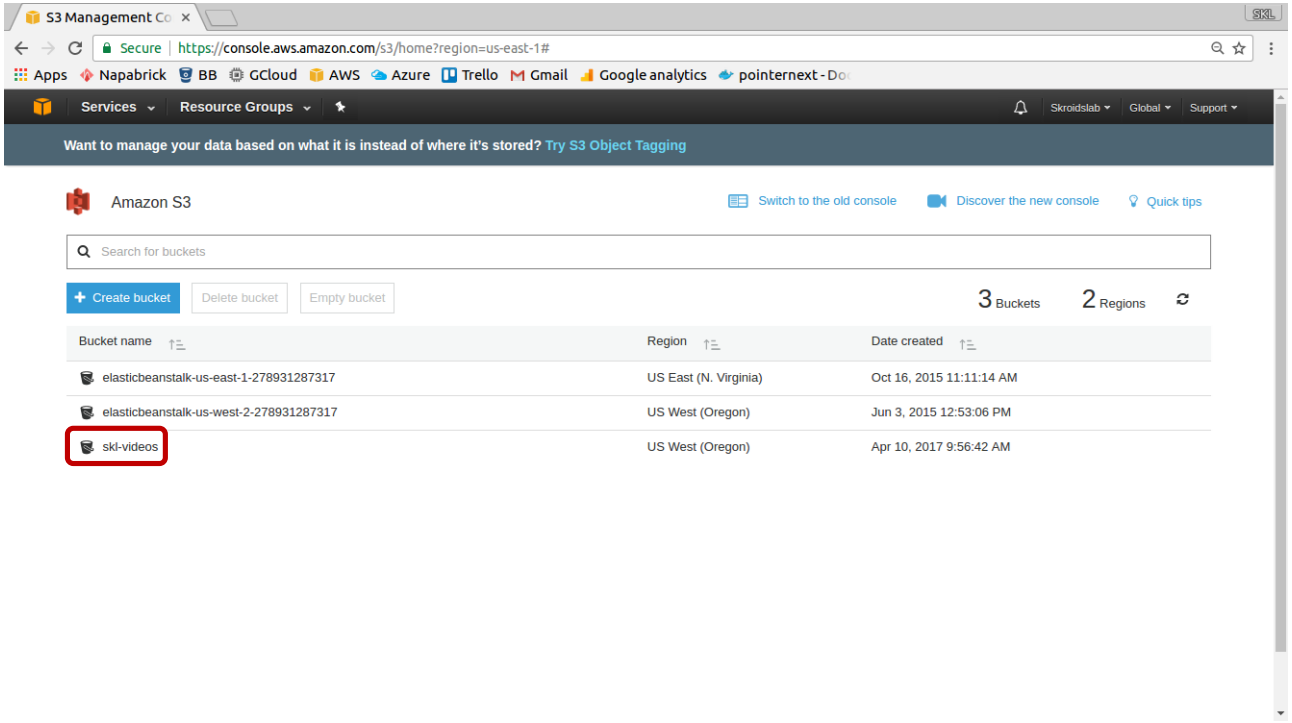
Activity - S3



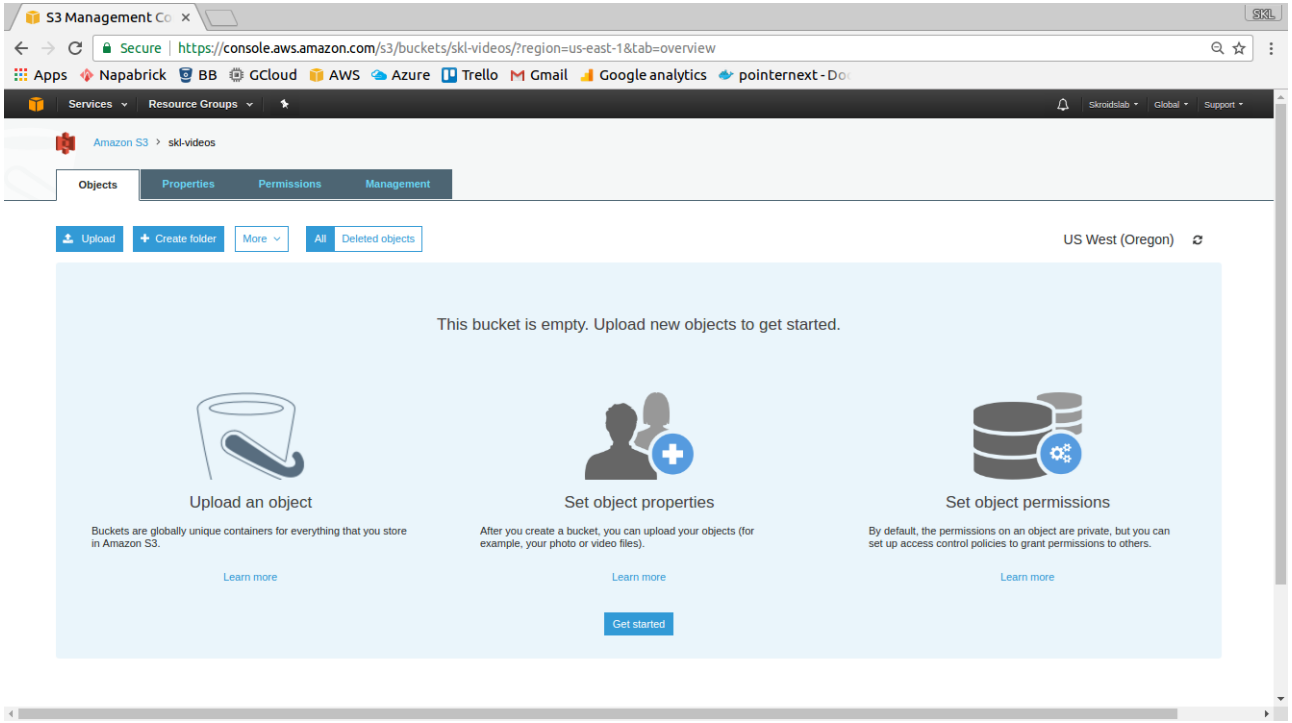
Activity - S3



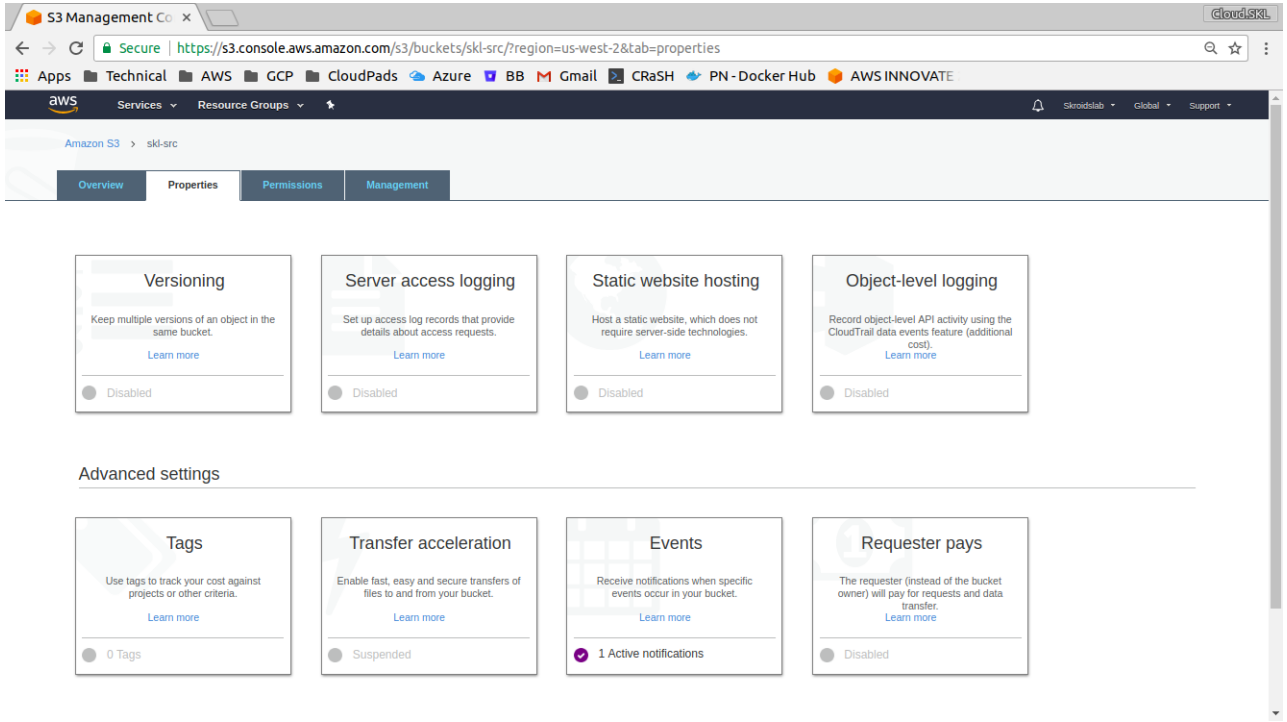
Activity - S3



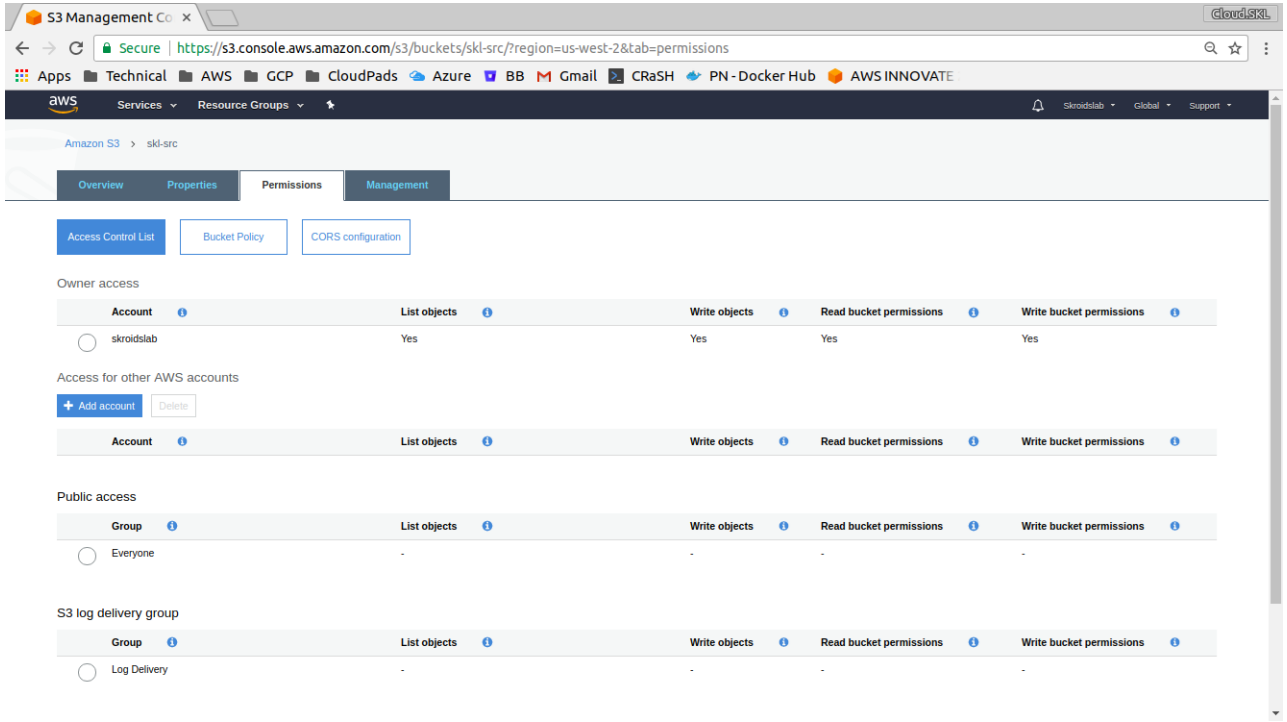
Activity - S3



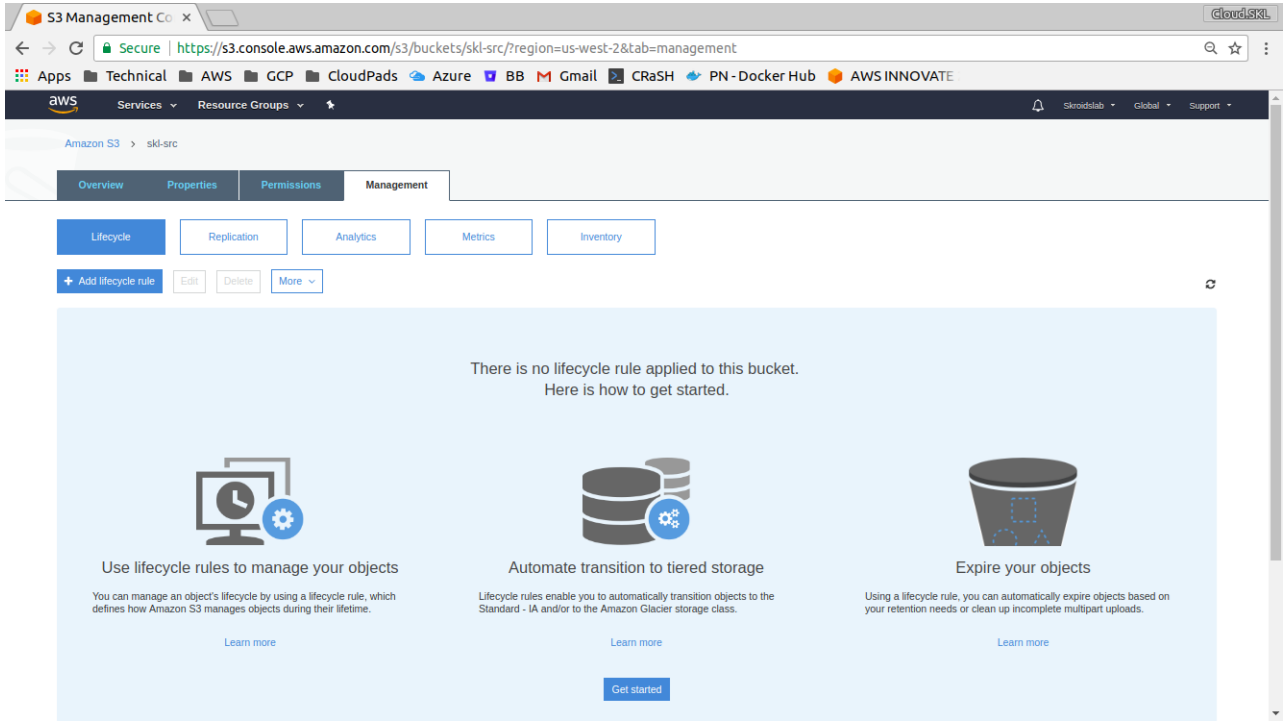
Activity - S3



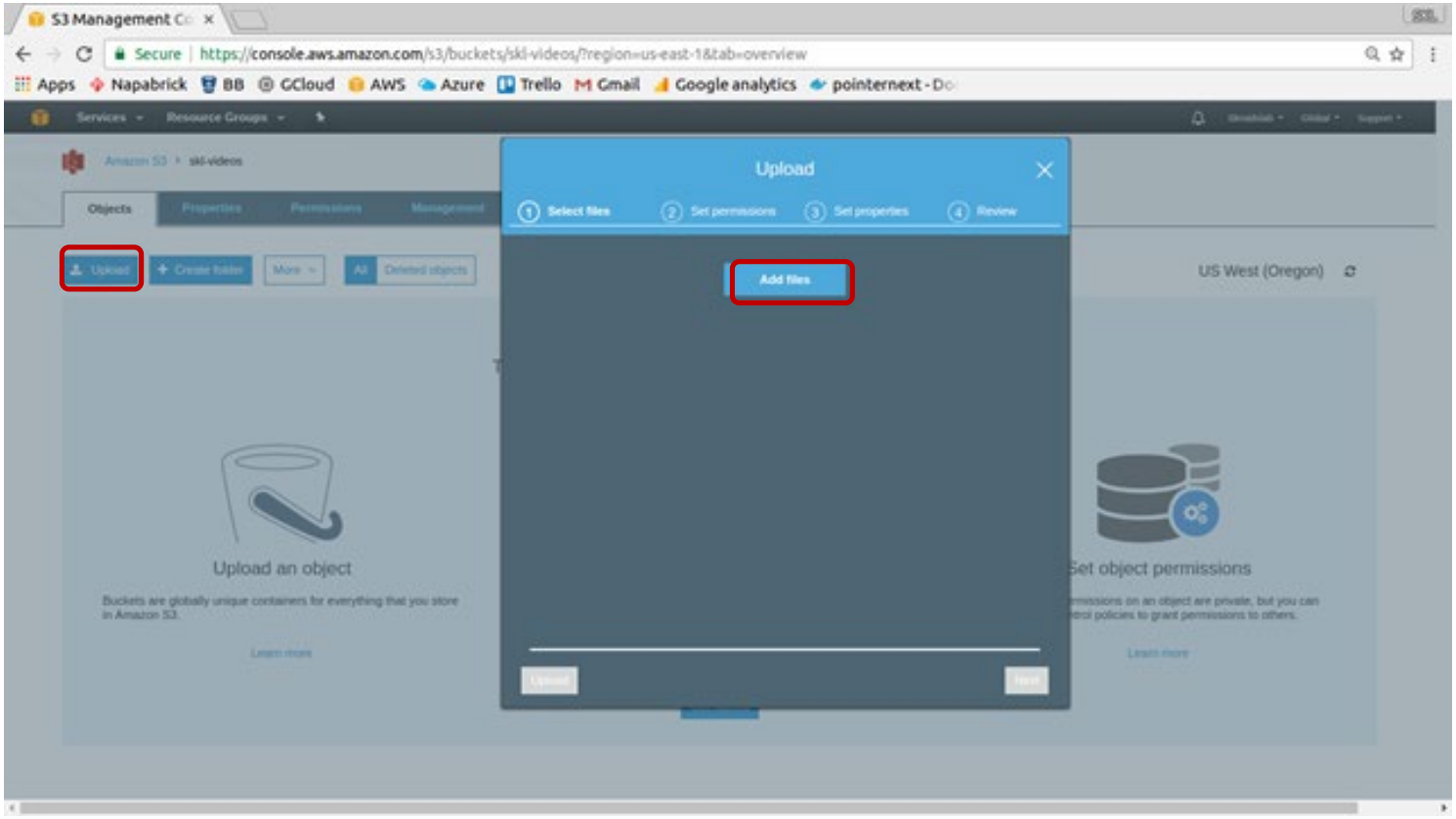
Activity - S3



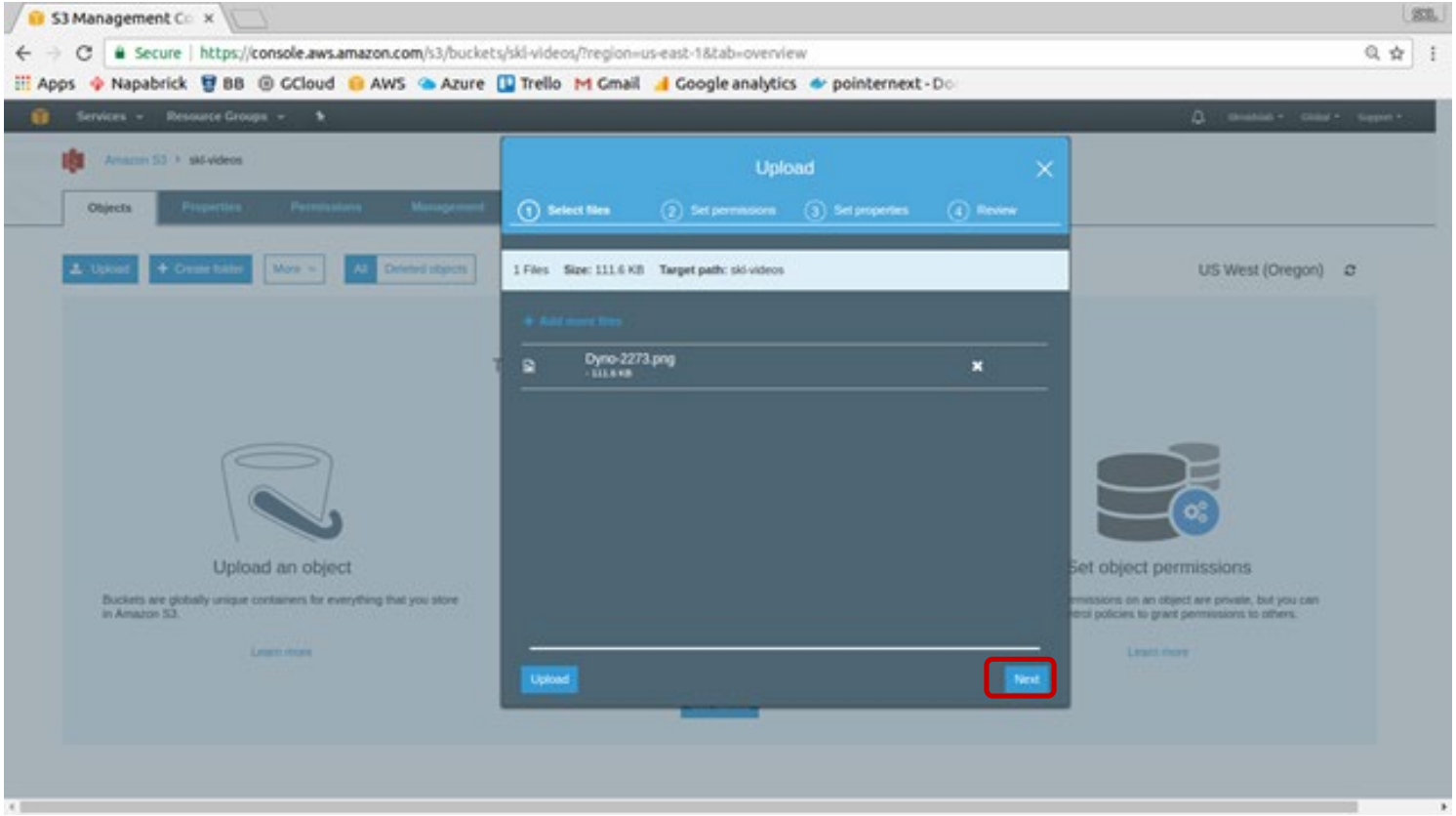
Activity - S3



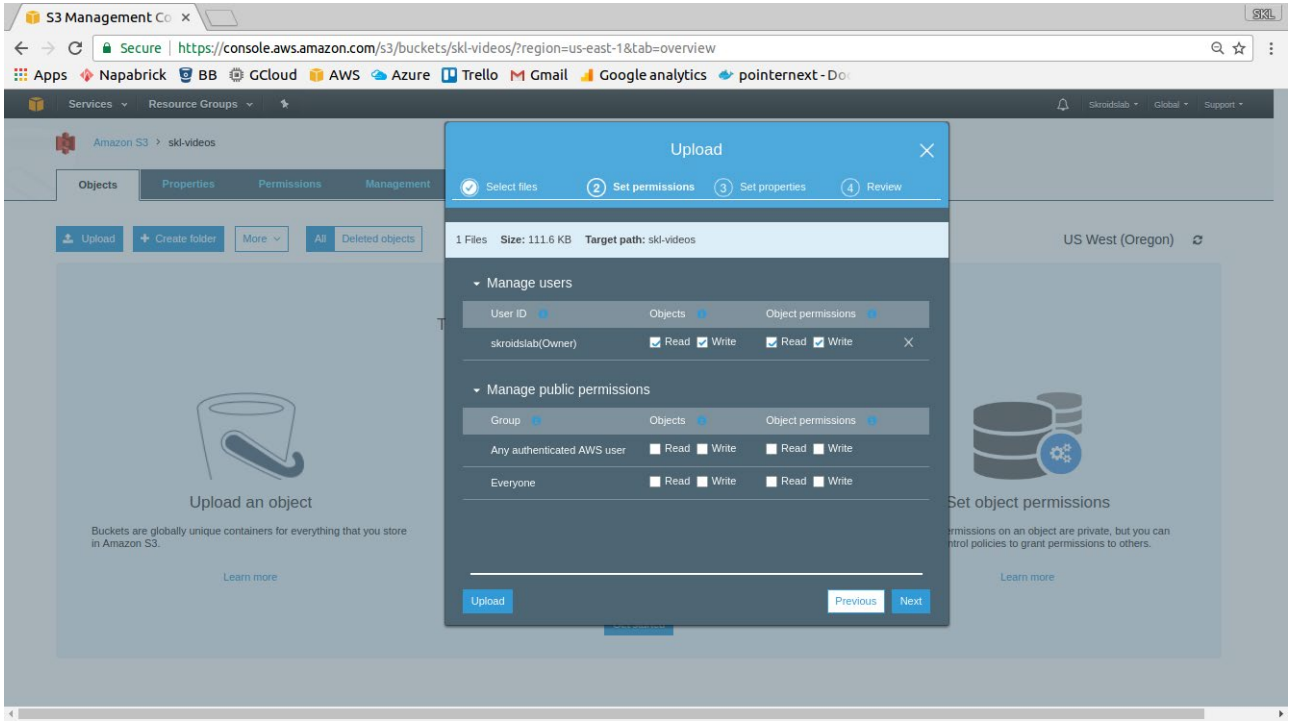
Activity - S3



Activity - S3

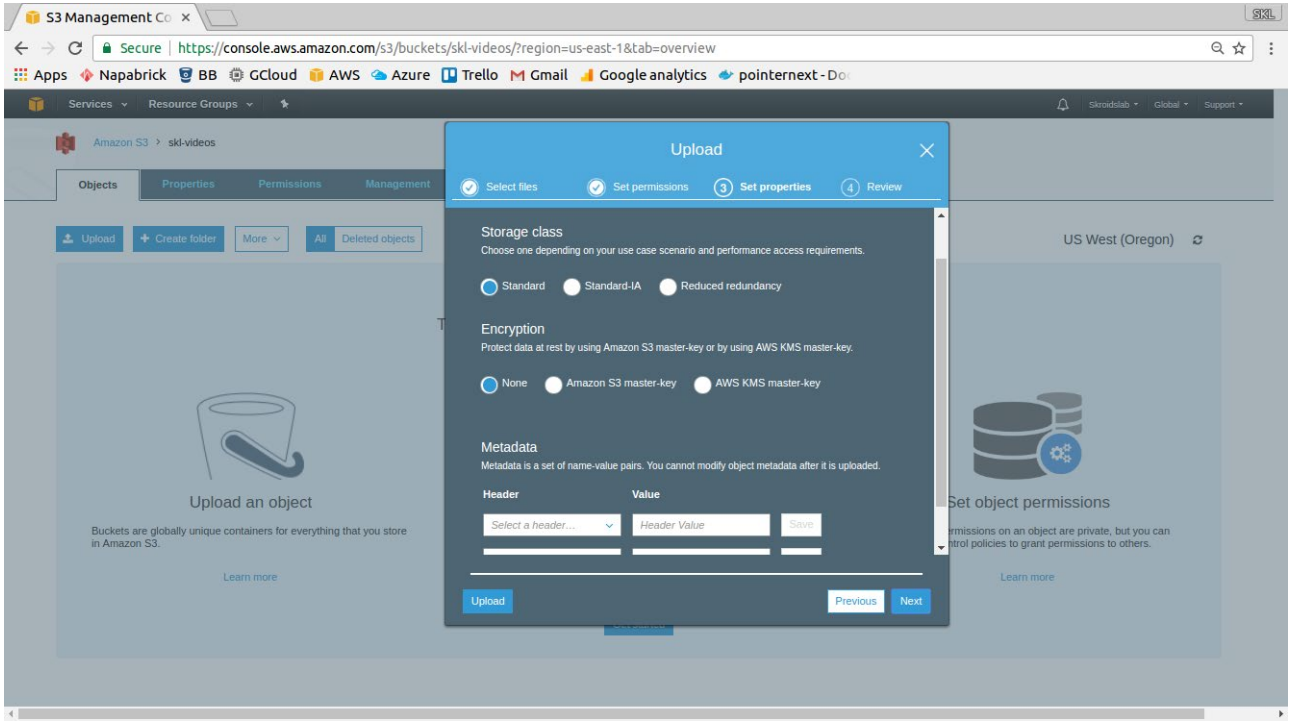


Activity - S3



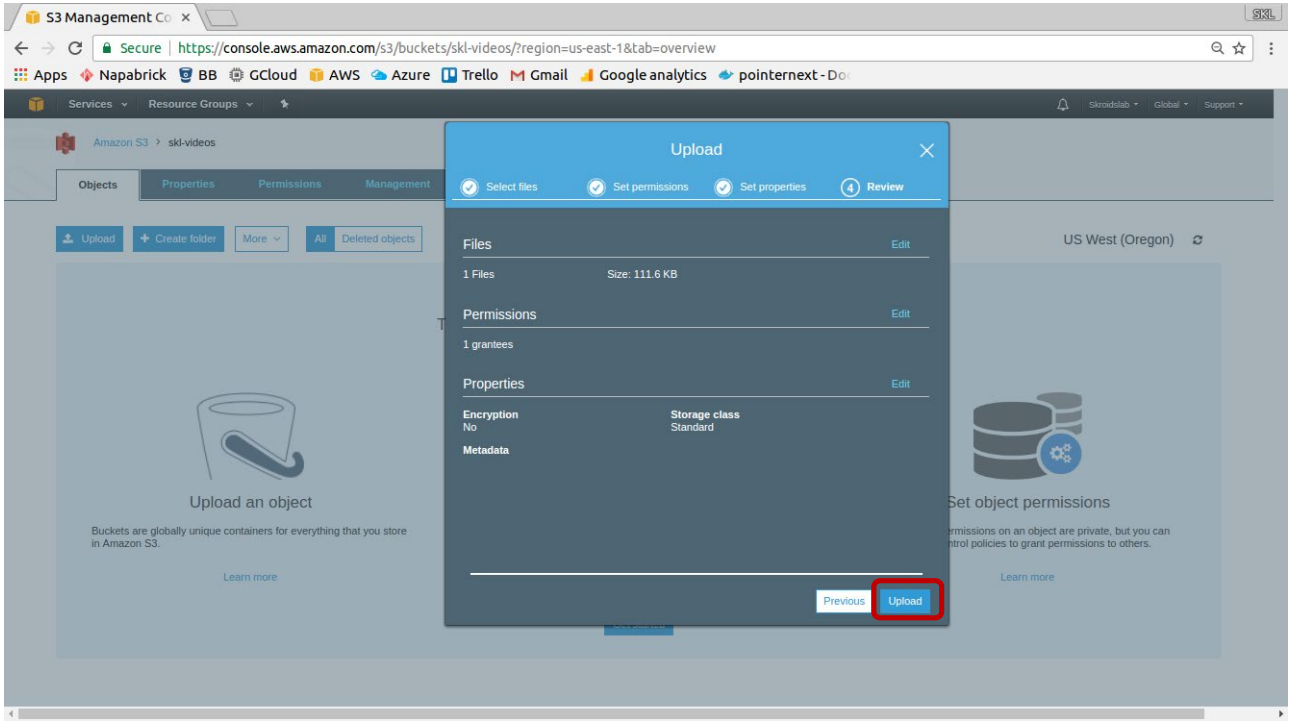
Leave all as defaults, we will modify these later

Activity - S3

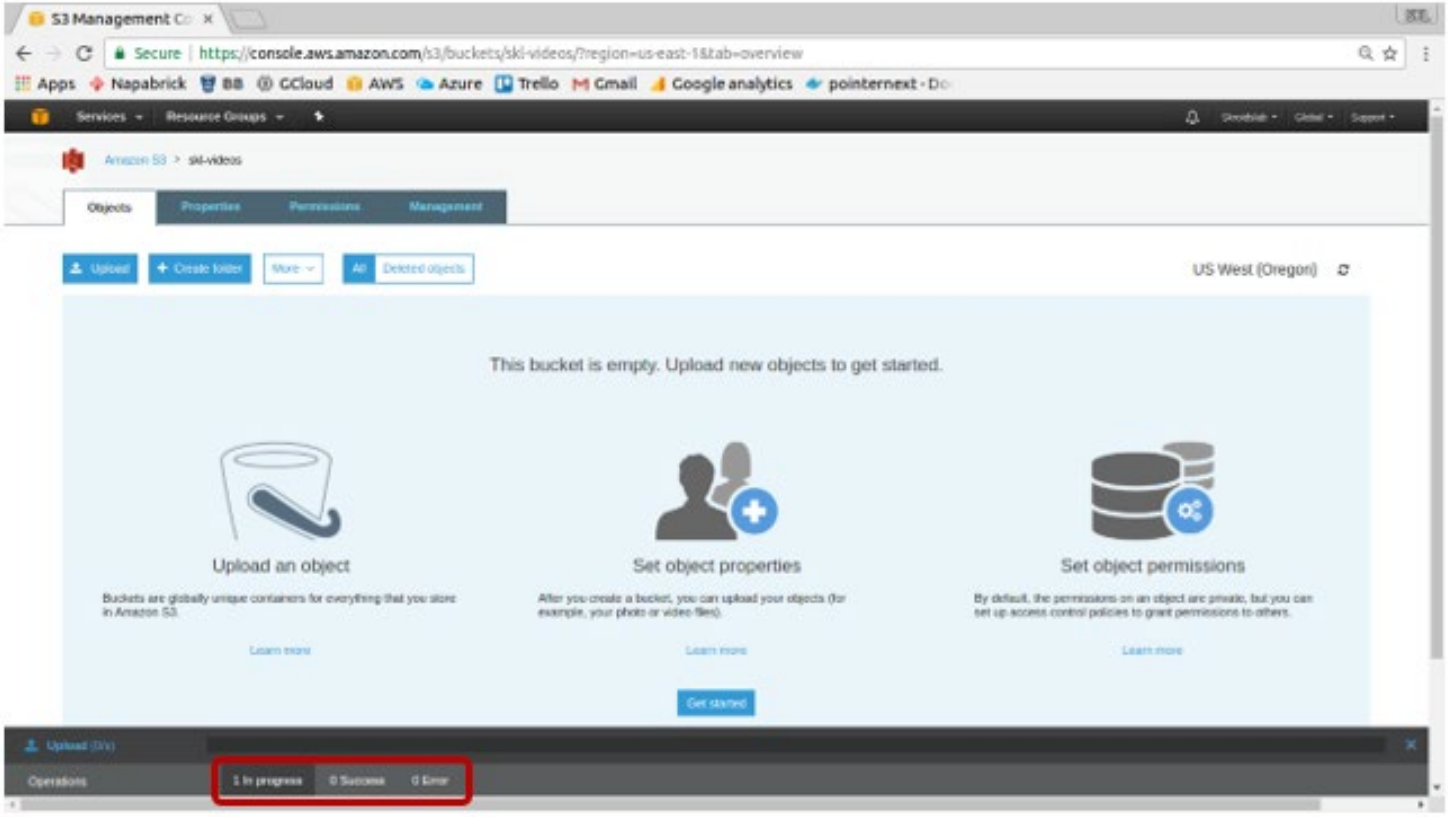


Leave all as defaults, we will modify these later

Activity - S3

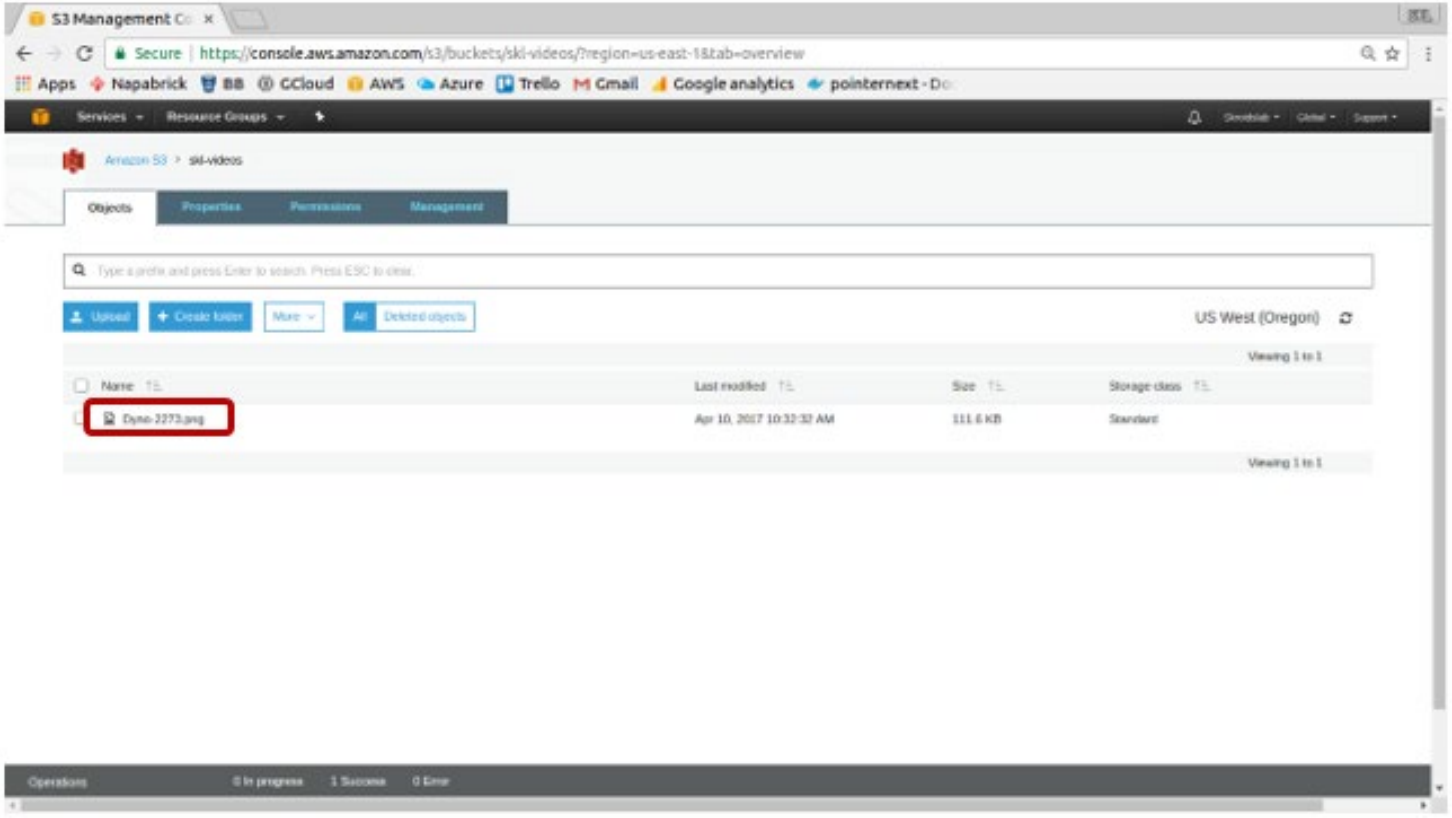


Activity - S3

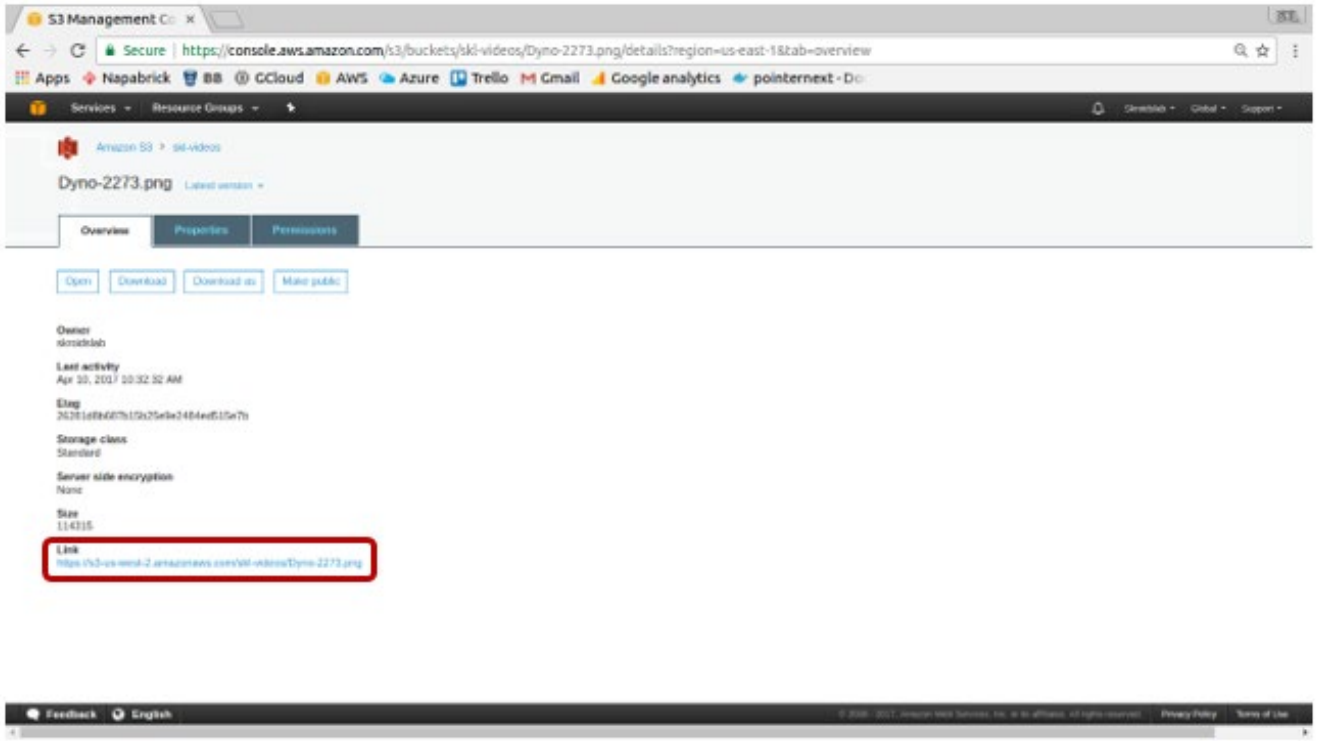


Activity - S3

greatlearning

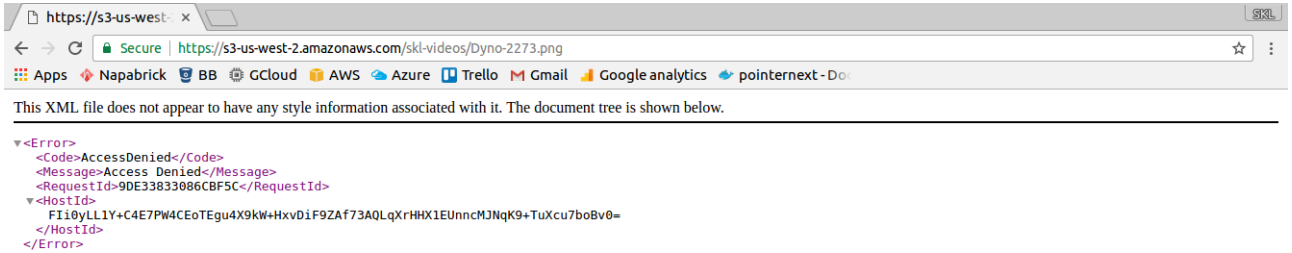


Activity - S3

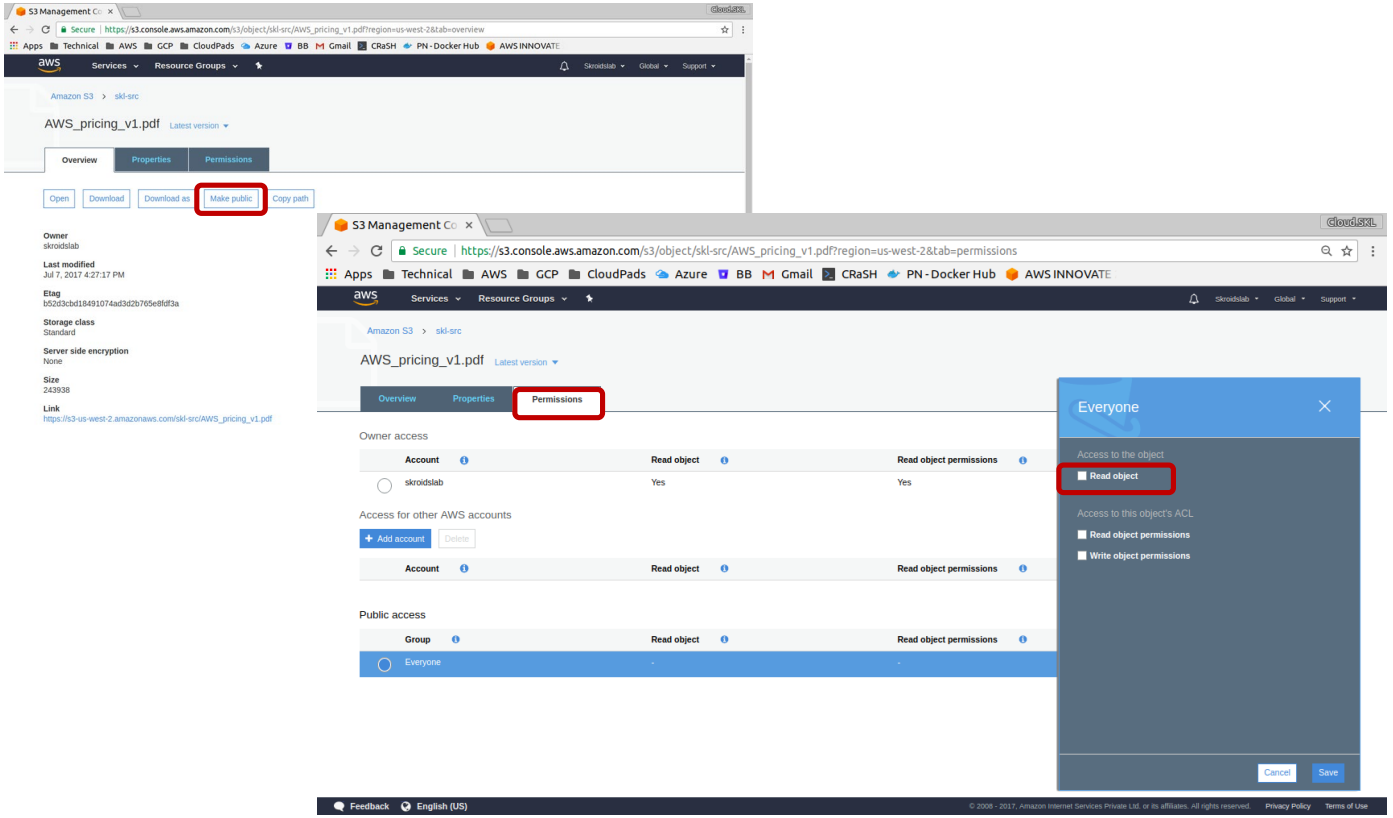


Note - Look at the format of the bucket URL

Activity - S3

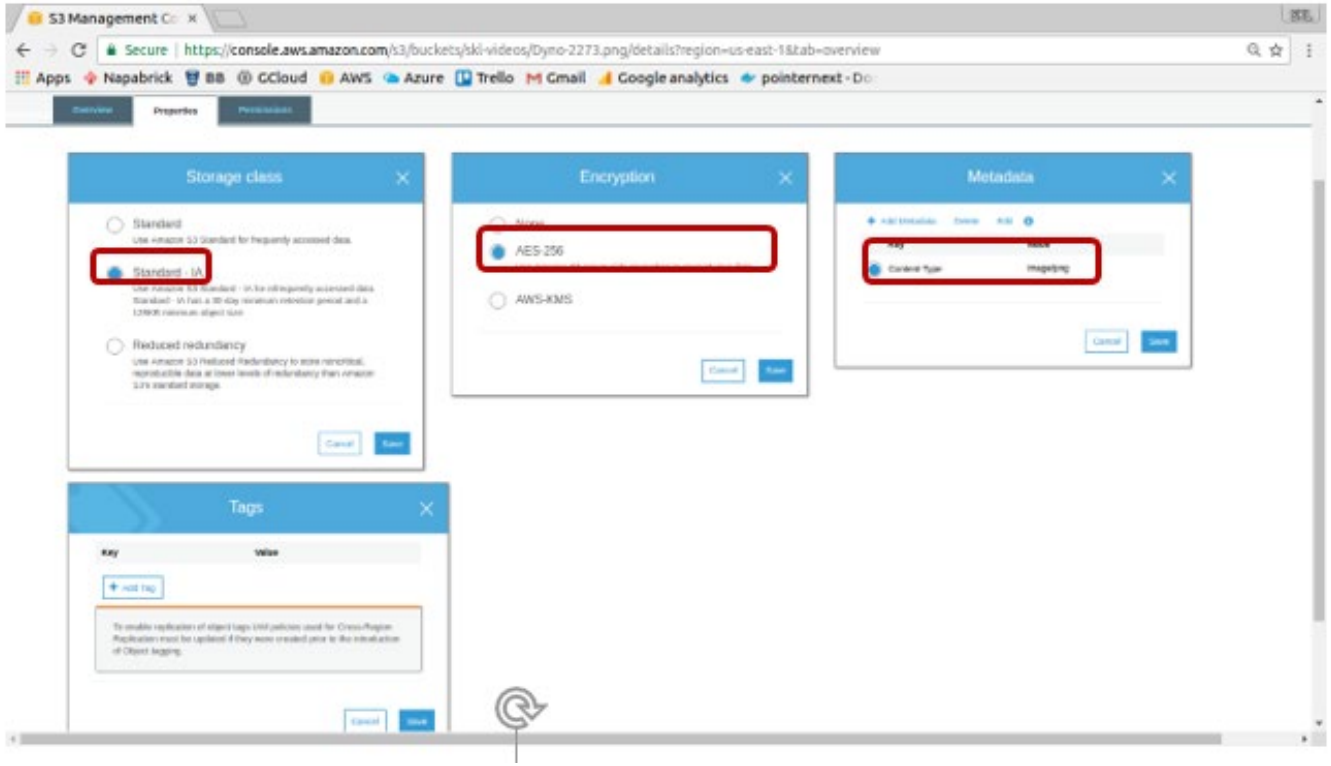


Activity - S3



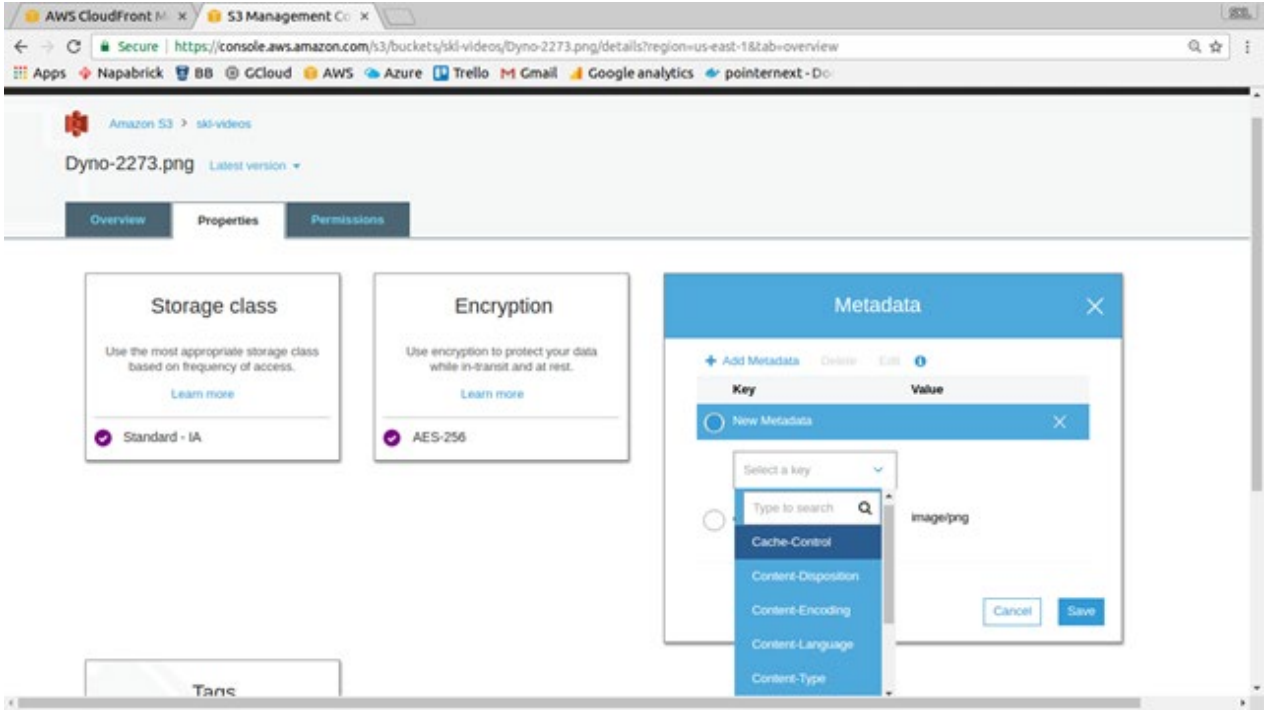
Now access the same link and we should be able to access the object

Activity - S3



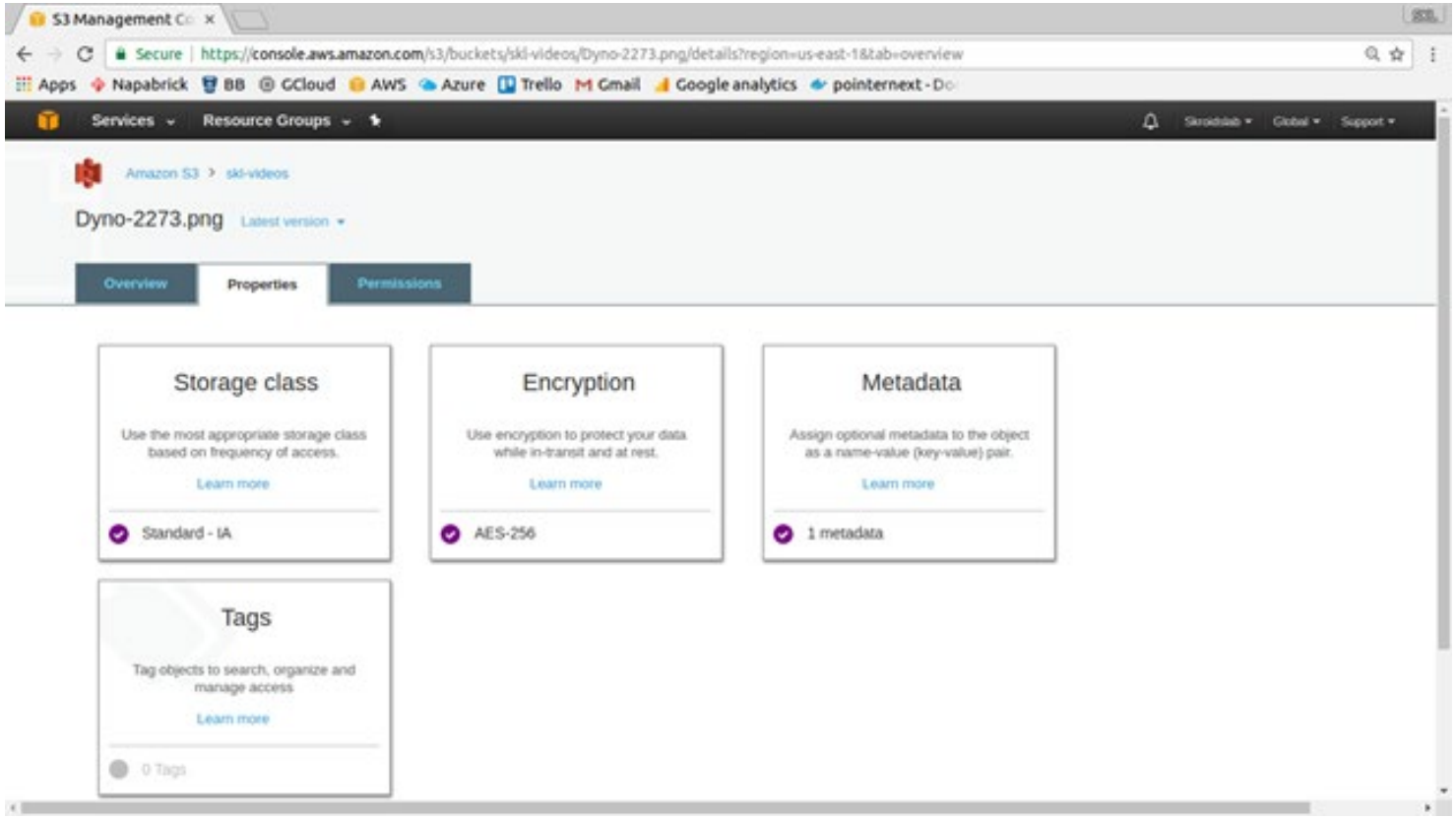
Encryption will be at rest.

Activity - S3



Metadata can contain cache control etc. We will see this later in cloudfront.

Activity - S3

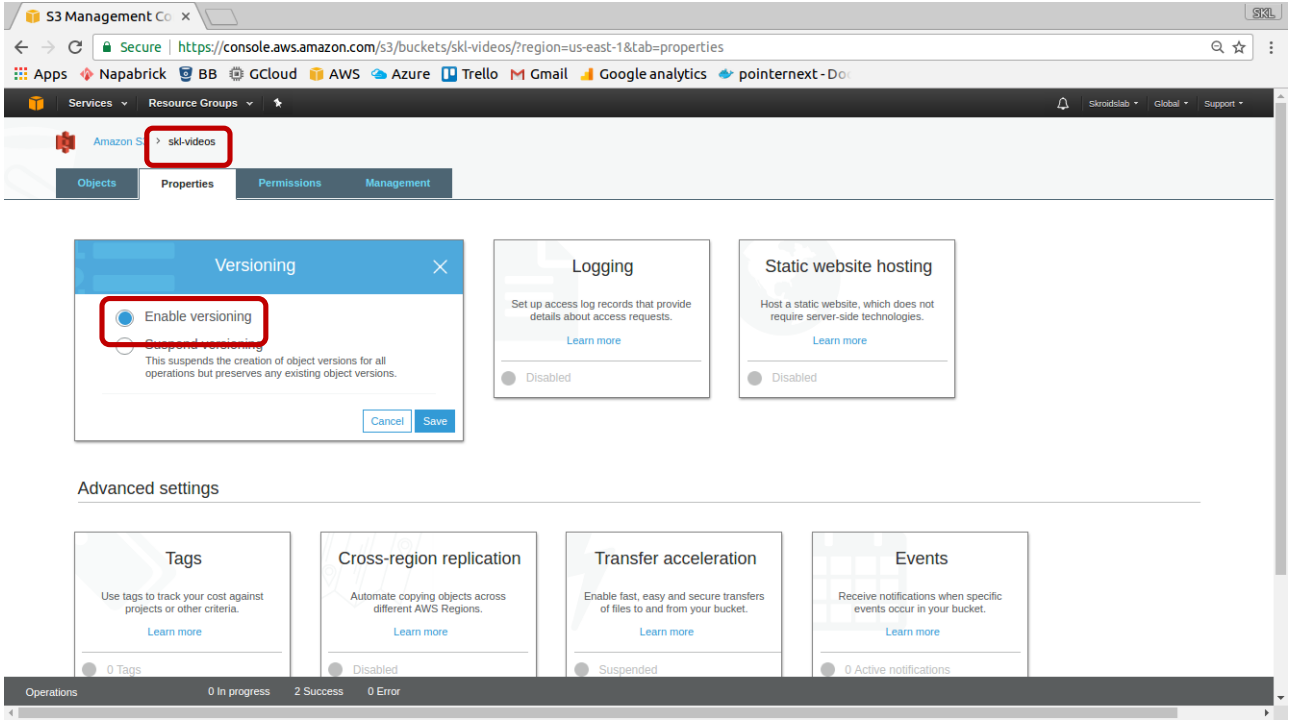


greatlearning

Storage and Content Delivery

S3 - version management

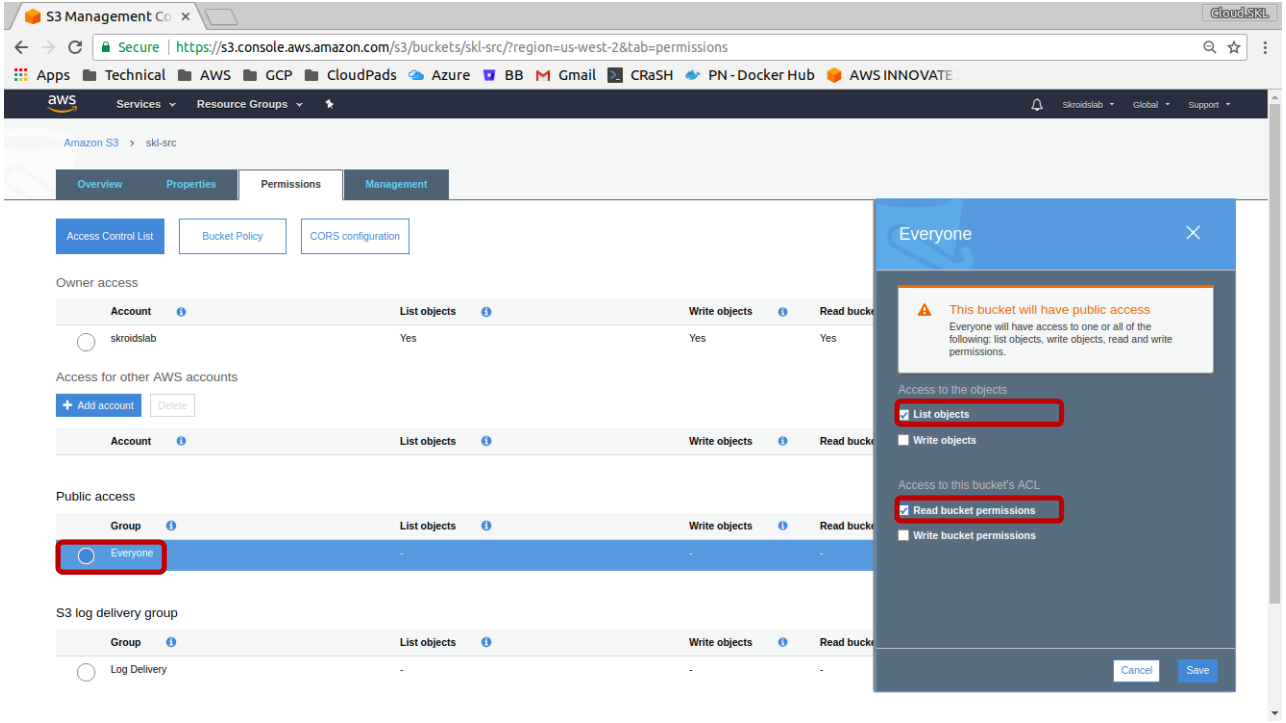
Activity - S3 versioning



Versioning once enabled cannot be disabled.

Activity - S3 versioning

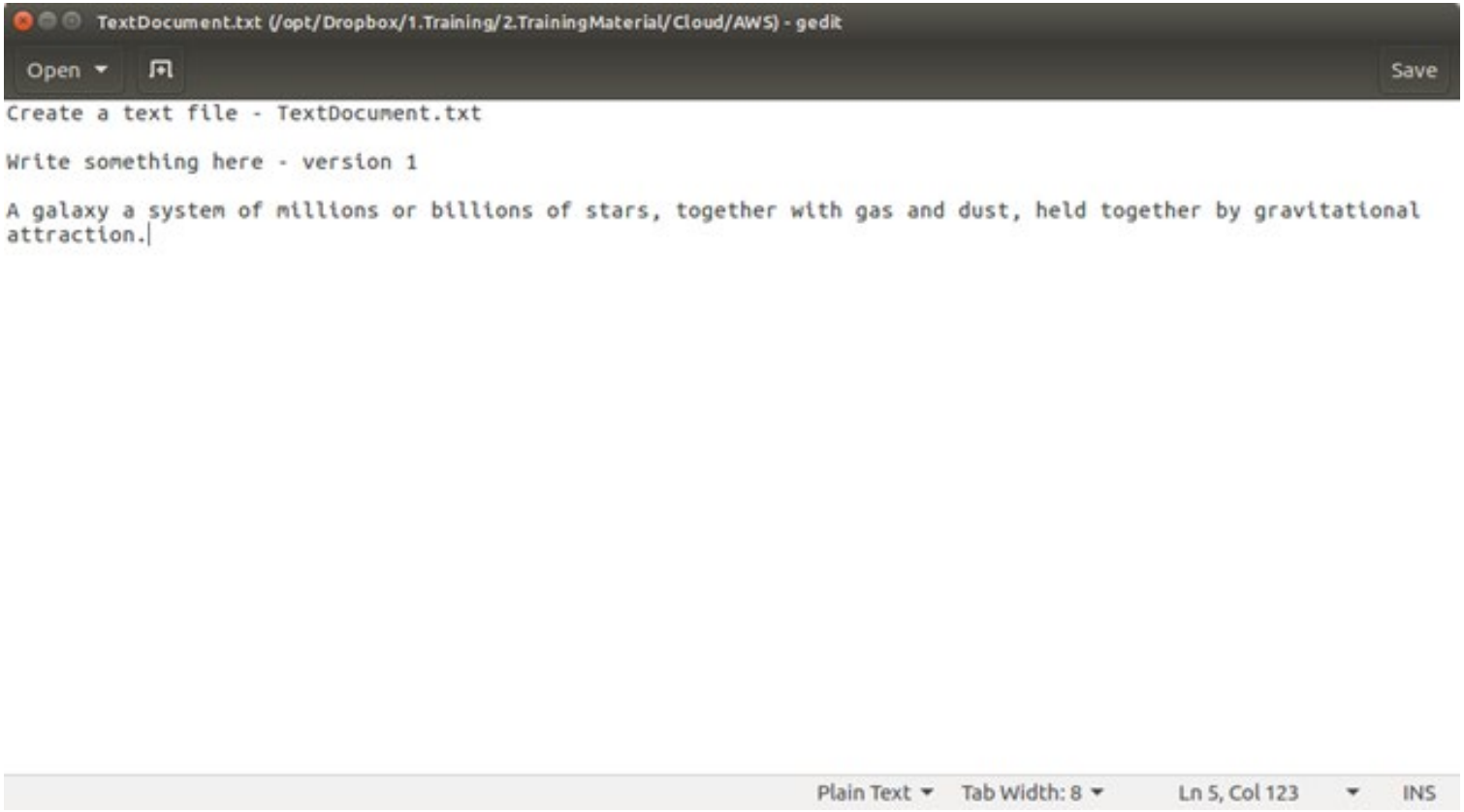
greatlearning



Make the bucket public

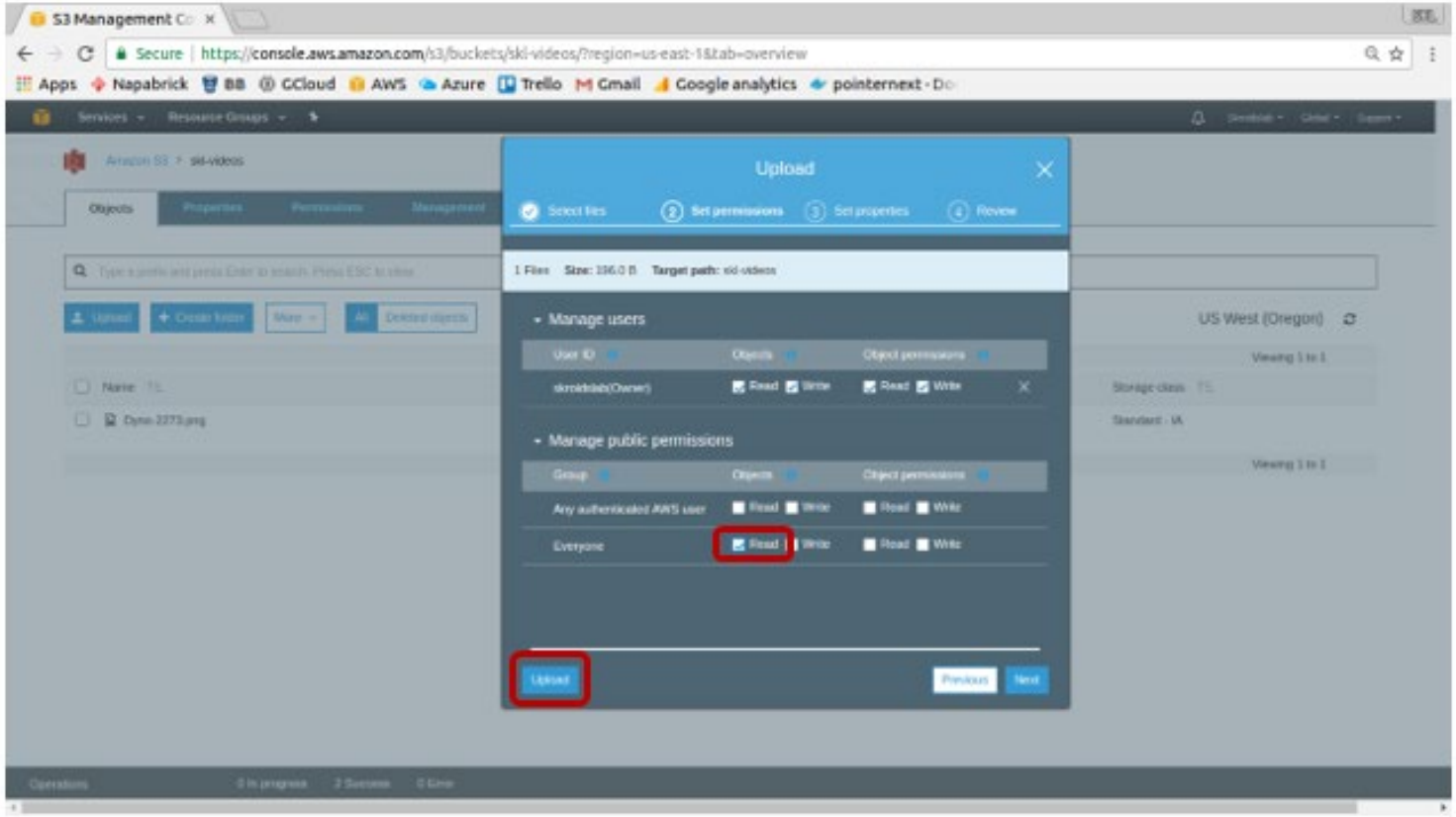
Activity - S3 versioning

greatlearning



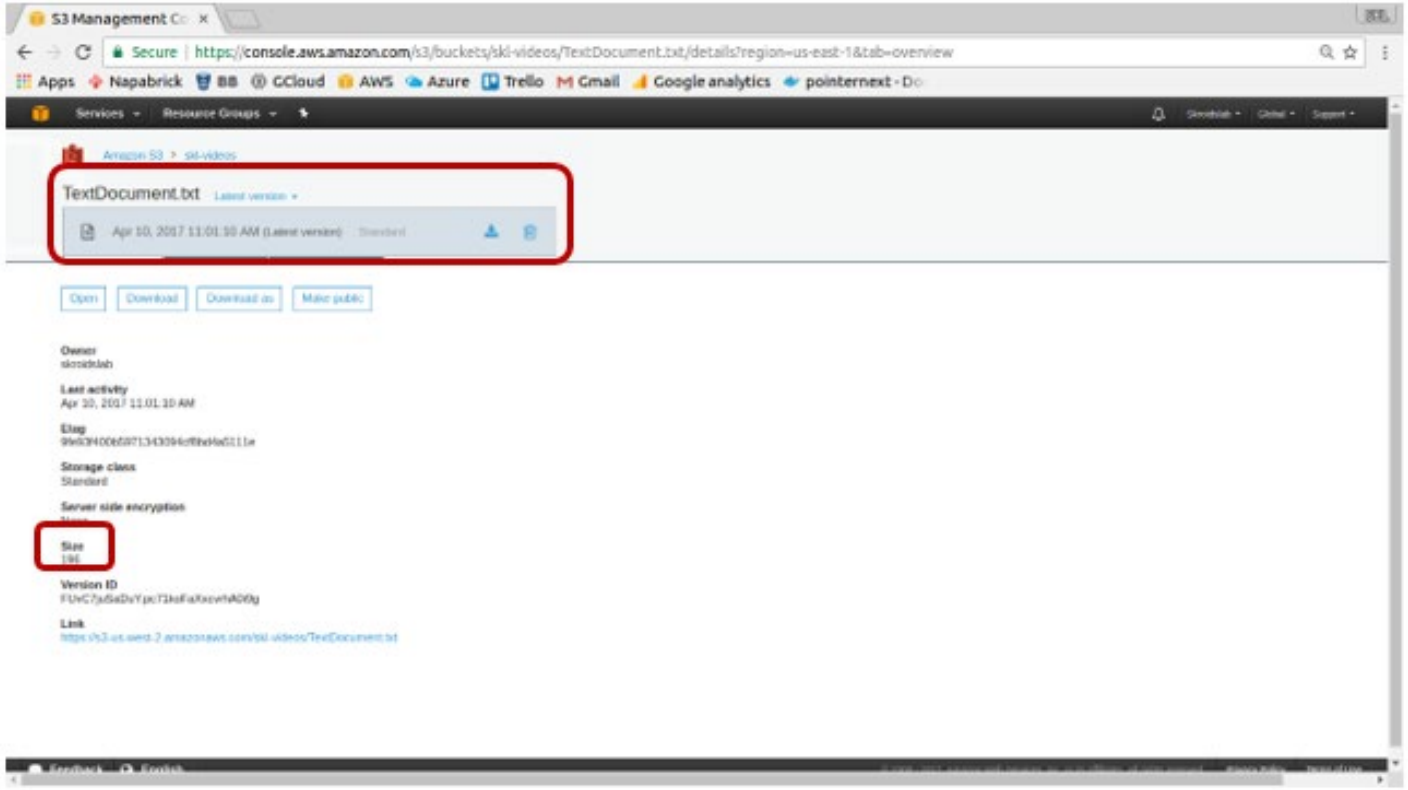
Activity - S3 versioning

greatlearning



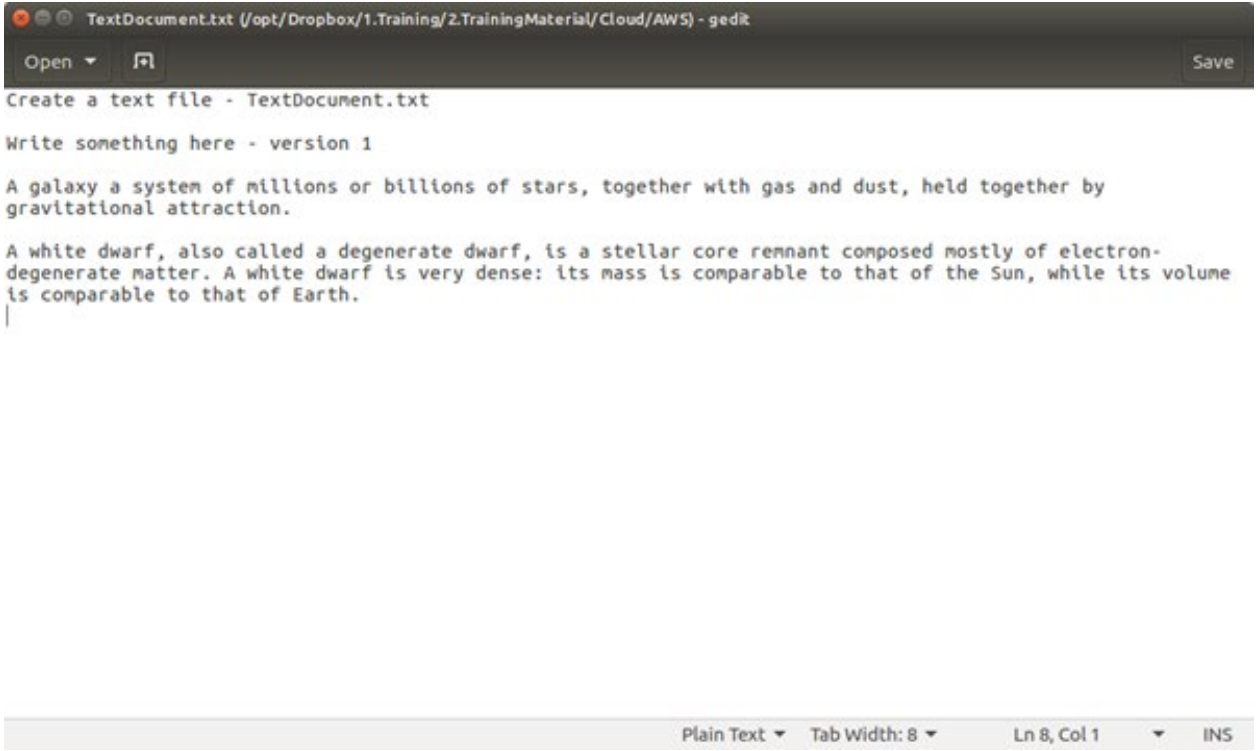
Activity - S3 versioning

greatlearning



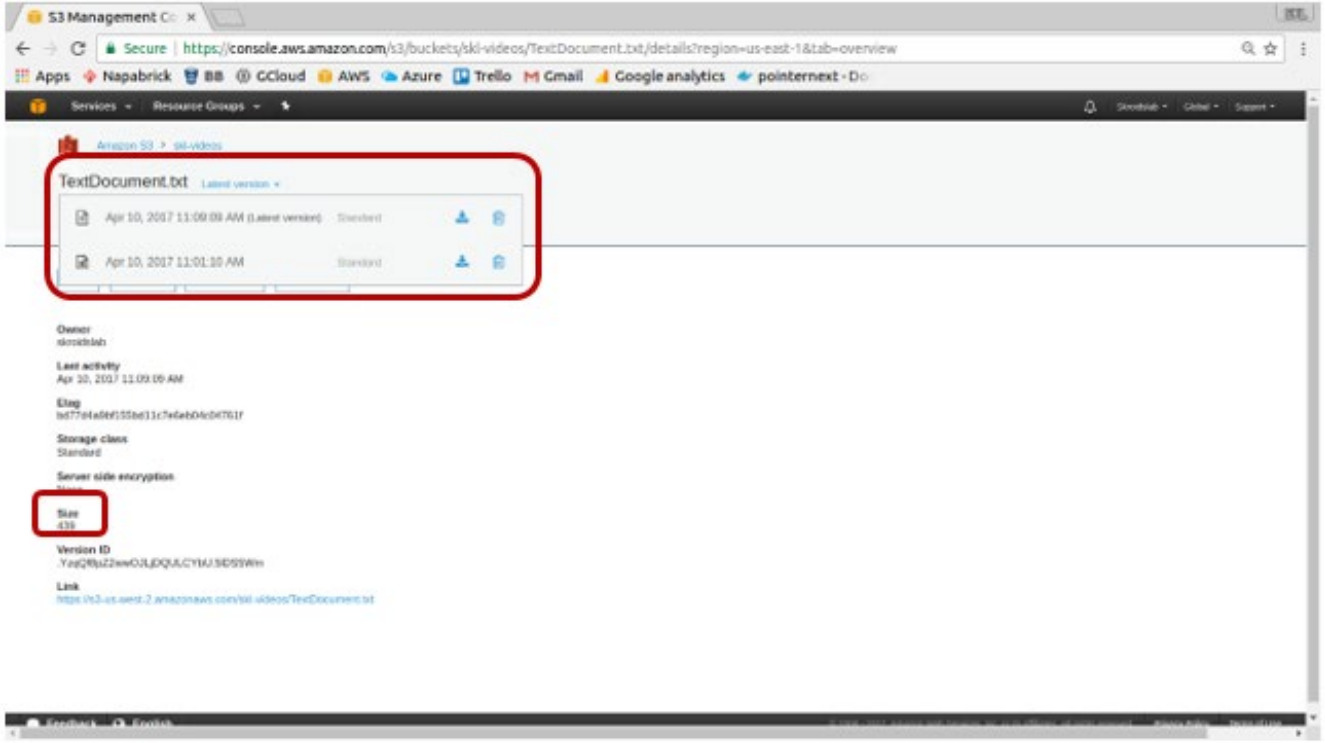
Activity - S3 versioning

greatlearning



Upload the modified file, keep the exact same name!
Permission must be given as "READ" to public again

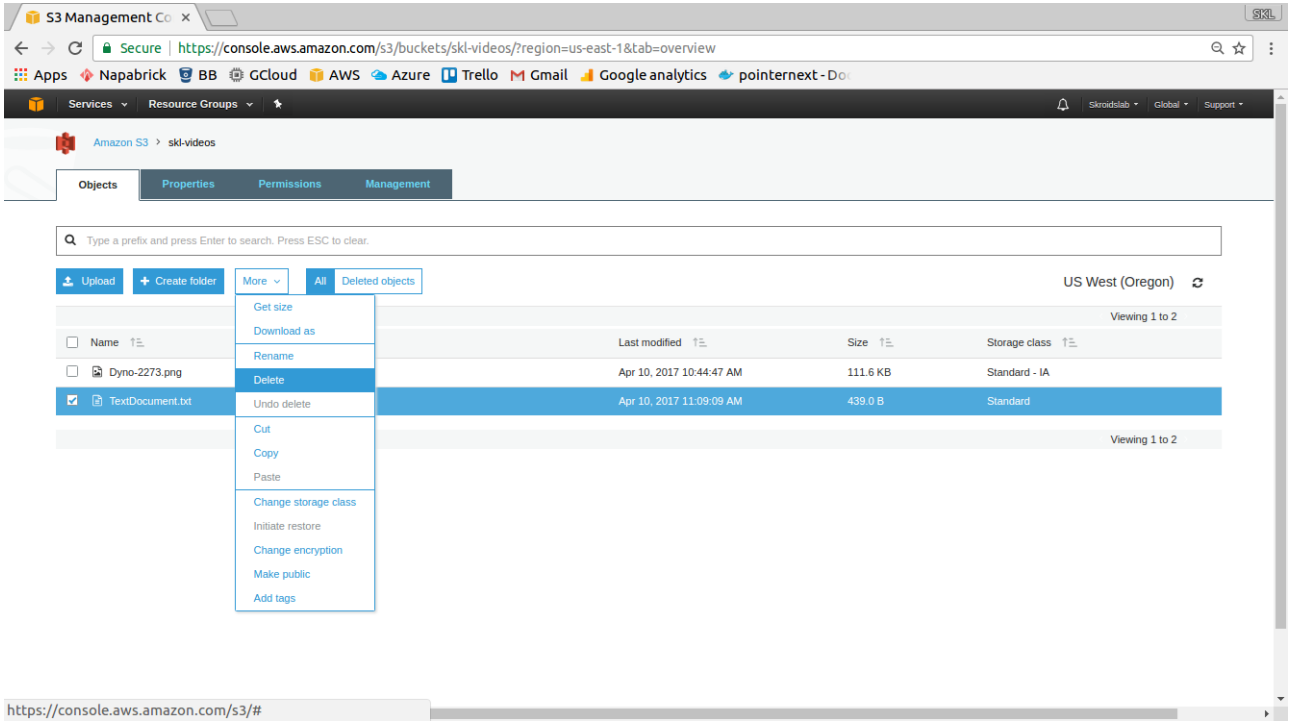
Activity - S3 versioning



Each version takes space! Be careful. You can delete a version (cannot be restored). Object can be restored

Activity - S3 versioning

greatlearning



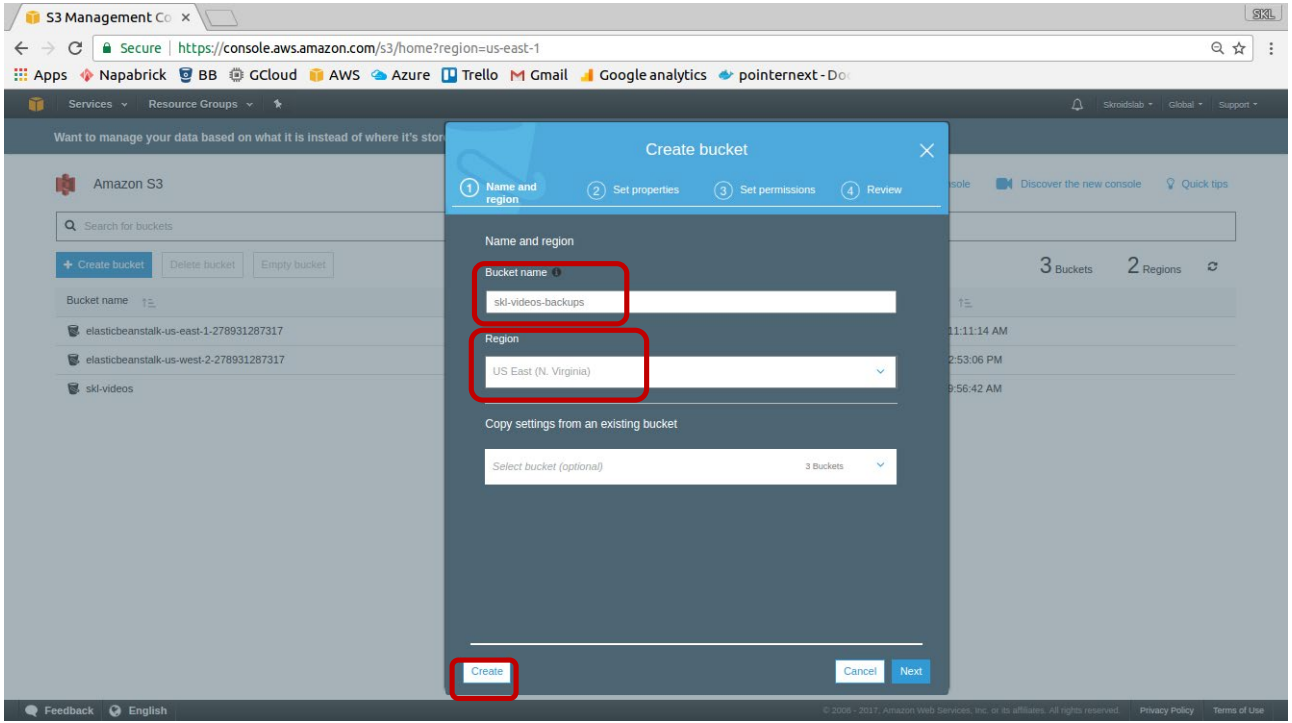
We can enable a MFA to delete an object - complex to setup and cannot be done from console.

greatlearning

Storage and Content Delivery

S3 - cross region replication

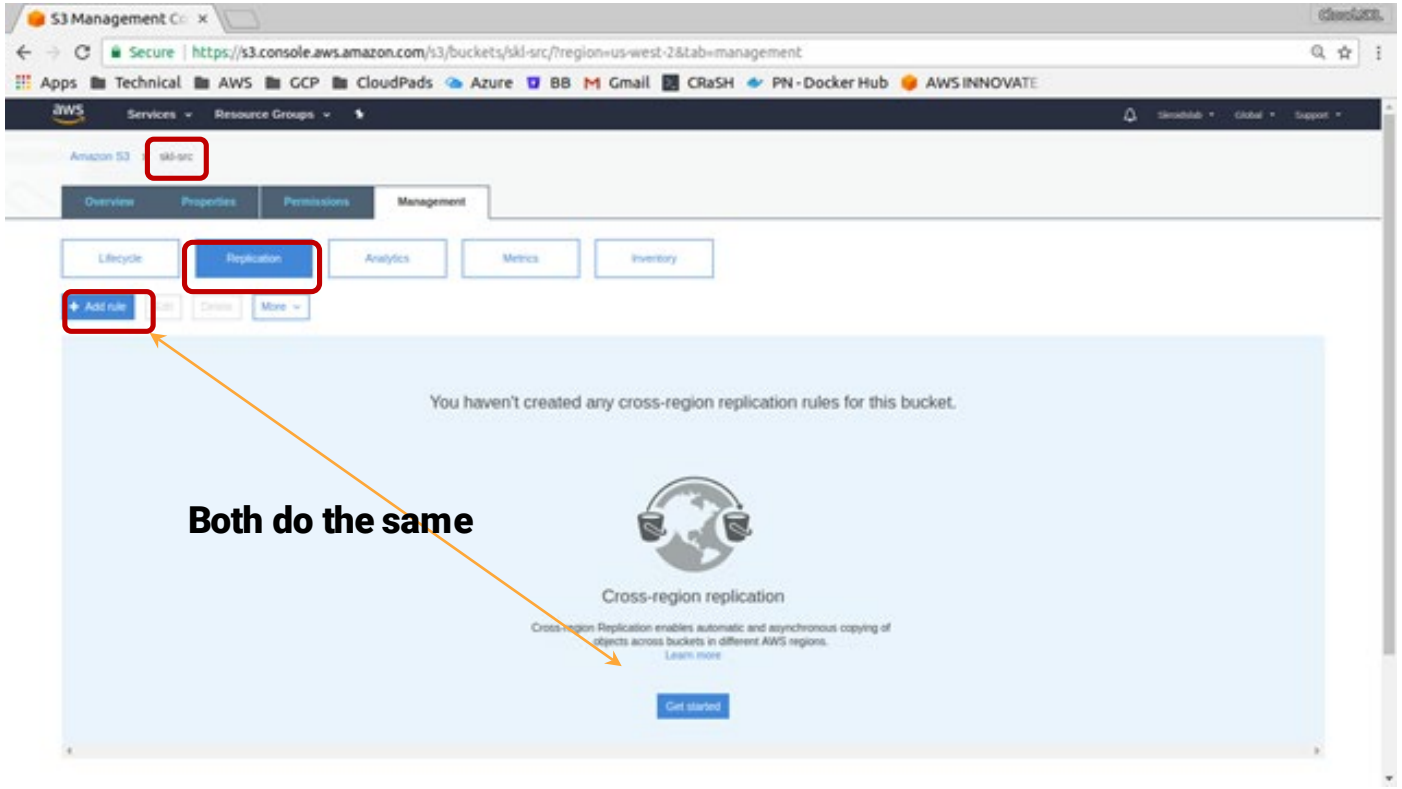
Activity - S3 Cross region replica



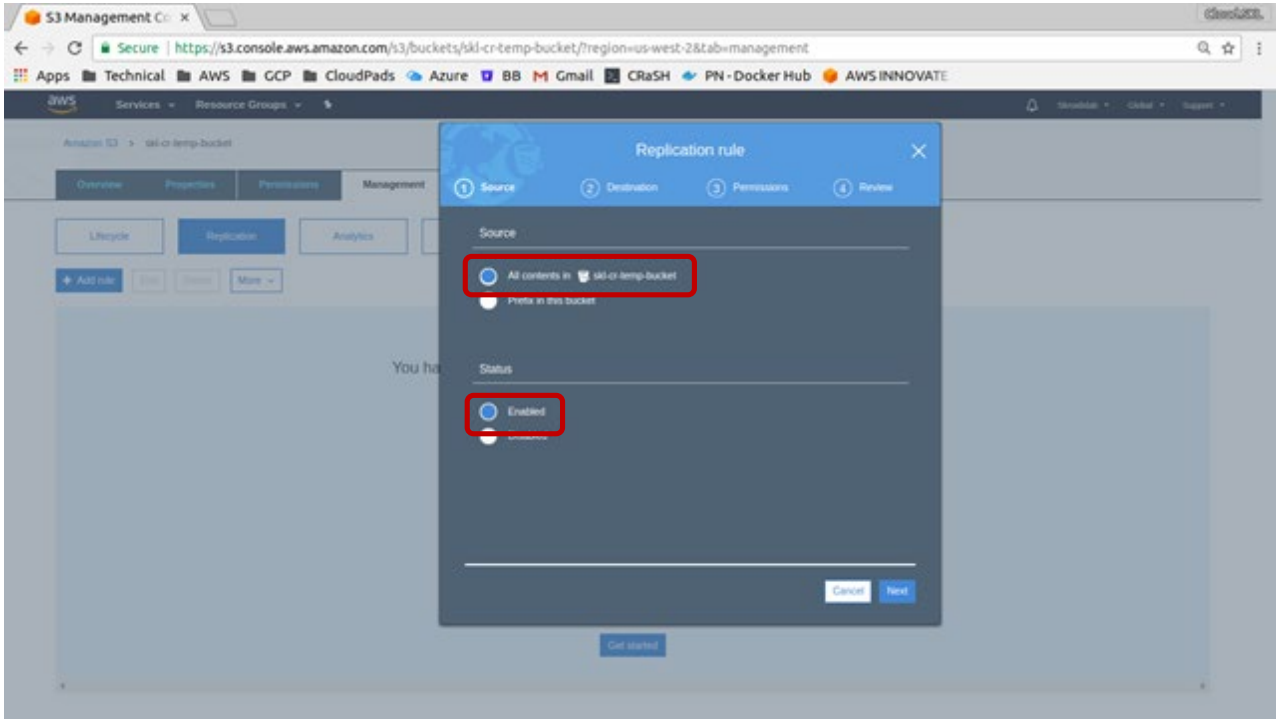
Create a new bucket in the east coast, go to properties and enable versioning

Activity - S3 Cross region replica

greatlearning



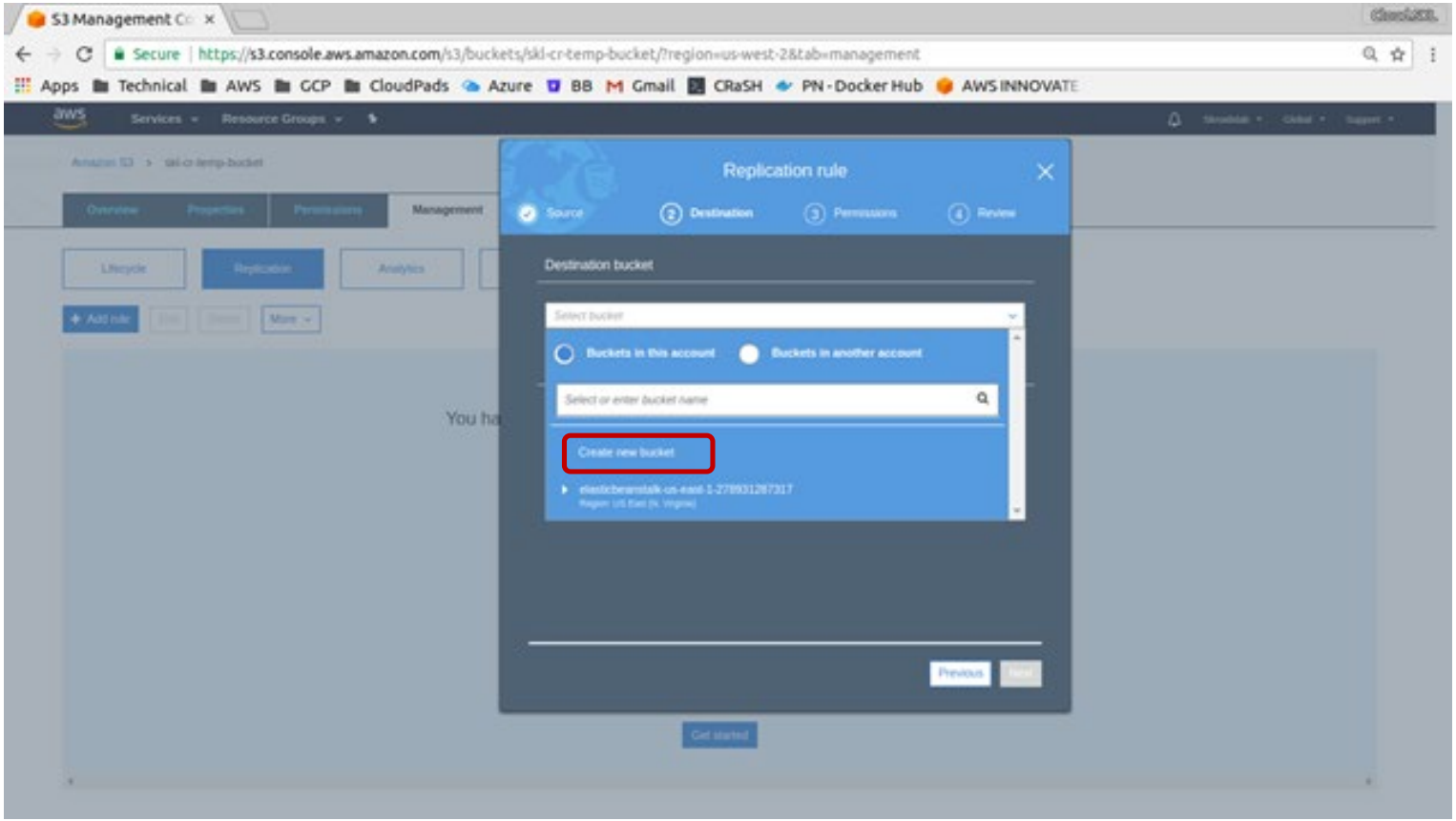
Activity - S3 Cross region replica



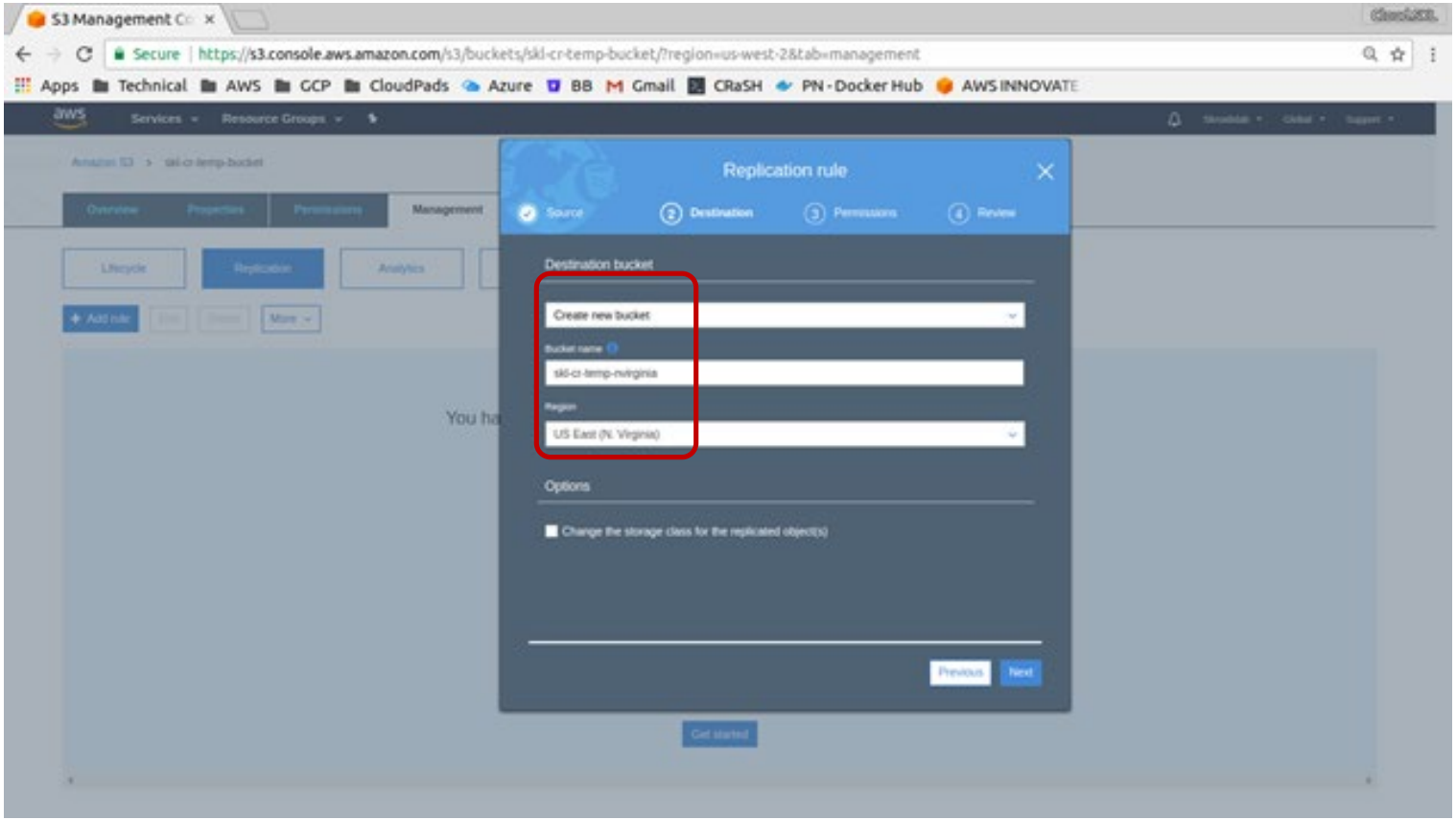
Existing objects will not be replicated! Upload another version of the galaxy txt file and you will find ALL previous versions will be replicated. Multi region replication and replication chaining is not supported.

Activity - S3 Cross region replica

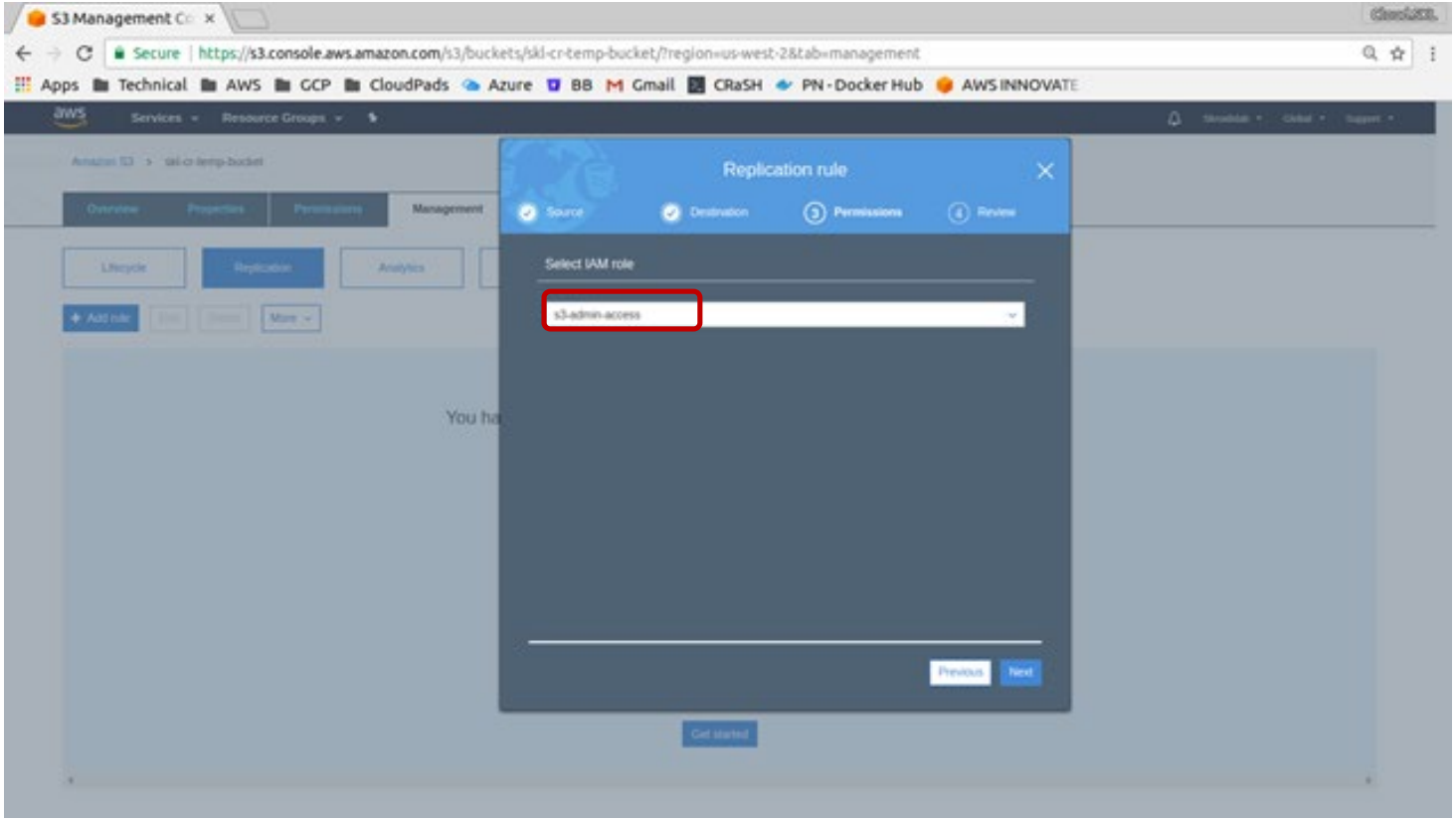
greatlearning



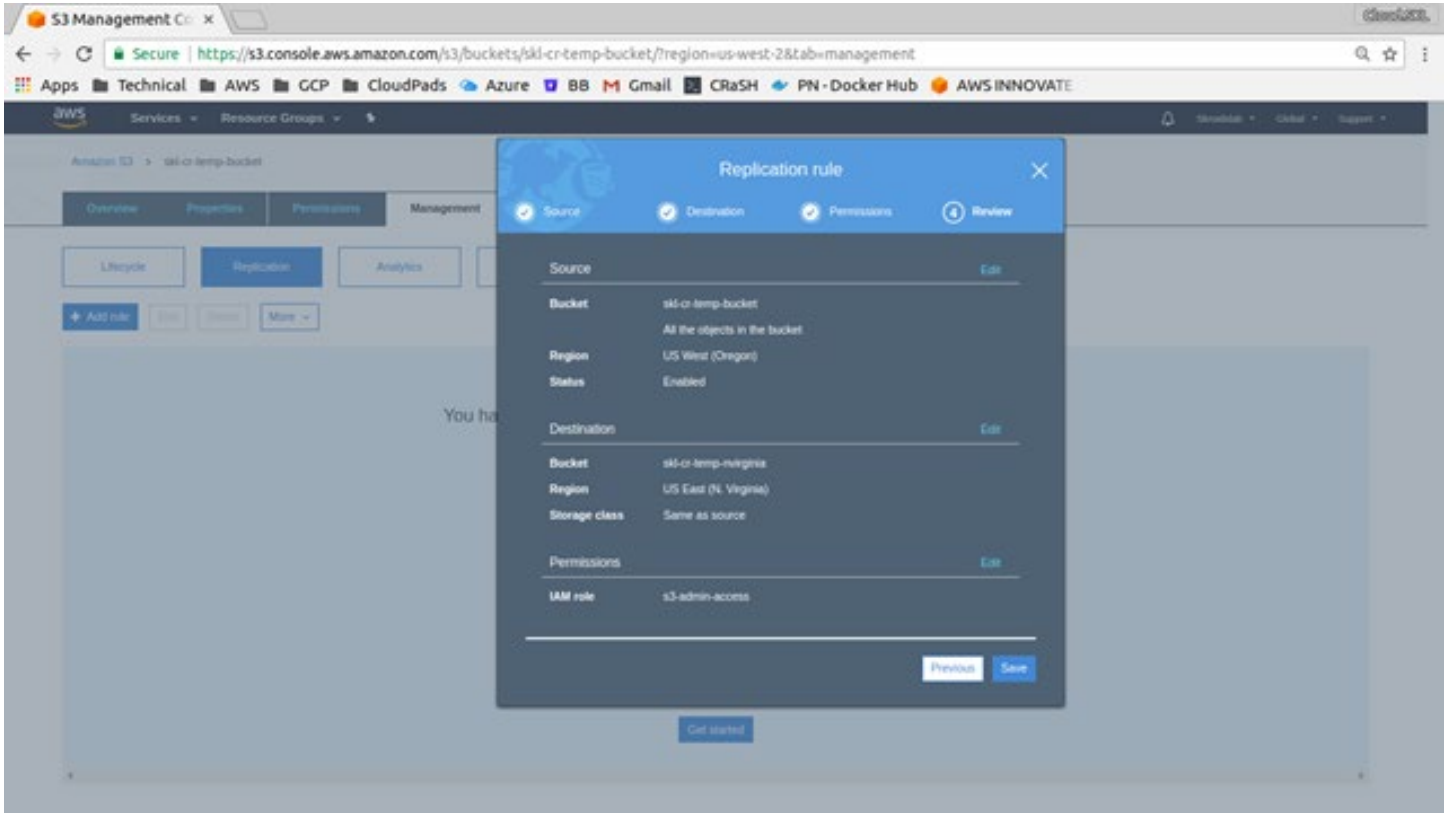
Activity - S3 Cross region replica



Activity - S3 Cross region replica

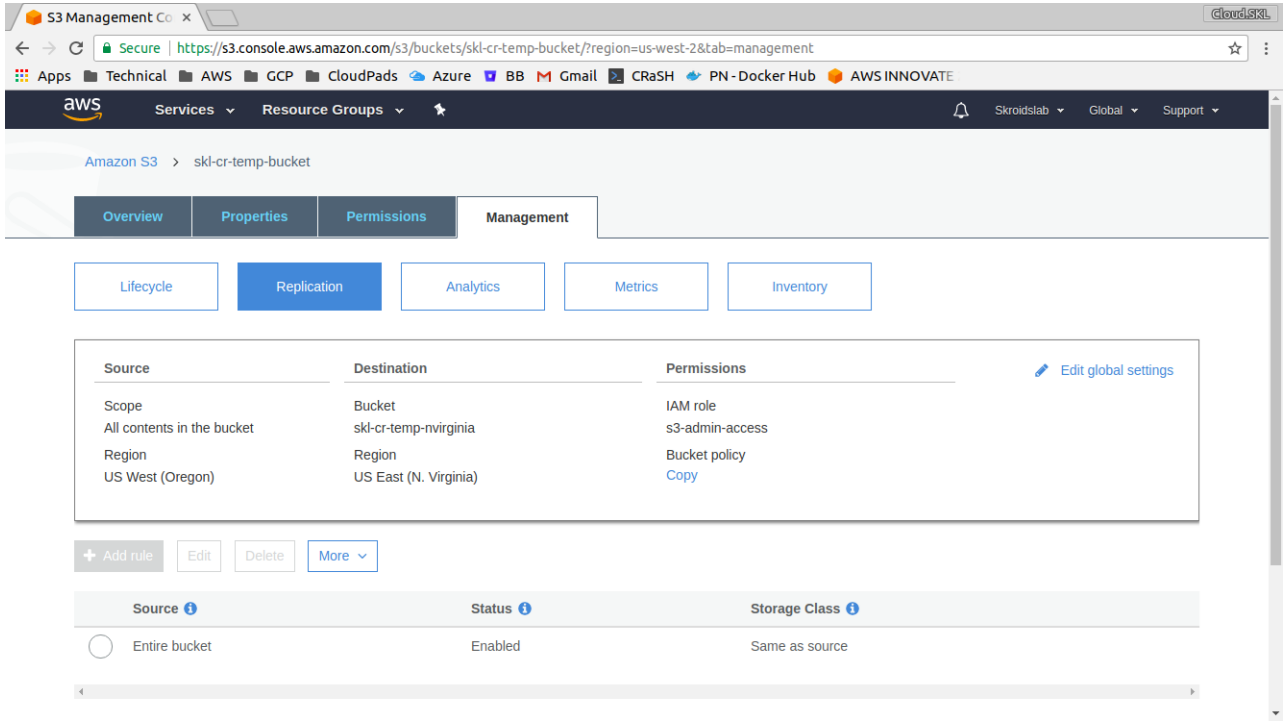


Activity - S3 Cross region replica



Activity - S3 Cross region replica

greatlearning



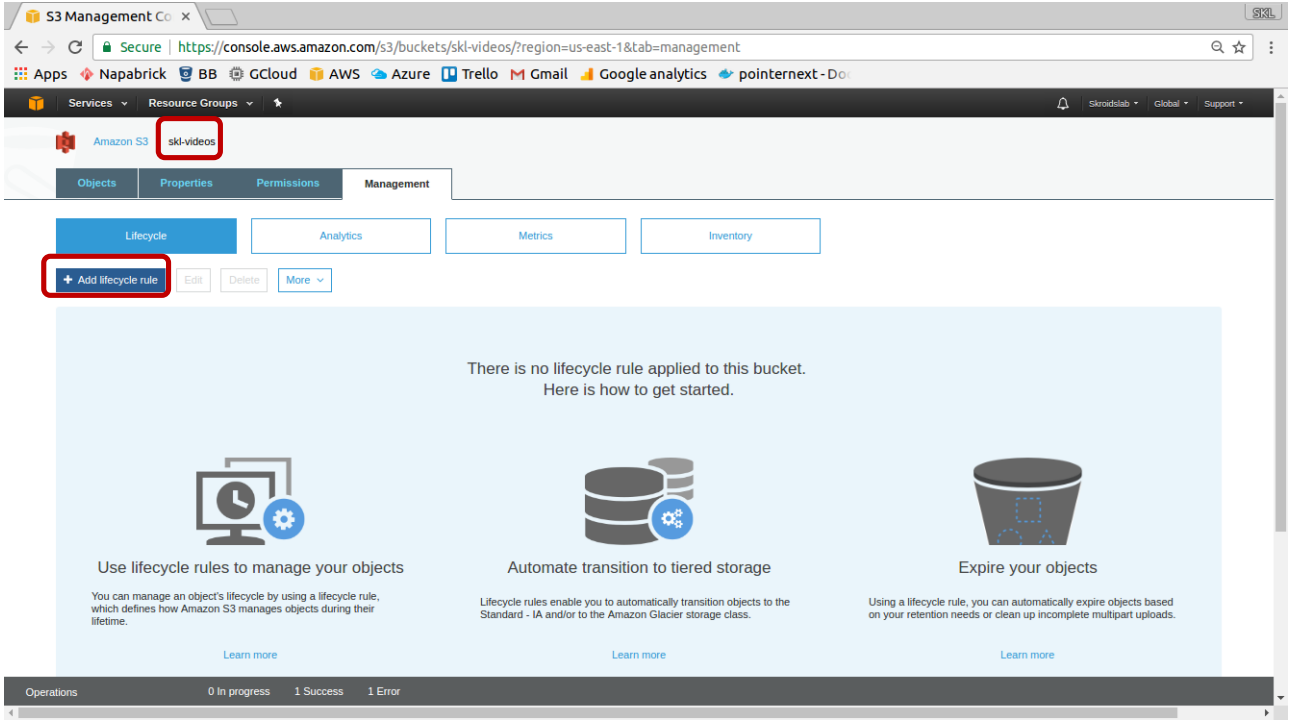
greatlearning

Storage and Content Delivery

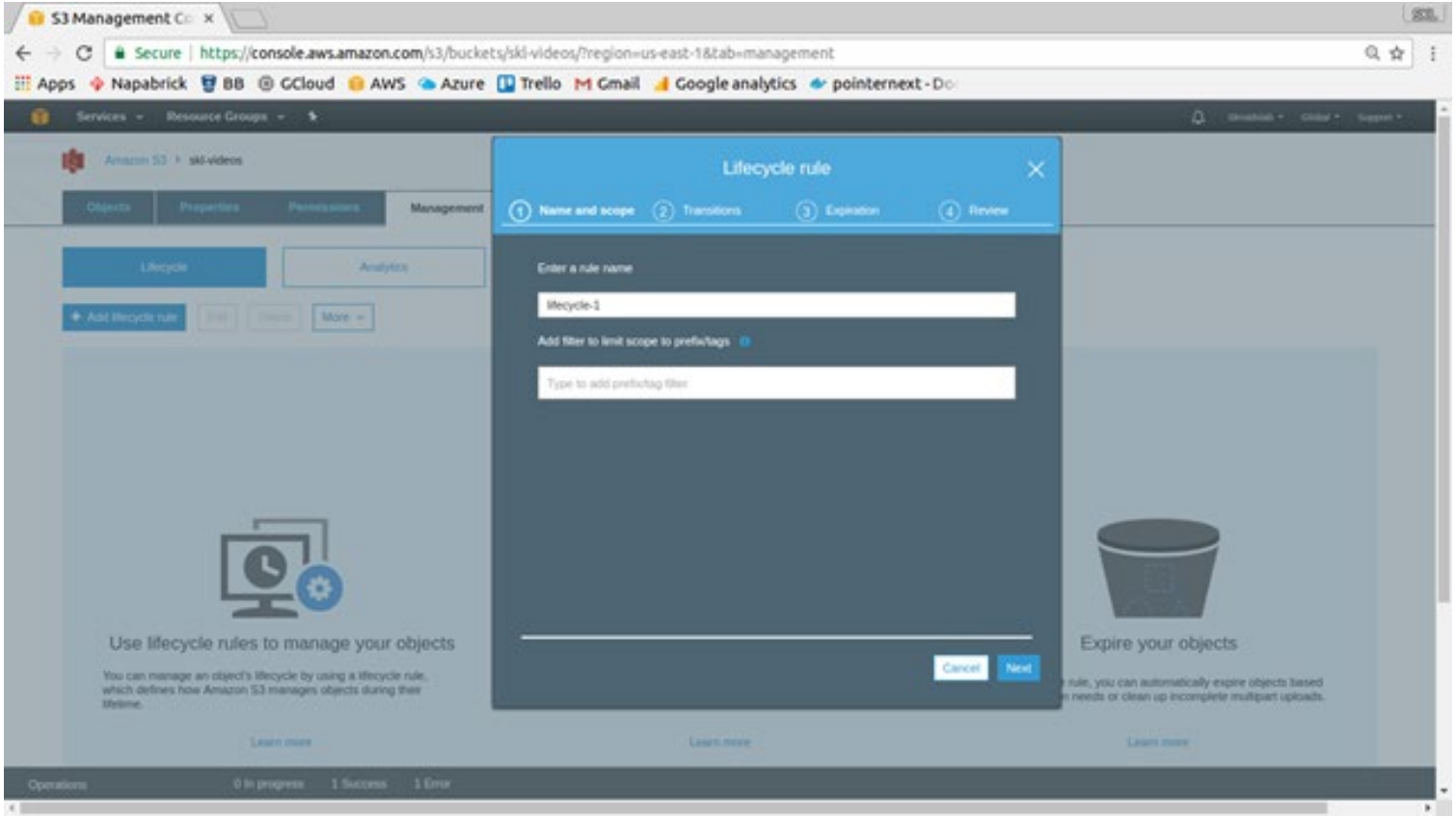
S3 - Lifecycle management

Activity - S3 lifecycle

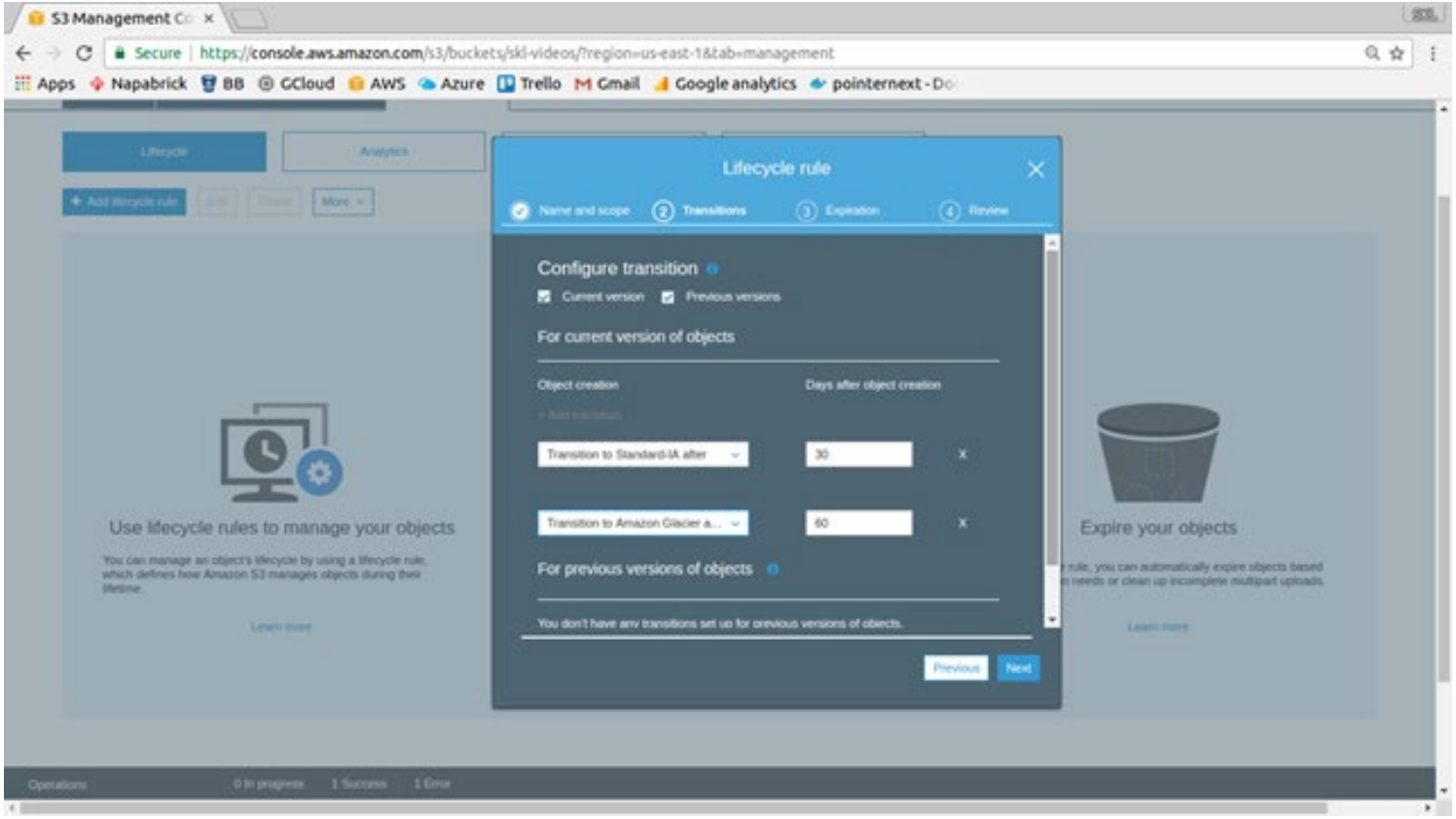
greatlearning



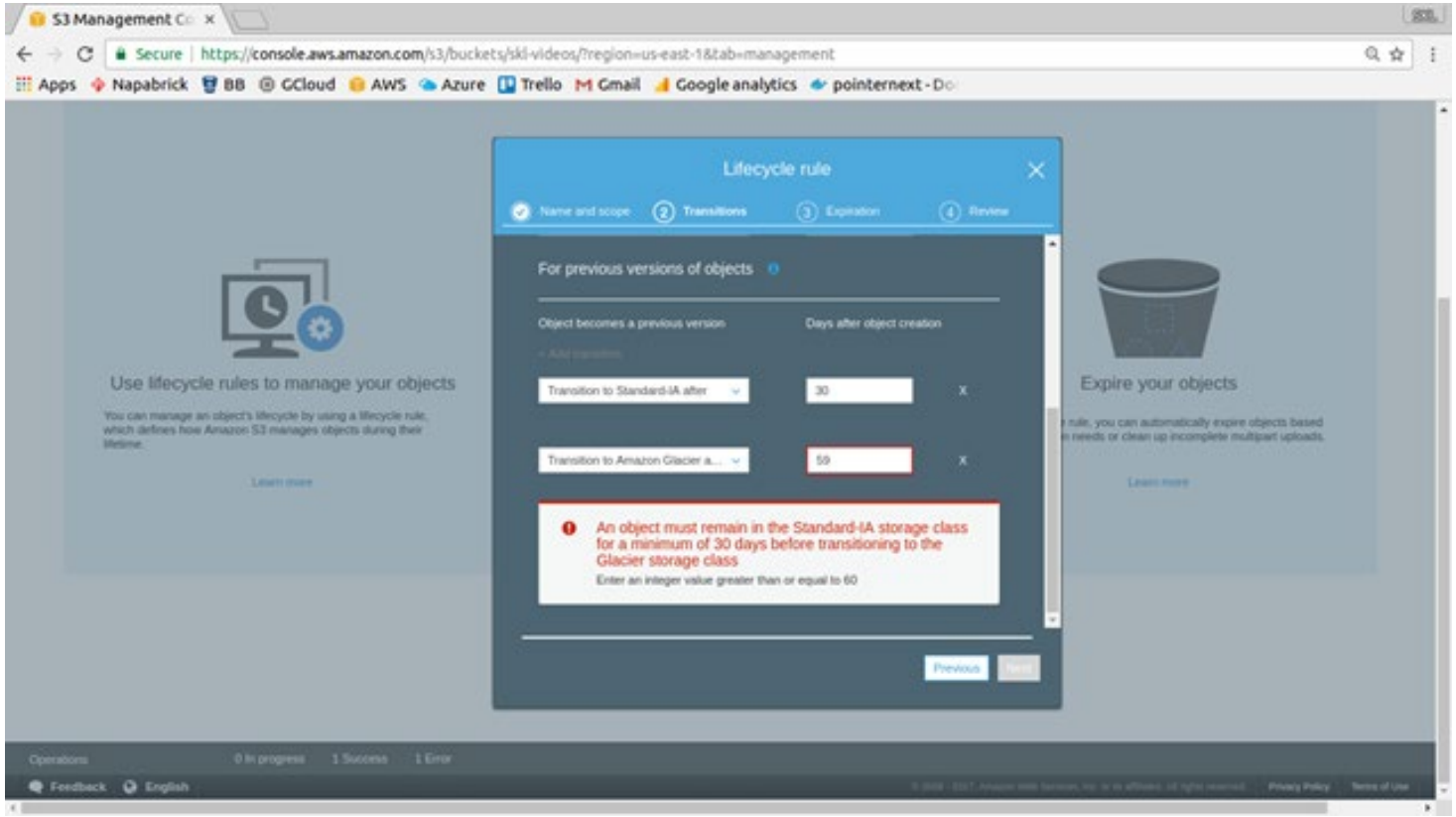
Activity - S3 lifecycle



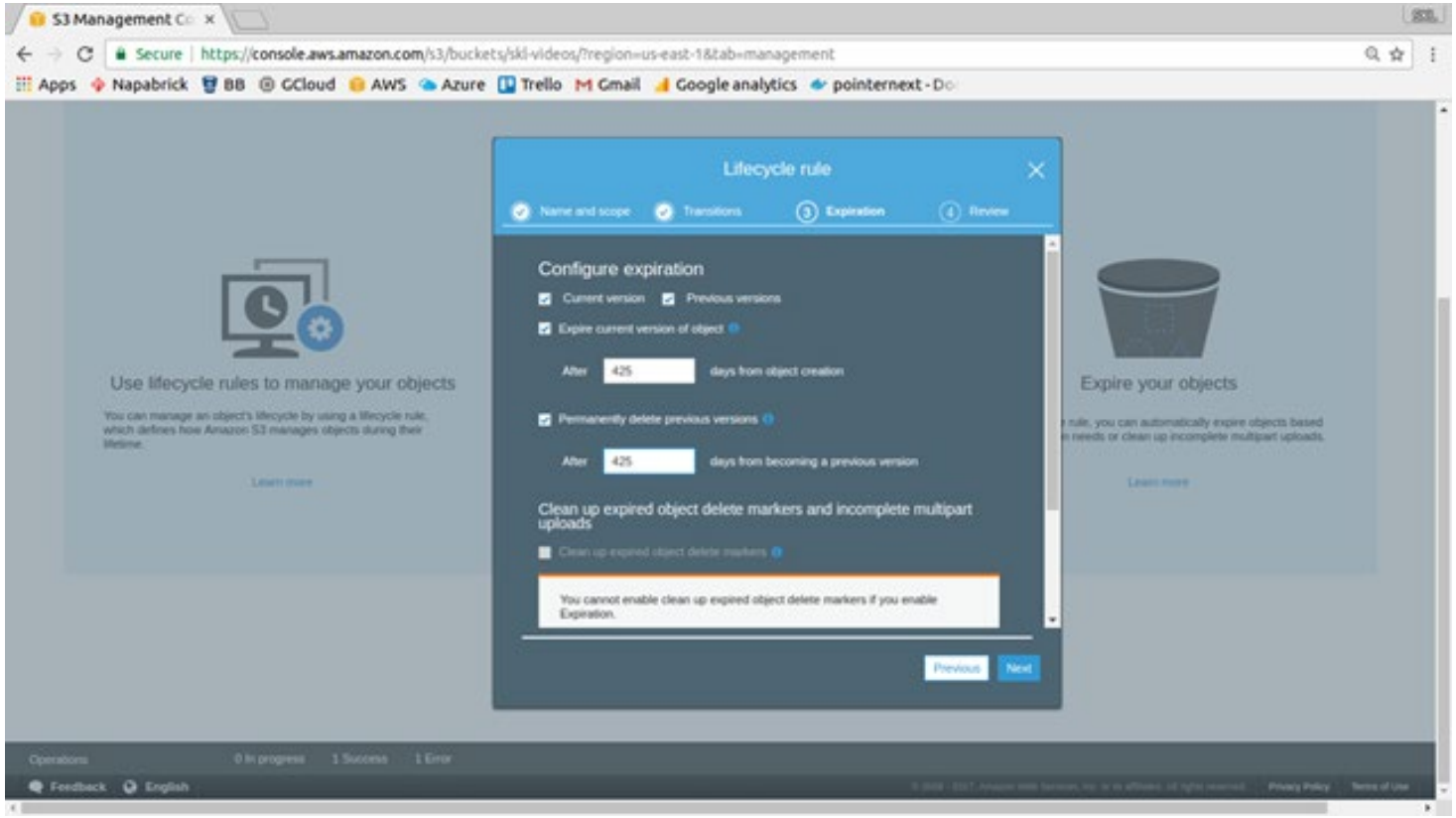
Activity - S3 lifecycle



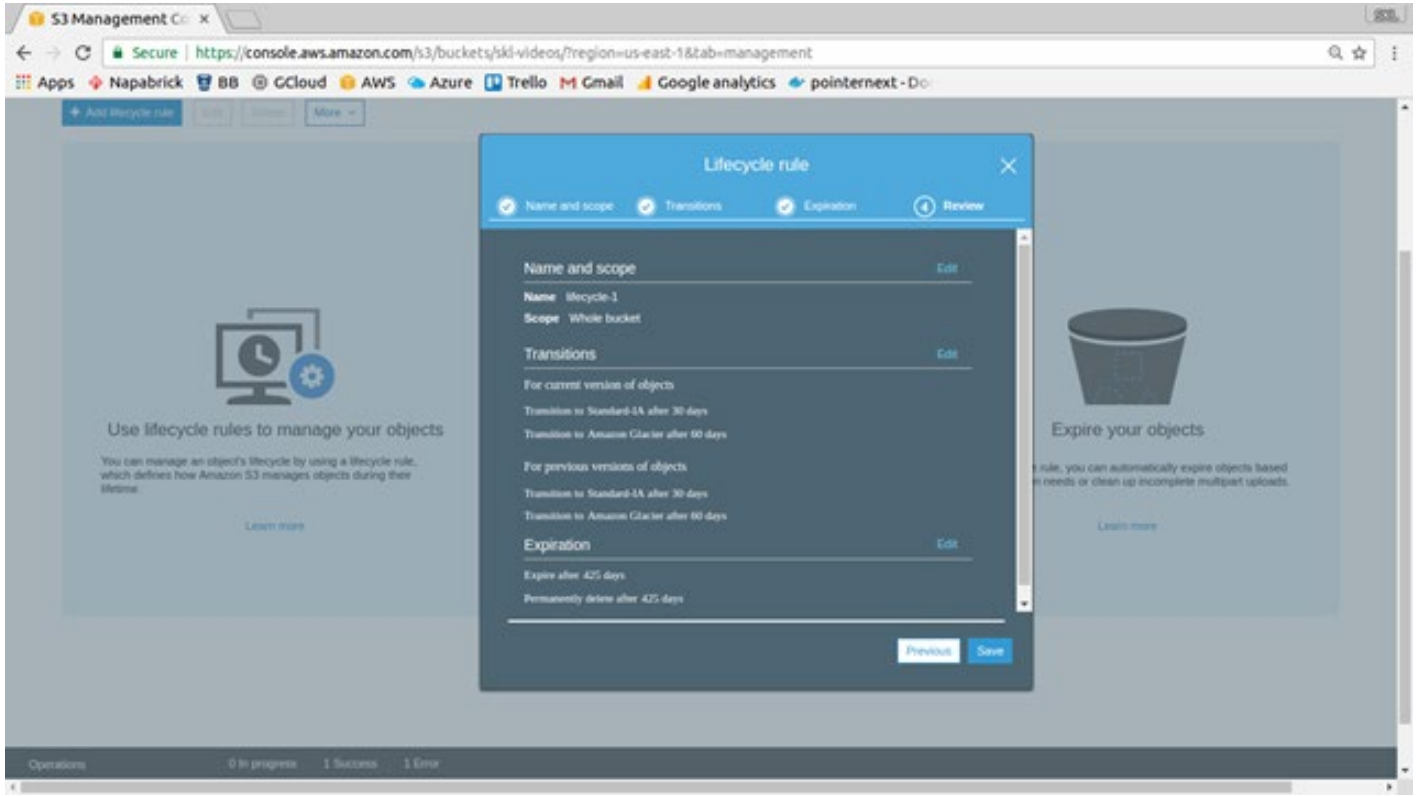
Activity - S3 lifecycle



Activity - S3 lifecycle

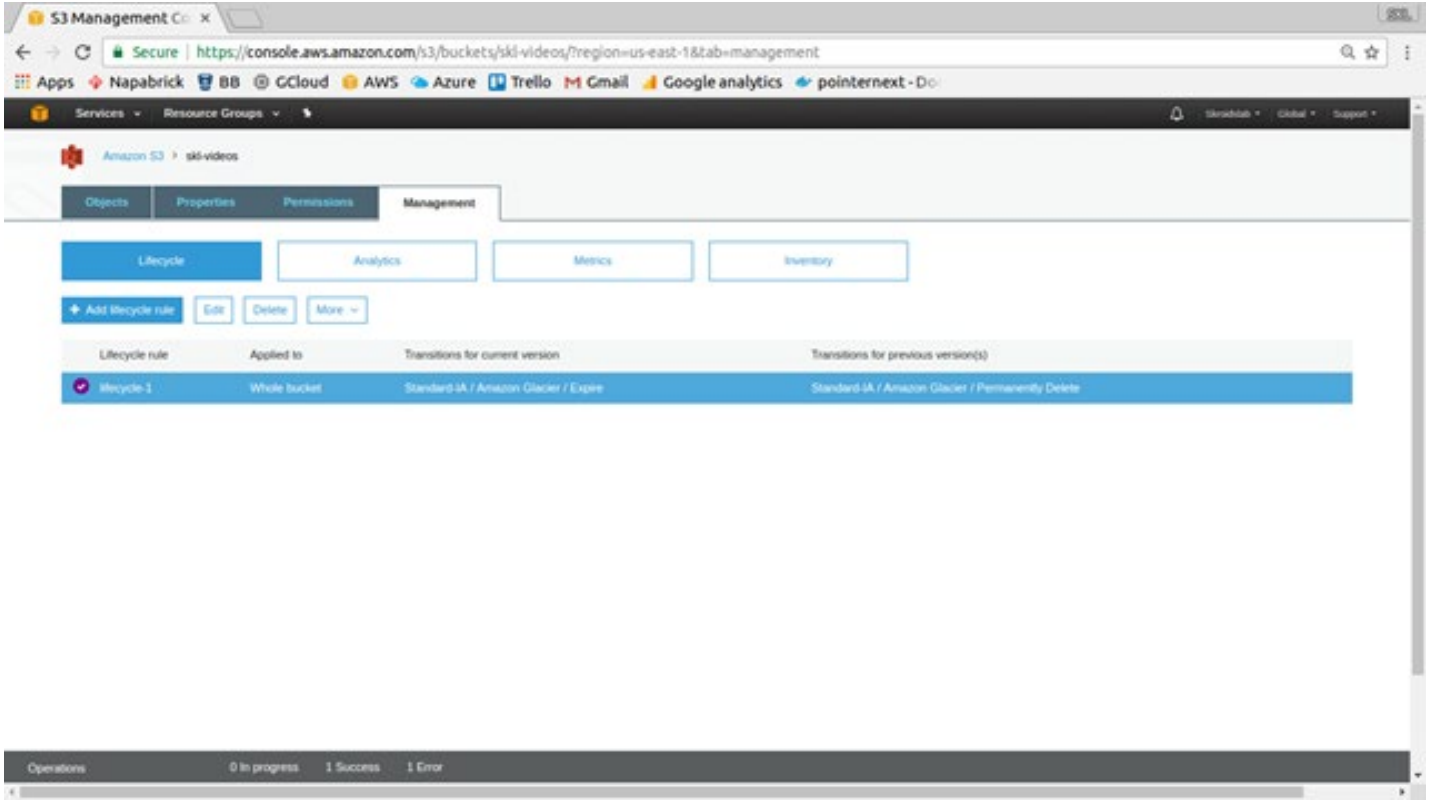


Activity - S3 lifecycle

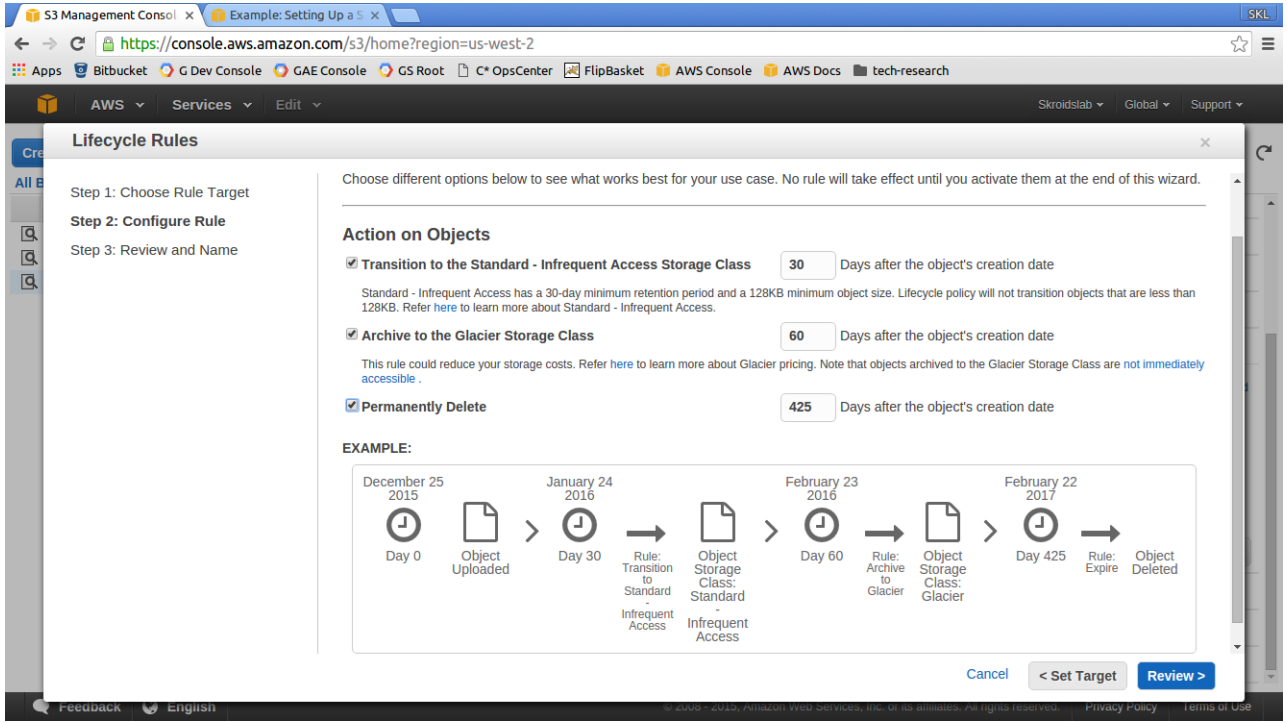


Activity - S3 lifecycle

greatlearning

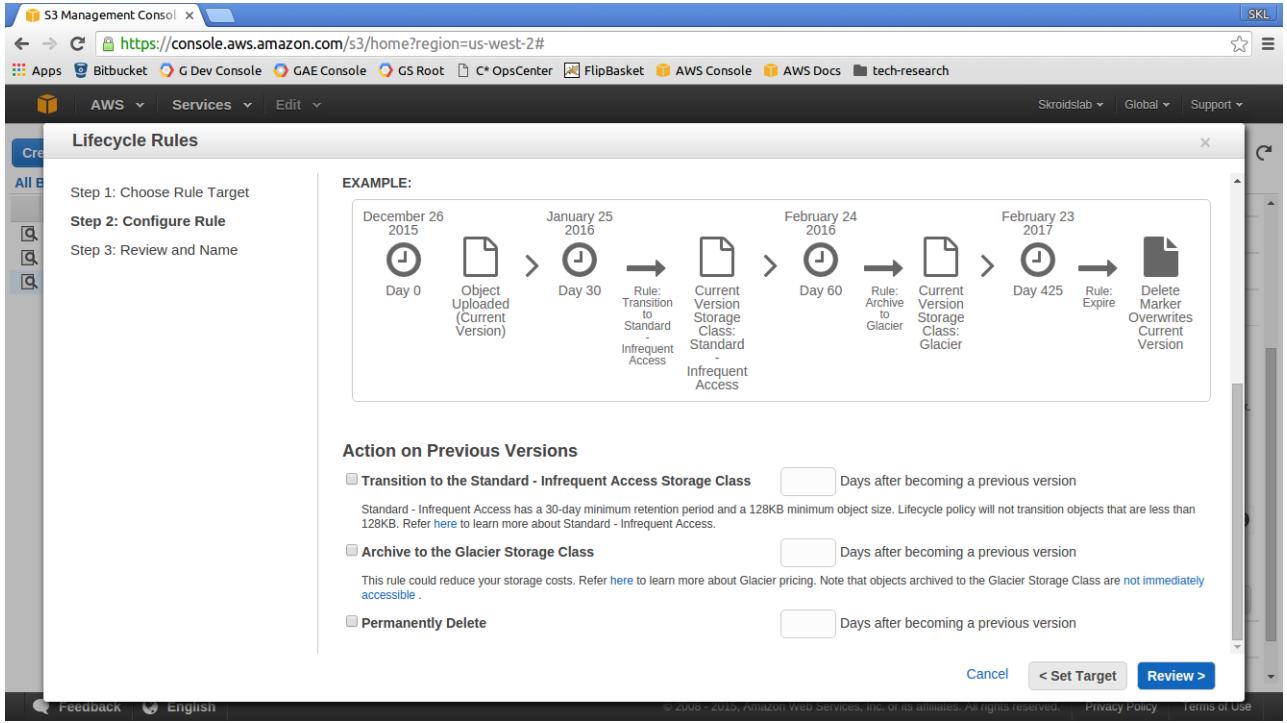


Activity - S3 lifecycle (old UI)



Activity - S3 lifecycle (old UI)

greatlearning



greatlearning

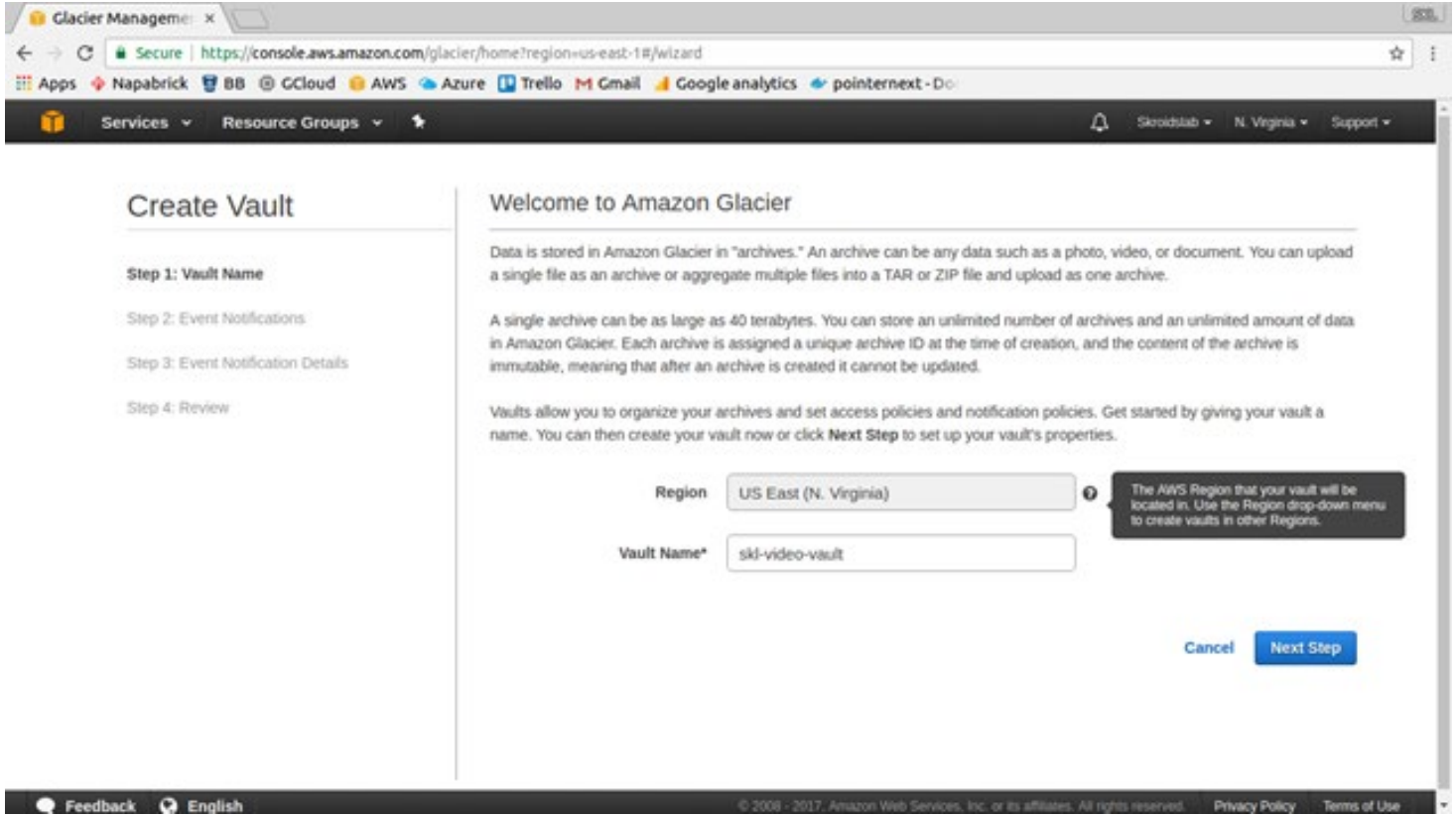
Storage and Content Delivery

Glacier

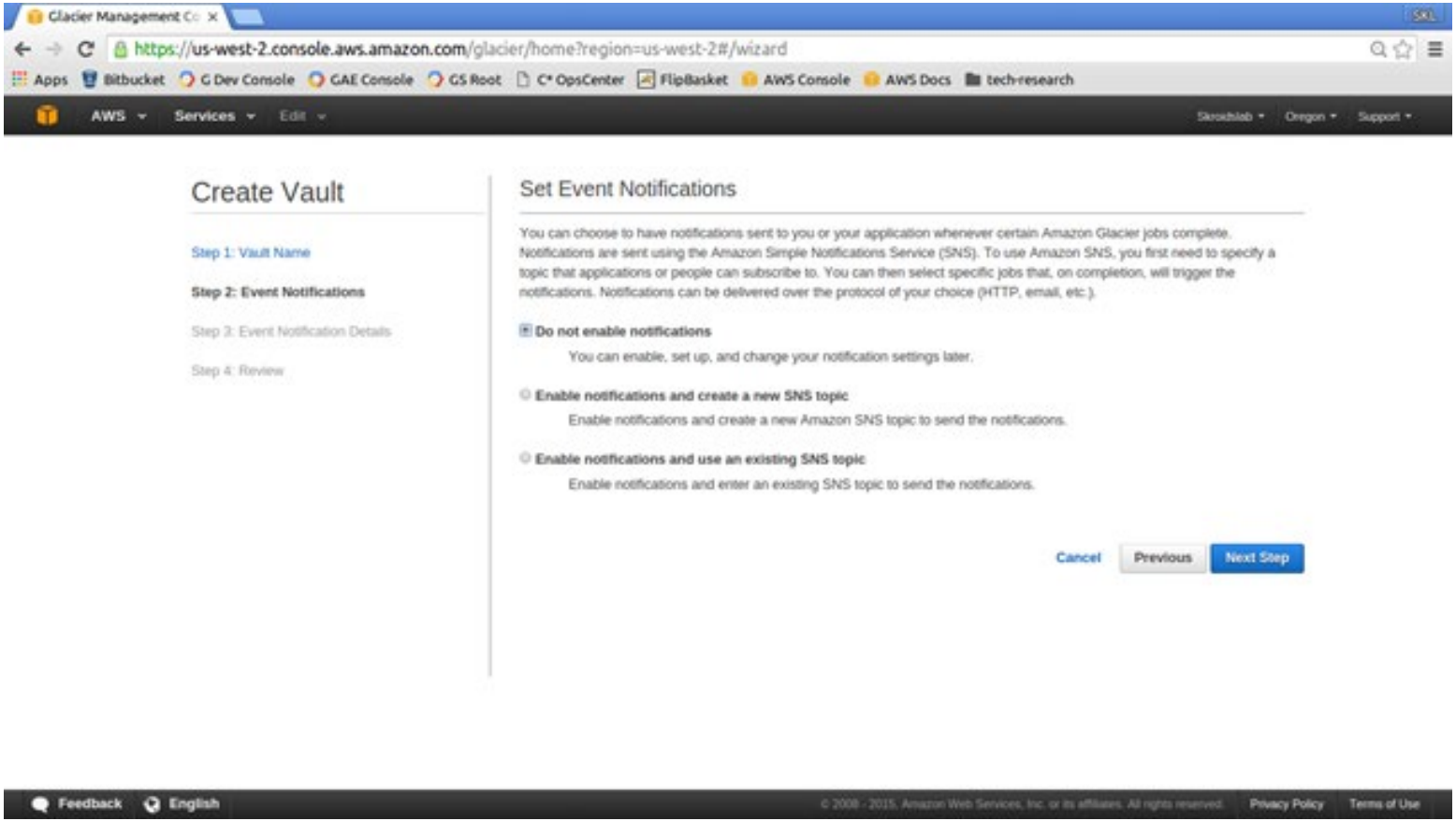
Glacier

- Used for data archival only (e.g. regulatory requirements for keeping data for 'x' years)
- Really cheap $0.01/GB (region specific)
- Infrequently accessed data
- Single archive size is 40TB, can store as many archives
- Need to store for a min of 90 days
- Good use case is to use with versioning + lifecycle management
    - Versioning can quickly create many versions of the files and it can get expensive
    - Here lifecycle management can help

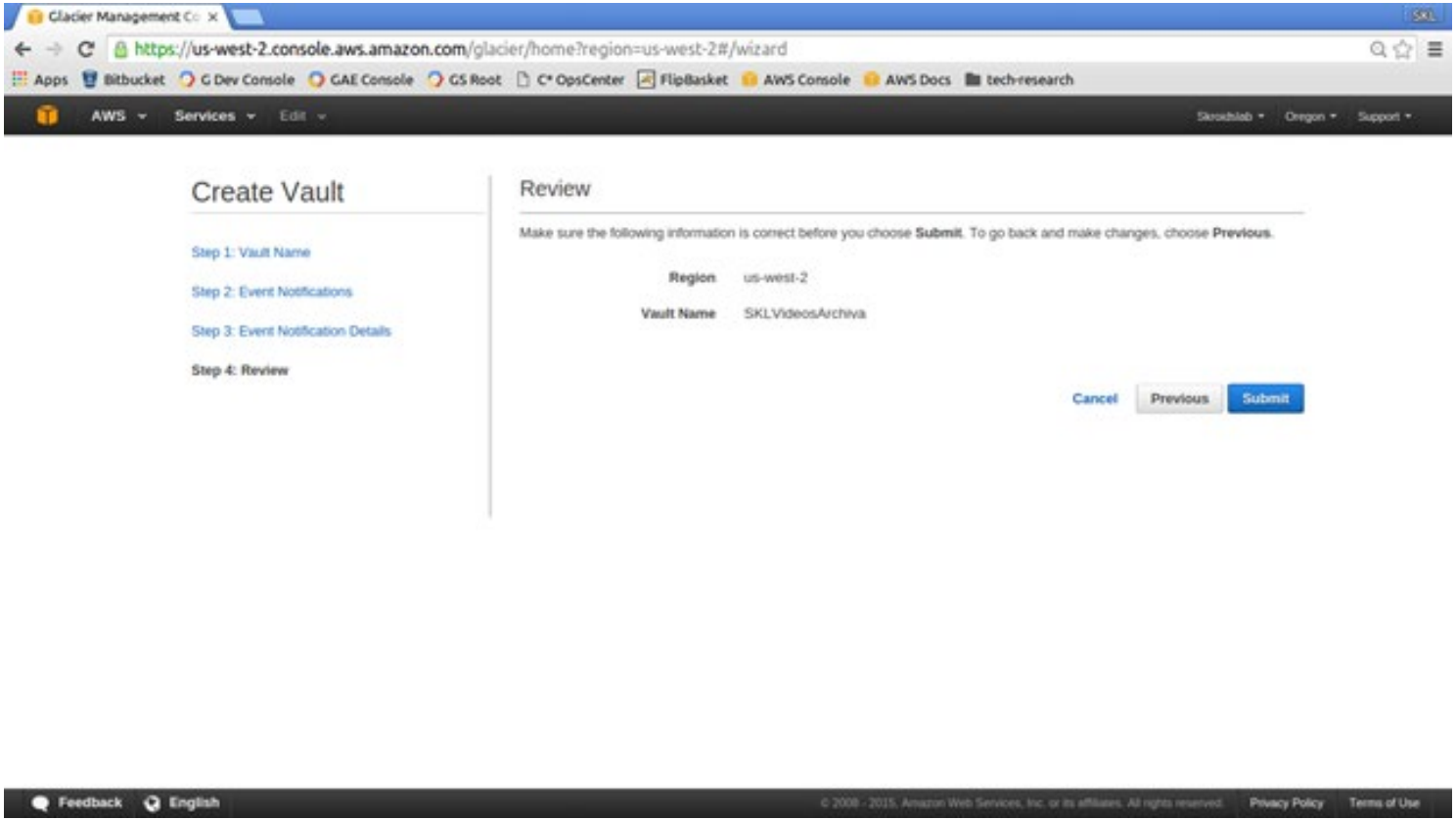
Activity - Glacier



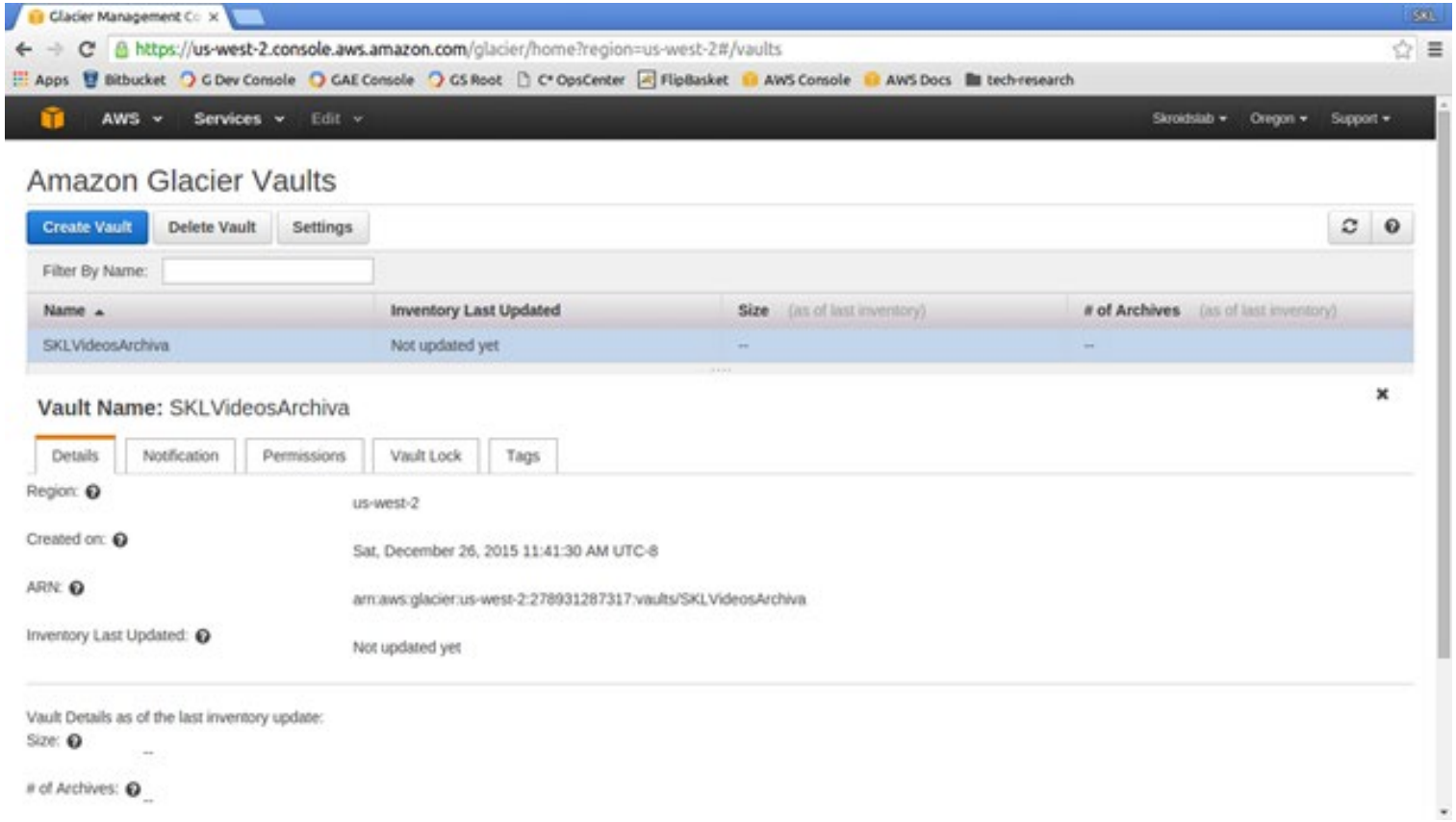
Activity - Glacier



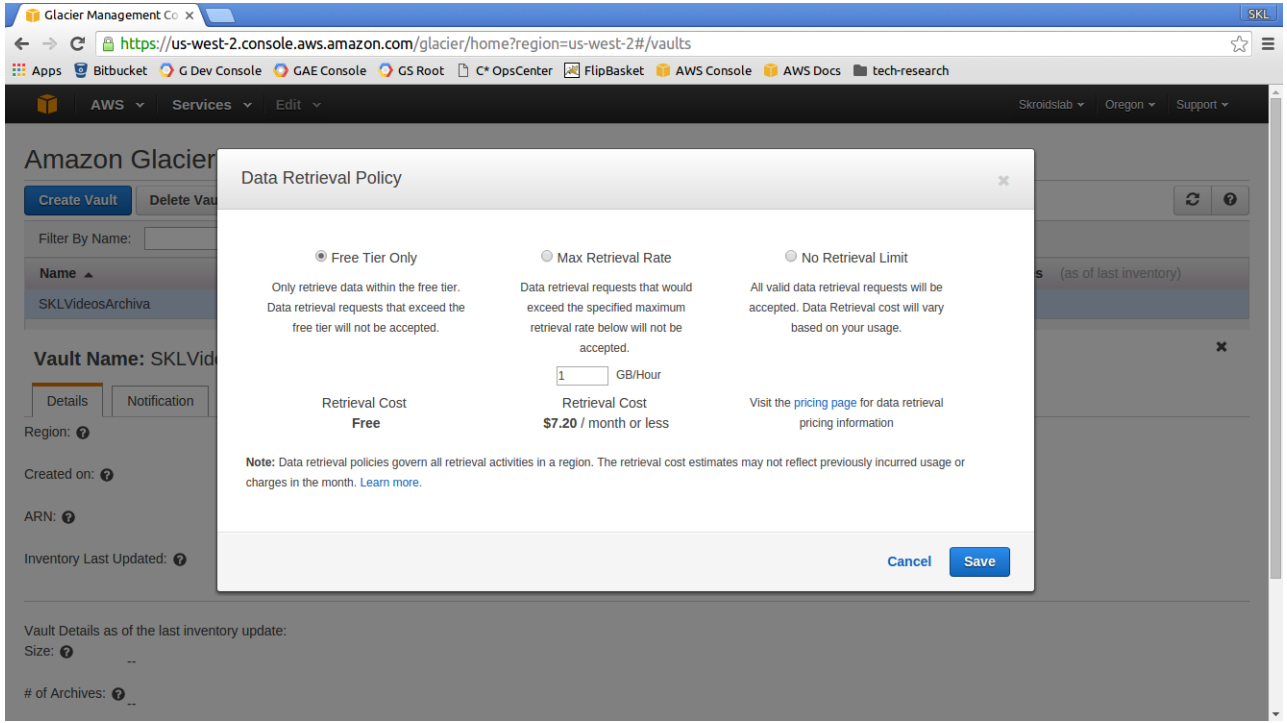
Activity - Glacier



Activity - Glacier



Activity - Glacier



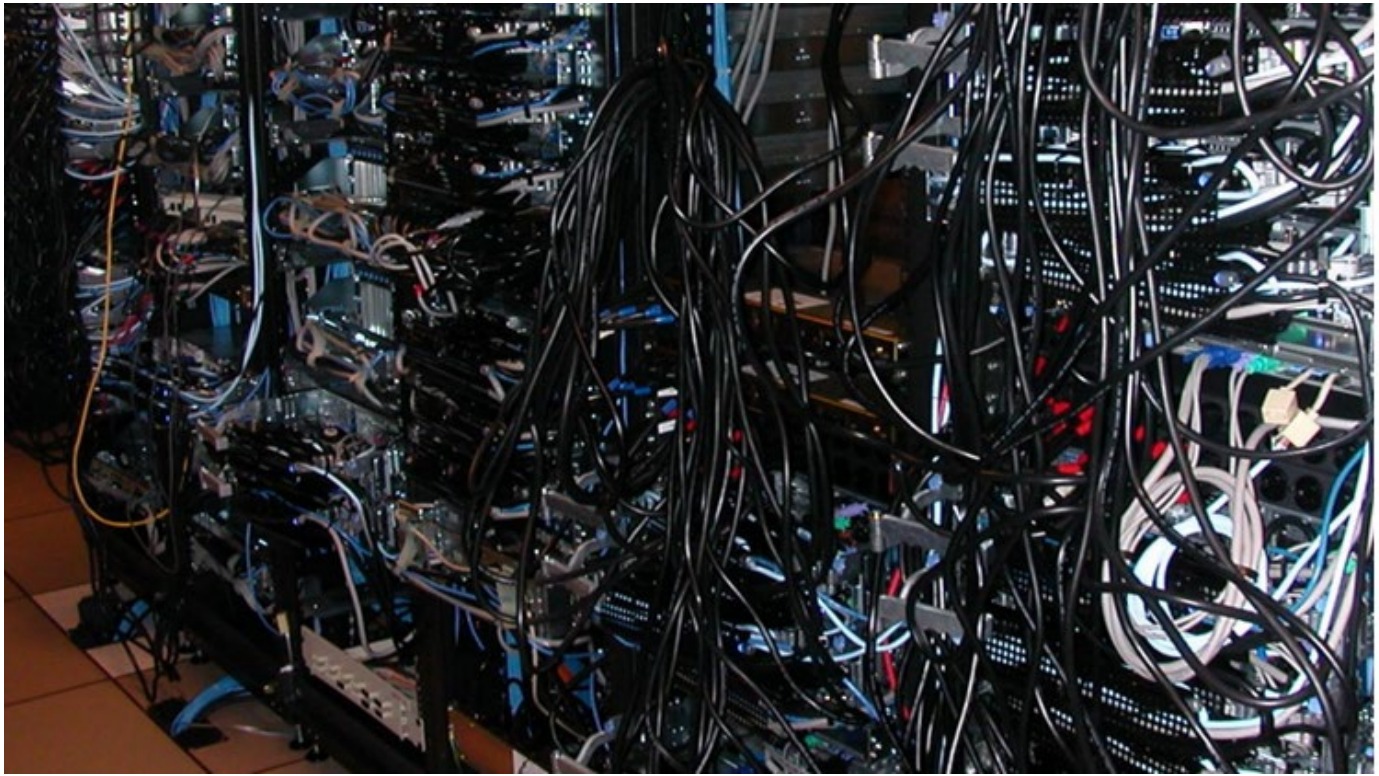
greatlearning

Networking

VPC

Let's talk about this ...

greatlearning

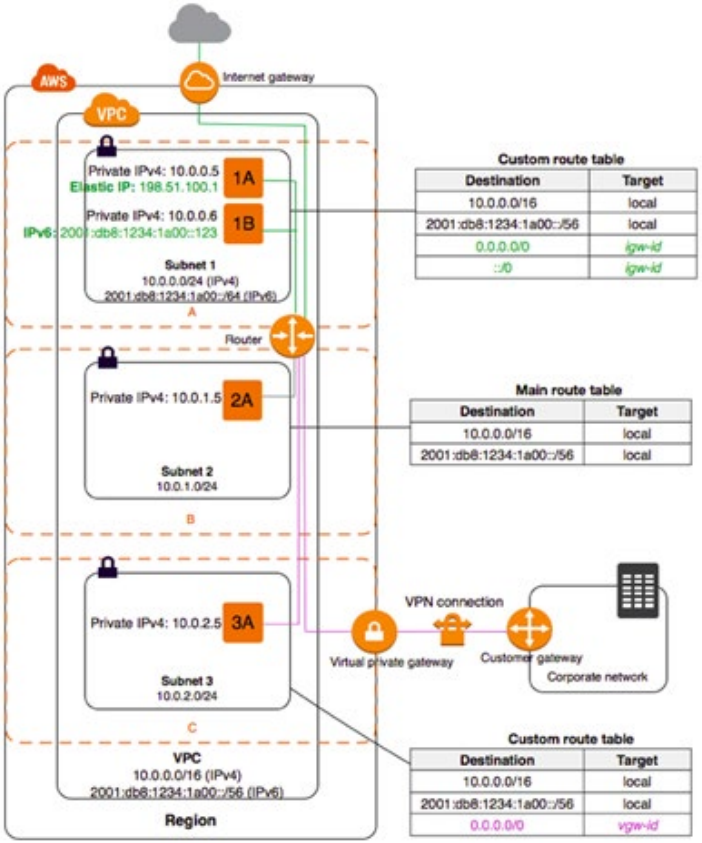


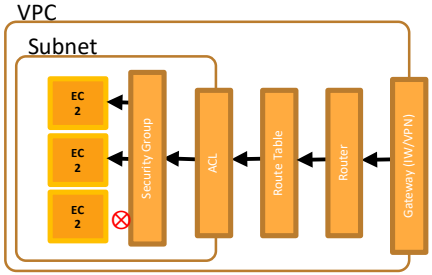
VPC - Virtual Private Cloud

greatlearning

- An AZ is a physical data center but a VPC is like a virtual/logical DC
- Consists of
  - Internet gateways or Virtual Private Gateway
  - Route tables, N/W ACL (stateless)
  - Subnets, Security Groups (are stateful)
- Can have multiple VPCs and can connect one to the other
- VPC can span multiple AZ but not region
- One Subnet "usually" maps to a single AZ (can create more than 1 subnet in the same AZ for a given VPC)
- Default VPC if deleted can be restored by contacting AWS only - careful!
- Peering VPC means connecting multiple VPC together (same or different regions). Can be done with other AWS accounts too
- No Transitive peering, aka one VPC cannot talk to another VPC via some other VPC.
- By default, 5 VPCs are allowed per region and 200 subnets per VPC (both are soft limits)
- Amazon reserves the first 4 IP addresses and the last one 1 IP address of every subnet for IP networking purposes*

VPC - Setup in a given region





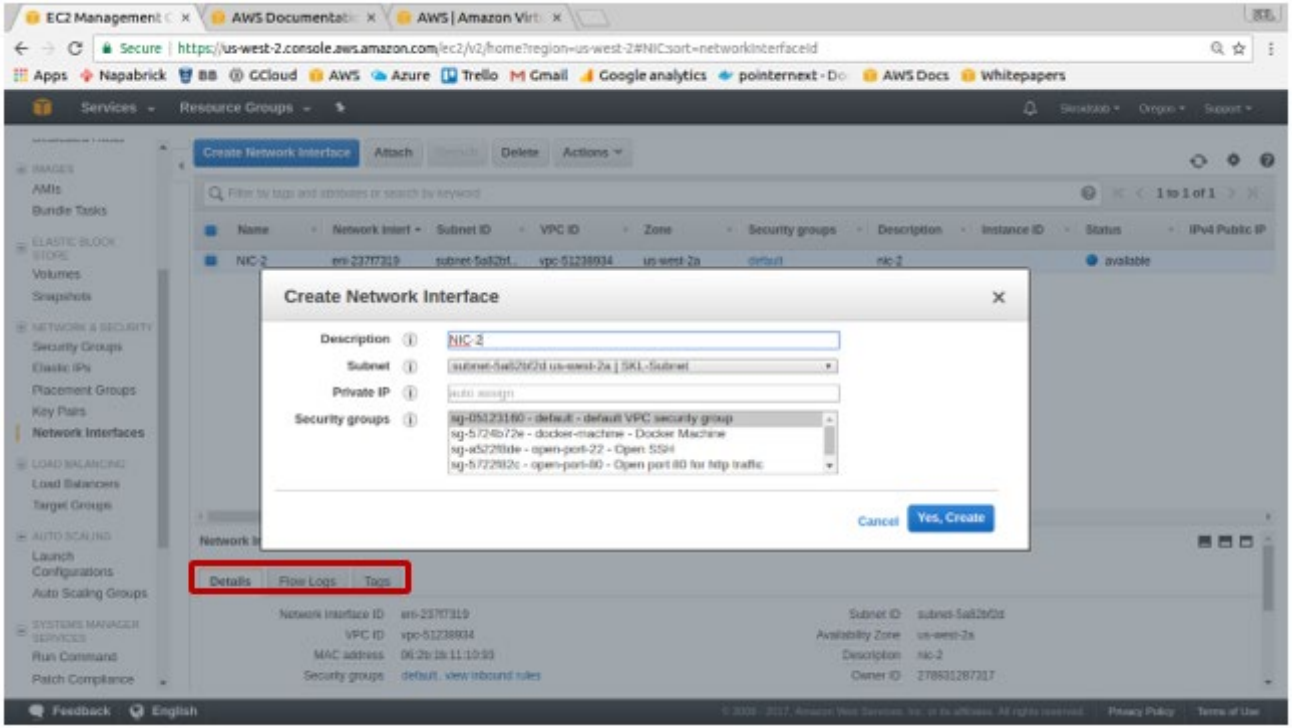
- **AWS provides two features that you can use to increase security in your VPC**
  - **Security groups control inbound and outbound traffic for your instances (stateful)**
  - **Network ACLs control inbound and outbound traffic for your subnets (stateless)**
- **Every subnet that you create is automatically associated with the VPC's default network ACL**
- **If 2A needs to go to the internet then use NAT gateway or NAT instance placed in Subnet 1. Ensure that NAT can receive traffic from an SG that is allocated to 2A**

VPC

- You can assign a single CIDR block to a VPC. The allowed block size is between a /16 netmask and /28 netmask
- The number of addresses of a subnet may be calculated as $2^{\text{address length} - \text{prefix length}}$
  - /28 means $2^{32-28} = 2^4 = 16$ addresses
  - /16 means $2^{32-16} = 2^{16} = 65536$ addresses
- A few examples
  - 192.168.100.14/24 represents the IPv4 address 192.168.100.14 and its associated routing prefix 192.168.100.0, or equivalently, its subnet mask 255.255.255.0, which has 24 leading 1-bits
  - the IPv4 block 192.168.100.0/22 represents the 1024 IPv4 addresses from 192.168.100.0 to 192.168.103.255 [x.x.100.0 to x.x.103.255 = 256 addresses times 4 = 1024 addresses]
- AWS VPC can contain from 16 to 65,536 IP addresses.
- The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC), or a subset (for multiple subnets).
- If you create more than one subnet in a VPC, the CIDR blocks of the subnets cannot overlap.

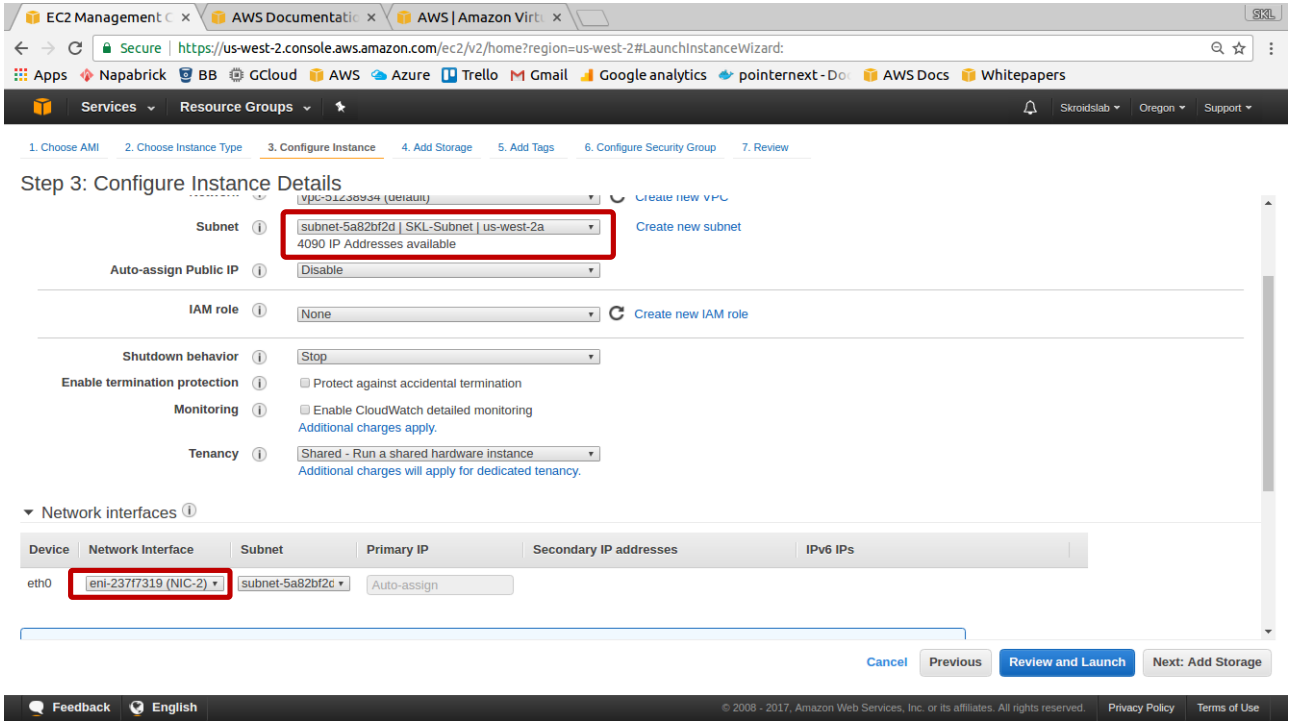
http://www.subnet-calculator.com/cidr.php

Adding more than 1 NIC to EC2



Flow logs allow you to trace all requests going through the VPC

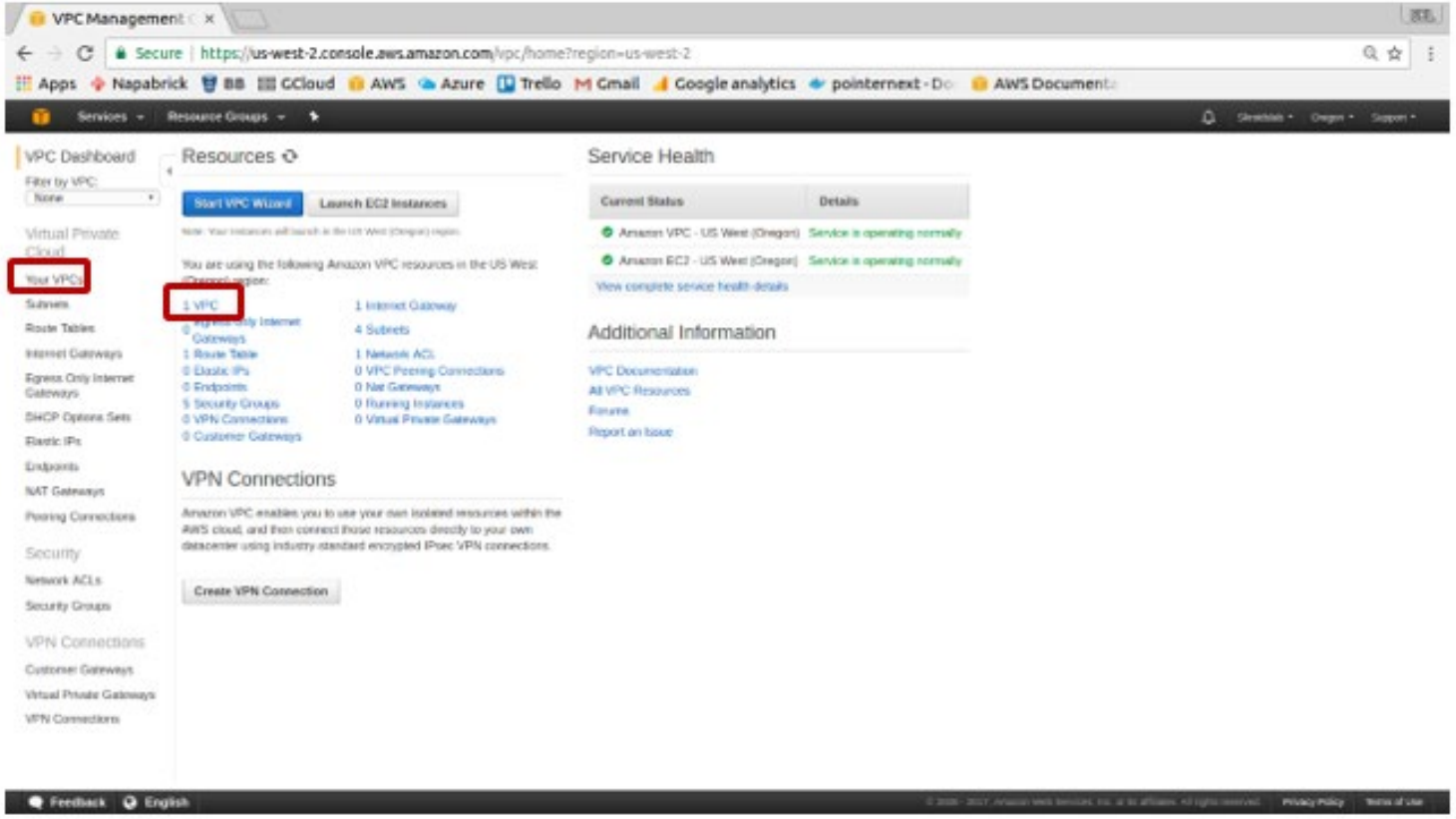
Add VPC and more than 1 NIC to EC2



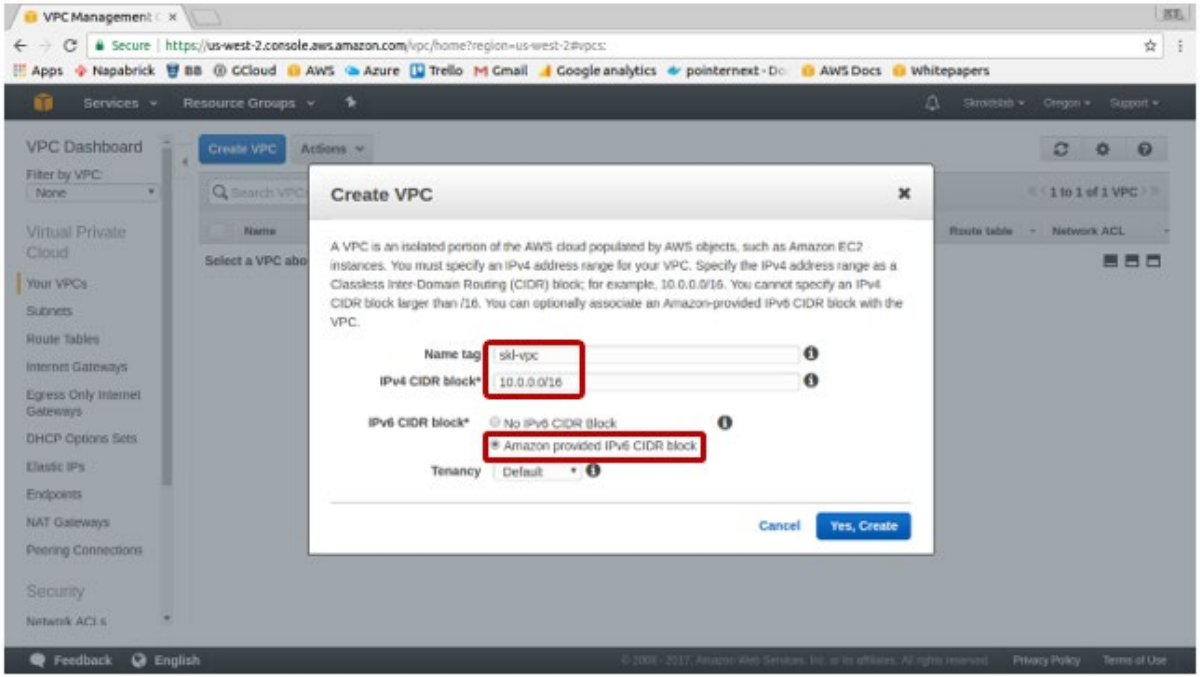
If your applications benefit from high packet-per-second performance and/or low latency networking, EC2 "Enhanced Networking" will provide significantly improved performance, consistency of performance and scalability (EC2 faq)

Activity - VPC (Region)

greatlearning



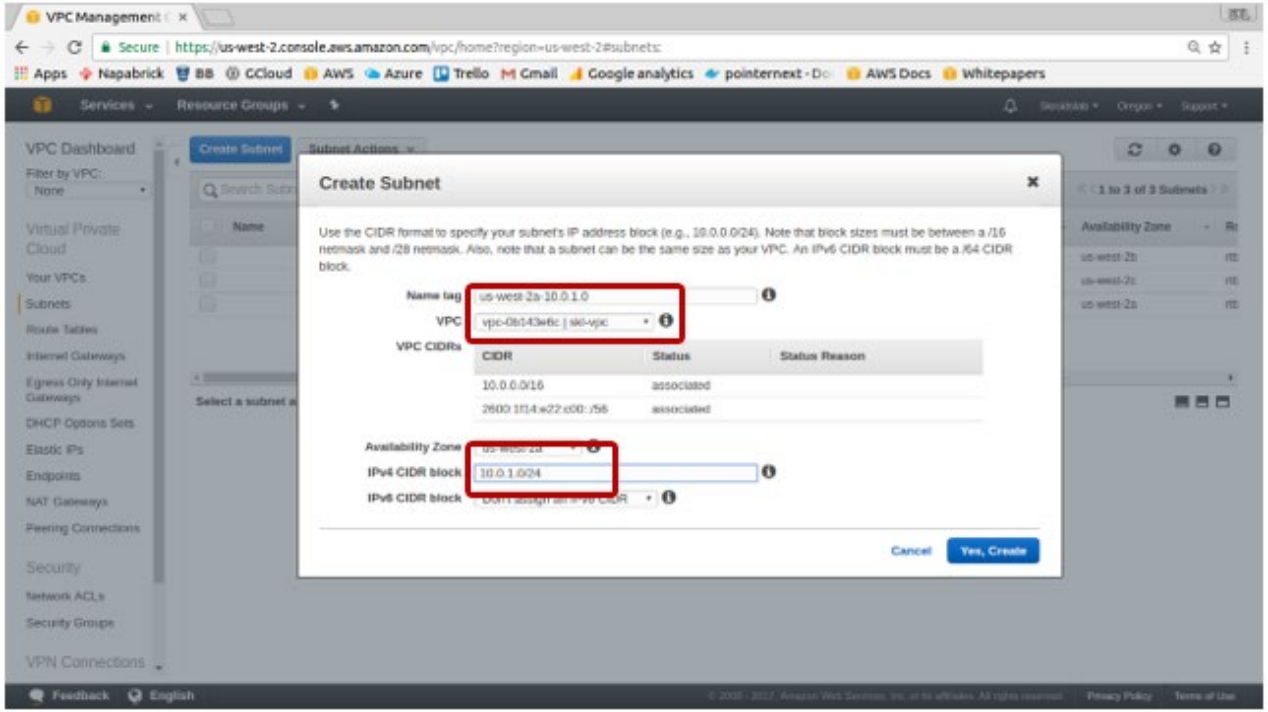
Activity - VPC



Creating the VPC also created main route table, default security group, ACL but no subnet, internet gateway

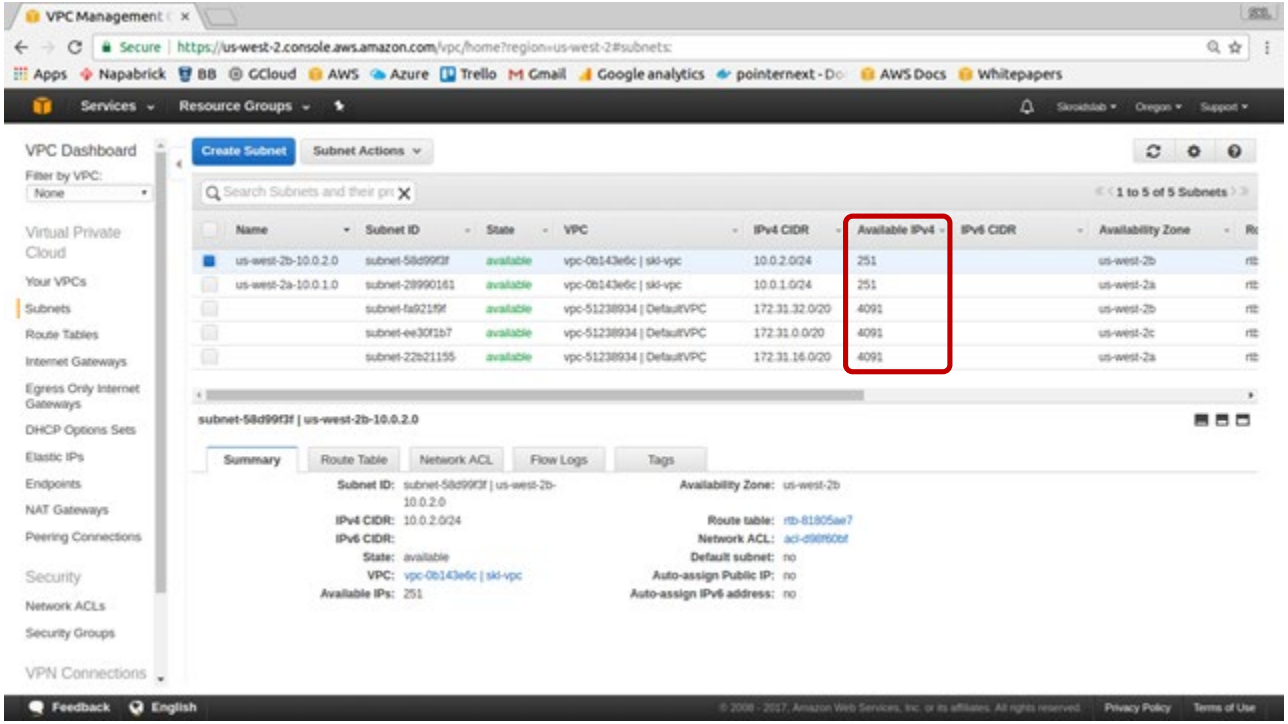
Activity - Subnet (Availability Zone)

greatlearning



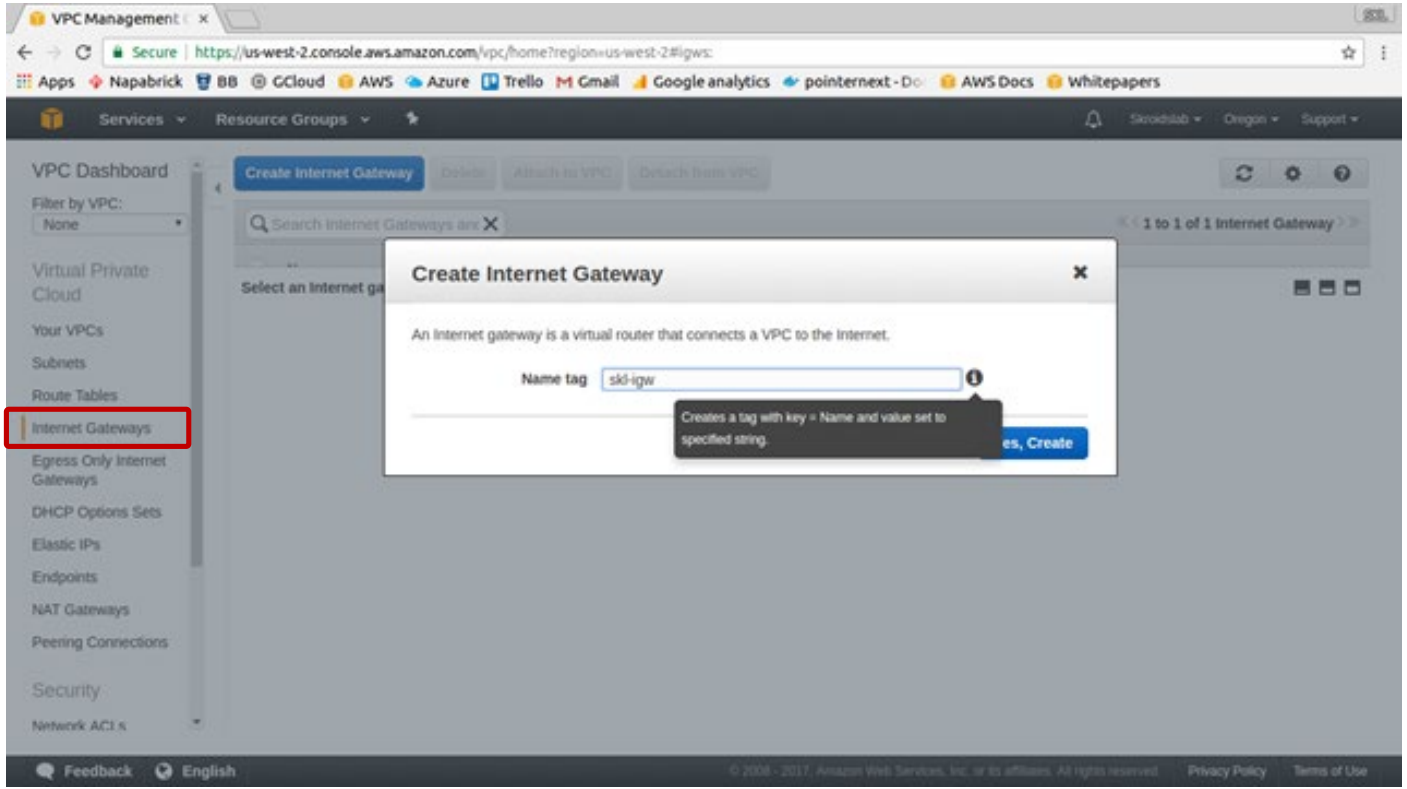
Create a subnet (AZ) in a given region, notice the naming
Create 1 more subnet with CIDR 10.0.2.0/24 in another AZ

Activity - Subnet

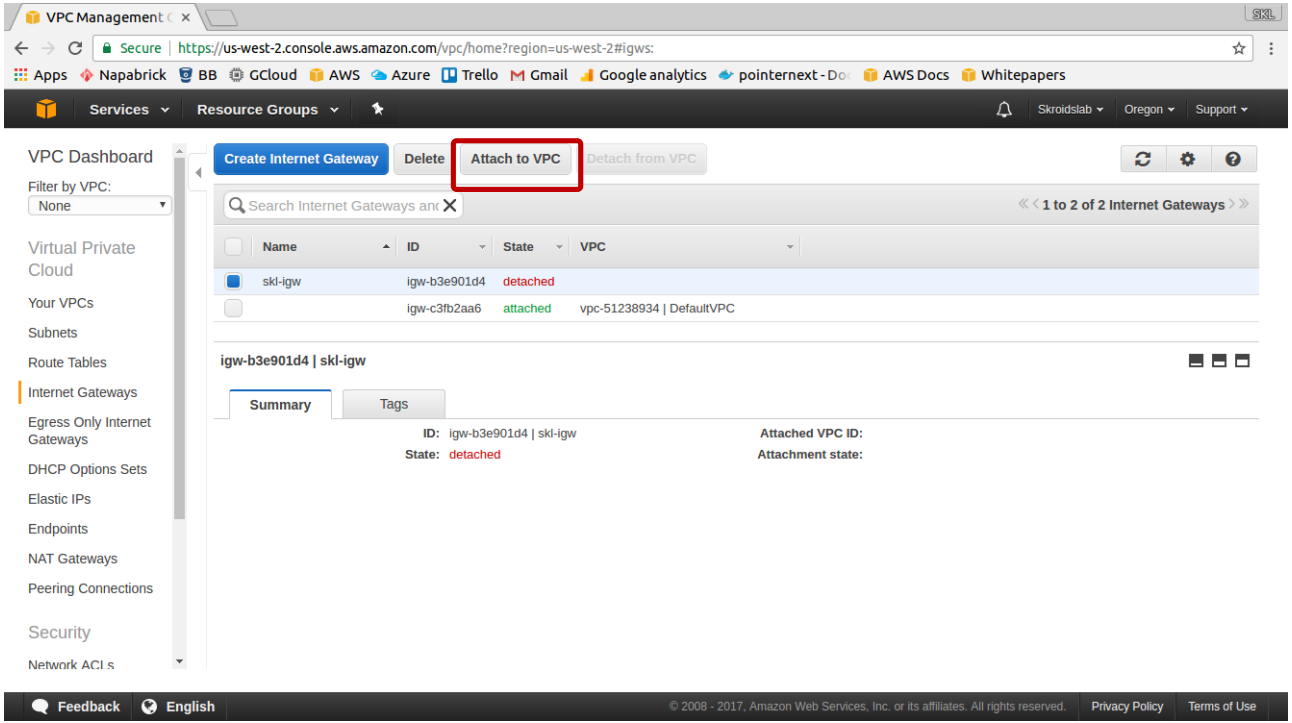


We will now make 1 public subnet (need IG) and the other private

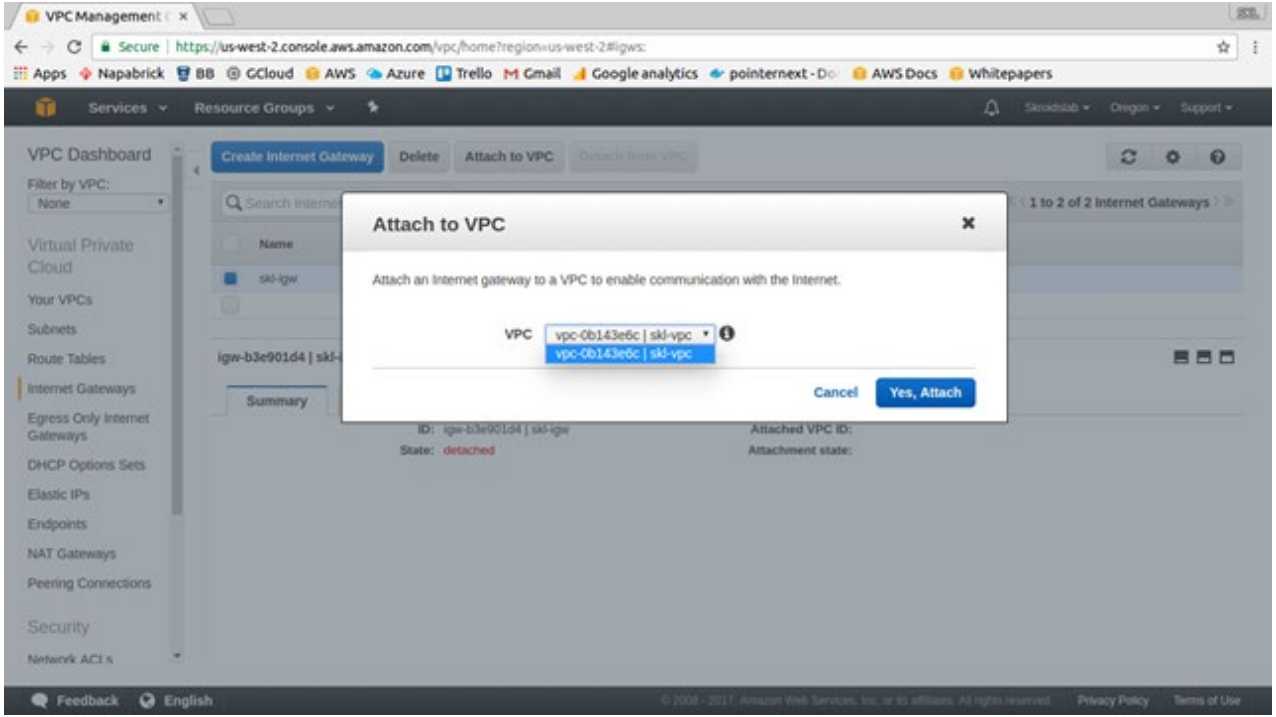
Activity - Internet Gateway



Activity - IG to VPC association

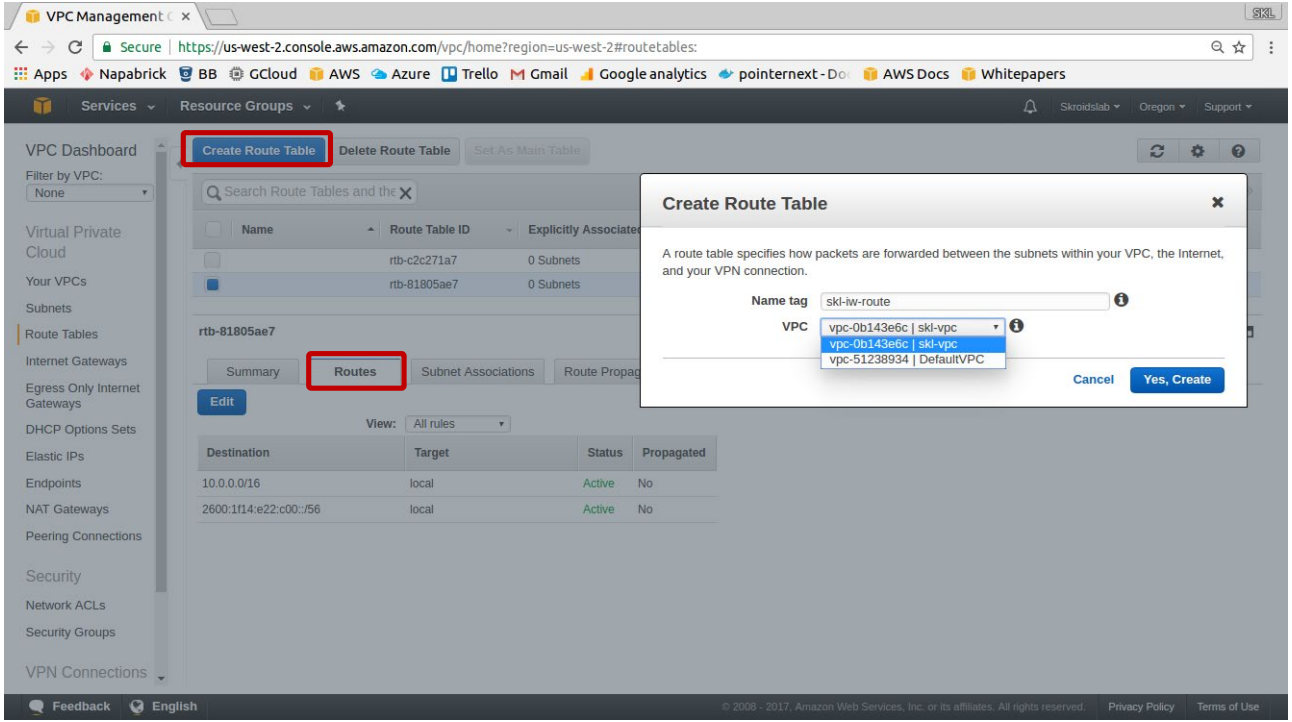


Activity - IG to VPC association



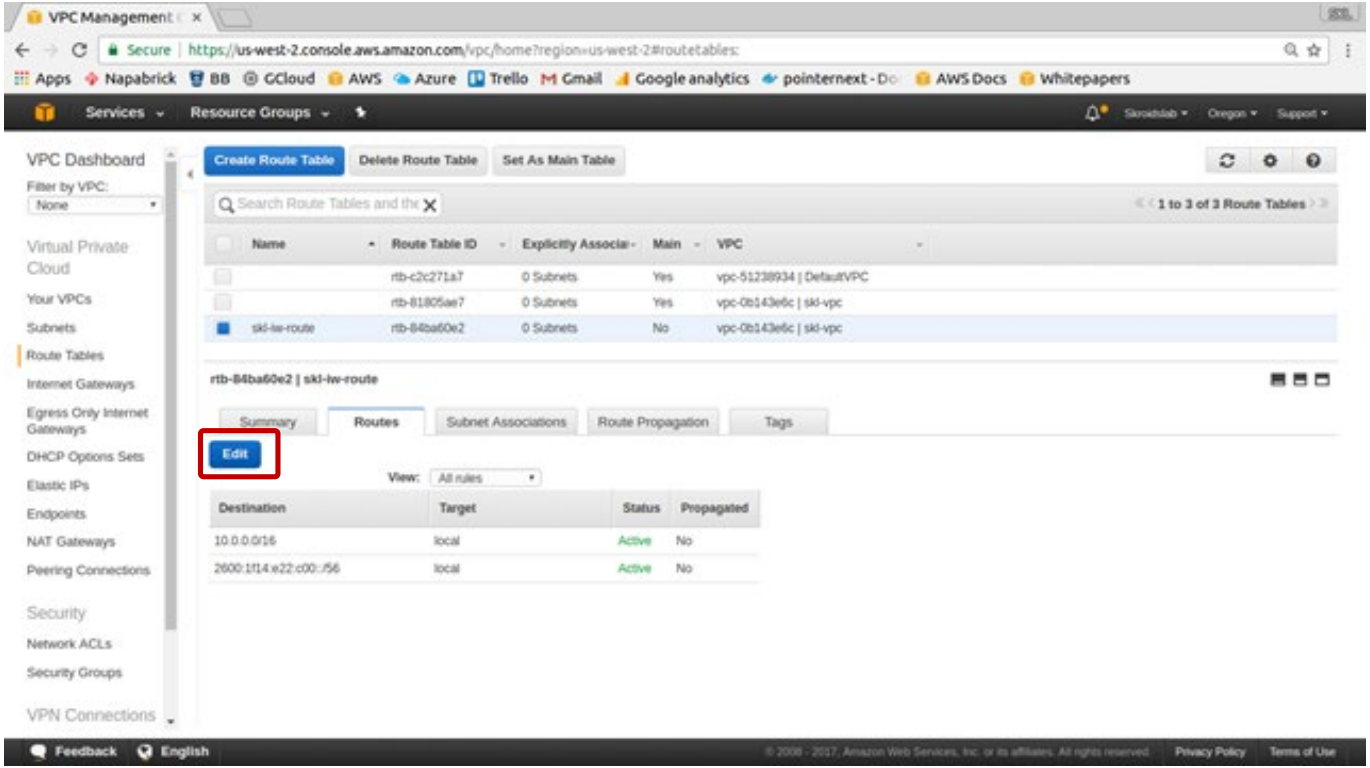
Cannot assign more than 1 IGW to a vpc. The subnets however can not go out to the internet just yet.

Activity - Route Table (RT)

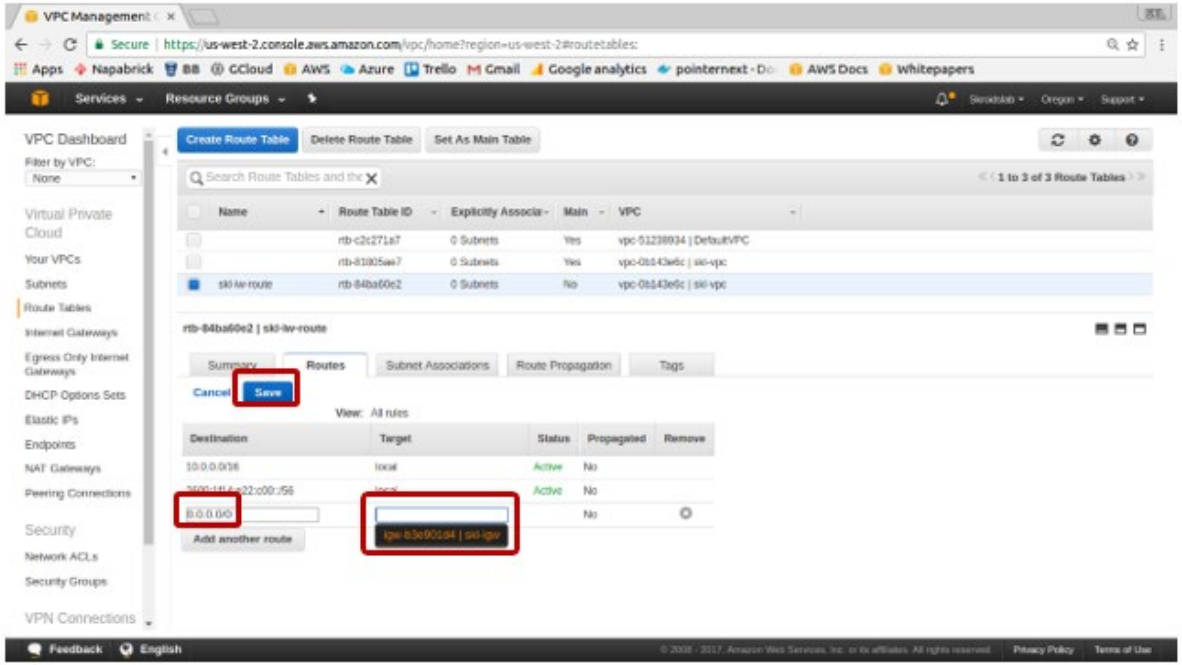


The IG can be associated to the main VPC RT but that will let out all the VPC to the internet, hence this custom RT for the new VPC

Activity - Attach IG to RT

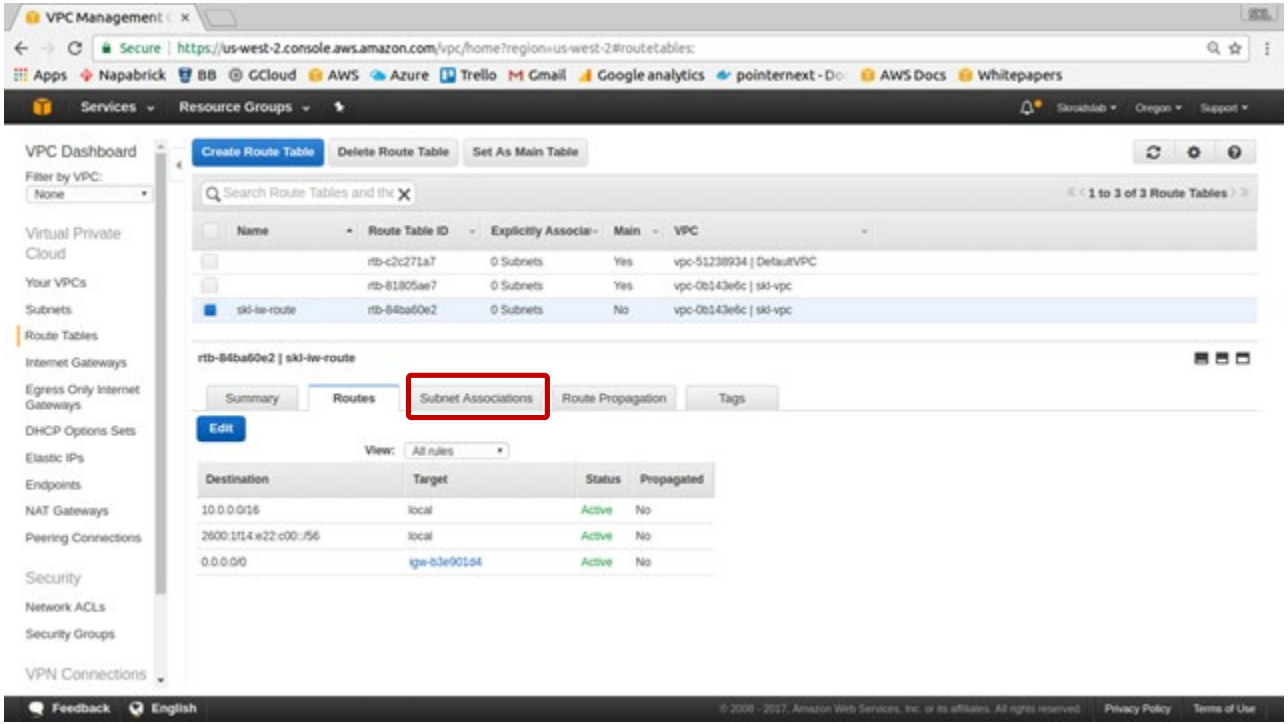


Activity - Attach IG to RT



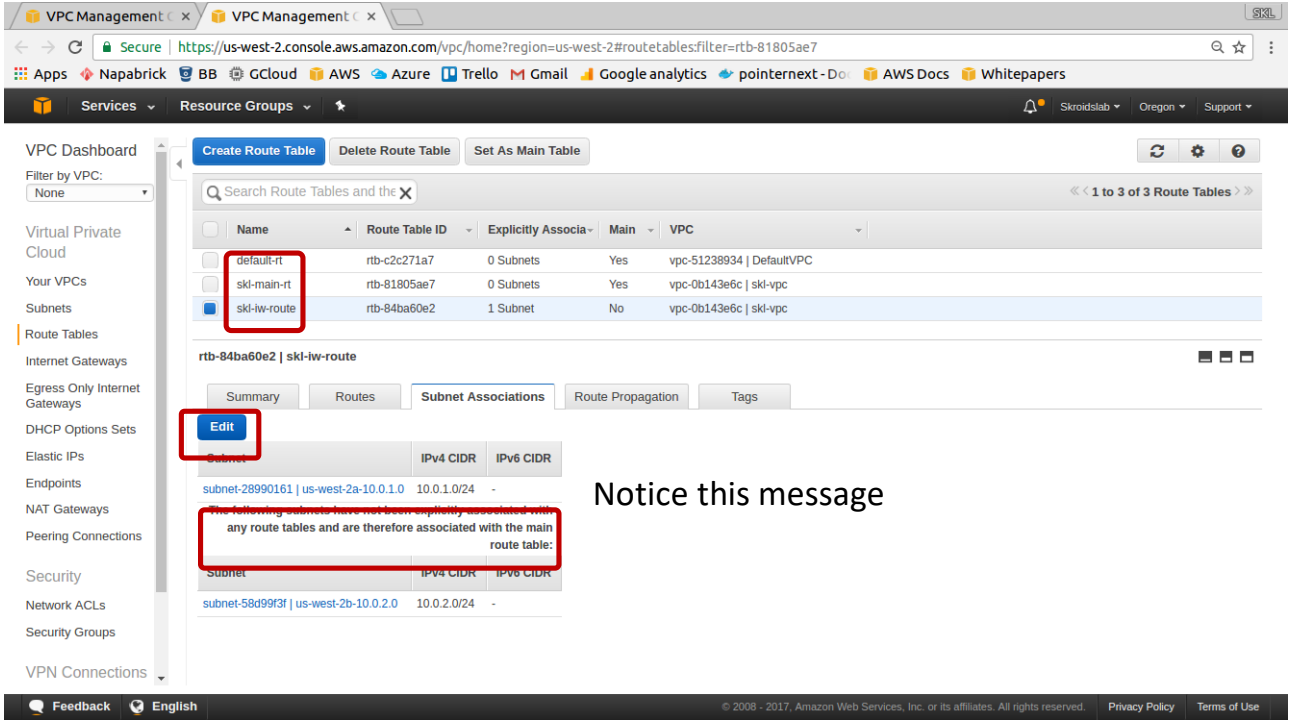
Let's now update the route table as follows -
0.0.0.0/0 lets out all traffic and associate with the IG

Activity - attach RT to subnet



Activity - attach RT to subnet

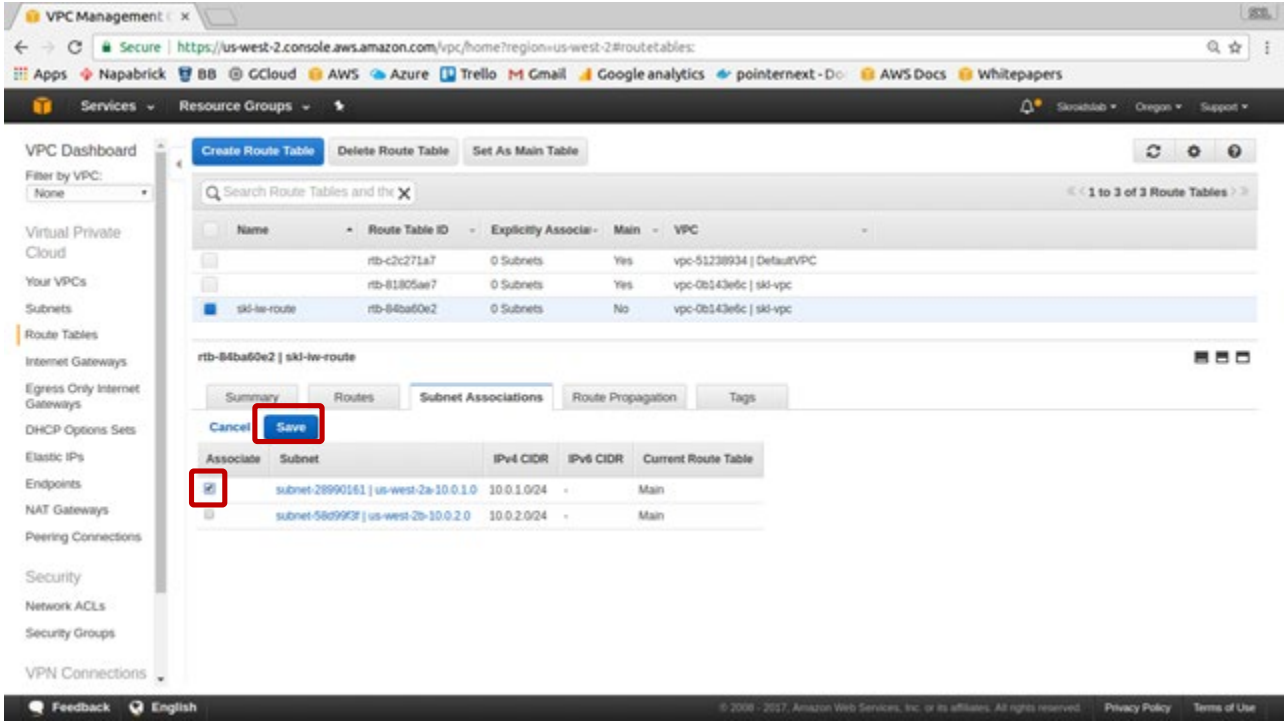
greatlearning



Notice this message

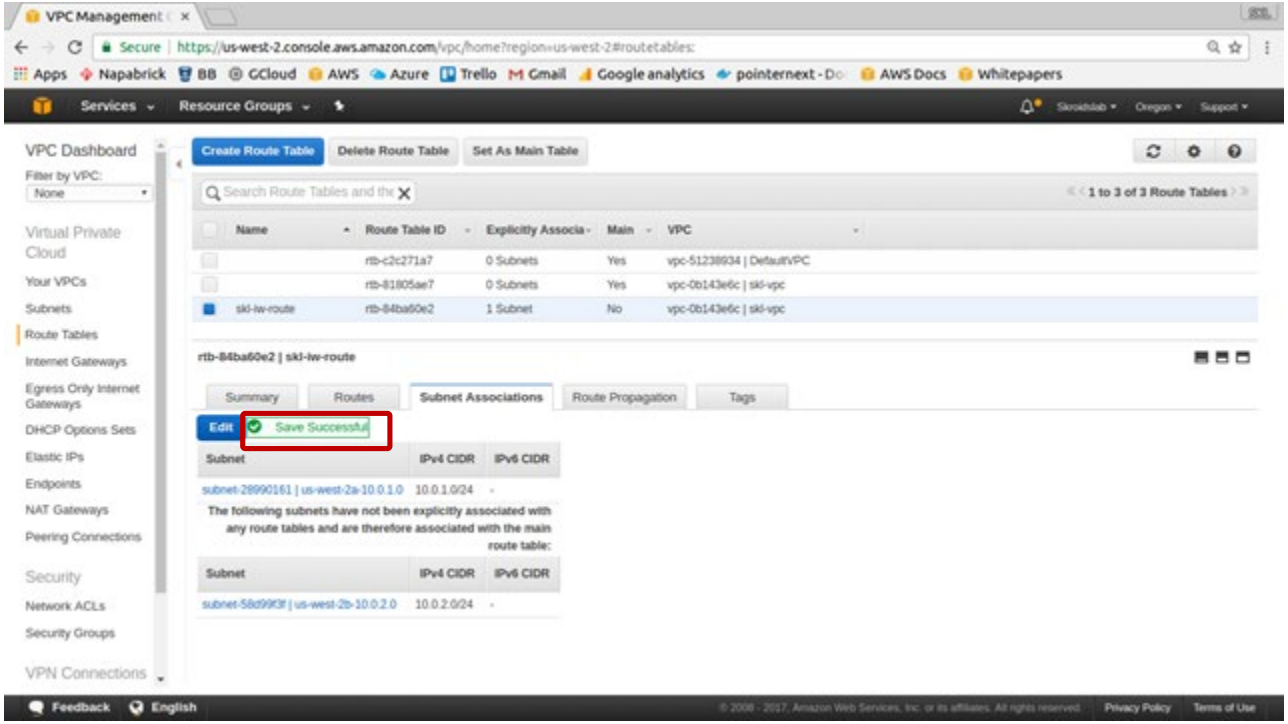
Name the RTs for better readability

Activity - attach RT to subnet



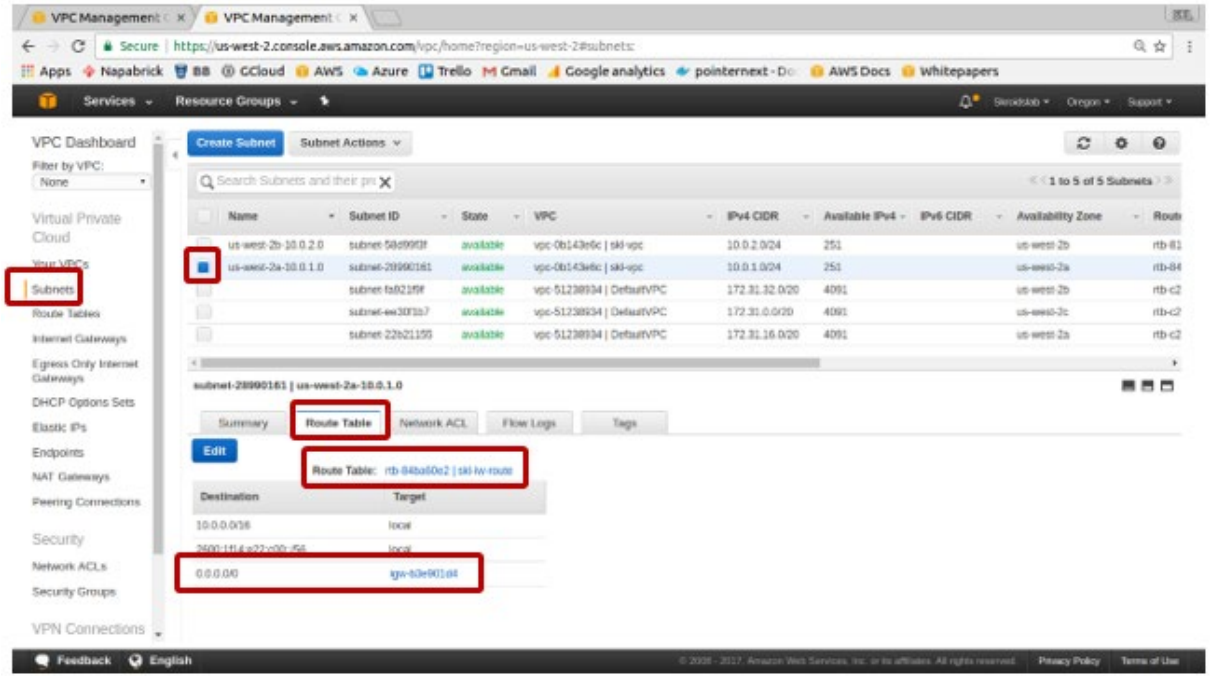
Now only this subnet will be able to access internet and not the other one!

Activity - attach RT to subnet



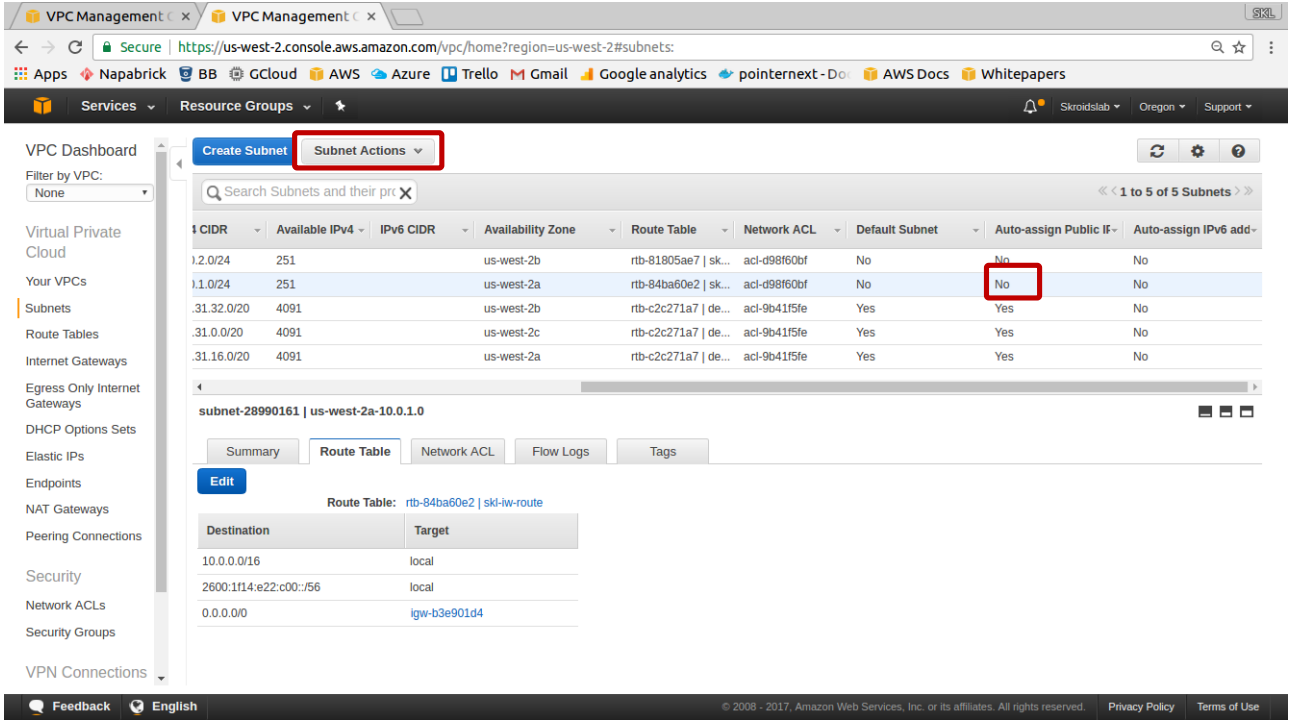
Activity - Subnet associated to RT

greatlearning



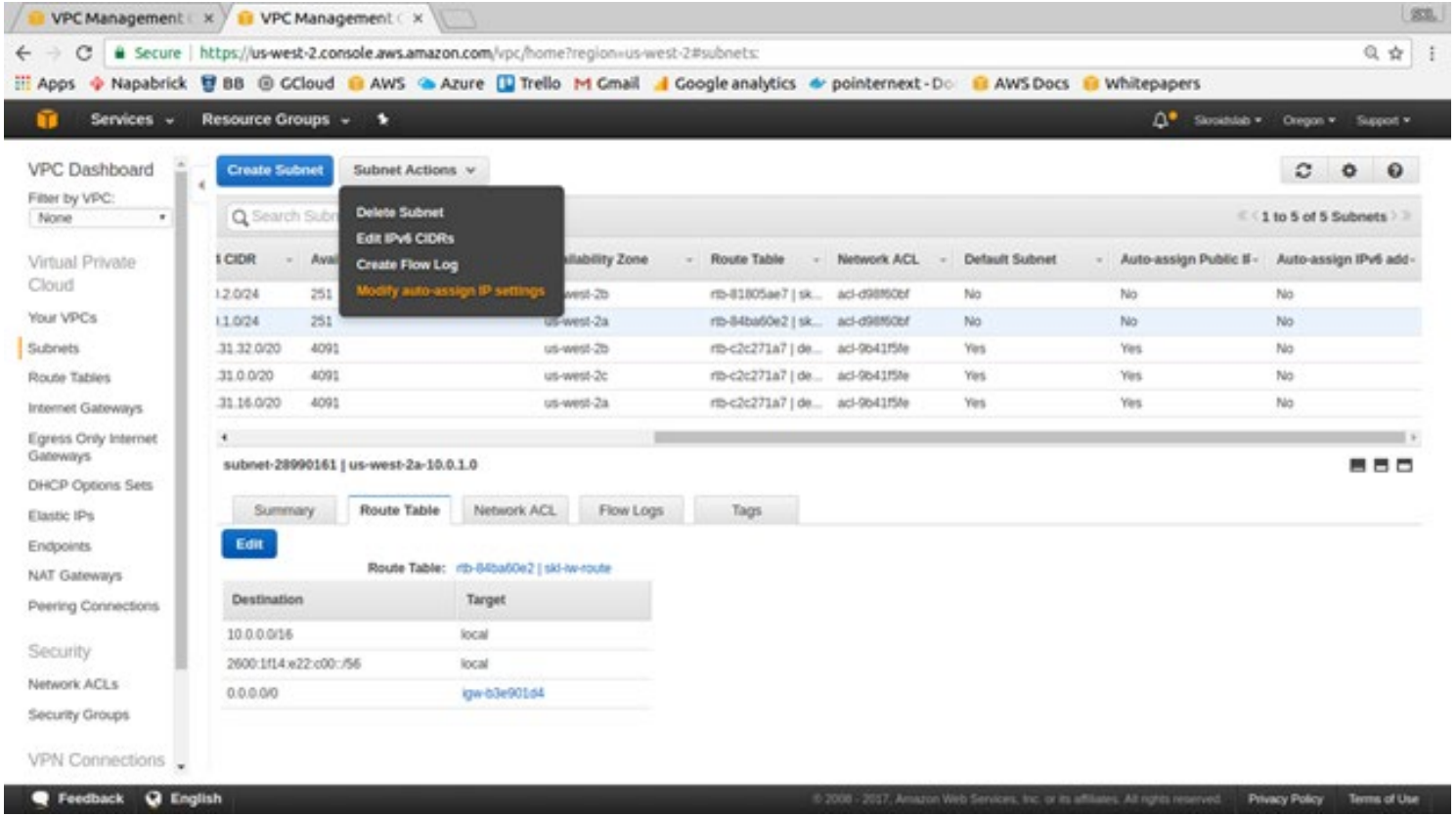
Observe the route table associations. A subnet can be associated with multiple RT. Scroll to the right ...

Activity - Subnet rule needs Public IP

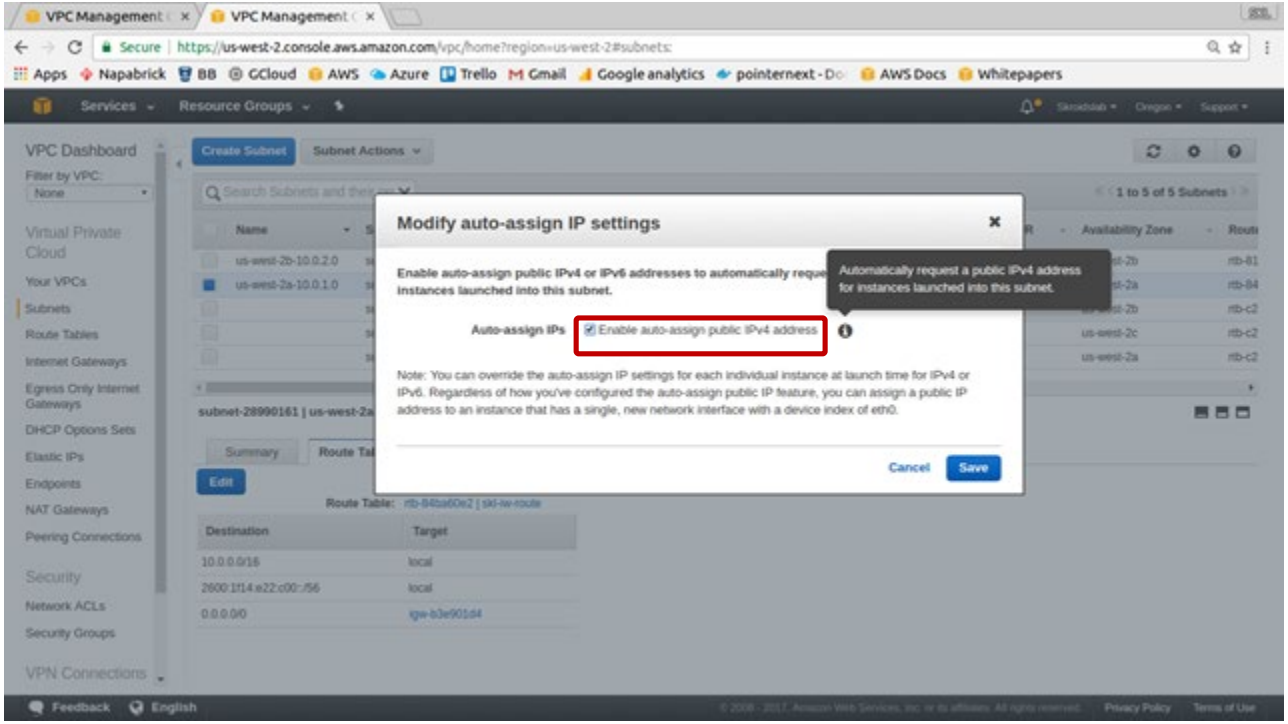


Activity - Subnet rule needs Public IP

greatlearning

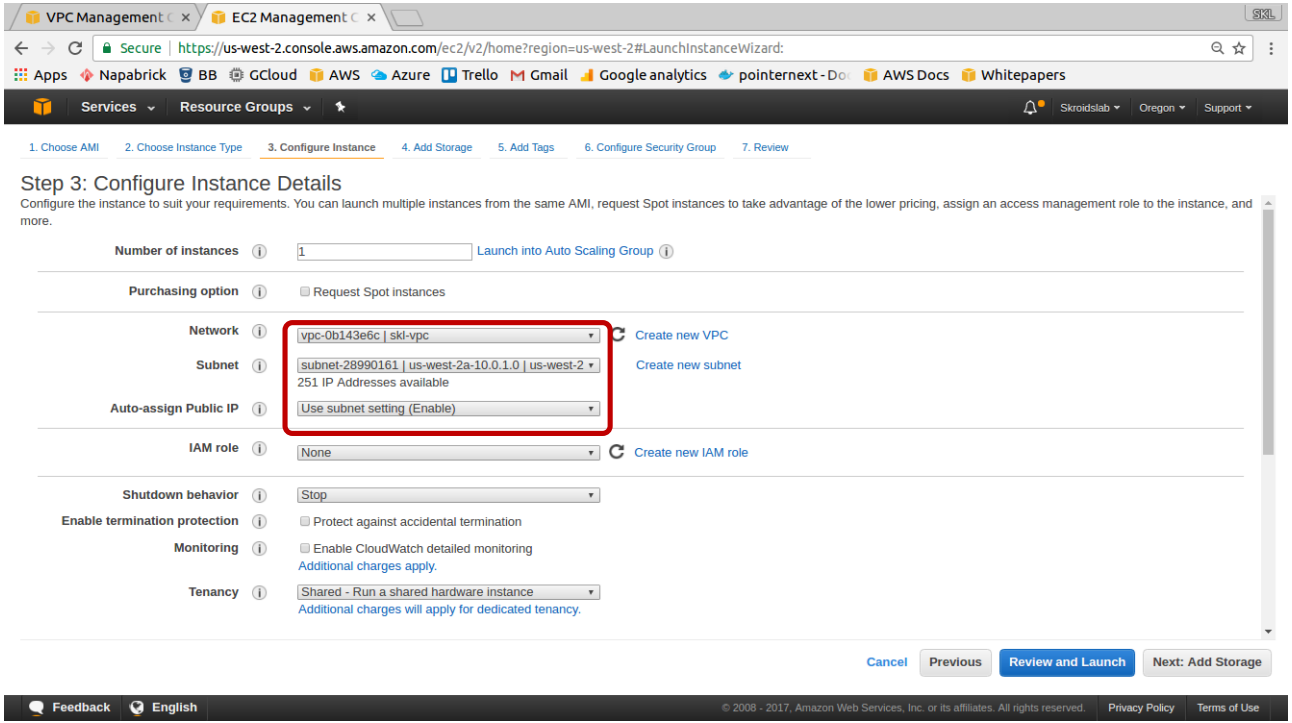


Activity - Subnet rule needs Public IP

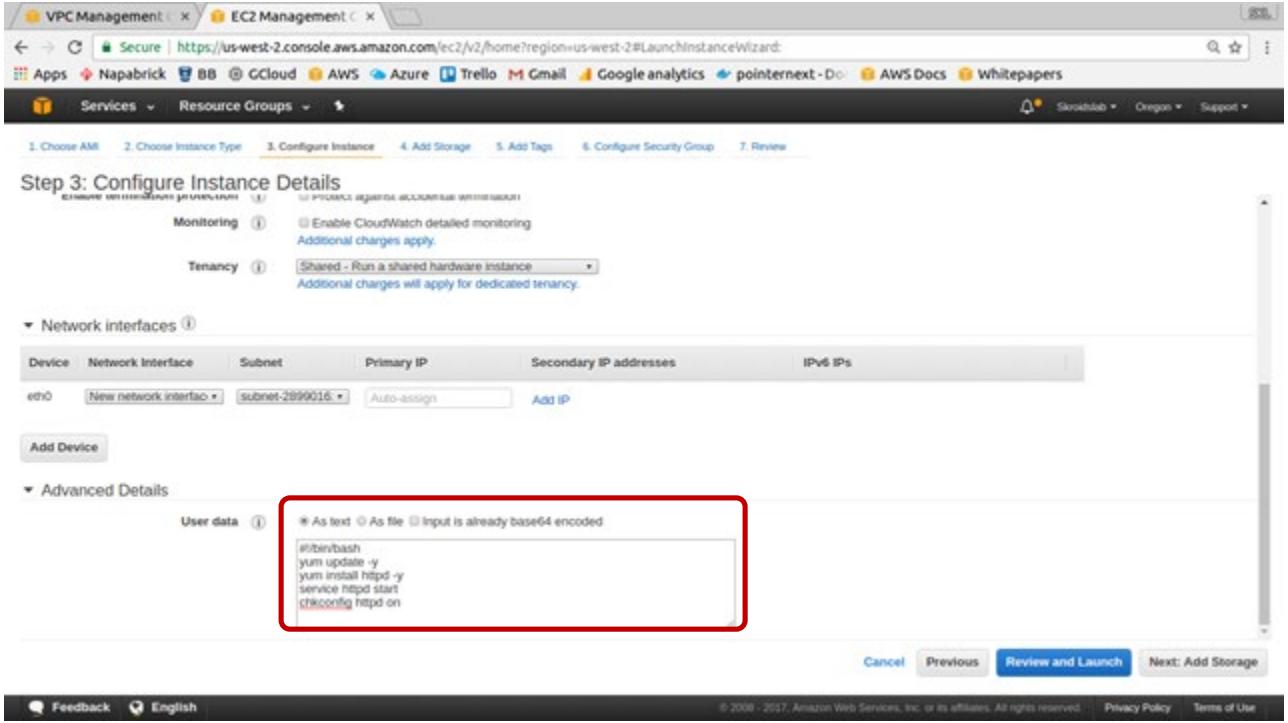


If you forget, you can enable at the time of launching EC2

Activity - launch EC2 in subnet 1

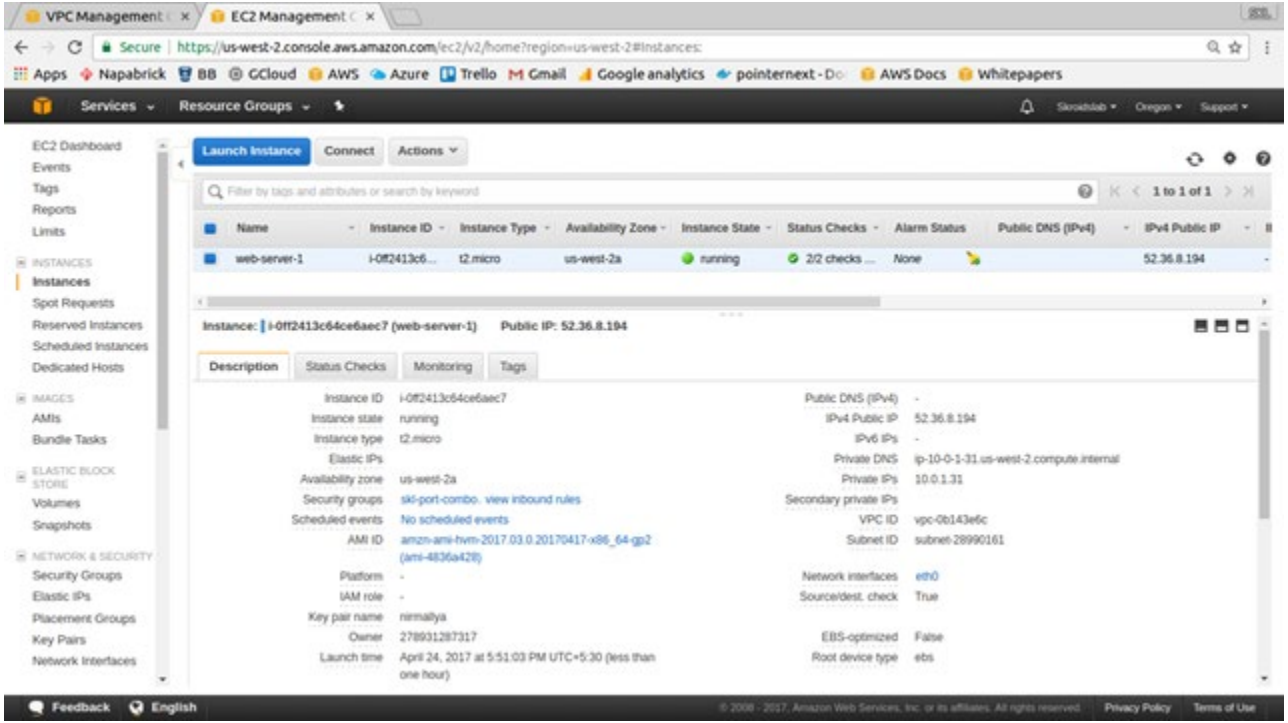


Activity - launch EC2 in subnet 1



Make a security group allowing http, https & SSH. Ensure that you use the PEM that you had downloaded earlier.

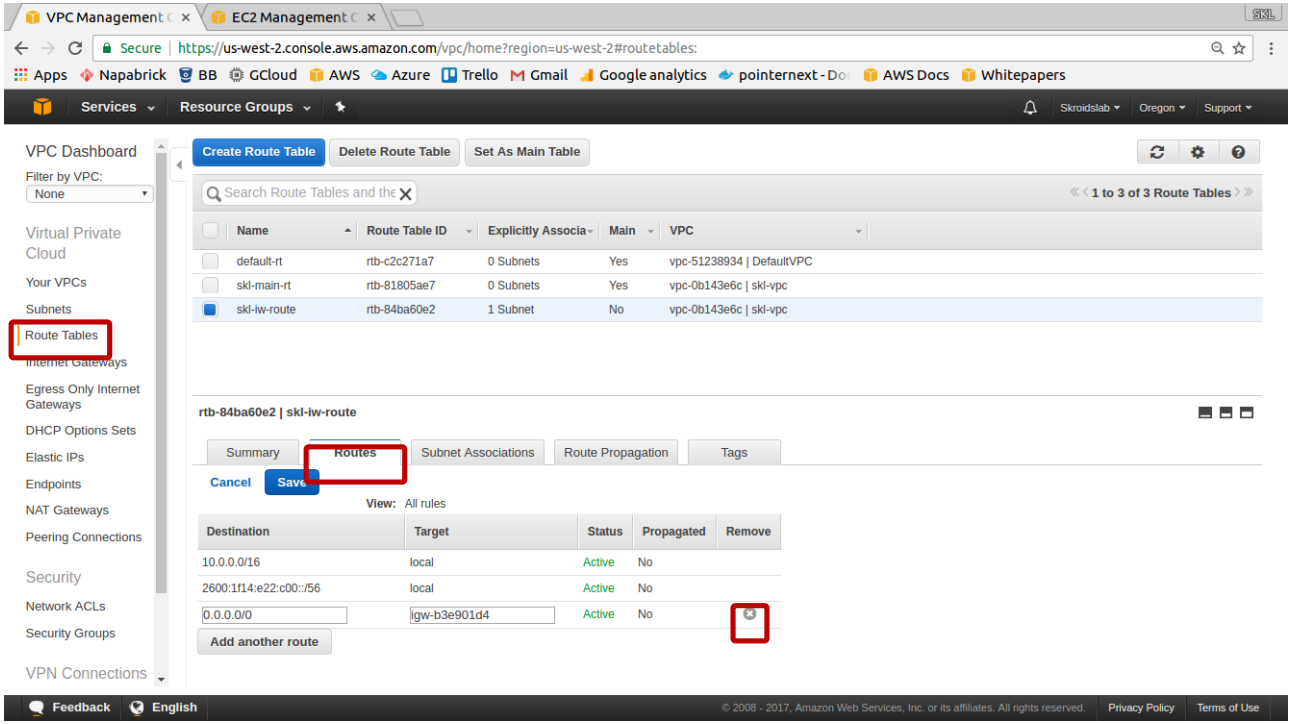
Activity - launch EC2 in subnet 1



Hit the public IP and you should be able to see the web page

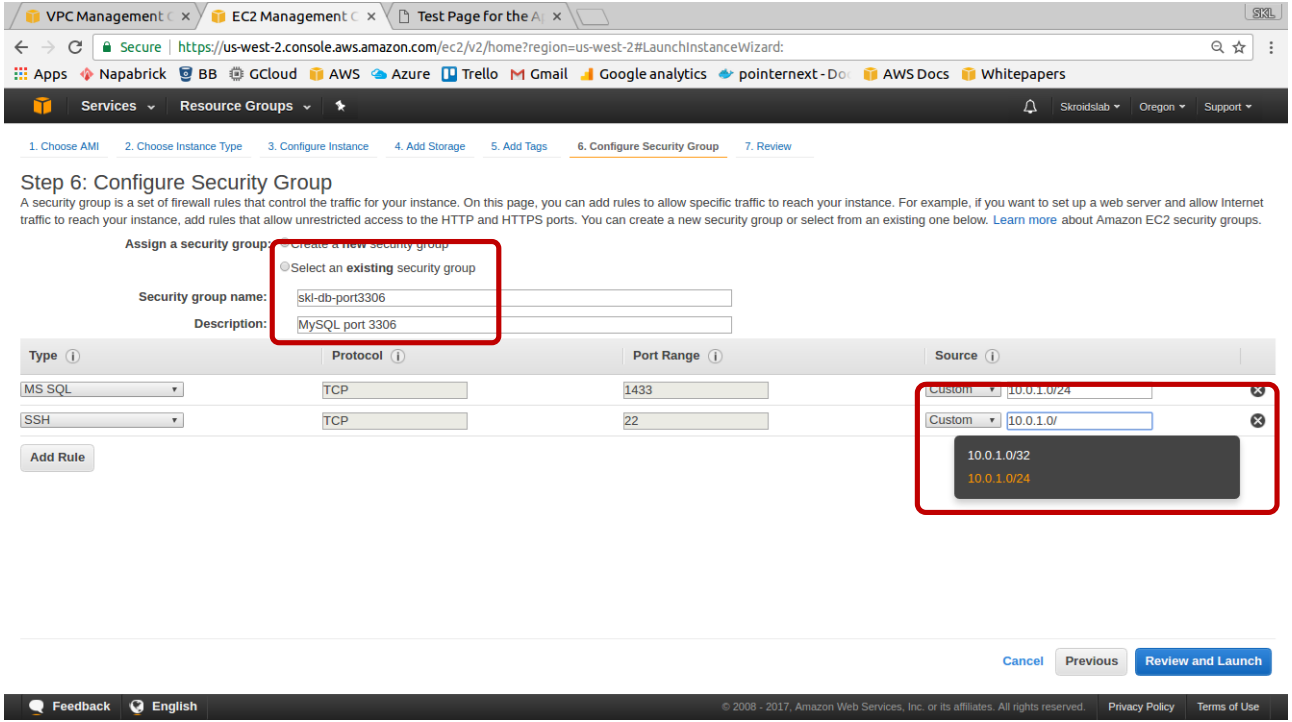
Activity - Test the IG+RT

greatlearning



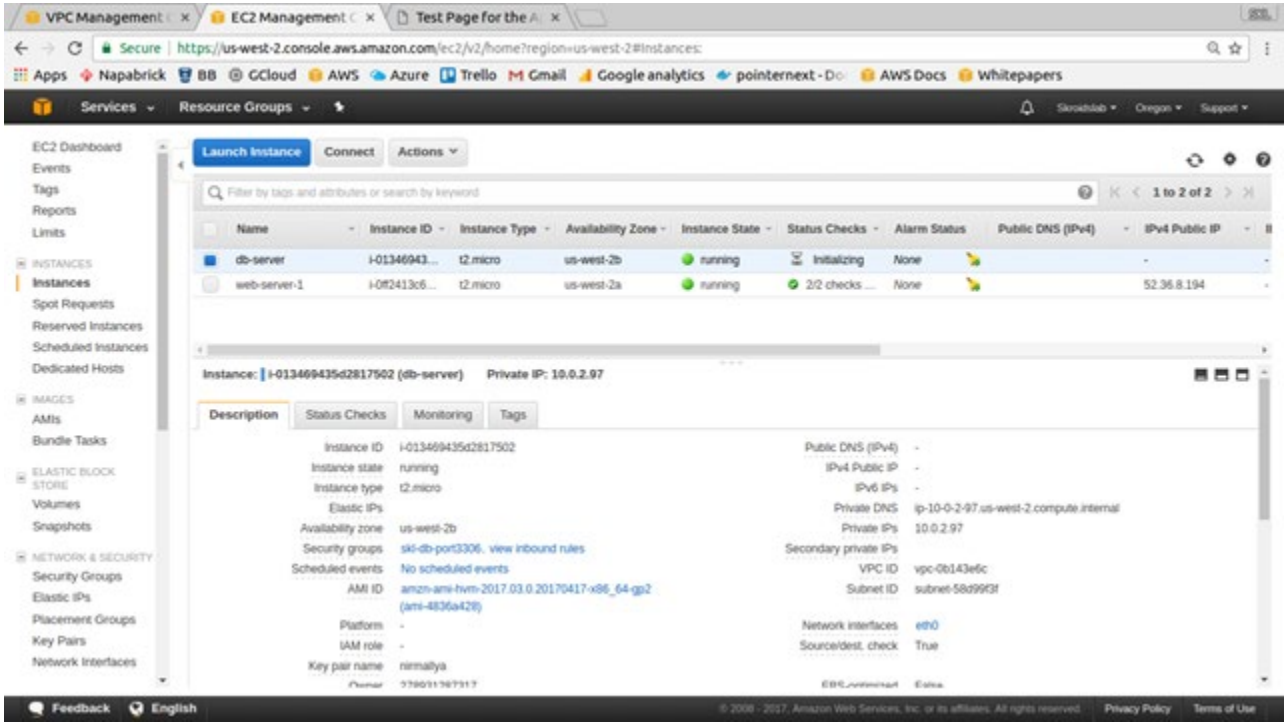
Remove the IG and refresh the page, add it back again.

Activity - Launch EC2 in subnet 2



Allow all subnet 1 instances to be able to SSH and connect to MySQL running on EC2 instance in subnet 2. Add v4 ICMP as well as a rule. Proceed to launch the instance. PEM as usual.

Activity - Launch EC2 in subnet 2



Notice no public IP address has been allocated

Activity - SSH to web server

```
nirmallya@aconite-ubuntu:/opt/Cloud/AWS/AWS-resources$ ssh ec2-user@52.36.8.194 -i nirmallya.pem
The authenticity of host '52.36.8.194 (52.36.8.194)' can't be established.
ECDSA key fingerprint is SHA256:gvZU6mqKj/yRUimasZxHwmmsDqiSCpAhIN0ISb+5euo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '52.36.8.194' (ECDSA) to the list of known hosts.

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2017.03-release-notes/
[ec2-user@ip-10-0-1-31 ~]$ sudo su
[root@ip-10-0-1-31 ec2-user]# ping 10.0.2.97
PING 10.0.2.97 (10.0.2.97) 56(84) bytes of data.
64 bytes from 10.0.2.97: icmp_seq=1 ttl=255 time=1.13 ms
64 bytes from 10.0.2.97: icmp_seq=2 ttl=255 time=0.993 ms
64 bytes from 10.0.2.97: icmp_seq=3 ttl=255 time=0.957 ms
64 bytes from 10.0.2.97: icmp_seq=4 ttl=255 time=1.00 ms
^C
— 10.0.2.97 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.957/1.022/1.138/0.079 ms
[root@ip-10-0-1-31 ec2-user]#
```

We are able to ping the instance in the private subnet 2

Activity - SSH from web server to db

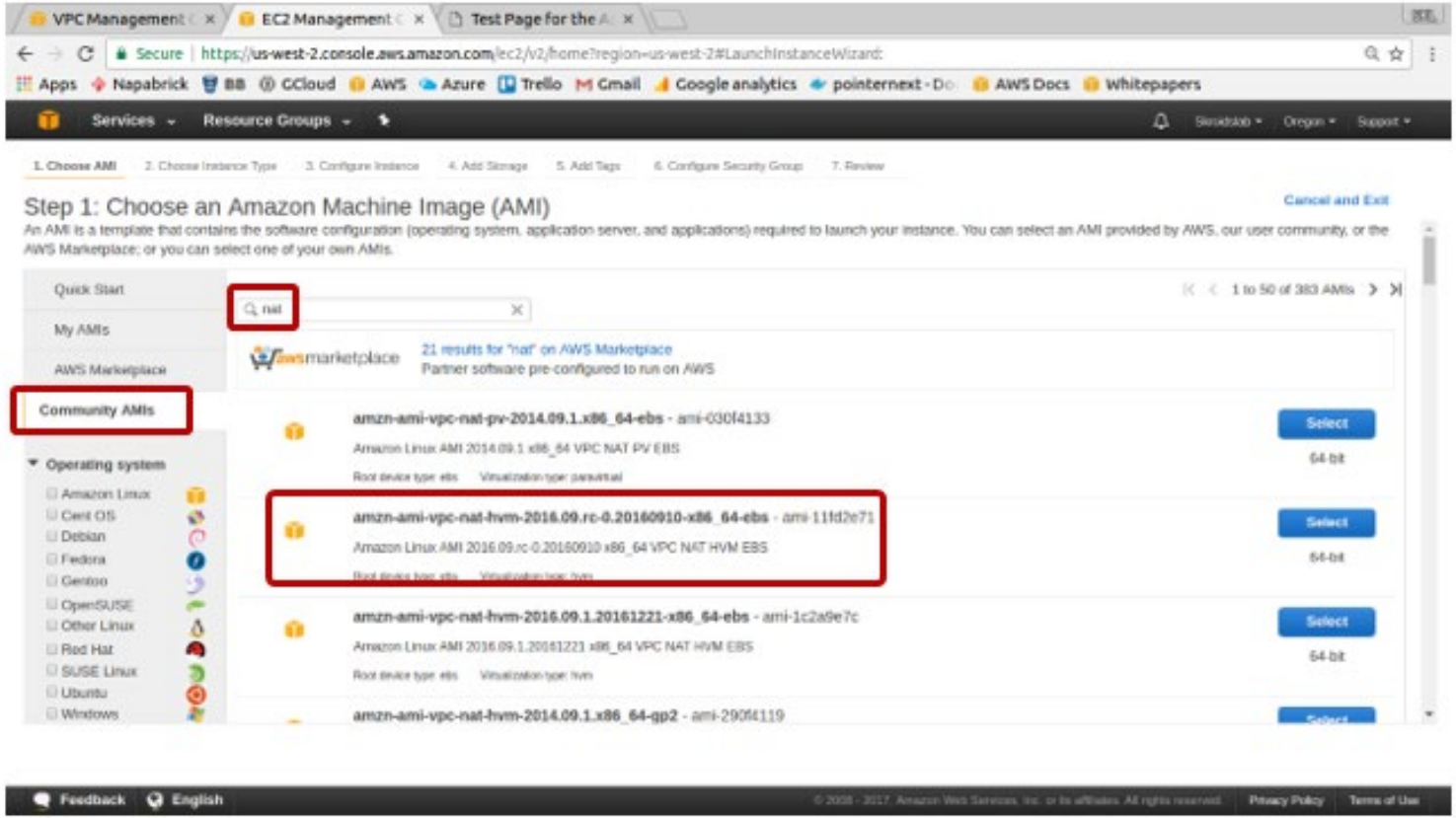
greatlearning

```
[root@ip-10-0-1-31 ec2-user]# nano nirmallya.pem
copy paste the pem contents from local machine to here; remove new lines that show up between the PEM contents
[root@ip-10-0-1-31 ec2-user]# chmod 400 nirmallya.pem
[root@ip-10-0-1-31 ec2-user]# ssh ec2-user@10.0.2.97 -i nirmallya.pem
The authenticity of host '10.0.2.97 (10.0.2.97)' can't be established.
ECDSA key fingerprint is eb:95:17:ae:2a:c6:8e:bc:77:78:b8:7e:ca:38:0b:6b.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.97' (ECDSA) to the list of known hosts.

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2017.03-release-notes/
[ec2-user@ip-10-0-2-97 ~]$ sudo su
[ec2-user@ip-10-0-2-97 ~]# yum update -y
```

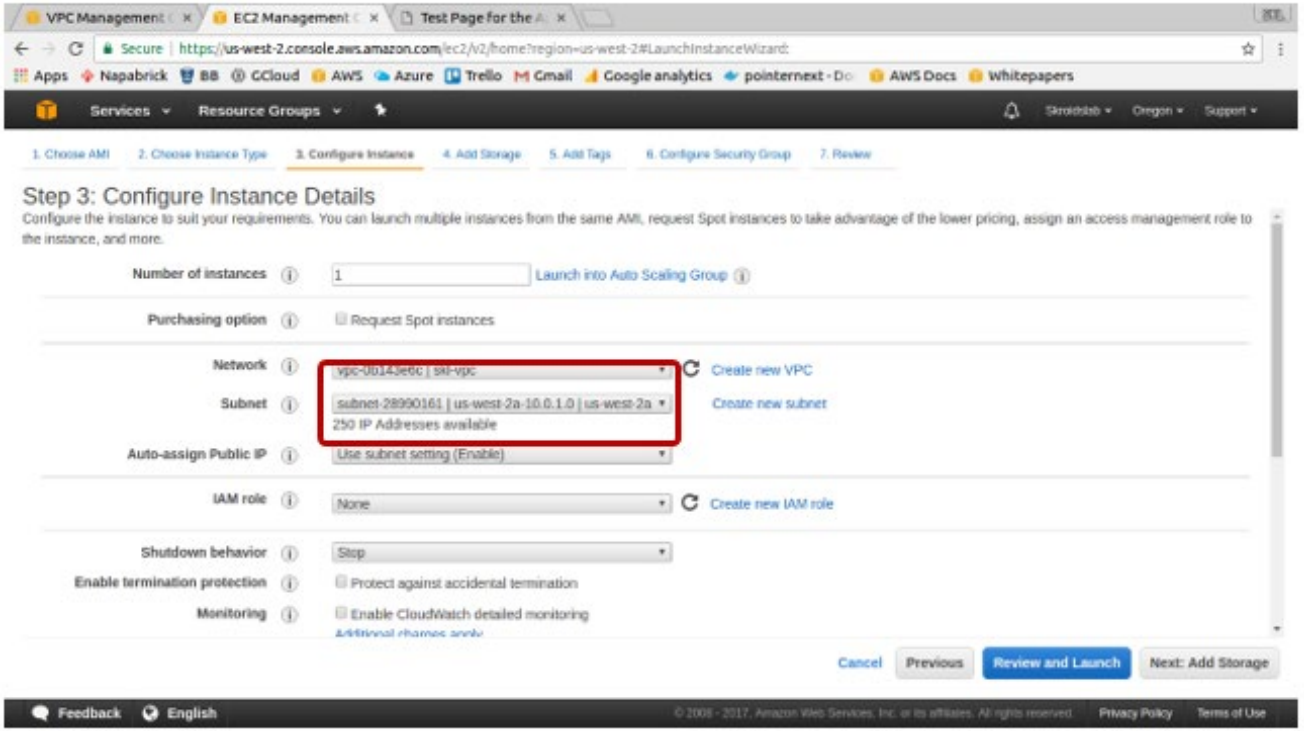
Nothing happens because there is no internet access!!
We need NAT ... keep this terminal window open

Activity - NAT instance

greatlearning



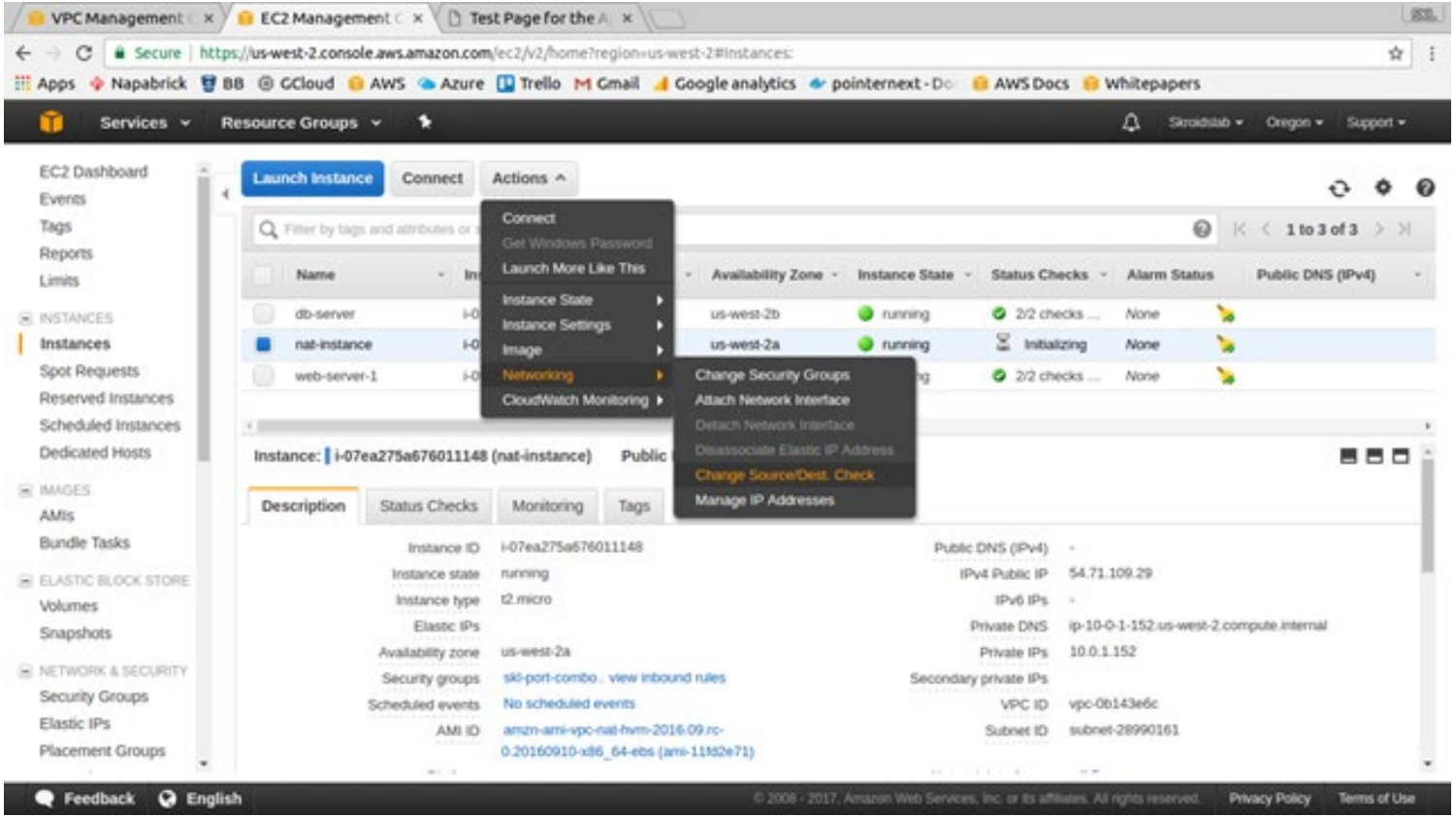
Activity - NAT instance



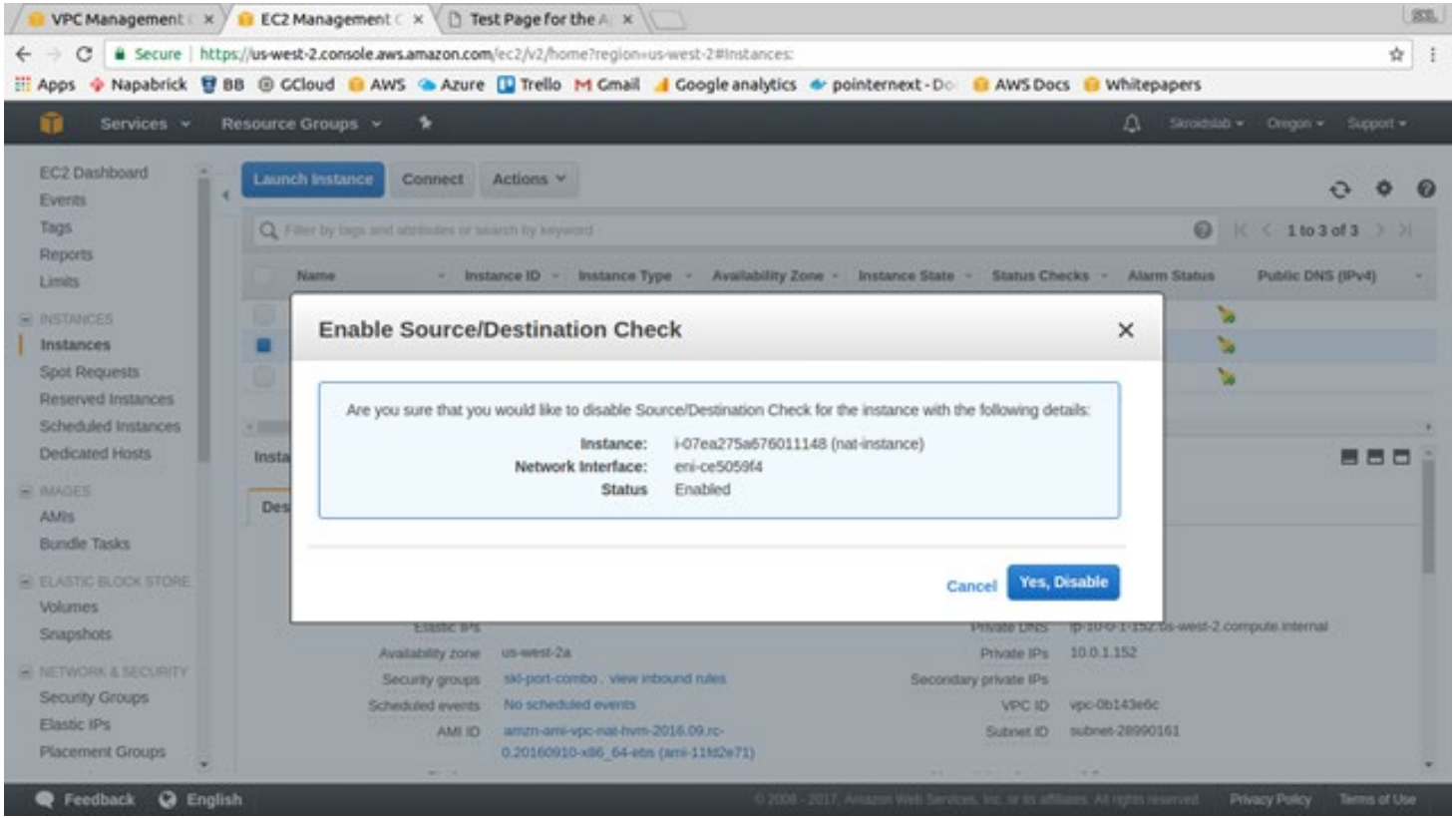
Later, choose the security group of PORT 22 + 80

Activity - NAT instance

greatlearning

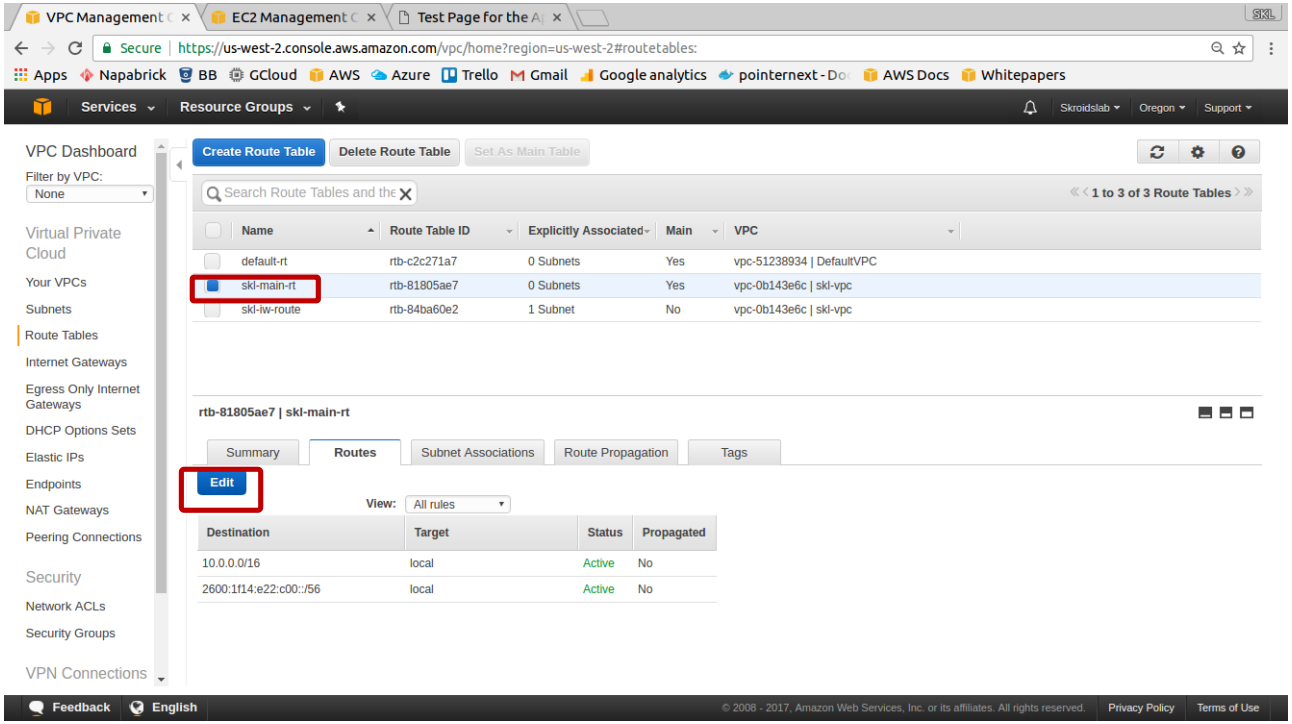


Activity - NAT instance



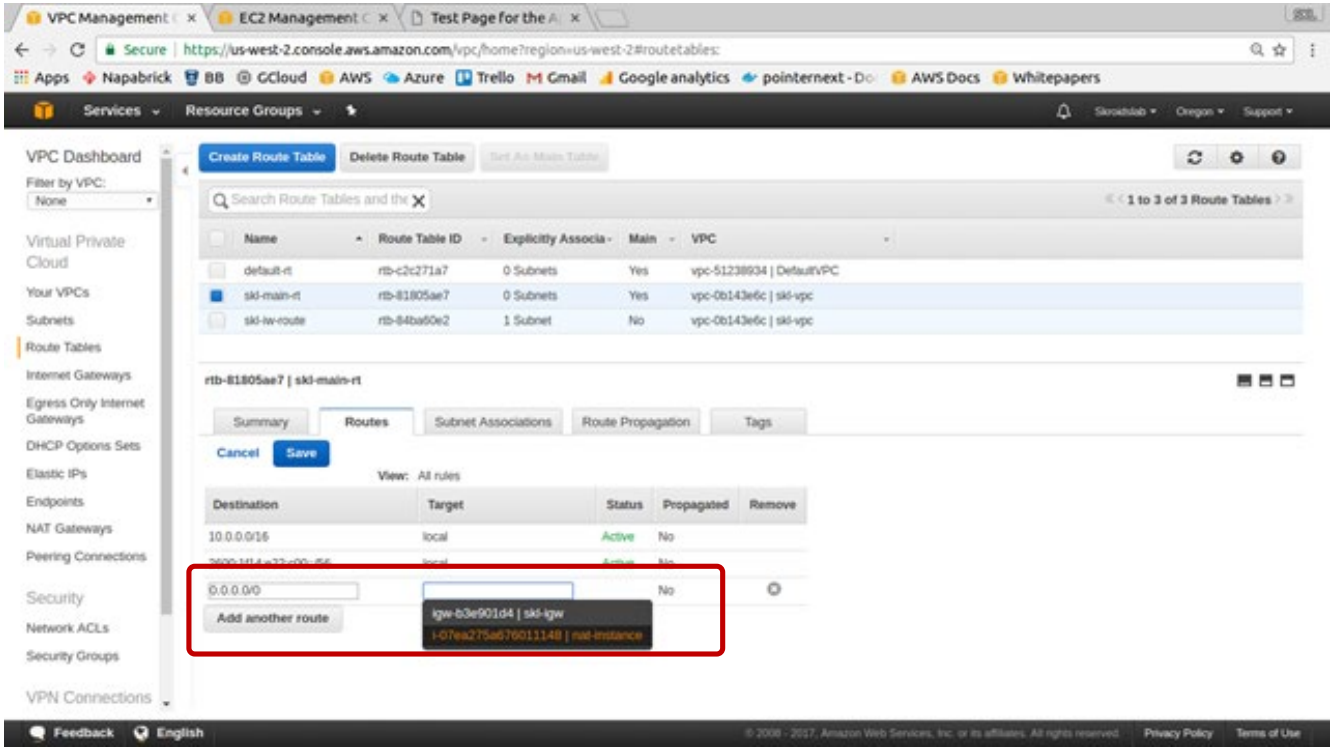
Activity - NAT instance association with VPC main RT

greatlearning



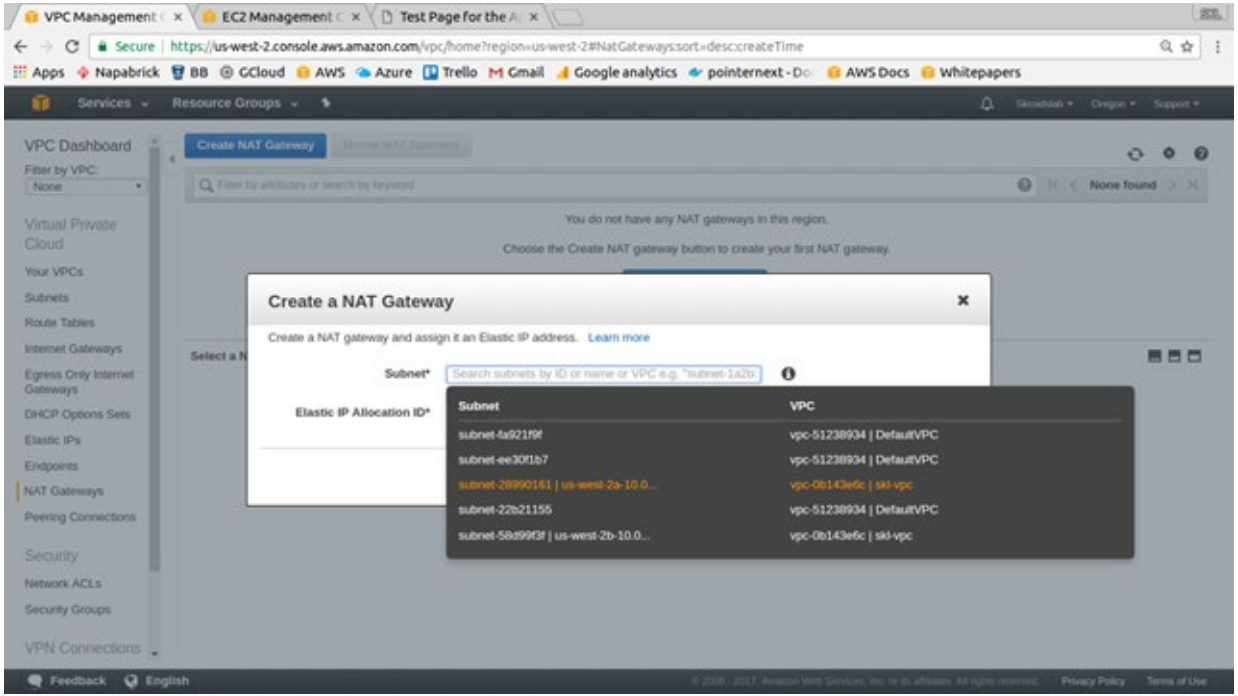
Activity - NAT instance association with VPC main RT

greatlearning



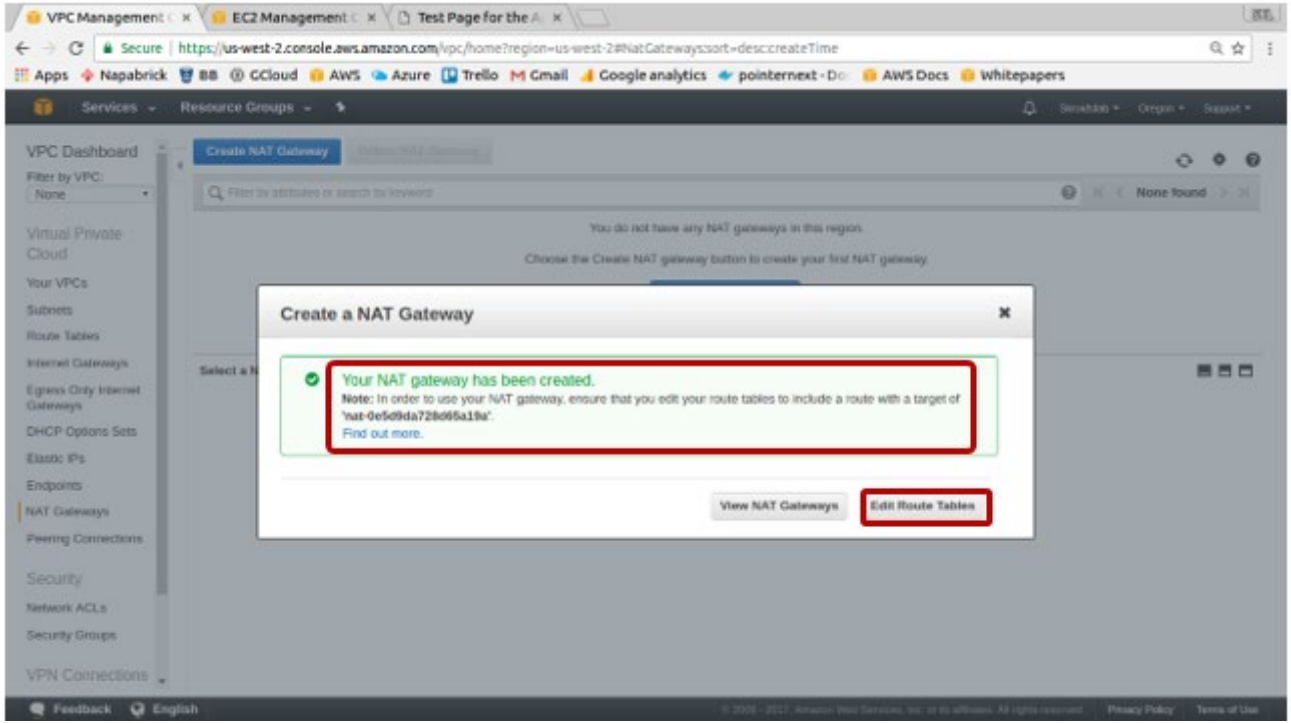
Go to the terminal window of db (that is already open) and try
 # yum install mysql -y

Activity - NAT Gateway



Allocate the elastic IP as well.

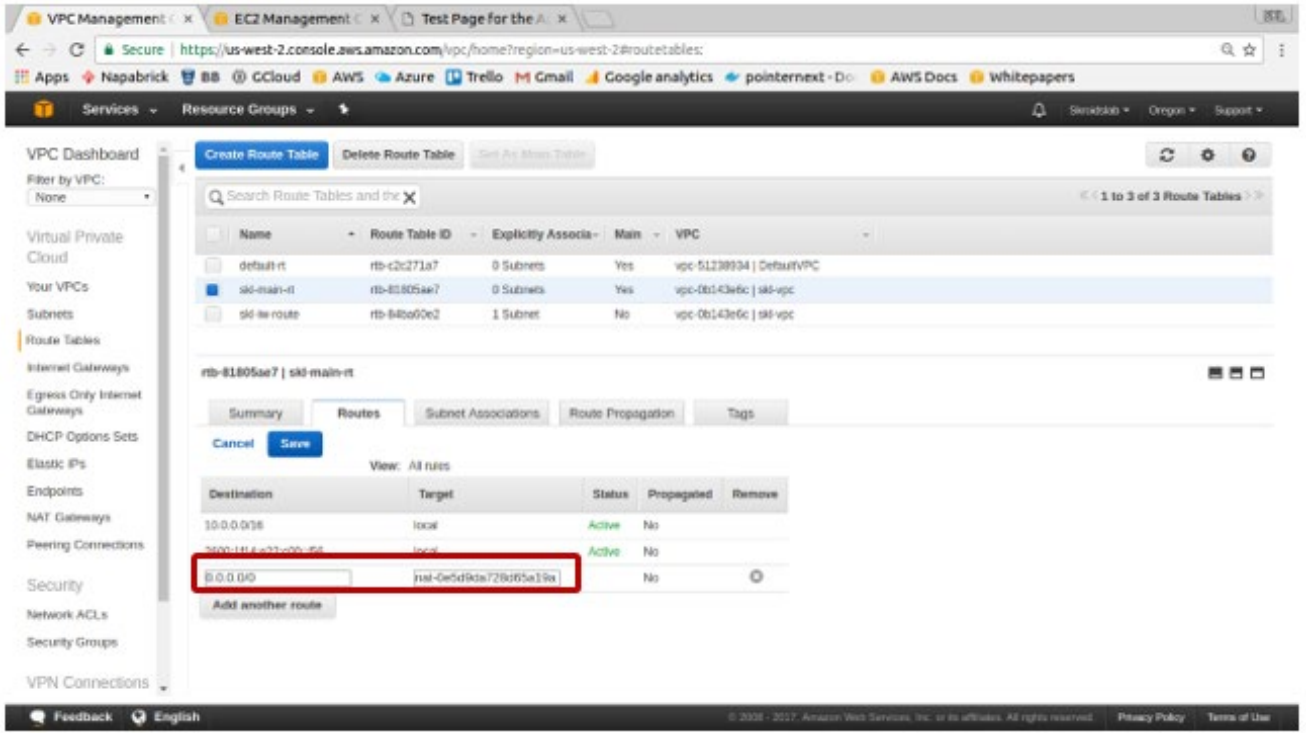
Activity - NAT Gateway



No need to put the NAT gateway behind the SG, no EC2 instance, will autoscale etc.

Activity - NAT Gateway association with VPC main RT

greatlearning

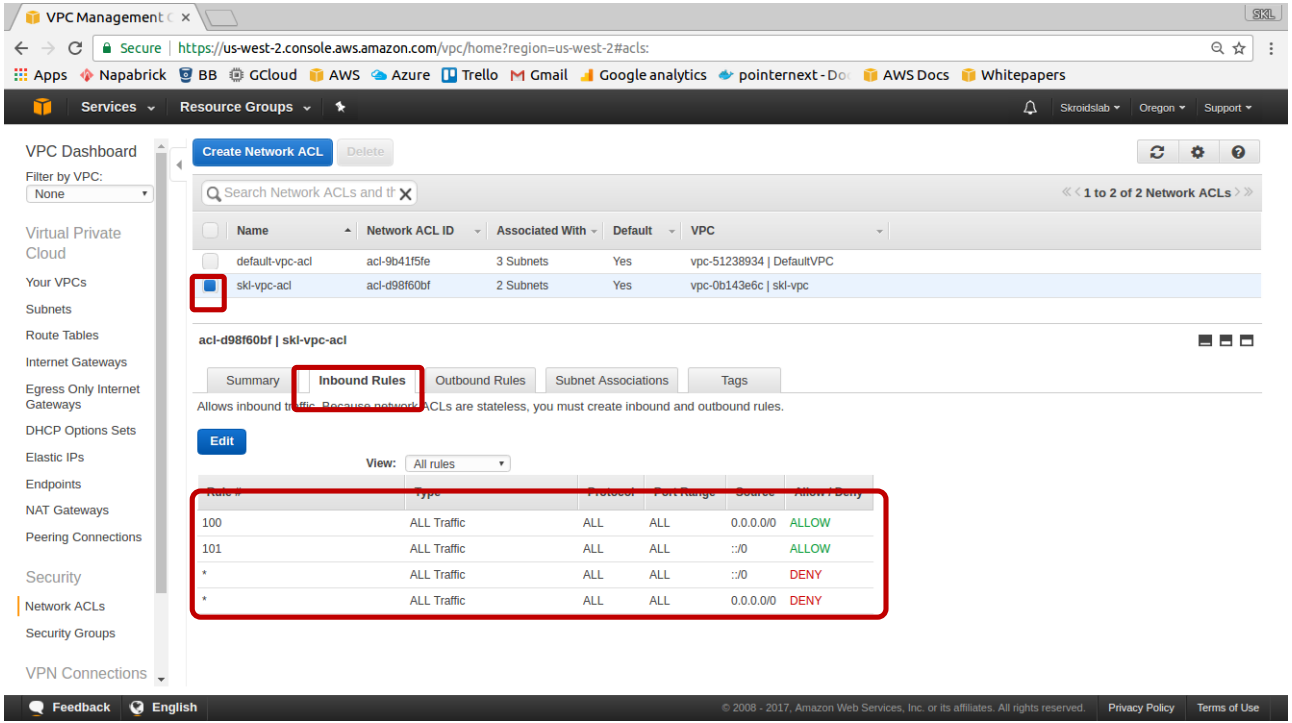


Go back to the terminal window of DB and execute

 # yum update -y

Activity - ACL

greatlearning

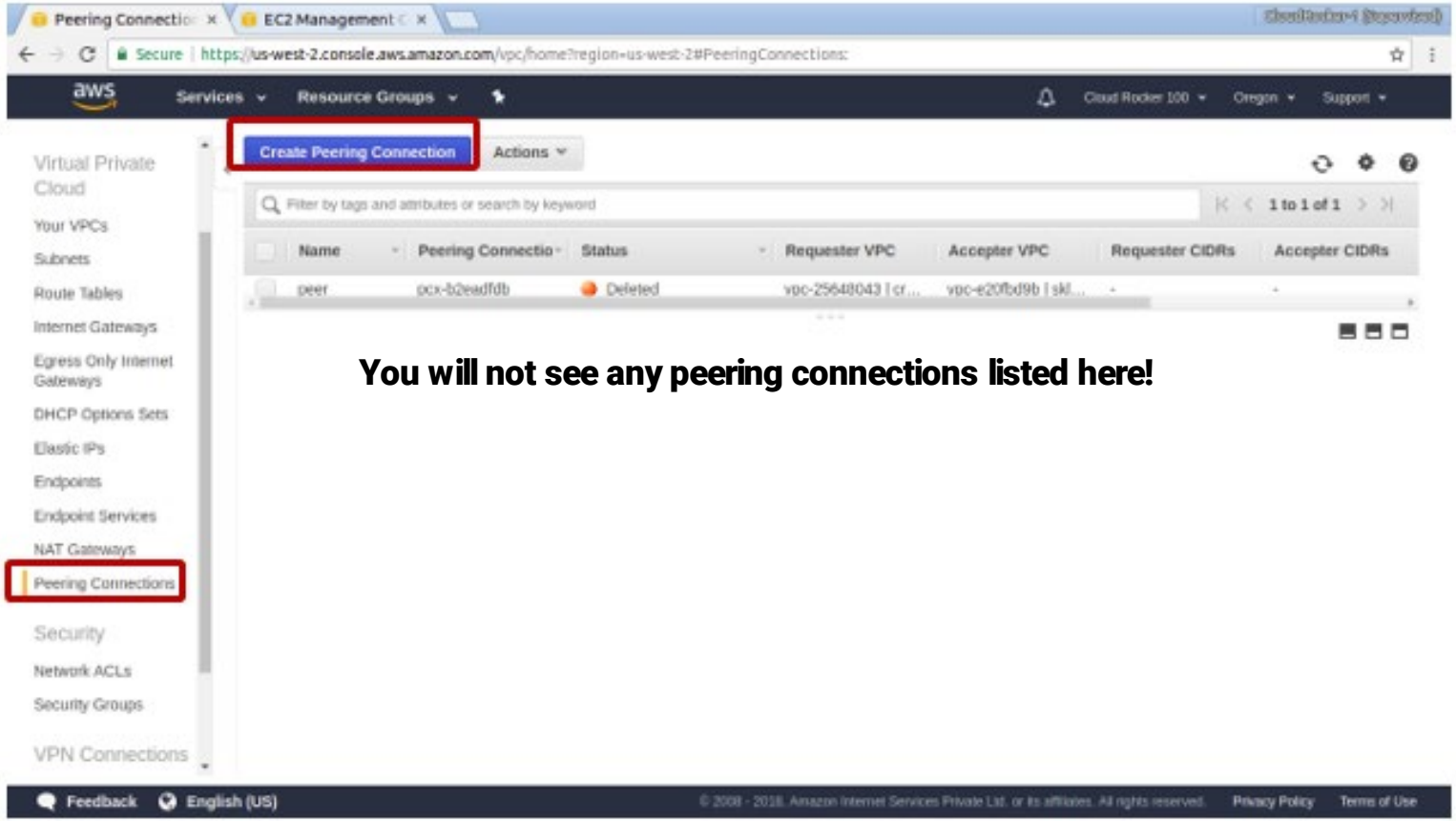


Name the ACLs for better readability
The rule # * means it will match if no other rule matches.
Lower rule numbers take effect

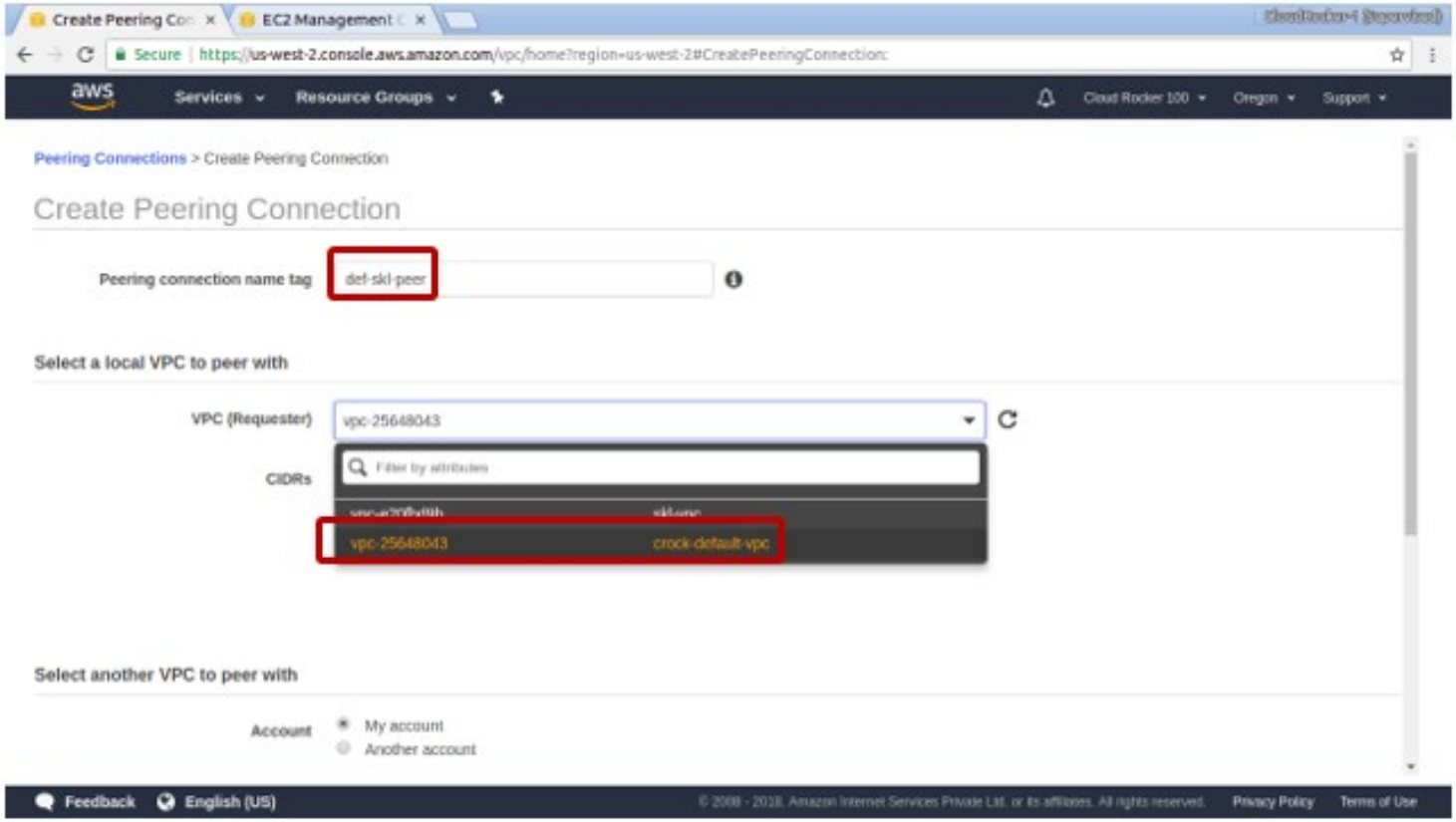
Activity - Peering

- Ensure we have 2 VPCs - default and the custom
- Launch 2 EC2 instances, 1 in each VPC
- Open the following ports
  - Default VPC - Port 22 and all V4 ICMP
  - Custom VPC - Port all V4 ICMP
- SSH to the EC2 instance that is in the default VPC
- Ping the EC2 instance that is in the custom VPC and there will be no response
- Now let's setup peering

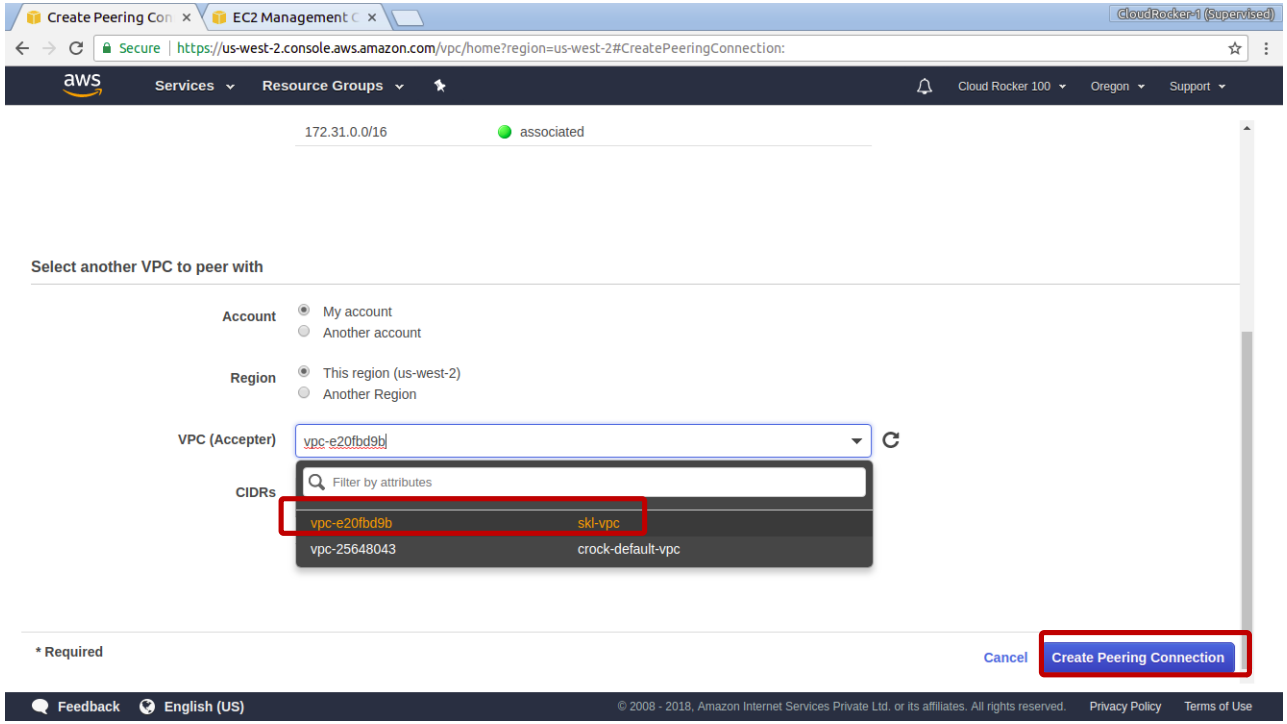
Activity - Peering



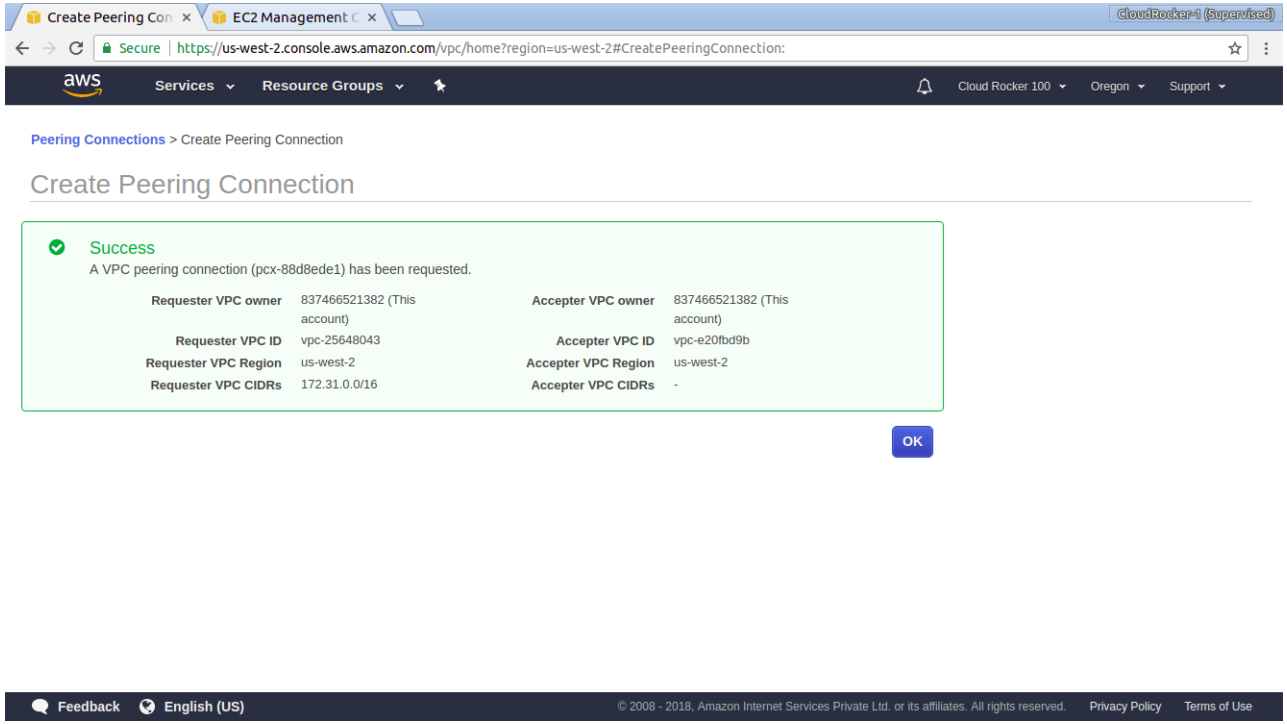
Activity - Peering



Activity - Peering

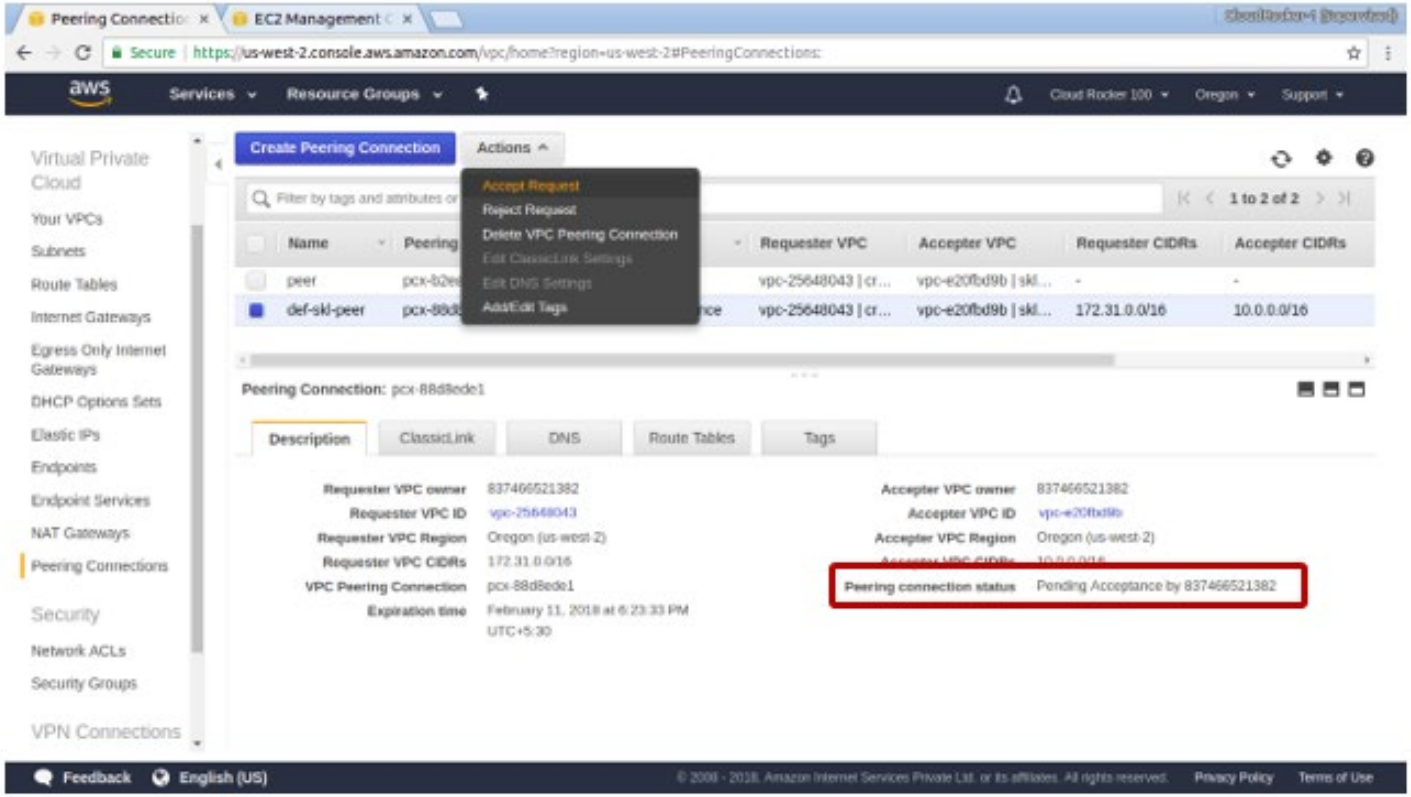


Activity - Peering

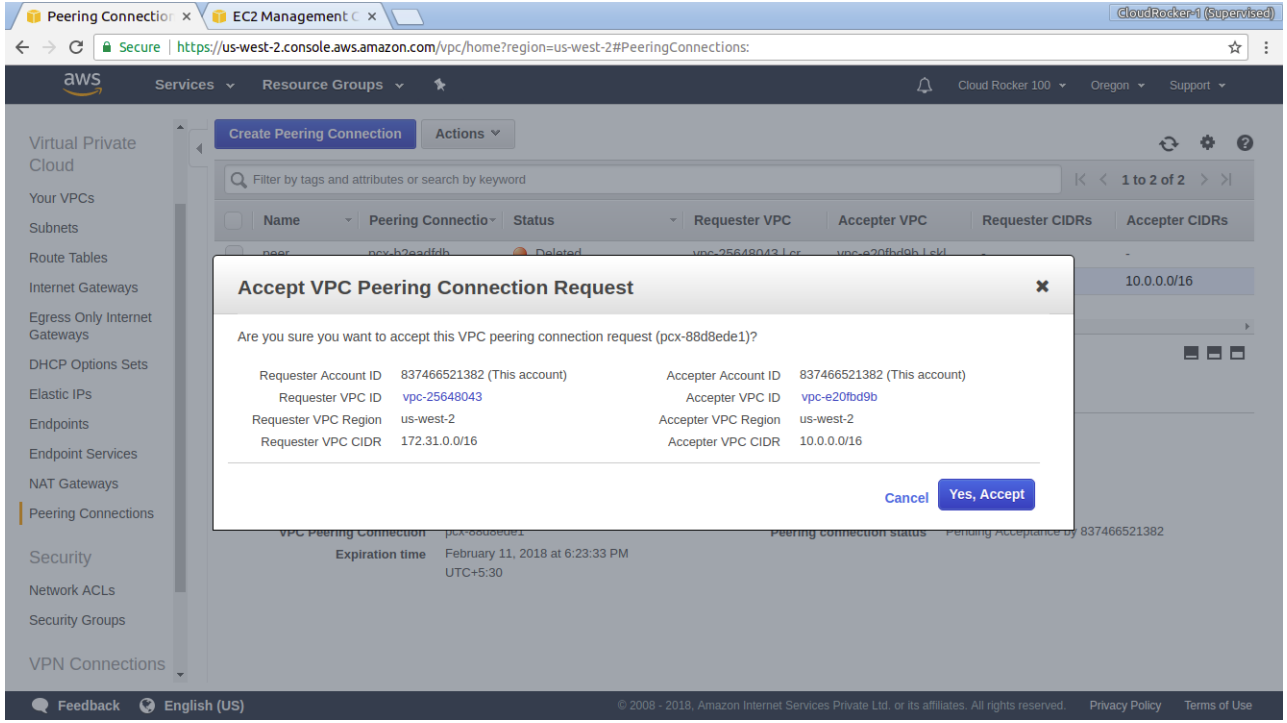


Activity - Peering

greatlearning

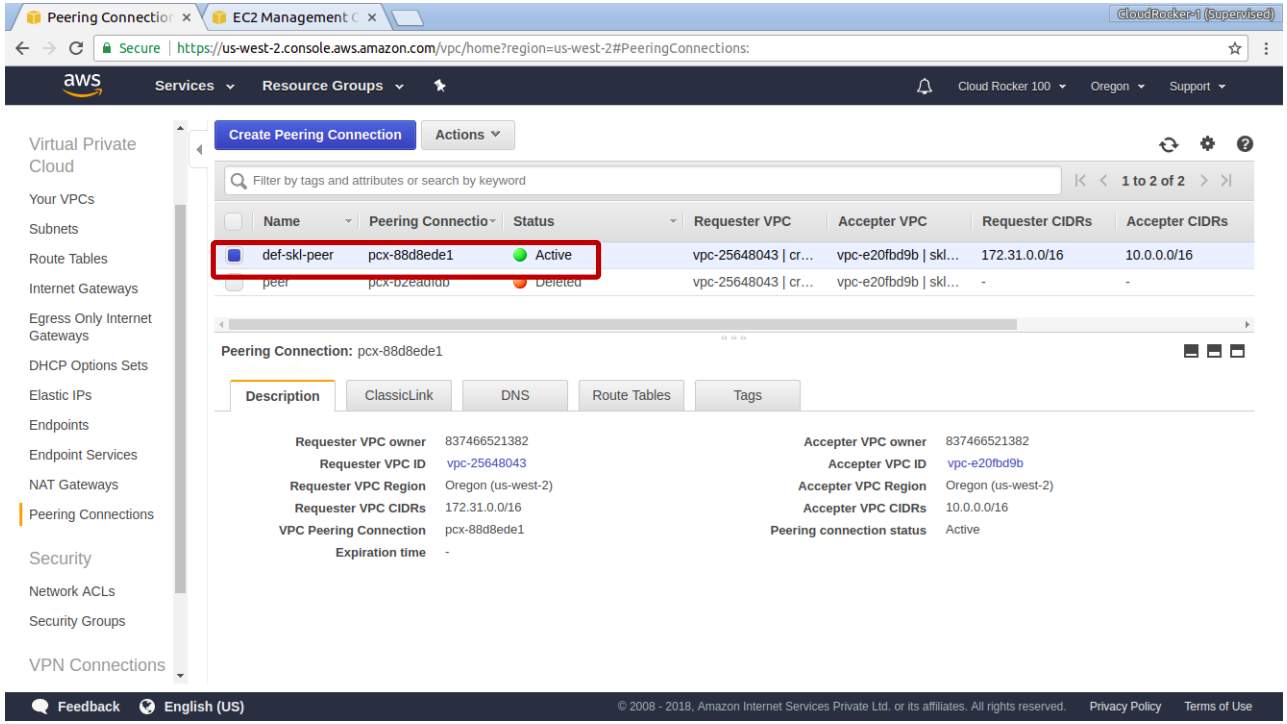


Activity - Peering



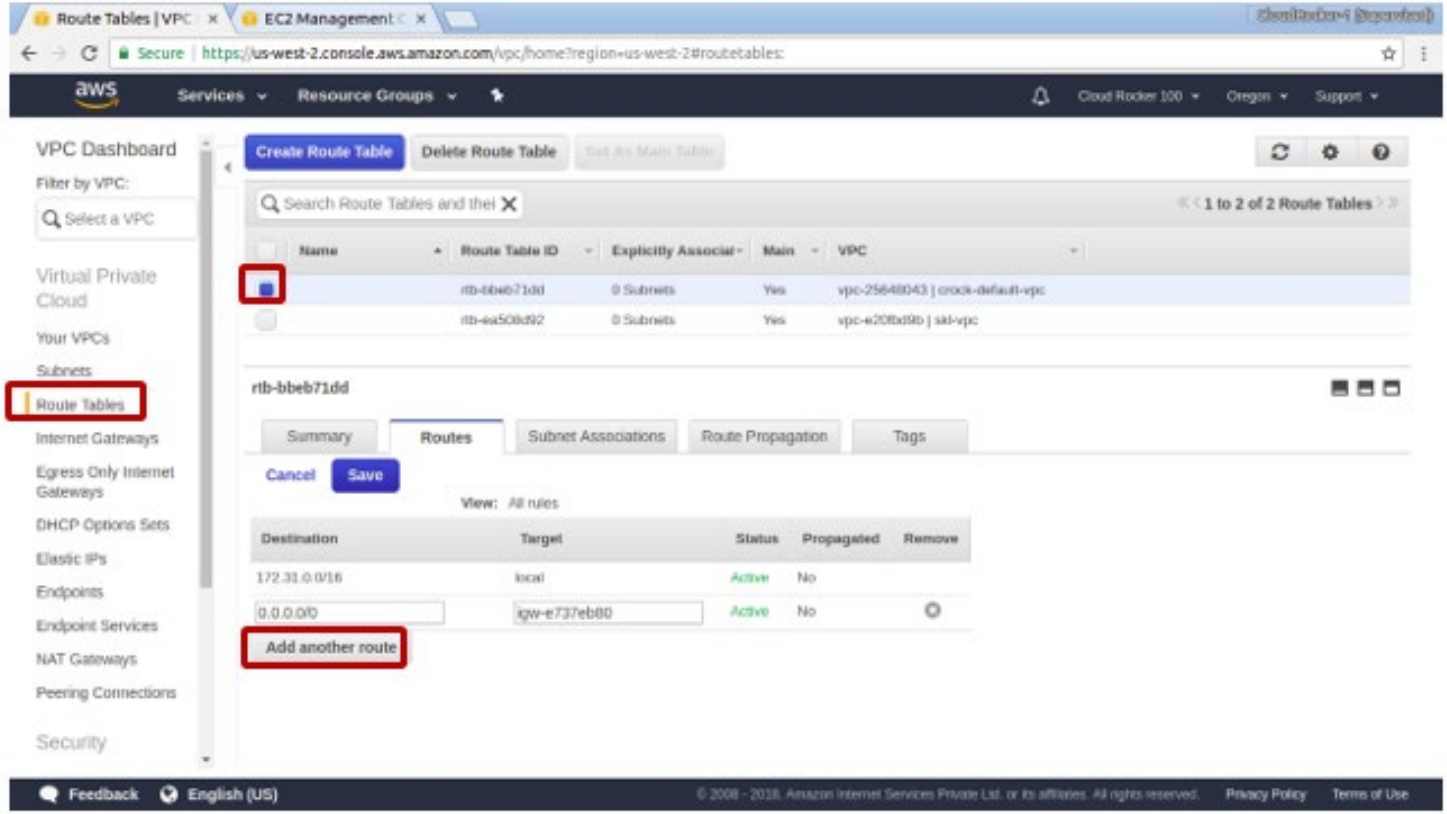
Activity - Peering

greatlearning

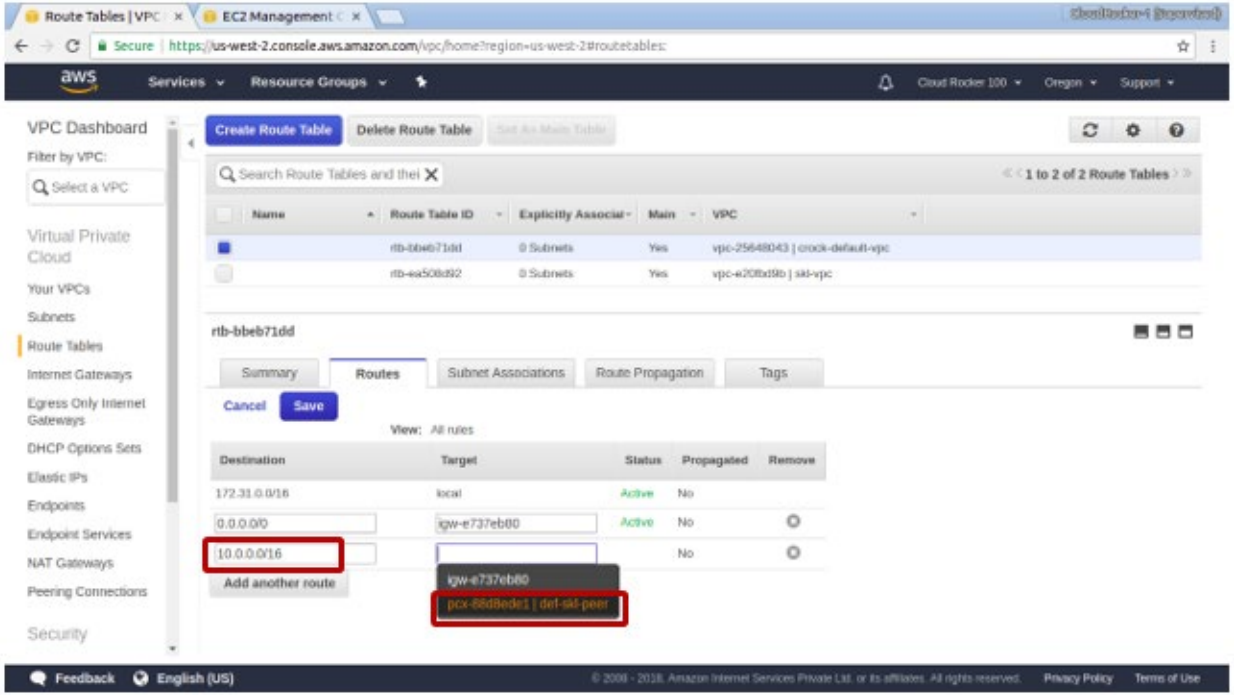


Activity - Peering

greatlearning

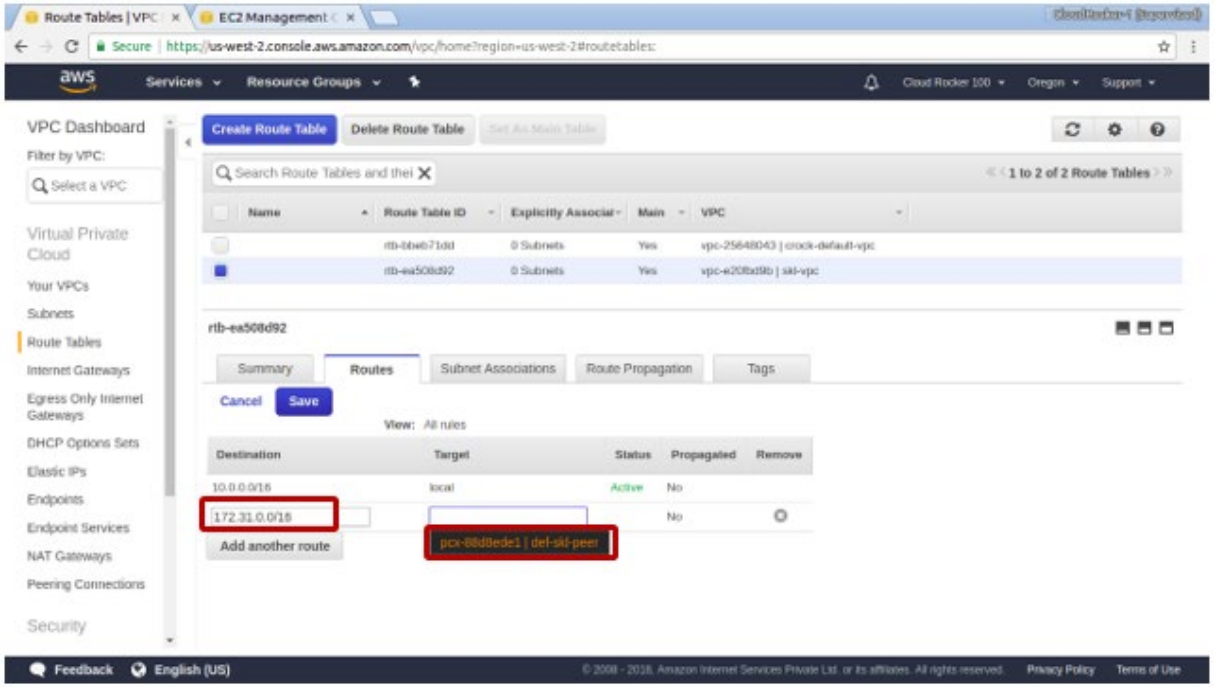


Activity - Peering



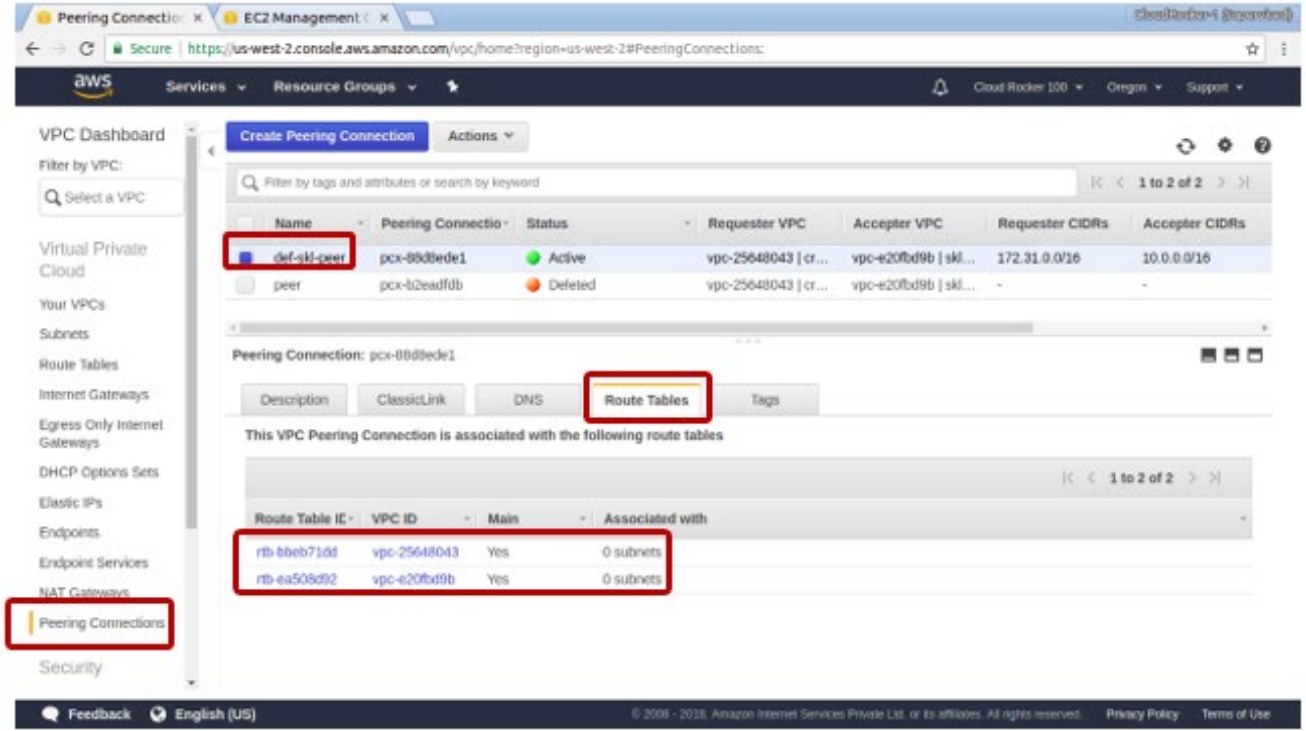
Select "route tables" and select the default VPC main RT and a route for the whole CIDR of the custom VPC, Click SAVE!

Activity - Peering



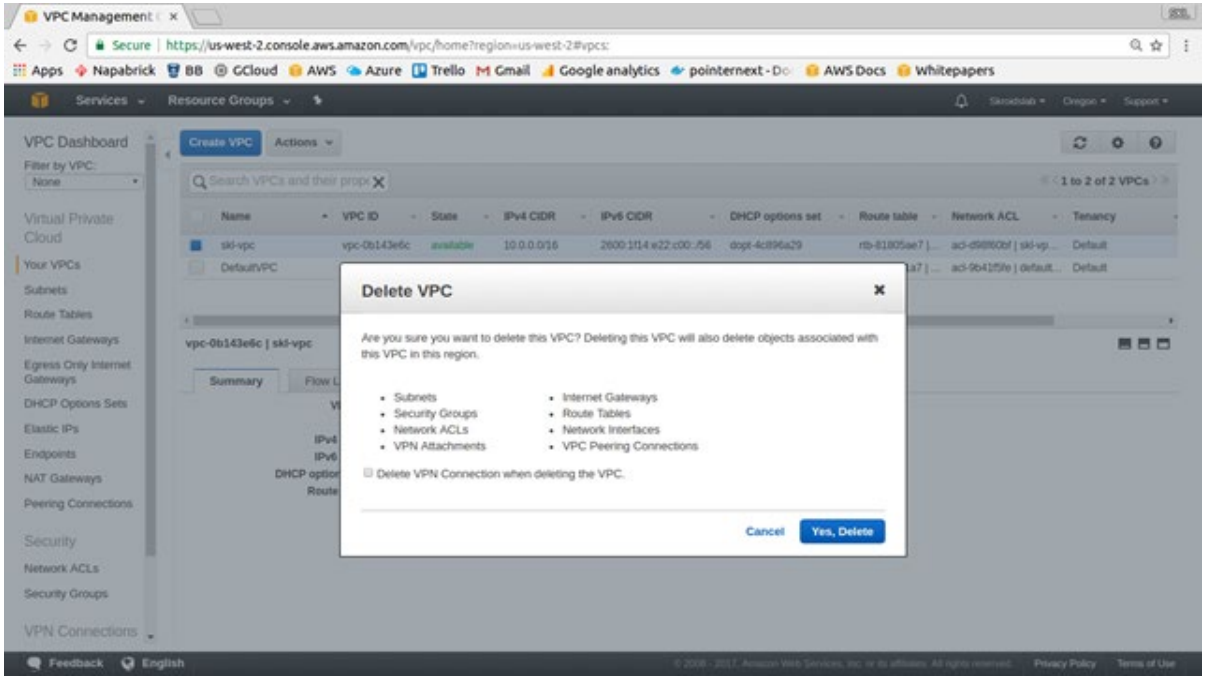
Now select the custom VPC main RT and a route for the whole CIDR of the default VPC, Click SAVE!

Activity - Peering



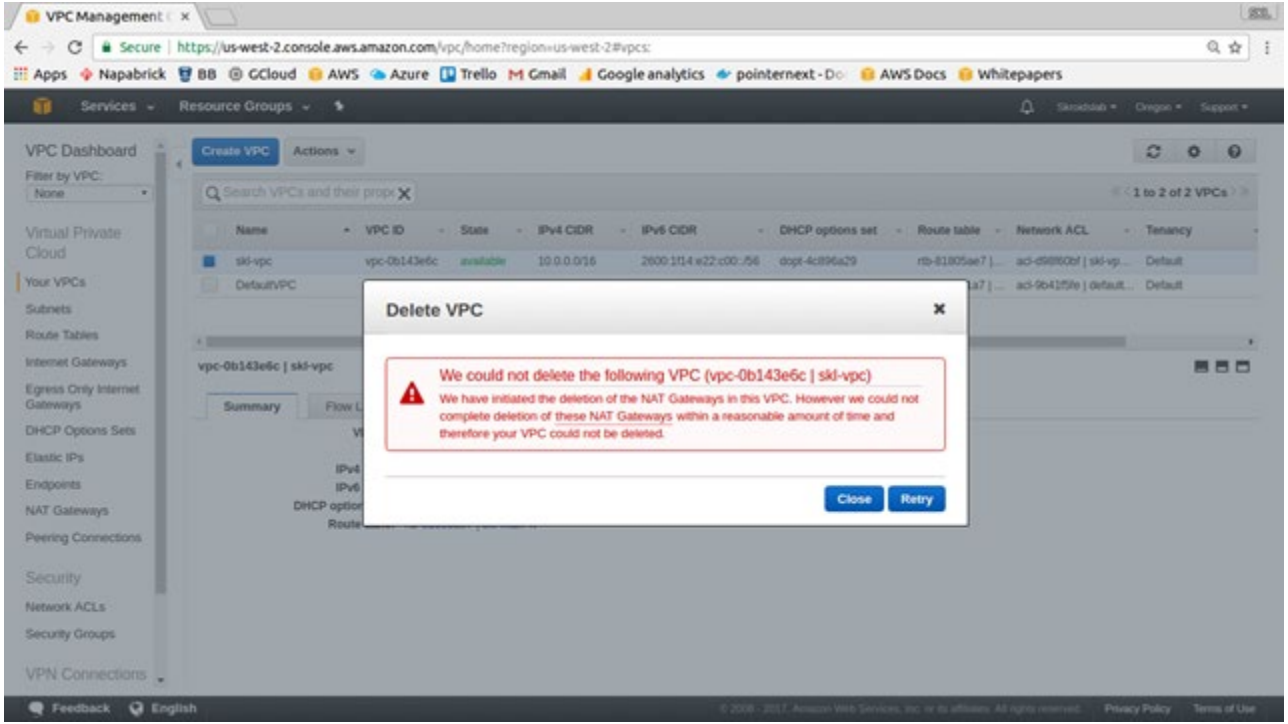
Verify that both VPCs have the RT updated with each other's CIDR blocks. Now go back to the terminal window and ping the EC2 instance in the custom VPC from the default VPC and ping will respond back!

Activity - Cleanup



Ensure the EC2 instances are deleted first!

Activity - Cleanup



Give it some time!

greatlearning

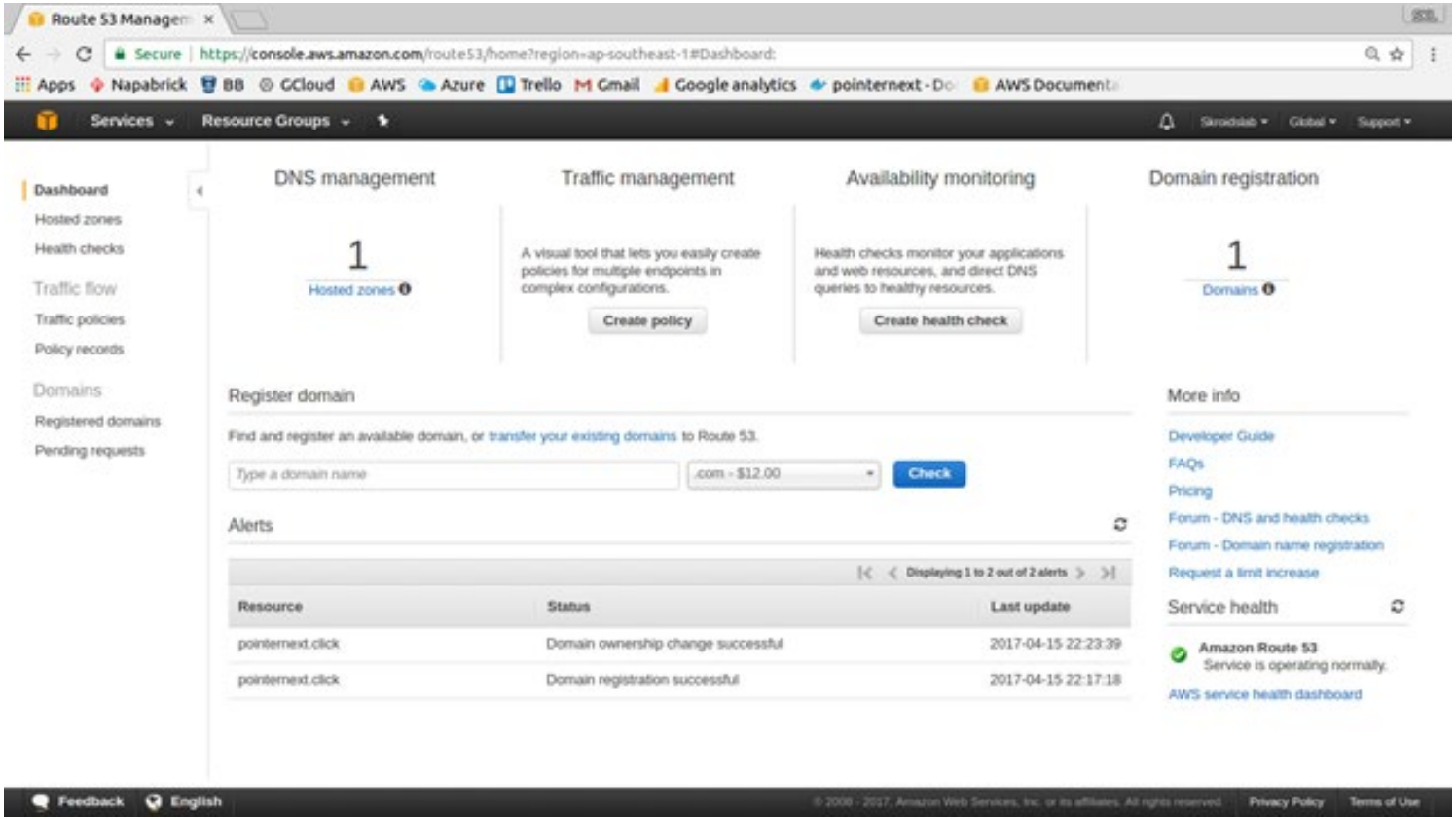
Networking

Route 53

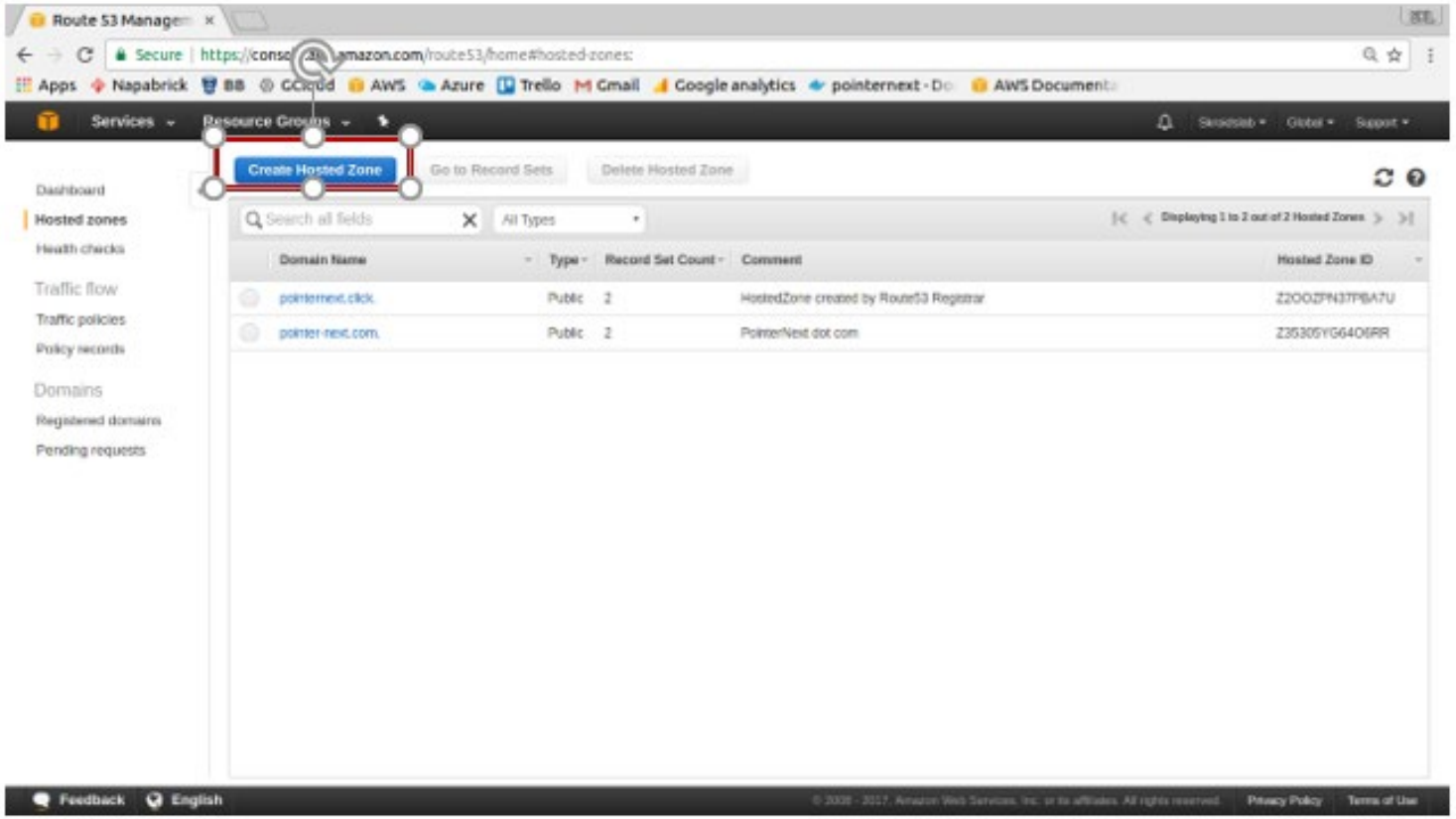
Route 53 - DNS service

- Basically an IP to domain resolution and is a "Global" service and not specific to a region
- DNS port is on 53, hence the name Route 53
- Top level domain names
- No free tier, $0.50/month/hosted zone
- There is a limit to the number of domains you can manage but it can be raised by contacting AWS support
- NS (Name Server) records
  - Used by top level domain servers to direct traffic to content DNS server which contains the DNS records
- A records
  - IP address to the domain name translation
- TTL
  - How long a DNS record is cached in local PC
- C NAME
  - Canonical Name to resolve one domain to another
  - Individual resources cannot be mapped
  - Chargeable for the resolution service per call
- Alias records (Route 53 specific)
  - Preferred choice over cname
  - Resource record mapping to ELB, CloudFront, S3 buckets with websites
  - No charge

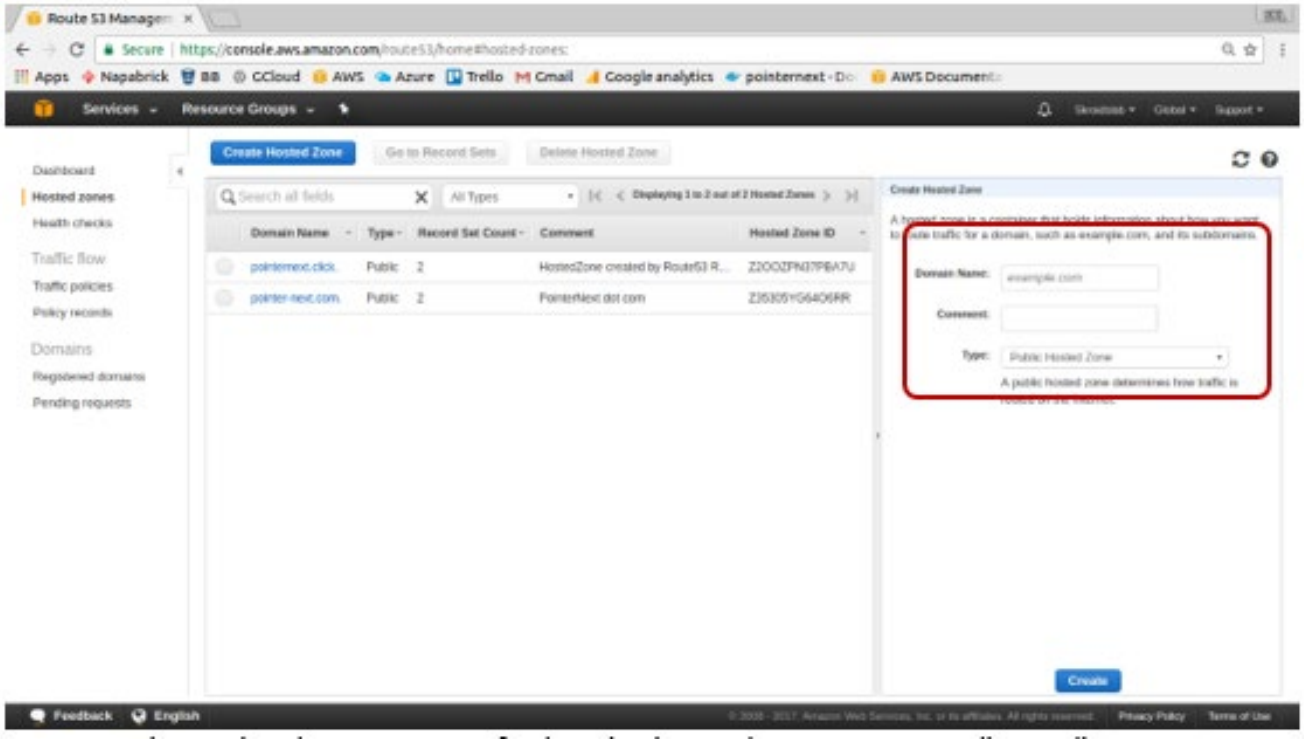
Route 53 dashboard



Route 53 Hosted zones

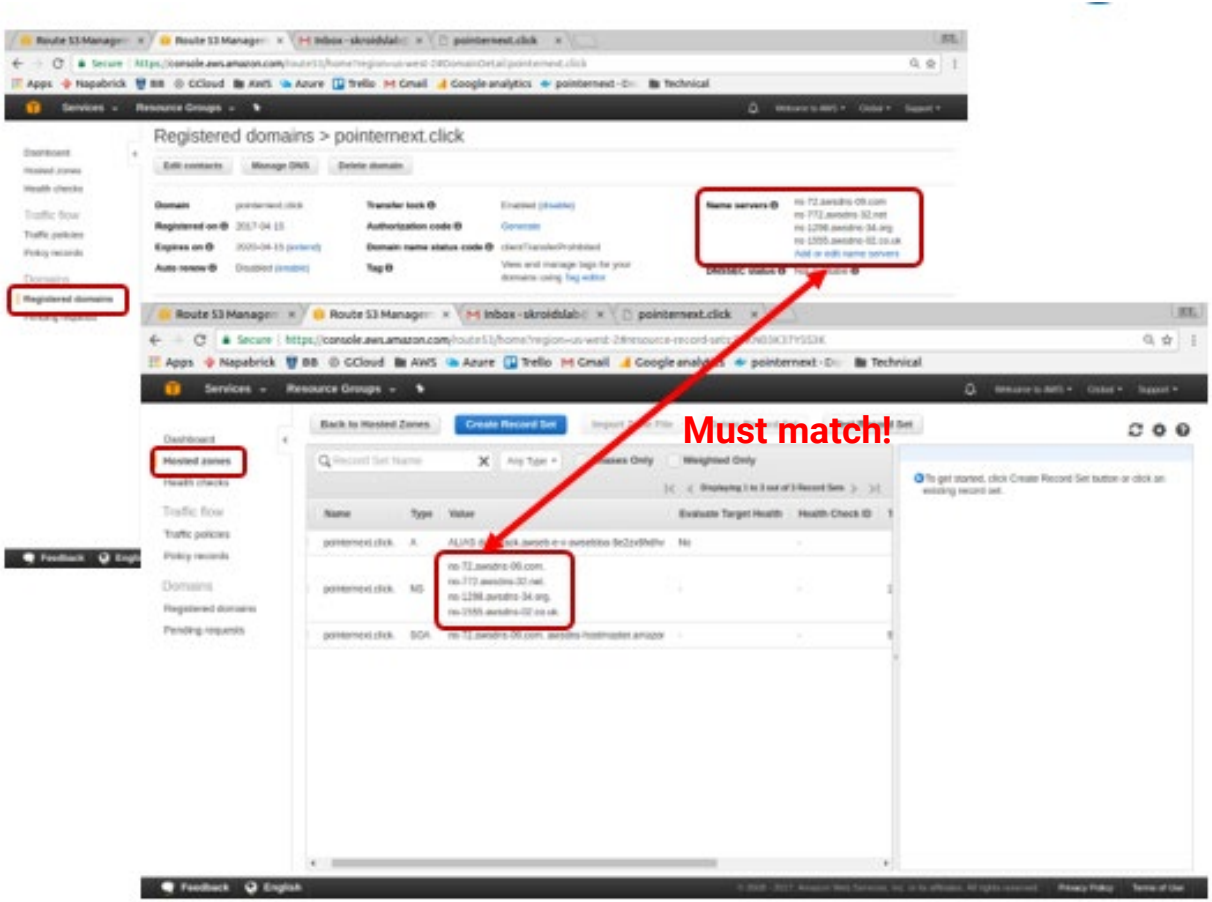


Route 53 Hosted zones



We now have the domains specified in the hosted zones, time to "route" traffic via these domains!

Route 53 NS settings

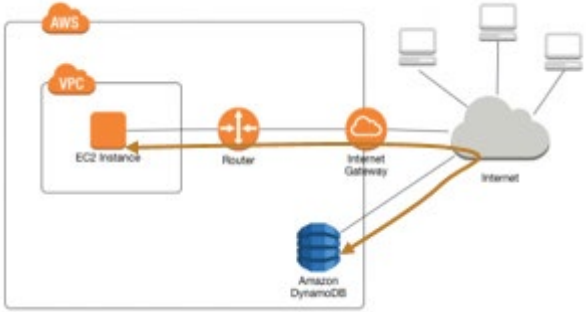


Activity - Route 53 Routing

greatlearning

- Various routing logic can be chosen from depending on the need
- Simple
  - Default and used when we have a single resource, e.g. 1 web server
  - No real intelligence in this routing
- Weighted
  - Split traffic to two different resources based on weights
- Latency
  - Send traffic based on lowest latency for the end user
- Failover
  - DC/DR setup, monitors health and then redirects traffic
- Geolocation
  - Route traffic from the region closest to your users

Activity - VPC Endpoints



Old approach

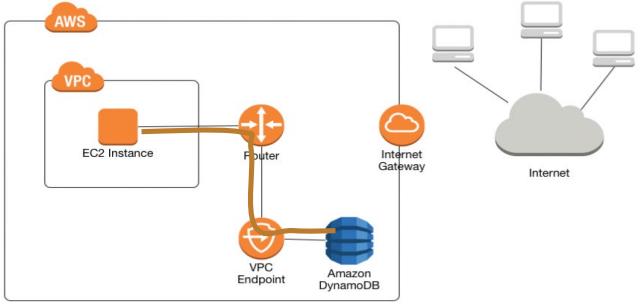
If you wanted your EC2 instances in your VPC to be able to access DynamoDB, you had two options.

1. You could use an Internet Gateway (with a NAT Gateway or assigning your instances public IPs)

2. You could route all of your traffic to your local infrastructure via VPN or AWS Direct Connect and then back to DynamoDB

New approach

Now we can grab one of the custom VPCs and provision an endpoint using either the console or the CLI. The process remains the same as that of S3



https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html