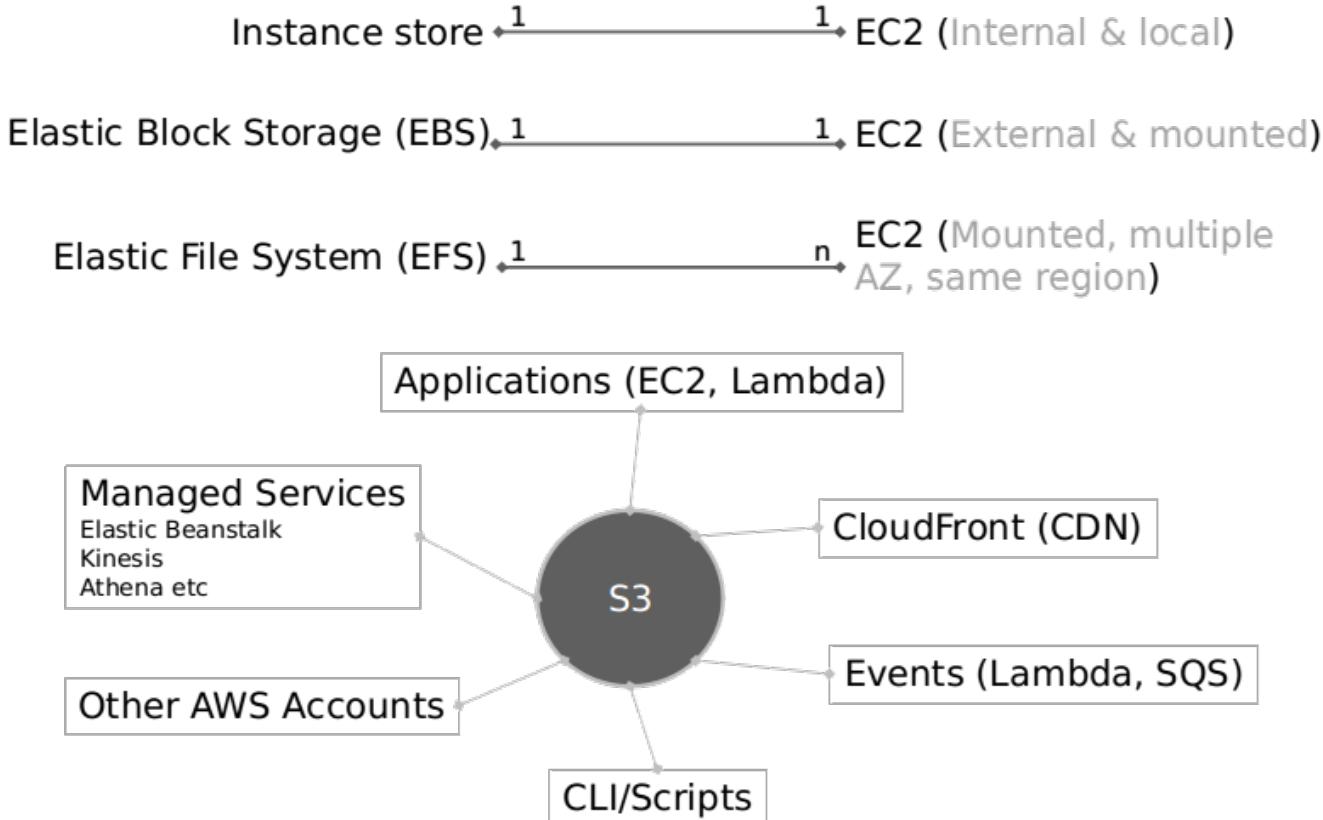


Storage and Content Delivery

Volume > Snapshot > Volume

Storage overview



Activity - Volumes

The screenshot shows the AWS EC2 Management Console with the 'Create Volume' interface open. On the left, the navigation menu is visible, showing options like EC2 Dashboard, Instances, Images, and Elastic Block Store (with 'Volumes' selected). The main area displays a table of volumes, with two entries shown:

Name	Volume ID	Size	Type	IOPS	Snapshot	Created	Availability Zone	State
Instance1-OS	vol-29b210de	8 GiB	gp2	24 / 3000	snap-ad8e61f8	December 13, 2015...	us-west-2b	in-use
Instance2-OS	vol-e7582401	8 GiB	standard	-	snap-ad8e61f8	December 13, 2015...	us-west-2c	in-use

Below the table, a specific volume is selected: "Volumes: vol-29b210de (Instance1-OS)". The details for this volume are displayed in a card:

Description	Status Checks	Monitoring	Tags
Volume ID: vol-29b210de	Size: 8 GiB	Created: December 13, 2015 at 5:12:44 PM UTC-5:30	Alarm status: None
State: in-use	Snapshot: snap-ad8e61f8	Availability Zone: us-west-2b	Encrypted: Not Encrypted
Attachment information: i-48072c8c (Http Server1) (/dev/xvda)	KMS Key ID: [redacted]	KMS Key Aliases: [redacted]	
Volume type: gp2	Product codes: -	KMS Key ARN: [redacted]	
IOPS: 24 / 3000			

At the bottom of the page, there are links for Feedback, English, and footer information: © 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use.

Activity - Volumes

The screenshot shows the AWS EC2 Management console interface. The left sidebar has a tree view with categories like EC2 Dashboard, Instances, Images, Volumes, and Network & Security. Under Volumes, 'Volumes' is selected. The main content area has a title 'Create Volume' and a table of volumes. One volume, 'web-server-1', is selected and highlighted in blue. The table columns include Name, Volume ID, Size, Volume Type, IOPS, Snapshot, Created, Availability Zone, State, Alarm Status, and Attachment Information. The selected volume's details are shown below the table: Name: web-server-1, Volume ID: vol-0f5e68cf9d632e76, Size: 8 GiB, Volume Type: standard, IOPS: -, Snapshot: snap-066b501..., Created: April 12, 2017 at 5:14:40 PM UTC+5:30, Availability Zone: us-west-2c, State: In-use, Alarm Status: None, Attachment Information: i-0749a28555320db7 (web-server-1):/dev/xvda (attached). Below the table, there are tabs for Description, Status Checks, Monitoring, and Tags. The Status Checks tab is active. It shows Volume Status: Okay, Availability Zone: us-west-2c, IO Status: Enabled (Since April 12, 2017 at 5:14:40 PM UTC+5:30), and Auto-Enabled IO: Enabled (Edit). A note says: 'Find out more about working with volume status checks and events. If you need technical assistance with your volume, post your issue to the [Developer Forums](#) or visit our [Support Center](#).'

Activity - Volumes

The screenshot shows the AWS EC2 Management console with the 'Volumes' section selected. The left sidebar includes links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances, AMIs, Bundle Tasks, ELASTIC BLOCK STORE (with 'Volumes' selected), Snapshots, NETWORK & SECURITY (with Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), and LOAD BALANCING (with Load Balancers, Target Groups). The main content area displays a table of volumes, showing one entry: 'web-server-1' (Volume ID: vol-08f5e68c..., Size: 8 GiB, Type: standard, Snapshot: snap-066b501..., Created: April 12, 2017 at 5:20:11, Availability Zone: us-west-2c, State: in-use, Alarm Status: None, Attachment Information: i-0749a28555320dbf7 (web-server-1):/dev/xvda (attached)). Below the table are tabs for Description, Status Checks, Monitoring (selected), and Tags, with a 'Create Alarm' button. A section titled 'CloudWatch metrics:' shows eight line graphs for Read Bandwidth, Write Bandwidth, Read Throughput, Write Throughput, Average Queue Length, Time Spent Idle (Percent), Average Read Size, and Average Write Size over a one-hour period from 07:00 to 07:30 on April 13. The bottom of the page includes a feedback link, language selection (English), and a footer with copyright information.

Activity - Volumes

The screenshot shows the AWS EC2 Management console with the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#CreateVolume>. The page is titled 'Create Volume'. A dropdown menu for 'Volume Type' is open, showing options: General Purpose SSD (GP2), Provisioned IOPS SSD (IO1), Cold HDD (SC1), Throughput Optimized HDD (ST1), and Magnetic. The 'Magnetic' option is selected. Other fields visible include 'Size (GiB)' set to 10, 'Availability Zone*' set to us-west-2a, and 'Encryption' checked.

Volumes > Create Volume

Create Volume

Volume Type: Magnetic

Size (GiB): 10 (Min: 1 GiB, Max: 1024 GiB)

IOPS: Not applicable

Availability Zone*: us-west-2a

Throughput (MB/s): Not applicable

Snapshot ID: Select a snapshot

Encryption: Encrypt this volume

Tags: Create additional tags

* Required

Cancel **Create Volume**

Feedback English (US) © 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Activity - Volumes

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with links like EC2 Dashboard, Instances, Images, and Elastic Block Store (which is currently selected). In the main content area, a table lists three volumes: Instance1-OS, Instance2-OS, and vol-387cdecf. A context menu is open over the third volume, showing options: Delete Volume, Attach Volume, Detach Volume, Force Detach Volume, Create Snapshot, Change Auto-Enable IO Setting, and Add/Edit Tags. Below the table, a detailed view of the selected volume (vol-387cdecf) is shown with fields for Volume ID, Size, Created, State, Attachment information, and various status metrics.

Name	Volume Type	IOPS	Snapshot	Created	Availability Zone	State
Instance1-OS	gp2	24 / 3000	snap-ad8e61f8	December 13, 2015...	us-west-2b	in-use
Instance2-OS	standard	-	snap-ad8e61f8	December 13, 2015...	us-west-2c	in-use
vol-387cdecf	standard	-		December 13, 2015...	us-west-2b	available

Volumes: vol-387cdecf

Description Status Checks Monitoring Tags

Volume ID	vol-387cdecf	Alarm status	None
Size	10 GiB	Snapshot	-
Created	December 13, 2015 at 7:59:02 PM UTC+5:30	Availability Zone	us-west-2b
State	available	Encrypted	Not Encrypted
Attachment information	Volume type	standard	KMS Key ID
	Product codes	-	KMS Key Aliases
	IOPS	-	KMS Key ARN

Feedback English © 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Activity - Volumes

The screenshot shows the AWS EC2 Management Console interface. The main navigation bar includes tabs for EC2 Management Console, web-lb-1-1634359284.us-west-2, and Amazon EC2 Instance IP. The browser address bar shows the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Volumes:sort=createTime>. The AWS logo and navigation dropdown are visible at the top.

The main content area displays the 'EC2 Dashboard' and 'Events' sections. A prominent 'Create Volume' button is visible. An 'Actions' dropdown menu is open. A modal dialog box titled 'Attach Volume' is displayed, containing the following fields:

- Volume: vol-387cdecf in us-west-2b
- Instance: i-48072c8c in us-west-2b
- Device: i-48072c8c (Http Server1) (running)

A note in the dialog box states: "Note: Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdp internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp."

At the bottom right of the dialog box are 'Cancel' and 'Attach' buttons. Below the dialog, the 'Volumes' section of the dashboard is visible, showing a table with columns: Name, Created, State, Availability Zone, Encrypted, KMS Key ID, KMS Key Aliases, and KMS Key ARN. One volume entry is shown:

Name	Created	State	Availability Zone	Encrypted	KMS Key ID	KMS Key Aliases	KMS Key ARN
vol-387cdecf	December 13, 2015 at 7:59:02 PM UTC+5:30	available	us-west-2b	Not Encrypted			

The left sidebar contains navigation links for Volumes, Snapshots, NETWORK & SECURITY (Security Groups, Elastic IPs, Placement Groups), and other AWS services like OpsCenter, FlipBasket, AWS Console, AWS Docs, and tech-research.

At the bottom of the page, there are links for Feedback, English, and footer text: © 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use.

Activity - Volumes

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation includes links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances, AMIs, Dedicated Hosts, and Elastic Block Store (selected). Under EBS, the 'Volumes' link is highlighted. The main content area displays a table of volumes with columns: Name, Volume ID, Size, Volume Type, IOPS, Snapshot, Created, Availability Zone, and State. Three volumes are listed: Instance1-OS, Instance2-OS, and vol-387cdef. The volume vol-387cdef is selected, shown in a detailed view below the table. The detailed view shows the following information:

Description	Value	Description	Value
Volume ID	vol-387cdef	Alarm status	None
Size	10 GiB	Snapshot	-
Created	December 13, 2015 at 7:59:02 PM UTC+5:30	Availability Zone	us-west-2b
State	in-use	Encrypted	Not Encrypted
Attachment information	i-48072c8c (Http Server1) :/dev/sdf (attached)	KMS Key ID	-
Volume type	standard	KMS Key Aliases	-
Product codes	-	KMS Key ARN	-

At the bottom of the page, there are links for Feedback, English, and footer text: © 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use.

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

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with links like EC2 Dashboard, Instances, Images, and Elastic Block Store (Volumes). The main area displays a list of volumes, with one specific volume selected: vol-387cddecf. A context menu is open over this volume, showing options: Delete Volume, Attach Volume, Detach Volume, Force Detach Volume, Create Snapshot, Change Auto-Enable IO Setting, and Add/Edit Tags. Below the volume list, there's a detailed view of the selected volume's properties, including Volume ID, Size, Created, State, Attachment information, Volume type, and Product codes. The volume is currently attached to an instance (i-48072c8c) and is in the standard gp2 type.

Name	Volume Type	IOPS	Snapshot	Created	Availability Zone	State
Instance1-OS	gp2	24 / 3000	snap-ad8e61f8	December 13, 2015...	us-west-2b	in-use
Instance2-OS	standard	-	snap-ad8e61f8	December 13, 2015...	us-west-2c	in-use
vol-387cddecf	standard	-		December 13, 2015...	us-west-2b	in-use

Volumes: vol-387cddecf

Description	Status Checks	Monitoring	Tags
Volume ID: vol-387cddecf	Size: 10 GiB	Created: December 13, 2015 at 7:59:02 PM UTC+5:30	State: in-use
Attachment information: i-48072c8c (Http Server1) :/dev/sdf (attached)	Volume type: standard	Product codes: -	Alarm status: None
			Snapshot: -
			Availability Zone: us-west-2b
			Encrypted: Not Encrypted
			KMS Key ID: KMS Key ARN: KMS Key Aliases:

Activity - Volumes

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with links like EC2 Dashboard, Instances, Images, and Elastic Block Store (selected). Under EBS, 'Volumes' is also selected. The main content area displays a table of volumes, with one volume highlighted. A modal dialog titled 'Detach Volume' is open over the table, asking 'Are you sure you want to detach this volume? vol-387cdecf'. At the bottom of the dialog are 'Cancel' and 'Yes, Detach' buttons. The background table shows the following data:

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone	State
Instance1-OS	vol-29b210de	8 GiB	gp2	24 / 3000	snap-ad8e61f8	December 13, 2015...	us-west-2b	in-use
Instance2-OS	vol-e7582401	8 GiB	standard	-	snap-ad8e61f8	December 13, 2015...	us-west-2c	in-use
	vol-387cdecf	-	-	-	-	December 13, 2015...	us-west-2b	in-use

Activity - Volumes

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation menu includes options like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, and Elastic Block Store (with Volumes and Snapshots selected). The main content area displays a table of existing volumes, with three rows visible:

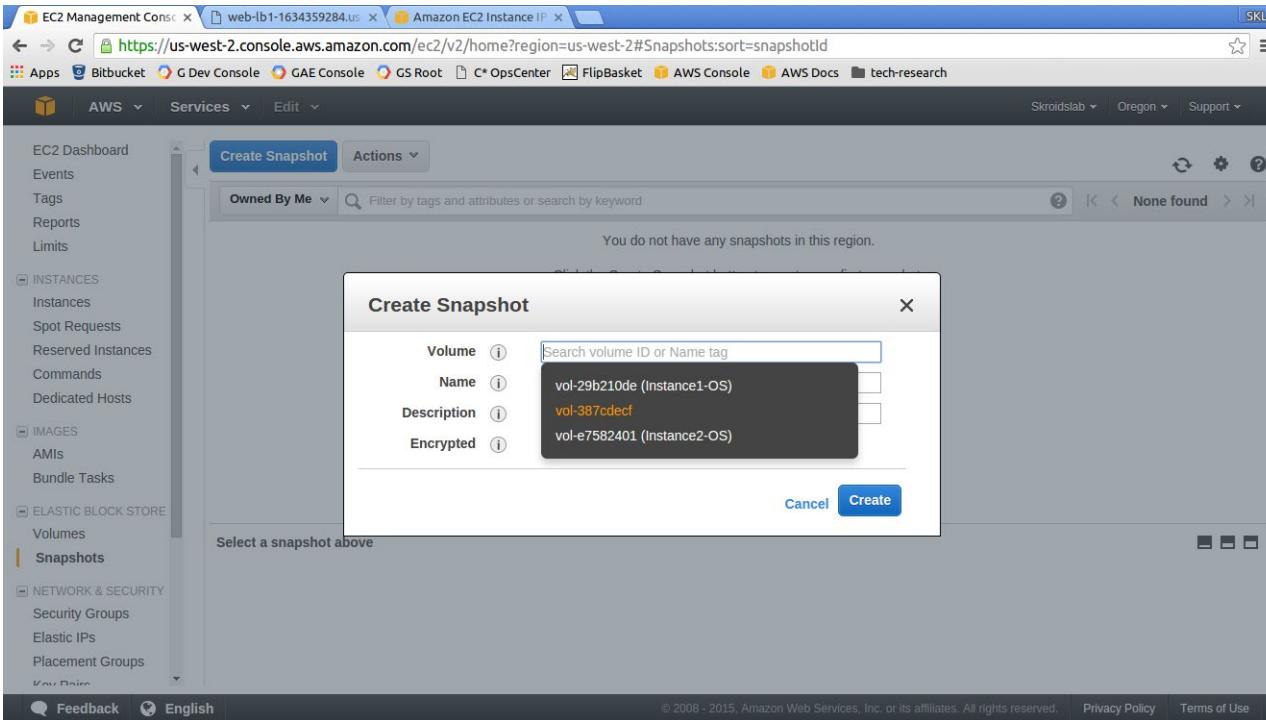
	Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone	State
	Instance1-OS	vol-29b210de	8 GiB	gp2	24 / 3000	snap-ad8e61f8	December 13, 2015...	us-west-2b	in-use
	Instance2-OS	vol-e7582401	8 GiB	standard	-	snap-ad8e61f8	December 13, 2015...	us-west-2c	in-use
		vol-387cdefc	10 GiB	standard	-		December 13, 2015...	us-west-2b	available

A message at the bottom of the table says "Select a volume above". The top navigation bar shows tabs for EC2 Management Console, web-lb-1-1634359284.us, and Amazon EC2 Instance IP. The URL in the address bar is https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Volumes:sort=createTime. The browser toolbar includes icons for Apps, Bitbucket, G Dev Console, GAE Console, GS Root, C* OpsCenter, FlipBasket, AWS Console, AWS Docs, and tech-research.

Activity - Snapshot from Volume

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation menu is visible, with the 'Solutions' volume selected under the 'VOLUMES' section. The main content area displays the 'Create Snapshot' page for the 'Solutions' volume. The page includes a search bar, a message stating 'You do not have any snapshots in this region.', and a prominent blue 'Create Snapshot' button. The top navigation bar shows the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Snapshots:sort=snapshotId>.

Activity - Snapshot from Volume



Activity - Snapshot from Volume

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation menu includes options like EC2 Dashboard, Instances, AMIs, Volumes, and Snapshots. The 'Volumes' section is currently selected. The main content area displays a message: "You do not have any snapshots in this region." A modal dialog box titled "Create Snapshot" is open in the center. It contains the following fields:

Setting	Value
Volume	vol-387cdecf
Name	Appdata
Description	A snapshot of the application data
Encrypted	No

At the bottom of the dialog, there are "Cancel" and "Create" buttons.

Activity - Snapshot from Volume

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation bar includes links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances, AMIs, Dedicated Hosts, Images, and Elastic Block Store. Under the Elastic Block Store section, the 'Solutions' link is highlighted. The main content area displays a table of snapshots owned by the user, with one entry for 'Appdata'. The detailed view for this snapshot shows its ID as 'snap-6fb43a3d', status as 'pending', and volume as 'vol-387cdecf'. It also lists the start time as December 13, 2015 at 8:35:09 PM UTC+5:30, owner as '278931287317', and a description of 'A snapshot of the application data'. The progress is shown as 0%.

Name	Snapshot ID	Size	Description	Status	Started
Appdata	snap-6fb43a3d	10 GiB	A snapshot of the application data	completed	December 13, 2015 at 8:35:09 PM UTC+5:30

Snapshot: snap-6fb43a3d (Appdata)

Description **Permissions** **Tags**

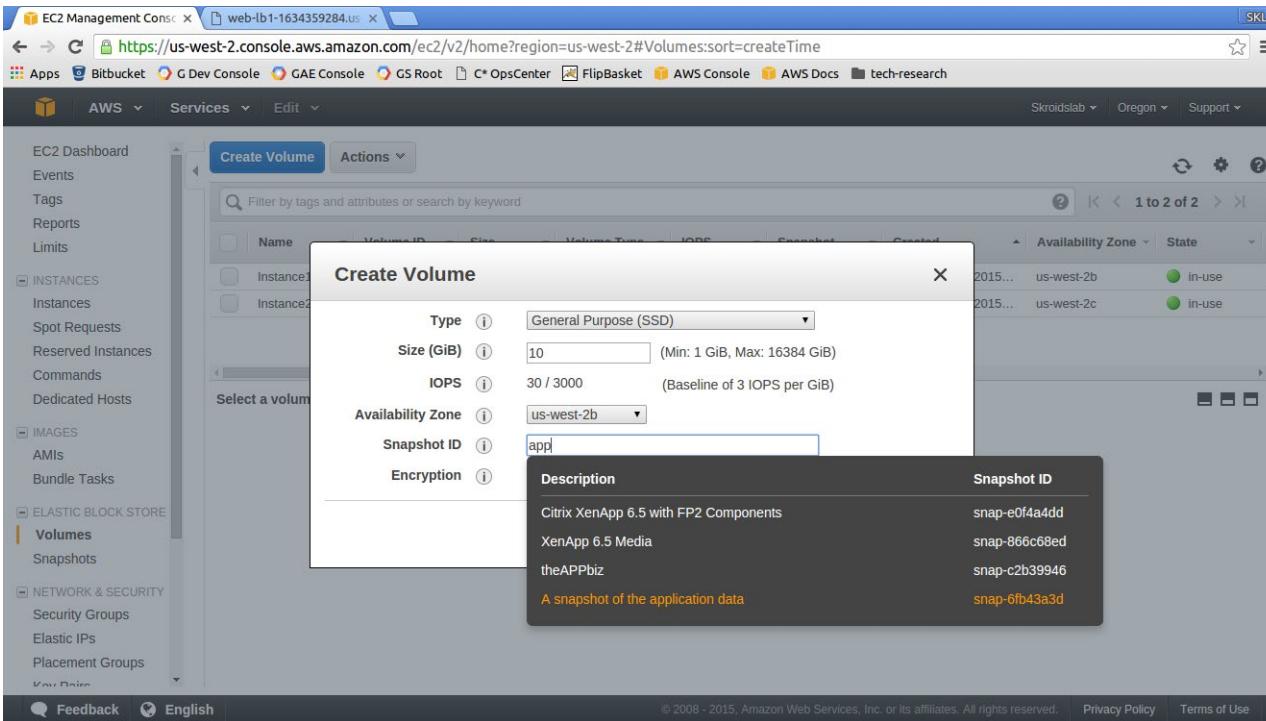
Snapshot ID	snap-6fb43a3d	Progress	0%
Status	pending	Capacity	10 GiB
Volume	vol-387cdecf	Encrypted	Not Encrypted
Started	December 13, 2015 at 8:35:09 PM UTC+5:30	KMS Key ID	
Owner	278931287317	KMS Key Aliases	
Product codes	-	KMS Key ARN	
Description	A snapshot of the application data		

Activity - Volume from Snapshot

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with links like EC2 Dashboard, Instances, AMIs, and Elastic Block Store (which is currently selected). In the main content area, a volume named 'vol-387cddecf' is displayed with details such as Volume ID, Size (10 GiB), Created (December 13, 2015 at 7:59:02 PM UTC+5:30), State (available), and Volume Type (standard). A context menu is open over this volume, showing options: Delete Volume, Attach Volume, Detach Volume, Force Detach Volume, Create Snapshot, Change Auto-Enable IO Setting, and Add/Edit Tags. The 'Create Snapshot' option is highlighted.

Volume Type	IOPS	Snapshot	Created	Availability Zone	State
gp2	24 / 3000	snap-ad8e61f8	December 13, 2015...	us-west-2b	in-use
standard	-	snap-ad8e61f8	December 13, 2015...	us-west-2c	in-use
standard	-		December 13, 2015...	us-west-2b	available

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

- 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



Storage and Content Delivery

Elastic File System - EFS

Activity - EFS

- **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

The screenshot shows the AWS Management Console for Amazon Elastic File System (EFS). The browser title bar reads "Elastic File System | Amazon Elastic File". The URL is "https://us-west-2.console.aws.amazon.com/efs/home?region=us-west-2#/firstrun". The top navigation bar includes links for "Secure", "AWS Documenta", and various services like Napabrick, BB, GCloud, AWS, Azure, Trello, Gmail, Google analytics, pointernext, AWS Documenta, and AWS Lambda. The main content area features a large red icon of a stack of three boxes. Below it is the heading "Amazon Elastic File System (EFS)" and the subtext "Amazon EFS provides file storage for use with your EC2 instances." A prominent blue button labeled "Create file system" is centered. Below this, a link to "Getting started guide" is visible. The page is divided into three main sections: "Create" (with an icon of a folder plus sign), "Access" (with an icon of a cloud and a double arrow), and "Manage" (with an icon of a person silhouette and a gear). Each section contains descriptive text about its function.

Create

Create an Amazon EFS file system to store your files in the Amazon cloud. A file system grows and shrinks automatically with the files you put in, and you pay only for what you use.

Access

Write files to and read files from your Amazon EFS file system by using the NFSv4 protocol. Any number of EC2 instances can work with your file system at the same time, and your instances can be in multiple Availability Zones in a region.

Manage

You can easily administer your file system using the Amazon EFS console, CLI, and SDK.

Activity - EFS

greatlearning

The screenshot shows the 'Create file system' wizard on the Amazon EFS console. The current step is 'Step 1: Configure file system access'. The page title is 'Configure file system access'. A note states: 'An Amazon EFS file system is accessed by EC2 instances running inside one of your VPCs. Instances connect to a file system by using a network interface called a mount target. Each mount target has an IP address, which we assign automatically or you can specify.' A dropdown menu labeled 'VPC' is set to 'vpc-51238934 (default)'. Below this, there's a section titled 'Create mount targets' with a table. The table has columns: Availability Zone, Subnet, IP address, and Security groups. Three rows are listed for 'us-west-2':

- us-west-2a: Subnet 'subnet-22b21155 (default)', IP address 'Leave blank for automatic', Security groups 'sg-05123160 - default'
- us-west-2b: Subnet 'subnet-fa921f9f (default)', IP address 'Automatic', Security groups 'sg-05123160 - default'
- us-west-2c: Subnet 'subnet-ee30f1b7 (default)', IP address 'Automatic', Security groups 'sg-05123160 - default'

Red boxes highlight the 'Availability Zone' column for the first three rows and the 'IP address' input field for the first row. At the bottom right are 'Cancel' and 'Next Step' buttons.

Activity - EFS

The screenshot shows the AWS EFS wizard at Step 2: Configure optional settings. The URL is <https://us-west-2.console.aws.amazon.com/efs/home?region=us-west-2#/wizard/2>. The page includes sections for Add tags, Choose performance mode, and Enable encryption.

Add tags: A table shows a single tag: Name (Value: skl-efs). The 'Name' input field is highlighted with a red box.

Key	Value
Name	skl-efs

Choose performance mode: The 'General Purpose (default)' radio button is selected.

Enable encryption: A checkbox labeled 'Enable encryption' is present.

Activity - EFS

greatlearning

The screenshot shows the 'Create file system' wizard in the AWS Management Console. The current step is 'Step 3: Review and create'. The page title is 'Review and create'.

File system access:

VPC	Availability Zone	Subnet	IP address	Security groups
vpc-51238934 (default)	us-west-2a	subnet-22b21155 (default)	Automatic	sg-05123160 - default
	us-west-2b	subnet-fa921f9f (default)	Automatic	sg-05123160 - default
	us-west-2c	subnet-ee30f1b7 (default)	Automatic	sg-05123160 - default

Optional settings:

- Tags: Name: skl-efs
- Performance mode: General Purpose (default)

Buttons at the bottom: Cancel, Previous, Create File System.

Activity - EFS

The screenshot shows the AWS Elastic File System (EFS) console. A success message indicates a new file system has been created. The file system table lists 'skl-efs' with details: Name: 'skl-efs', File system ID: 'fs-b914c010', Metered size: 6.0 KiB, Number of mount targets: 3, and Creation date: 2017-04-14T14:42:10Z. The 'File system access' section shows the DNS name: 'fs-b914c010.efs.us-west-2.amazonaws.com'. The 'Mount targets' table lists three targets across three Availability Zones (us-west-2a, us-west-2b, us-west-2c) in the VPC 'vpc-51238934 (default)', all currently in a 'Creating' state.

VPC	Availability Zone	Subnet	IP address	Mount target ID	Network interface ID	Security groups	Life cycle state
vpc-51238934 (default)	us-west-2a	subnet-22b21155 (default)	172.31.16.150	fsmr-e97ea840	eni-6722605d		Creating
	us-west-2b	subnet-fa921f9f (default)	172.31.43.97	fsmr-e87ea841	eni-aec3e086		Creating
	us-west-2c	subnet-ee30f1b7 (default)	172.31.14.13	fsmr-eb7ea842	eni-c270ebce		Creating

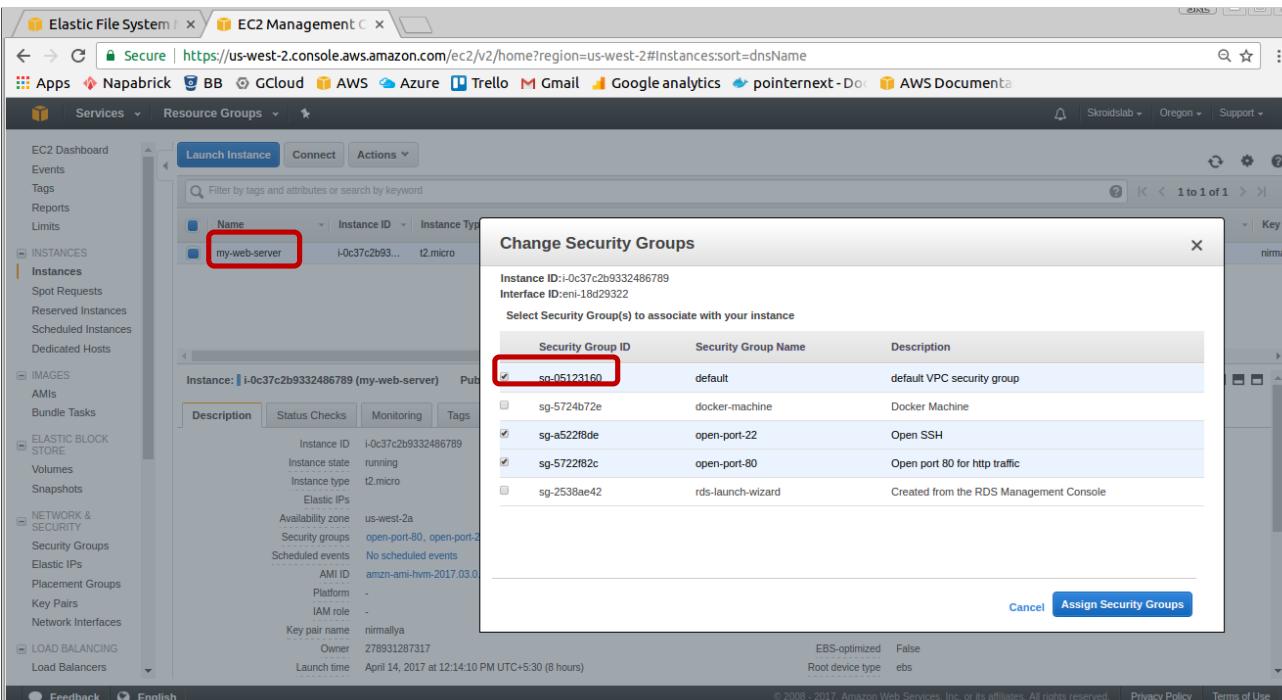
Activity - EFS

The screenshot shows the AWS Elastic File System (EFS) console. A file system named 'ski-efs' is listed in the 'File systems' table. The table includes columns for Name, File system ID, Metered size, Number of mount targets, and Creation date. Below the table, 'Other details' show the Owner ID (278931287317), Life cycle state (Available), and Performance mode (General Purpose). Under 'File system access', the DNS name is listed as fs-b914c010.efs.us-west-2.amazonaws.com. The 'Amazon EC2 mount instructions' section is highlighted with a red box. The 'Mount targets' table lists three targets across three subnets in the us-west-2a, us-west-2b, and us-west-2c VPCs. The IP address 172.31.16.150 and the Security group sg-05123160 - default are highlighted with red boxes.

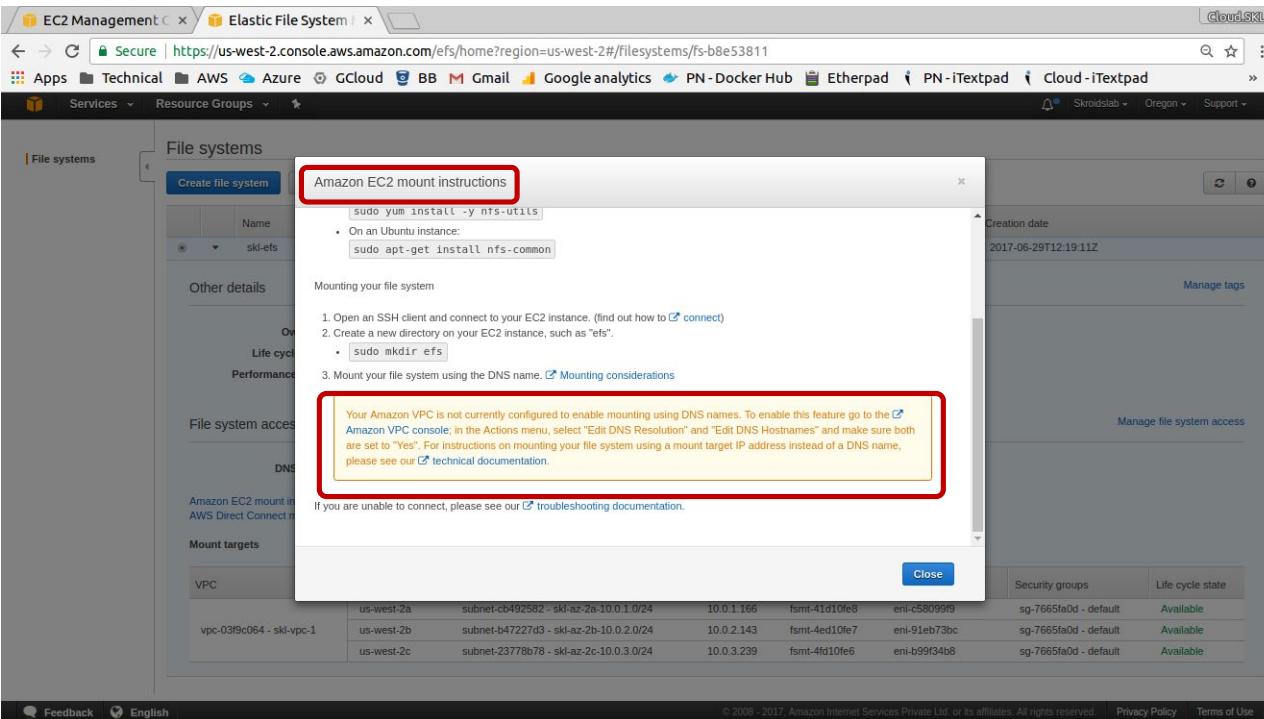
VPC	Availability Zone	Subnet	IP address	Mount target ID	Network interface ID	Security groups	Life cycle state
vpc-51238934 (default)	us-west-2a	subnet-22b21155 (default)	172.31.16.150	fsmt-e97ea840	eni-6722605d	sg-05123160 - default	Available
	us-west-2b	subnet-fa921f9f (default)	172.31.43.97	fsmt-e87ea841	eni-aec3e086	sg-05123160 - default	Available
	us-west-2c	subnet-ee30fb1b7 (default)	172.31.14.13	fsmt-eb7ea842	eni-c270ebce	sg-05123160 - default	Available

**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



**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

The screenshot shows the AWS VPC Management console. On the left, there's a sidebar with various VPC-related options like Subnets, Route Tables, and Security Groups. A context menu is open over a specific VPC entry ('vpc-03f9c064 | skl-vpc-1'). The menu items are: Create VPC, Actions, Delete VPC, Edit CIDRs, Edit DHCP Options Sets, **Edit DNS Resolution**, Edit DNS Hostnames, and Create Flow Log. The 'Edit DNS Resolution' option is highlighted with a red box. Two modal dialogs are displayed: 'Edit DNS Resolution' (with 'DNS Resolution' radio buttons set to 'Yes') and 'Edit DNS Hostnames' (with 'DNS Hostnames' radio buttons set to 'Yes'). Both dialogs have 'Save' and 'Cancel' buttons.

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

Activity - EFS

The screenshot shows the AWS Management Console with the 'Elastic File System' tab selected. A modal window titled 'Amazon EC2 mount instructions' is open, displaying the following content:

Amazon EC2 mount instructions

2. Open an SSH client and connect to your EC2 instance. (find out how to [connect](#))
3. Install the nfs client on your EC2 instance.

- On an Amazon Linux, Red Hat Enterprise Linux, or SuSE Linux instance:
`sudo yum install -y nfs-utils`
- On an Ubuntu instance:
`sudo apt-get install nfs-common`

Mounting your file system

1. Open an SSH client and connect to your EC2 instance. (find out how to [connect](#))
2. Create a new directory on your EC2 instance, such as "efs".

- `sudo mkdir efs`

3. Mount your file system using the DNS name. [Mounting considerations](#)

- `sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2 fs-b8e53811.efs.us-west-2.amazonaws.com:/ efs`

If you are unable to connect, please see our [troubleshooting documentation](#).

Close

Feedback English

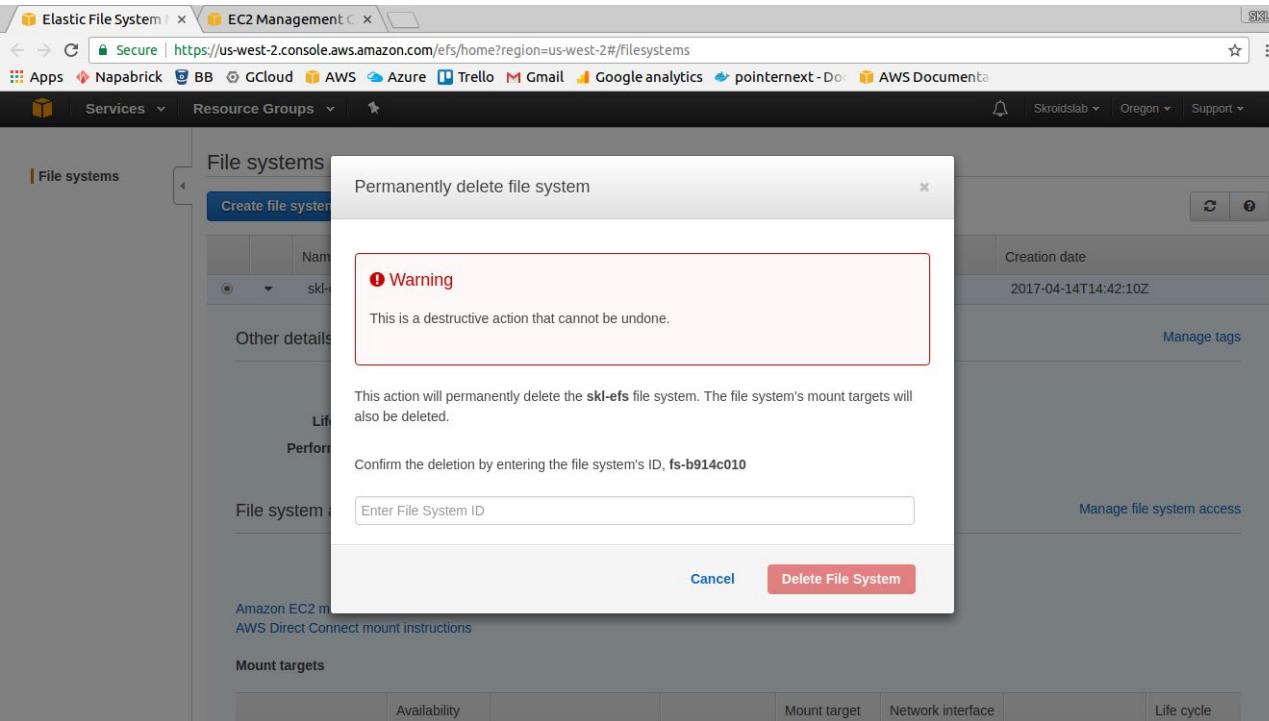
© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Popup after clicking on "EC2 mount instructions" link

Activity - EFS

- 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





Storage and Content Delivery

S3

Simple storage service - S3

- 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

- **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

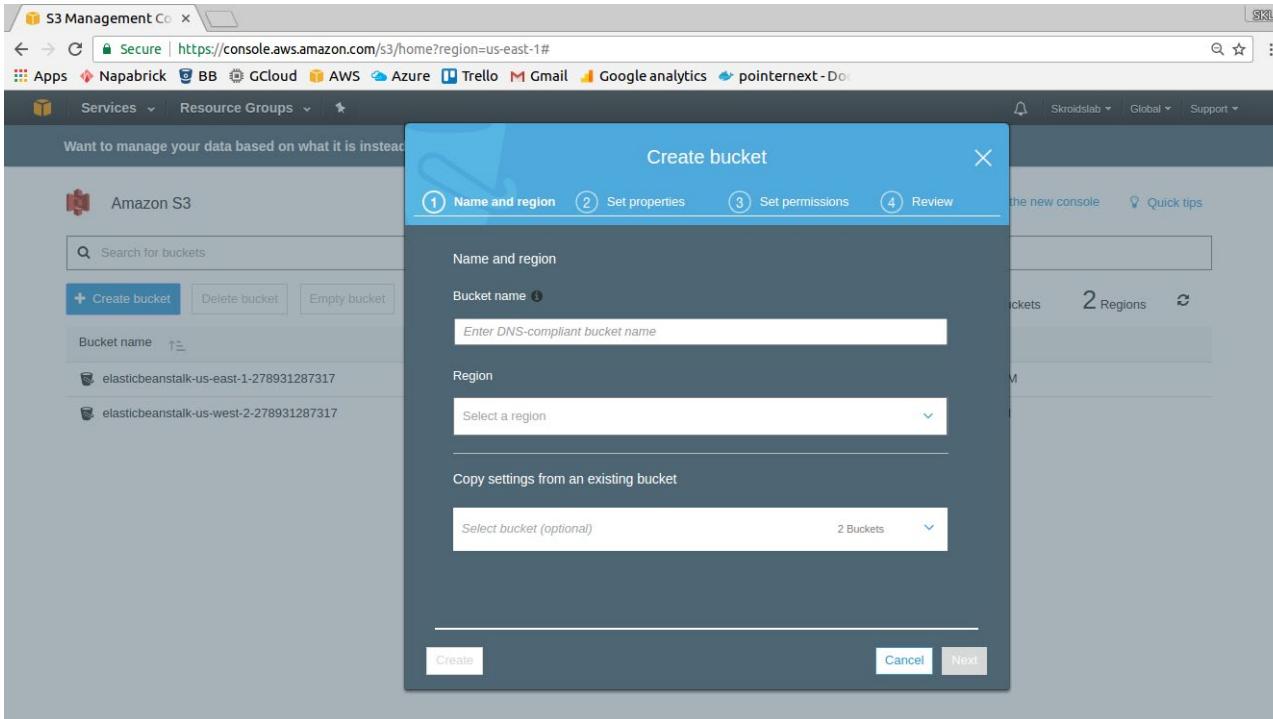
- **Consistency**
 - Read after write consistency for PUTS of new objects (insert a new object and it is immediately consistent)
 - Eventual consistency for overwrites across all the availability zones (also depends on file size)
- **Atomic operation**
 - Either new data or old data but no corruption 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

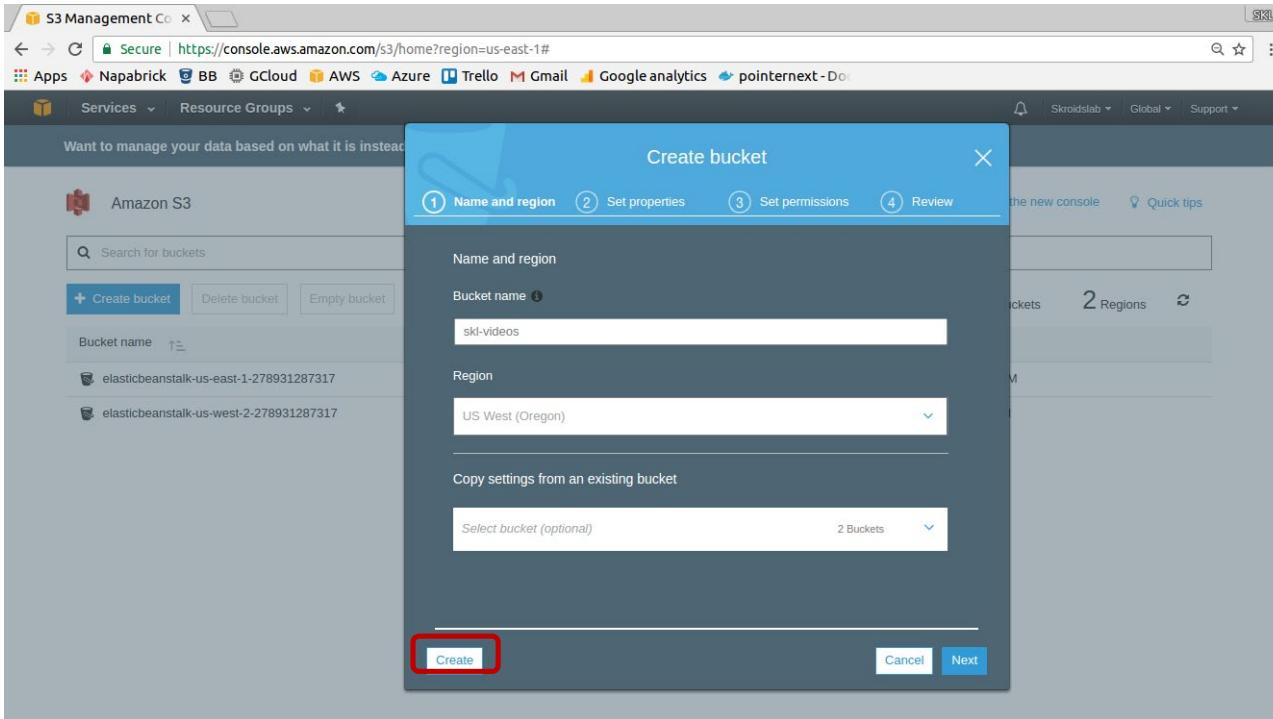
The screenshot shows the AWS S3 Management Console interface. At the top, there's a navigation bar with links to various services like Napabrick, BB, GCloud, AWS, Azure, Trello, Gmail, Google analytics, and pointernext. Below the navigation bar, a banner suggests trying S3 Object Tagging. The main area is titled "Amazon S3" and features a search bar labeled "Search for buckets". A red box highlights the "Create bucket" button. To the right, it displays "2 Buckets" and "2 Regions". The table below lists the buckets:

Bucket name	Region	Date created
elasticbeanstalk-us-east-1-278931287317	US East (N. Virginia)	Oct 16, 2015 11:11:14 AM
elasticbeanstalk-us-west-2-278931287317	US West (Oregon)	Jun 3, 2015 12:53:06 PM

Activity - S3



Activity - S3



Activity - S3

The screenshot shows the AWS S3 Management Console interface. At the top, there's a navigation bar with links for Secure, Apps, Napabrick, BB, GCloud, AWS, Azure, Trello, Gmail, Google analytics, and pointernext. Below the navigation bar, the main header reads "Amazon S3". A search bar labeled "Search for buckets" is present. Below the search bar are three buttons: "+ Create bucket", "Delete bucket", and "Empty bucket". To the right of these buttons, it displays "3 Buckets" and "2 Regions". The main content area lists three buckets:

Bucket name	Region	Date created
elasticbeanstalk-us-east-1-278931287317	US East (N. Virginia)	Oct 16, 2015 11:11:14 AM
elasticbeanstalk-us-west-2-278931287317	US West (Oregon)	Jun 3, 2015 12:53:06 PM
skl-videos	US West (Oregon)	Apr 10, 2017 9:56:42 AM

A red box highlights the "skl-videos" bucket.

Activity - S3

The screenshot shows the Amazon S3 Management Console interface. At the top, the URL is https://console.aws.amazon.com/s3/buckets/skl-videos/?region=us-east-1&tab=overview. The navigation bar includes links for Apps, Napabrick, BB, GCloud, AWS, Azure, Trello, Gmail, Google analytics, and pointernext. The main content area displays the 'skl-videos' bucket under the 'Amazon S3' section. The 'Objects' tab is selected. Below the tabs are buttons for 'Upload', '+ Create folder', and 'More'. A status message says 'This bucket is empty. Upload new objects to get started.' Three call-to-action cards are present: 'Upload an object' (with a bucket icon), 'Set object properties' (with two user icons and a plus sign), and 'Set object permissions' (with a database icon). Each card has a 'Learn more' link and a 'Get started' button.

This bucket is empty. Upload new objects to get started.

Upload an object

Buckets are globally unique containers for everything that you store in Amazon S3.

Learn more

Set object properties

After you create a bucket, you can upload your objects (for example, your photo or video files).

Learn more

Set object permissions

By default, the permissions on an object are private, but you can set up access control policies to grant permissions to others.

Learn more

Get started

Activity - S3

The screenshot shows the AWS S3 Management Console for the bucket 'skl-src'. The top navigation bar includes links for Secure, Apps, Technical, AWS, GCP, CloudPads, Azure, BB, Gmail, CRASH, PN - Docker Hub, and AWS INNOVATE. The main content area displays various configuration options:

- Versioning:** Keep multiple versions of an object in the same bucket. Status: Disabled.
- Server access logging:** Set up access log records that provide details about access requests. Status: Disabled.
- Static website hosting:** Host a static website, which does not require server-side technologies. Status: Disabled.
- Object-level logging:** Record object-level API activity using the CloudTrail data events feature (additional cost). Status: Disabled.

Advanced settings

- Tags:** Use tags to track your cost against projects or other criteria. Status: 0 Tags.
- Transfer acceleration:** Enable fast, easy and secure transfers of files to and from your bucket. Status: Suspended.
- Events:** Receive notifications when specific events occur in your bucket. Status: 1 Active notifications.
- Requester pays:** The requester (instead of the bucket owner) will pay for requests and data transfer. Status: Disabled.

Activity - S3

The screenshot shows the AWS S3 Management Console for the bucket 'skl-src'. The 'Permissions' tab is selected. The 'Access Control List' section shows 'Owner access' for the account 'skroidslab' with full permissions (List objects, Write objects, Read bucket permissions, Write bucket permissions) enabled. The 'Access for other AWS accounts' section is empty. The 'Public access' section shows 'Everyone' with full permissions. The 'S3 log delivery group' section shows 'Log Delivery' with full permissions.

Account	List objects	Write objects	Read bucket permissions	Write bucket permissions
skroidslab	Yes	Yes	Yes	Yes

Account	List objects	Write objects	Read bucket permissions	Write bucket permissions

Group	List objects	Write objects	Read bucket permissions	Write bucket permissions
Everyone				

Group	List objects	Write objects	Read bucket permissions	Write bucket permissions
Log Delivery				

Activity - S3

S3 Management Console Cloud SKL

Secure | https://s3.console.aws.amazon.com/s3/buckets/skl-src/?region=us-west-2&tab=management

CloudPads Azure BB Gmail CRaSH PN - Docker Hub AWS INNOVATE

Amazon S3 > skl-src

Overview Properties Permissions Management

Lifecycle Replication Analytics Metrics Inventory

+ Add lifecycle rule Edit Delete More

There is no lifecycle rule applied to this bucket.
Here is how to get started.

 Use lifecycle rules to manage your objects

You can manage an object's lifecycle by using a lifecycle rule, which defines how Amazon S3 manages objects during their lifetime.

[Learn more](#)

 Automate transition to tiered storage

Lifecycle rules enable you to automatically transition objects to the Standard - IA and/or to the Amazon Glacier storage class.

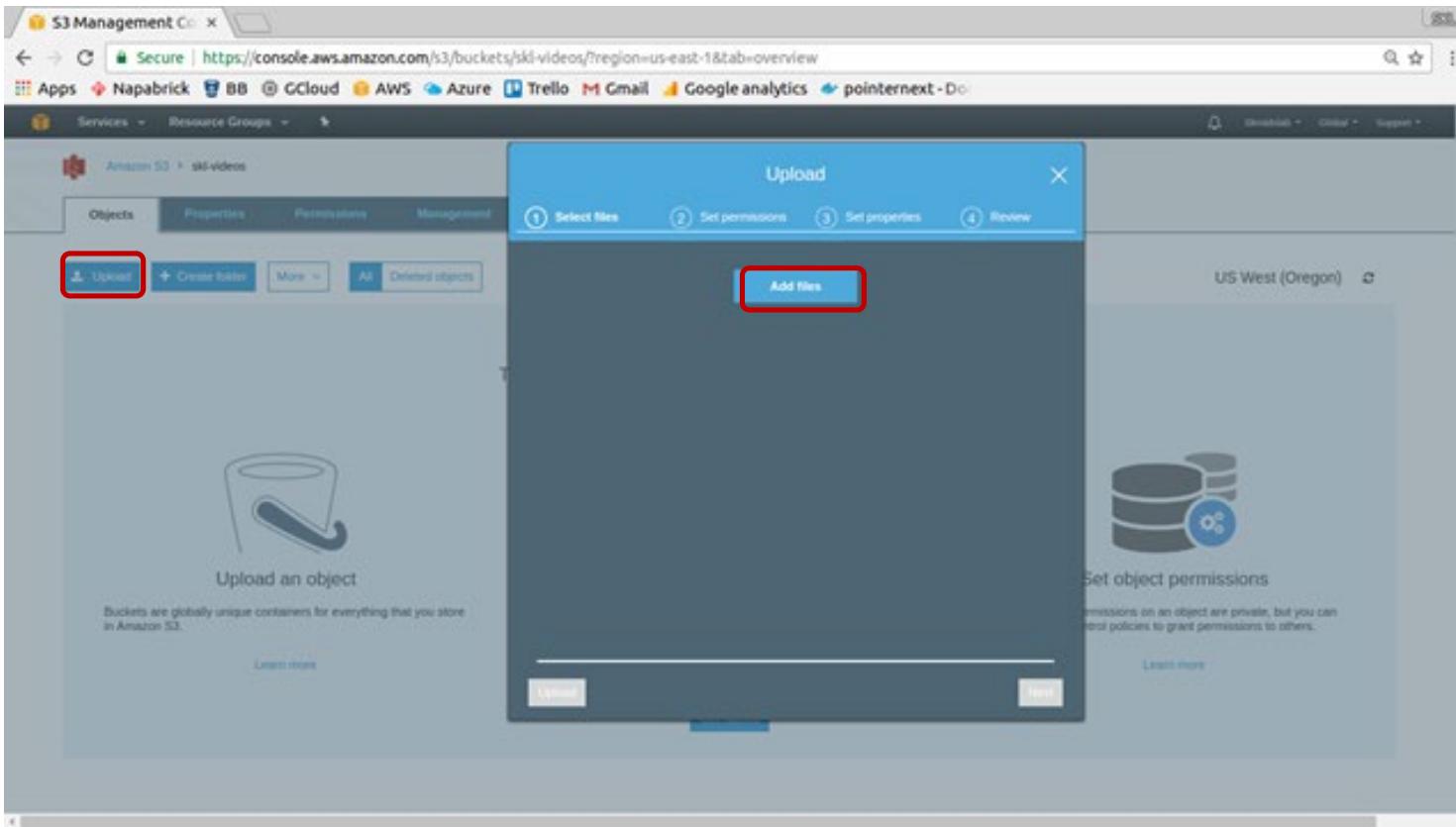
[Learn more](#) [Get started](#)

 Expire your objects

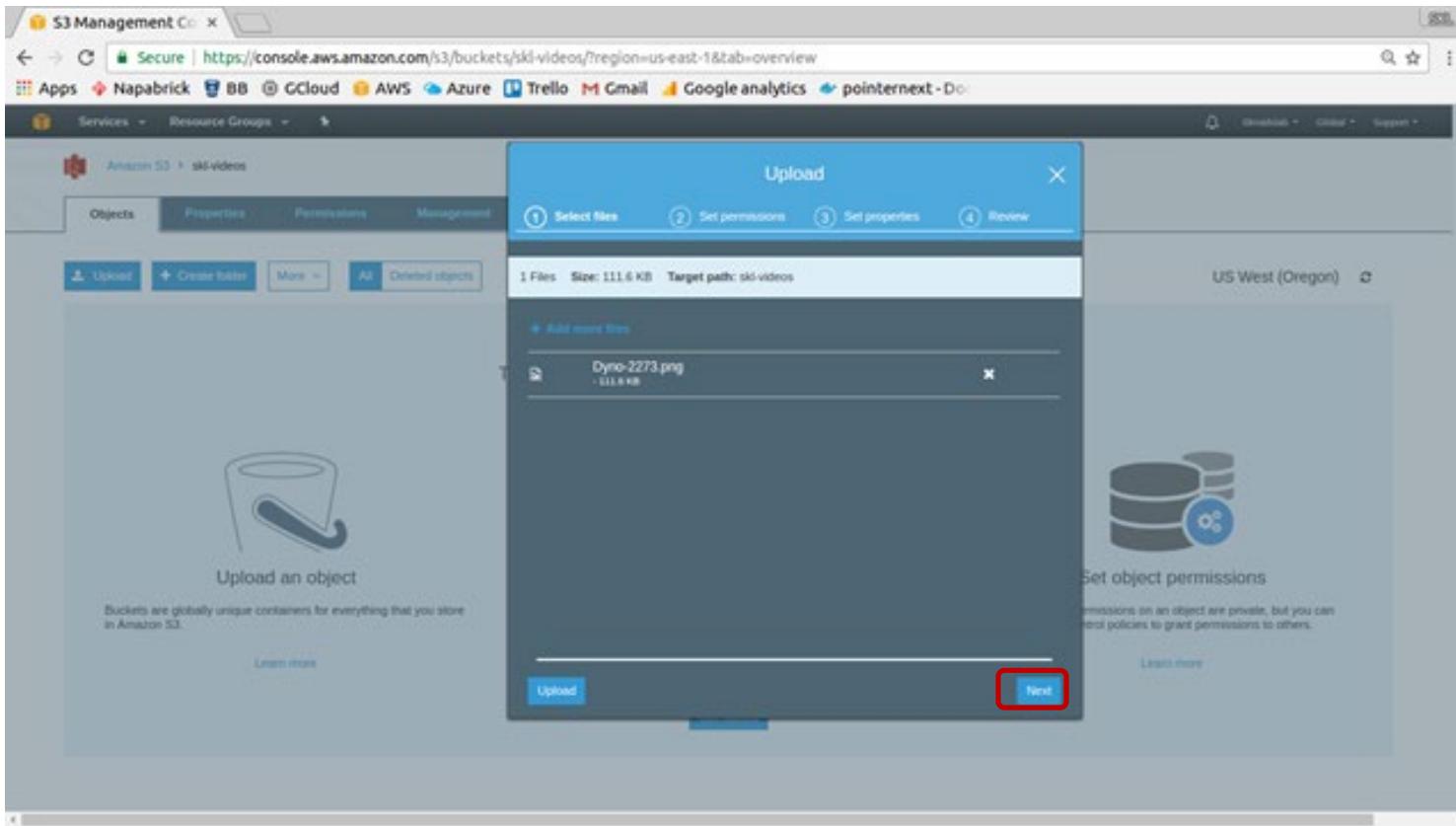
Using a lifecycle rule, you can automatically expire objects based on your retention needs or clean up incomplete multipart uploads.

[Learn more](#)

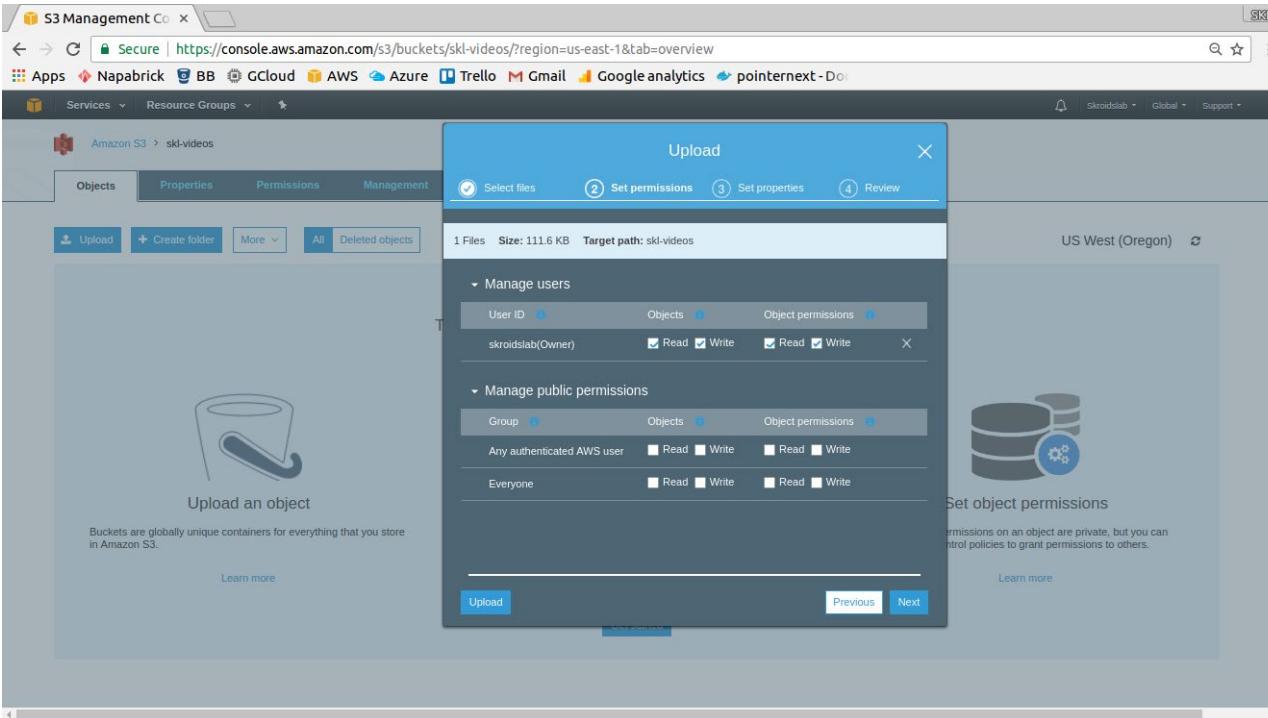
Activity - S3



Activity - S3

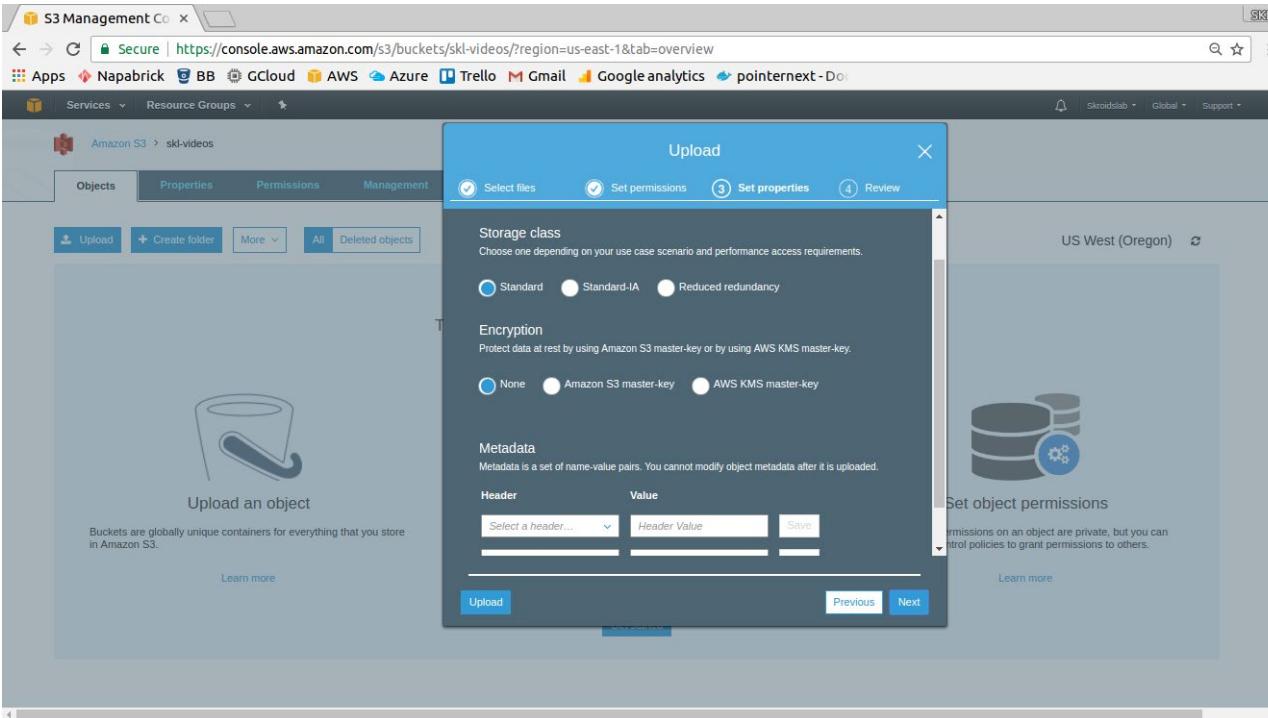


Activity - S3



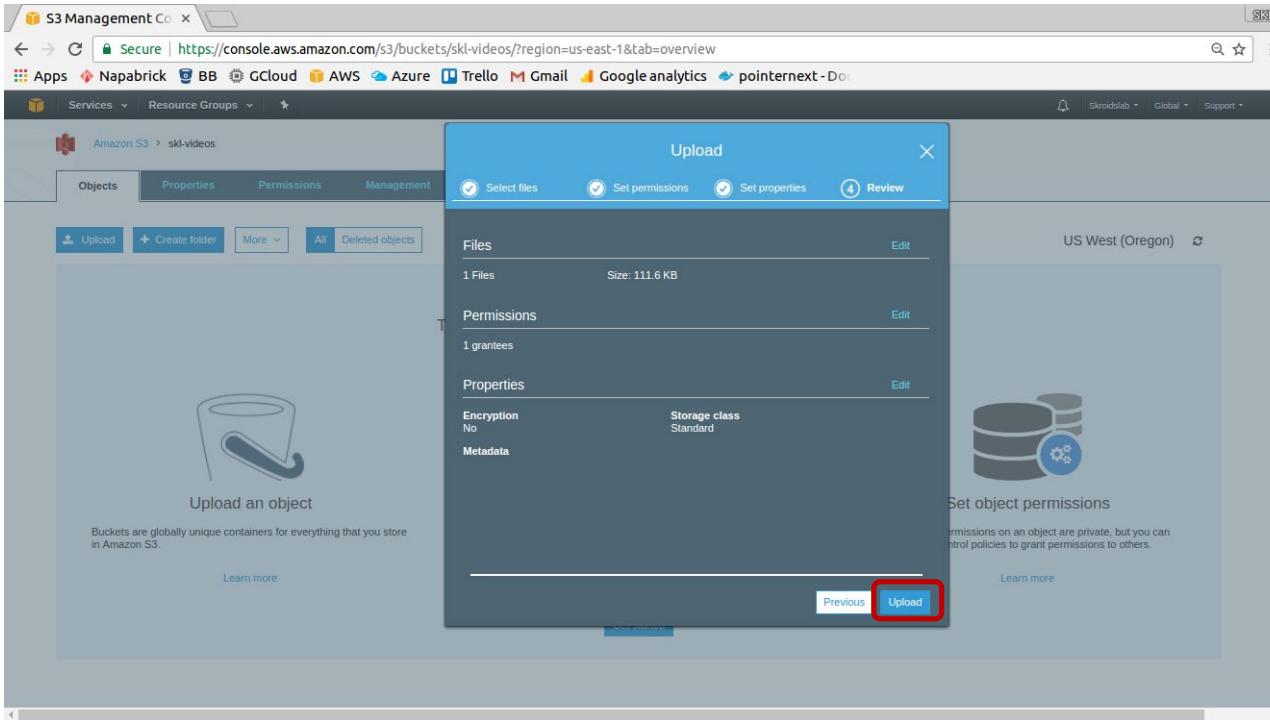
Leave all as defaults, we will modify these later

Activity - S3



Leave all as defaults, we will modify these later

Activity - S3



Activity - S3

The screenshot shows the AWS S3 Management Console interface. At the top, the URL is https://console.aws.amazon.com/s3/buckets/ski-videos/?region=us-east-1&tab=overview. The navigation bar includes links for Apps, Napabrick, GCloud, AWS, Azure, Trello, Gmail, Google analytics, pointernext, Services, Resource Groups, and Support.

The main content area displays the 'Amazon S3 > ski-videos' bucket. The 'Objects' tab is selected. A message says "This bucket is empty. Upload new objects to get started." Below this, there are three sections: "Upload an object" (with a bucket icon), "Set object properties" (with a person and plus icon), and "Set object permissions" (with a database icon). Each section has a "Learn more" link and a "Get started" button. At the bottom of the page, a progress bar shows "1 In progress", "0 Success", and "0 Error".

Activity - S3

The screenshot shows the AWS S3 Management Console interface. The URL in the browser is <https://console.aws.amazon.com/s3/buckets/ski-videos?region=us-east-1&tab=overview>. The page displays a single object named "Dyne-2273.png" in the "Objects" tab. The object details are as follows:

Name	Last modified	Size	Storage class
Dyne-2273.png	Apr 10, 2017 10:32:33 AM	111.6 KB	Standard

At the bottom of the console, there is an "Operations" bar with status indicators: 0 In progress, 1 Success, 0 Error.

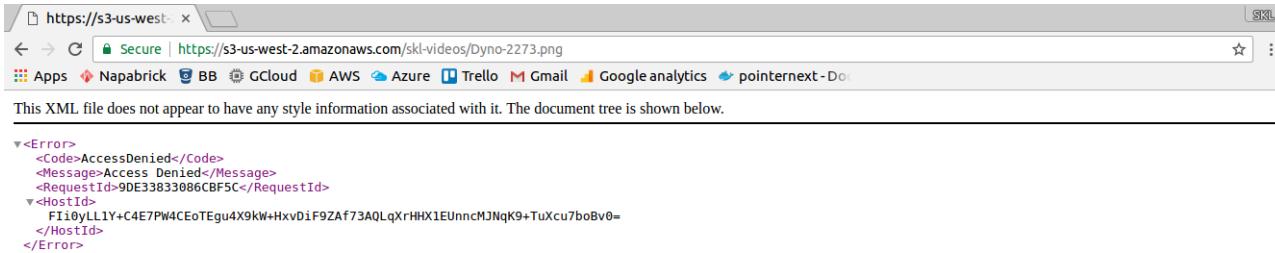
Activity - S3

The screenshot shows the AWS S3 Management Console interface. The URL in the browser is <https://console.aws.amazon.com/s3/buckets/skl-videos/Dyno-2273.png/details?region=us-east-1&tab=overview>. The file 'Dyno-2273.png' is selected in the 'skl-videos' bucket. The 'Properties' tab is active. Below it, there are four buttons: 'Open', 'Download', 'Download as', and 'Make public'. The 'Link' button is highlighted with a red box, showing the URL <https://s3-us-west-2.amazonaws.com/skl-videos/Dyno-2273.png>. Other visible details include the owner 'sklvideobucket', last activity on Apr 10, 2017 at 10:32:52 AM, the ID '26251e16640fbf1525e0e2464ef515e7b', storage class 'Standard', server-side encryption 'None', and size '114315' bytes.

Note - Look at the format of the bucket URL

227

Activity - S3



The screenshot shows a browser window with the URL <https://s3-us-west-2.amazonaws.com/skl-videos/Dyno-2273.png>. The page content is an XML error document:

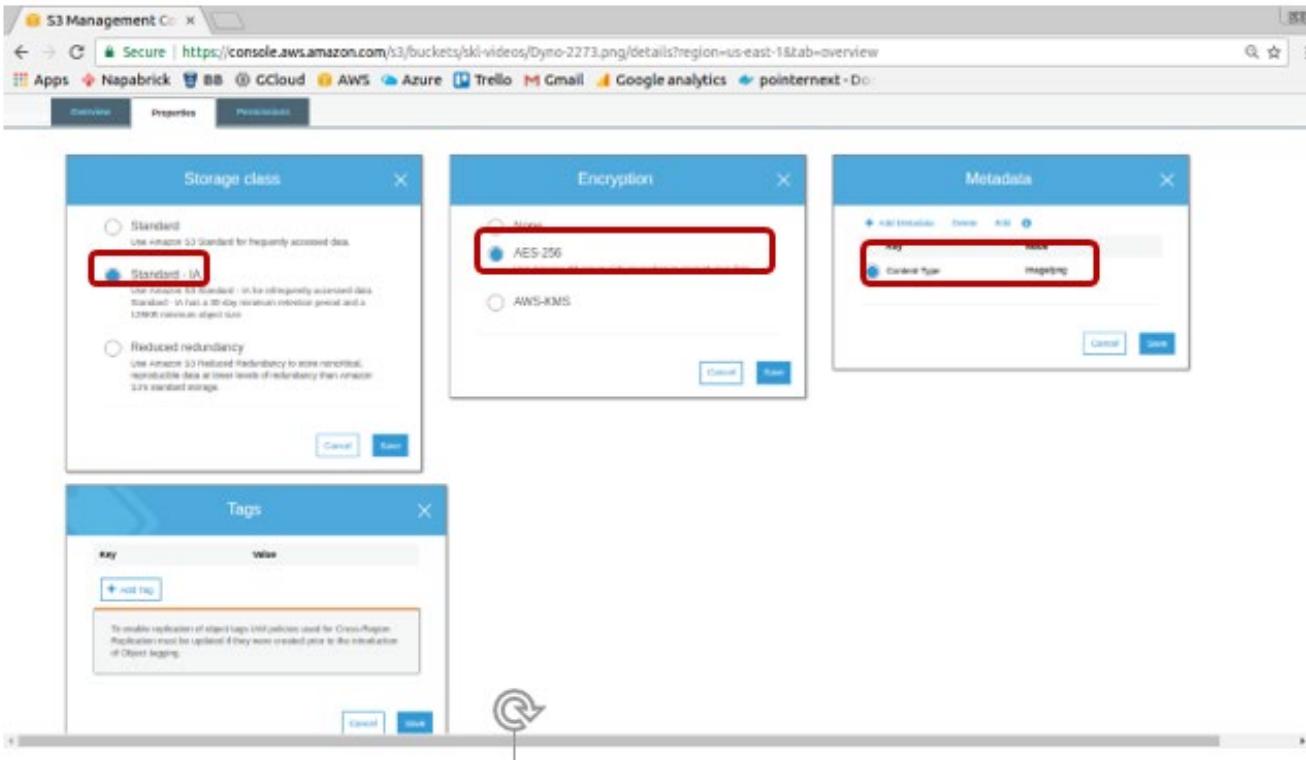
```
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>9DE33B33086CBF5C</RequestId>
  <><HostId>
    Fii0yLL1Y+C4E7PW4CEoTEgu4X9kW+HxvDif9ZAf73AQLqXrHHX1EUnncMJNqK9+TuXcu7boBv0=
  </HostId>
</Error>
```

Activity - S3

The screenshot shows the AWS S3 Management Console interface. On the left, there is a navigation bar with links like 'AWS', 'Services', 'Resource Groups', etc. Below it, the 'Amazon S3' section shows an object named 'AWS_pricing_v1.pdf'. The 'Properties' tab is currently active, with a red box highlighting the 'Make public' button. To the right, the 'Permissions' tab is also active, with a red box highlighting its header. A modal window titled 'Everyone' is displayed, showing access permissions for the object. Under 'Access to the object', the 'Read object' checkbox is checked and highlighted with a red box. At the bottom of the modal, there are 'Cancel' and 'Save' buttons.

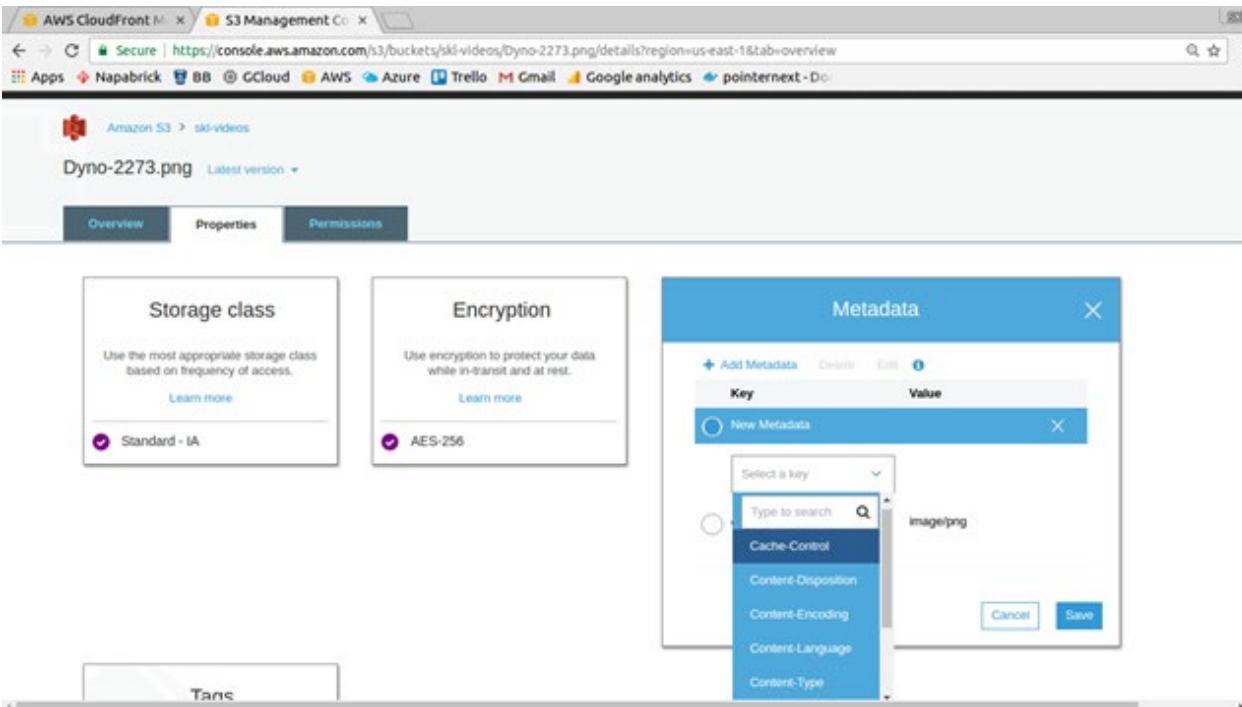
Now access the same link and we should be able to access the object

Activity - S3



Encryption will be at rest.

Activity - S3



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

Activity - S3

The screenshot shows the Amazon S3 Management Console interface. At the top, the URL is https://console.aws.amazon.com/s3/buckets/skl-videos/Dyno-2273.png/details?region=us-east-1&tab=overview. The navigation bar includes links for Apps, Napabrick, BB, GCloud, AWS, Azure, Trello, Gmail, Google analytics, and pointernext. Below the navigation bar, the main header shows 'Amazon S3' and the bucket name 'skl-videos'. The object name 'Dyno-2273.png' is displayed with a 'Latest version' link. A navigation bar at the top of the main content area includes 'Overview' (which is selected), 'Properties', and 'Permissions'.

Storage class
Use the most appropriate storage class based on frequency of access.
[Learn more](#)
 Standard - IA

Encryption
Use encryption to protect your data while in-transit and at rest.
[Learn more](#)
 AES-256

Metadata
Assign optional metadata to the object as a name-value (key-value) pair.
[Learn more](#)
 1 metadata

Tags
Tag objects to search, organize and manage access.
[Learn more](#)
 0 Tags

Storage and Content Delivery

S3 - version management

Activity - S3 versioning

The screenshot shows the AWS S3 Management Console with the URL <https://console.aws.amazon.com/s3/buckets/skl-videos/?region=us-east-1&tab=properties>. The 'Properties' tab is selected. A red box highlights the 'Amazon S3 > skl-videos' breadcrumb navigation path. On the left, a modal window titled 'Versioning' has its 'Enable versioning' button highlighted with a red box. The 'Logging' and 'Static website hosting' sections are also visible. Below the modal, the 'Advanced settings' section contains four cards: 'Tags', 'Cross-region replication', 'Transfer acceleration', and 'Events'. At the bottom, a summary bar shows 'Operations' (0 Tags, 0 in progress, 2 Success, 0 Error), 'Cross-region replication' (Disabled), 'Transfer acceleration' (Suspended), and 'Events' (0 Active notifications).

Versioning once enabled cannot be disabled.

Activity - S3 versioning

The screenshot shows the AWS S3 Management Console for the 'skl-src' bucket. The 'Permissions' tab is selected. A modal dialog for the 'Everyone' group is open, showing access permissions:

- This bucket will have public access:** Everyone will have access to one or all of the following: list objects, write objects, read and write permissions.
- Access to the objects:** List objects (highlighted with a red box)
- Access to this bucket's ACL:** Read bucket permissions (highlighted with a red box)

Below the modal, the main interface shows other permission settings:

- Owner access:** skroldslab has Yes for List objects, Write objects, and Read bucket permissions.
- Access for other AWS accounts:** An account named 'skroldslab' has Yes for List objects, Write objects, and Read bucket permissions.
- Public access:** The 'Everyone' group has Yes for List objects, Write objects, and Read bucket permissions. This row is highlighted with a red box.
- S3 log delivery group:** Log Delivery has No for all permissions.

Make the bucket public

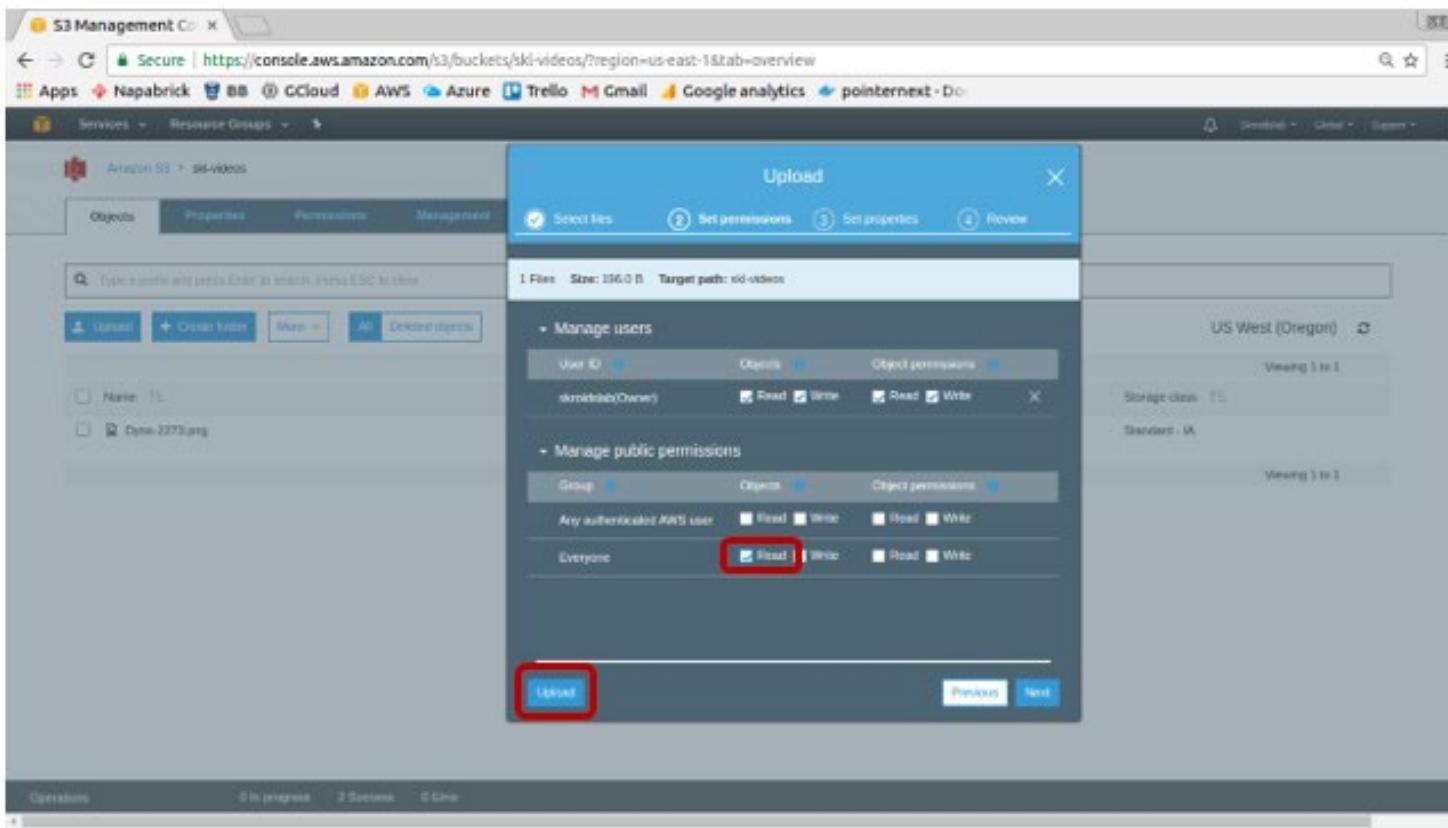
Activity - S3 versioning

The screenshot shows a Gedit text editor window titled "TextDocument.txt (/opt/Dropbox/1.Training/2.TrainingMaterial/Cloud/AWS) - gedit". The window has a dark theme. At the top, there are buttons for "Open" (with a dropdown arrow), "Save" (disabled), and other standard file operations. The main text area contains the following content:

```
Create a text file - TextDocument.txt
Write something here - version 1
A galaxy a system of millions or billions of stars, together with gas and dust, held together by gravitational
attraction.|
```

At the bottom of the window, there is a toolbar with buttons for "Plain Text" (with a dropdown arrow), "Tab Width: 8" (with a dropdown arrow), "Ln 5, Col 123" (with a dropdown arrow), and "INS".

Activity - S3 versioning



Activity - S3 versioning

The screenshot shows the AWS S3 Management Console with the URL <https://console.aws.amazon.com/s3/buckets/skl-videos/TextDocument.txt/details?region=us-east-1&tab=overview>. The file 'TextDocument.txt' is selected, and its details are displayed. A red box highlights the 'Last modified' timestamp 'Apr 10, 2017 11:01:59 AM (Latest version)'. Another red box highlights the 'Size' value '196'. The page includes standard S3 actions like Open, Download, Download as, and Make public.

Owner: skl-videos

Last activity: Apr 10, 2017 11:01:59 AM

Etag: 95c3400e5871343394cf0f0d6511be

Storage class: Standard

Server side encryption:

Size: 196

Version ID: fUvc7y5aDvYpxt2kfiaXxevrA09g

Link: <https://s3.us-west-2.amazonaws.com/skl-videos/TextDocument.txt>

Activity - S3 versioning

```
TextDocument.txt (/opt/Dropbox/1.Training/2.TrainingMaterial/Cloud/AWS) - gedit
Open Save
Create a text file - TextDocument.txt
Write something here - version 1
A galaxy a system of millions or billions of stars, together with gas and dust, held together by gravitational attraction.

A white dwarf, also called a degenerate dwarf, is a stellar core remnant composed mostly of electron-degenerate matter. A white dwarf is very dense: its mass is comparable to that of the Sun, while its volume is comparable to that of Earth.
|
```

Plain Text Tab Width: 8 Ln 8, Col 1 INS

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

Activity - S3 versioning

TextDocument.txt (Latest version)

Last modified	Version ID	Storage class
Apr 10, 2017 11:09:08 AM (Latest version)	YzgQ0juz2nwOJJDQACYIAJSD95Wh	Standard
Apr 10, 2017 11:01:00 AM	YzgQ0juz2nwOJJDQACYIAJSD95Wh	Standard

Owner: srujanlab

Last activity: Apr 10, 2017 11:09:08 AM

Size: 438

Version ID: YzgQ0juz2nwOJJDQACYIAJSD95Wh

Link: https://s3.us-east-1.amazonaws.com/ski-videos/TextDocument.txt

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

Activity - S3 versioning

The screenshot shows the AWS S3 Management Console interface. The URL in the browser is <https://console.aws.amazon.com/s3/buckets/skl-videos/?region=us-east-1&tab=overview>. The page displays the 'Objects' tab for the 'skl-videos' bucket. A context menu is open over the 'TextDocument.txt' file, with the 'Delete' option selected. The table lists two objects:

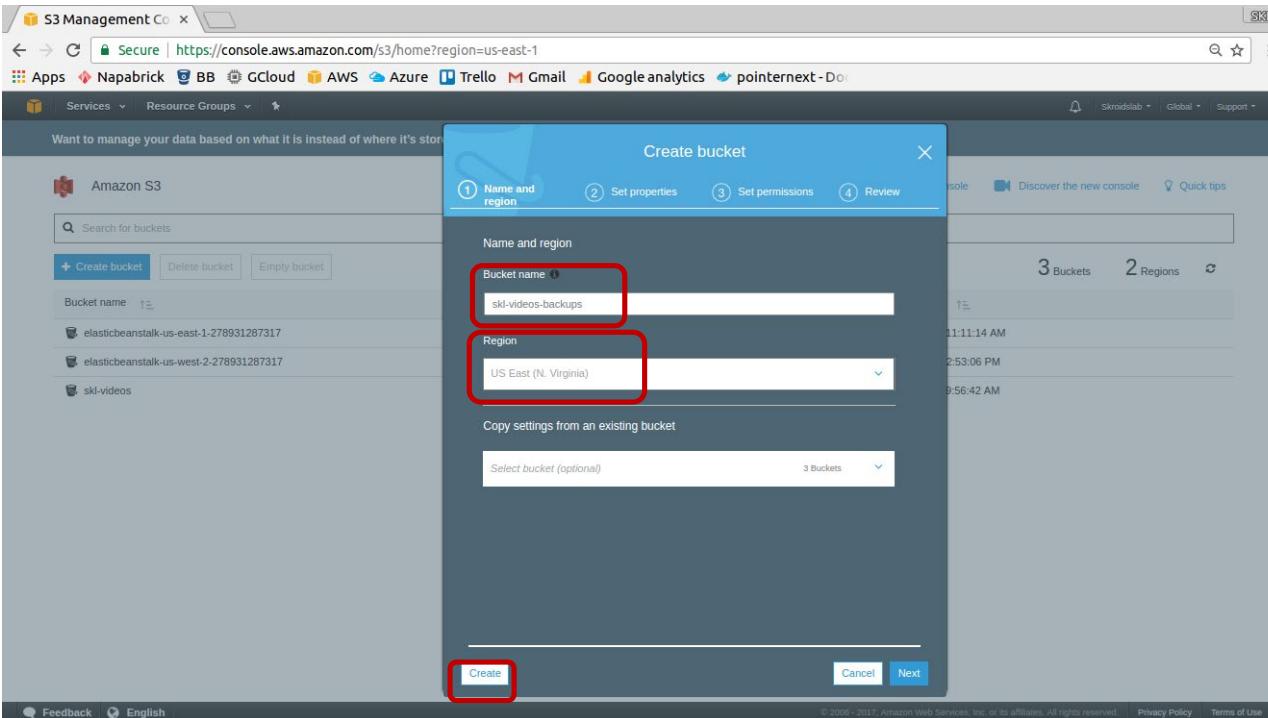
Name	Last modified	Size	Storage class
Dyno-2273.png	Apr 10, 2017 10:44:47 AM	111.6 KB	Standard - IA
TextDocument.txt	Apr 10, 2017 11:09:09 AM	439.0 B	Standard

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

Storage and Content Delivery

S3 - cross region replication

Activity - S3 Cross region replica



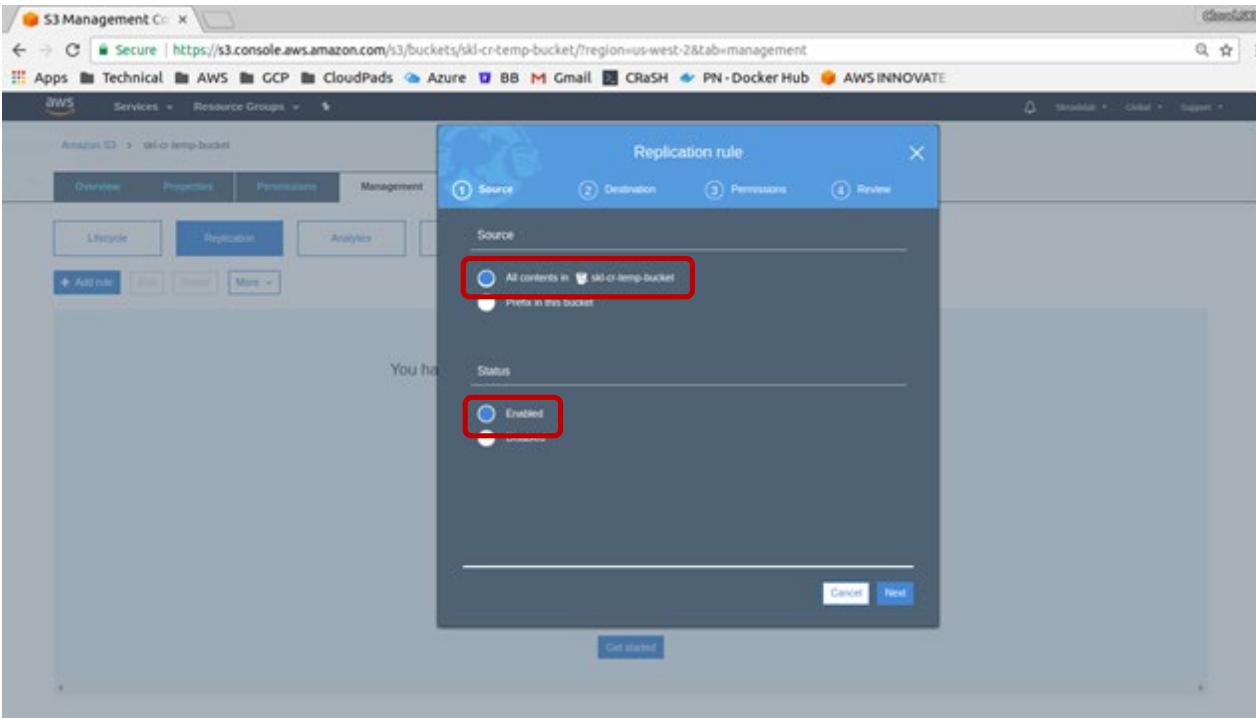
Create a new bucket in the east coast, go to properties and enable versioning

Activity - S3 Cross region replica

The screenshot shows the AWS S3 Management Console for a bucket named 'skl-src'. The 'Replication' tab is selected, indicated by a red box. Below it, a blue button labeled 'Add rule' is also highlighted with a red box. An orange arrow points from the text 'Both do the same' to this 'Add rule' button. The main content area displays a message: 'You haven't created any cross-region replication rules for this bucket.' It features a globe icon and a section titled 'Cross-region replication' with the subtext: 'Cross-region Replication enables automatic and asynchronous copying of objects across buckets in different AWS regions.' A 'Learn more' link and a 'Get started' button are also present.

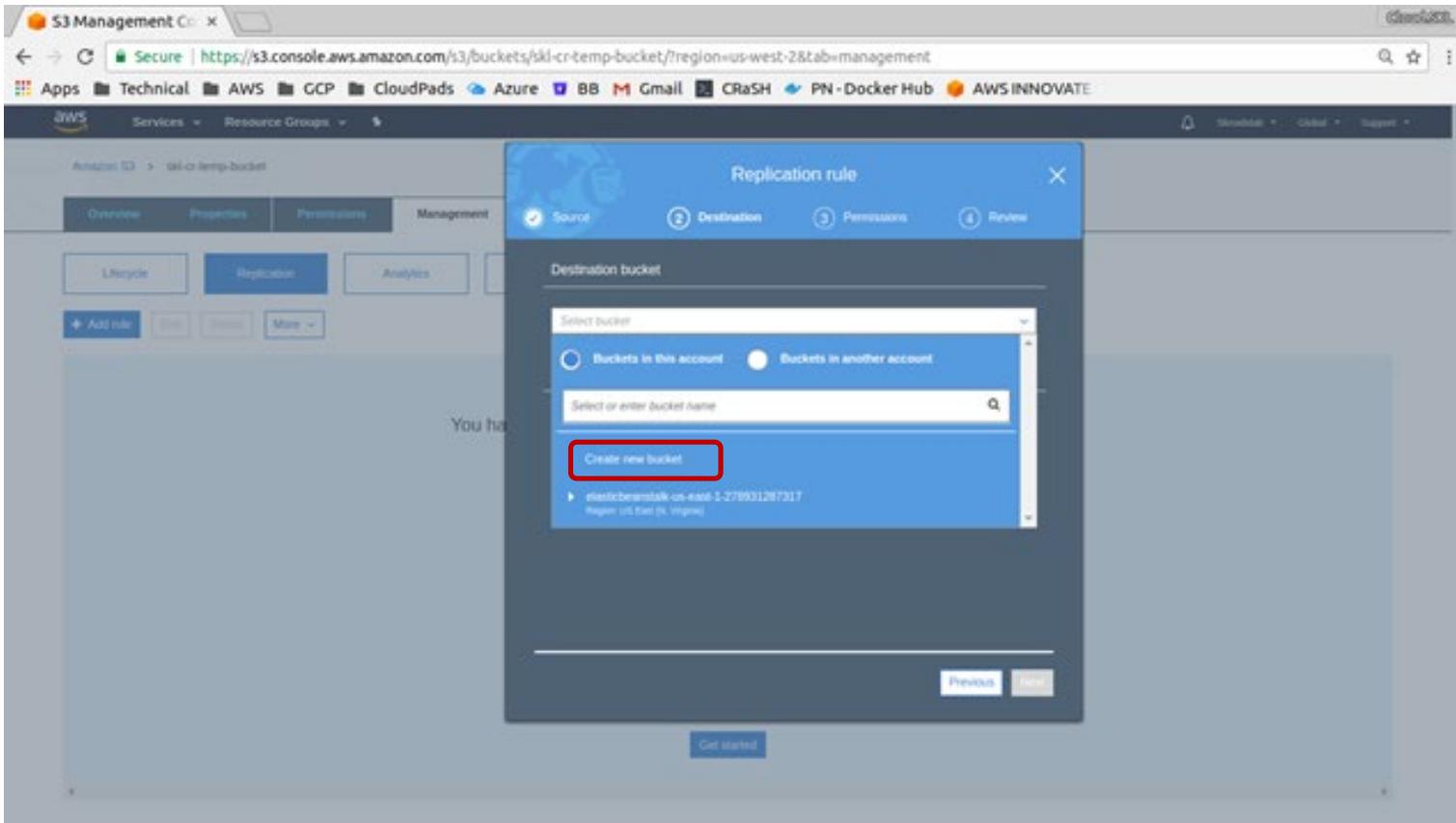
Both do the same

Activity - S3 Cross region replica

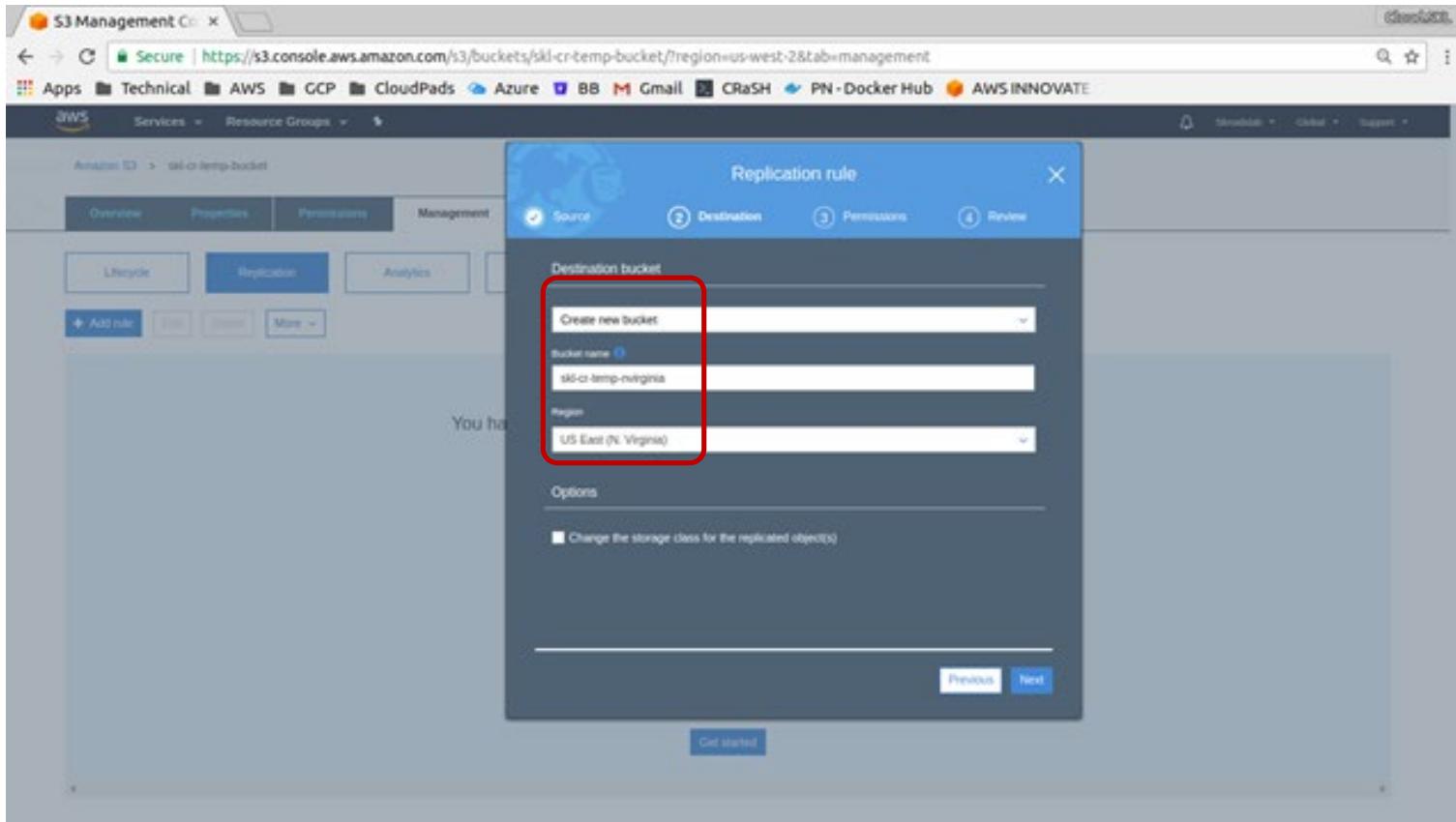


Existing objects will not be replicated! Upload another version of the galaxy txt file and you will find ALL previous versions will be replicated. Multi region replication and replication chaining is not supported.

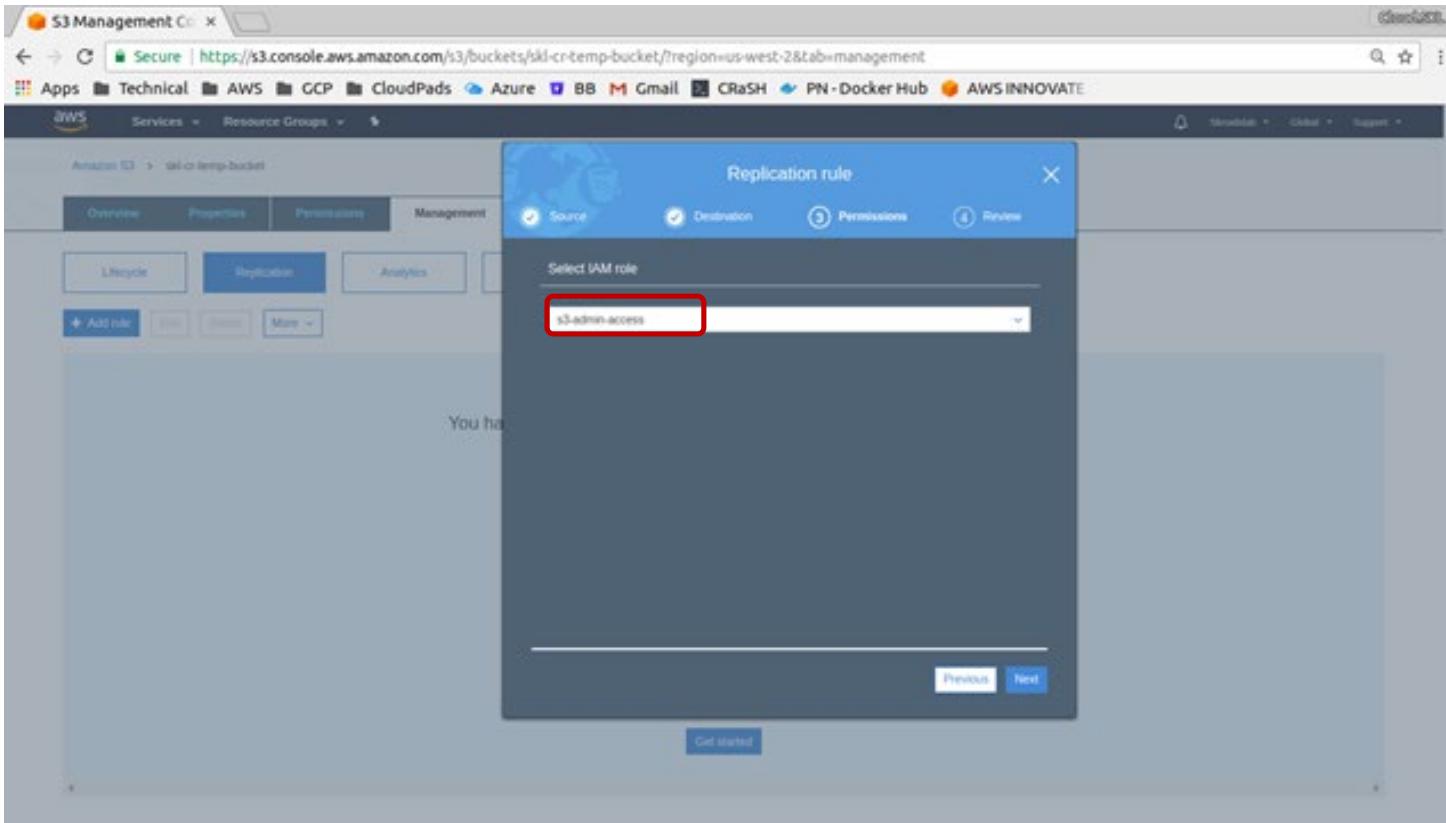
Activity - S3 Cross region replica



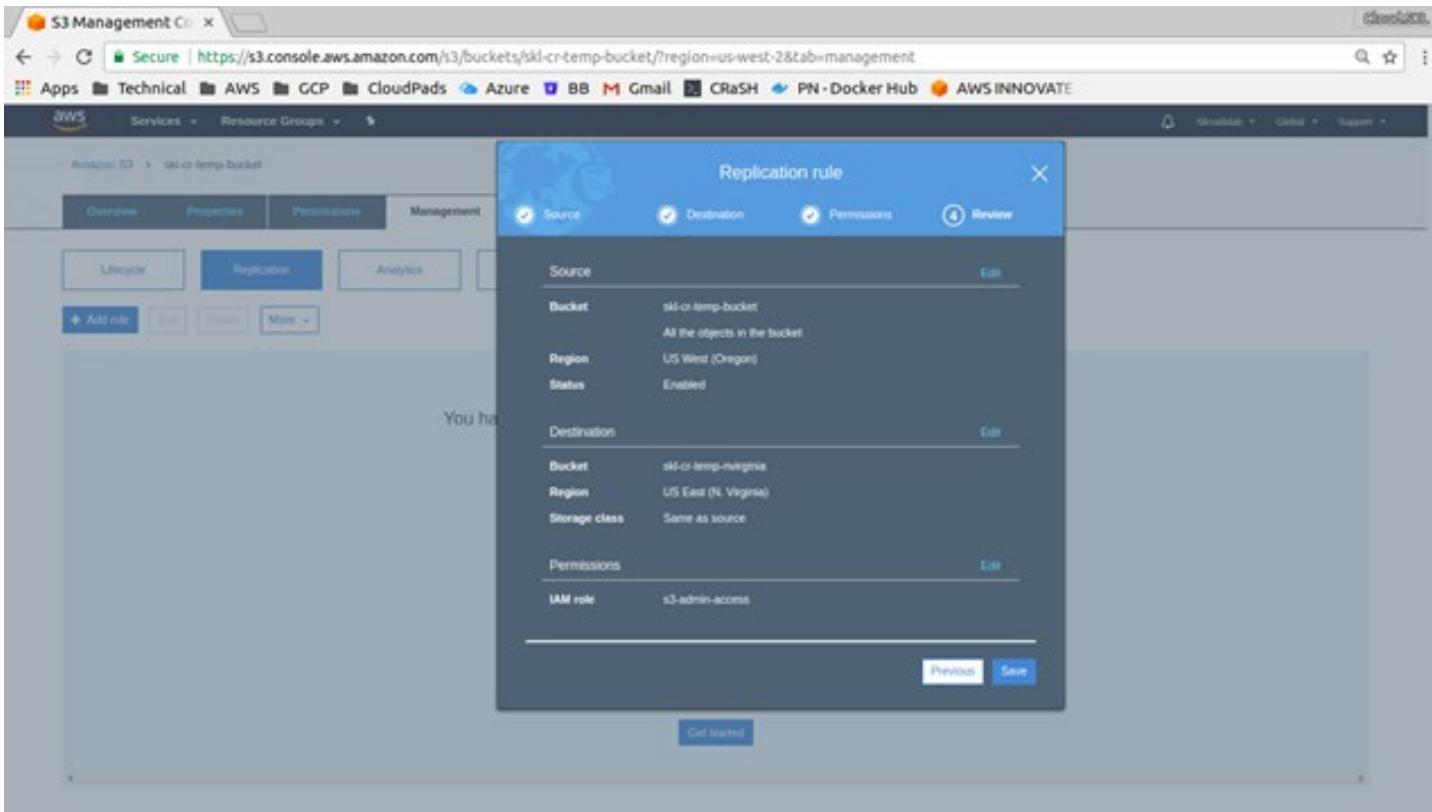
Activity - S3 Cross region replica



Activity - S3 Cross region replica



Activity - S3 Cross region replica



Activity - S3 Cross region replica

The screenshot shows the AWS S3 Management Console for the bucket 'skl-cr-temp-bucket'. The 'Management' tab is selected, and the 'Replication' sub-tab is active. A table displays the replication rule:

Source	Destination	Permissions
Scope All contents in the bucket	Bucket skl-cr-temp-nvirginia	IAM role s3-admin-access
Region US West (Oregon)	Region US East (N. Virginia)	Bucket policy Copy

Below the table, there are buttons for '+ Add rule', 'Edit', 'Delete', and 'More'. At the bottom, a summary row shows: Source (Entire bucket), Status (Enabled), and Storage Class (Same as source).

Storage and Content Delivery

S3 - Lifecycle management

Activity - S3 lifecycle

The screenshot shows the AWS S3 Management Console interface. At the top, the URL is https://console.aws.amazon.com/s3/buckets/skl-videos/?region=us-east-1&tab=management. The left sidebar shows 'Amazon S3' and 'skl-videos'. The main navigation bar has tabs: Objects, Properties, Permissions, and Management. The 'Management' tab is selected. Below it, there are four buttons: Lifecycle (highlighted with a red box), Analytics, Metrics, and Inventory.

The 'Lifecycle' section contains a button '+ Add lifecycle rule' which is also highlighted with a red box. Below this, a message says: 'There is no lifecycle rule applied to this bucket. Here is how to get started.' It features three cards:

- Use lifecycle rules to manage your objects**: Shows an icon of a computer monitor with a gear. Text: 'You can manage an object's lifecycle by using a lifecycle rule, which defines how Amazon S3 manages objects during their lifetime.' Buttons: 'Learn more' and 'Operations' (0 In progress, 1 Success, 1 Error).
- Automate transition to tiered storage**: Shows an icon of two stacked cylinders with gears. Text: 'Lifecycle rules enable you to automatically transition objects to the Standard - IA and/or to the Amazon Glacier storage class.' Buttons: 'Learn more' and 'Operations' (0 In progress, 1 Success, 1 Error).
- Expire your objects**: Shows an icon of a trash bin with dashed lines. Text: 'Using a lifecycle rule, you can automatically expire objects based on your retention needs or clean up incomplete multipart uploads.' Buttons: 'Learn more' and 'Operations' (0 In progress, 1 Success, 1 Error).

Activity - S3 lifecycle

The screenshot shows the AWS S3 Management Console interface for creating a new lifecycle rule. The main navigation bar at the top includes links for Secure, Apps, Napabrick, BB, GCloud, AWS, Azure, Trello, Gmail, Google analytics, and pointernext-Doc.

The left sidebar shows the bucket 'ski-videos' with tabs for Objects, Properties, Permissions, and Management. The Management tab is selected, and the Lifecycle sub-tab is active. A button labeled '+ Add lifecycle rule' is visible.

A modal window titled 'Lifecycle rule' is open, divided into four steps: 1. Name and scope, 2. Transitions, 3. Expiration, and 4. Review. Step 1 is currently active, with the sub-step 'Enter a rule name' highlighted. The rule name 'Recycle-1' is entered in the input field. Below it is a section for 'Add filter to limit scope to prefix/tag' with a placeholder 'Type to add prefix/tag filter'.

In the background, there are three informational cards: 'Use lifecycle rules to manage your objects', 'Expire your objects', and another partially visible card about managing multipart uploads.

Activity - S3 lifecycle

The screenshot shows the AWS S3 Management Console with the URL <https://console.aws.amazon.com/s3/buckets/skl-videos/?region=us-east-1&tab=management>. The main interface has tabs for 'Lifecycle' and 'Analytics'. A modal window titled 'Lifecycle rule' is open, currently on step 2 'Transitions'. The modal title is 'Configure transition'.

Current version Previous versions

For current version of objects

Object creation Days after object creation

+ Add transition

Transition to Standard-IA after 30

Transition to Amazon Glacier after 60

For previous versions of objects

You don't have any transitions set up for previous versions of objects.

Previous Next

On the left, there's a sidebar with the text 'Use lifecycle rules to manage your objects' and 'You can manage an object's lifecycle by using a lifecycle rule, which defines how Amazon S3 manages objects during their lifetime.' Below it are 'Learn more' and 'Operations' (0 In progress, 1 Success, 1 Error).

On the right, there's a section titled 'Expire your objects' with the text 'With a lifecycle rule, you can automatically expire objects based on age or storage class, or clean up incomplete multipart uploads.' Below it is 'Learn more'.

Activity - S3 lifecycle

The screenshot shows the AWS S3 Management Console with the URL <https://console.aws.amazon.com/s3/buckets/skl-videos/?region=us-east-1&tab=management>. A modal window titled "Lifecycle rule" is open, showing the "Transitions" step. The rule is defined for "For previous versions of objects". It includes two transitions:

- Transition to Standard-IA after 30 days
- Transition to Amazon Glacier after 59 days

A validation error message is displayed for the second transition: "An object must remain in the Standard-IA storage class for a minimum of 30 days before transitioning to the Glacier storage class. Enter an integer value greater than or equal to 60".

Below the modal, the main S3 management interface shows sections for "Use lifecycle rules to manage your objects" and "Expire your objects".

Activity - S3 lifecycle

The screenshot shows the AWS S3 Management console with the URL <https://console.aws.amazon.com/s3/buckets/s3l-videos/?region=us-east-1&tab=management>. A modal window titled "Lifecycle rule" is open, showing the "Expiration" step (step 3 of 4). The configuration includes:

- Configure expiration:**
 - Current version
 - Previous versions
 - Expire current version of object
- After days from object creation
- Permanently delete previous versions
- After days from becoming a previous version
- Clean up expired object delete markers and incomplete multipart uploads:**
 - Clean up expired object delete markers

A note at the bottom states: "You cannot enable clean up expired object delete markers if you enable Expiration."

At the bottom of the modal are "Previous" and "Next" buttons.

Below the modal, the main S3 Management interface shows the following statistics:
Operations: 0 In progress, 1 Success, 1 Error
Feedback: English

Activity - S3 lifecycle

The screenshot shows the AWS S3 Management Console with a modal dialog titled "Lifecycle rule". The dialog is divided into four tabs: "Name and scope" (selected), "Transitions", "Expiration", and "Review".

Name and scope:

- Name: Lifecycle-1
- Scope: Whole bucket

Transitions:

- For current version of objects:
 - Transition to Standard-IA after 30 days
 - Transition to Amazon Glacier after 60 days
- For previous versions of objects:
 - Transition to Standard-IA after 30 days
 - Transition to Amazon Glacier after 60 days

Expiration:

- Expire after 425 days
- Permanently delete after 425 days

Review:

Next Step: Save

The background of the console shows a sidebar with "Operations" and status metrics: 0 In progress, 1 Success, 1 Error.

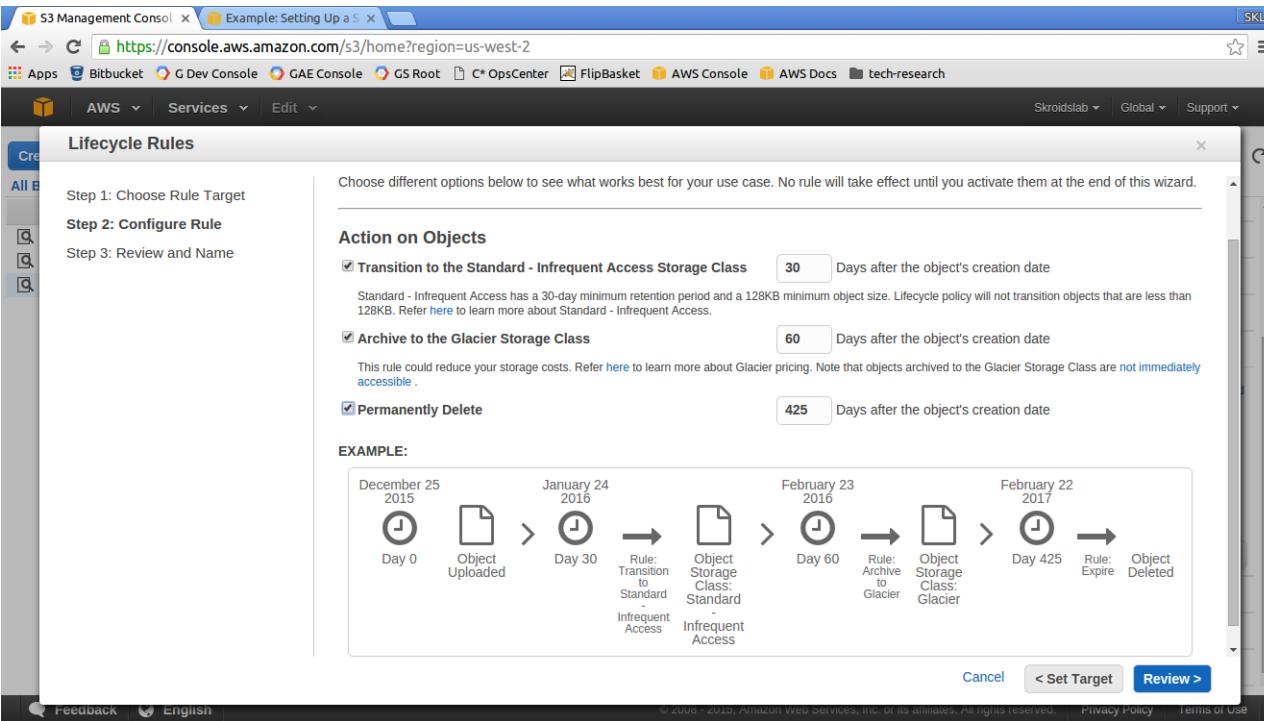
Activity - S3 lifecycle

The screenshot shows the AWS S3 Management Console interface. The URL in the browser is <https://console.aws.amazon.com/s3/buckets/s3-videos?region=us-east-1&tab=management>. The navigation bar includes links for Apps, Napabrick, BB, GCloud, AWS, Azure, Trello, Gmail, Google analytics, and pointernext. The main menu has options for Services, Resource Groups, and Management. The Management tab is selected, showing tabs for Objects, Properties, Permissions, and Management. The Management tab is further divided into Lifecycle, Analytics, Metrics, and Inventory. The Lifecycle tab is selected. A button for '+ Add lifecycle rule' is visible. Below it, there is a table listing a single lifecycle rule:

Lifecycle rule	Applied to	Transitions for current version	Transitions for previous version(s)
Recycle-1	Whole bucket	Standard-IA / Amazon Glacier / Expire	Standard-IA / Amazon Glacier / Permanently Delete

At the bottom of the page, there is a footer with status indicators: Operations (0 In progress, 1 Success, 1 Error).

Activity - S3 lifecycle (old UI)



Activity - S3 lifecycle (old UI)

S3 Management Console < https://console.aws.amazon.com/s3/home?region=us-west-2# AWS Bitbucket G Dev Console GAE Console GS Root OpsCenter FlipBasket AWS Console AWS Docs tech-research Skroidslab Global Support

Lifecycle Rules

Step 1: Choose Rule Target
Step 2: Configure Rule
Step 3: Review and Name

EXAMPLE:

December 26 2015
Day 0
Object Uploaded (Current Version) > January 25 2016
Day 30
Rule: Transition to Standard - Infrequent Access
Current Version Storage Class: Standard - Infrequent Access
February 24 2016
Day 60
Rule: Archive to Glacier
Current Version Storage Class: Glacier
February 23 2017
Day 425
Rule: Expire
Delete Marker Overwrites Current Version

Action on Previous Versions

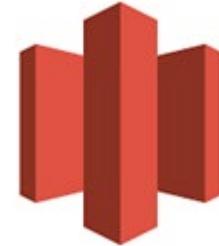
Transition to the Standard - Infrequent Access Storage Class Days after becoming a previous version
Standard - Infrequent Access has a 30-day minimum retention period and a 128KB minimum object size. Lifecycle policy will not transition objects that are less than 128KB. Refer [here](#) to learn more about Standard - Infrequent Access.

Archive to the Glacier Storage Class Days after becoming a previous version
This rule could reduce your storage costs. Refer [here](#) to learn more about Glacier pricing. Note that objects archived to the Glacier Storage Class are [not immediately accessible](#).

Permanently Delete Days after becoming a previous version

Cancel < Set Target Review >

Feedback English © 2006 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use



Storage and Content Delivery

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

The screenshot shows the 'Create Vault' wizard on the Amazon Glacier Management console. The left sidebar lists steps: Step 1: Vault Name (selected), Step 2: Event Notifications, Step 3: Event Notification Details, and Step 4: Review. The main content area is titled 'Welcome to Amazon Glacier'. It explains that data is stored in 'archives' and provides details about archive sizes and immutability. A callout box points to the 'Region' field, which is set to 'US East (N. Virginia)'. The 'Vault Name*' field contains 'skd-video-vault'. At the bottom right are 'Cancel' and 'Next Step' buttons.

Glacier Management x

Secure | https://console.aws.amazon.com/glacier/home?region=us-east-1#/wizard

Apps Napabrick BB GCloud AWS Azure Trello Gmail Google analytics pointernext -Do

Services Resource Groups

Create Vault

Welcome to Amazon Glacier

Data is stored in Amazon Glacier in "archives." An archive can be any data such as a photo, video, or document. You can upload a single file as an archive or aggregate multiple files into a TAR or ZIP file and upload as one archive.

A single archive can be as large as 40 terabytes. You can store an unlimited number of archives and an unlimited amount of data in Amazon Glacier. Each archive is assigned a unique archive ID at the time of creation, and the content of the archive is immutable, meaning that after an archive is created it cannot be updated.

Vaults allow you to organize your archives and set access policies and notification policies. Get started by giving your vault a name. You can then create your vault now or click Next Step to set up your vault's properties.

Region: US East (N. Virginia)

Vault Name*: skd-video-vault

The AWS Region that your vault will be located in. Use the Region drop-down menu to create vaults in other Regions.

Cancel Next Step

Feedback English

© 2006 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Activity - Glacier

The screenshot shows a web browser window for the AWS Glacier Management Console. The URL in the address bar is <https://us-west-2.console.aws.amazon.com/glacier/home?region=us-west-2#/wizard>. The browser's navigation bar includes links for Apps, Bitbucket, G Dev Console, GAE Console, GS Root, C* OpsCenter, FlipBasket, AWS Console, AWS Docs, and tech-research. The AWS logo is in the top left, and the region is set to Oregon.

Create Vault

Step 1: Vault Name
Step 2: Event Notifications
Step 3: Event Notification Details
Step 4: Review

Set Event Notifications

You can choose to have notifications sent to you or your application whenever certain Amazon Glacier jobs complete. Notifications are sent using the Amazon Simple Notifications Service (SNS). To use Amazon SNS, you first need to specify a topic that applications or people can subscribe to. You can then select specific jobs that, on completion, will trigger the notifications. Notifications can be delivered over the protocol of your choice (HTTP, email, etc.).

Do not enable notifications
You can enable, set up, and change your notification settings later.

Enable notifications and create a new SNS topic
Enable notifications and create a new Amazon SNS topic to send the notifications.

Enable notifications and use an existing SNS topic
Enable notifications and enter an existing SNS topic to send the notifications.

Cancel **Previous** **Next Step**

Activity - Glacier

The screenshot shows a web browser window for the AWS Glacier Management Console. The URL in the address bar is <https://us-west-2.console.aws.amazon.com/glacier/home?region=us-west-2#/wizard>. The browser's navigation bar includes links for Apps, Bitbucket, G Dev Console, GAE Console, GS Root, C* OpsCenter, FlipBasket, AWS Console, AWS Docs, and tech-research. The AWS logo, Services dropdown, and Edit button are also visible.

The main content area is titled "Create Vault". On the left, a vertical sidebar lists the steps: Step 1: Vault Name, Step 2: Event Notifications, Step 3: Event Notification Details, and Step 4: Review. The "Review" step is currently selected.

The "Review" section contains the following information:

- Region: us-west-2
- Vault Name: SKLVideosArchiva

At the bottom right of the review section are three buttons: "Cancel", "Previous", and "Submit".

At the very bottom of the page, there is a footer bar with links for Feedback, English, Privacy Policy, and Terms of Use. The footer also includes a copyright notice: "© 2006 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved."

Activity - Glacier

The screenshot shows the AWS Glacier Management Console interface. At the top, there's a navigation bar with links like 'AWS', 'Services', and 'Edit'. Below it, the main title is 'Amazon Glacier Vaults'. There are three buttons: 'Create Vault', 'Delete Vault', and 'Settings'. A 'Filter By Name:' input field is present. The main table lists one vault:

Name	Inventory Last Updated	Size (as of last inventory)	# of Archives (as of last inventory)
SKLVideosArchiva	Not updated yet	--	--

Below the table, a modal window is open for the 'SKLVideosArchiva' vault. It shows the following details:

Details	Notification	Permissions	Vault Lock	Tags
Region: us-west-2				
Created on: Sat, December 26, 2015 11:41:30 AM UTC-8				
ARN: arn:aws:glacier:us-west-2:278931287317:vaults/SKLVideosArchiva				
Inventory Last Updated: Not updated yet				

At the bottom of the modal, it says 'Vault Details as of the last inventory update:' followed by 'Size: --' and '# of Archives: --'.

Activity - Glacier

The screenshot shows the 'Data Retrieval Policy' dialog box over a background of the AWS Glacier Management console. The dialog box contains three policy options:

- Free Tier Only**: Only retrieve data within the free tier. Data retrieval requests that exceed the free tier will not be accepted.
- Max Retrieval Rate**: Data retrieval requests that would exceed the specified maximum retrieval rate below will not be accepted. A slider is set to 1 GB/Hour.
- No Retrieval Limit**: All valid data retrieval requests will be accepted. Data Retrieval cost will vary based on your usage.

Below the policies, it says "Retrieval Cost Free" and "Retrieval Cost \$7.20 / month or less". A note at the bottom states: "Note: Data retrieval policies govern all retrieval activities in a region. The retrieval cost estimates may not reflect previously incurred usage or charges in the month. [Learn more](#)".

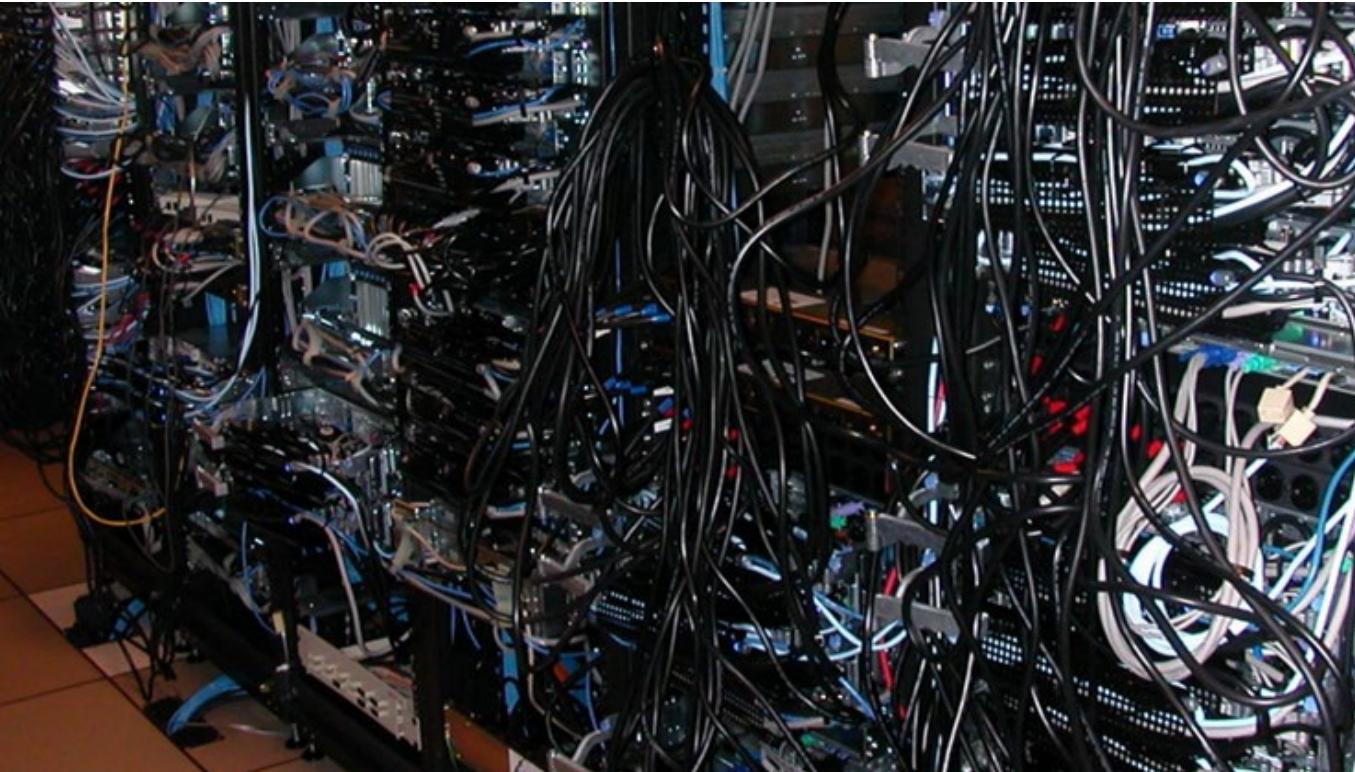
At the bottom right of the dialog box are "Cancel" and "Save" buttons.



Networking

VPC

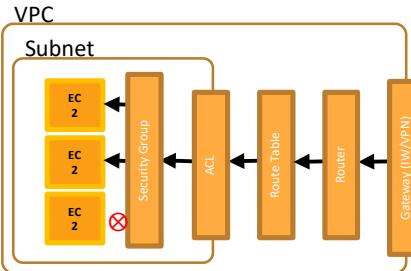
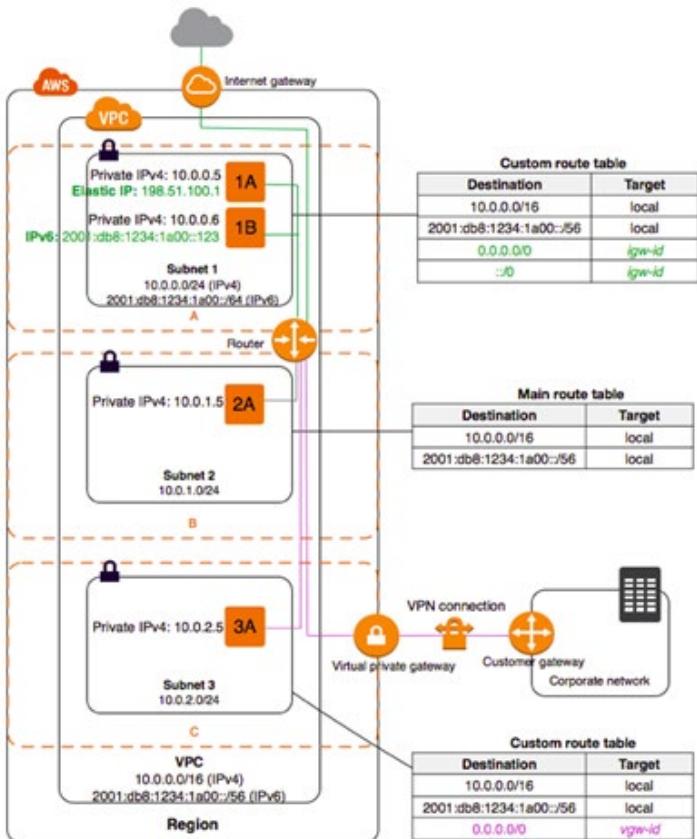
Let's talk about this ...



VPC - Virtual Private Cloud

- 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

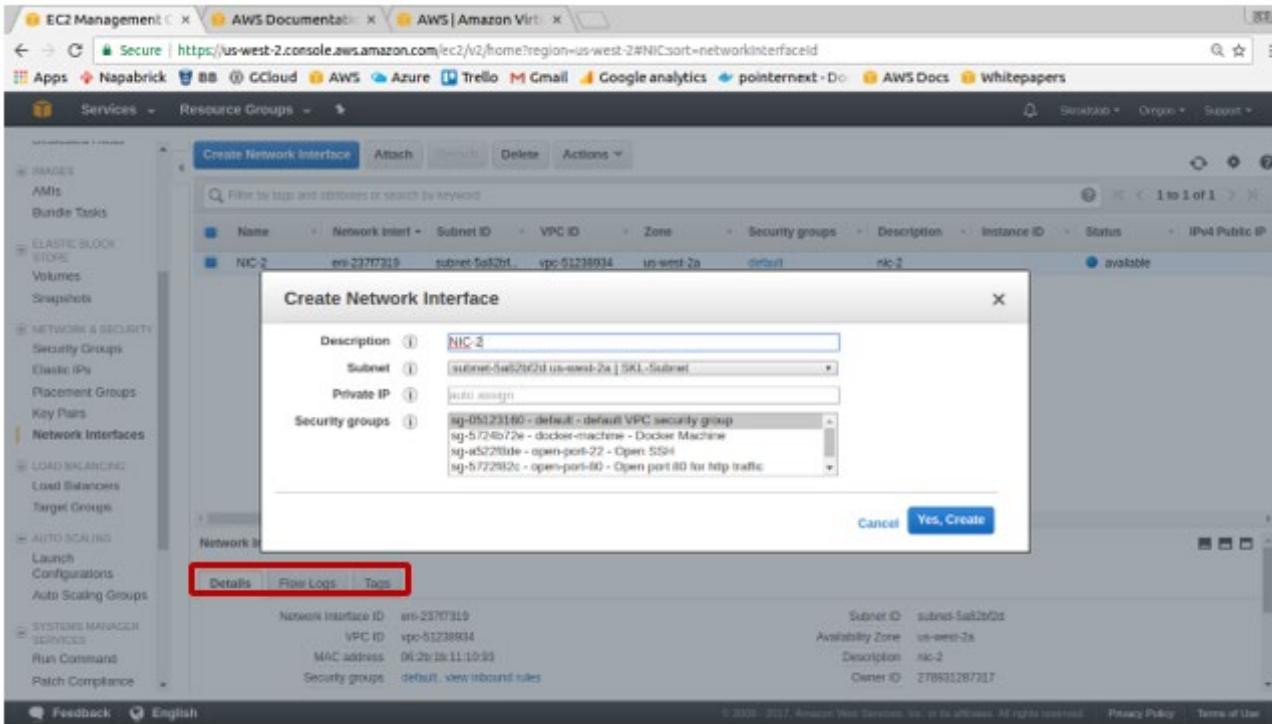


- AWS provides two features that you can use to increase security in your VPC**
 - Security groups control inbound and outbound traffic for your instances (stateful)**
 - Network ACLs control inbound and outbound traffic for your subnets (stateless)**
- Every subnet that you create is automatically associated 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**

- 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

The screenshot shows the AWS EC2 Management console interface. The user is in the 'Launch Instance Wizard' at Step 3: Configure Instance Details. The 'Subnet' dropdown is highlighted with a red box, showing 'subnet-5a82bf2d | SKL-Subnet | us-west-2a' and '4096 IP Addresses available'. Below it, the 'Auto-assign Public IP' dropdown is set to 'Disable'. Under 'Network interfaces', the 'Device' column shows 'eth0' and the 'Network Interface' column shows 'eni-237f7319 (NIC-2)'. At the bottom, there are buttons for 'Cancel', 'Previous', 'Review and Launch' (which is blue), and 'Next: Add Storage'.

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)

The screenshot shows the AWS VPC Management console interface. On the left, there's a sidebar with various navigation links under 'Virtual Private Cloud' and 'Your VPCs'. The 'Your VPCs' link is highlighted with a red box. In the main content area, there's a summary of resources: 1 VPC, 1 Internet Gateway, 4 Subnets, 1 Route Table, 0 Elastic IPs, 0 Endpoints, 0 Security Groups, 0 VPN Connections, and 0 Customer Gateways. Below this, there's a 'VPN Connections' section with a 'Create VPN Connection' button.

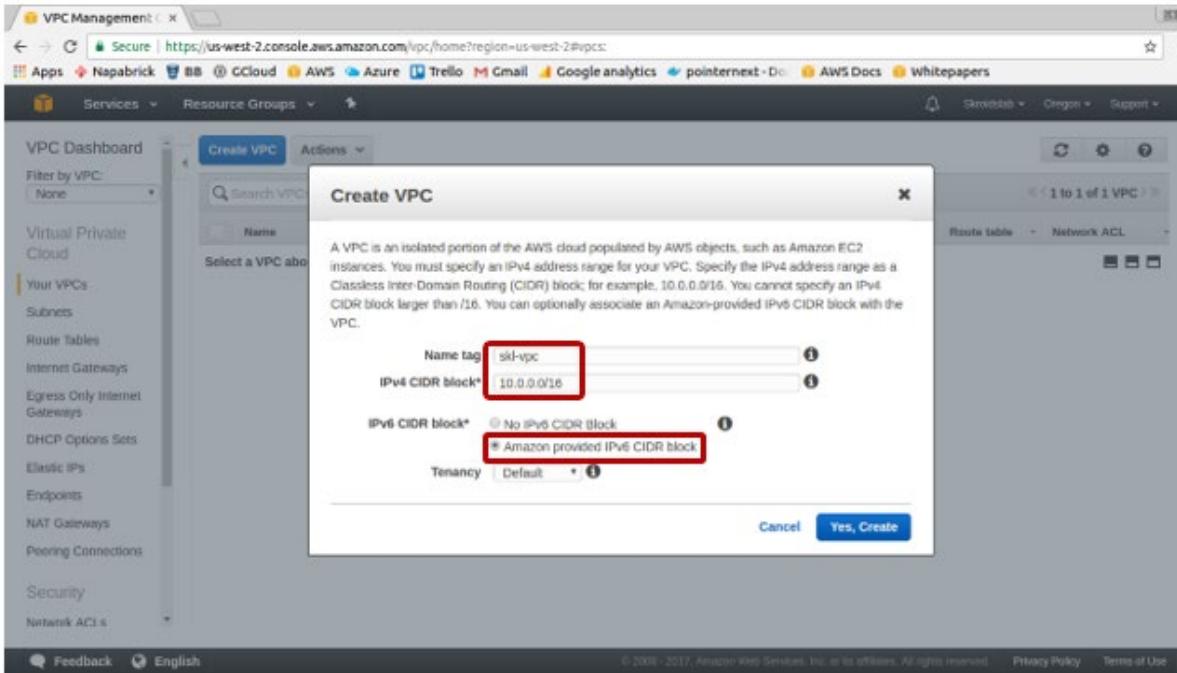
Service Health

Current Status	Details
● Amazon VPC - US West (Oregon)	Service is operating normally
● Amazon EC2 - US West (Oregon)	Service is operating normally

Additional Information

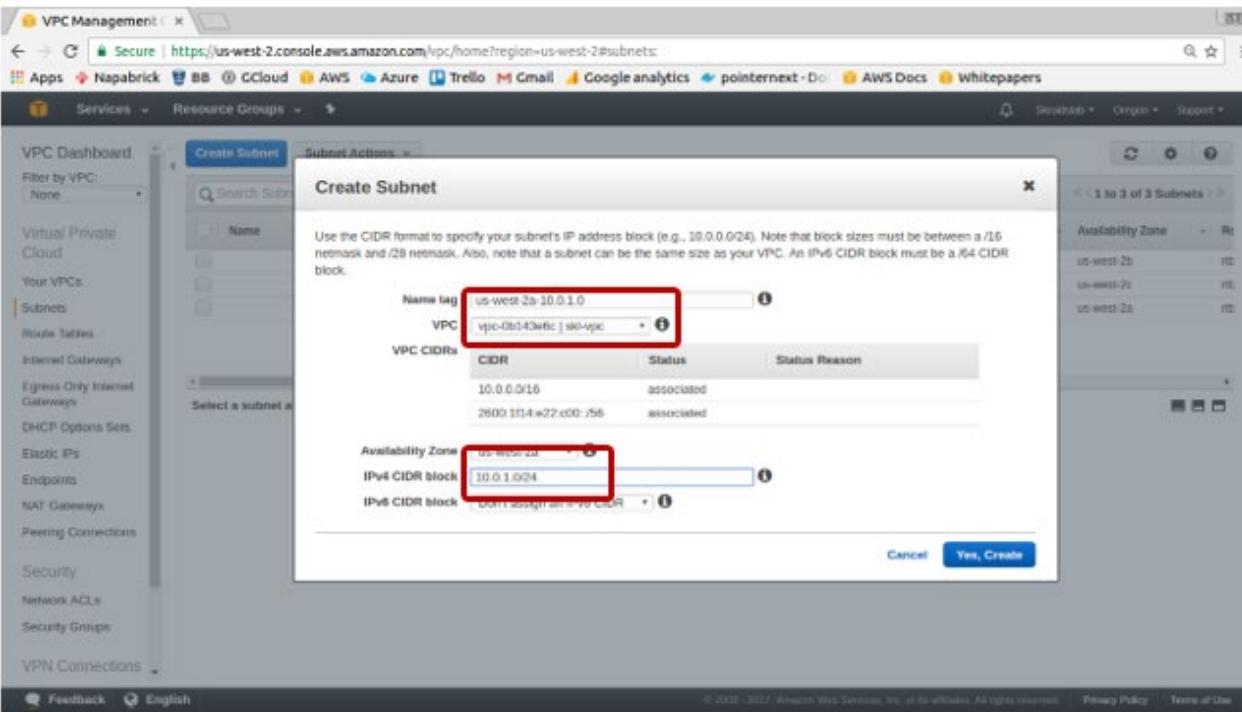
- VPC Documentation
- All VPC Resources
- Forum
- Report an issue

Activity - VPC



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

Activity - Subnet (Availability Zone)



**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

The screenshot shows the AWS VPC Management console with the URL <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#subnets>. The left sidebar lists various VPC-related resources. The main area displays a table of subnets:

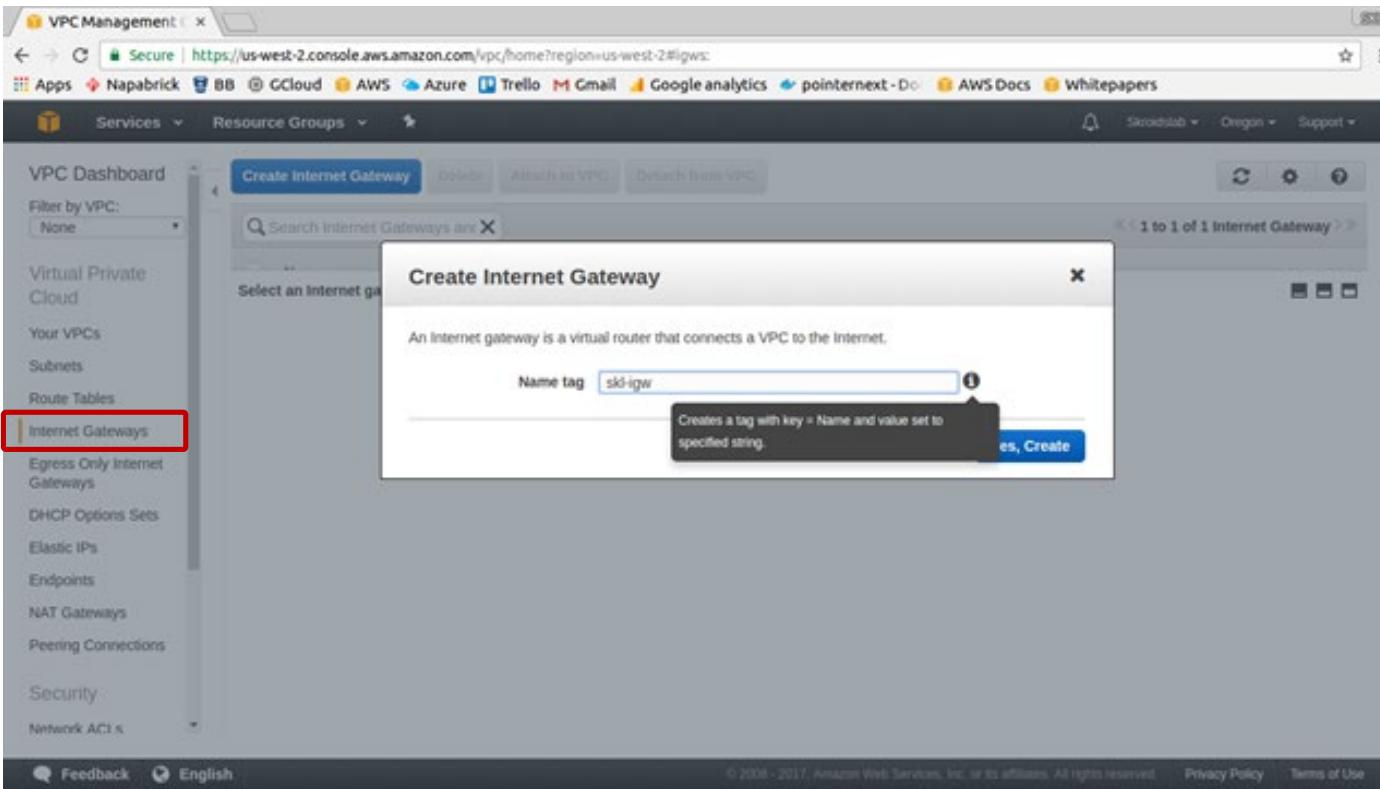
Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Region
us-west-2b-10.0.2.0	subnet-58d99f3f	available	vpc-0b143e6c sk8-vpc	10.0.2.0/24	251		us-west-2b	US West (N. California)
us-west-2a-10.0.1.0	subnet-28990181	available	vpc-0b143e6c sk8-vpc	10.0.1.0/24	251		us-west-2a	US West (N. California)
	subnet-fa9219f1	available	vpc-51238934 DefaultVPC	172.31.32.0/20	4091		us-west-2b	US West (N. California)
	subnet-ee30f1b7	available	vpc-51238934 DefaultVPC	172.31.0.0/20	4091		us-west-2c	US West (N. California)
	subnet-22b21155	available	vpc-51238934 DefaultVPC	172.31.16.0/20	4091		us-west-2a	US West (N. California)

Below the table, details for the subnet **subnet-58d99f3f | us-west-2b-10.0.2.0** are shown:

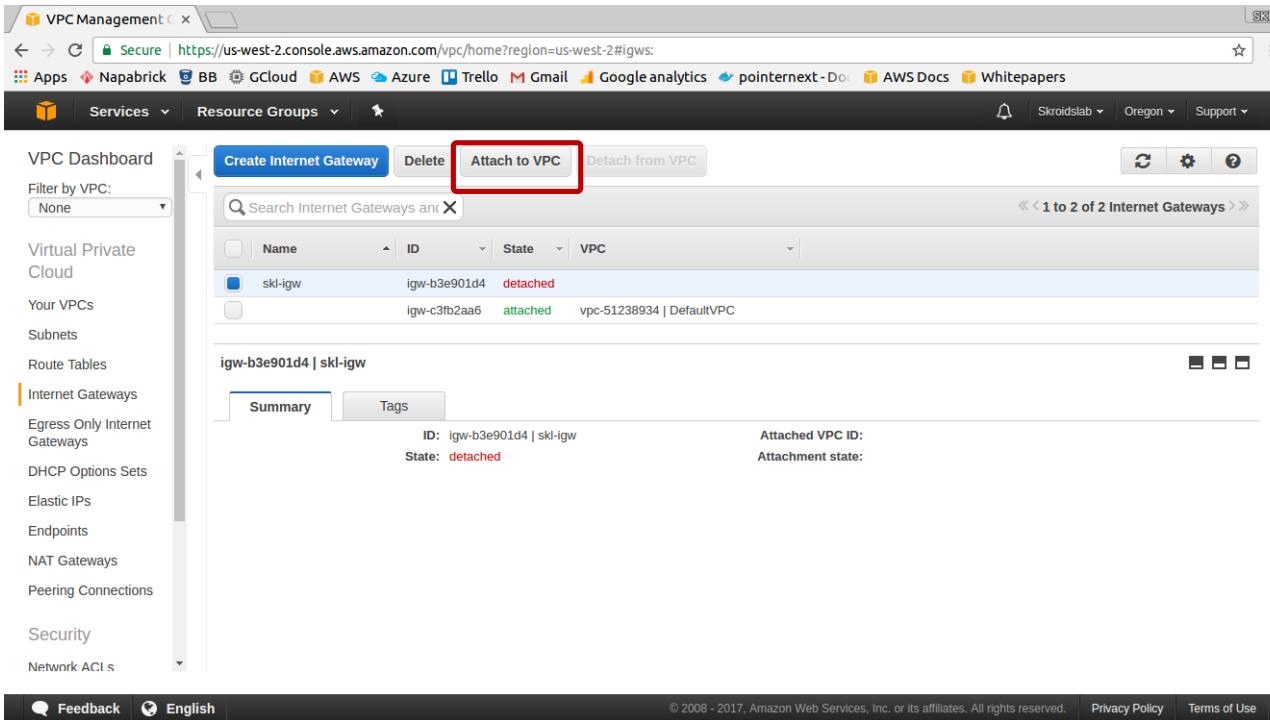
- Summary tab selected.
- Route Table: rtb-81805ae7
- Network ACL: acl-d98f505f
- Default subnet: no
- Auto-assign Public IP: no
- Auto-assign IPv6 address: no

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

Activity - Internet Gateway

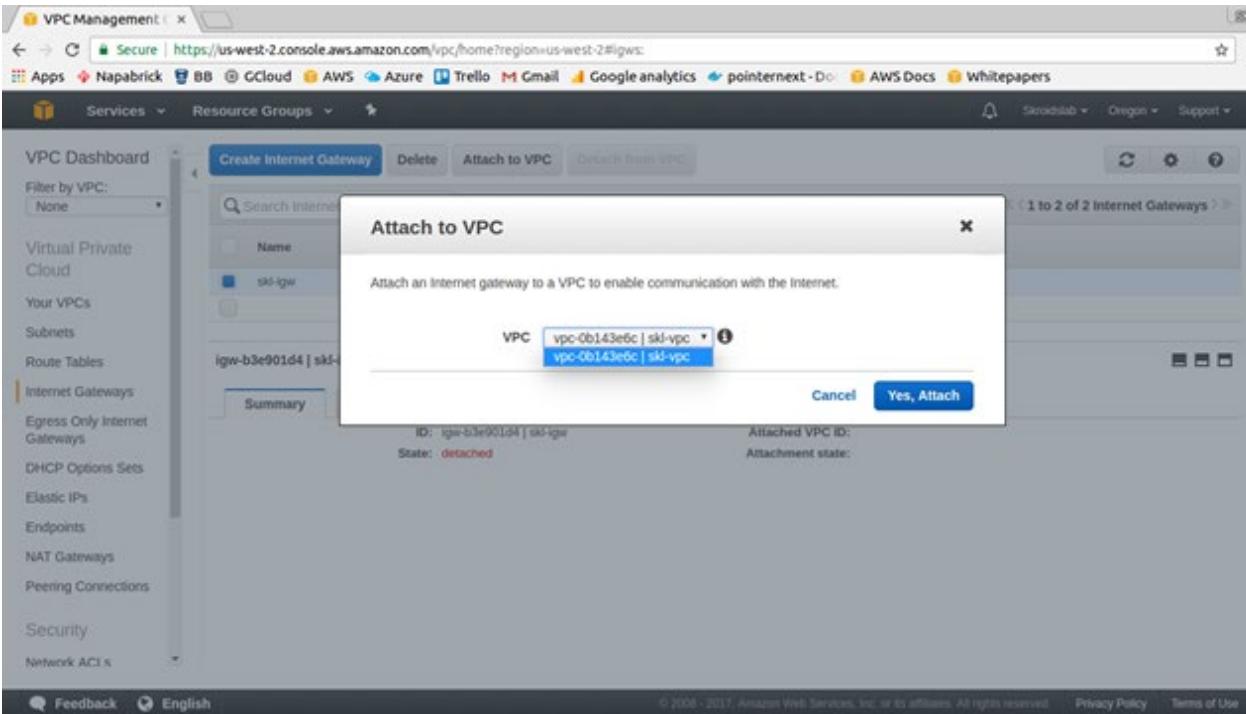


Activity - IG to VPC association



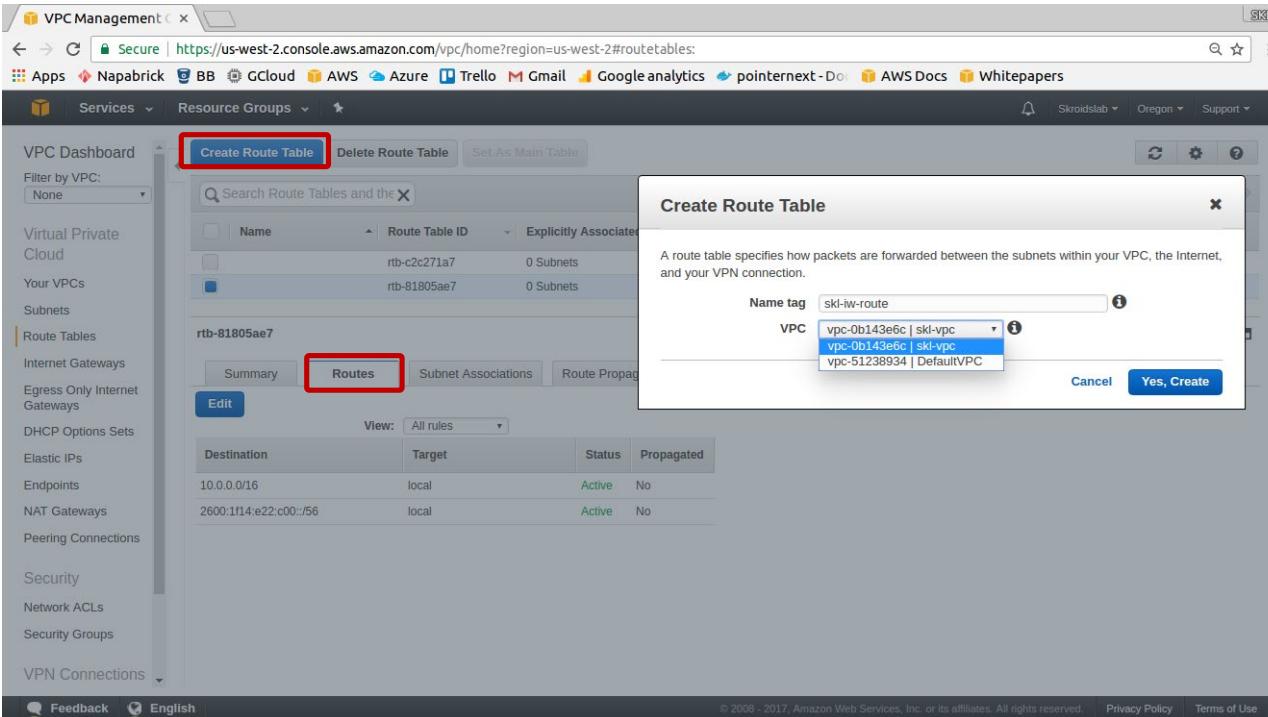
The screenshot shows the AWS VPC Management console with the URL <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#igws>. The left sidebar navigation bar includes links for VPC Dashboard, Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways (which is selected and highlighted in orange), Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, NAT Gateways, Peering Connections, Security, and Network ACLs. The main content area displays a table of Internet Gateways. The first row, 'skl-igw' (ID: igw-b3e901d4), has its 'State' field set to 'detached'. The second row, 'igw-c3fb2aa6' (ID: igw-c3fb2aa6), has its 'State' field set to 'attached' and is associated with the VPC 'vpc-51238934 | DefaultVPC'. Below the table, a detailed view for 'igw-b3e901d4 | skl-igw' is shown, with tabs for 'Summary' (selected) and 'Tags'. The 'Summary' tab displays the ID as 'igw-b3e901d4 | skl-igw', the state as 'Attached' (detached), and the Attached VPC ID as 'vpc-51238934 | DefaultVPC'. The 'Tags' tab is currently empty. At the top of the main content area, there are four buttons: 'Create Internet Gateway', 'Delete', 'Attach to VPC' (which is highlighted with a red box), and 'Detach from VPC'.

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

The screenshot shows the AWS VPC Management console with the 'Route Tables' page selected. On the left sidebar, under 'Route Tables', the 'Edit' button for the 'rtb-84ba60e2 | skl-lw-route' route table is highlighted with a red box.

Route Tables List:

Name	Route Table ID	Explicitly Associated	Main	VPC
rtb-c2c271a7	0 Subnets	Yes	vpc-51238934 DefaultVPC	
rtb-81805ae7	0 Subnets	Yes	vpc-0b143e6c skl-vpc	
rtb-84ba60e2 skl-lw-route	0 Subnets	No	vpc-0b143e6c skl-vpc	

rtb-84ba60e2 | skl-lw-route Route Table Details:

Summary	Routes	Subnet Associations	Route Propagation	Tags
Edit				

Routes Table:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
2600:1f14:ec22:c00::/56	local	Active	No

Activity - Attach IG to RT

The screenshot shows the AWS VPC Management console with the URL <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#routetables>. The left sidebar is collapsed, and the main area displays a table of Route Tables. One route table, named 'rtb-84ba60e2 | skt-lw-route', is selected and shown in detail. This route table has no subnets associated with it. The 'Routes' tab is active, showing two routes:

Destination	Target	Status	Propagated	Remove
10.0.0.0/8	local	Active	No	
0.0.0.0/0	igw-036002d4 sd-igw	Active	No	

A red box highlights the 'Save' button at the top of the route table configuration page. Another red box highlights the '0.0.0.0/0' destination field and the target 'igw-036002d4 | sd-igw' in the routes table.

**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

The screenshot shows the AWS VPC Management console with the URL <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#routetables>. The left sidebar navigation includes:

- VPC Dashboard
- Virtual Private Cloud
- Your VPCs
- Subnets
- Route Tables** (selected)
- Internet Gateways
- Egress Only Internet Gateways
- DHCP Options Sets
- Elastic IPs
- Endpoints
- NAT Gateways
- Peering Connections
- Security
- Network ACLs
- Security Groups
- VPN Connections

The main content area displays three route tables:

Name	Route Table ID	Explicitly Associated	Main	VPC
rtb-c2c271a7	rtb-81805ae7	0 Subnets	Yes	vpc-51230934 DefaultVPC
rtb-B4ba60e2 skj-lw-route	rtb-B4ba60e2	0 Subnets	No	vpc-0b5143e6c skj-vpc

For the selected route table (rtb-B4ba60e2), the tabs are:

- Summary
- Routes**
- Subnet Associations** (highlighted with a red box)
- Route Propagation
- Tags

The Subnet Associations table shows:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
2600:114:e22:c00::/56	local	Active	No
0.0.0.0	igw-b3e901d4	Active	No

Activity - attach RT to subnet

The screenshot shows the AWS VPC Management console with the URL <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#routetablesfilter=rtb-81805ae7>. The left sidebar lists various VPC components: Virtual Private Cloud, Your VPCs, Subnets, Route Tables (selected), Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, NAT Gateways, Peering Connections, Security, Network ACLs, Security Groups, and VPN Connections. The main area displays three route tables in a table:

Name	Route Table ID	Explicitly Associated	Main	VPC
default-rt	rtb-c2c271a7	0 Subnets	Yes	vpc-51238934 DefaultVPC
skl-main-rt	rtb-81805ae7	0 Subnets	Yes	vpc-0b143e6c skl-vpc
skl-lw-route	rtb-84ba60e2	1 Subnet	No	vpc-0b143e6c skl-vpc

Below the table, a message "rtb-84ba60e2 | skl-lw-route" is displayed. Underneath, there are tabs: Summary, Routes, Subnet Associations (selected), Route Propagation, and Tags. A blue "Edit" button is highlighted with a red box. The Subnet Associations tab shows two subnets:

Subnet	IPv4 CIDR	IPv6 CIDR
subnet-28990161 us-west-2a-10.0.1.0	10.0.1.0/24	-
subnet-58d99f3f us-west-2b-10.0.2.0	10.0.2.0/24	-

A message box contains the text: "any route tables and are therefore associated with the main route table;".

Notice this message

Name the RTs for better readability

Activity - attach RT to subnet

The screenshot shows the AWS VPC Management console with the URL <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#routetables>. The left sidebar is collapsed, and the main area displays a list of Route Tables. One route table, named 'skj-lw-route', is selected and shown in detail. The 'Subnet Associations' tab is active, showing two subnets associated with this route table. A red box highlights the 'Associate' checkbox for the first subnet, and another red box highlights the 'Save' button at the top of the page.

Associate	Subnet	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input checked="" type="checkbox"/>	subnet-28990161 us-west-2a-10.0.1.0	10.0.1.0/24	-	Main
<input checked="" type="checkbox"/>	subnet-58d990f us-west-2b-10.0.2.0	10.0.2.0/24	-	Main

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

Activity - attach RT to subnet

The screenshot shows the AWS VPC Management console with the Route Tables page open. A route table named 'skj-lw-route' is selected. The 'Edit' button is highlighted with a red box, and a green success message 'Save Successful' is displayed above it. The 'Subnet Associations' tab is active, showing two subnets associated with the route table:

Subnet	IPv4 CIDR	IPv6 CIDR
subnet-28990161 us-west-2a-10.0.1.0	10.0.1.0/24	-
subnet-58d993f us-west-2b-10.0.2.0	10.0.2.0/24	-

Activity - Subnet associated to RT

The screenshot shows the AWS VPC Management console with the 'Subnets' tab selected. A specific subnet, 'us-west-2a-10.0.1.0', is highlighted with a red box. Below it, its route table associations are displayed in a table. The 'Route Table' tab is selected, and the table shows two entries:

Destination	Target
10.0.0.0/8	local
0.0.0.0/0	igw-63e901d4

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

Activity - Subnet rule needs Public IP

The screenshot shows the AWS VPC Management console with the URL <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#subnets>. The left sidebar lists various VPC components: Virtual Private Cloud, Your VPCs, Subnets (highlighted in orange), Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, NAT Gateways, Peering Connections, Security, Network ACLs, Security Groups, and VPN Connections. The main area displays a table of subnets with the following columns: CIDR, Available IPv4, IPv6 CIDR, Availability Zone, Route Table, Network ACL, Default Subnet, Auto-assign Public IP (highlighted with a red box), and Auto-assign IPv6 address. There are five subnets listed:

CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Route Table	Network ACL	Default Subnet	Auto-assign Public IP	Auto-assign IPv6 address
1.2.0/24	251		us-west-2b	rtb-81805ae7 sk...	acl-d98f60bf	No	No	No
1.1.0/24	251		us-west-2a	rtb-84ba60e2 sk...	acl-d98f60bf	No	No	No
31.32.0/20	4091		us-west-2b	rtb-c2c271a7 de...	acl-9b41f5fe	Yes	Yes	No
31.0.0/20	4091		us-west-2c	rtb-c2c271a7 de...	acl-9b41f5fe	Yes	Yes	No
31.16.0/20	4091		us-west-2a	rtb-c2c271a7 de...	acl-9b41f5fe	Yes	Yes	No

Below the table, a specific subnet is selected: **subnet-28990161 | us-west-2a-10.0.1.0**. The **Edit** button is highlighted. The Route Table is set to **rtb-84ba60e2 | skl-lw-route**. The Route Table details show three entries:

Destination	Target
10.0.0.0/16	local
2600:1f14:e22:c00::/56	local
0.0.0.0	igw-b3e901d4

Activity - Subnet rule needs Public IP

The screenshot shows the AWS VPC Management console with the URL <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#subnets>. The left sidebar lists various VPC components: Virtual Private Cloud, Your VPCs, Subnets (selected), Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, NAT Gateways, Peering Connections, Security, Network ACLs, Security Groups, and VPN Connections. The main area displays a table of subnets. A context menu is open over the first subnet (subnet-28990161) in the list, with the option "Modify auto-assign IP settings" highlighted. The subnet table has columns for CIDR, Availability Zone, Route Table, Network ACL, Default Subnet, Auto-assign Public IP, and Auto-assign IPv6 address. The subnet details page shows a route table entry for 10.0.0.0/16 pointing to "local".

CIDR	Availability Zone	Route Table	Network ACL	Default Subnet	Auto-assign Public IP	Auto-assign IPv6 address
12.0/24	us-west-2b	rtb-81805ae7 sk... rtb-81805ae7 sk...	aci-d98f5c6f	No	No	No
11.0/24	us-west-2a	rtb-84ba60e2 sk... rtb-84ba60e2 sk...	aci-d98f5c6f	No	No	No
31.32.0/20	us-west-2b	rtb-c2c271a7 de... rtb-c2c271a7 de...	aci-9b415fe	Yes	Yes	No
31.0.0/20	us-west-2c	rtb-c2c271a7 de... rtb-c2c271a7 de...	aci-9b415fe	Yes	Yes	No
31.16.0/20	us-west-2a	rtb-c2c271a7 de... rtb-c2c271a7 de...	aci-9b415fe	Yes	Yes	No

subnet-28990161 | us-west-2a-10.0.1.0

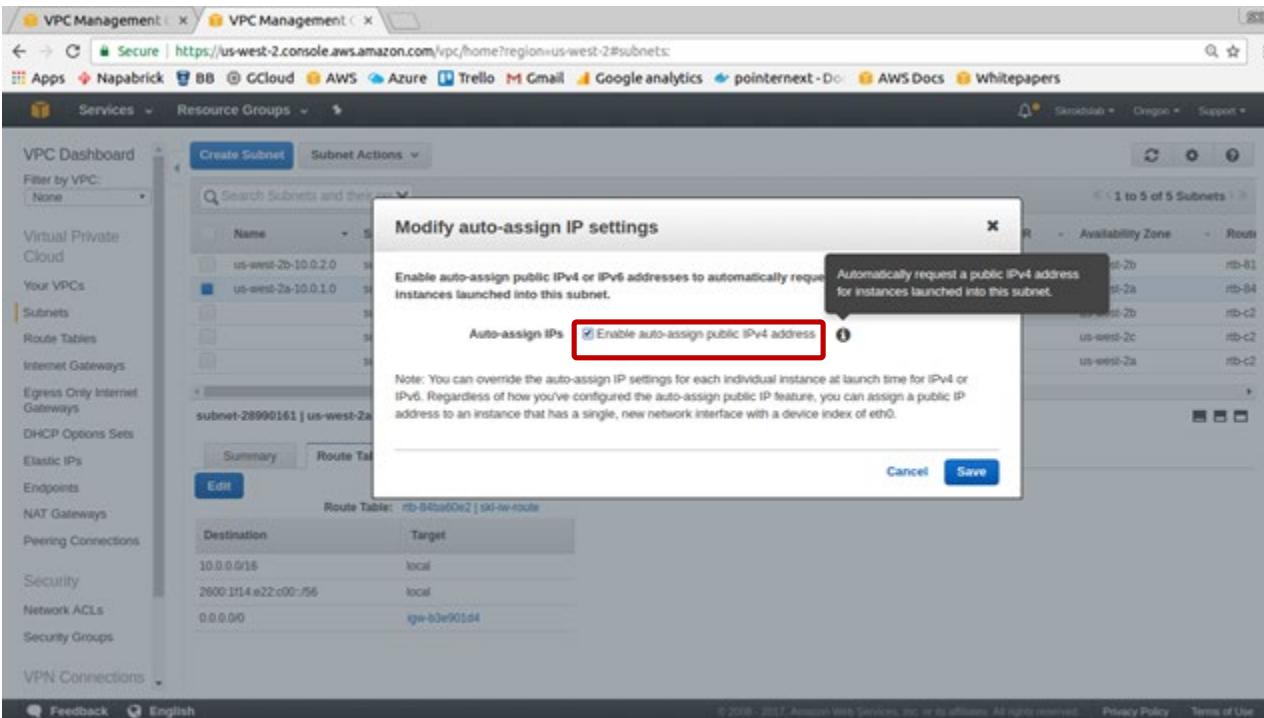
Summary Route Table Network ACL Flow Logs Tags Edit

Route Table: rtb-84ba60e2 | sk-nw-route

Destination	Target
10.0.0.0/16	local
2600:1f14:x22:c00::/56	local
0.0.0.0/0	igw-b3e901d4

Feedback English © 2006 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Activity - Subnet rule needs Public IP



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

Activity - launch EC2 in subnet 1

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

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

Purchasing option: Request Spot instances

Network: [Create new VPC](#)
Subnet: [Create new subnet](#)
vpc-0b143e6c | skl-vpc
subnet-28990161 | us-west-2a-10.0.1.0 | us-west-2
251 IP Addresses available

Auto-assign Public IP: [Use subnet setting \(Enable\)](#)

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

Shutdown behavior: Stop

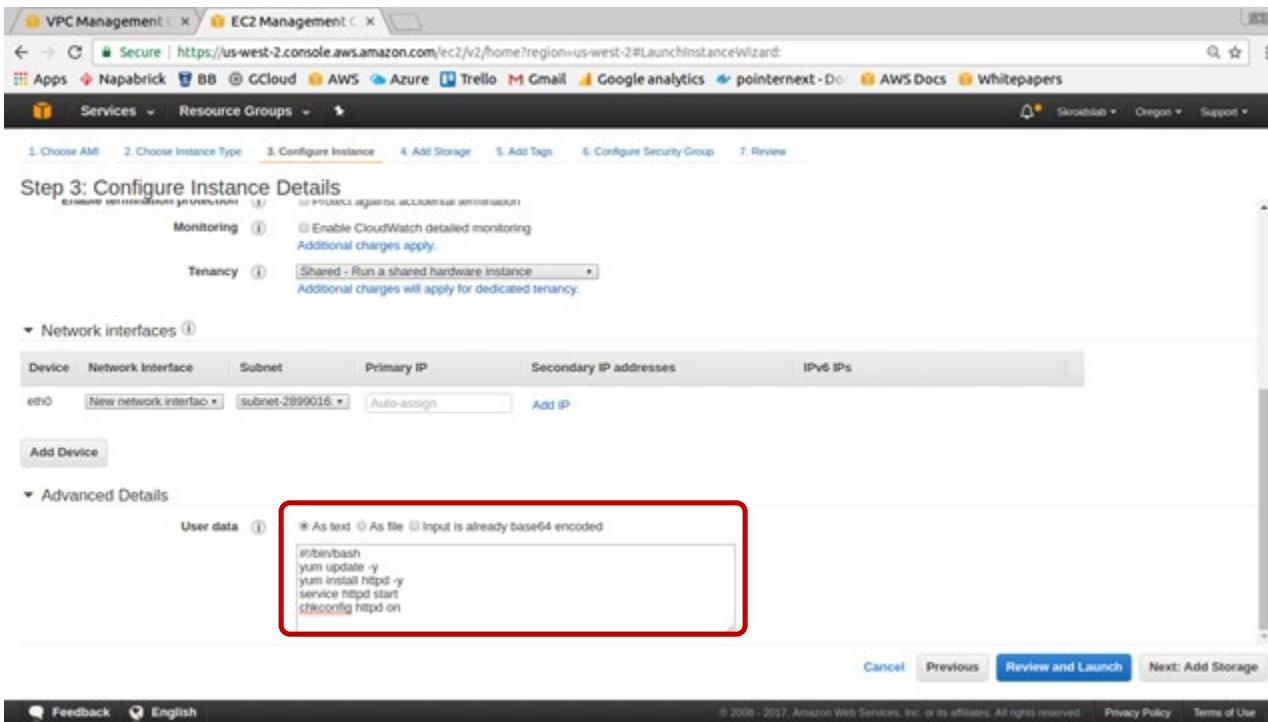
Enable termination protection: Protect against accidental termination

Monitoring: Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy: Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

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

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

The screenshot shows the AWS EC2 Management console interface. On the left, there's a sidebar with navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, AMIs, Bundle Tasks, Elastic Block Store, Volumes, Snapshots, Network & Security, Security Groups, Elastic IPs, Placement Groups, Key Pairs, and Network Interfaces. The main content area displays the 'Launch Instance' button and a table of instances. A single instance, 'web-server-1', is listed with the following details:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
web-server-1	i-0ff2413c6...	t2.micro	us-west-2a	running	2/2 checks ...	None	-	52.36.8.194

Below the table, the instance details for 'i-0ff2413c64ce6aec7 (web-server-1)' are shown with a Public IP of 52.36.8.194. The detailed information includes:

Attribute	Value
Instance ID	i-0ff2413c64ce6aec7
Instance state	running
Instance type	t2.micro
Elastic IPs	-
Availability zone	us-west-2a
Security groups	skl-port-combo, view inbound rules
Scheduled events	No scheduled events
AMI ID	amzn-ami-hvm-2017.03.0.20170417-x86_64-gp2 (ami-4836a42f)
Platform	-
IAM role	-
Key pair name	nmallya
Owner	278931287317
Launch time	April 24, 2017 at 5:51:03 PM UTC+5:30 (less than one hour)
Public DNS (IPv4)	-
IPv4 Public IP	52.36.8.194
IPv6 IPs	-
Private DNS	ip-10-0-1-31.us-west-2.compute.internal
Private IP	10.0.1.31
Secondary private IPs	-
VPC ID	vpc-0b143e6c
Subnet ID	subnet-28990161
Network interfaces	eth0
Source/dest. check	True
EBS-optimized	False
Root device type	ebs

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

Activity - Test the IG+RT

The screenshot shows the AWS VPC Management console. In the sidebar, under 'Route Tables', there is a red box highlighting the 'Route Tables' link. On the main page, a table lists three route tables: 'default-rt', 'skl-main-rt', and 'skl-lw-route'. The 'skl-lw-route' table has a red box around its row. In the 'Routes' tab of the 'skl-lw-route' details view, there is a red box around the 'Save' button in the sub-menu. Another red box highlights the delete icon for a route entry with destination '0.0.0.0/0' and target 'igw-b3e901d4'.

Name	Route Table ID	Explicitly Associated Subnets	Main	VPC
default-rt	rtb-c2c271a7	0 Subnets	Yes	vpc-51238934 DefaultVPC
skl-main-rt	rtb-81805ae7	0 Subnets	Yes	vpc-0b143e6c skl-vpc
skl-lw-route	rtb-84ba60e2	1 Subnet	No	vpc-0b143e6c skl-vpc

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
2600:1f14:e22:c00::/56	local	Active	No	
0.0.0.0/0	igw-b3e901d4	Active	No	

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

Activity - Launch EC2 in subnet 2

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group:

Create a new security group
 Select an existing security group

Security group name:
skl-db-port3306

Description:
MySQL port 3306

Type	Protocol	Port Range	Source
MS SQL	TCP	1433	Custom 10.0.1.0/24
SSH	TCP	22	Custom 10.0.1.0/32 10.0.1.0/24

Add Rule

Cancel Previous Review and Launch

Feedback English Privacy Policy Terms of Use

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

The screenshot shows the AWS EC2 Management console interface. On the left, a sidebar lists various services: EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images (AMIs), Elastic Block Store (Volumes, Snapshots), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces). The main content area displays a table of instances. Two instances are listed: 'db-server' (Instance ID: i-013469435d2817502) and 'web-server-1' (Instance ID: i-0ff2413c6...). Both are t2.micro type, running in us-west-2b and us-west-2a availability zones respectively. The 'db-server' instance is currently initializing. Below the table, a detailed view for the 'db-server' instance is shown, including fields like Instance ID, Instance state, Instance type, Availability zone, Security groups, Scheduled events, AMI ID, Platform, IAM role, Key pair name, and a numeric identifier. The 'Description' tab is selected, showing the following details:

Attribute	Value
Instance ID	i-013469435d2817502
Instance state	running
Instance type	t2.micro
Elastic IPs	-
Availability zone	us-west-2b
Security groups	skl-db-port3306, view inbound rules
Scheduled events	No scheduled events
AMI ID	amazon-ami-hvm-2017.03.0.20170417-x86_64-gp2 (ami-4836a42f)
Platform	-
IAM role	-
Key pair name	nirmalya
Number	5796911967717

Below the table, there are tabs for 'Status Checks', 'Monitoring', and 'Tags'. At the bottom of the page, there are links for 'Feedback', 'English', and a copyright notice: © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use.

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

```
[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

Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Cancel and Exit

Quick Start

My AMIs

AWS Marketplace

Community AMIs

Operating system

- Amazon Linux
- Cent OS
- Debian
- Fedora
- Gentoo
- OpenSUSE
- Other Linux
- Red Hat
- SUSE Linux
- Ubuntu
- Windows

Search: nat

marketplace 21 results for "nat" on AWS Marketplace Partner software pre-configured to run on AWS

amzn-ami-vpc-nat-pv-2014.09.1.x86_64-ebs - ami-030f4133	Select	64-bit
Amazon Linux AMI 2014.09.1.x86_64 VPC NAT PV EBS Root device type: ebs - Virtualization type: paravirtual		
amzn-ami-vpc-nat-hvm-2016.09.rc-0.20160910-x86_64-ebs - ami-11fd2e71	Select	64-bit
Amazon Linux AMI 2016.09.rc-0.20160910 x86_64 VPC NAT HVM EBS Root device type: ebs - Virtualization type: hvm		
amzn-ami-vpc-nat-hvm-2016.09.1.20161221-x86_64-ebs - ami-1c2a9e7c	Select	64-bit
Amazon Linux AMI 2016.09.1.20161221 x86_64 VPC NAT HVM EBS Root device type: ebs - Virtualization type: hvm		
amzn-ami-vpc-nat-hvm-2014.09.1.x86_64-gp2 - ami-290f4119	Select	64-bit

Feedback English

© 2006 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Activity - NAT instance

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1

Purchasing option: Request Spot instances

Network: vpc-001496c | us-west-2

Subnet: subnet-28990161 | us-west-2a | 10.0.1.0 | us-west-2a
250 IP Addresses available

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

IAM role: None

Shutdown behavior: Stop

Enable termination protection: Protect against accidental termination

Monitoring: Enable CloudWatch detailed monitoring Amazon CloudWatch Metrics

Later, choose the security group of PORT 22 + 80

Activity - NAT instance

The screenshot shows the AWS EC2 Management console interface. On the left, there's a sidebar with navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images (AMIs), Elastic Block Store (Volumes, Snapshots), Network & Security (Security Groups, Elastic IPs, Placement Groups), and VPC Management.

In the main area, the 'Instances' section is selected. A table lists three instances: 'db-server', 'nat-instance' (which is highlighted with a blue square), and 'web-server-1'. The 'nat-instance' row has a context menu open, showing options like Connect, Launch More Like This, Instance State, Instance Settings, Image, Networking (selected), Change Security Groups, Attach Network Interface, Detach Network Interface, Disassociate Elastic IP Address, Change Source/Dest. Check, and Manage IP Addresses.

Below the table, detailed information for the 'nat-instance' is shown:

Description	Instance ID: i-07ea275a676011148	Public DNS (IPv4): 54.71.109.29
Status Checks	Instance state: running	IPv6 IPs: -
Monitoring	Instance type: t2.micro	Private DNS: ip-10-0-1-152.us-west-2.compute.internal
Tags	Elastic IPs: -	Private IPs: 10.0.1.152
	Availability zone: us-west-2a	Secondary private IPs: -
	Security groups: skt-port-combo, view Inbound rules	VPC ID: vpc-0b143e6c
	Scheduled events: No scheduled events	Subnet ID: subnet-28990161
	AMI ID: amzn-ami-vpc-nat-hvm-2016.09.rc-0.20160910-x86_64-eks (ami-11fd2e71)	

At the bottom, there are links for Feedback, English, and other AWS services like VPC Management, EC2 Management, and Test Page for the API.

Activity - NAT instance

The screenshot shows the AWS EC2 Management console interface. On the left, there's a sidebar with navigation links for Services (EC2 Dashboard, Events, Tags, Reports, Limits), Instances (Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts), Images (AMIs, Bundle Tasks), Elastic Block Store (Volumes, Snapshots), and Network & Security (Security Groups, Elastic IPs, Placement Groups). The main area displays a list of instances, with one instance selected. A modal dialog box is centered over the list, titled "Enable Source/Destination Check". Inside the dialog, a message asks, "Are you sure that you would like to disable Source/Destination Check for the instance with the following details?". Below the message, it lists the instance details: Instance: i-07ea275a676011148 (nat-instance), Network Interface: eni-ce5059f4, and Status: Enabled. At the bottom right of the dialog are "Cancel" and "Yes, Disable" buttons. In the background, the instance details are shown in a larger table, including fields like Elastic IP, Availability zone, Security groups, Scheduled events, AMI ID, Private DNS, Private IP, Secondary private IPs, VPC ID, and Subnet ID.

Elastic IP	Private DNS
None	ip-20-0-1-152.us-west-2.compute.internal
Availability zone	Private IPs
us-west-2a	10.0.1.152
Security groups	Secondary private IPs
sk8-port-combo , view inbound rules	
Scheduled events	VPC ID
No scheduled events	vpc-0b143e6c
AMI ID	Subnet ID
amzn-ami-vpc-nat-hvm-2016.09.rc-0.20160910-x86_64-ena (ami-11kd0e71)	subnet-28990161

Activity - NAT instance association with VPC main RT

greatlearning

The screenshot shows the AWS VPC Management console with the following details:

- Route Tables List:** Shows three route tables:
 - default-rt (RTB ID: rtb-c2c271a7)
 - skl-main-rt (RTB ID: rtb-81805ae7) - This table is selected and highlighted with a red box.
 - skl-lw-route (RTB ID: rtb-84ba60e2)
- Selected Route Table Details:** The 'skl-main-rt' table is shown in more detail.
 - Edit Button:** The 'Edit' button is highlighted with a red box.
 - Routes Tab:** The 'Routes' tab is active, showing the following routes:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
2600:1f14:e22:c00::/56	local	Active	No

Activity - NAT instance association with VPC main RT

The screenshot shows the AWS VPC Management console with the 'Route Tables' section selected. The left sidebar lists various VPC components, and the main area displays three route tables:

Name	Route Table ID	Explicitly Associated	Main	VPC
default-rt	rtb-c2c271a7	0 Subnets	Yes	vpc-51238934 DefaultVPC
skl-main-rt	rtb-81805ae7	0 Subnets	Yes	vpc-0b143e6c skl-vpc
skl-tw-route	rtb-84ba60e2	1 Subnet	No	vpc-0b143e6c skl-vpc

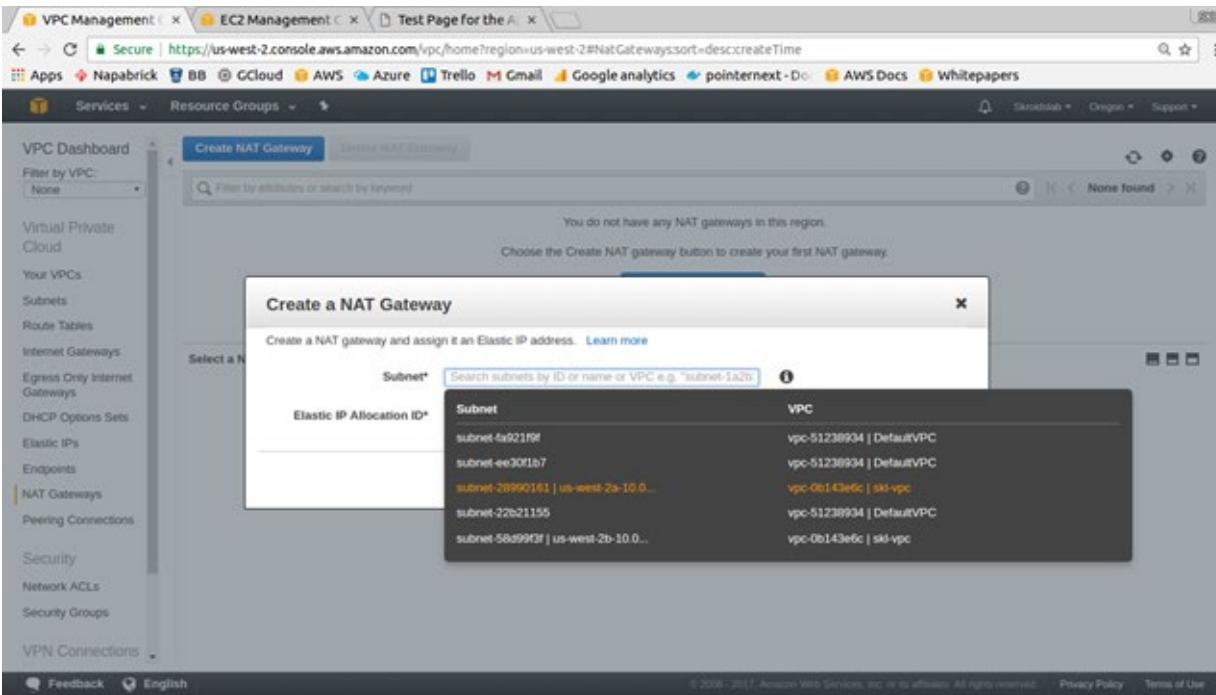
For the 'skl-main-rt' table, the 'Routes' tab is active, showing one route entry:

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0	igw-b3e901d4 skl-igw	Active	No	

A red box highlights the '0.0.0.0/0' row, which points to the target 'igw-b3e901d4 | skl-igw'. Below this row is a button labeled 'Add another route'.

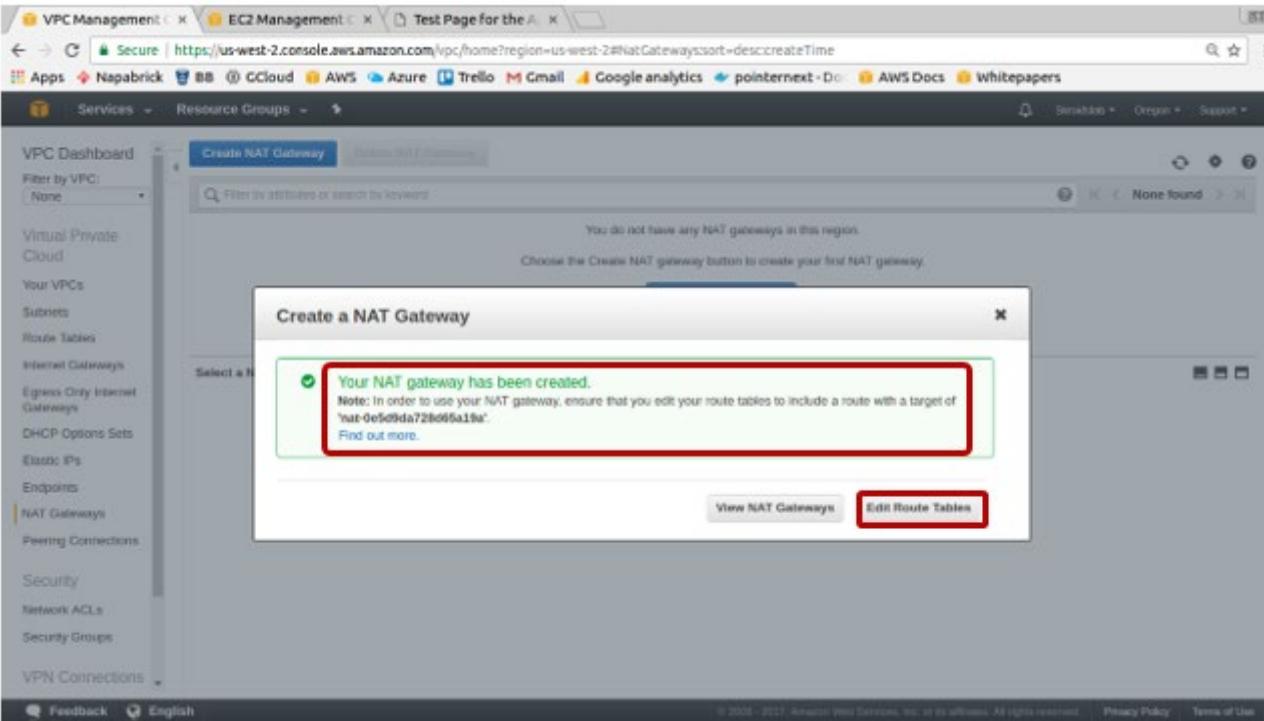
Go to the terminal window of db (that is already open) and try
yum install mysql -y

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

The screenshot shows the AWS VPC Management console with the 'Route Tables' page open. The 'sd-main-rt' route table is selected. The 'Routes' tab is active, displaying the following routes:

Destination	Target	Status	Propagated	Remove
0.0.0.0/0	nat-05d943e729d05a19a	Active	No	<input type="radio"/>
2600::/32	local	Active	No	<input type="radio"/>

Go back to the terminal window of DB and execute
yum update -y

Activity - ACL

The screenshot shows the AWS VPC Management console with the Network ACLs section selected. A red box highlights the 'Inbound Rules' tab. Another red box highlights the rule table, which lists four rules:

Rule #	Type	Protocol	Port Range	Source	Action
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
101	ALL Traffic	ALL	ALL	::/0	ALLOW
*	ALL Traffic	ALL	ALL	::/0	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

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

The screenshot shows the AWS VPC Peering Connections page. On the left sidebar, under the 'Virtual Private Cloud' section, the 'Peering Connections' item is highlighted with a red box. At the top center, there is a blue button labeled 'Create Peering Connection'. Below it, a table displays one peering connection entry:

Name	Peering Connection ID	Status	Requester VPC	Acceptor VPC	Requester CIDRs	Acceptor CIDRs
peer	pcx-b2eadfdb	Deleted	vpc-256480431 or...	vpc-e20fb9b1 skl...	-	-

A message in the center of the page reads: **You will not see any peering connections listed here!**

Activity - Peering

The screenshot shows the 'Create Peering Connection' page in the AWS Management Console. The top navigation bar includes tabs for 'Create Peering Conn.' and 'EC2 Management'. The URL is https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#CreatePeeringConnection. The AWS logo and navigation links for 'Services' and 'Resource Groups' are visible. On the right, there are status indicators for 'Cloud Rocker 100', 'Oregon', and 'Support'.

The main section is titled 'Create Peering Connection'. A red box highlights the 'Peering connection name tag' input field, which contains 'def-skl-peer'. Below it, a dropdown menu labeled 'VPC (Requester)' shows 'vpc-25648043' selected. A red box highlights the 'CIDRs' dropdown menu, which lists two entries: 'vpc-25648043' and 'crock-default-vpc'. The bottom section, 'Select another VPC to peer with', includes an 'Account' dropdown with 'My account' selected.

Activity - Peering

The screenshot shows the 'Create Peering Connection' wizard in the AWS Management Console. The top navigation bar includes tabs for 'Create Peering Conn' (active), 'EC2 Management', and 'CloudRocker-1 (Supervised)'. The URL is https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#CreatePeeringConnection:.

The main form has the following fields:

- Select another VPC to peer with**
- Account:** My account (radio button selected)
- Region:** This region (us-west-2) (radio button selected)
- VPC (Acceptor):** A dropdown menu showing 'vpc-e20fb9b'.
- CIDRs:** A dropdown menu showing two entries:
 - vpc-e20fb9b (highlighted with a red box)
 - vpc-25648043A search bar above the list says 'Filter by attributes'.

At the bottom of the form are buttons for *** Required**, **Create Peering Connection** (highlighted with a red box), **Cancel**, and links for **Feedback**, **English (US)**, **© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.**, **Privacy Policy**, and **Terms of Use**.

Activity - Peering

The screenshot shows a browser window for the AWS EC2 Management console, specifically the 'Create Peering Connection' page. The URL is <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#CreatePeeringConnection>. The page title is 'Create Peering Connection'. A green success message box contains the following information:

Requester VPC owner	837466521382 (This account)	Acceptor VPC owner	837466521382 (This account)
Requester VPC ID	vpc-25648043	Acceptor VPC ID	vpc-e20fb9b
Requester VPC Region	us-west-2	Acceptor VPC Region	us-west-2
Requester VPC CIDRs	172.31.0.0/16	Acceptor VPC CIDRs	-

At the bottom right of the message box is a blue 'OK' button.

At the bottom of the page, there are links for 'Feedback', 'English (US)', and copyright information: '© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.' followed by 'Privacy Policy' and 'Terms of Use'.

Activity - Peering

Screenshot of the AWS VPC Peering Connections page.

The screenshot shows a list of peering connections. One connection, "def-sk1-peer" (ID: pcx-88d8ede1), is selected. A context menu is open over this connection, with "Accept Request" highlighted.

	Requester VPC	Acceptor VPC	Requester CIDRs	Acceptor CIDRs
peer	vpc-25648043 cr...	vpc-e20fbdb9b skl...	-	-
def-sk1-peer	vpc-25648043 cr...	vpc-e20fbdb9b skl...	172.31.0.0/16	10.0.0.0/16

Details for Peering Connection: pcx-88d8ede1:

Description	ClassicLink	DNS	Route Tables	Tags
Requester VPC owner: 837466521382	Requester VPC ID: vpc-25648043	Requester VPC Region: Oregon (us-west-2)	Requester VPC CIDRs: 172.31.0.0/16	Acceptor VPC owner: 837466521382
Requester VPC Connection: pcx-88d8ede1	Expiration time: February 11, 2018 at 6:23:33 PM UTC+5:30	Acceptor VPC ID: vpc-e20fbdb9b	Acceptor VPC Region: Oregon (us-west-2)	Acceptor VPC CIDRs: 10.0.0.0/16
Peering connection status: Pending Acceptance by 837466521382				

Footer:

- Feedback
- English (US)
- © 2006 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
- Privacy Policy
- Terms of Use

Activity - Peering

The screenshot shows the AWS VPC Management console with the 'Peering Connections' tab selected. A modal dialog box titled 'Accept VPC Peering Connection Request' is displayed in the center. The dialog asks if the user wants to accept a request from account 837466521382 (This account) with VPC ID vpc-25648043. It lists the requester's details: Account ID 837466521382 (This account), VPC ID vpc-25648043, Region us-west-2, and CIDR 172.31.0.0/16. It also lists the accepter's details: Account ID 837466521382 (This account), VPC ID vpc-e20fd9b, Region us-west-2, and CIDR 10.0.0.0/16. At the bottom of the dialog are 'Cancel' and 'Yes, Accept' buttons. The background shows a table of existing peering connections, with one entry for 'peer' (Status: Deleted) and another for 'new-hadoopdb' (Status: Pending Acceptance by 837466521382). The table includes columns for Name, Status, Requester VPC, Acceptor VPC, Requester CIDRs, and Acceptor CIDRs.

Name	Status	Requester VPC	Acceptor VPC	Requester CIDRs	Acceptor CIDRs
peer	Deleted	vpc-25648043	vpc-e20fd9b	-	-
new-hadoopdb	Pending Acceptance by 837466521382	vpc-25648043	vpc-e20fd9b	10.0.0.0/16	10.0.0.0/16

Activity - Peering

The screenshot shows the AWS VPC Peering Connections page. On the left, a sidebar lists various VPC-related services. The main area displays a table of peering connections. One connection, 'def-skl-peer' (pcx-88d8ede1), is highlighted with a red box and marked as 'Active'. Another connection, 'peer' (pcx-bzeaudub), is marked as 'Deleted'. Below the table, a detailed view of the active connection is provided.

Name	Peering Connection ID	Status	Requester VPC	Acceptor VPC	Requester CIDRs	Acceptor CIDRs
def-skl-peer	pcx-88d8ede1	Active	vpc-25648043 cr...	vpc-e20fbdb9b skl...	172.31.0.0/16	10.0.0.0/16
peer	pcx-bzeaudub	Deleted	vpc-25648043 cr...	vpc-e20fbdb9b skl...	-	-

Peering Connection: pcx-88d8ede1

Description	ClassicLink	DNS	Route Tables	Tags
Requester VPC owner	837466521382	Acceptor VPC owner	837466521382	
Requester VPC ID	vpc-25648043	Acceptor VPC ID	vpc-e20fbdb9b	
Requester VPC Region	Oregon (us-west-2)	Acceptor VPC Region	Oregon (us-west-2)	
Requester VPC CIDRs	172.31.0.0/16	Acceptor VPC CIDRs	10.0.0.0/16	
VPC Peering Connection	pcx-88d8ede1	Peering connection status	Active	
Expiration time	-			

Activity - Peering

The screenshot shows the AWS VPC Route Tables page. On the left sidebar, under the 'Route Tables' section, there is a red box highlighting the 'Route Tables' link. In the main content area, a new route table is being created. A red box highlights the 'Create Route Table' button. The search bar shows 'rtb-bbeb71dd'. The table lists two existing route tables:

Name	Route Table ID	Explicitly Associated	Main	VPC
rtb-bbeb71dd	rtb-bbeb71dd	0 Subnets	Yes	vpc-25648043 crock-default-vpc
rtb-ea508d92	rtb-ea508d92	0 Subnets	Yes	vpc-e205bd9b sal-vpc

The newly created route table 'rtb-bbeb71dd' is selected. The 'Routes' tab is active, showing one route entry:

Destination	Target	Status	Propagated	Remove
172.31.0.0/16	local	Active	No	(radio button)
0.0.0.0	igw-e737eb80	Active	No	(radio button)

A red box highlights the 'Add another route' button at the bottom of the routes table.

At the bottom of the page, there are links for Feedback, English (US), and a footer with copyright information: © 2008 – 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use.

Activity - Peering

The screenshot shows the AWS VPC Route Tables interface. On the left sidebar, under 'Route Tables', the 'rtb-bbeb71dd' route table is selected. The main area displays two route tables:

Name	Route Table ID	Explicitly Associated	Main	VPC
rtb-bbeb71dd	rtb-bbeb71dd	0 Subnets	Yes	vpc-25648043 crock-default-vpc
	rtb-ea50bd92	0 Subnets	Yes	vpc-ea20bd92 skt-vpc

The 'rtb-bbeb71dd' route table is currently selected. The 'Routes' tab is active, showing the following routes:

Destination	Target	Status	Propagated	Remove
172.31.0.0/16	local	Active	No	
0.0.0.0/0	igw-e737eb80	Active	No	
10.0.0.0/16	gw-e737eb80		No	

A red box highlights the '10.0.0.0/16' destination and its target 'gw-e737eb80'. A tooltip for 'gw-e737eb80' indicates it is 'pcx-08d8ed61 | def-sk-peer'. The 'Save' button is visible at the top of the route table configuration.

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

The screenshot shows the AWS VPC Route Tables interface. On the left, there's a sidebar with navigation links: VPC Dashboard, Filter by VPC (with a dropdown menu), Virtual Private Cloud, Your VPCs, Subnets, Route Tables (which is selected and highlighted in orange), Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Endpoint Services, NAT Gateways, Peering Connections, and Security.

In the main content area, there's a search bar at the top labeled "Search Route Tables and their..." followed by a table with columns: Name, Route Table ID, Explicitly Associated, Main, and VPC. Two route tables are listed:

Name	Route Table ID	Explicitly Associated	Main	VPC
rtb-0b4671dd	0 Subnets	Yes	No	vpc-25648d43 crock-default-vpc
rtb-ea508d92	0 Subnets	Yes	No	vpc-e20fbdbb sil-vpc

Below the table, a specific route table named "rtb-ea508d92" is selected. It has tabs for Summary, Routes (which is selected and highlighted in blue), Subnet Associations, Route Propagation, and Tags. There are "Cancel" and "Save" buttons, with "Save" being the active button.

The "Routes" tab displays a table with columns: Destination, Target, Status, Propagated, and Remove. One row is shown:

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	(remove)

Below this table, there are buttons for "Add another route" and a text input field containing "172.31.0.0/16" which is highlighted with a red box. To the right of this input field is a dropdown menu with the value "pcx-08d8ede1 | def-sil-peer" also highlighted with a red box.

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

Activity - Peering

The screenshot shows the AWS VPC Management console with the 'Peering Connections' section selected. Two peering connections are listed:

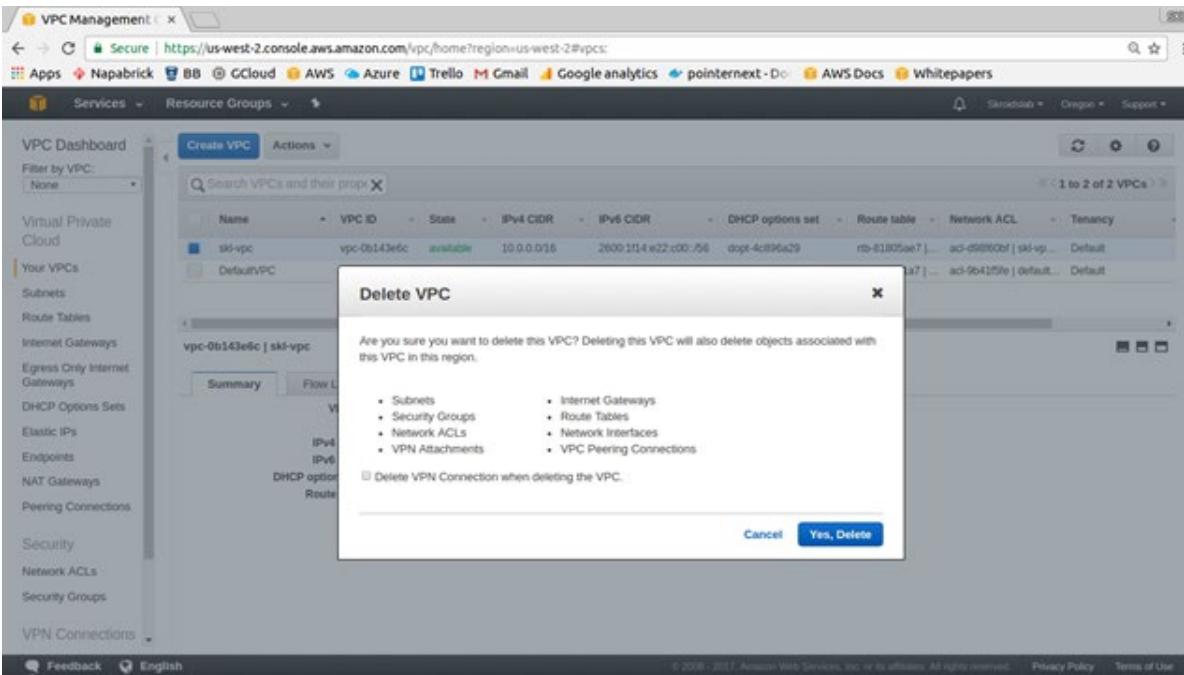
Name	Peering Connection ID	Status	Requester VPC	Acceptor VPC	Requester CIDRs	Acceptor CIDRs
def-sm-peer	pcx-80d8ede1	Active	vpc-25648043 cr...	vpc-e20fb9b skl...	172.31.0.0/16	10.0.0.0/16
peer	pcx-d2eedfbd	Deleted	vpc-25648043 cr...	vpc-e20fb9b skl...	-	-

For the active connection, the 'Route Tables' tab is selected, showing the associated route tables:

Route Table ID	VPC ID	Main	Associated with
rtb-bbeb71dd	vpc-25648043	Yes	0 subnets
rtb-ea508d92	vpc-e20fb9b	Yes	0 subnets

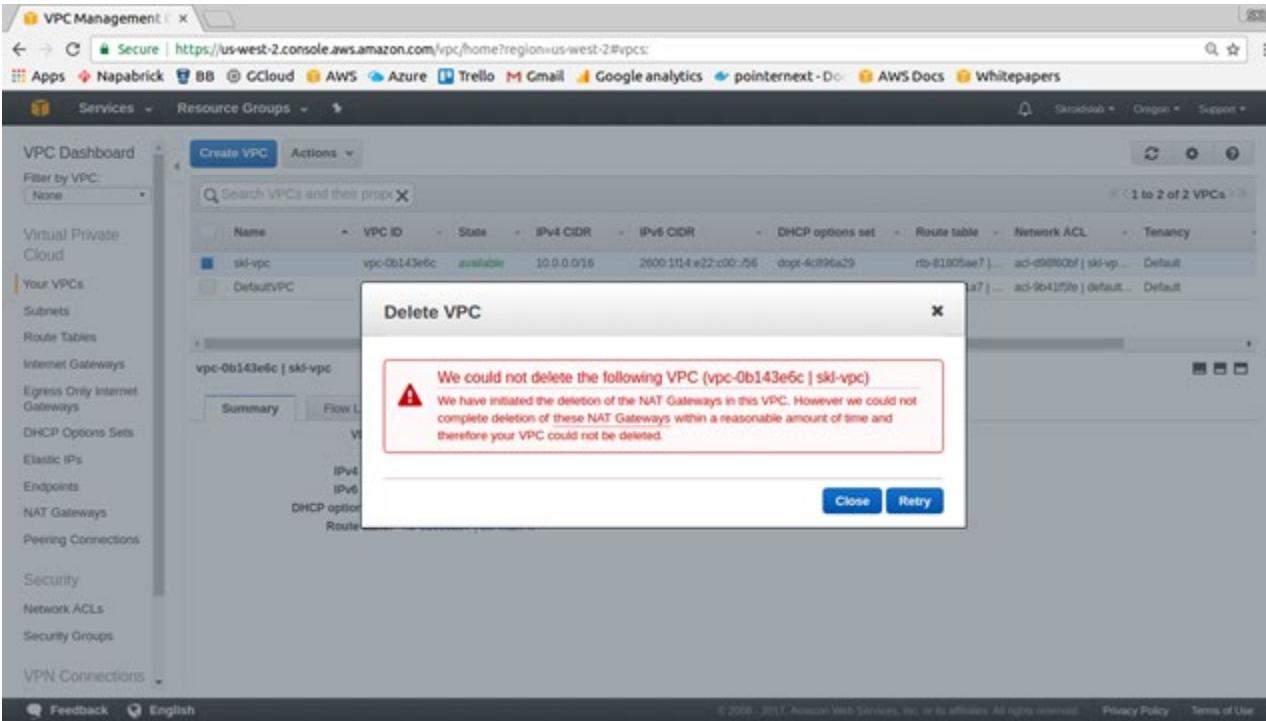
Verify that both VPCs have the RT updated with each other's CIDR blocks. Now go back to the terminal window and ping the EC2 instance in the custom VPC from the default VPC and ping will respond back!

Activity - Cleanup



Ensure the EC2 instances are deleted first!

Activity - Cleanup



Give it some time!



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

The screenshot shows the AWS Route 53 Management Dashboard. On the left, a sidebar lists navigation options: Dashboard, Hosted zones, Health checks, Traffic flow, Traffic policies, Policy records, Domains, Registered domains, and Pending requests. The main content area is divided into four main sections:

- DNS management:** Shows 1 Hosted zones. A visual tool for creating policies for multiple endpoints in complex configurations. Includes a "Create policy" button.
- Traffic management:** A visual tool for easily creating policies for multiple endpoints in complex configurations. Includes a "Create policy" button.
- Availability monitoring:** Health checks monitor applications and web resources, directing DNS queries to healthy resources. Includes a "Create health check" button.
- Domain registration:** Shows 1 Domains. Includes a "Register domain" section for finding and registering available domains, and an "Alerts" section listing two alerts for "pointernext.click".

At the bottom, there's a "More info" section with links to Developer Guide, FAQs, Pricing, Forum - DNS and health checks, Forum - Domain name registration, Request a limit increase, Service health (showing Amazon Route 53 is operating normally), and the AWS service health dashboard.

Route 53 Hosted zones

The screenshot shows the AWS Route 53 Management Console interface. The left sidebar has a 'Hosted zones' section selected. The main area displays a table of hosted zones with two entries:

Domain Name	Type	Record Set Count	Comment	Hosted Zone ID
pointer.click.	Public	2	HostedZone created by Route53 Registrar	Z200ZPN3TPBA7U
pointer-next.com.	Public	2	PointerNext dot com	Z35305YGG6405RR

At the top, there is a red box highlighting the 'Create Hosted Zone' button. A red arrow points from the 'Hosted zones' link in the sidebar to the 'Create Hosted Zone' button. Another red arrow points from the 'Hosted zones' link in the sidebar to the table header.

Route 53 Hosted zones

The screenshot shows the AWS Route 53 Manager interface. On the left, a sidebar menu includes options like Dashboard, Hosted zones (which is selected and highlighted in orange), Health checks, Traffic flow, Traffic policies, Policy records, Domains, Registered domains, and Pending requests. The main content area has a title bar with 'Create Hosted Zone' and buttons for 'Go to Record Sets' and 'Delete Hosted Zone'. A search bar at the top of the list table says 'Search all fields' and 'All Types'. Below it, a table lists two existing hosted zones: 'pointernext.click.' and 'pointer.next.com.'. The 'pointer.next.com.' entry includes a tooltip: 'A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.' A red box highlights the 'Domain Name' field in the 'Create Hosted Zone' form on the right, which contains the value 'example.com'. Other fields in the form include 'Comment' (empty), 'Type' (set to 'Public Hosted Zone'), and a note below stating 'A public hosted zone determines how traffic is handled for your resources.' At the bottom of the form is a blue 'Create' button.

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

Route 53 NS settings

The screenshot shows two views of the AWS Route 53 console. The top view is for the domain `pointernext.click`, specifically the `NS` resource record set. The bottom view is for the same domain, showing the `Hosted zones` section where the `NS` records are listed.

Top View: Registered domains > pointernext.click

- Left sidebar: Services, Resource Groups.
- Domain details:
 - Domain: `pointernext.click`
 - Registered on: 2017-04-18
 - Expires on: 2020-04-15 (pending)
 - Auto-renew: Enabled (auto)
- Right pane:
 - Name servers:
 - ns-172.awsdns-00.com
 - ns-177.awsdns-32.net
 - ns-1296.awsdns-34.org
 - ns-3395.awsdns-02.co.uk
 - Add or edit name servers

Bottom View: Hosted zones > pointernext.click

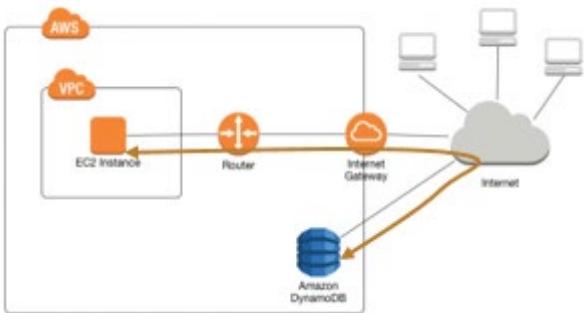
- Left sidebar: Services, Resource Groups.
- Hosted zones:
 - pointernext.click
- Table:
 - Record Set Name: `NS`
 - Name: `pointernext.click`
 - Type: `NS`
 - Value:
 - ns-172.awsdns-00.com
 - ns-177.awsdns-32.net
 - ns-1296.awsdns-34.org
 - ns-3395.awsdns-02.co.uk

A red arrow points from the "Name servers" list in the top view to the "Value" column in the bottom view, with the text "Must match!" overlaid.

Activity - Route 53 Routing

- 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

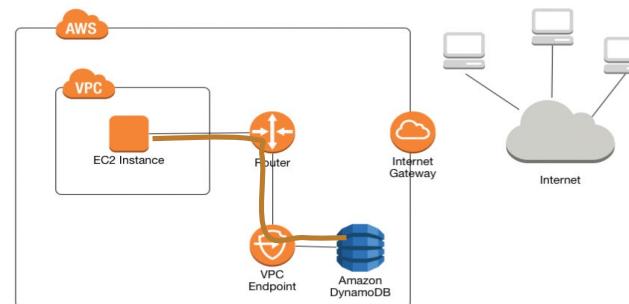
Activity - VPC Endpoints



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>