

# **Course: Cloud Computing on AWS**

## **By Nirmallya Mukherjee**

# Introduction

**Cloud fundamentals & VERY useful links**

# Documentation

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

# Certification prep



## Exam overview

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

## Study materials

- <https://aws.amazon.com/whitepapers/>
- <https://aws.amazon.com/architecture/>
- <https://aws.amazon.com/ec2/faqs/>
- <http://docs.aws.amazon.com/autoscaling/latest/userguide/as-instance-termination.html>
- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html>
- <https://aws.amazon.com/premiumsupport/knowledge-center/snapshot-ebs-raid-array/>
- <https://aws.amazon.com/ec2/vm-import/>
- [http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Subnets.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html)
- <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html>
- <http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html>
- <http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/LSI.html>
- <https://aws.amazon.com/devpay/>
- <http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>
- <http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-anatomy.html>
- <http://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html>
- Interesting-> <https://www.awsarchitectureblog.com/2014/04/shuffle-sharding.html>
- Free datasets-> <https://aws.amazon.com/public-datasets/>

# Introduction

## Understanding billing and alerts

# Billing - dashboard

greatlearning

The screenshot shows the AWS Management Console with the URL <https://us-west-2.console.aws.amazon.com/console/home?region=us-west-2>. The top navigation bar includes links for Apps (Napabrick, BB, GCloud, AWS, Azure, Trello, Gmail, Google analytics, pointernext), and a search bar. The main menu has 'Services' and 'Resource Groups' dropdowns.

The left sidebar is titled 'AWS services' and lists recently visited services (Billing, IAM, EC2, EC2 Container Service, Elastic Beanstalk) and all services under Compute, Storage, and Management Tools categories.

The right sidebar features a 'Helpful links' section with 'My Account' (My Organization, My Billing Dashboard, My Security Credentials), a 'Sign Out' link, and a 'Create an organization' button (enclosed in a red box). Below this is a 'What's new?' section with announcements for Amazon Chime and Elastic Volumes for Amazon EBS, each with a 'Learn more' link.

A red box highlights the 'My Organization' link in the 'Helpful links' section.

Bottom navigation bar: https://console.aws.amazon.com/billing/home?region=us-west-2

# Billing - dashboard

greatlearning

The screenshot shows the AWS Billing Management dashboard. At the top, it displays the current month-to-date balance for April 2017, which is \$0.00. Below this, there is a bar chart comparing costs from Last Month (March 2017) and Month-to-Date (April 2017). The chart shows a blue bar for March at \$0.02 and a green bar for April at \$0.01. To the right of the chart, a table provides a breakdown of charges:

Category	Amount Due
No Amount Due	\$0.00
Tax	\$0.00
Total	\$0.00

Below the chart, there are two checkboxes: "Important Information about these Costs" and "Include Subscription Charges". The "Include Subscription Charges" checkbox is checked. Under the "Alerts & Notifications" section, there is a callout box with the following text:

Monitor your estimated charges. [Enable Now](#) to begin setting billing alerts that automatically e-mail you when charges reach a threshold you define.

IAM access to your account's billing information is not enabled. You can enable it on the [Account Information](#) page.

At the bottom of the page, there are links for Feedback, English, Privacy Policy, and Terms of Use.

# Billing - dashboard

The screenshot shows the AWS Billing Management Preferences page. On the left, a sidebar lists various options like Dashboard, Bills, Cost Explorer, etc., with 'Preferences' selected. The main area is titled 'Preferences' and contains three sections:

- Receive PDF Invoice By Email**: Turn on this feature to receive a PDF version of your invoice by email. Invoices are generally available within the first three days of the month.
- Receive Billing Alerts**: Turn on this feature to monitor your AWS usage charges and recurring fees automatically, making it easier to track and manage your spending on AWS. A note below says: "You can set up billing alerts to receive email notifications when your charges reach a specified threshold. Once enabled, this preference cannot be disabled. Manage Billing Alerts or try the new budgets feature!" This section is highlighted with a red rectangle and a red arrow points to it from the bottom.
- Receive Billing Reports**: Turn on this feature to receive ongoing reports of your AWS charges once or more daily. AWS delivers these reports to the Amazon S3 bucket that you specify where indicated below. For consolidated billing customers, AWS generates reports only for paying accounts. Linked accounts cannot sign up for billing reports.

Below the sections are input fields for "Save to S3 Bucket:" (with "bucket name" placeholder) and a "Verify" button, followed by a "Save preferences" button at the bottom.

**click**

# Billing - dashboard

The screenshot shows the AWS CloudWatch Billing Alarms page. The left sidebar has a 'Billing' section with a 'Create Alarm' button highlighted by a red box. The main content area is titled 'Billing Alarms' and explains how CloudWatch can monitor AWS bill charges via email alerts. It mentions free alarms and notifications. The right sidebar contains 'Additional Info' links.

Billing Alarms

Amazon CloudWatch can help you monitor the charges on your [AWS bill](#) by sending you email alerts when charges exceed a threshold you define.

Once you update your preferences in the Account Billing console, you will begin receiving Amazon CloudWatch metrics that reflect your month-to-date AWS charges. Then, you can create a billing alarm by specifying a spending threshold and an e-mail address to notify. [Learn more about billing alerts](#)

You get 10 free alarms and 1,000 free e-mail notifications each month as part of the [AWS Free Tier](#).

[Create Alarm](#)

**Additional Info**

- [Getting Started Guide](#)
- [Monitoring Scripts Guide](#)
- [Overview and Features](#)
- [Documentation](#)
- [Forums](#)
- [Report an Issue](#)

# Billing - dashboard

The screenshot shows the 'Create Alarm' dialog box for a 'Billing Alarm'. The dialog is titled 'Create Alarm' and has a sub-section titled 'Billing Alarm'. It contains instructions: 'You can create a billing alarm to receive e-mail alerts when your AWS charges exceed a threshold you choose. Simply:' followed by three steps: 1. Enter a spending threshold, 2. Provide an email address, 3. Check your inbox for a confirmation email and click the link provided. A red box highlights the input field 'exceed: \$ 10 USD'. Below this, there's a note: 'Reminder: for each address you add, you will receive an email from AWS with the subject "AWS Notification - Subscription Confirmation". Click the link provided in the message to confirm that AWS may deliver alerts to that address.' The 'Alarm Preview' section shows a graph titled 'EstimatedCharges > 10' with a blue line above a red horizontal line at the value of 10. The 'Additional Info' sidebar on the right includes links to 'Getting Started Guide', 'Monitoring Scripts Guide', 'Overview and Features', 'Documentation', 'Forums', and 'Report an Issue'. At the bottom of the dialog, there are buttons for 'Cancel', 'Previous', 'Next', and a prominent blue 'Create Alarm' button.

**The email needs to be verified in 72hrs.**

# Billing - dashboard, itemized view

The screenshot shows the AWS Billing Management Dashboard. On the left, a sidebar lists various services: Dashboard, Bills, Cost Explorer, Budgets, Reports, Cost Allocation Tags, Payment Methods, Payment History, Consolidated Billing, Preferences, Credits, Tax Settings, and DevPay. The main area features a large bar chart titled "Spend Summary" showing spending for March (Last Month), April (Month-to-Date), and April (Forecast). The total for April is \$28.31. Below the chart is a section titled "What's New in AWS Billing and Cost Management?" which includes links to AWS Budgets, Cost Explorer, and the ability to upload Cost and Usage Reports. To the right is a donut chart titled "Month-to-Date Spend by Service" showing the distribution of costs across different services. A red box highlights a table of detailed service costs:

Service	Cost
Registrar	\$21.00
EC2	\$2.41
Route53	\$1.01
S3	\$0.08
Other Services	\$0.13
Tax	\$3.68
<b>Total</b>	<b>\$28.31</b>

At the bottom, there are sections for "Alerts & Notifications" and "Important Information about these Costs".

# How much are we talking about?

The screenshot shows the AWS EC2 Management console interface. On the left, a sidebar lists various services: EC2 Dashboard, Instances, Images, Elastic Block Store, Network & Security, and more. The main content area displays resource statistics for the US West (Oregon) region:

Category	Value
Running Instances	0
Dedicated Hosts	0
Volumes	0
Key Pairs	2
Placement Groups	0
Elastic IPs	0
Snapshots	0
Load Balancers	0
Security Groups	5

A callout box highlights a promotional message: "Just need a simple virtual private server? Get everything you need to jumpstart your project - compute, storage, and networking – for a low, predictable price. Try Amazon Lightsail for free."

In the center, there's a "Create Instance" section with a "Launch Instance" button. Below it, a note says: "Note: Your instances will launch in the US West (Oregon) region".

The right side of the page contains sections for "Account Attributes" (Supported Platforms, VPC, Default VPC), "Additional Information" (Getting Started Guide, Documentation, All EC2 Resources, Forums, Pricing), and "AWS Marketplace" (listing Barracuda NextGen Firewall F-Series - PAYG).

At the bottom, there are links for Feedback, English, and a footer with copyright information: "© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use".

# How much are we talking about?

The screenshot shows the AWS EC2 Management console with the 'Pricing' tab selected. The left sidebar lists various EC2-related links, with 'Pricing' highlighted. The main content area is divided into two main sections: 'On-Demand' and 'Spot Instances'.

**On-Demand**

With On-Demand instances, you pay for compute capacity by the hour with no long-term commitments or upfront payments. You can increase or decrease your compute capacity depending on the demands of your application and only pay the specified hourly rate for the instances you use.

On-Demand instances are recommended for:

- Users that prefer the low cost and flexibility of Amazon EC2 without any up-front payment or long-term commitment
- Applications with short-term, spiky, or unpredictable workloads that cannot be interrupted
- Applications being developed or tested on Amazon EC2 for the first time

**See On-Demand Pricing**

**Spot Instances**

Amazon EC2 Spot instances allow you to bid on spare Amazon EC2 computing capacity for up to 90% off the On-Demand price. [Learn More.](#)

Spot instances are recommended for:

- Applications that have flexible start and end times
- Applications that are only feasible at very low compute prices
- Users with urgent computing needs for large amounts of additional capacity

**See Spot Pricing**

**Related Links**

- Amazon EC2 Spot Instances
- Amazon EC2 Reserved Instances
- Amazon EC2 Dedicated Hosts
- Amazon EC2 Dedicated Instances
- Windows Instances

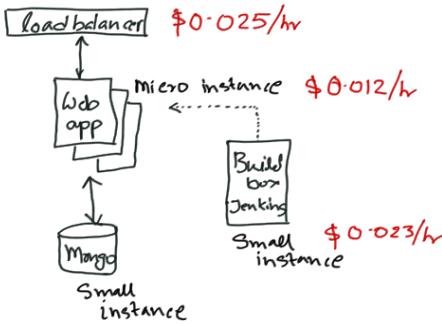
VIA AMAZON CLOUD ON AWS

# How much are we talking about?

The screenshot shows the AWS EC2 Management console with the URL <https://aws.amazon.com/ec2/pricing/on-demand/>. The left sidebar includes links for Amazon EC2, Product Details, Instances, Developer Resources, FAQs, Getting Started, Amazon EC2 Run Command, and Pricing. The main content area is titled "Windows with SQL Enterprise" and shows a table of instance types with their specifications and prices.

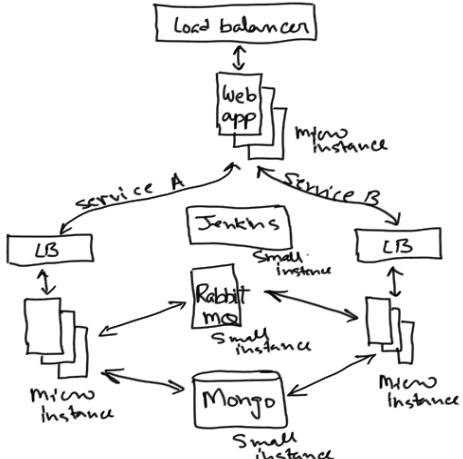
Instance Type	vCPU	ECU	Memory (GiB)	Instance Storage (GB)	Linux/UNIX Usage
t2.nano	1	Variable	0.5	EBS Only	\$0.0059 per Hour
t2.micro	1	Variable	1	EBS Only	\$0.012 per Hour
t2.small	1	Variable	2	EBS Only	\$0.023 per Hour
t2.medium	2	Variable	4	EBS Only	\$0.047 per Hour
t2.large	2	Variable	8	EBS Only	\$0.094 per Hour
t2.xlarge	4	Variable	16	EBS Only	\$0.188 per Hour
t2.2xlarge	8	Variable	32	EBS Only	\$0.376 per Hour
m4.large	2	6.5	8	EBS Only	\$0.108 per Hour

# How much are we talking about?



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

Per hour cost is ~ \$0.11



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

Per hour cost is ~ \$0.26

# Cost of Ownership

AWS Management AWS Total Cost of C x SKL

Secure | https://aws.amazon.com/tco-calculator/ Apps Napabrick BB GCloud AWS Azure Trello Gmail Google analytics pointernext - Doc AWS Documenta

Menu Amazon web services Products Solutions Pricing Software Support Customers Partners Enterprises Startups More English My Account Sign In to the Console

ABOUT AWS  
TCO Calculator  
RELATED LINKS  
What is Cloud Computing?  
AWS Free Usage Tier

## AWS Total Cost of Ownership (TCO) Calculators

AWS helps you reduce Total Cost of Ownership (TCO) by reducing the need to invest in large capital expenditures and providing a pay-as-you-go model that empowers you to invest in the capacity you need and use it only when the business requires it.

Our TCO calculators allow you to estimate the cost savings when using AWS and provide a detailed set of reports that can be used in executive presentations. The calculators also give you the option to modify assumptions that best meet your business needs.

### AWS Total Cost of Ownership (TCO) Calculator

Use this new calculator to compare the cost of your applications in an on-premises or traditional hosting environment to AWS. Describe your on-premises or hosting environment configuration to produce a detailed cost comparison with AWS.

What kind of resources are you comparing against?  
What kind of resources do you have available?

Services  
AWS provides many services to make it easier to build, run, and manage your applications. You can choose from a variety of services to get started.

Compute  
Compute services are designed to help you build, run, and scale your applications. You can choose from a variety of compute services to get started.

Storage  
Storage services are designed to help you store, manage, and analyze your data. You can choose from a variety of storage services to get started.

You could save 69% a year by moving your infrastructure to AWS.  
Your three year total savings equals to \$ 654,804

1. Describe your existing or planned on-premises or hosting infrastructure in four steps, or enter detailed configurations.

2. Get an instant summary report which shows you the three year TCO comparison by cost categories.

3. Download a full report including detailed cost breakdowns, Methodology, Assumptions, and FAQ or store the report in Amazon S3 for sharing with others.

Ready to find out how much you could be saving in the AWS Cloud?

Launch the TCO Calculator »

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

# Cost of Ownership

The screenshot shows the AWS Management console with the TCO Calculator open. A red box highlights the 'Advanced' button at the top right of the calculator's header.

**AWS Total Cost of Ownership (TCO) Calculator** Advanced

Use this calculator to compare the cost of running your applications in an on-premises or colocation environment to AWS. Describe your on-premises or colocation configuration to produce a detailed cost comparison with AWS. You can switch between the basic and advanced views to provide additional configuration details.

Select Currency: United States Dollar

What type of environment are you comparing against?  On-Premises  Colocation

Which AWS region is ideal for your geo requirements? Asia Pacific (Singapore)

Choose workload type: General

**Servers**  
Are you comparing physical servers or virtual machines?  Physical Servers  Virtual Machines  
Provide your configuration details:

Server Type	App. Name	Number of VMs	CPU Cores	Memory(GB)	Hypervisor	Guest OS	DB Engine	VM Usage (%)	Optimize By	Virtualization Host	
Non DB	AppServer	20	8	128	VMware	Linux		65	RAM	Host 1: 2 CPU, €	X
Non DB	WebServer	5	4	64	VMware	Linux		40	RAM	Host 1: 2 CPU, €	X
DB	DB	2	8	256	VMware		MySQL	75	RAM	Host 1: 2 CPU, €	X

Total no.of VMs: 27 + Add Row

# Cost of Ownership

AWS Management   TCO Calculator

Secure | https://awstcoccalculator.com

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

Contact Sales

Amazon web services

Storage

Provide your storage footprint details

Storage Type	Raw Storage Capacity	% Accessed Infrequently	Max IOPS for Application	Backup % Month
SAN	100 TB		25000	100

+ Add Row

Network

Provide your Data Center Bandwidth details (Optional)

Data Center Bandwidth (Mbit/s)	Peak/Average Ratio
250	5

IT Labor

Provide your Data Center Staff details (Optional)

Burdened Annual Salary	Number of VMs per Admin
\$ 50,000	2

Calculate TCO

CERTIFIED BY ✓  
FROST & SULLIVAN

# Cost of Ownership

The screenshot shows the AWS TCO Calculator interface. At the top, there's a navigation bar with tabs for 'AWS Management' and 'TCO Calculator'. Below the navigation is a toolbar with various icons for 'Apps', 'Napabrick', 'BB', 'GCloud', 'AWS', 'Azure', 'Trello', 'Gmail', 'Google analytics', 'pointernext - Do', and 'AWS Documenta'. The main content area features the AWS logo and buttons for 'Contact Sales' and 'Download Report'. A central heading reads 'AWS Total Cost of Ownership (TCO) Calculator'. Below it, a message asks if users are satisfied with the calculator, with thumbs up and thumbs down icons. Another message invites users to take a survey about the calculator. A large callout bubble from a cartoon character says 'Cloud it is!!'. The 'On-Premises vs. AWS Summary' section highlights a 41% savings by moving to AWS, totaling \$1,766,989 over three years. A '3 Years Cost Breakdown' chart compares On-Premises costs (Server, Storage, Network, IT Labor) against AWS costs. A table summarizes the 3-year total cost of ownership for Server and Storage.

You could save **41%** a year by moving your infrastructure to AWS.  
Your three year total savings would be **\$ 1,766,989**.

3 Years Cost Breakdown

Legend: Server (Yellow), Storage (Blue), Network (Light Blue), IT Labor (Orange)

	On-Premises	AWS
Server	\$ 1,311,277	\$ 974,508
Storage	\$ 614,960	\$ 403,960



# Identity and Access Management (IAM)

## Fundamentals & Multi Factor Authentication setup

# Overview - Security services

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

# Activity - Custom AWS signin URL

The screenshot shows the AWS IAM Management Console dashboard. A red box highlights the "Welcome to Identity and Access Management" section, which contains the "IAM users sign-in link" and its URL: <https://sklabs.signin.aws.amazon.com/console>. This URL is also copied to the clipboard.

**Note:** The Password Policy page has been renamed to Account Settings. Click Account Settings to find your account's password policy and other configuration options.

**Welcome to Identity and Access Management**

IAM users sign-in link:  
<https://sklabs.signin.aws.amazon.com/console> [Customize](#) | [Copy Link](#)

**IAM Resources**

Users: 0	Roles: 2
Groups: 0	Identity Providers: 0
Customer Managed Policies: 0	

**Security Status** 1 out of 5 complete.

- Delete your root access keys
- Activate MFA on your root account
- Create individual IAM users
- Use groups to assign permissions

**Feature Spotlight**

Introduction to AWS IAM

0:00 / 2:16

**Additional Information**

[IAM documentation](#)  
[Web Identity Federation Playground](#)  
[Policy Simulator](#)  
[Videos, IAM release history and additional resources](#)

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

# Activity - MFA setup

- Good idea to enable on the root account
  - Root a/c is the email that you used to signup in AWS
  - Can be setup on all accounts
- Install the "AWS Virtual MFA" on your mobile device, choices are
  - Google authenticator app (install this)
  - AWS Virtual MFA app - provided by "AWS Mobile LLC"

# Activity - MFA setup

IAM Management Cons x SKL

https://console.aws.amazon.com/iam/home?region=ap-southeast-1#home

Apps Bitbucket G Dev Console GAE Console GS Root C\* OpsCenter FlipBasket AWS Console tech-research

AWS Services Edit Skroidslab Global Support

Dashboard Search IAM

Details Groups Users Roles Policies Identity Providers Account Settings Credential Report

Encryption Keys

The Password Policy page has been renamed to Account Settings. Click Account Settings to find your account's password policy and other configuration options.

Welcome to Identity and Access Management

IAM users sign-in link: https://sklabs.signin.aws.amazon.com/console

Manage MFA Device

Select the type of MFA device to activate:

A virtual MFA device

A hardware MFA device

For more information about supported MFA devices, see [AWS Multi-Factor Authentication](#).

Cancel Next Step

Activate multi-factor authentication (MFA) on your AWS root account to add another layer of protection to help keep your account secure. [Learn More](#)

Manage MFA

Create individual IAM users

Introduction to AWS IAM

Additional Information

IAM documentation Web Identity Federation Playground Policy Simulator Videos, IAM release history and additional resources

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

# Activity - MFA setup

IAM Management Cons × Multi-Factor Authentica × SKL

https://console.aws.amazon.com/iam/home?region=ap-southeast-1#home

Apps Bitbucket G Dev Console GAE Console GS Root C\* OpsCenter FlipBasket AWS Console tech-research

AWS Services Edit Skroidslab Global Support

Dashboard Search IAM

Details Groups Users Roles Policies Identity Providers Account Settings Credential Report

Encryption Keys

The Password Policy page has been renamed to Account Settings. Click Account Settings to find your account's password policy and other configuration options.

Welcome to Identity and Access Management

IAM users sign-in link:

https://

Manage MFA Device

To activate a virtual MFA device, you must first install an AWS MFA-compatible application on the user's smartphone, PC, or other device. You can find a list of AWS MFA-compatible applications [here](#). After the application is installed, click Next Step to configure the virtual MFA.

Don't show me this dialog box again.

Cancel Previous Next Step

Activate multi-factor authentication (MFA) on your AWS root account to add another layer of protection to help keep your account secure. [Learn More](#)

Manage MFA

Create individual IAM users

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

# Activity - MFA setup

SKL

C India 29/0 (15.3 ov, M V x IAM Management Cons x

https://console.aws.amazon.com/iam/home?region=ap-southeast-1#home

Apps Bitbucket G Dev Console GAE Console GS Root C OpsCenter FlipBasket AWS Console tech-research

Manage MFA Device

If your virtual MFA application supports scanning QR codes, scan the following image with your smartphone's camera.



Show secret key for manual configuration

After the application is configured, enter two consecutive authentication codes in the boxes below and click Activate Virtual MFA.

Authentication Code 1

Authentication Code 2

Cancel Previous Activate Virtual MFA

Feedback English

Skroidslab Global Support

Introduction to AWS IAM 0:00 / 2:16

... 0:00 / 2:16

Additional Information Documentation Identity Federation Playground Simulator IAM release history and final resources

# Activity - MFA setup

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



# Compute - Part I

## EC2 introduction

# Overview - Elastic Compute Cloud

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

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

# Overview - Elastic Compute Cloud

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

# Activity - EC2 Dashboard

The screenshot shows the AWS EC2 Management Console dashboard for the US West (Oregon) region. The left sidebar contains navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances (Instances, Spot Requests, Reserved Instances, Commands, Dedicated Hosts), Images (AMIs, Bundle Tasks), Elastic Block Store (Volumes, Snapshots), Network & Security (Security Groups, Elastic IPs, Placement Groups), and Key Pairs.

The main content area displays the following information:

- Resources:** You are using the following Amazon EC2 resources in the US West (Oregon) region:
  - 0 Running Instances
  - 0 Dedicated Hosts
  - 0 Volumes
  - 0 Key Pairs
  - 0 Placement Groups
  - 0 Elastic IPs
  - 0 Snapshots
  - 0 Load Balancers
  - 1 Security Groups
- A callout box states: "Easily run and manage Docker applications. Try Amazon EC2 Container Service."
- Create Instance:** To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.  
[Launch Instance](#)
- Note:** Your instances will launch in the US West (Oregon) region
- Service Health:** Service Status: US West (Oregon): This service is operating normally
- Scheduled Events:** US West (Oregon): No events
- Account Attributes:** Supported Platforms: VPC; Default VPC: vpc-51238934
- Additional Information:** Getting Started Guide, Documentation, All EC2 Resources, Forums, Pricing, Contact Us
- AWS Marketplace:** Find free software trial products in the AWS Marketplace from the [EC2 Launch Wizard](#). Or try these popular AMIs: Tableau Server (10 users) Provided by Tableau

At the bottom, there are links for Feedback, English, Copyright notice (2008-2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.), Privacy Policy, and Terms of Use.

# Activity - EC2 launch instance

The screenshot shows the AWS EC2 Management Console interface. The URL in the address bar is <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard>. The top 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 user is signed in as Skroidslab, located in Oregon, with Support options available.

The main content area displays the "Step 1: Choose an Amazon Machine Image (AMI)" page. The steps are numbered 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Tag Instance, 6. Configure Security Group, and 7. Review. A "Cancel and Exit" button is visible on the right.

**Quick Start** sidebar:

- My AMIs
- AWS Marketplace
- Community AMIs
- Free tier only (i)

**Amazon Linux AMI 2015.09.1 (HVM), SSD Volume Type - ami-f0091d91**

**Select** button (64-bit)

Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

Root device type: ebs Virtualization type: hvm

**Red Hat Enterprise Linux 7.1 (HVM), SSD Volume Type - ami-4dbf9e7d**

**Select** button (64-bit)

Red Hat Enterprise Linux version 7.1 (HVM), EBS General Purpose (SSD) Volume Type

Root device type: ebs Virtualization type: hvm

**SUSE Linux Enterprise Server 12 (HVM), SSD Volume Type - ami-d7450be7**

**Select** button (64-bit)

SUSE Linux Enterprise Server 12 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.

Root device type: ebs Virtualization type: hvm

Navigation: < 1 to 22 of 22 AMIs >

# Activity - EC2 launch instance

The screenshot shows the AWS EC2 Management Console Launch Instance Wizard at Step 2: Choose an Instance Type. The URL is <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard:2>. The page displays a table of instance types, with the t2.micro type selected. A tooltip indicates it is a "Free tier eligible" instance.

**Step 2: Choose an Instance Type**

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	m4.large	2	8	EBS only	Yes	Moderate

Currently selected: t2.micro (Variable clock speed, Intel Xeon Family, 1 GiB memory, EBS only)  
All generations

Filter by: All instance types Current generation Show/Hide Columns

Cancel Previous Review and Launch Next: Configure Instance Details

# Activity - EC2 launch instance

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#LaunchInstanceWizard>. The top navigation bar includes links for Apps, AWS, GCP, CloudPads, Azure, BB, Gmail, CRaSH, PN-Docker Hub, AWS INNOVATE, GA PointerNext, Services, Resource Groups, EC2, S3, Lambda, and CloudWatch Metrics. The user is on Step 3: Configure Instance Details, which is the third step in the Launch Instance Wizard. The page title is "Step 3: Configure Instance Details". A sub-instruction says: "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." The configuration fields include:

- Number of instances:** 1 (checkbox for "Launch into Auto Scaling Group" is available)
- Purchasing option:** Request Spot instances (checkbox)
- Network:** vpc-51238934 | default-vpc (default) (dropdown, options: Create new VPC)
- Subnet:** No preference (default subnet in any Availability Zone) (dropdown, options: Create new subnet)
- Auto-assign Public IP:** Use subnet setting (Enable) (dropdown)
- IAM role:** None (dropdown, options: Create new IAM role)
- Shutdown behavior:** Stop (dropdown)
- Enable termination protection:** Protect against accidental termination (checkbox)
- Monitoring:** Enable CloudWatch detailed monitoring (checkbox, note: Additional charges apply)
- Tenancy:** Shared - Run a shared hardware instance (dropdown, note: Additional charges will apply for dedicated tenancy)
- T2 Unlimited:** Enable (checkbox, note: Additional charges may apply)

At the bottom, there are buttons for "Cancel", "Previous", "Review and Launch" (highlighted in blue), and "Next: Add Storage". The footer includes links for Feedback, English (US), and legal notices: © 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved., Privacy Policy, and Terms of Use.

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

# Activity - EC2 launch instance

EC2 Management > EC2 > Launch Instance Wizard

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

Current price:

Availability Zone	Current price
us-west-2a	\$0.0058 USD
us-west-2b	\$0.0057 USD
us-west-2c	\$0.0058 USD

Maximum price: \$ [e.g. 0.045 = 4.5 cents/instance (Optional)]

Persistent request: [checkbox]

Launch group: [Optional]

Request valid from: Any time

Request valid to: Any time

Network: vpc-51238934 | default-vpc (default)

Create new VPC

Subnet: No preference (default subnet in any Availability Zone)

Create new subnet

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

IAM role: None

Create new IAM role

Monitoring: [checkbox] Enable CloudWatch detailed monitoring  
Additional charges apply.

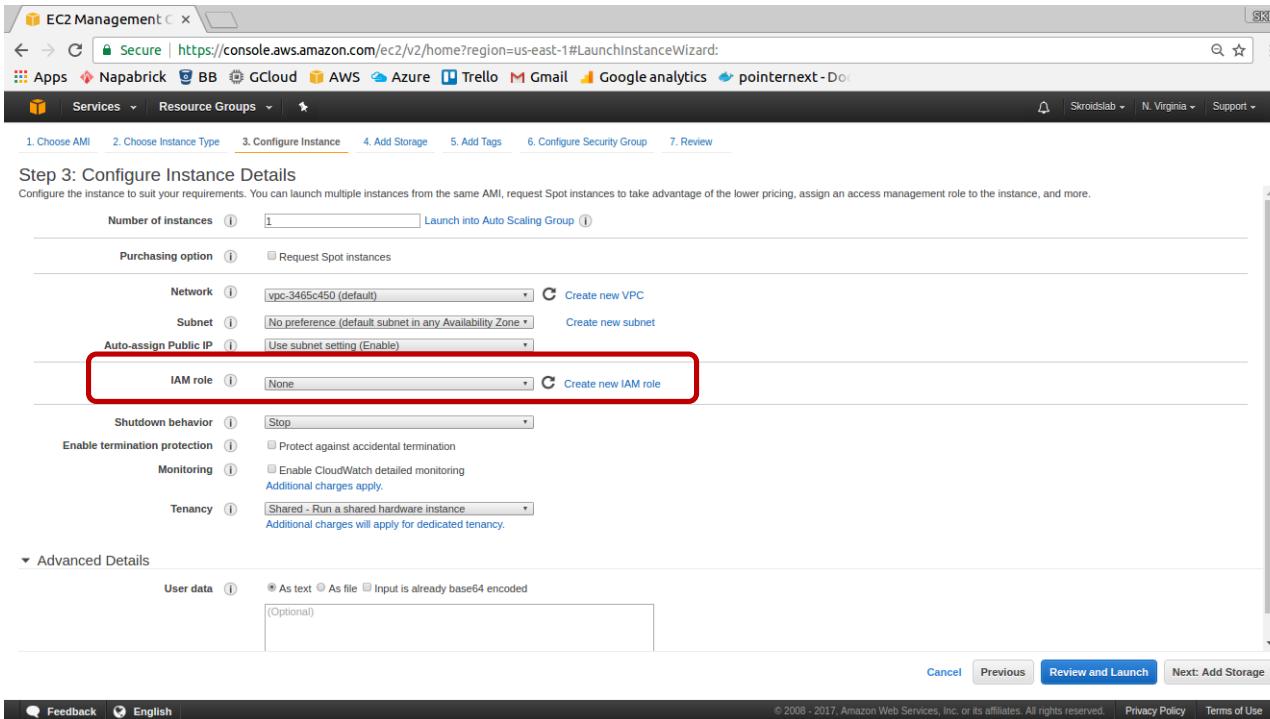
Advanced Details

Cancel Previous Review and Launch Next: Add Storage

Feedback English (US)

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

# Activity - EC2 launch instance



The screenshot shows the AWS EC2 Management console with the URL <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard>. The page is titled "Step 3: Configure Instance Details". It displays various configuration options for launching an EC2 instance, including the number of instances (1), purchasing option (Request Spot instances), network (vpc-3465c450), subnet (No preference), and auto-assign public IP (Use subnet setting). A red box highlights the "IAM role" dropdown, which is set to "None". Other visible options include shutdown behavior (Stop), enable termination protection (Protect against accidental termination), monitoring (Enable CloudWatch detailed monitoring), and tenancy (Shared - Run a shared hardware instance). At the bottom, there's an "Advanced Details" section for user data, and at the very bottom, buttons for "Cancel", "Previous", "Review and Launch", and "Next: Add Storage".

**Important! What happens if you miss adding a role?**

# Activity - EC2 launch instance

The screenshot shows the AWS EC2 Management Console interface for launching an instance. The URL in the browser is <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard>. The top 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 user is currently at Step 4: Add Storage, which is highlighted in the breadcrumb trail.

**Step 4: Add Storage**

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination	Encrypted
Root	/dev/xvda	snap-ad8e61f8	8	General Purpose (SSD)	24 / 3000	<input checked="" type="checkbox"/>	Not Encrypted

**Add New Volume**

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Buttons at the bottom: Cancel, Previous, **Review and Launch**, Next: Tag Instance.

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

# Activity - EC2 launch instance

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	snapshot-0fb695076fc43043	8	General Purpose SSD (GP2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	Search (case-insensit)	500	General Purpose SSD (GP2)	1500 / 3000	N/A	<input type="checkbox"/>	

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Cancel Previous Review and Launch Next: Add Tags

Feedback English © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

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

# Activity - EC2 launch instance

The screenshot shows the AWS EC2 Management console with the URL <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:5>. The top navigation bar includes links for Apps, Napabrick, BB, GCloud, AWS, Azure, Trello, Gmail, Google analytics, and pointernext. The main navigation bar shows Services and Resource Groups. The breadcrumb trail indicates the user is at Step 5 of the Launch Instance Wizard.

**Step 5: Add Tags**

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

The interface shows two input fields: "Key" (127 characters maximum) and "Value" (255 characters maximum). Below these fields is a message: "This resource currently has no tags". A note below the fields says: "Choose the Add tag button or [click to add a Name tag](#). Make sure your [IAM policy](#) includes permissions to create tags." At the bottom left is a "Add Tag" button with the note "(Up to 50 tags maximum)". At the bottom right are buttons for "Cancel", "Previous", "Review and Launch" (which is highlighted in blue), and "Next: Configure Security Group".

# Activity - EC2 launch instance

The screenshot shows the AWS EC2 Management console with the URL <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard>. The browser tabs include EC2 Management, SKL, Secure, and various bookmarks like Apps, Napbrick, BB, GCloud, AWS, Azure, Trello, Gmail, Google analytics, and pointernext. The main navigation bar has links for Services (selected), Resource Groups, and a bell icon. The region is set to N. Virginia.

The wizard is at Step 5: Add Tags. The steps are: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags (selected), 6. Configure Security Group, 7. Review.

**Step 5: Add Tags**

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

Key	(127 characters maximum)	Value	(255 characters maximum)	Instances	Volumes	
Name		http-server-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="X"/>
Owner		Nirmallya		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="X"/>
Empld		16528		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="X"/>
Department		SI		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="X"/>

**Add another tag** (Up to 50 tags maximum)

Cancel Previous **Review and Launch** Next: Configure Security Group

Feedback English © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

# Activity - EC2 launch instance

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#LaunchInstanceWizard>. The navigation bar includes CloudSKL, Apps, Technical, AWS, GCP, CloudPads, Azure, BB, Gmail, CRASH, PN-Docker Hub, and AWS INNOVATE. The main menu has Services and Resource Groups.

The wizard is at Step 6: Configure Security Group. The steps are: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group (highlighted), 7. Review.

**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: open-ssh

Description: Open port 22 for SSH

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Anywhere	0.0.0.0/0, ::/0 ssh

Add Rule

**Warning**  
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel Previous Review and Launch

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

# Activity - EC2 launch instance

EC2 Management C x SKL

Secure | https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard:

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

Services Resource Groups

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

Step 6: Configure Security Group

A security group is a set of firewall rules that control incoming and outgoing traffic to your instances, and allow Internet traffic to reach your instance, among other things. Learn more about Amazon EC2 security groups.

Assign a security group:

Security group name:

Description:

Type:  SSH

Add Rule

**Warning**  
Rules with source of 0.0.0.0/0 allow all traffic.

**Boot from General Purpose (SSD)**

General Purpose (SSD) volumes provide the ability to burst to 3000 IOPS per volume, independent of volume size, to meet the performance needs of most applications and also deliver a consistent baseline of 3 IOPS/GiB.

Make General Purpose (SSD) the default boot volume for all instance launches from the console going forward (recommended).

Make General Purpose (SSD) the boot volume for this instance.

Continue with Magnetic as the boot volume for this instance.

Free tier eligible customers can get up to 30GB of General Purpose (SSD) storage.

Don't show again

Next

Cancel Previous Review and Launch

Feedback English

© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

# Activity - EC2 launch instance

The screenshot shows the AWS EC2 Management Console at the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard:>. The browser title bar says "EC2 Management Cons x". The navigation bar includes links for Apps, Bitbucket, G Dev Console, GAE Console, GS Root, OpsCenter, FlipBasket, AWS Console, AWS Docs, and tech-research. The top right shows account information: Skroddab, Oregon, Support.

The main content area is titled "Step 7: Review Instance Launch". It displays the following details:

- AMI Details:** Amazon Linux AMI 2015.09.1 (HVM), SSD Volume Type - ami-f0091d91. Status: Free tier eligible.
- Instance Type:** t2.micro (Edit instance type). Configuration: ECUs: Variable, vCPUs: 1, Memory (GiB): 1, Instance Storage (GB): EBS only, EBS-Optimized Available: -, Network Performance: Low to Moderate.
- Security Groups:** Security group name: launch-wizard-1, Description: launch-wizard-1 created 2015-12-13T17:02:39.635+05:30. Rules: Type: SSH, Protocol: TCP, Port Range: 22, Source: 0.0.0.0/0. (Edit security groups)
- Instance Details:** (Edit instance details)
- Storage:** (Edit storage) - Root volume: Type: gp2, Device: /dev/xvda, Snapshot: snap-ad8e61f8, Size (GiB): 8, Volume Type: gp2, IOPS: 24 / 3000, Delete on Termination: Yes, Encrypted: Not Encrypted.
- Tags:** (Edit tags) - Name: Http Server, Owner: Nirmallya.

At the bottom, there are "Cancel", "Previous", and "Launch" buttons. The footer includes links for Feedback, English, Privacy Policy, and Terms of Use, along with copyright information: © 2008–2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Activity - EC2 launch instance

The screenshot shows the AWS EC2 Management Console interface. The main window displays Step 7: Review Instance Launch. It includes sections for AMI Details (Amazon Linux AMI 2015.09.1), Instance Type (t2.micro), and Security Groups. A modal dialog box titled "Select an existing key pair or create a new key pair" is open in the center. The dialog contains instructions about key pairs, a dropdown menu for creating a new key pair ("Create a new key pair"), a text input field for the key pair name ("Key pair name" with "nirmallya" typed in), and a "Download Key Pair" button. Below the button is a note: "You have to download the private key file (\*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created." At the bottom of the dialog are "Cancel" and "Launch Instances" buttons. The background of the main window shows the continuation of the instance configuration process.

# Activity - EC2 launch instance

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#LaunchInstanceWizard>. The browser title bar says "EC2 Management". The top navigation bar includes links for Apps (Napabrick, BB, GCloud, AWS, Azure, Trello, Gmail, Google analytics, pointernext), Services (selected), Resource Groups, and various AWS regions (Skroldslab, Oregon, Support). The main content area is titled "Launch Status". It displays a green box with a checkmark stating "Your instances are now launching" and a link to "View launch log". Below it is a blue box with an info icon and the text "Get notified of estimated charges", which includes a link to "Create billing alerts". A section titled "How to connect to your instances" follows, with a note about instances launching and a link to "View Instances". A "Helpful resources" section lists links to "How to connect to your Linux instance", "Learn about AWS Free Usage Tier", "Amazon EC2: User Guide", and "Amazon EC2: Discussion Forum". A final section lists actions like "Create status check alarms", "Create and attach additional EBS volumes", and "Manage security groups". A "View Instances" button is at the bottom right.

# Activity - EC2 launch instance

The screenshot shows the AWS EC2 Management Console interface. On the left, a sidebar menu lists various services: EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Commands, Dedicated Hosts, Images (AMIs, Bundle Tasks), Elastic Block Store (Volumes, Snapshots), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs). The main content area has tabs for Launch Instance, Connect, and Actions. A search bar at the top says "Filter by tags and attributes or search by keyword". Below it is a table with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, Public DNS, and Public IP. One row is shown: "Http Server" (Instance ID i-48072c8c, t2.micro, us-west-2b, running, Initializing, None, ec2-54-201-208-132.us-west-2.compute.amazonaws.com, 54.201.208.132). A red box highlights the "Public DNS" value. Below the table, detailed instance information is displayed in two columns:

Instance ID	i-48072c8c	Public DNS	ec2-54-201-208-132.us-west-2.compute.amazonaws.com
Instance state	running	Public IP	54.201.208.132
Instance type	t2.micro	Elastic IP	-
Private DNS	ip-172-31-44-93.us-west-2.compute.internal	Availability zone	us-west-2b
Private IPs	172.31.44.93	Security groups	launch-wizard-1, view rules
Secondary private IPs		Scheduled events	No scheduled events
VPC ID	vpc-51238934	AMI ID	amzn-ami-hvm-2015.09.1.x86_64-gp2 (ami-f0091d91)
Subnet ID	subnet-fa921f9f	Platform	-
Network interfaces	eth0	IAM role	-
Source/dest. check	True	Key pair name	nirmalya

At the bottom, 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 - EC2 launch instance

The screenshot shows the AWS EC2 Management Console interface. On the left, a sidebar navigation menu includes options like 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), and Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces). The main content area displays a table of instances. One instance, named 'web-server-1' with the ID i-0749a285532..., is highlighted. The table columns include Name, Instance State, Status Checks, Alarm Status, Public DNS (IPv4), and IPv4 Public IP. The instance state is 'running', with 2/2 checks passing. The Public DNS is ec2-34-209-133-152.us-west-2.compute.amazonaws.com and the IPv4 Public IP is 34.209.133.152. Below the table, two callout boxes provide details about system and instance status checks. A red box highlights the 'System reachability check passed' status under System Status Checks.

This check verifies that your instance is reachable. We test that we are able to get network packets to your instance. If this check fails, there may be an issue with the infrastructure hosting your instance (such as AWS power, networking or software systems). You may need to restart or replace the instance, wait for our systems to resolve the issue, or seek technical support.

This check does not validate that your operating system and applications are accepting traffic.

This check verifies that your instance's operating system is accepting traffic. If this check fails, you may need to reboot your instance or make modifications to your operating system configuration.

System Status Checks

These checks monitor the AWS systems required to use this instance and ensure they are functioning properly.

**System reachability check passed**

Additional Resources

Submit feedback if our checks do not reflect your experience with this instance or if they do not detect the issues you are having. Please note that we will not respond to customer support issues reported via this form. Please post your issue on the [Developer Forums](#) or contact [AWS Support](#) if you need technical assistance with this instance.

Feedback English

© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

# Activity - EC2 launch instance

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

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

# Activity - EC2 install http server

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

OR

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

# Compute - Part I

## Security groups

# Activity - Security group

EC2 Management Consc x SKL

https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Instances:sort=dnsName

Apps Bitbucket G Dev Console GAE Console GS Root C\* OpsCenter FlipBasket AWS Console AWS Docs tech-research

AWS Services Edit Skroidslab Oregon Support

EC2 Dashboard Events Tags Reports Limits

**INSTANCES**

**Instances** (Selected) Spot Requests Reserved Instances Commands Dedicated Hosts

**IMAGES**

AMIs Bundle Tasks

**ELASTIC BLOCK STORE**

Volumes Snapshots

**NETWORK & SECURITY**

Security Groups Elastic IPs Placement Groups Key Pairs

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS	Public IP
Http Server	i-48072c8c	t2.micro	us-west-2b	running	2/2 checks ...	None	ec2-54-201-208-132.us... 54.201	-

Instance: i-48072c8c (Http Server) Public DNS: ec2-54-201-208-132.us-west-2.compute.amazonaws.com

Description Status Checks Monitoring Tags

Instance ID	i-48072c8c	Public DNS	ec2-54-201-208-132.us-west-2.compute.amazonaws.com
Instance state	running	Public IP	54.201.208.132
Instance type	t2.micro	Elastic IP	-
Private DNS	ip-172-31-44-93.us-west-2.compute.internal	Availability zone	us-west-2b
Private IPs	172.31.44.93	Security groups	launch-wizard-1, <a href="#">view rules</a>
Secondary private IPs			
VPC ID	vpc-51238934		
Subnet ID	subnet-fa921f9f		
Network interfaces	eth0		
Source/dest. check	True		

Security Groups associated with i-48072c8c

Ports	Protocol	Source	launched-wizard-1
22	tcp	0.0.0.0/0	✓

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

# Activity - Security group

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation menu includes: Instances, Spot Requests, Reserved Instances, Commands, Dedicated Hosts, IMAGES (AMIs, Bundle Tasks), ELASTIC BLOCK STORE (Volumes, Snapshots), NETWORK & SECURITY (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), LOAD BALANCING (Load Balancers), and AUTO SCALING (Launch Configurations). The 'Security Groups' option under 'NETWORK & SECURITY' is selected.

The main content area displays the 'Create Security Group' dialog box. The 'Security group name' field contains 'port-80'. The 'Description' field contains 'Open port 80'. The 'VPC' dropdown is set to 'vpc-51238934 (172.31.0.0/16) \*'. Below the dialog, a note states '\* denotes default VPC'. Under the 'Security group rules' section, the 'Inbound' tab is selected. A single rule is listed: Type: HTTP, Protocol: TCP, Port Range: 80, Source: Anywhere (0.0.0.0/0). An 'Add Rule' button is available to add more rules. At the bottom right of the dialog are 'Cancel' and 'Create' buttons.

# Activity - Security group

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with sections like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, AMIs, and more. The Instances section is currently selected. In the main area, an instance named "Http Server" (i-48072c8c) is listed in the "Instances" table. The "Actions" dropdown menu is open over this instance, showing options like Connect, Get Windows Password, Launch More Like This, Instance State, Instance Settings, Image, Networking, Change Security Groups, Attach Network Interface, Detach Network Interface, Disassociate Elastic IP Address, Change Source/Dest. Check, and Manage Private IP Addresses. Below the table, detailed information about the instance is provided, including its Instance ID, Instance state (running), Instance type (t2.micro), Private DNS (ip-172-31-44-93.us-west-2.compute.internal), Private IPs (172.31.44.93), Secondary private IPs, VPC ID (vpc-51238934), Subnet ID (subnet-fa921f9f), Network interfaces (eth0), and Source/dest. check (True). The instance also has Public DNS (ec2-54-201-208-132.us-west-2.compute.amazonaws.com), Public IP (54.201.208.132), and an Elastic IP (None). It is located in the us-west-2b Availability zone and belongs to the launch-wizard-1 security group. Other details include Scheduled events (No scheduled events), AMI ID (amzn-ami-hvm-2015.09.1.x86\_64-gp2 (ami-f0091d91)), Platform (-), IAM role (-), and Key pair name (nirmalya).

# Activity - Security group

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation menu includes options like EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Commands, Dedicated Hosts, AMIs, Bundle Tasks, Volumes, Snapshots, Security Groups, Elastic IPs, Placement Groups, and Key Pairs. The main content area displays a modal dialog titled "Change Security Groups". Inside the dialog, the Instance ID is listed as i-48072c8c and the Interface ID as eni-49e0a430. A sub-section titled "Select Security Group(s) to associate with your instance" lists three security groups:

Security Group ID	Name	Description
sg-05123160	default	default VPC security group
sg-a76855c3	launch-wizard-1	launch-wizard-1 created 2015-12-13T17:02:39.635+05:30
sg-1b665b7f	port-80	Open port 80

At the bottom right of the dialog are "Cancel" and "Assign Security Groups" buttons. Below the dialog, the instance details show Network interfaces: eth0, Source/dest. check: True, IAM role: -, Key pair name: nirmallya. The footer of the page includes links for Feedback, English, Privacy Policy, and Terms of Use.

# Fleet of EC2 instances

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

# Activity - Instance template

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.

**Keep this AMI ID handy**

Quick Start	AMIs	Action
My AMIs	Amazon Linux AMI 2017.09.1 (HVM), SSD Volume Type - ami-bf4193c7	Select
AWS Marketplace	Red Hat Enterprise Linux 7.4 (HVM), SSD Volume Type - ami-9fa343e7	Select
Community AMIs	SUSE Linux Enterprise Server 12 SP3 (HVM), SSD Volume Type - ami-e3ef329b	Select
<input type="checkbox"/> Free tier only	Ubuntu Server 16.04 LTS (HVM), SSD Volume Type - ami-0def3275	Select

# Activity - Instance template

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#LaunchInstanceWizard>. The navigation bar includes CloudSKL, Secure, Apps, AWS, GCP, CloudPads, Azure, BB, Gmail, CRASH, PN-Docker Hub, AWS INNOVATE, GA PointerNext, Services (EC2 selected), Resource Groups, S3, Lambda, Skroidslab, Oregon, Support.

The wizard is at Step 6: Configure Security Group. The instructions state: "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."

Below the instructions, there is a radio button group for "Assign a security group":  Create a new security group and  Select an existing security group. The "Select an existing security group" option has a red box around it.

Security Group ID	Name	Description	Actions
sg-05123160	default	default VPC security group	<a href="#">Copy to new</a>
sg-32750e48	open-8080	Open port 8080 for tomcat to go through	<a href="#">Copy to new</a>
sg-0f64b-74	open-port-22	Open SSH	<a href="#">Copy to new</a>
sg-e866f993	open-port-80	Open HTTP	<a href="#">Copy to new</a>
sg-bd00f0c7	open-rdp	Open port 3389 for remote desktop for Windows	<a href="#">Copy to new</a>
sg-4c465436	open-ssh	Open port 22 for SSH	<a href="#">Copy to new</a>
sg-bc83bfcc	rds-launch-wizard	Created from the RDS Management Console	<a href="#">Copy to new</a>
sg-d47159af	rds-launch-wizard-2	Created from the RDS Management Console	<a href="#">Copy to new</a>

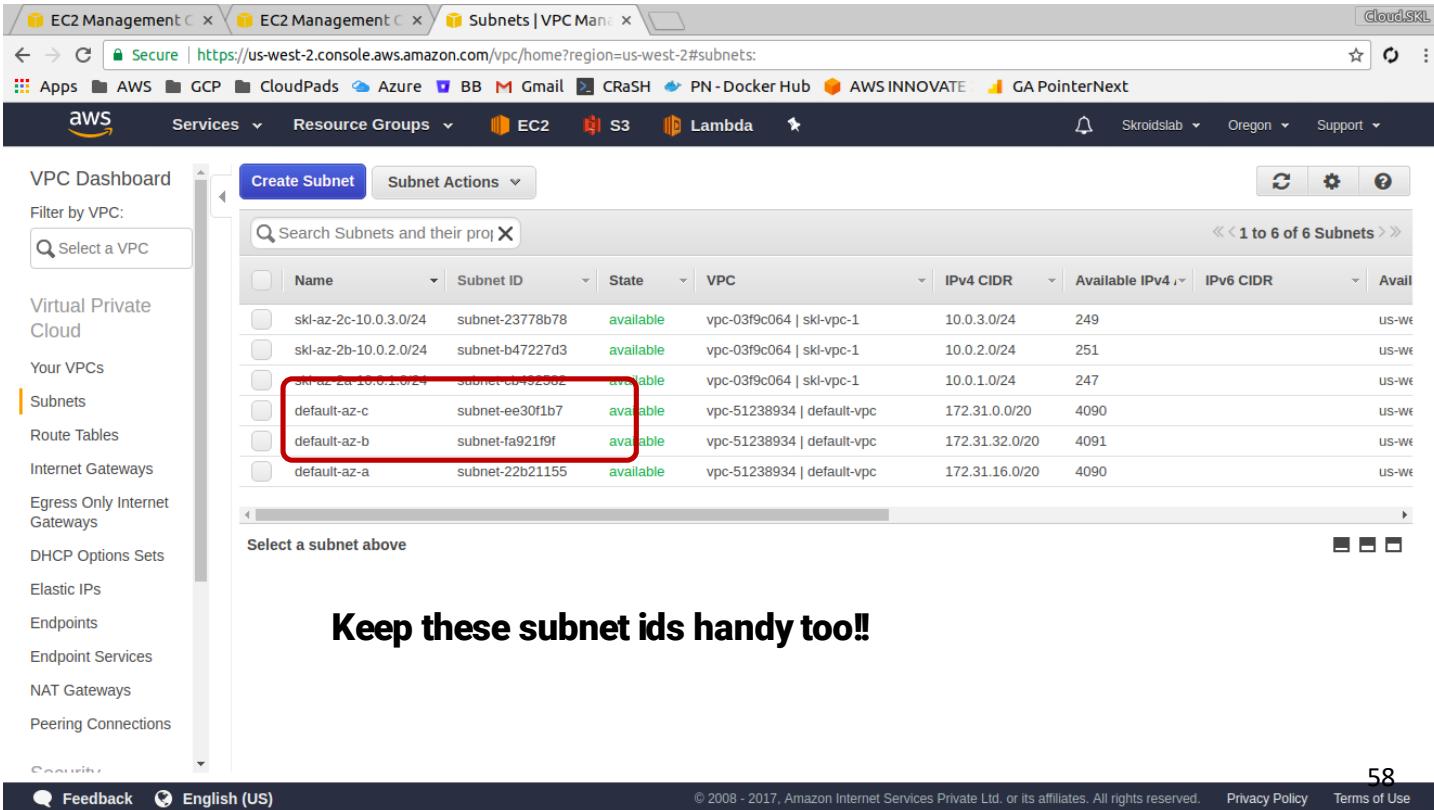
Select a security group above to view its inbound rules.

**Keep these SG ids handy!**

Cancel Previous Review and Launch

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

# Activity - Instance template



The screenshot shows the AWS VPC Subnets management console. The left sidebar navigation includes options like VPC Dashboard, Filter by VPC (with a dropdown menu), Virtual Private Cloud, Your VPCs, Subnets (which is selected and highlighted in orange), Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Endpoint Services, NAT Gateways, and Peering Connections. The main content area displays a table of subnets with columns: Name, Subnet ID, State, VPC, IPv4 CIDR, Available IPv4, IPv6 CIDR, and Available IPv6. Two specific subnets, 'default-az-c' and 'default-az-b', are highlighted with a red box around their rows. A callout text at the bottom center says 'Keep these subnet ids handy too!!'. The bottom navigation bar includes links for Feedback, English (US), Copyright notice, Privacy Policy, and Terms of Use.

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Available IPv6
skl-az-2c-10.0.3.0/24	subnet-23779b78	available	vpc-03f9c064   skl-vpc-1	10.0.3.0/24	249		US-West
skl-az-2b-10.0.2.0/24	subnet-b47227d3	available	vpc-03f9c064   skl-vpc-1	10.0.2.0/24	251		US-West
skl-az-2a-10.0.1.0/24	subnet-cb492502	available	vpc-03f9c064   skl-vpc-1	10.0.1.0/24	247		US-West
<b>default-az-c</b>	<b>subnet-ee30f1b7</b>	<b>available</b>	vpc-51238934   default-vpc	172.31.0.0/20	4090		US-West
<b>default-az-b</b>	<b>subnet-fa9219f</b>	<b>available</b>	vpc-51238934   default-vpc	172.31.32.0/20	4091		US-West
default-az-a	subnet-22b21155	available	vpc-51238934   default-vpc	172.31.16.0/20	4090		US-West

Keep these subnet ids handy too!!

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

# Activity - Instance template

The screenshot shows the AWS EC2 Management console interface. The top navigation bar includes links for Secure, EC2, S3, Lambda, and other services like Apps, AWS, GCP, CloudPads, Azure, BB, Gmail, CRaSH, PN-Docker Hub, AWS INNOVATE, and GA PointerNext. The main content area has a title "Create launch template" with a red box around it, and a search bar below it. A message states "You do not have any Launch Templates in this region" with a sub-instruction "Click the Create Launch Template button to create your first Launch Template". On the left sidebar, under the "INSTANCES" section, the "Launch Templates" item is highlighted with a red box. Other items in the sidebar include Instances, Spot Requests, Reserved Instances, Dedicated Hosts, Scheduled Instances, AMIs, Bundle Tasks, Volumes, and Snapshots. At the bottom, there are links for Feedback, English (US), and footer text: "© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use".

# Activity - Instance template

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#CreateTemplate:>. The page is titled "Create launch template".

**What would you like to do?**

- Create a new template
- Create a new template version

**Launch template name\***

**Template version description**

You can optionally specify a source template if you would like to create a template from another existing template.

**Source template**

**Launch template contents**

Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

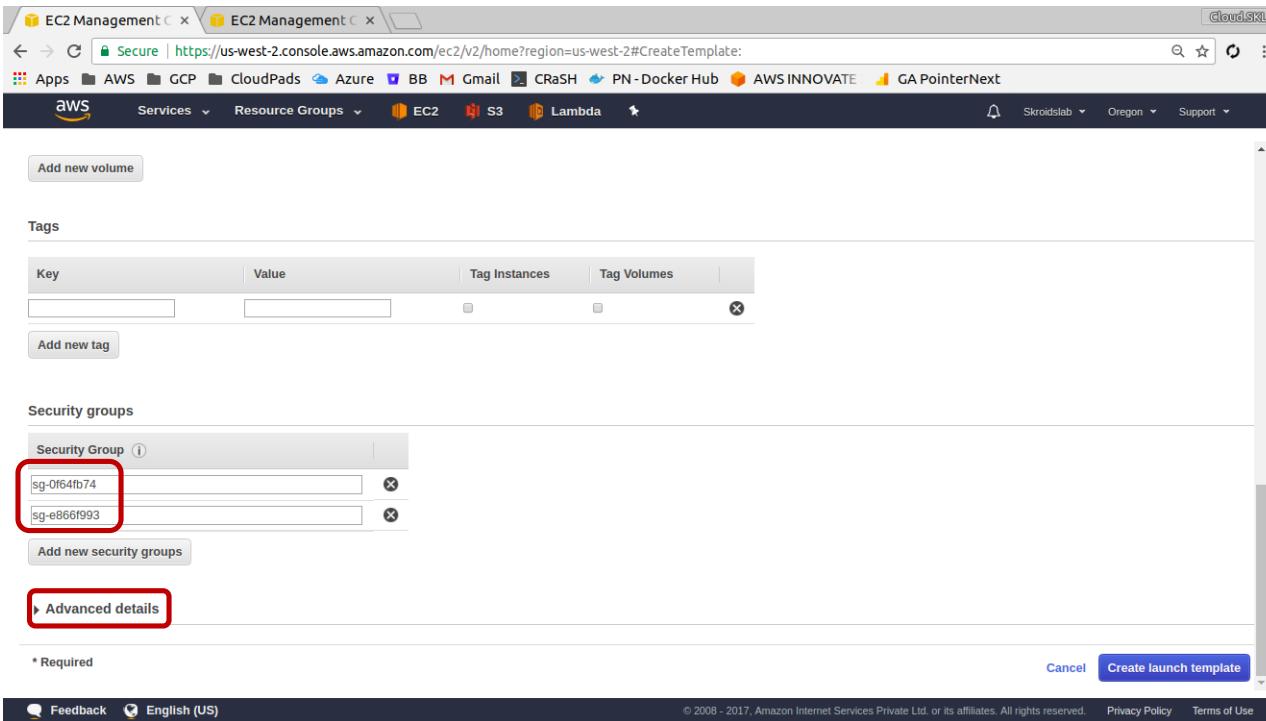
**AMI ID**

**Instance type**

**Key pair name**

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

# Activity - Instance template



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#CreateTemplate>. The top navigation bar includes links for Apps, AWS, GCP, CloudPads, Azure, BB, Gmail, CRaSH, PN-Docker Hub, AWS INNOVATE, GA PointerNext, Services, Resource Groups, EC2, S3, Lambda, and various account and support options.

The main content area is titled "Create template" and shows the "Security groups" step. It lists two selected security groups: "sg-0f64fb74" and "sg-e8661993". A red box highlights these two entries. Below the list is a button labeled "Add new security groups".

At the bottom of the form, there is a "Required" field indicator and a "Create launch template" button. The footer contains links for Feedback, English (US), and legal notices: "© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.", "Privacy Policy", and "Terms of Use".

# Activity - Instance template

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#CreateTemplate>. The 'EC2' service is selected in the navigation bar. The page displays fields for creating an instance template:

- Placement group name: e.g. My Placement Group
- EBS-optimized instance: Don't include in launch template
- Tenancy: Shared - Run a shared hardware instance (highlighted with a red box)
- RAM disk ID: e.g. ari-123456789
- Kernel ID: e.g. aki-123456789
- User data:

```
#!/bin/bash
yum update -y
yum install httpd -y
service httpd start
chkconfig httpd on
```

(highlighted with a red box)

At the bottom, there is a note: \* Required and a blue 'Create launch template' button.

# Activity - Instance template

The screenshot shows the AWS EC2 Management console with two tabs open: 'EC2 Management' and 'EC2 Management'. The URL in the address bar is <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#CreateTemplate>. The navigation bar includes links for Apps, AWS, GCP, CloudPads, Azure, BB, Gmail, CRaSH, PN-Docker Hub, AWS INNOVATE, GA PointerNext, Services (with EC2 selected), S3, Lambda, and other support links.

The main content area displays a 'Create launch template' page. A green success message box contains the text: 'Success: Your launch template (HttpServerTemplate lt-0502a872ab511dcc7 Version 1) has been successfully created!'. Below this, under 'Next steps:', there are three options: 'Launch an instance from this template.', 'Create an Auto Scaling group from your template.', and 'Create Spot Fleet.' Each option has a descriptive paragraph and a blue link below it: 'Launch instance from this template.', 'Create Auto Scaling group', and 'Create Spot Fleet.'

At the bottom of the page, there are links for 'Feedback', 'English (US)', and 'Feedback' again. The footer contains the text: '© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use'.

# Activity - Instance template

Launch 2 more instances using the instance template

The screenshot shows the AWS EC2 Management console interface. The left sidebar contains navigation links for EC2 Dashboard, Instances, Launch Templates, and other services like S3 and Lambda. The main content area displays resource statistics: 1 Running Instances, 0 Dedicated Hosts, 3 Volumes, 2 Key Pairs, 0 Elastic IPs, 1 Snapshots, 1 Load Balancers, and 13 Security Groups. A promotional banner for EC2 Spot instances is visible. Below this, the 'Create Instance' section is shown, featuring a 'Launch Instance' button and a dropdown menu with 'Launch instance from template' highlighted. The 'Service Health' section indicates normal operation for US West (Oregon) and the us-west-2a availability zone. The right sidebar includes sections for Account Attributes (Supported Platforms: vpc-51238934), Additional Information (Getting Started Guide, Documentation, etc.), and AWS Marketplace (listing Barracuda NextGen Firewall F-Series - PAYG).

# Activity - Instance template

Source launch template\* lt-0502a872ab511dcc7

Source template version\* 1 (Default)

Source version description

Filter by attributes

Version	Description
1 (Default)	Contains Amazon AMI linux and Apache http server

Number of instances 1 (Default)

Instance details

Your instance details are listed below. Any fields that are not specified as part of the configuration below will use the template or default values for those fields. Ensure that you have permissions to override these parameters or your instance launch will fail.

AMI ID\* ami-bf4193c7

Instance type t2.micro

Network type VPC

Subnet subnet-fa921f9f

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

After this add the "tag"

# Activity - Instance template

Secure | https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceFromTemplate:

CloudSKL

CloudPads CRASH PN - Docker Hub AWS INNOVATE GA PointerNext

aws Services Resource Groups EC2 S3 Lambda

Skroidlab Oregon Support

Security Group

sg-0f64fb74 sg-e866f993 Add new security groups

Network interfaces

Device	Network interface	Description	Subnet	Auto-assign public IP	Primary IP	Secondary IP	IPv6 IPs	Security group ID	Delete on termination
--------	-------------------	-------------	--------	-----------------------	------------	--------------	----------	-------------------	-----------------------

Currently no network interface details are specified and therefore the instance will launch with the template default network interface settings.

Add network interface Advanced details

\* Required Cancel Launch instance from template

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

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

# Activity - Instance template

- Goto <https://www.base64encode.org/>
  - Click on the "Encode" tab
  - Paste the full user data in the text area
- The encoded string will look like this
  - lyEvYmluL2Jhc2gNCnl1bSB1cGRhdGUgLXkNCnl1bSBpbnN0YWxslGh0dHBkIC15DQpzZXJ2aWNlIGh0dHBkIHN0YXJ0DQpjGtjb25maWcgahR0cGQgb24=

# Fleet of EC2 instances

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

# Compute - Part I

## Load balancing

# Activity - load balancer

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation menu is visible, with the 'Load Balancers' option under the 'LOAD BALANCING' section highlighted. The main content area displays a message stating, "You do not have any load balancers in this region." Below this message, there is a link to the 'FAQ' and 'Getting Started Guide'. A descriptive text block explains that ELB accepts only well-formed TCP connections and will automatically scale to absorb additional traffic without extra charges. At the bottom of the page, there is a 'Select a Load Balancer' section.

You do not have any load balancers in this region.

To learn about Elastic Load Balancing, see our [FAQ](#) and [Getting Started Guide](#).

Click "Create Load Balancer" to create a load balancer that distributes traffic across your instances.

ELB accepts only well-formed TCP connections. This means that many common DDoS attacks, like SYN floods or UDP reflection attacks will not be accepted by ELB and will not be passed to your application. When ELB detects these types of attacks, it will automatically scale to absorb the additional traffic but you will not incur any additional charges.

Select a Load Balancer

Feedback English

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

# Activity - load balancer

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#SelectCreateELBWizard>. The page title is "Select load balancer type". It displays three options: Application Load Balancer, Network Load Balancer, and Classic Load Balancer. The "Application Load Balancer" section is highlighted with a red box around its "Create" button. Below it, a descriptive text explains that it's suitable for web applications with HTTP and HTTPS traffic, mentioning advanced routing and TLS termination. The "Network Load Balancer" section shows a "TCP" icon and a "Create" button. The "Classic Load Balancer" section is labeled "PREVIOUS GENERATION for HTTP, HTTPS, and TCP" and also has a "Create" button. At the bottom, there are links for "Learn more >" and "Cancel".

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

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

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

# Activity - http load balancer

EC2 Management Cloud SKL

Secure | https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#V2CreateELBWizardtype=application

Apps Technical AWS GCP CloudPads Azure BB Gmail CRASH PN - Docker Hub AWS INNOVATE

Services Resource Groups

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 1: Configure Load Balancer

Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected network with a listener that receives HTTP traffic on port 80.

Name: web-lb

Scheme: internet-facing

IP address type: ipv4

Listeners

A listener is a process that checks for connection requests, using the protocol and port that you configured.

Load Balancer Protocol	Load Balancer Port
HTTP	80

Add listener Cancel Next: Configure Security Settings

Feedback English (US) Privacy Policy Terms of Use

# Activity - http load balancer

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#V2CreateELBWizard?type=application>. The page is titled "Step 1: Configure Load Balancer".

The "Availability Zones" section is active, showing a table of subnets:

VPC	Availability Zone	Subnet ID	Subnet IPv4 CIDR	Name
vpc-51238934 (172.31.0.0/16)   default-vpc (default)	us-west-2a	subnet-22b21155	172.31.16.0/20	default-az-a
	us-west-2b	subnet-fa921f9f	172.31.32.0/20	default-az-b
	us-west-2c	subnet-ee30f1b7	172.31.0.0/20	default-az-c

Below the table, there is a "Tags" section and a "Next: Configure Security Settings" button.

# Activity - http load balancer

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#V2CreateELBWizardtype=application>. The top navigation bar includes links for Secure, Apps, Technical, AWS, GCP, CloudPads, Azure, BB, Gmail, CRA\$H, PN - Docker Hub, AWS INNOVATE, Services, Resource Groups, and various account and support options.

The main content area displays the 'Create ELB Wizard' for an application load balancer. The current step is 'Step 2: Configure Security Settings'. A prominent yellow warning box contains the message: '⚠ Improve your load balancer's security. Your load balancer is not using any secure listener. If your traffic to the load balancer needs to be secure, use the HTTPS protocol for your front-end connection. You can go back to the first step to add/configure secure listeners under Basic Configuration section. You can also continue with current settings.'

At the bottom of the page, there are buttons for 'Cancel', 'Previous', and 'Next: Configure Security Groups'. The footer includes links for Feedback, English (US), Privacy Policy, and Terms of Use, along with copyright information: '© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.'

# Activity - http load balancer

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#V2CreateELBWizardType=application>. The navigation bar includes links for Secure, Apps, Technical, AWS, GCP, CloudPads, Azure, BB, Gmail, CRA\$H, PN - Docker Hub, and AWS INNOVATE. The main content area is titled "Step 3: Configure Security Groups". A sub-header states: "A security group is a set of firewall rules that control the traffic to your load balancer. On this page, you can add rules to allow specific traffic to reach your load balancer. First, decide whether to create a new security group or select an existing one." Below this, there are two radio button options: "Create a new security group" and "Select an existing security group", with the latter being selected and highlighted with a red box. A table lists existing security groups with columns for Security Group ID, Name, Description, and Actions. One row, "sg-e866f993", has its checkbox selected and highlighted with a blue box. At the bottom, there are "Cancel", "Previous", and "Next: Configure Routing" buttons.

Security Group ID	Name	Description	Actions
sg-05123160	default	default VPC security group	<a href="#">Copy to new</a>
sg-32750e48	open-8080	Open port 8080 for tomcat to go through	<a href="#">Copy to new</a>
sg-0f64fb74	open-port-22	Open SSH	<a href="#">Copy to new</a>
<input checked="" type="checkbox"/> sg-e866f993	open-port-80	Open HTTP	<a href="#">Copy to new</a>
sg-bdb0f0c7	open-rdp	Open port 3389 for remote desktop for Windows	<a href="#">Copy to new</a>
sg-d47159af	rds-launch-wizard-2	Created from the RDS Management Console	<a href="#">Copy to new</a>

# Activity - http load balancer

Step 4: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. Note that each target group can be associated with only one load balancer.

**Target group**

Target group	New target group
Name	web-lb-tg
Protocol	HTTP
Port	80
Target type	instance

**Health checks**

Protocol	HTTP
Path	/health.html
Advanced health check settings	
Port	<input checked="" type="radio"/> traffic port <input type="radio"/> override
Healthy threshold	2
Unhealthy threshold	2
Timeout	5 seconds
Interval	30 seconds
Success codes	200

**You can specify any private IP address or can select instance (easier). Can route traffic via VPN to on prem instances as well**

**This health check is very important and will be required during "AutoScale Groups" exercise**

# Activity - http load balancer

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#V2CreateELBWizardtype=application>. The page is titled "Step 5: Register Targets".

**Registered targets**

To deregister instances, select one or more registered instances and then click Remove.

Remove	Instance	Name	Port	State	Security groups	Zone
<input type="checkbox"/>	i-0a7d5ab10c30ec512	http-server-1	80	running	open-port-80	us-west-2a
<input type="checkbox"/>	i-027a305ddf97b6470	http-server-2	80	running	open-ssh, open-port-80	us-west-2b

**Instances**

To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

**Add to registered** on port 80

**Search Instance**

Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
i-0a7d5ab10c30ec512	http-server-1	running	open-port-80	us-west-2a	subnet-22b21155	172.31.16.0/20
i-027a305ddf97b6470	http-server-2	running	open-ssh, open-port-80	us-west-2b	subnet-fa921f9f	172.31.32.0/20

**Buttons:** Cancel, Previous, Next: Review

# Activity - http load balancer

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#V2CreateELBWizardtype=application>. The top navigation bar includes links for Apps, Technical, AWS, GCP, CloudPads, Azure, BB, Gmail, CRaSH, PN - Docker Hub, and AWS INNOVATE. The main content area is titled "Step 6: Review" with the sub-instruction "Please review the load balancer details before continuing". The configuration details are as follows:

- Load balancer**: Name: web-lb, Scheme: internet-facing, Listeners: Port:80 - Protocol:HTTP (warning icon), IP address type: ipv4, VPC: vpc-51238934 (default-vpc), Subnets: subnet-22b21155 (default-az-a), subnet-fa921f9f (default-az-b), subnet-ee30f1b7 (default-az-c), Tags: None.
- Security settings**: Certificate name: None, Security policy name: None.
- Security groups**: Security groups: sg-e866ff993.
- Routing**: Target group: New target group, Target group name: web-lb-tg, Port: 80, Target type: instance, Protocol: HTTP, Health check protocol: HTTP, Path: /health.html, Health check port: traffic port, Unhealthy threshold: 2.

At the bottom right, there are "Cancel", "Previous", and "Create" buttons, with "Create" being highlighted by a red box.

# Activity - http load balancer

The screenshot shows a browser window for the AWS EC2 Management console at the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#V2CreateELBWizard?type=application>. The page title is "Load Balancer Creation Status". A green success message box contains the text: "Successfully created load balancer Load balancer web-lb was successfully created. Note: It might take a few minutes for your load balancer to be fully set up and ready to route traffic, and for the targets to complete the registration process and pass the initial health checks." A "Close" button is visible in the bottom right corner of the message box. At the bottom of the page, there are links for Feedback, English (US), Privacy Policy, and Terms of Use.

# Activity - http load balancer

The screenshot shows the AWS EC2 Management console with the URL <https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2#LoadBalancers>. The left sidebar navigation includes AMIs, Bundle Tasks, ELASTIC BLOCK STORE (Volumes, Snapshots), NETWORK & SECURITY (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), LOAD BALANCING (Load Balancers, Target Groups), AUTO SCALING (Launch Configurations, Auto Scaling Groups), and SYSTEMS MANAGER SERVICES (Run Command). The 'Load Balancers' section is currently selected. The main content area displays a table of existing load balancers:

Name	DNS name	State	VPC ID	Availability Zones	Type
awseb-e-v-AWSEBLba-8E2...	awseb-e-v-AWSEBLba-8E2...	active	vpc-03f9c064	us-west-2a, us-west-2b...	classic
web-lb	web-lb-1312964949.us-west...	active	vpc-51238934	us-west-2a, us-west-2c...	application

Below the table, the details for the 'web-lb' load balancer are shown under the 'Basic Configuration' section:

Name:	web-lb	Creation time:	September 10, 2017 at 11:32:45 AM UTC+5:30
ARN:	arn:aws:elasticloadbalancing:us-west-2:278931287317:loadbalancer/app/web-lb/b072fdcc7c095379	Hosted zone:	Z1H1FL5HABSF5
DNS name:	web-lb-1312964949.us-west-2.elb.amazonaws.com (A Record)	State:	active
Scheme:	internet-facing	VPC:	vpc-51238934
Type:	application	IP address type:	ipv4
AWS WAF Web ACL:			

# Activity - http load balancer

The screenshot shows the AWS EC2 Management console with the URL <https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2#TargetGroups>. The left sidebar navigation includes sections for NETWORK & SECURITY (Security Groups, Placement Groups, Key Pairs, Network Interfaces), LOAD BALANCING (Load Balancers, Target Groups), AUTO SCALING (Launch Configurations, Auto Scaling Groups), SYSTEMS MANAGER SERVICES (Run Command, State Manager, Configuration Compliance, Automations, Patch Compliance, Patch Baselines), and SYSTEMS MANAGER (SHADED DOCUMENTS). The 'Target Groups' tab is selected and highlighted with a red box. The main content area displays a table for the target group 'web-lb-tg' with one entry: Name: web-lb-tg, Port: 80, Protocol: HTTP, Target type: instance, VPC ID: vpc-51238934. Below the table, a message states: 'The load balancer starts routing requests to a newly registered target as soon as the registration process completes and the target passes the initial health checks. If demand on your targets increases, you can register additional targets. If demand on your targets decreases, you can deregister targets.' A blue 'Edit' button is present. A yellow box highlights the 'Targets' tab. The 'Registered targets' section shows two entries: Instance ID i-0a7d5ab10c30ec512, Name http-server-1, Port 80, Availability Zone us-west-2a, Status unhealthy (with a red box); and Instance ID i-027a305ddff97b6470, Name http-server-2, Port 80, Availability Zone us-west-2b, Status unhealthy (with a red box). The bottom of the page includes links for Feedback, English (US), and footer text: © 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use.

**Port from the http LB is automatically mapped**

# Activity - http load balancer

The screenshot shows the AWS EC2 Management console with the URL <https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2#TargetGroups>. The left sidebar is collapsed, and the main content area displays the 'Target Groups' page for a target group named 'web-lb-tg'. The target group is configured for port 80, protocol HTTP, and target type instance, associated with VPC ID vpc-51238934.

**Target group: web-lb-tg**

**Registered targets**

Instance ID	Name	Port	Availability Zone	Status
i-06596d9beec271915	http-server-1	80	us-west-2a	healthy ⓘ
i-0669978a9c0b15f3	http-server-2	80	us-west-2b	healthy ⓘ

**Availability Zones**

Availability Zone	Target count	Healthy?
us-west-2b	1	Yes

Feedback English (US)

# Activity - load balancer

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

# Activity - load balancer

The screenshot shows the AWS EC2 Management console with the URL <https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2#TargetGroups>. The left sidebar navigation includes Services, Resource Groups, ELASTIC BLOCK STORE, SECURITY GROUPS, LOAD BALANCING, AUTO SCALING, and SYSTEMS MANAGER SERVICES. Under LOAD BALANCING, 'Target Groups' is selected. A target group named 'web-lb-tg' is listed in the main pane. A modal window titled 'Edit attributes' is open over the target group details. The modal contains fields for 'Deregistration delay' (300 seconds), 'Stickiness' (checkboxes for 'Disable stickiness' and 'Enable load balancer generated cookie stickiness' (which is checked)), and 'Stickiness duration' (1 day). At the bottom of the modal, there are 'Cancel' and 'Save' buttons.

# Reference - classic load balancer

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#CreateELBWizard>. The page is titled "Step 1: Define Load Balancer".

**Basic Configuration**

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you might create. You will also need to configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your load balancer with a standard web server on port 80.

Load Balancer name: **Web-LB1**  
Create LB Inside: **My Default VPC (172.31.0.0/16)**  
Create an internal load balancer:  (What's this?)  
Enable advanced VPC configuration:   
Listener Configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port
HTTP	80	HTTP	80

Add

**Select Subnets**

You will need to select a Subnet for each Availability Zone where you wish traffic to be routed by your load balancer. If you have instances in only one Availability Zone, please select at least two Subnets in different Availability Zones to provide higher availability for your load balancer.

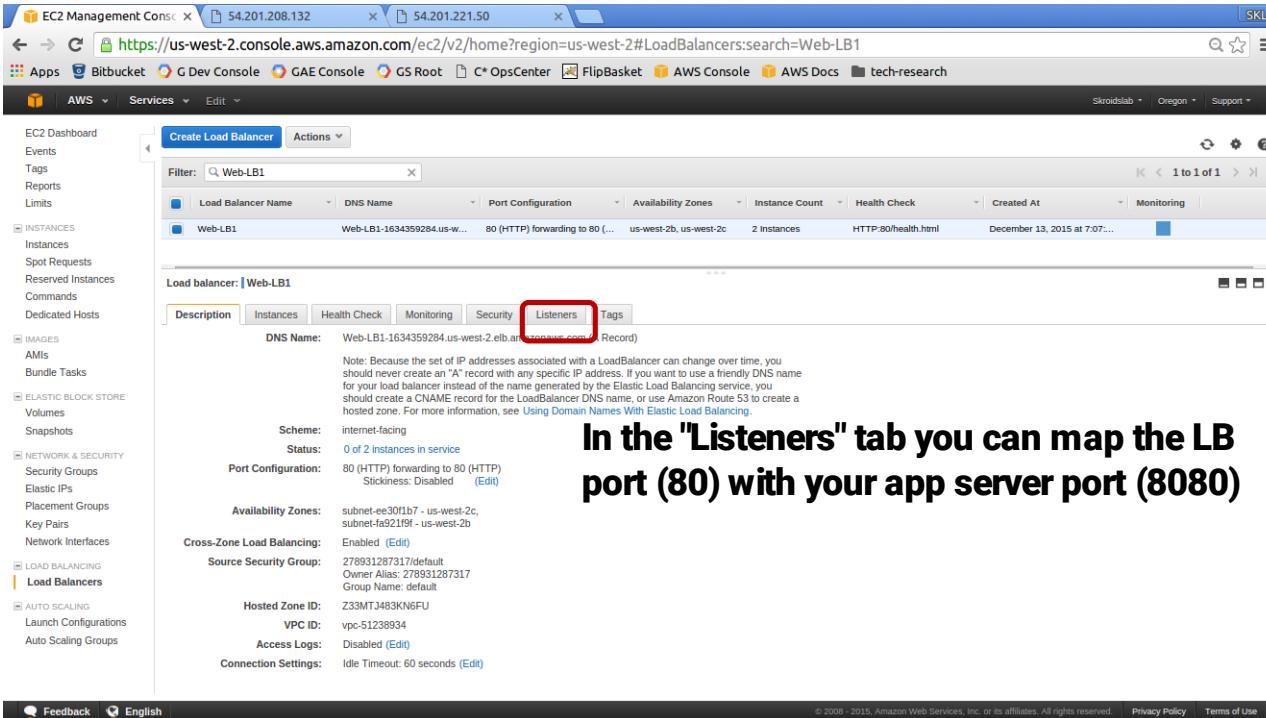
VPC: **vpc-51238934 (172.31.0.0/16)**

Available Subnets				
Actions	Availability Zone	Subnet ID	Subnet CIDR	Name
	us-west-2a	subnet-22b21155	172.31.16.0/20	

Selected Subnets				
Actions	Availability Zone	Subnet ID	Subnet CIDR	Name
	us-west-2b	subnet-fa92119f	172.31.32.0/20	
	us-west-2c	subnet-ee30f1b7	172.31.0.0/20	

Cancel | Next: Assign Security Groups

# Reference - classic load balancer



The screenshot shows the AWS EC2 Management Console with the Load Balancers page open. On the left sidebar, under the LOAD BALANCING section, the 'Load Balancers' option is selected. In the main content area, a table lists a single load balancer named 'Web-LB1'. Below the table, the configuration for 'Web-LB1' is shown. The 'Listeners' tab is highlighted with a red box. The configuration details include:

- DNS Name:** Web-LB1-1634359284.us-west-2.elb.amazonaws.com
- Scheme:** internet-facing
- Status:** 0 of 2 instances in service
- Port Configuration:** 80 (HTTP) forwarding to 80 (HTTP)  
Stickiness: Disabled ([Edit](#))
- Availability Zones:** subnet-ea30fb7 - us-west-2c, subnet-fa921f9 - us-west-2b
- Cross-Zone Load Balancing:** Enabled
- Source Security Group:** 278931287317/default  
Owner Alias: 278931287317  
Group Name: default
- Hosted Zone ID:** Z33MTJ483KNG6FU
- VPC ID:** vpc-51238934
- Access Logs:** Disabled ([Edit](#))
- Connection Settings:** Idle Timeout: 60 seconds ([Edit](#))

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



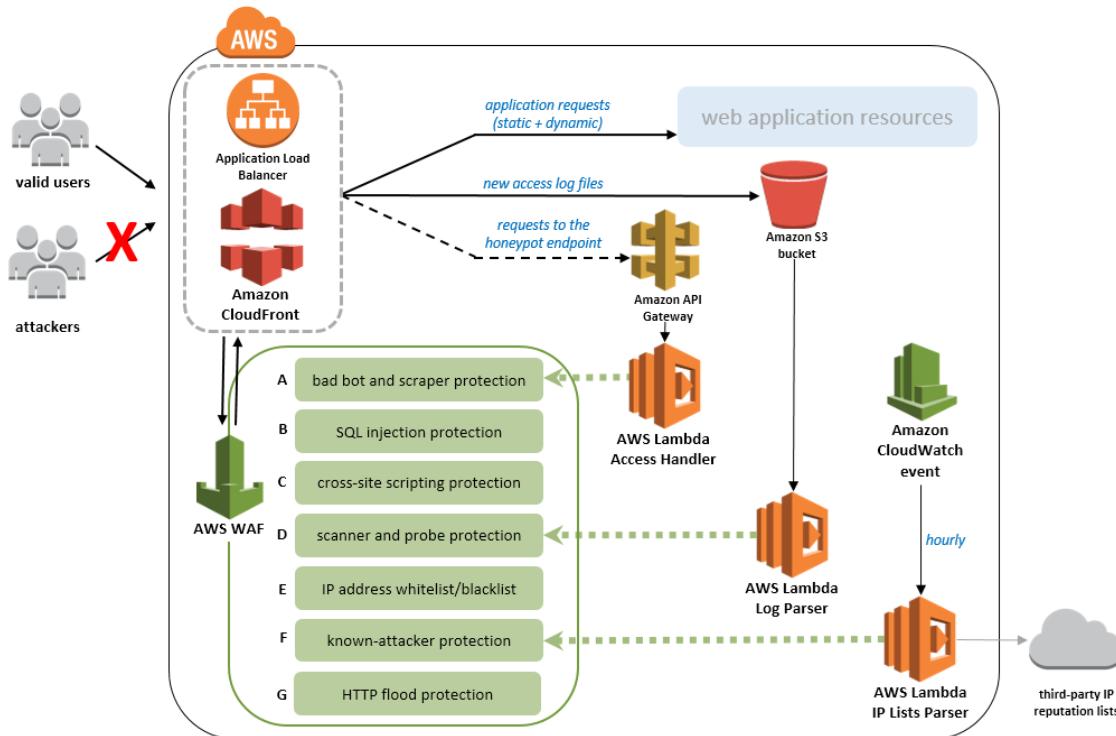
# Compute - Part I

**Web Application Firewall (WAF)**  
**Shield - discussion**

# WAF exercise prerequisites

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

# LB and WAF & other components



**WAF can sit in front of LB or CDN**

The screenshot shows the AWS WAF & Shield console homepage. At the top, there's a navigation bar with tabs for EC2 Management, AWS WAF & Shield, and CloudSKL. The URL in the address bar is <https://console.aws.amazon.com/waf/home?region=us-west-2#/intro>. Below the address bar is a search bar and a navigation menu with links for Apps, AWS, GCP, CloudPads, GL, Azure, BB, Gmail, CRaSH, PN-Docker Hub, AWS INNOVATE, GA PointerNext, Services, Resource Groups, and Support.

The main content area features a large green downward arrow icon and the text "AWS WAF and AWS Shield". Below this, it says "AWS WAF and AWS Shield help protect your AWS resources from web exploits and DDoS attacks".

Three service cards are displayed below:

- AWS WAF**: Represented by a cloud icon with a brick wall. Description: "AWS WAF is a web application firewall service that helps protect your web apps from common exploits that could affect app availability, compromise security, or consume excessive resources." Call-to-action button: [Go to AWS WAF](#)
- AWS Shield**: Represented by a shield icon. Description: "AWS Shield provides expanded DDoS attack protection for your AWS resources. Get 24/7 support from our DDoS response team and detailed visibility into DDoS events." Call-to-action button: [Go to AWS Shield](#)
- AWS Firewall Manager**: Represented by a circular icon with a brick wall and arrows. Description: "AWS Firewall Manager simplifies your AWS WAF administration and maintenance tasks across multiple accounts and resources." Call-to-action button: [Go to AWS Firewall Manager](#)

Screenshot of the AWS WAF & Shield console home page.

The browser title bar shows "EC2 Management" and "AWS WAF & Shield". The address bar shows "Secure | https://console.aws.amazon.com/waf/home#/wafhome". The AWS navigation bar includes links for Apps, AWS, GCP, CloudPads, GL, Azure, BB, Gmail, CRaSH, PN - Docker Hub, AWS INNOVATE, GA PointerNext, and CloudSKL. The user menu shows "Skroidslab", "Global", and "Support".

The left sidebar menu includes:

- AWS WAF
  - Web ACLs
  - Rules
  - Marketplace
- Conditions
- Cross-site scripting
- Geo match
- IP addresses
- Size constraints
- SQL injection
- String and regex matching

---

- AWS Shield
  - Summary
  - Protected resources
- Incidents
- Global threat environment

The main content area displays the "AWS WAF" page with a "Configure web ACL" button. It features three icons illustrating key features:

- Web traffic filtering with custom rules**: Shows a flowchart with arrows passing through a filter icon.
- Block malicious requests**: Shows a monitor icon with a shield icon.
- Tune your rules and monitor traffic**: Shows a monitor icon with a graph icon.

Below each feature is a brief description:

- Web traffic filtering with custom rules: Create custom rules that can allow, block, or count web requests based on originating IP addresses or strings that appear in web requests.
- Block malicious requests: Configure AWS WAF to recognize and block common web application security risks like SQL injection (SQLi) and cross-site scripting (XSS).
- Tune your rules and monitor traffic: Review details about the web requests that AWS WAF allows, blocks, or counts, and update rules to thwart new attacks.

At the bottom, there are links for Feedback, English (US), Copyright notice (© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.), Privacy Policy, and Terms of Use.

The screenshot shows the AWS WAF & Shield wizard interface. The title bar says "Set up a web access control list (web ACL)". On the left, there's a sidebar with steps: Step 1: Name web ACL, Step 2: Create conditions, Step 3: Create rules, Step 4: Review and create. The main content area has three columns: "Concepts overview" (with sections for Conditions, Rules contain conditions, and Web ACLs contain rules), "IP match condition example" (listing IP ranges like 192.0.2.0/24, 192.51.100.0/24, 2001:db8:a0b:12f0:ac34:1:1:1/128, and 2001:db8:a0b:12f0:0:0:0/64), and "String match condition example" (listing "Bad bots").

Scroll down and click "Next"

# WAF - ACL

The screenshot shows the AWS WAF & Shield wizard interface for creating a new web ACL. The page title is "Set up a web access control list (web ACL)". On the left, there's a sidebar with navigation links: Concepts overview, Step 1: Name web ACL (which is highlighted in orange), Step 2: Create conditions, Step 3: Create rules, and Step 4: Review and create.

The main form is titled "Name web ACL". It contains the following fields:

- Web ACL name\***: A text input field containing "webapp-acl", which is highlighted with a red box.
- CloudWatch metric name\***: A text input field containing "webappacl".
- Region\***: A dropdown menu showing "US West (Oregon)", which is highlighted with a red box.
- AWS resource to associate**: A dropdown menu showing "web-lb".

Below the form, there's a note: "Use global to create WAF resources that you would associate with CloudFront distributions and other regions for WAF resources that you would associate with ALBs in that region." At the bottom right of the form, there are "Cancel", "Previous", and "Next" buttons. The "Next" button is highlighted with a red box.

# WAF - Conditions

The screenshot shows the AWS WAF & Shield console with the URL <https://console.aws.amazon.com/waf/home#/wizard/>. The left sidebar shows navigation steps: Concepts overview, Step 1: Name web ACL, Step 2: Create conditions (which is selected), Step 3: Create rules, and Step 4: Review and create. The main content area is titled "Create conditions". It contains two sections: "Cross-site scripting match conditions" and "Geo match conditions". Each section has a "Name" input field and a "Create condition" button. The "Create condition" button in the "Cross-site scripting match conditions" section is highlighted with a red box and an orange arrow pointing to it from the text below. The "Create condition" button in the "Geo match conditions" section is also highlighted with a red box and an orange arrow pointing to it from the text below. To the right, there is a "Concepts overview" sidebar with examples of Web ACL rules.

Set up a web access control list (web ACL)

Concepts overview

Step 1: Name web ACL

**Step 2: Create conditions**

Step 3: Create rules

Step 4: Review and create

Create conditions

Conditions specify the filters that you want to use to allow or block requests that are forwarded to AWS resources such as Amazon CloudFront distributions.

Cross-site scripting match conditions

Name	Create condition
You don't have any cross-site scripting match conditions. Choose <a href="#">Create XSS match condition</a> to get started.	

A cross-site scripting match condition specifies the parts of a web request (such as a User-Agent header) that you want AWS WAF to inspect for cross-site scripting threats. [Learn more](#)

Geo match conditions

Name	Create condition
You don't have any geo match conditions. Choose <a href="#">Create condition</a> to get started.	

A geo match condition lets you allow, block, or count web requests based on the geographic origin of the request. [Learn more](#)

Concepts overview

**Web ACL example**  
if requests match

- Rule 1, Bad User-Agents, then block
  - IP match condition  
Suspicious IPs
  - and
  - String match condition  
Bad bots

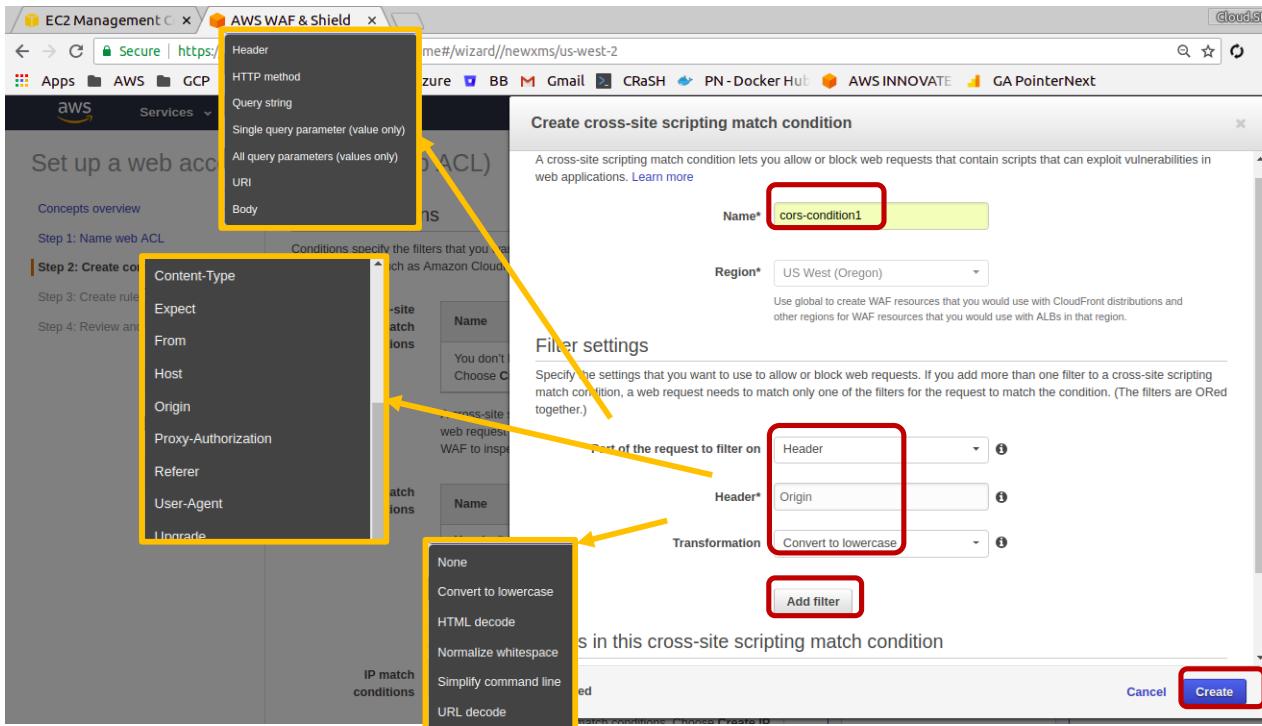
or if requests match

- Rule 2, Detect SQLi, then block
  - SQL injection match condition  
SQLi checks

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

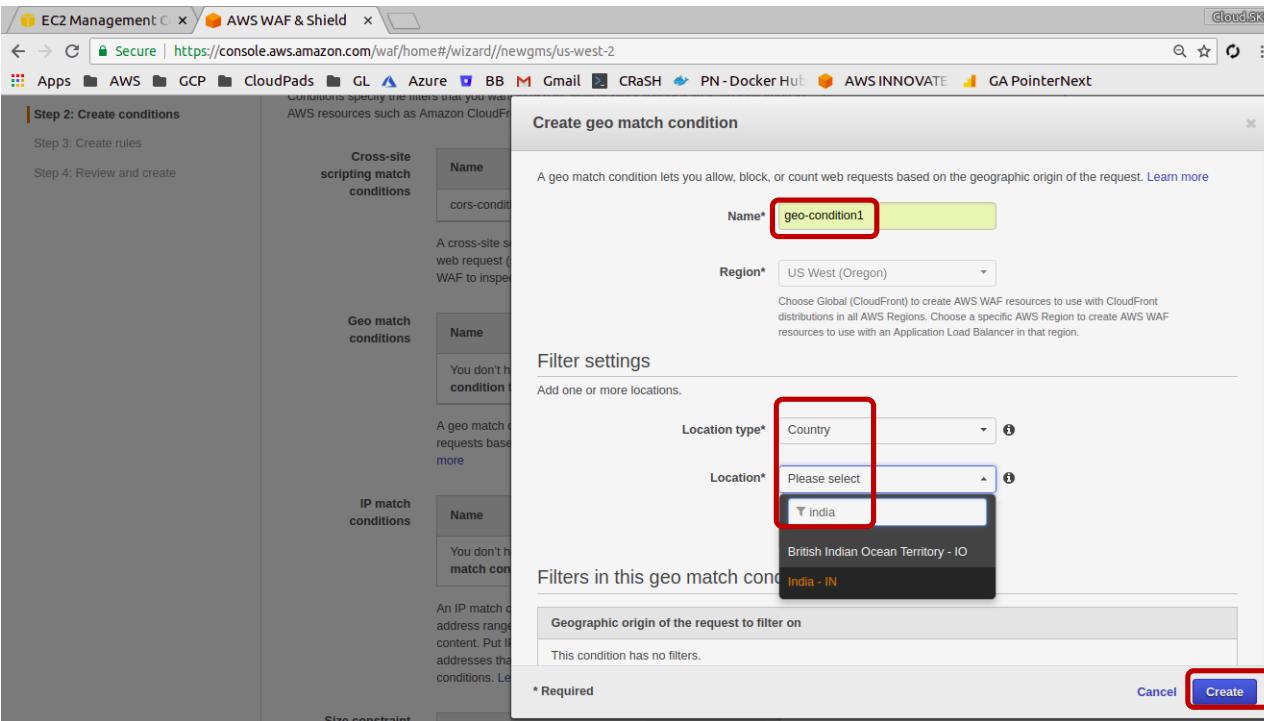
# WAF - CORS condition

greatlearning



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

# WAF - Geo/country condition



# WAF - IP match condition

Create IP match condition

An IP match condition contains a list of IP addresses and/or IP address ranges. These IPs are the source of the requests that you want to allow or block. [Learn more](#)

Name\* ipmatch-condition1

Region\* US West (Oregon)

Use global to create WAF resources that you would use with CloudFront distributions and other regions for WAF resources that you would use with ALBs in that region.

IP addresses

Add one or more IP addresses or IP address ranges by using CIDR notation.

IP Version\*  IPv4  IPv6

Address\* 122.179.50.121/32

AWS WAF supports /8 or any range from /16 to /32 CIDR blocks for IPv4 Examples:  
For a single IP address, please specify like 192.0.2.44/32  
For an IP range from 192.0.2.0 to 192.0.2.255, please use 192.0.2.0/24

Add IP address or range

\* Required

Cancel Create

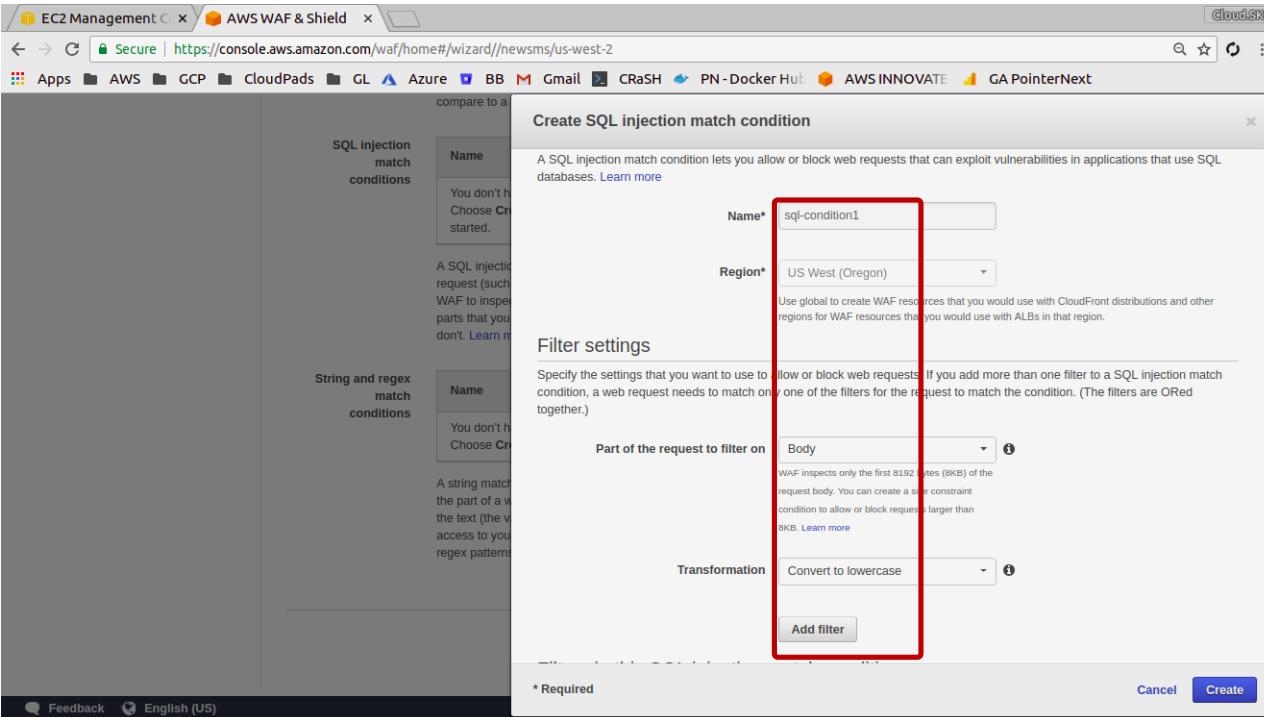
Use the IP of your own laptop

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

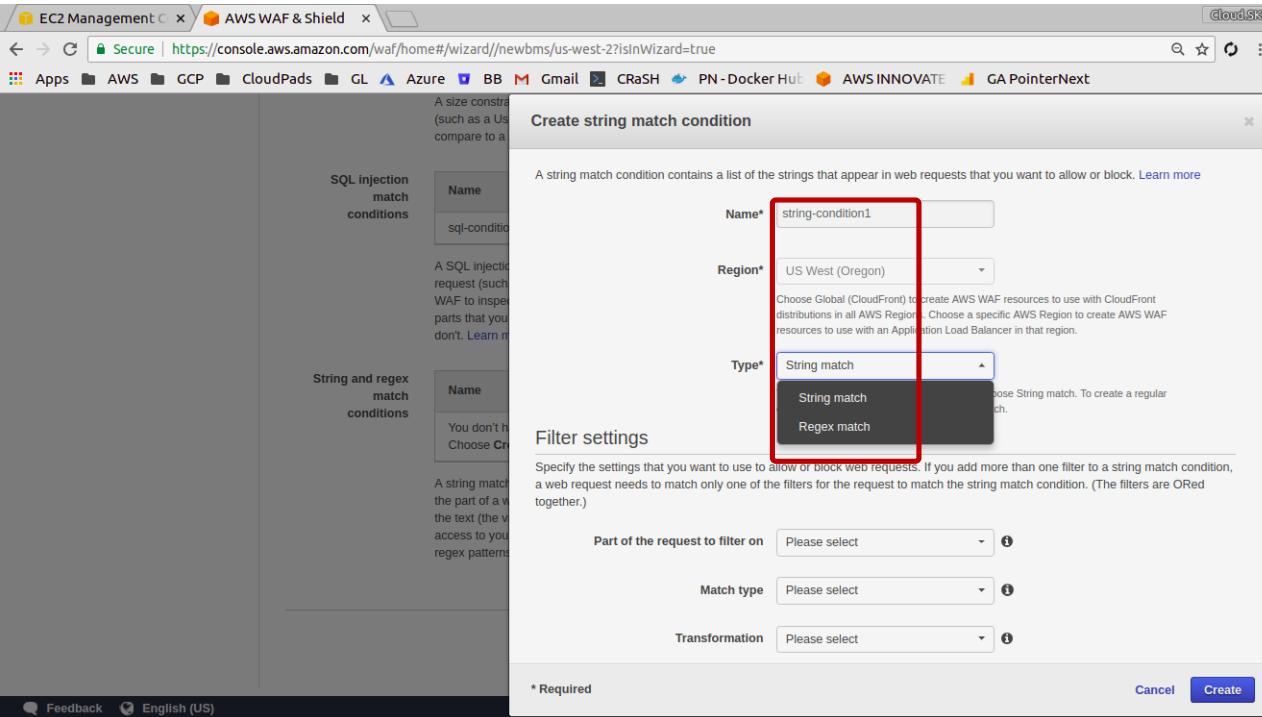
# WAF - Size check condition

The screenshot shows the AWS WAF & Shield console with the URL <https://console.aws.amazon.com/waf/home#/wizard//newscc/us-west-2>. The left sidebar lists several match conditions: Size constraint conditions, SQL injection match conditions, and String and regex match conditions. The main area is titled "Create size constraint condition".  
**Name:** size-condition1  
**Region:** US West (Oregon)  
**Filter settings:**  
Specify the settings that you want to use to allow or block web requests. If you add more than one filter to a size constraint condition, a web request needs to match only one of the filters for the request to match the condition. (The filters are ORed together.)  
**Part of the request to filter on:** All query parameters (values only)  
**Comparison operator:** Greater than  
**Size (Bytes):** 1024  
**Transformation:** None  
**Add filter**  
**\* Required** **Create**

# WAF - SQL injection condition



# WAF - String match condition



# WAF - String match condition

The screenshot shows the 'Create string match condition' dialog box in the AWS WAF & Shield console. The dialog is titled 'Create string match condition' and contains several configuration fields:

- Filter settings**: A descriptive text block explaining that the filters are ORed together.
- Part of the request to filter on**: Set to 'Body'. A note states: "WAF inspects only the first 8192 bytes (8KB) of the request body. You can create a size constraint condition to allow or block requests larger than 8KB. Learn more".
- Match type**: Set to 'Contains word'.
- Transformation**: Set to 'Convert to lowercase'.
- Value is base64-encoded**: An unchecked checkbox.
- Value to match\***: The input field contains the value 'fraud string'.

A red box highlights the 'Value to match\*' field and its associated tooltip. The tooltip specifies: "Type the value that you want to search for in the specified part of web requests. If you specify a base64-encoded value, the unencoded value can't exceed 50 characters." To the right of the dialog, two annotations are present:

- First 8k only**: Points to the note about byte limit.
- Max 50 chars**: Points to the tooltip for the 'Value to match\*' field.

# WAF - condition summary

The screenshot shows the AWS WAF & Shield console with the URL <https://console.aws.amazon.com/waf/home#/wizard/>. The page title is "Set up a web access control list (web ACL)". On the left, there is a sidebar with navigation links: Concepts overview, Step 1: Name web ACL, Step 2: Create conditions (which is selected and highlighted in orange), Step 3: Create rules, and Step 4: Review and create.

The main content area is titled "Create conditions". It contains three sections:

- Cross-site scripting match conditions:** A table with one row. The "Name" column contains "cors-condition1", which is highlighted with a red box. The "Create condition" button is to the right.
- Geo match conditions:** A table with one row. The "Name" column contains "geo-condition1", which is highlighted with a red box. The "Create condition" button is to the right.
- IP match conditions:** A table with one row. The "Name" column contains "ipmatch-condition1", which is highlighted with a red box. The "Create condition" button is to the right.

To the right of the main content area, there is a "Concepts overview" sidebar with examples of how conditions can be used in a Web ACL:

- Web ACL example if requests match:**
  - Rule 1, Bad User-Agents, then block
    - IP match condition: Suspicious IPs
    - and
    - String match condition: Bad bots
- or if requests match:**
  - Rule 2, Detect SQLi, then block
    - SQL injection match condition: SQLi checks
  - otherwise, perform the default action
  - Default action

**and other conditions. Scroll down and click "Next"**

# WAF - Rules

The screenshot shows the AWS WAF & Shield console with the URL <https://console.aws.amazon.com/waf/home#/wizard>. The page title is "Set up a web access control list (web ACL)". On the left, a sidebar lists steps: "Concepts overview", "Step 1: Name web ACL", "Step 2: Create conditions", "Step 3: Create rules" (which is highlighted with an orange border), and "Step 4: Review and create". The main content area is titled "Create rules" and contains the following sections:

- Rules:** A dropdown menu set to "Select a rule" and a button labeled "Add rule to web ACL". To the right of the "Add rule to web ACL" button is a red rectangular box highlighting the "Create rule" button.
- If a request matches all of the conditions in a rule, take the corresponding action:** A table with columns "Order", "Rule", and "Action". It includes a note: "Create new rule using IP match or string match conditions created in previous step."
- If a request doesn't match any rules, take the default action:** A section with two radio button options:
  - Allow all requests that don't match any rules
  - Block all requests that don't match any rules

At the bottom of the main form are buttons: "\* Required", "Cancel", "Previous", "Review and create".

To the right of the main form is a "Concepts overview" sidebar with examples of Web ACL rules:

- Web ACL example if requests match:**
  - Rule 1, Bad User-Agents, then block:**
    - IP match condition: Suspicious IPs
    - and
    - String match condition: Bad bots
- or if requests match:**
  - Rule 2, Detect SQLi, then block:**
    - SQL injection match condition: SQLi checks
- otherwise, perform the default action:**
  - Default action:**

**Rules will use the conditions defined earlier**

# WAF - Rules

The screenshot shows the AWS WAF & Shield 'Create rule' wizard. On the left, a sidebar displays the progress: 'String match condition created successfully.', 'Set up a web access control list (web ACL)', 'Step 1: Name web ACL', 'Step 2: Create conditions', 'Step 3: Create rules' (highlighted in orange), and 'Step 4: Review and create'. The main panel is titled 'Create rule' and contains the following fields:

- Name\*: webrule1
- CloudWatch metric name\*: webrule1
- Rule type\*: **Regular rule** (highlighted with a red box)
- Region\*

Below these fields is a section titled 'Add conditions' with a sub-section 'When a request' containing a dropdown set to 'does' and a filter condition 'match at least one of the filters in the cross-site scripting match condition'. A note states: 'With CloudFront distributions and other regions for WAF resources that would use ALBs in that region.' At the bottom of the 'Add conditions' section is a 'Create' button.

# WAF - Rules

The screenshot shows the AWS WAF & Shield 'Create rule' wizard. The main panel displays the 'Create rule' configuration with fields for Name (webrule1), CloudWatch metric name (webrule1), Rule type (Regular rule), and Region (US West (Oregon)). Below these, a section titled 'Add conditions' is expanded, showing a dropdown menu with options: 'When a request does' (highlighted with a red box) and 'originate from an IP address in' (also highlighted with a red box). Other visible condition types include 'match at least one of the filters in the cross-site scripting match condition', 'match at least one of the filters in the size constraint condition', and 'match at least one of the filters in the SQL injection match condition'. At the bottom of the 'Add conditions' panel, there are 'Cancel' and 'Create' buttons.

# WAF - Rules

The screenshot shows the AWS WAF & Shield console with the URL <https://console.aws.amazon.com/waf/home#/wizard//newrule/us-west-2>. The browser tab is titled "AWS WAF & Shield". The main page displays a success message: "String match condition created successfully." Below it, the heading "Set up a web access control list (web ACL)" is followed by a navigation menu with the following steps:

- Step 1: Name web ACL
- Step 2: Create conditions
- Step 3: Create rules** (highlighted in orange)
- Step 4: Review and create

The "Create rules" section contains the following fields:

- Name\*: webrule1
- CloudWatch metric name\*: webrule1
- Rule type\*: Regular rule
- Region\*: US West (Oregon)

Below these fields is a note: "Use global to create WAF resources that you would use with CloudFront distributions and other regions for WAF resources that you would use with ALBs in that region."

The "Add conditions" section is expanded, showing a modal dialog. Inside the dialog, under "When a request", there is a dropdown menu with the option "originate from an IP address in" selected. A red box highlights the dropdown value "ipmatch-condition1". Below this, the "IP Addresses in ipmatch-condition1" field contains the value "122.179.50.121/32". There is also an "Add condition" button.

# WAF - Rules

The screenshot shows the AWS WAF & Shield console with the URL <https://console.aws.amazon.com/waf/home#/wizard//newrule/us-west-2>. The page is titled "Create rule". The "Region\*" dropdown is set to "US West (Oregon)". The "Add conditions" section contains two conditions:

- "When a request originates from an IP address in ipmatch-condition1"
- "When a request matches at least one of the filters in the cross-site scripting match condition" (highlighted with a red box)

At the bottom right of the "Add conditions" section, there is a "Create" button highlighted with a red box.

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

# WAF - Rules summary

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

String match condition created successfully.

Set up a web access control list (web ACL)

Concepts overview

Step 1: Name web ACL

Step 2: Create conditions

**Step 3: Create rules**

Step 4: Review and create

Create rules

Rules contain the conditions that you want to use to filter web requests. You add rules to a web ACL, and then specify whether you want to allow or block requests based on each rule. [Learn more](#)

Add rules to a web ACL

Rules Select a rule Add another rule Create rule

Rule created successfully.

If a request matches all of the conditions in a rule, take the corresponding action

Order	Rule	Action
1	webrule1	<input checked="" type="radio"/> Allow <input type="radio"/> Block <input type="radio"/> Count

If a request doesn't match any rules, take the default action

Default action\*  Allow all requests that don't match any rules  Block all requests that don't match any rules

Concepts overview

Web ACL example  
if requests match

Rule 1, Bad User-Agents, then block

IP match condition  
Suspicious IPs

and

String match condition  
Bad bots

or if requests match

Rule 2, Detect SQLi, then block

SQL injection match condition  
SQLi checks

otherwise, perform the default action

Default action

Allow requests that don't match any

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

# WAF - ACL creation final step

The screenshot shows the 'Review and create' step of the AWS WAF & Shield wizard. The left sidebar lists steps: Concepts overview, Step 1: Name web ACL, Step 2: Create conditions, Step 3: Create rules, and Step 4: Review and create (which is selected). The main area displays the configuration for a 'webapp-acl'. It includes fields for 'Web ACL name' (webapp-acl) and 'CloudWatch metric name' (webappacl). Below this is a 'Rules and actions' section with a table:

Order	Rule	Action
1	webrule1	Allow

There is also a section for 'Default action Block' which is currently empty. The next section is 'AWS resources using this web ACL' with a table:

Resource	Type
web-lb	Application load balancer

At the bottom right, there are 'Cancel', 'Previous', and 'Confirm and create' buttons. The 'Confirm and create' button is highlighted with a red box.

# WAF - ACL summary

The screenshot shows the AWS WAF & Shield console with the 'Web ACLs' section selected. A 'Create web ACL' button is visible. The 'Name' field contains 'webapp-acl'. The 'Edit web ACL' button is highlighted with a red box. The 'Rules' tab is selected, showing one rule named 'weerule1' with an 'Allow requests' action. The 'Default action' is set to 'Block all requests that don't match any rules'. Below this, the 'AWS resources using this web ACL' section lists an 'Application load balancer' named 'web-lb'.

Order	Rule	Type	Action
1	weerule1	Regular	Allow requests

Resource	Type
web-lb	Application load balancer

Edit web ACL webapp-acl

Rules weerule Add rule to web ACL

If a request matches all of the conditions in a rule, take the corresponding action

Order	Rule	Type	Action
1	weerule1	Regular	<input checked="" type="radio"/> Allow <input type="radio"/> Block <input type="radio"/> Count <input type="checkbox"/>
2	weerule1	Regular	<input type="radio"/> Allow <input type="radio"/> Block <input checked="" type="radio"/> Count <input type="checkbox"/>

If a request doesn't match any rules, take the default action

Default action  Allow all requests that don't match any rules  Block all requests that don't match any rules

Cancel Update

The screenshot shows the AWS WAF & Shield console. On the left, a sidebar menu includes options like Rules, Marketplace, Conditions, Cross-site scripting, Geo match, IP addresses, Size constraints, SQL injection, String and regex matching, AWS Shield (Summary, Protected resources, Incidents, Global threat environment), and AWS FMS. The main area displays a success message: "Web ACL updated successfully." Below this, the "Web ACLs" section shows a table with one entry: "Name: webapp-acl". The "Rules" tab is selected, showing a table with two rules:

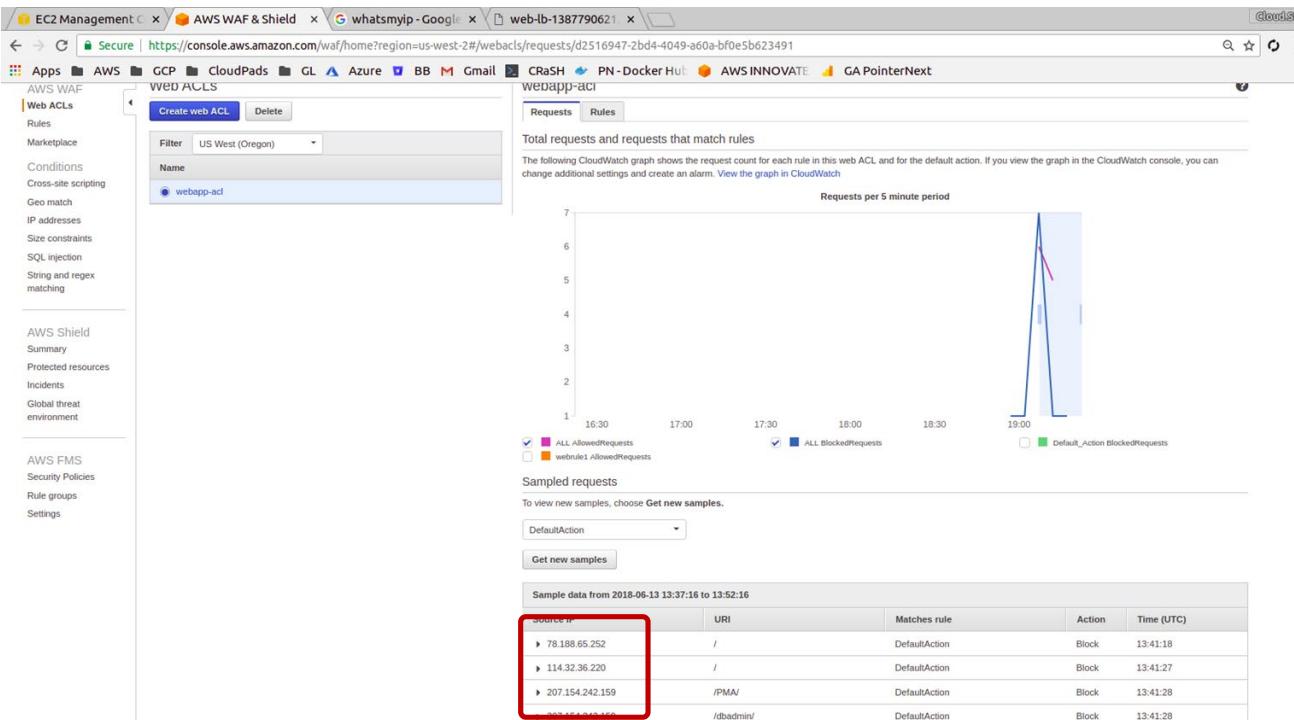
Order	Rule	Type	Action
1	webrule1	Regular	Allow requests
2	webrule1	Regular	Block requests

Below the rules, there's a section for default actions: "Default action: Block all requests that don't match any rules". At the bottom, it shows "AWS resources using this web ACL" with one entry: "Resource: web-lb, Type: Application load balancer".

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

# WAF - Testing

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



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

The screenshot shows a browser window with the AWS WAF & Shield interface. The URL is <https://console.aws.amazon.com/waf/home?region=us-west-2#/webacs/requests/d2516947-2bd4-4049-a60a-bf0e5b623491>. The page displays a table of sample data from June 13, 2018, between 13:37:16 and 13:52:16. The table has columns: Source IP, URI, Matches rule, Action, and Time (UTC). Three rows of data are shown, each with expanded details about Client information, Request line, and Request headers. The Client information for each row is highlighted with a red box.

Sample data from 2018-06-13 13:37:16 to 13:52:16				
Source IP	URI	Matches rule	Action	Time (UTC)
▼ 78.188.65.252	/	DefaultAction	Block	13:41:18
<b>Client information:</b> Source IP: 78.188.65.252 Country: TR				
Request line: Method: GET URI: /				
Request headers: Host: web-lb-1387790621.us-west-2.elb.amazonaws.com				
▼ 114.32.36.220	/	DefaultAction	Block	13:41:27
<b>Client information:</b> Source IP: 114.32.36.220 Country: TW				
Request line: Method: GET URI: /				
Request headers: Host: web-lb-1387790621.us-west-2.elb.amazonaws.com				
▼ 207.154.242.159	/PMA/	DefaultAction	Block	13:41:28
<b>Client information:</b> Source IP: 207.154.242.159 Country: DE				
Request line: Method: HEAD URI: /PMA/				

**Look at the country information!!**

**Scary, don't you think?**

# WAF - Cleanup

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

# Compute - Part I

## Boot volume and Instance types

# EC2 - Boot volume types

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

# EC2 - Boot volume types

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.

Quick Start    My AMIs    AWS Marketplace    **Community AMIs**

Operating system    Architecture    **Root device type**

**Instance store**

Search community AMIs

AMI Name	Description	Select	Architecture
amzn-ami-pv-2012.09.1.i386-s3 - ami-0427ad34	Amazon Linux AMI i386 S3 Root device type: instance-store    Virtualization type: paravirtual	Select	32-bit
amzn-ami-minimal-pv-2013.09.1.i386-s3 - ami-061c8436	Amazon Linux AMI i386 MINIMAL S3 Root device type: instance-store    Virtualization type: paravirtual	Select	32-bit
amzn-ami-minimal-pv-2017.03.rc-0.20170320-x86_64-s3 - ami-0a3ab26a	Amazon Linux AMI 2017.03.rc-0.20170320 x86_64 Minimal PV S3 Root device type: instance-store    Virtualization type: paravirtual	Select	64-bit
amzn-ami-hvm-2013.09.2.x86_64-s3 - ami-0cf2973c	Amazon Linux AMI x86_64 HVM S3 Root device type: instance-store    Virtualization type: hvm	Select	64-bit
amzn-ami-minimal-pv-2013.09.1.x86_64-s3 - ami-0e1c843e		Select	

Get an instance store based EC2 instance

# EC2 - Other types of instances

The screenshot shows the EC2 Management console interface. The left sidebar navigation includes: 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), NETWORK & SECURITY (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), and LOAD BALANCING (Load Balancers). The main content area displays the 'Welcome to Amazon EC2 Spot instances' page. It features a 'Get started' button and three sections: 'EC2 Spot instances value' (with icons of a server and a coin, and a server with a plus sign), 'Name Your Price' (text: 'With Spot Instances, you never pay more than your bid price. Because Spot instances run on spare Amazon EC2 capacity, you can save up to 90% compared to On-Demand prices.'), 'Easily Provision Capacity' (text: 'Select and request the instances that match your application and cost requirements, and optimize for lowest cost or even distribution.'), and 'Increase Throughput' (text: 'Speed up or scale out your application by provisioning more compute capacity for a given budget.').

# EC2 - Other types of instances

The screenshot shows the AWS EC2 Management console with the 'Purchase Reserved Instances' dialog box open. The dialog box has the following settings:

- Platform: Linux/UNIX
- Tenancy: Default
- Offering Class: Any
- Instance Type: m4.large
- Term: Any
- Payment Option: Any

The main table lists various AWS sellers offering reserved instances for the m4.large instance type. Each row includes columns for Seller, Term, Effective Rate, Upfront Price, Hourly Rate, Payment Option, Offering Class, Quantity Available, Desired Quantity, Normalized units per hour, and an 'Add to Cart' button.

Seller	Term	Effective Rate	Upfront Price	Hourly Rate	Payment Option	Offering Class	Quantity Available	Desired Quantity	Normalized units per hour	Action
AWS	36 months	\$0.067	\$0.00	\$0.067	No Upfront	convertible	Unlimited	1	4	Add to Cart
AWS	12 months	\$0.074	\$0.00	\$0.074	No Upfront	standard	Unlimited	1	4	Add to Cart
AWS	12 months	\$0.064	\$276.00	\$0.032	Partial Upfront	standard	Unlimited	1	4	Add to Cart
AWS	12 months	\$0.062	\$541.00	\$0.000	All Upfront	standard	Unlimited	1	4	Add to Cart
AWS	36 months	\$0.043	\$565.00	\$0.022	Partial Upfront	standard	Unlimited	1	4	Add to Cart
AWS	36 months	\$0.057	\$745.00	\$0.029	Partial Upfront	convertible	Unlimited	1	4	Add to Cart
AWS	36 months	\$0.040	\$1,062.00	\$0.000	All Upfront	standard	Unlimited	1	4	Add to Cart
AWS	36 months	\$0.056	\$1,461.00	\$0.000	All Upfront	convertible	Unlimited	1	4	Add to Cart

You currently have no items in your cart.

# EC2 - Other types of instances

The screenshot shows the EC2 Management console interface. The left sidebar menu includes options like 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), NETWORK & SECURITY (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), and LOAD BALANCING (Load Balancers). The main content area displays the 'Welcome to Amazon EC2 Scheduled Reserved Instances' page, which explains that Scheduled Instances allow users to reserve Amazon EC2 instances on a recurring schedule. It features a 'Purchase Scheduled Instances' button and a note about Standard Reserved Instances. Below this, there are three sections: 'Reserve Capacity' (illustrated with a server icon and a checkmark), 'Plan Ahead and Save' (illustrated with a computer monitor and a dollar sign), and 'Run on Your Schedule' (illustrated with a calendar and a gear). Each section has a brief description and a 'Learn more' link.

Welcome to Amazon EC2 Scheduled Reserved Instances

Scheduled Instances allow you to reserve Amazon EC2 instances on a recurring schedule. You can purchase daily, weekly, or monthly reservations to ensure your applications have the compute capacity you need, when you need it.

[Purchase Scheduled Instances](#)

Prefer to reserve capacity on a continuous (24x7) basis? Check out [Standard Reserved Instances](#).

**More about Scheduled Reserved Instances**

**Reserve Capacity**

Like Standard Reserved Instances, Scheduled Instances allow you to reserve Amazon EC2 computing capacity so that you can launch the number of instances you reserved when you need them.

[Learn more](#)

**Plan Ahead and Save**

Scheduled Instances are cost-effective for workloads that run on a daily, weekly, or monthly recurring schedules. You pay only for the time you reserved.

[Learn more](#)

**Run on Your Schedule**

You can use Scheduled Instances for applications that do not require 24x7 access to capacity, such as overnight analytics jobs, weekday 9-to-5 financial processes, or monthly statistical modeling.

[Learn more](#)

# EC2 - Other types of instances

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#Hosts:sort=hostId>. The left sidebar menu is open, showing various EC2 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, Key Pairs, Network Interfaces). The 'Dedicated Hosts' option under INSTANCES is selected and highlighted with an orange border. The main content area displays a section titled 'Welcome to Dedicated Hosts' with a heading 'My Dedicated Host'. It shows a diagram of a server with three instances labeled 'My Instance 1', 'My Instance 2', and 'My Instance 3'. Below the diagram, a text block explains what a Dedicated Host is: 'An Amazon EC2 Dedicated host is a physical server with EC2 instance capacity dedicated for your use and allows you to reliably launch EC2 instances on the same Dedicated host over time. You have visibility over how your Dedicated hosts are utilized and you can determine how many sockets and cores are installed on the server. These features allow you to minimize licensing costs in a bring-your-own-license (BYOL) scenario and help you address corporate compliance and regulatory requirements.' A blue 'Allocate a Host' button is located below this text. At the bottom of the page, there's a 'More about Dedicated Hosts' link and a footer bar with links for Feedback, English, Privacy Policy, and Terms of Use.

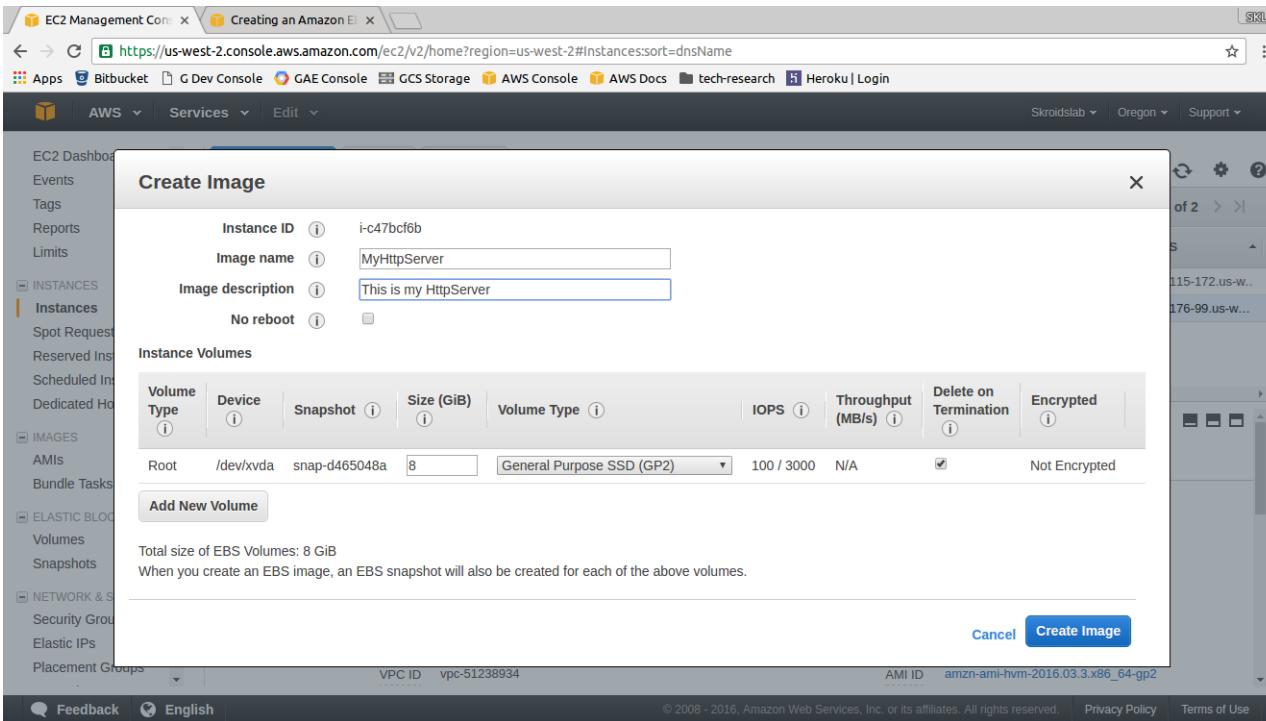
# Compute - Part II

AMI

# Activity - AMI from an existing instance

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with sections like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, AMIs, and more. The 'Instances' section is currently selected. In the main content area, an instance named 'Original' (ID: i-c47bcf6b) is listed as 'running'. A context menu is open over this instance, with the 'Image' option expanded, showing 'Create Image' as the selected option. Below the instance details, there are tabs for Description, Status Checks, Monitoring, and Tags. The 'Description' tab is active, showing various instance metadata such as Instance ID, Public DNS, Public IP, Instance state, Instance type, Private DNS, Private IPs, Secondary private IPs, VPC ID, and AMI ID.

# Activity - AMI



# Activity - AMI (auto snapshot created)

greatlearning

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation menu includes: 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 'Schemas' option under 'Elastic Block Store' is highlighted with an orange bar.

The main content area displays a table titled 'Create Snapshot' with one item listed:

Name	Snapshot ID	Size	Description	Status	Started
	snap-3ffc6f79	8 GiB	Created by CreateImage(i-c47bcf6b) for ami-93488bf3 from vol-d04ce659	completed	July 12, 2016 at 1:05:47

Below the table, a detailed view for 'Snapshot: snap-3ffc6f79' is shown with tabs for Description, Permissions, and Tags. The Description tab displays the following information:

Snapshot ID	Progress	Capacity
snap-3ffc6f79	100%	8 GiB
Status	Completed	Encrypted
vol-d04ce659	Not Encrypted	KMS Key ID
Started	July 12, 2016 at 1:05:47 PM UTC+5:30	KMS Key Aliases
Owner	278931287317	KMS Key ARN
Product codes	-	
Description	Created by CreateImage(i-c47bcf6b) for ami-93488bf3 from vol-d04ce659	

At the bottom of the page, there are links for Feedback, English, Copyright notice (© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.), Privacy Policy, and Terms of Use.

# Activity - AMI

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation bar includes links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, AMIs (selected), and Bundle Tasks. Under the Images section, there is also a link for Elastic Block Store (Volumes and Snapshots). The Network & Security section lists Security Groups, Elastic IPs, and Placement Groups.

The main content area displays a table of owned AMIs. A single row is selected, showing details for an AMI named "MyAMI". The table columns include Name, AMI ID, Source, Owner, Visibility, Status, Creation Date, and Platform. The AMI "MyAMI" has the following details:

Name	AMI ID	Source	Owner	Visibility	Status	Creation Date	Platform
MyAMI	ami-93488bf3	278931287317/M...	278931287317	Private	available	July 12, 2016 at 1:05:30 PM ...	Other

Below the table, a preview image titled "Image: ami-93488bf3" is shown. The image is a small thumbnail of the AMI. Below the image, there are three tabs: Details (selected), Permissions, and Tags. The Details tab displays the following information:

AMI ID	Owner	AMI Name	Source
ami-93488bf3	278931287317	MyAMI	278931287317/MyAMI
Status	Creation date	State Reason	Platform
available	July 12, 2016 at 1:05:30 PM UTC+5:30	-	Other Linux
Architecture	Virtualization type	Image Type	Description
x86_64	hvm	machine	-
Root Device Name	RAM disk ID	Root Device Type	Kernel ID
/dev/xvda	-	ebs	-
Product Codes		Block Devices	
-		/dev/xvda-snap-3ffc679:8:true:gp2	

At the bottom of the page, there are links for Feedback, English, Privacy Policy, and Terms of Use. The footer contains the copyright notice: © 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Activity - AMI

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation bar includes links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Spot Requests, Reserved Instances, Commands, Dedicated Hosts, Images, AMIs, and Bundle Tasks. Under the IMAGES section, AMIs is selected. The main content area displays a table of AMIs under the heading "Owned by me". One row is selected, showing the details for the AMI named "MyHttpServerAMI". The "Image: ami-e1889480" section provides detailed information about the AMI, including its ID, owner, status, creation date, architecture, virtualization type, root device name, RAM disk ID, product codes, and various source and platform details.

AMI Name	AMI ID	Source	Owner	Visibility	Status	Creation Date	Platform
MyHttpServer...	ami-e1889480	278931287317...	278931287317	Private	available	December 13, 2015 at 10:41...	Other Linux

**Image: ami-e1889480**

Details		Permissions	Tags	Edit
AMI ID	ami-e1889480	AMI Name	MyHttpServerAMI	
Owner	278931287317	Source	278931287317/MyHttpServerAMI	
Status	available	State Reason	-	
Creation date	December 13, 2015 at 10:41:20 PM UTC+5:30	Platform	Other Linux	
Architecture	x86_64	Image Type	machine	
Virtualization type	paravirtual	Description	This is my http server AMI	
Root Device Name	/dev/sda1	Root Device Type	ebs	
RAM disk ID	-	Kernel ID	-	
Product Codes	-	Block Devices	/dev/sda1=snap-b1b72bea:8:true:gp2	

# Activity - AMI

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with sections like EC2 Dashboard, Instances, Images, and Elastic Block Store. The 'AMIs' section is currently selected. In the main content area, an AMI named 'MyHttpServerAMI' is listed in a table. A context menu is open over this AMI, showing options: Launch, Spot Request, Deregister, Register New AMI, Copy AMI, Modify Image Permissions (which is highlighted in orange), Add/Edit Tags, and Modify Boot Volume Setting.

AMI ID	Source	Owner	Visibility	Status	Creation Date	Platform
ami-e1889480	278931287317/...	278931287317	Private	available	December 13, 2015 at 10:41...	Other Linux

**AMI Details:**

AMI ID	ami-e1889480	AMI Name	MyHttpServerAMI
Owner	278931287317	Source	278931287317/MyHttpServerAMI
Status	available	State Reason	-
Creation date	December 13, 2015 at 10:41:20 PM UTC+5:30	Platform	Other Linux
Architecture	x86_64	Image Type	machine
Virtualization type	paravirtual	Description	This is my http server AMI
Root Device Name	/dev/sda1	Root Device Type	ebs
RAM disk ID	-	Kernel ID	-
Product Codes	-	Block Devices	/dev/sda1=snap-b1b72bea:8:true:gp2

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

# Activity - AMI

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with options like EC2 Dashboard, Instances, Images, AMIs, and others. The main area shows a table of AMIs, with one row selected. A modal dialog box is open in the center, titled "Modify Image Permissions". The dialog displays the current permission status ("This image is currently: Public") and allows changing it to "Private". It also includes fields for "AWS Account Number" and "Add Permission", and a checkbox for granting "create volume" permissions to associated snapshots. At the bottom of the dialog are "Cancel" and "Save" buttons. The background table lists the AMI details: Name (MyHttpServerAMI), Description (This is my http server AMI), Root Device Name (/dev/sda1), Root Device Type (ebs), RAM disk ID (-), Kernel ID (-), Product Codes (-), and Block Devices (/dev/sda1=snap-b1b72bea:8:true:gp2).

# Activity - AMI

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

# Compute - Part II

## CLI and bootstrap scripts

# Activity - CLI setup

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

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

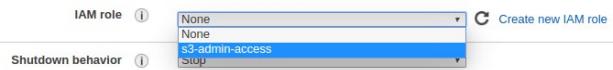
# Activity - CLI

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

# Activity - CLI

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

Step 3: Configure Instance Details



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

# Activity - Bootstrap script

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

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

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

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

# Compute - Part II

## EC2 Autoscaling

# Activity - Config group & Autoscale

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

# Question

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

# Activity - Launch configuration

The screenshot shows the AWS Auto Scaling console at the URL <https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2#LaunchConfigurations>. The left sidebar is collapsed, and the main content area displays the 'Welcome to Auto Scaling' page. A red box highlights the 'Launch Configurations' link under the 'LOAD BALANCING' section. The page features three main sections: 'Reusable Instance Templates', 'Automated Provisioning', and 'Adjustable Capacity', each with an icon and a brief description.

Welcome to Auto Scaling

You can use Auto Scaling to manage Amazon EC2 capacity automatically, maintain the right number of instances for your application, operate a healthy group of instances, and scale it according to your needs.

[Learn more](#)

[Create Auto Scaling group](#)

Note: To create your Auto Scaling groups in a different region, select your region from the navigation bar.

**Benefits of Auto Scaling**

**Reusable Instance Templates**

Provision instances based on a reusable template you define, called a launch configuration.

[Learn more](#)

**Automated Provisioning**

Keep your Auto Scaling group healthy and balanced, whether you need one instance or 1,000.

[Learn more](#)

**Adjustable Capacity**

Maintain a fixed group size or adjust dynamically based on Amazon CloudWatch metrics.

[Learn more](#)

**Additional Information**

[Getting Started Guide](#)  
[Documentation](#)  
[All EC2 Resources](#)  
[Forums](#)  
[Pricing](#)  
[Contact Us](#)

# Activity - Launch configuration

The screenshot shows the 'Create Auto Scaling Group' wizard in the AWS Management Console. The URL is <https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2#CreateAutoScalingGroup:source=wizard>. The top navigation bar includes links for EC2 Management, Secure, and various AWS services like Apps, Napabrick, BB, GCloud, AWS, Azure, Trello, Gmail, Google analytics, pointernext-Doc, and AWS Documenta. The user is signed in as Skroidslab with Oregon selected as the region.

**Create Auto Scaling Group**

To create an Auto Scaling group, you will first need to choose a template that your Auto Scaling group will use when it launches instances for you, called a launch configuration. Choose a launch configuration or create a new one, and then apply it to your group.

Later, if you want to use a different template, you can create another launch configuration and apply it to this group, even if you already have instances running in it. Using this method, you can update the software that your group uses when it launches new instances.

**Step 1: Create launch configuration**

First, define a template that your Auto Scaling group will use to launch instances. You can change your group's launch configuration at any time.

**Step 2: Create Auto Scaling group**

Next, give your group a name and specify how many instances you want to run in it. Your group will maintain this number of instances, and replace any that become unhealthy or impaired. You can optionally configure your group to adjust its capacity according to

[Cancel](#) [Create launch configuration](#)

Feedback English © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

# Activity - Launch configuration

The screenshot shows the AWS EC2 Management Console interface for creating a launch configuration. The top navigation bar includes links for EC2 Management Console, Apps, Bitbucket, G Dev Console, GAE Console, GS Root, AWS Console, AWS Docs, and tech-research. The user is in the Oregon region.

The main content area displays the 'Create Launch Configuration' wizard, step 1: Choose AMI. It shows a list of available AMIs:

- Amazon Linux AMI 2015.09.1 (HVM), SSD Volume Type - ami-f0091d91**  
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.  
Root device type: ebs Virtualization type: hvm  
**Select** button (disabled)
- Red Hat Enterprise Linux 7.2 (HVM), SSD Volume Type - ami-775e4f16**  
Red Hat Enterprise Linux version 7.2 (HVM), EBS General Purpose (SSD) Volume Type  
Root device type: ebs Virtualization type: hvm  
**Select** button (disabled)
- SUSE Linux Enterprise Server 12 SP1 (HVM), SSD Volume Type - ami-d2627db3**  
SUSE Linux Enterprise Server 12 Service Pack 1 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.  
Root device type: ebs Virtualization type: hvm  
**Select** button (disabled)
- Ubuntu Server 14.04 LTS (HVM), SSD Volume Type - ami-5189a661**  
**Select** button (disabled)

On the left, a sidebar titled 'Quick Start' offers links for My AMIs, AWS Marketplace, Community AMIs, and a checkbox for 'Free tier only'. The 'Free tier only' checkbox is checked.

At the bottom, 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 - Launch configuration

The screenshot shows the AWS EC2 Management console with the URL <https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2#CreateLaunchConfiguration:CreationFlowType=linkToASGCreation>. The page is titled "Create Launch Configuration".

The navigation bar at the top includes links for Apps, Napabrick, BB, GCloud, AWS, Azure, Trello, Gmail, Google analytics, pointernext, AWS Documenta, Services, Resource Groups, and Support.

The main content area shows the "Choose Instance Type" step of the wizard. The steps are numbered 1. Choose AMI, 2. Choose Instance Type, 3. Configure details, 4. Add Storage, 5. Configure Security Group, and 6. Review.

A message states: "Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs."

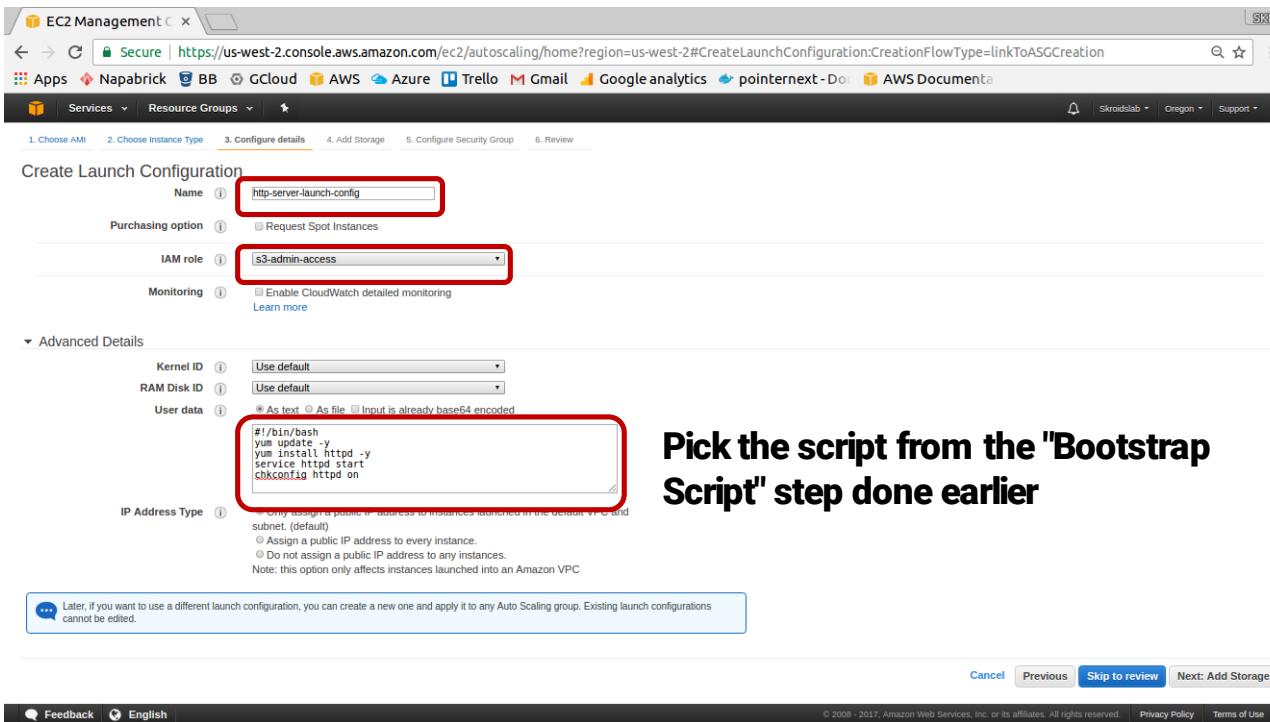
Below this is a table titled "Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)". The table filters by "All instance types" and "Current generation". It lists the following instance types:

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
<input checked="" type="checkbox"/>	General purpose	<b>t2.micro</b> Free tier eligible	1	1	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate
<input type="checkbox"/>	General purpose						

At the bottom of the table are buttons for "Cancel", "Previous", and "Next: Configure details".

The footer of the page includes links for Feedback, English, and various legal notices: © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved., Privacy Policy, and Terms of Use.

# Activity - Launch configuration



Create Launch Configuration

Name: http-server-launch-config

Purchasing option: Request Spot Instances

IAM role: s3-admin-access

Monitoring: Enable CloudWatch detailed monitoring

Advanced Details

Kernel ID: Use default

RAM Disk ID: Use default

User data:

```
#!/bin/bash
yum update -y
yum install httpd -y
service httpd start
chkconfig httpd on
```

IP Address Type: Only assign a public IP address to instances launched in the default VPC and subnet. (default)

Later, if you want to use a different launch configuration, you can create a new one and apply it to any Auto Scaling group. Existing launch configurations cannot be edited.

Cancel Previous Skip to review Next: Add Storage

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

# Activity - Launch configuration

The screenshot shows the AWS EC2 Management console with the URL <https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2#CreateLaunchConfiguration:CreationFlowType=linkToASGCreation>. The navigation bar includes links for Apps, Napabrick, BB, GCloud, AWS, Azure, Trello, Gmail, Google analytics, pointernext - Do, AWS Documenta, Services, Resource Groups, and various account and support options.

The main content area displays the 'Create Launch Configuration' wizard, currently on step 4: Add Storage. The steps are numbered 1. Choose AMI, 2. Choose Instance Type, 3. Configure details, 4. Add Storage, 5. Configure Security Group, and 6. Review.

**Create Launch Configuration**  
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes.  
<https://docs.aws.amazon.com/console/ec2/launchinstance/storage> about storage options in Amazon EC2.

The storage configuration table shows one volume entry:

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput	Delete on Termination	Encrypted
Root	/dev/xvda	snap-066b5016ee2261563	8	General Purpose (SSD)	100 / 3000	N/A	<input checked="" type="checkbox"/>	No

**Add New Volume** button is available below the table.

A callout message states: Free tier eligible customers can get up to 30 GB of EBS storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

At the bottom, there are navigation buttons: Cancel, Previous, Skip to review, Next: Configure Security Group, and a feedback link.

# Activity - Launch configuration

The screenshot shows the AWS EC2 Management console with the URL <https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2#CreateLaunchConfiguration:CreationFlowType=linkToASGCreation>. The page is titled "Create Launch Configuration" and is currently on step 5: "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 ID	Name	VPC ID	Description	Actions
sg-05123160	default	vpc-51238934	default VPC security group	<a href="#">Copy to new</a>
sg-5724b72e	docker-machine	vpc-51238934	Docker Machine	<a href="#">Copy to new</a>
sg-a52f18de	open-port-22	vpc-51238934	Open SSH	<a href="#">Copy to new</a>
sg-5722f82c	open-port-80	vpc-51238934	Open port 80 for http traffic	<a href="#">Copy to new</a>
sg-2538ae42	rds-launch-wizard	vpc-51238934	Created from the RDS Management Console	<a href="#">Copy to new</a>

Inbound rules for sg-5722f82c Selected security groups: sg-5722f82c.

Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0

Buttons at the bottom: Cancel, Previous, Review.

# Activity - Launch configuration

**Create Launch Configuration**

Review the details of your launch configuration. You can go back to edit the details of each section before you finish.

**AMI Details**

**Amazon Linux AMI 2017.03.0 (HVM), SSD Volume Type - ami-8ca83fec**

The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

**Instance Type**

Instance Type	ECUs	vCPUs	Memory GiB	Instance Storage (GiB) GiB	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

**Launch configuration details**

**Name:** http-server-launch-config  
**Purchasing option:** On demand  
**EBS Optimized Monitoring:** No  
**IAM role:** s3-admin-access  
**Tenancy:** Shared tenancy (multi-tenant hardware)  
**Kernel ID:** Use default  
**RAM Disk ID:** Use default  
**User data:** iyEvYmluL2Jhc2gkexVlIHwZGF0ZSAleQp5dW0gaw5zdGFsbCBodHRwZCAleQpzZXJ2aWhlGh0dIBkiHhN0YXJ0CmNoa2NvbmtZp2yBodHRwZCBvbgo=

**IP Address Type:** Only assign a public IP address to instances launched in the default VPC and subnet. (default)

**Storage**

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput	Delete on Termination	Encrypted
Root	/dev/xvda	snap-066b5016ee2261	8	gp2	N/A	N/A	Yes	No

**Buttons:** Cancel, Previous, Create launch configuration

Pick the existing PEM and acknowledge in the next step

# Activity - Auto scale group

Select Load Balancing checkbox  
Select the existing target group

Health Check Type = EC2  
(requires the /health.html to be there in the scaled instances)

# Activity - Auto scale group

The screenshot shows the AWS Auto Scaling Group creation process at Step 2: Configure scaling policies. The URL is <https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2#CreateAutoScalingGroup:source=lc;launchConfigurationName=awseb-e-z1>. The page title is "Create Auto Scaling Group". It includes sections for "Increase Group Size" and "Decrease Group Size", both with "Add new alarm" buttons highlighted with a red box.

**Create Auto Scaling Group**

You can optionally add scaling policies if you want to adjust the size (number of instances) of your group automatically. A scaling policy is a set of instructions for making such adjustments in response to an Amazon CloudWatch alarm that you assign to it. In each policy, you can choose to add or remove a specific number of instances or a percentage of the existing group size, or you can set the group to an exact size. When the alarm triggers, it will execute the policy and adjust the size of your group accordingly. [Learn more](#) about scaling policies.

Keep this group at its initial size  
 Use scaling policies to adjust the capacity of this group

Scale between  and  instances. These will be the minimum and maximum size of your group.

**Increase Group Size**

Name:   
Execute policy when:  [Add new alarm](#) (highlighted with a red box)

Take the action:   instances [Add step](#)

Instances need:  seconds to warm up after each step

[Create a simple scaling policy](#)

**Decrease Group Size**

Name:   
Execute policy when:  [Add new alarm](#)

Take the action:   instances [Add step](#)

[Create a simple scaling policy](#)

Cancel Previous Review Next: Configure Notifications

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

# Activity - Auto scale group

The screenshot shows the AWS EC2 Management Console interface for creating an Auto Scaling Group. The main page displays sections for 'Increase Group Size' and 'Decrease Group Size', both using CloudWatch Metrics triggers. An 'Auto Scaling Policies' section is visible at the bottom. A modal window titled 'Create Alarm' is overlaid, detailing the configuration of a CloudWatch alarm named 'awsec2-ProdScaleGroup-High-CPU-Utilization'. The alarm triggers when CPU Utilization is greater than or equal to 10% for at least 2 consecutive periods of 5 minutes. The 'Create Alarm' button is at the bottom right of the modal.

# Activity - Auto scale group

The screenshot shows the 'Create Auto Scaling Group' wizard in the AWS EC2 Management console. The 'Increase Group Size' section is active, displaying a scaling policy named 'Increase Group Size' triggered by a CPUUtilization threshold of 80. It adds 1 instance when CPUUtilization <= 80 and removes 1 instance when CPUUtilization >= 30. The 'Instances need' field is set to 300 seconds to warm up after each step. The 'Decrease Group Size' section shows a similar policy triggered by a CPUUtilization threshold of 30, removing 1 instance when CPUUtilization >= 30.

**Increase Group Size**

Name: Increase Group Size  
Execute policy when: awsec2-http-server-auto-scale-CPUUtilization Edit Remove  
breaches the alarm threshold: CPUUtilization >= 80 for 300 seconds  
for the metric dimensions AutoscalingGroupName = http-server-auto-scale

Take the action: Add 1 instances when 80 <= CPUUtilization < infinity  
Add Step  
Instances need: 300 seconds to warm up after each step

Create a simple scaling policy (i)

**Decrease Group Size**

Name:   
Execute policy when: awsec2-http-server-auto-scale-High-CPUUtilization Edit Remove  
breaches the alarm threshold: CPUUtilization <= 30 for 300 seconds  
for the metric dimensions AutoscalingGroupName = http-server-auto-scale

Take the action: Remove 1 instances when 30 >= CPUUtilization > -infinity  
Add Step

Create a simple scaling policy (i)

Cancel Previous Review Next: Configure Notifications

# Activity - Auto scale group

The screenshot shows the AWS Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2#CreateAutoScalingGroup:source=lc;launchConfigurationName=awseb-e-z15h>. The page is titled "Create Auto Scaling Group" and is on step 3: "Configure Notifications".

**Send a notification to:** [redacted].com (dropdown menu) [create topic](#) [X](#)

**Whenever instances:**

- launch
- terminate
- fail to launch
- fail to terminate

[Add notification](#)

At the bottom, there are navigation links: [Cancel](#), [Previous](#), [Review](#), and [Next: Configure Tags](#).

# Activity - Auto scale group

The screenshot shows the AWS EC2 Management console with the URL <https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2#CreateAutoScalingGroup:source=lc;launchConfigurationName=http-server-launch-conf>. The page is titled "Create Auto Scaling Group". Step 4, "Configure Tags", is selected. A table shows one tag: Name (auto-scale-group-http-server) and Value (auto-scale-group-http-server). There is a checkbox labeled "Tag New Instances" which is checked. Below the table, there is a button "Add tag" and a note "49 remaining". At the bottom, there are buttons for "Cancel", "Previous", and "Review".

# Activity - Auto scale group

The screenshot shows the AWS Management Console EC2 Management Console interface for creating an Auto Scaling group. The URL in the browser is <https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2#CreateAutoScalingGroup:source=l;launchConfigurationName=awsec-e-zih>. The top navigation bar includes links for Apps, Bitbucket, G Dev Console, GAE Console, GS Root, AWS Console, AWS Docs, and tech-research. The AWS logo is in the top left, and the region is set to Oregon.

The main content area shows the "Create Auto Scaling Group" wizard, Step 5: Review. The steps are: 1. Configure Auto Scaling group details, 2. Configure scaling policies, 3. Configure Notifications, 4. Configure Tags, and 5. Review. Step 5 is highlighted with an orange underline.

**Create Auto Scaling Group**  
Please review your Auto Scaling group details. You can go back to edit changes for each section. Click **Create Auto Scaling group** to complete the creation of an Auto Scaling group.

**Auto Scaling Group Details**

Group name	ProdScaleGroup
Group size	1
Minimum Group Size	1
Maximum Group Size	6
Subnet(s)	subnet-fa9219f, subnet-ee30f1b7, subnet-22b21155
Load Balancers	Web-LB1
Health Check Type	ELB
Health Check Grace Period	300
Detailed Monitoring	No
Instance Protection	None

**Scaling Policies**

**Increase Group Size** With alarm = CPU>80%; Add 2 instances and 300 seconds for instances to warm up

**Decrease Group Size** With alarm = awsec2-ProdScaleGroup-High-CPU-Utilization; Remove 2 instances

**Notifications**

**Create Auto Scaling group**

At the bottom, there are links for Feedback, English, Copyright notice (© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.), Privacy Policy, and Terms of Use.

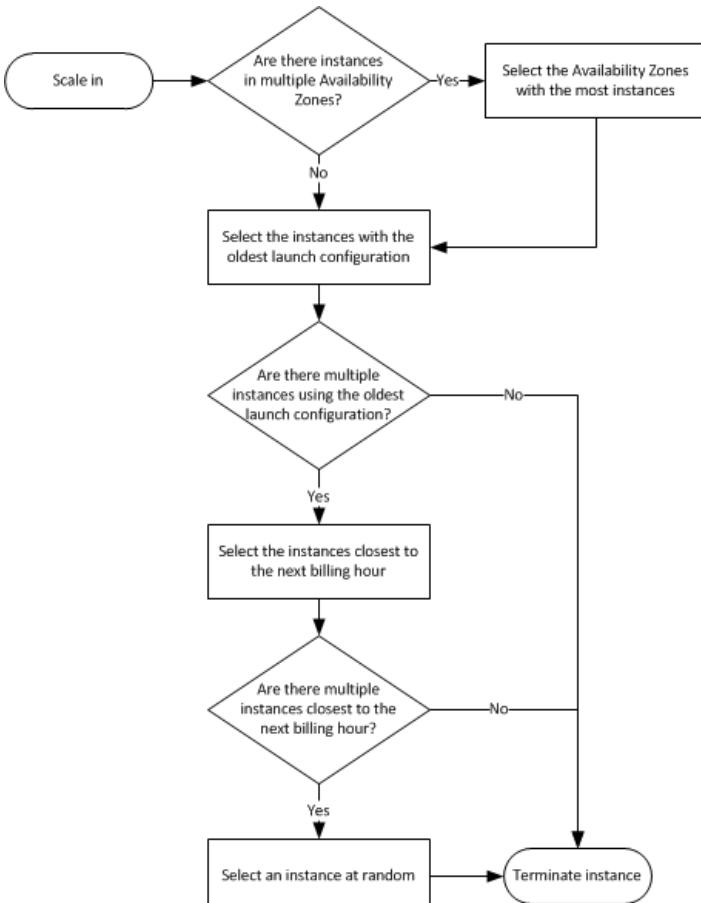
# Activity - Auto scale group

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation includes 'EC2 Dashboard', 'Events', 'Tags', 'Reports', 'Limits', 'INSTANCES' (with 'Instances', 'Spot Requests', 'Reserved Instances', 'Commands', 'Dedicated Hosts'), 'IMAGES' (with 'AMIs', 'Bundle Tasks'), 'ELASTIC BLOCK STORE' (with 'Volumes', 'Snapshots'), 'NETWORK & SECURITY' (with 'Security Groups', 'Elastic IPs', 'Placement Groups', 'Key Pairs'). The main content area shows a 'Create launch configuration' button, a 'Create Auto Scaling group' button, and an 'Actions' dropdown. A table lists 'Launch Configuration: awseb-e-zl5hc4mezj-stack-AWSEBAutoScalingLaunchConfiguration-LBMY3OYJMZ4N'. The table details are:

AMI ID	ami-63cdd902	Instance Type	t1.micro
IAM Instance Profile	aws-elasticbeanstalk-ec2-role	Kernel ID	
Key Name		Monitoring	false
EBS Optimized	false	Security Groups	awseb-e-zl5hc4mezj-stack-AWSEBSecurityGroup-1DAK9RORSWHFK
Spot Price		Creation Time	Wed Dec 16 11:16:47 GMT+530 2015
RAM Disk ID		Block Devices	-
User data	<a href="#">View User data</a>	IP Address Type	Only assign a public IP address to instances launched in the default VPC and subnet. (default)

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

# Auto scale instance termination



# Compute - Part II

## Instance metadata & Placement groups

# Activity - Instance metadata

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

# Activity - Placement groups

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

# Activity - Placement groups

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation includes sections for Instances, AMIs, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. The 'Placement Groups' section is currently selected. The main content area displays a message: "You do not have any placement groups defined." followed by "Click the Create Placement Group button to create one." A modal window titled "Create Placement Group" is centered, containing a text input field with the value "OregonGroup" and two buttons: "Cancel" and "Create". At the bottom of the main content area, there is a placeholder text: "Select a placement group above". The browser address bar shows the URL: <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#PlacementGroups:sort=groupName>.

# Activity - Placement groups

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#PlacementGroups:sort=groupName>. The left sidebar is collapsed, and the main content area displays the 'Placement Groups' section. At the top, there are buttons for 'Create Placement Group' and 'Delete Placement Group'. Below this is a search bar with the placeholder 'Filter by attributes or search by keyword'. A table lists one placement group: 'OregonPlacementGroup' with 'cluster' strategy and 'available' state. The table has columns for 'Group Name', 'Strategy', and 'State'. The 'OregonPlacementGroup' row is highlighted. Below the table, a section titled 'Placement Group: OregonPlacementGroup' provides detailed information about the group.

Group Name	Strategy	State
OregonPlacementGroup	cluster	available

**Placement Group: OregonPlacementGroup**

Group Name: OregonPlacementGroup  
Strategy: cluster  
State: available

# Activity - Placement groups

EC2 Management Console Placement Groups - Ami

https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard:

AWS Services Edit

Skroldslab Oregon Support

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

**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  Launch into Auto Scaling Group

Purchasing option  Request Spot instances

Network vpc-51238934 (172.31.0.0/16) (default)

Subnet No preference (default subnet in any Availability Zone)

Auto-assign Public IP Use subnet setting (Enable)

Placement group No placement group

IAM role OregonGroup

Shutdown behavior Stop

Enable termination protection  Protect against accidental termination

Monitoring  Enable CloudWatch detailed monitoring

Cancel Previous Review and Launch Next: Add Storage

Feedback English

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

# Compute - Part II

## Windows on EC2

# Windows EC2 instance

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

# Activity - Windows EC2 instance

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with sections like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, Elastic Block Store, Network & Security, and Key Pairs. The 'Instances' section is currently selected. In the main content area, a table lists three instances: 'Http Server1', 'Windows12', and 'Http Server2'. The 'Windows12' row is selected. A context menu is open over this row, with the 'Actions' option expanded. The menu items shown are 'Connect', 'Get Windows Password', 'Launch More Like This', 'Instance State', 'Instance Settings', 'Image', 'Networking', and 'CloudWatch Monitoring'. Below the table, detailed information for the selected instance (Windows12) is displayed, including Instance ID (i-71af84b5), Instance state (running), Instance type (t2.micro), Private DNS (ip-172-31-44-248.us-west-2.compute.internal), Private IPs (172.31.44.248), Secondary private IPs, Public DNS (ec2-54-201-218-158.us-west-2.compute.amazonaws.com), Public IP (54.201.218.158), Elastic IP (-), Availability zone (us-west-2b), Security groups (launch-wizard-2, view rules), and Scheduled events (No scheduled events). At the bottom of the page, there are links for Feedback, English, Privacy Policy, and Terms of Use.

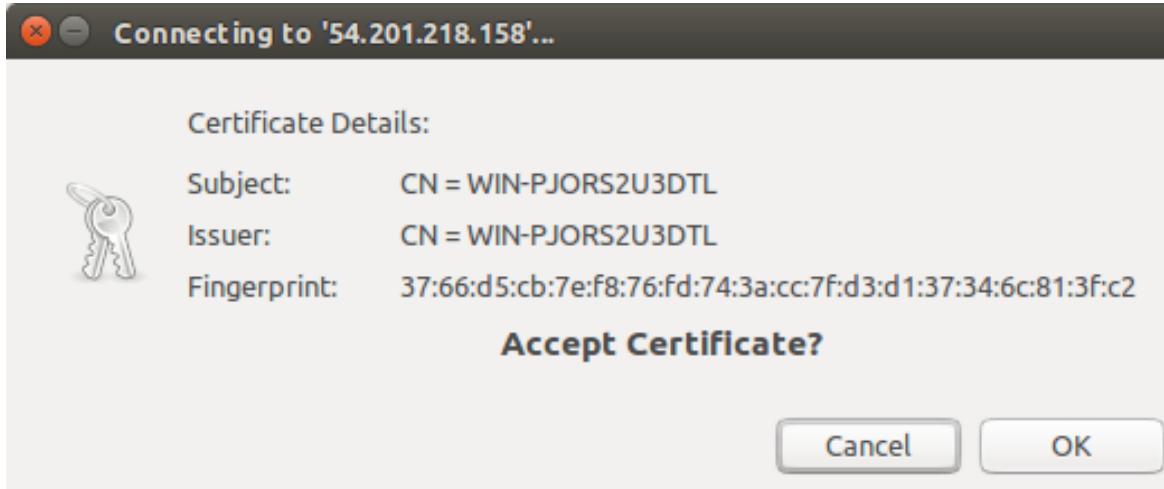
# Activity - Windows EC2 instance

The screenshot shows the AWS EC2 Management Console interface. On the left, the navigation pane is visible with sections like EC2 Dashboard, Instances (selected), Images, and Network & Security. In the center, there's a modal dialog titled "Retrieve Default Windows Administrator Password". The dialog contains instructions for remote access via Remote Desktop Connection, mentioning a default password created at launch and its availability in the system log. It also notes the association of a key pair named "nmwindows" with the instance. Below this, there are two options: "Key Pair Path" (with a "Choose File" button) and a text area containing the private key content. At the bottom of the dialog are "Cancel" and "Decrypt Password" buttons. To the right of the dialog, the main EC2 dashboard shows a list of instances with their Public DNS names and IP addresses. The first three instances listed are ec2-54-201-208-132.us-west-2.amazonaws.com, ec2-54-201-218-158.us-west-2.amazonaws.com, and ec2-54-201-221-50.us-west-2.amazonaws.com, all associated with the Public VPC.

# Activity - Windows EC2 instance

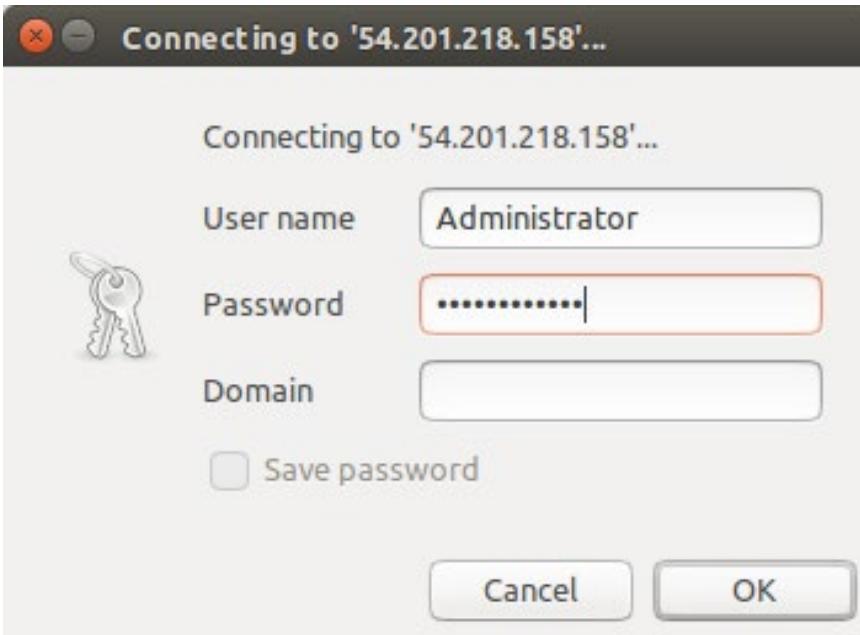
The screenshot shows the AWS EC2 Management Console interface. On the left, the navigation pane includes options like EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Commands, Dedicated Hosts, AMIs, Bundle Tasks, Volumes, Snapshots, Security Groups, Elastic IPs, Placement Groups, and Kinesis Data Firehose. The main content area has tabs for Launch Instance, Connect, and Actions. A modal window titled "Retrieve Default Windows Administrator Password" is open. It contains two sections: a green box with a checkmark stating "Password Decryption Successful" and a message that the password for instance i-71af84b5 (Windows12) was successfully decrypted. Below this is an orange box with a warning icon and the message "Password change recommended". It advises changing the default password to one that will be remembered. At the bottom of the modal, it says "You can connect remotely using this information:" followed by the Public IP (54.201.218.158), User name (Administrator), and Password (Password%tSNkbw8sF). A "Close" button is at the bottom right of the modal. In the background, there's a list of instances with their Public DNS names and IP addresses, all associated with the same Public IP (54.201.218.158). The status column shows "Public" for most instances. The bottom of the screen includes links for Feedback, English, and various AWS services.

# Activity - Windows EC2 instance

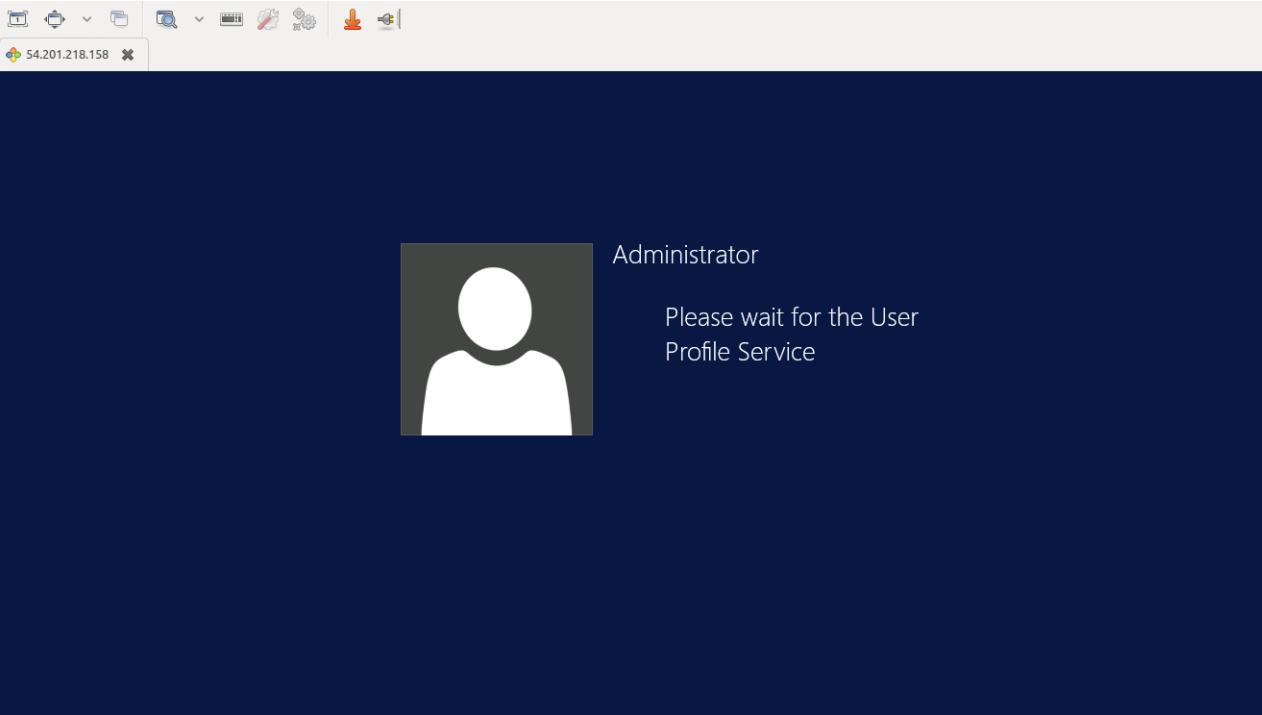


Total 0 items.

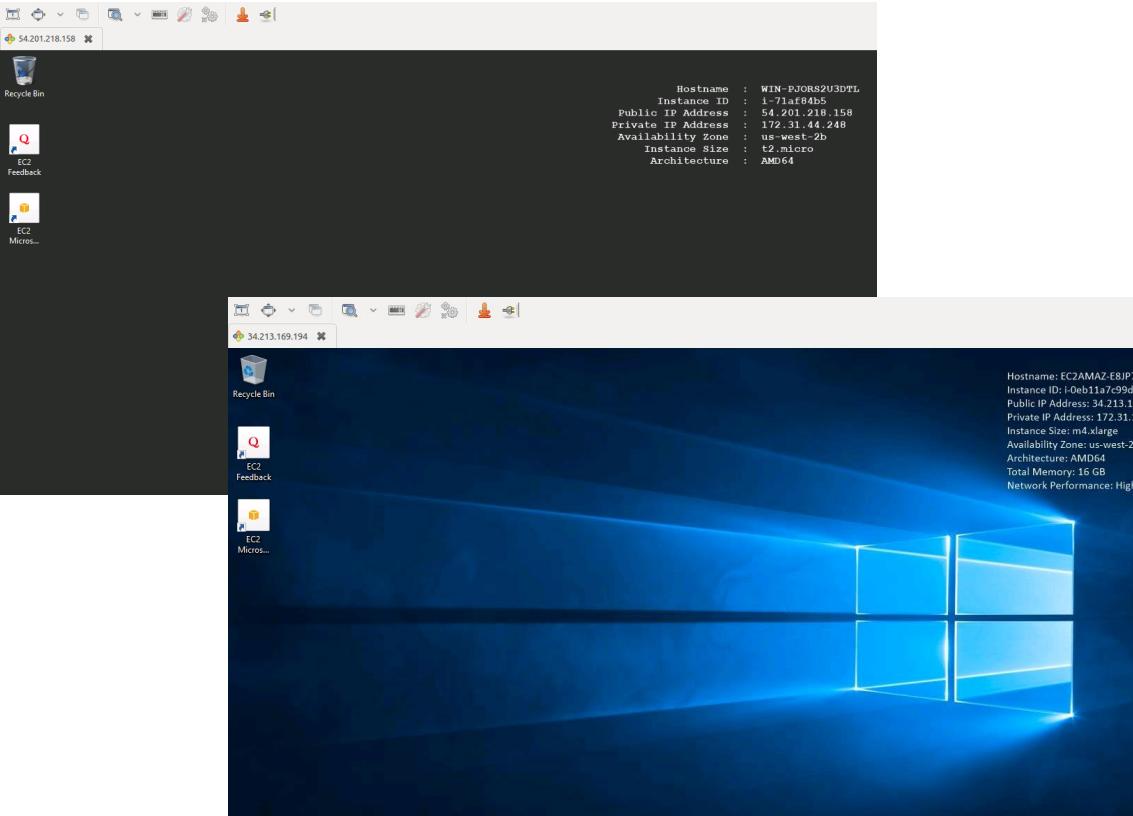
# Activity - Windows EC2 instance



# Activity - Windows EC2 instance



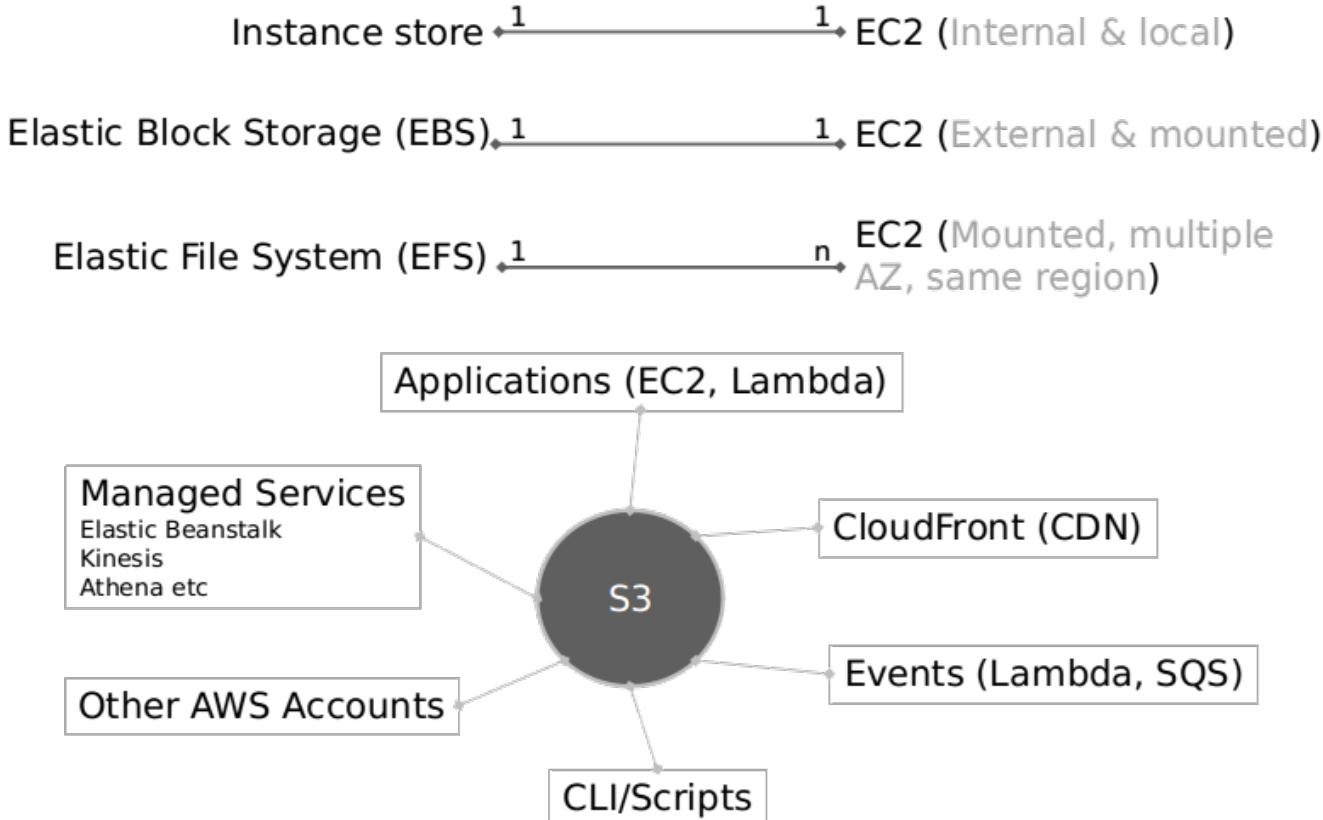
# Activity - Windows EC2 instance



# 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: <a href="#">[redacted]</a>	KMS Key Aliases: <a href="#">[redacted]</a>	
Volume type: gp2	Product codes: -	KMS Key ARN: <a href="#">[redacted]</a>	
IOPS: 24 / 3000			

At the bottom of the page, there are links for Feedback, English, and a footer with copyright information.

# Activity - Volumes

EC2 Management

Secure | https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Volume:sort=createTime

Services Resource Groups

Create Volume Actions

Name: web-server-1 Volume ID: vol-09f5e68cf9d632e76 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-0749a28555320dbf7 (web-server-1):/dev/xvda (attached)

Volumes: vol-08f5e68cf9d632e76 (web-server-1)

Description Status Checks Monitoring Tags

Volume Status: Okay Availability Zone: us-west-2c

IO Status: Enabled Since: April 12, 2017 at 5:14:40 PM UTC+5:30 Description: - IO Performance: Not Applicable Since: Description: This feature only applies to attached Provisioned IOPs volumes at this time.

Auto-Enabled IO: Enabled Edit

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](#).

Feedback English

© 2008 - 2017, 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 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 5:21:11, 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 user is in the 'Create Volume' section. The 'Volume Type' dropdown is set to 'Magnetic'. A modal window titled 'Filter by attributes' is open, listing the following volume types:

- General Purpose SSD (GP2)
- Provisioned IOPS SSD (IO1)
- Cold HDD (SC1)
- Throughput Optimized HDD (ST1)
- Magnetic

The 'Magnetic' option is highlighted in yellow. Other fields visible include 'Size (GiB)' (10), 'Availability Zone\*' (us-west-2a), and 'Encryption' (checkbox). The 'Create Volume' button is at the bottom right.

# 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-387cdect. 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 for the volume 'vol-387cdect' is shown, including its Volume ID, Size (10 GB), Created date (December 13, 2015 at 7:59:02 PM UTC+5:30), State (available), and various metadata fields like Volume Type (standard), Product codes, and IOPS.

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-387cdect	standard	-		December 13, 2015...	us-west-2b	available

**Volumes: vol-387cdect**

Description Status Checks Monitoring Tags

Volume ID	vol-387cdect	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		KMS Key ID	
Volume type	standard	KMS Key Aliases	
Product codes	-	KMS Key ARN	
IOPS	-		

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 such as Create Volume, Delete Volume, Attach Volume, Detach Volume, Force Detach Volume, Create Snapshot, Change Auto-Enable IO Setting, and Add/Edit Tags. The volume details page below shows information like Volume ID, Size, Created, State, Attachment information, Volume type, and Product codes.

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	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: KMS Key ARN: KMS Key Aliases:
Volume type: standard	
Product codes: -	

# 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). In the main area, a table lists volumes attached to instances. One volume, 'vol-387cdecf', is selected. A modal dialog titled 'Detach Volume' is open, asking 'Are you sure you want to detach this volume? vol-387cdecf'. Below the dialog, the volume details are shown: 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: -. To the right of the volume details, there are columns for Alarm status (None), Snapshot (-), Availability Zone (us-west-2b), Encrypted (Not Encrypted), KMS Key ID, KMS Key Aliases, and KMS Key ARN.

EC2 Management Console web-lb1-1634359284.us-west-2 Amazon EC2 Instance API

https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Volumes:sort=createTime

Skroldslab | Oregon | Support

Create Volume Actions

Filter by tags and attributes or search by keyword

1 to 3 of 3

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

**Detach Volume**

Are you sure you want to detach this volume?  
vol-387cdecf

Cancel Yes, Detach

Volume

Description Status Checks

Volumes

Volume

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 Aliases:

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 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:

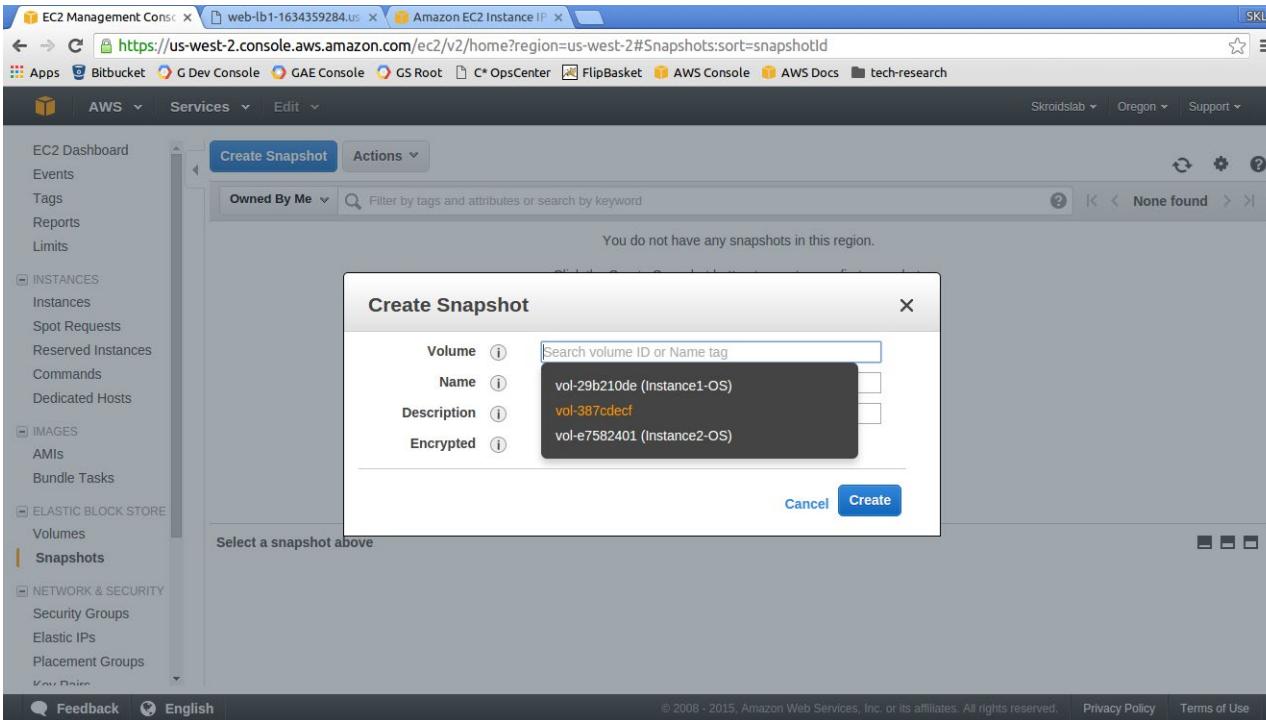
	Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone	State
	Instance1-OS	vol-29b210de	8 GiB	gp2	24 / 3000	snap-ad8e61f8	December 13, 2015...	us-west-2b	in-use
	Instance2-OS	vol-e7582401	8 GiB	standard	-	snap-ad8e61f8	December 13, 2015...	us-west-2c	in-use
		vol-387cdefc	10 GiB	standard	-		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 'S' icon under 'ELASTIC BLOCK STORE' selected, and 'Snapshots' highlighted. The main content area displays a message: 'You do not have any snapshots in this region.' Below this message is a blue 'Create Snapshot' button. At the bottom of the page, there is a footer bar with links for 'Feedback', 'English', 'Privacy Policy', and 'Terms of Use'. The browser's address 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 'Snapshots' option 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 right of the dialog box are two buttons: "Cancel" and "Create".

# 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**

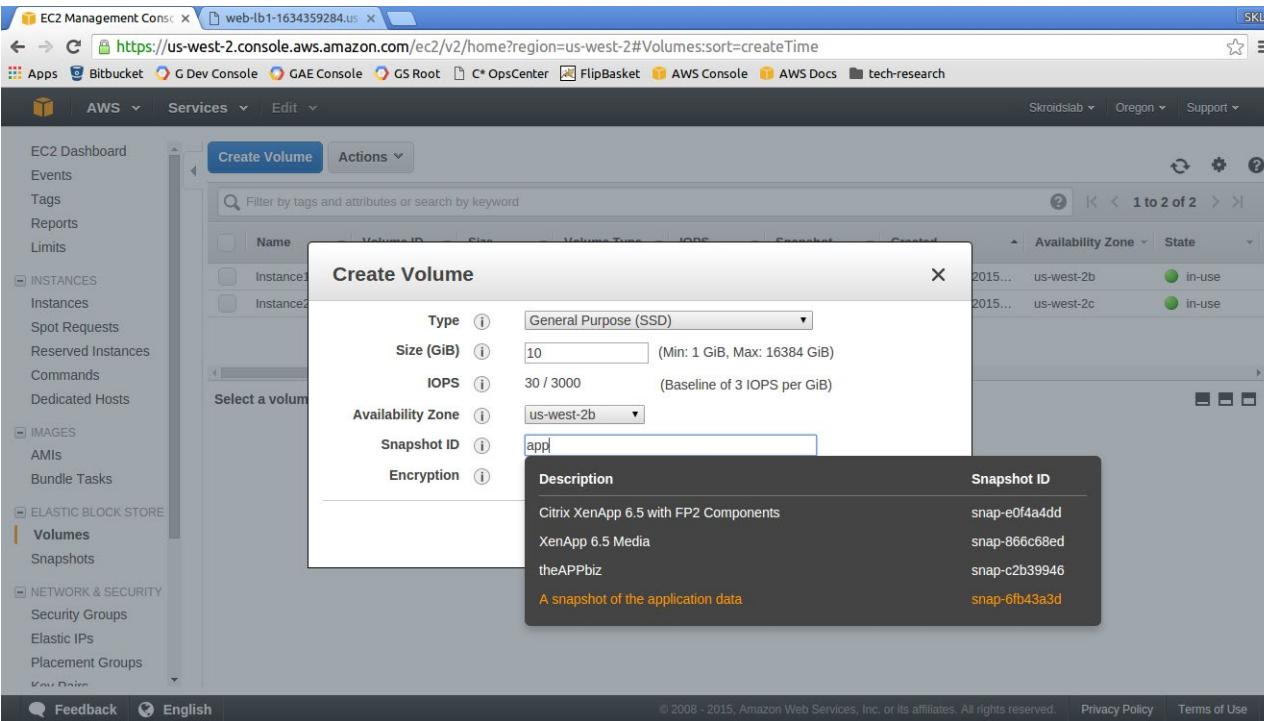
<b>Snapshot ID</b>	snap-6fb43a3d	<b>Progress</b>	0%
<b>Status</b>	pending	<b>Capacity</b>	10 GiB
<b>Volume</b>	vol-387cdecf	<b>Encrypted</b>	Not Encrypted
<b>Started</b>	December 13, 2015 at 8:35:09 PM UTC+5:30	<b>KMS Key ID</b>	
<b>Owner</b>	278931287317	<b>KMS Key Aliases</b>	
<b>Product codes</b>	-	<b>KMS Key ARN</b>	
<b>Description</b>	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 URL in the browser is <https://us-west-2.console.aws.amazon.com/efs/home?region=us-west-2#/firstrun>. The top navigation bar includes links for Secure, Apps (Napabrick, BB, GCloud, AWS, Azure, Trello, Gmail, Google analytics, pointernext, AWS Documenta), Services (selected), Resource Groups, and various AWS regions (Oregon, Support). A central icon of a stack of three boxes is displayed above the title.

## Amazon Elastic File System (EFS)

Amazon EFS provides file storage for use with your EC2 instances.

[Create file system](#)

[Getting started guide](#)

### 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, the 'Create mount targets' section lists three Availability Zones: us-west-2a, us-west-2b, and us-west-2c. For each zone, it shows the subnet (e.g., subnet-22b21155), IP address assignment ('Leave blank for automatic'), and security groups (e.g., sg-05123160 - default). The 'Availability Zone' and 'Subnet' columns have red boxes around them, and the 'IP address' column also has a red box around the 'Leave blank for automatic' option. At the bottom right are 'Cancel' and 'Next Step' buttons.

Create file system

Step 1: Configure file system access

Step 2: Configure optional settings

Step 3: Review and create

Configure file system access

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.

VPC vpc-51238934 (default)

Create mount targets

Instances connect to a file system by using mount targets you create. We recommend creating a mount target in each of your VPC's Availability Zones so that EC2 instances across your VPC can access the file system.

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

Cancel Next Step

# 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. At the top, there's a success message: "Success! You have created a file system. You can now mount it from an on-premises server over an NFSv4.1 client installed. You can also mount your file system from an on-premises server over an AWS Direct Connect connection. Click [here](#) for EC2 mount instructions, and [here](#) for on-premises mount instructions." Below this, there are three buttons: "Manage file system access", "Manage tags", and "Delete file system". A modal window is open, highlighting the "Manage file system access" button.

**File systems**

	Name	File system ID	Metered size	Number of mount targets	Creation date
*	skl-efs	fs-b914c010	6.0 KiB	3	2017-04-14T14:42:10Z

**Other details**

Owner ID: 278931287317  
Life cycle state: Available  
Performance mode: General Purpose

**File system access**

DNS name: fs-b914c010.efs.us-west-2.amazonaws.com

Amazon EC2 mount instructions  
AWS Direct Connect mount instructions

**Mount targets**

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

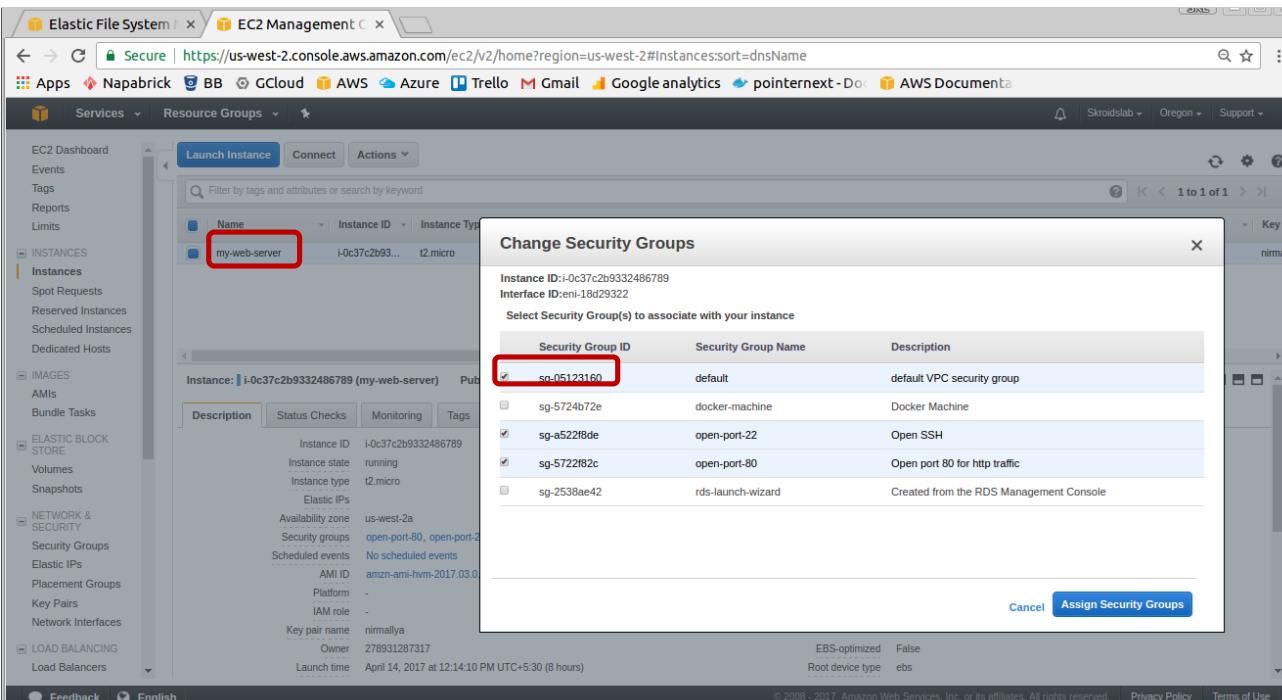
# Activity - EFS

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.

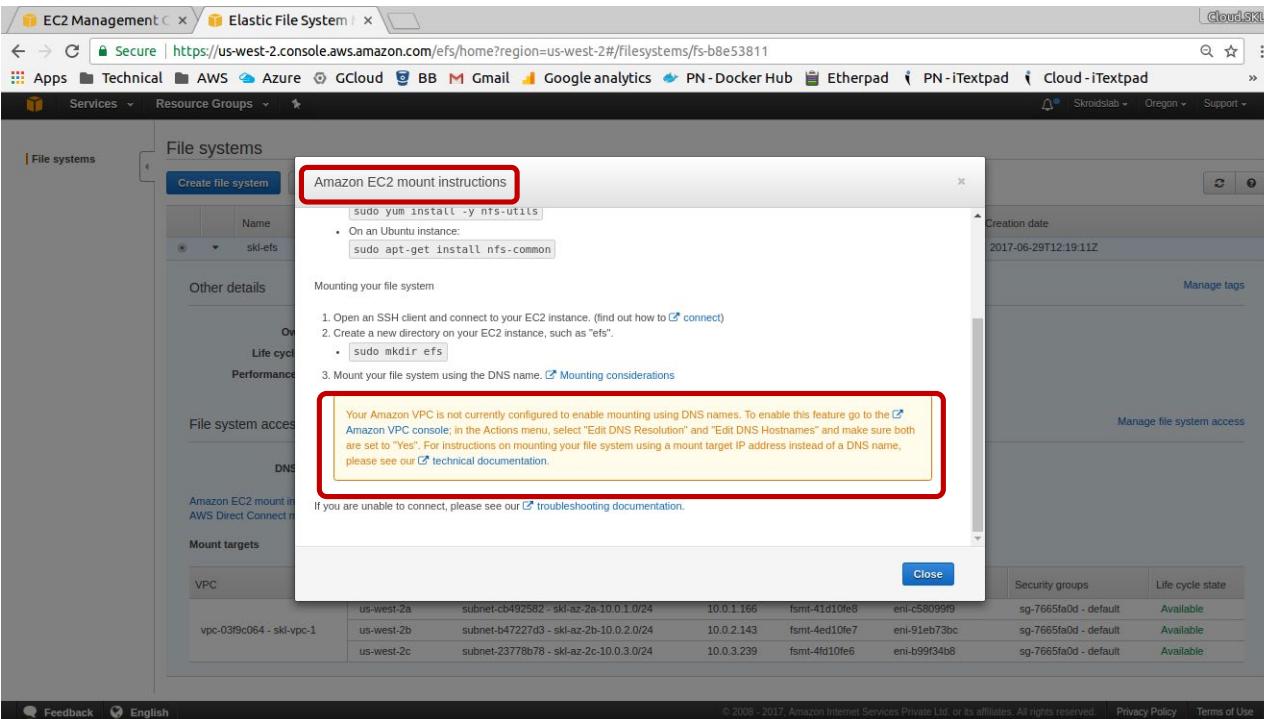
VPC	Availability Zone	Subnet	IP address	Mount target ID	Network interface ID	Security groups	Life cycle state
vpc-51238934 (default)	us-west-2a	subnet-22b21155 (default)	172.31.16.150	fsmt-e97ea840	eni-6722605d	sg-05123160 - default	Available
	us-west-2b	subnet-fa921f9f (default)	172.31.43.97	fsmt-e87ea841	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' and 'Edit DNS Hostnames'. Both dialogs have a 'DNS Resolution' section with 'Yes' and 'No' radio buttons, and a 'Save' button. The 'Edit DNS Resolution' dialog also has a 'Cancel' button.

**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

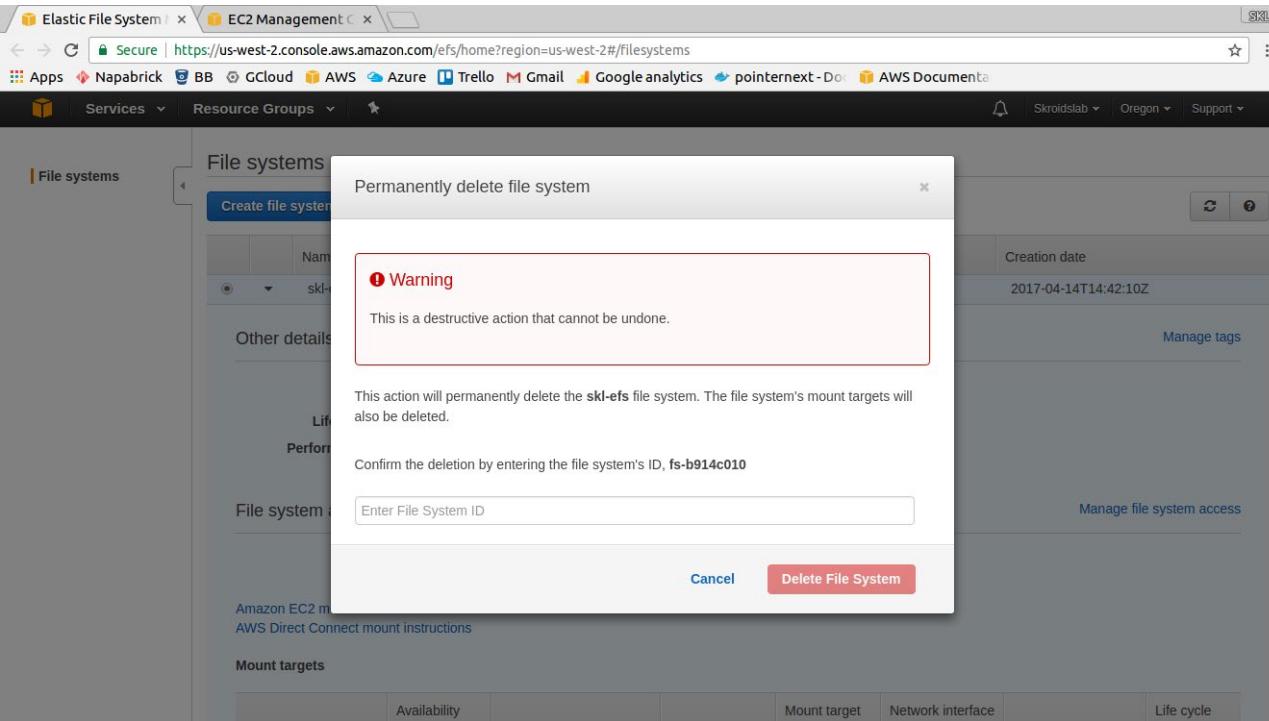
© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

**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

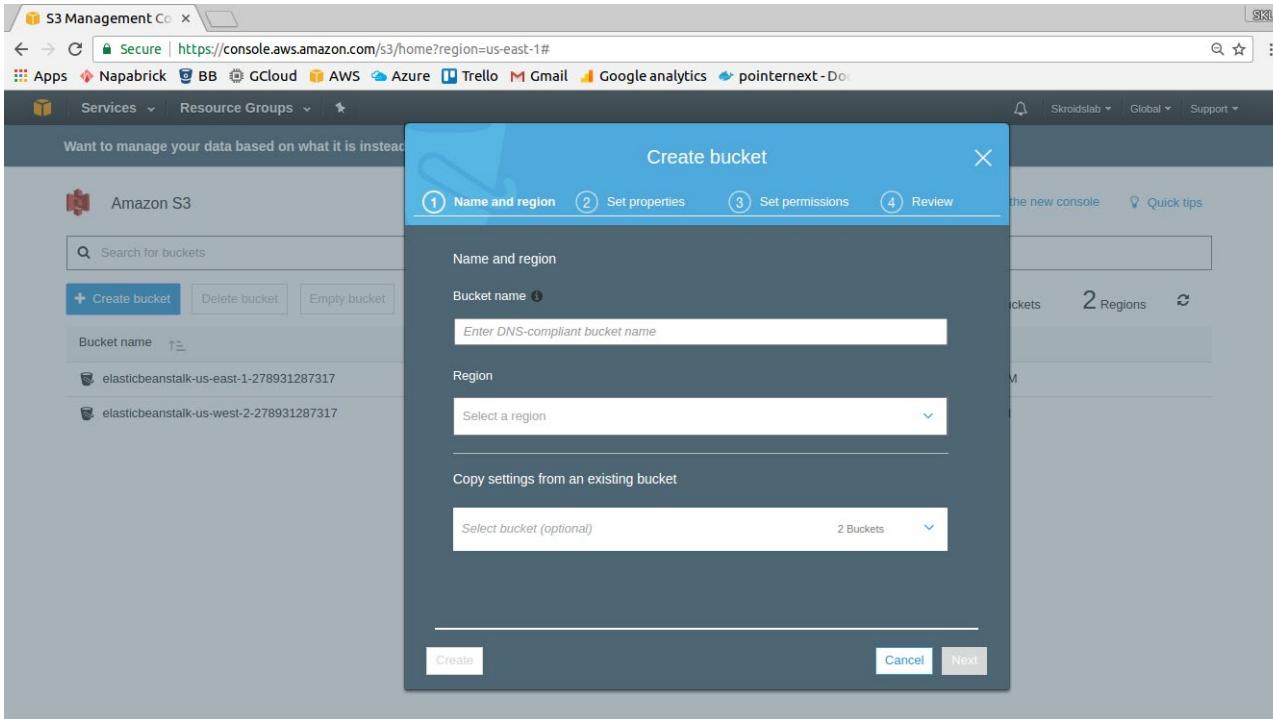
- **Consistency**
  - Read after write consistency for PUTS of new objects (insert a new object and it is immediately consistent)
  - Eventual consistency for overwrites across all the availability zones (also depends on file size)
- **Atomic operation**
  - Either new data or old data but no corruption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

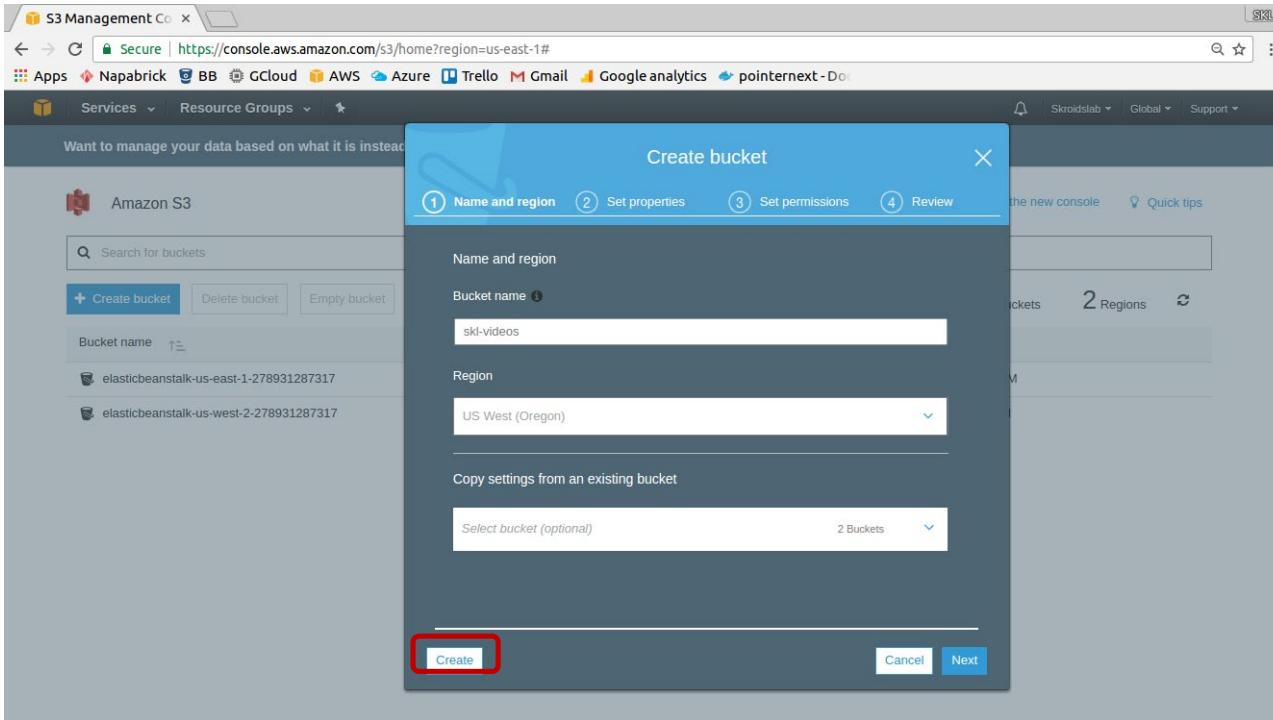
The screenshot shows the AWS S3 Management Console interface. At the top, there's a navigation bar with links to various services like Napabrick, BB, GCloud, AWS, Azure, Trello, Gmail, Google analytics, and pointernext. Below the navigation bar, a banner suggests trying S3 Object Tagging. The main area 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, pointernext, and Do. Below the navigation bar, the main header reads "Amazon S3". There are buttons for "Create bucket", "Delete bucket", and "Empty bucket". A search bar labeled "Search for buckets" is present. On the right, it shows "3 Buckets" and "2 Regions". The main table 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
skl-videos	US West (Oregon)	Apr 10, 2017 9:56:42 AM

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

# 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.

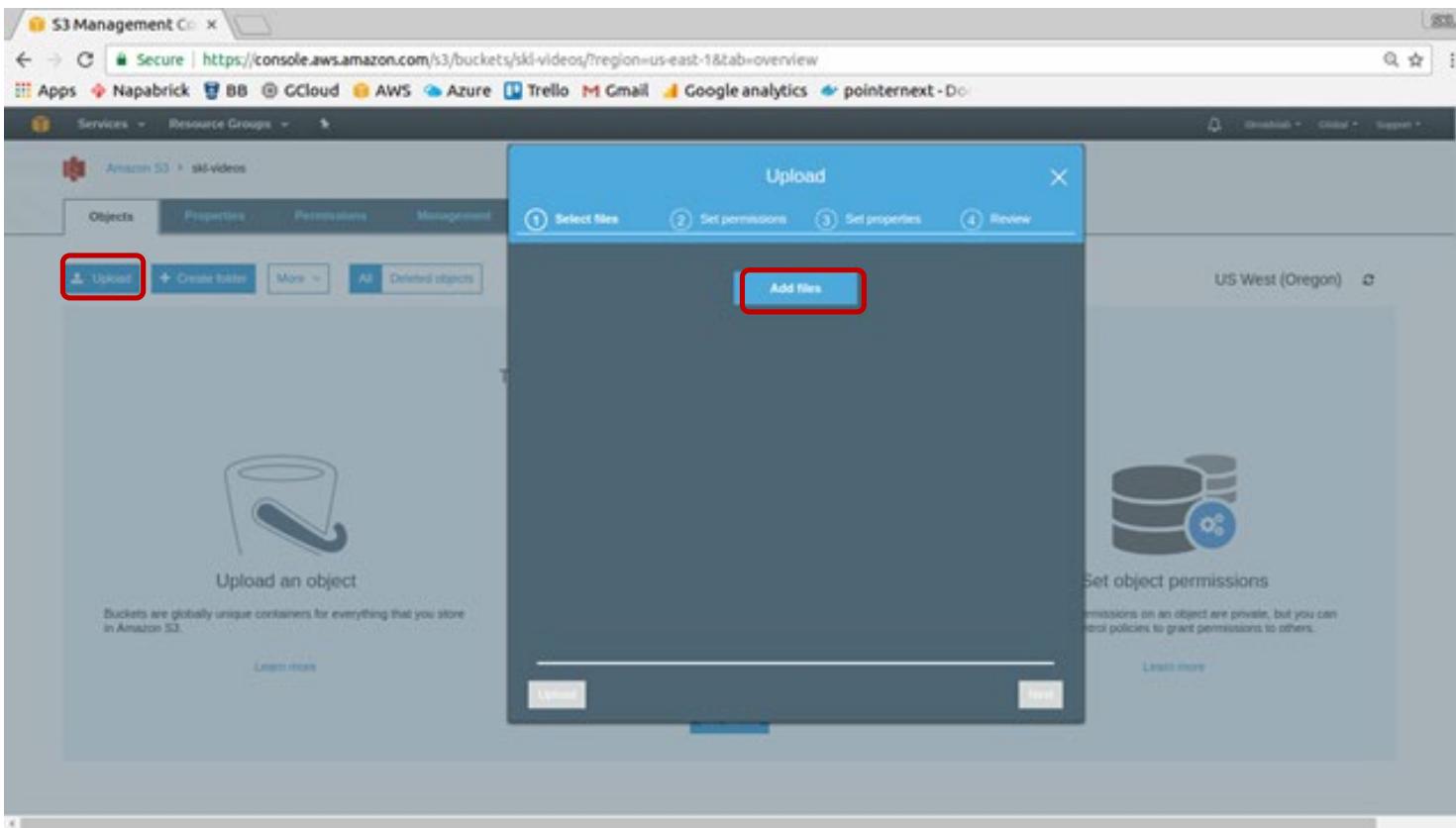
[Learn more](#) [Get started](#)

 Expire your objects

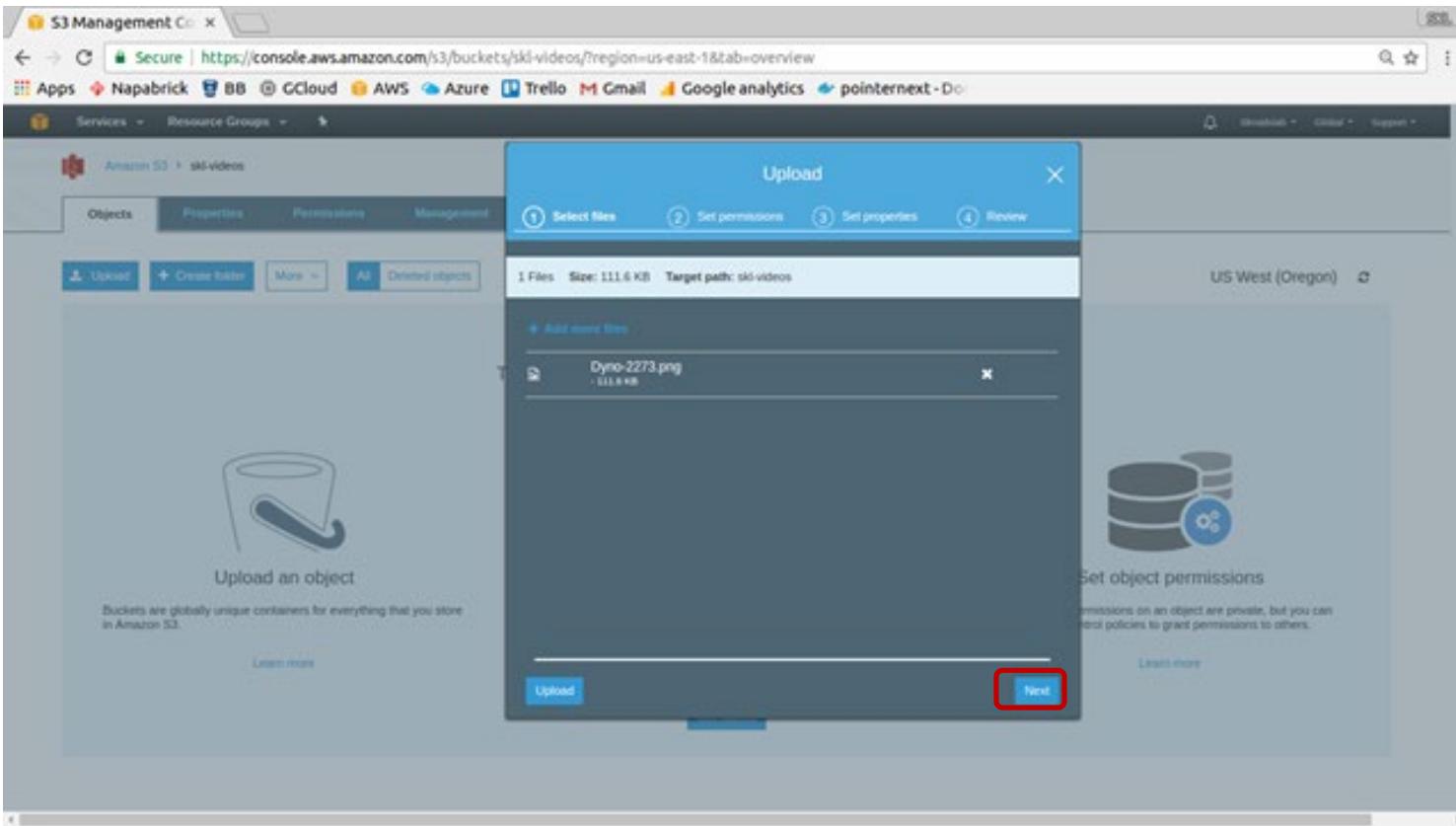
Using a lifecycle rule, you can automatically expire objects based on your retention needs or clean up incomplete multipart uploads.

[Learn more](#)

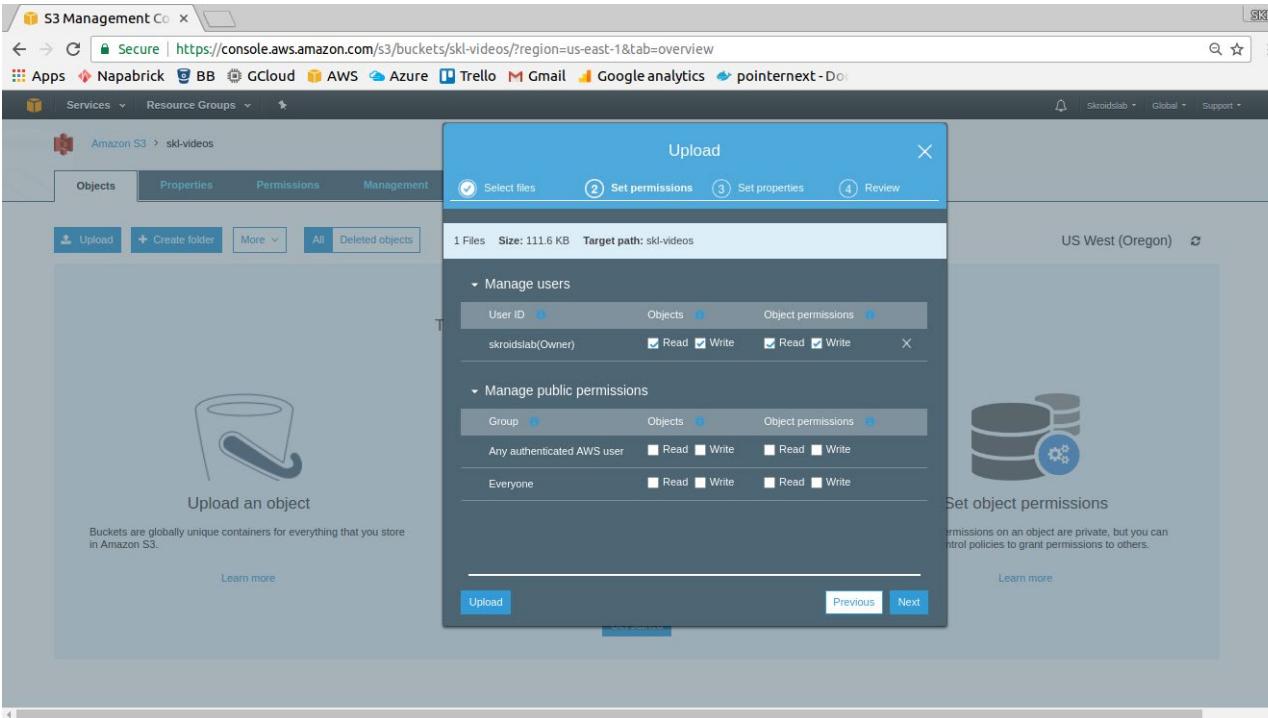
# Activity - S3



# Activity - S3

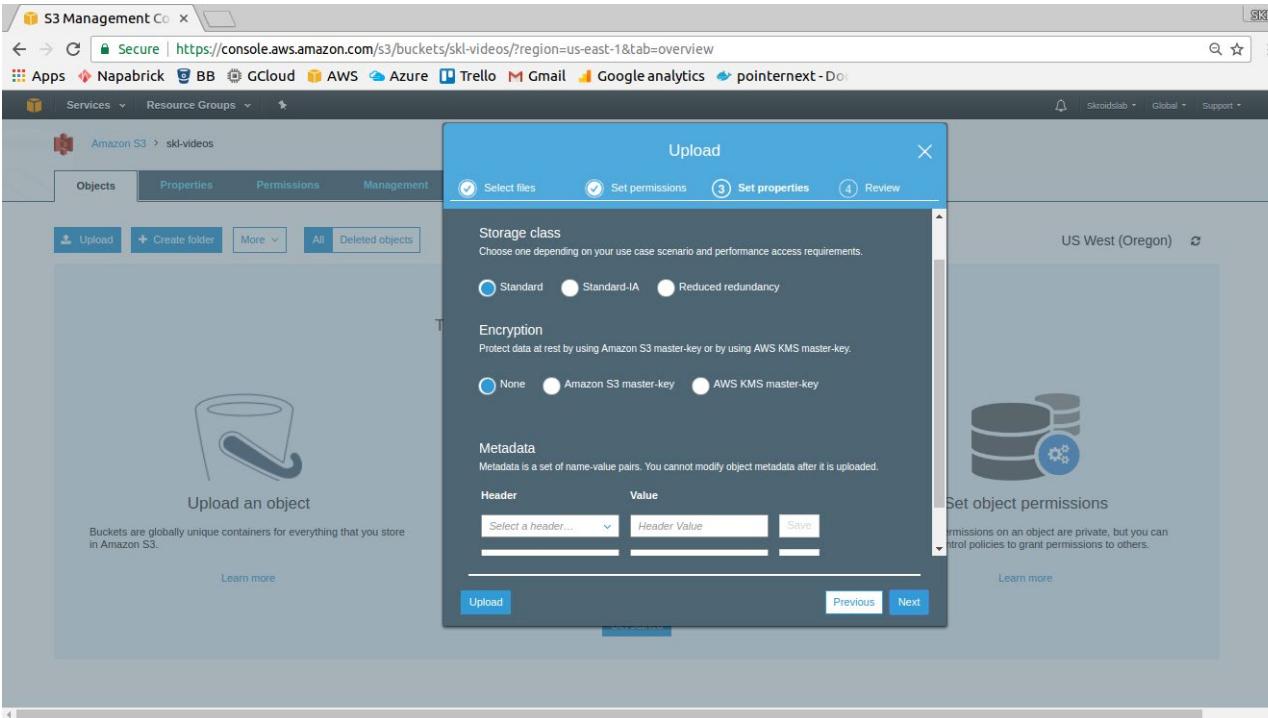


# Activity - S3



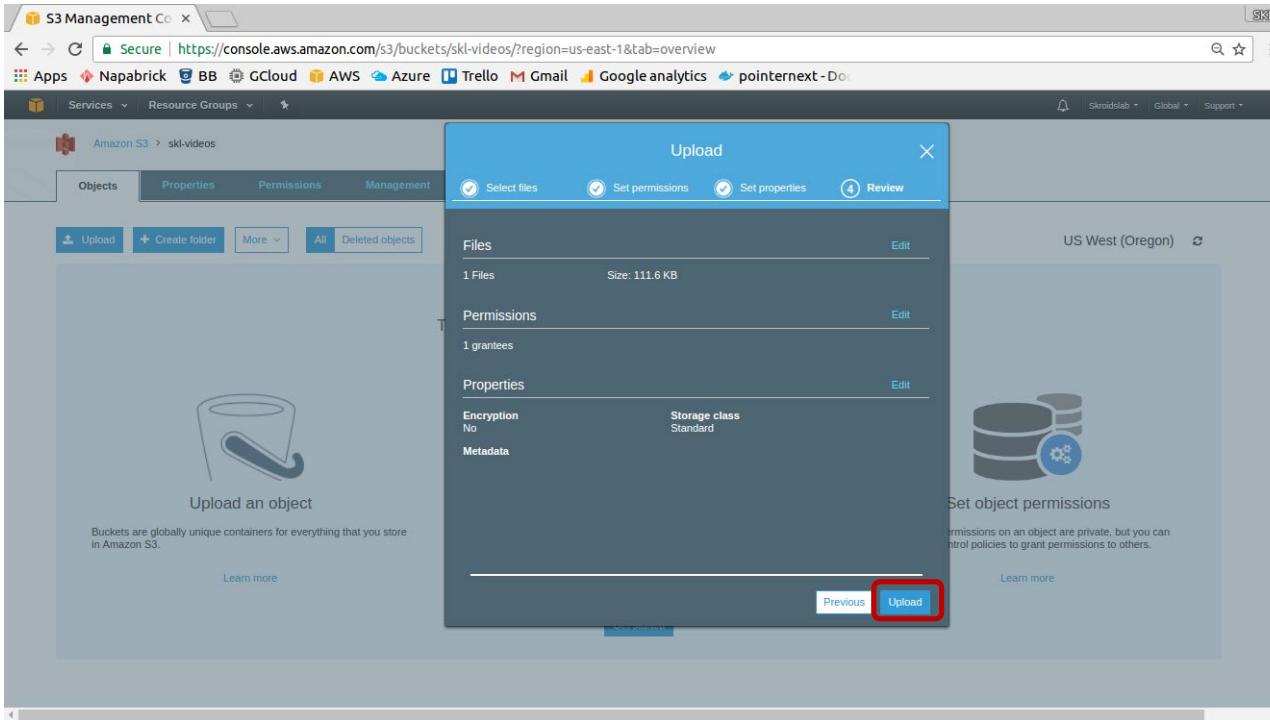
**Leave all as defaults, we will modify these later**

# 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 shows the 'Amazon S3 > ski-videos' bucket. The 'Objects' tab is selected, showing buttons for Upload, Create folder, More, All, and Deleted objects. The region is set to US West (Oregon). A message says 'This bucket is empty. Upload new objects to get started.' Below this 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. A progress bar at the bottom indicates '1 In progress', '0 Success', and '0 Error'. The status bar at the bottom shows 'Upload (1)'.

# 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.

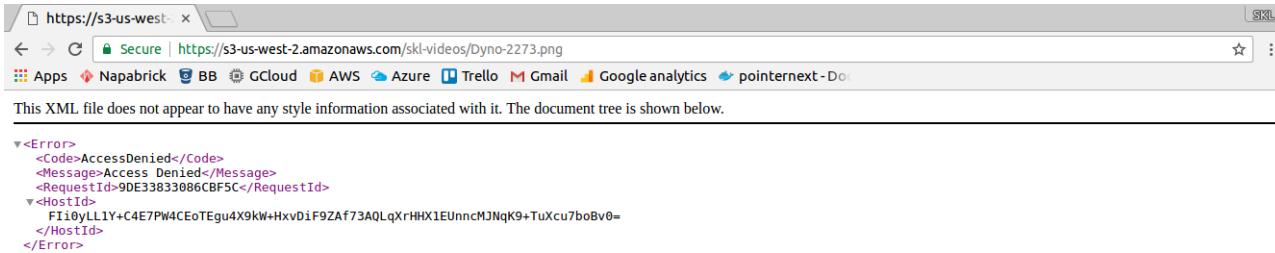
# Activity - S3

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 '26251e16640fb1fb25ebe2484ef515e7b', 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:

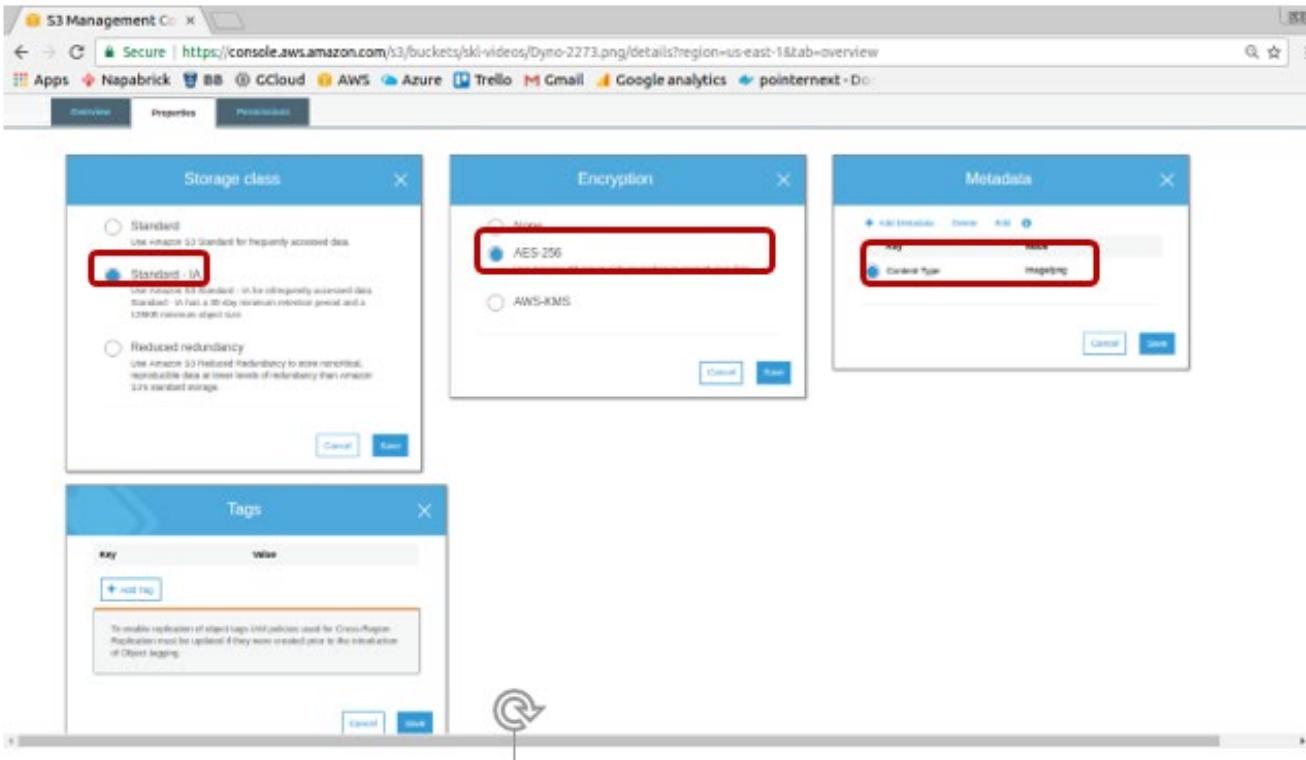
```
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>9DE33B33086CBF5C</RequestId>
  <><HostId>
    Fii0yLL1Y+C4E7PW4CEoTEgu4X9kW+HxvDif9ZAf73AQLqXrHHX1EUnncMJNqK9+TuXcu7boBv0=
  </HostId>
</Error>
```

# 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.

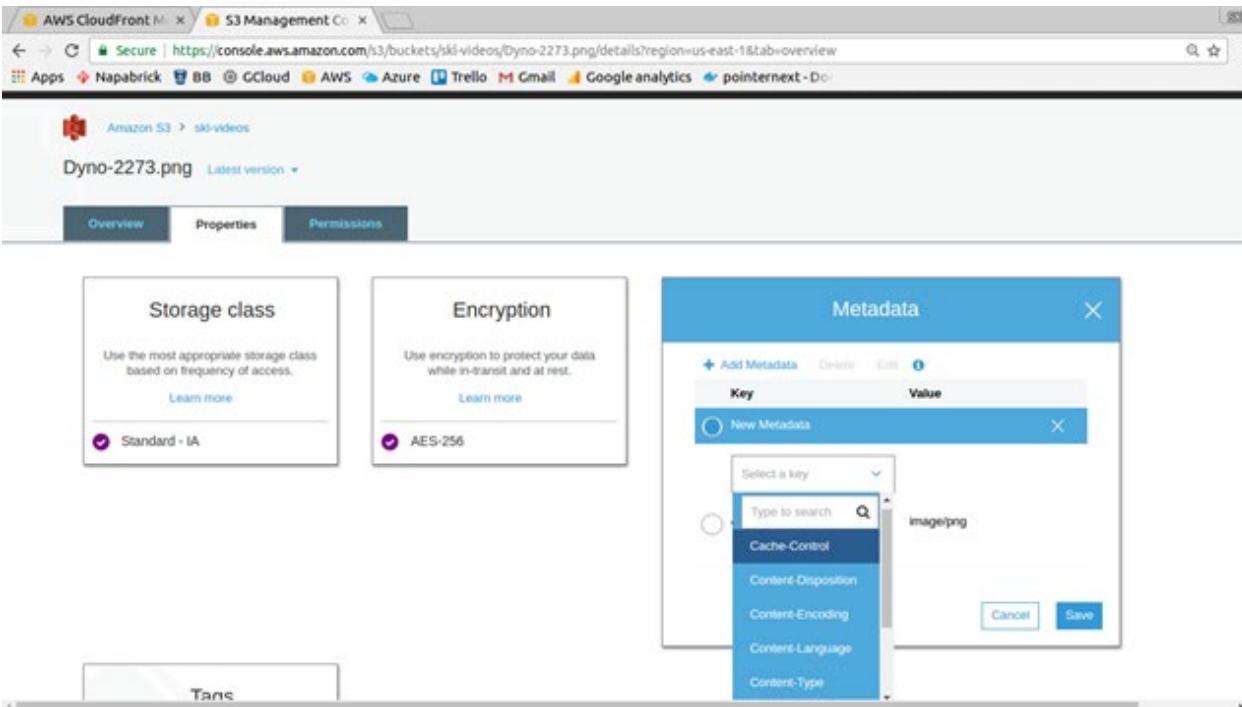
**Now access the same link and we should be able to access the object**

# 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 > skl-videos" and the object name "Dyno-2273.png". The "Latest version" is selected. A navigation bar at the top of the main content area has tabs for "Overview" (which is active), "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:

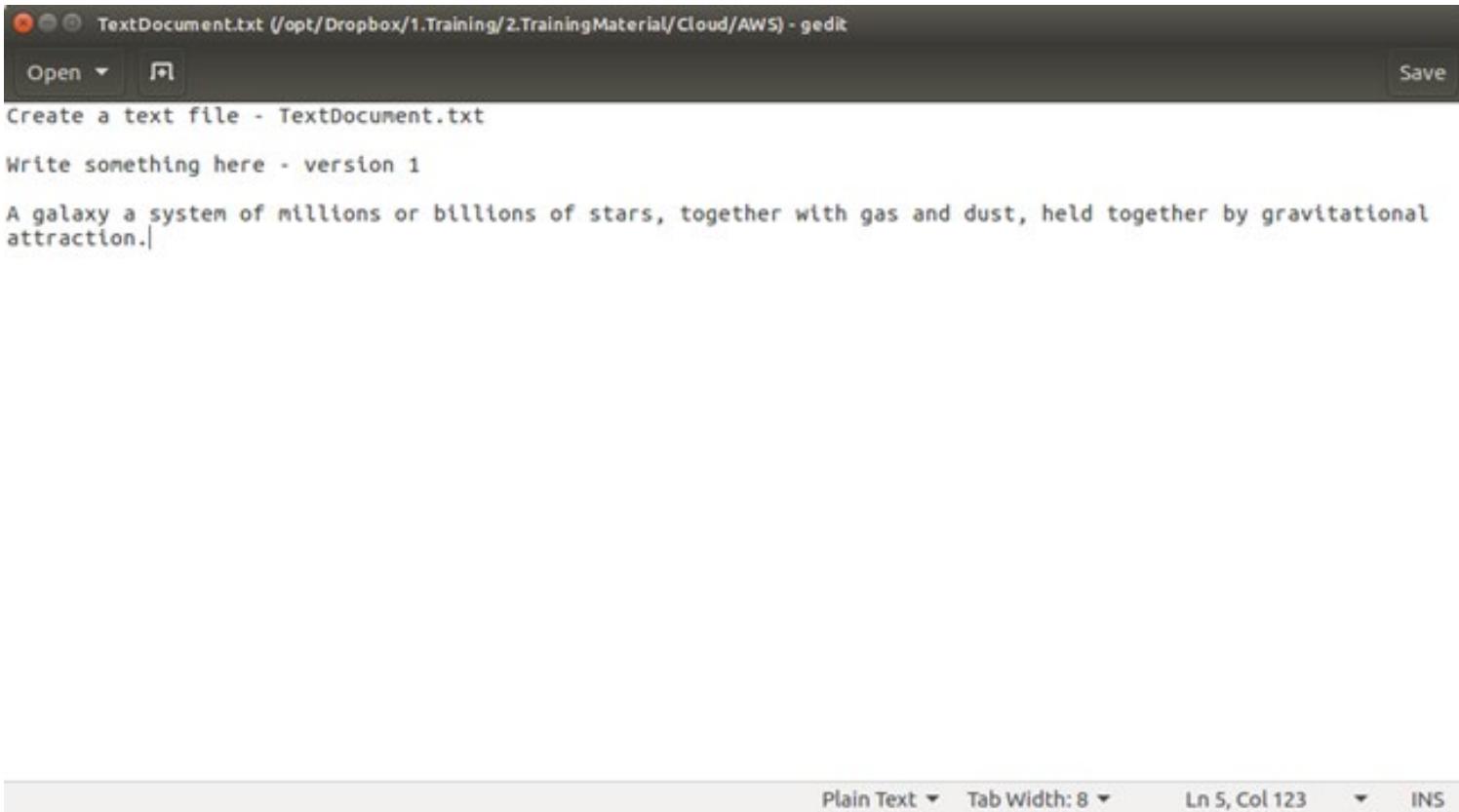
- This bucket will have public access:** Everyone will have access to one or all of the following: list objects, write objects, read and write permissions.
- Access to the objects:**  List objects (highlighted with a red box)
- Access to this bucket's ACL:**  Read bucket permissions (highlighted with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

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

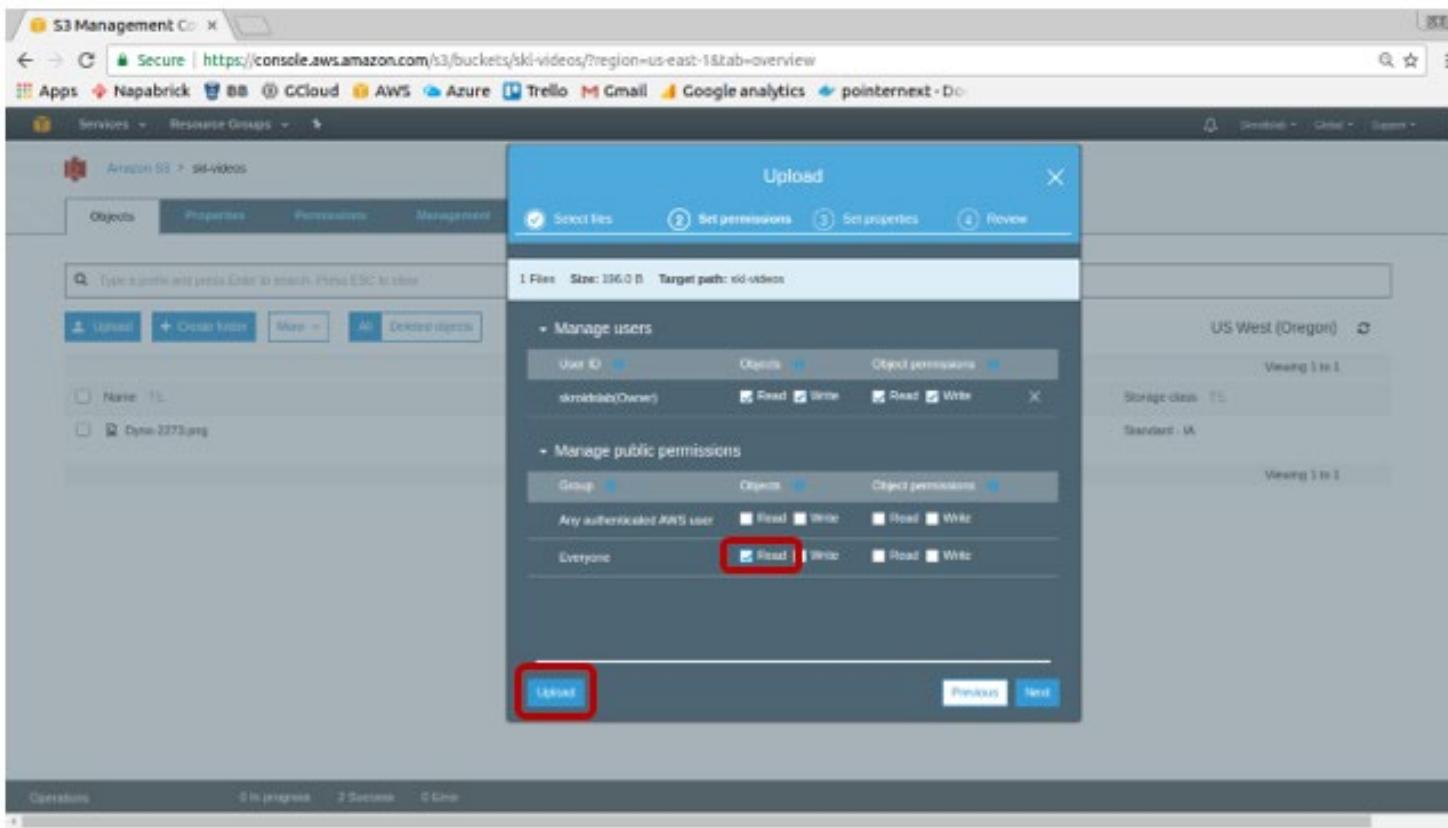
- Owner access:** skroldslab has Yes for List objects, Write objects, and Read bucket permissions.
- Access for other AWS accounts:** An account named 'skroldslab' is listed with Yes for List objects, Write objects, and Read bucket permissions.
- Public access:** The 'Everyone' group is selected (highlighted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

**Make the bucket public**

# Activity - S3 versioning



# 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 AWS navigation links like 'Open', 'Download', 'Download as', and 'Make public'.

Owner: skl-videoslab

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

Etag: 95c3400e58713433946cf8f8d6511be

Storage class: Standard

Server side encryption: None

Size: 196

Version ID: fUvc7y5aDvYpxt2kefiaXevrA09g

Link: <https://s3.us-east-1.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

Owner  
sridharlab

Last activity  
Apr 10, 2017 11:09:05 AM

Etag  
6d7781a6bf155be13c7eab0fc04761f

Storage class  
Standard

Server side encryption  
AES256

**Size**  
43B

Version ID  
YzgQ0juz2nwOJxDQwCYIAJ5D95Wh

Link  
<https://s3.us-east-2.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:

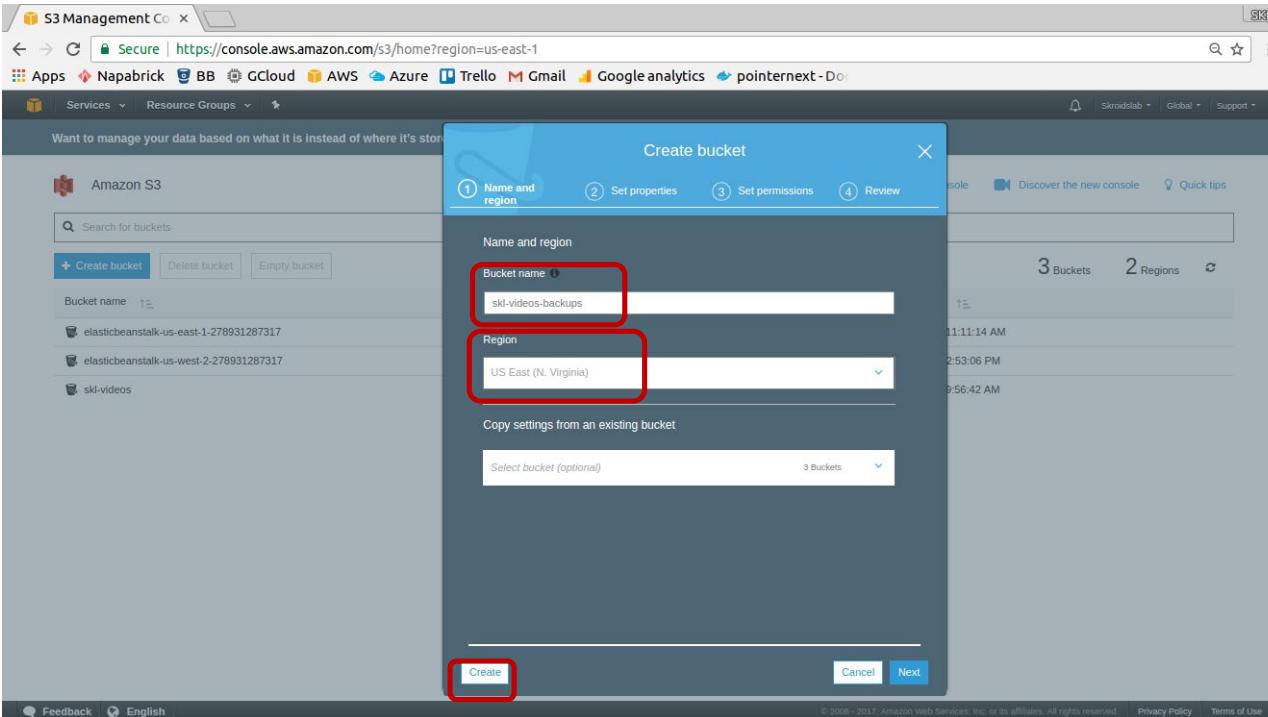
Name	Last modified	Size	Storage class
Dyno-2273.png	Apr 10, 2017 10:44:47 AM	111.6 KB	Standard - IA
TextDocument.txt	Apr 10, 2017 11:09:09 AM	439.0 B	Standard

**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



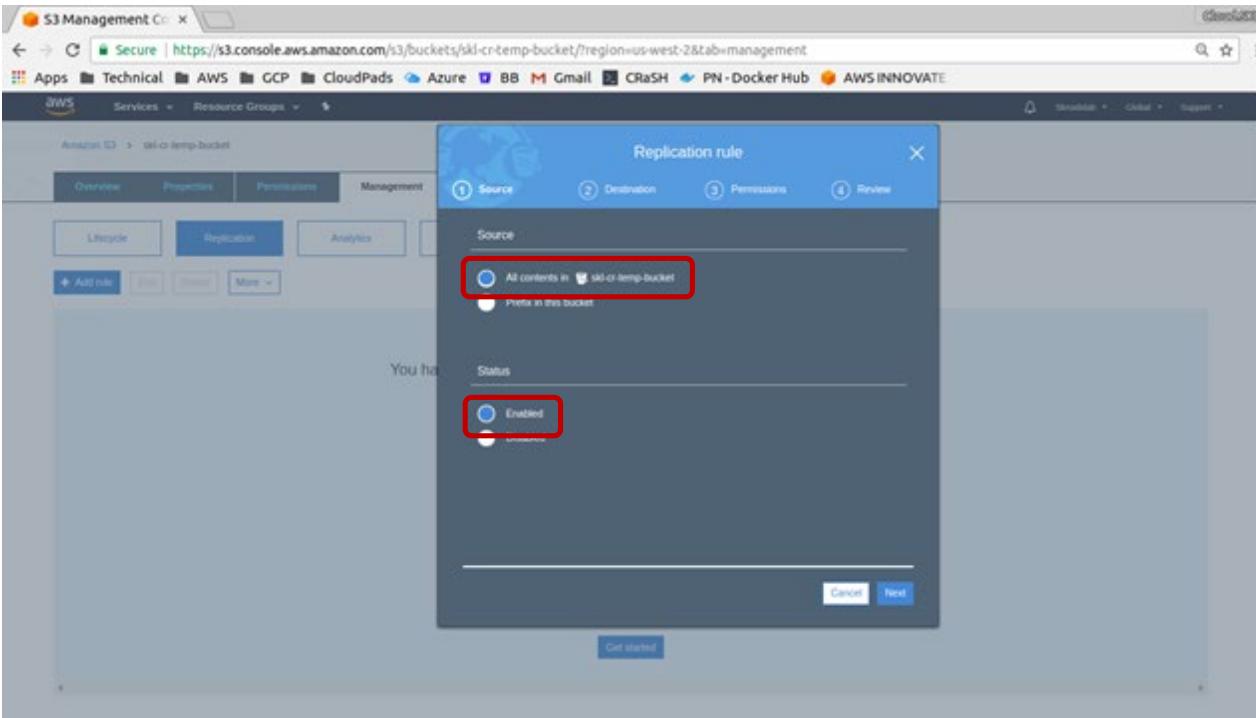
**Create a new bucket in the east coast, go to properties and enable versioning**

# 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.

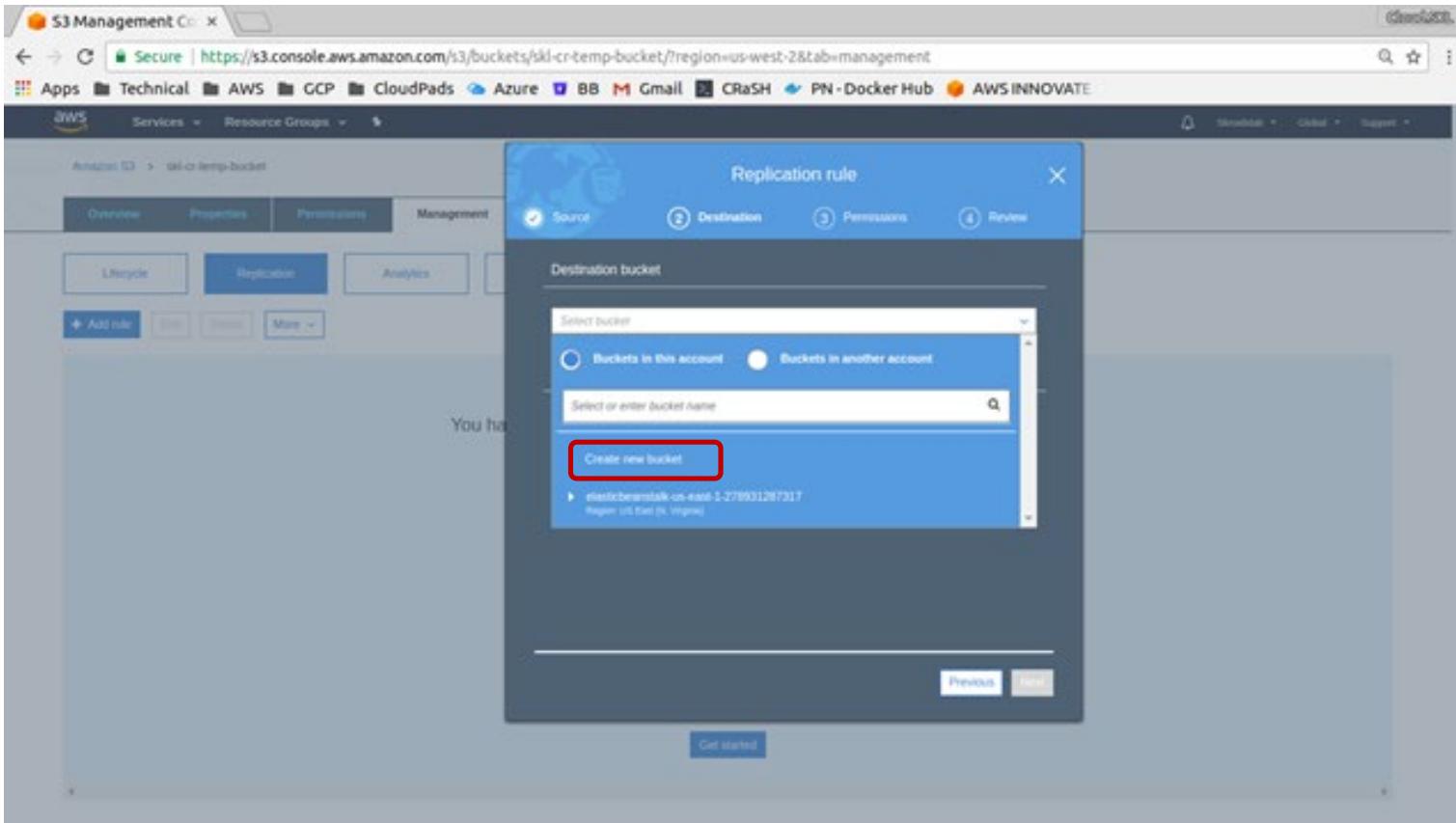
Both do the same

# Activity - S3 Cross region replica

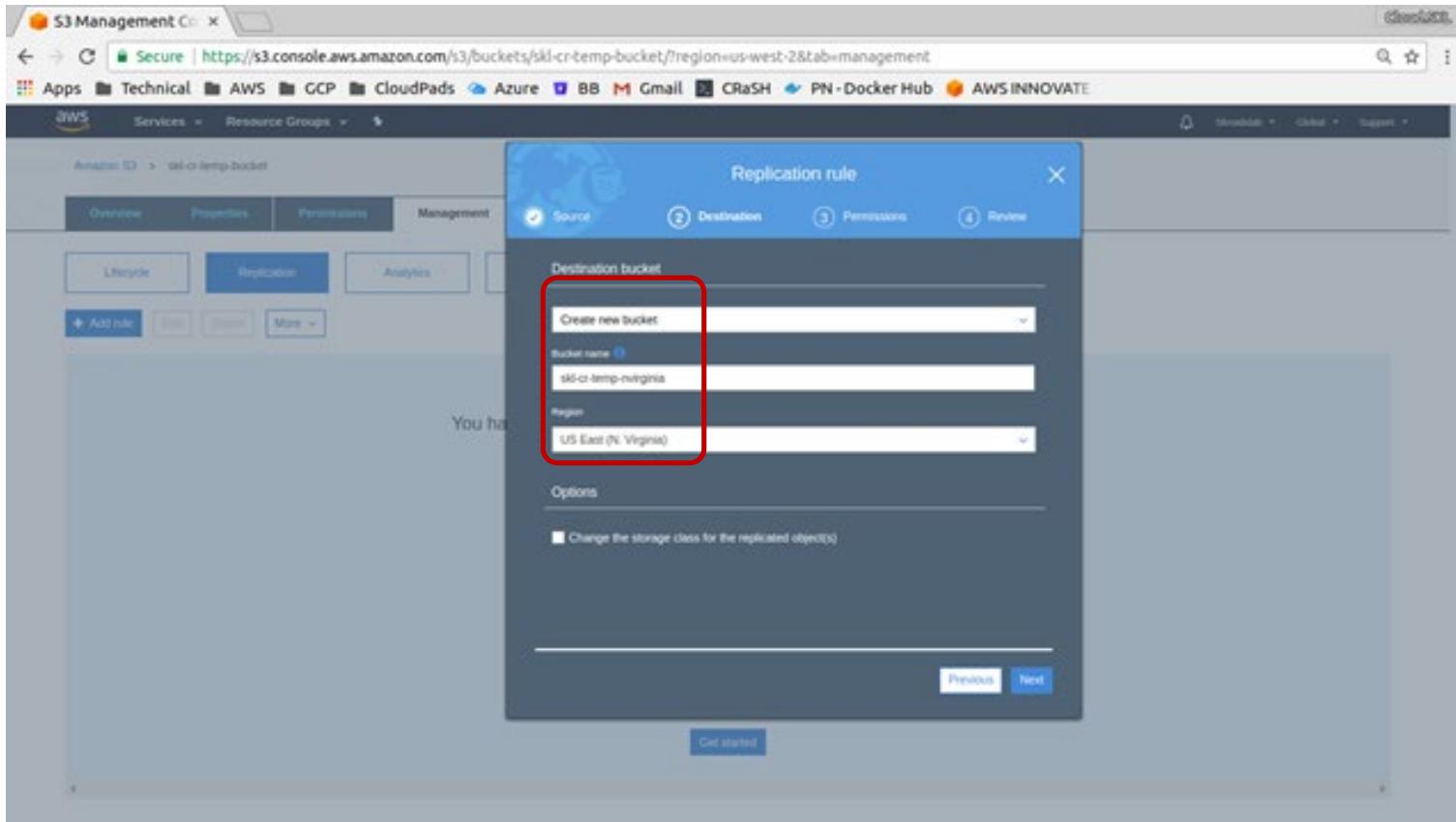


**Existing objects will not be replicated! Upload another version of the galaxy txt file and you will find ALL previous versions will be replicated. Multi region replication and replication chaining is not supported.**

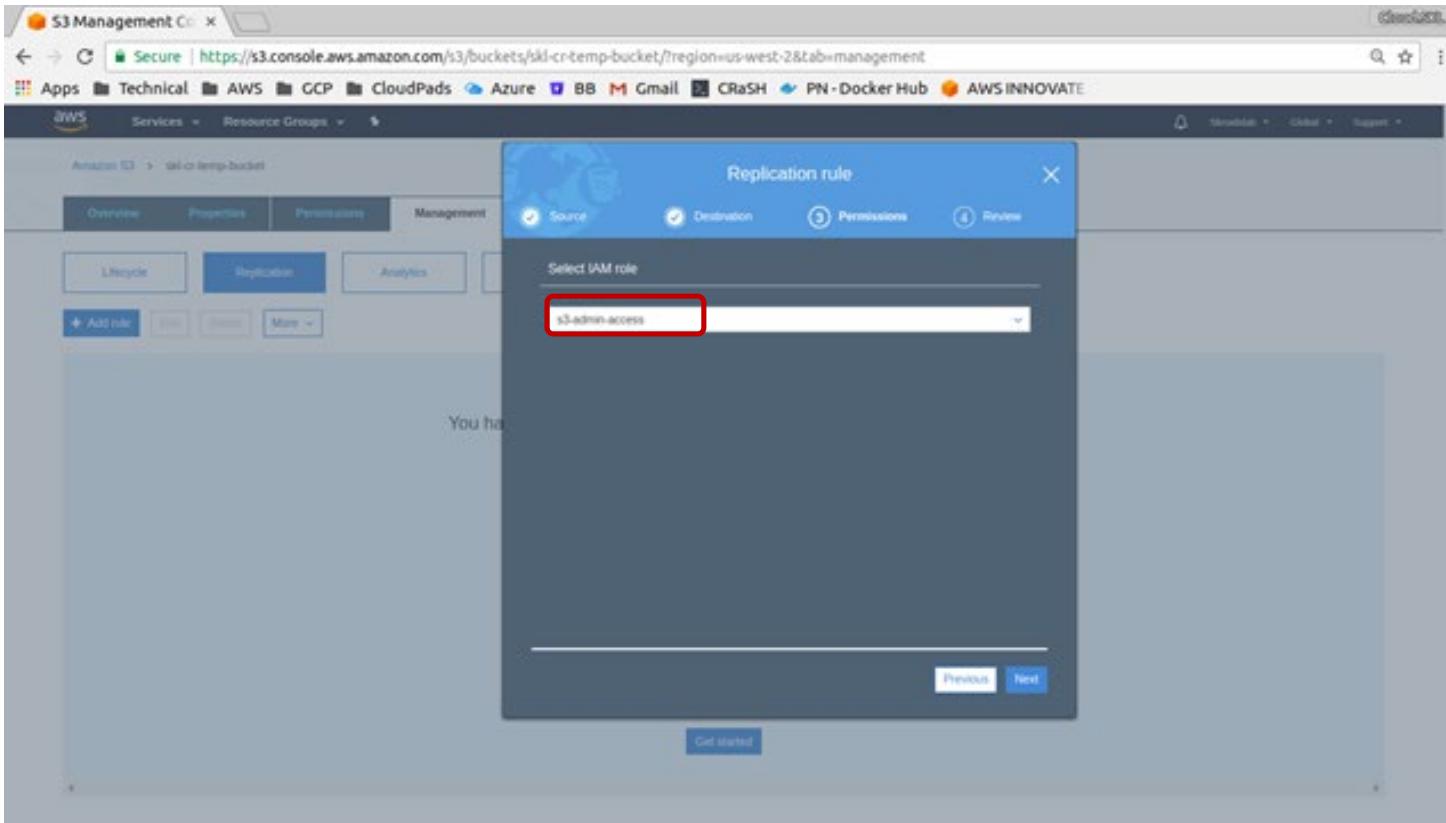
# Activity - S3 Cross region replica



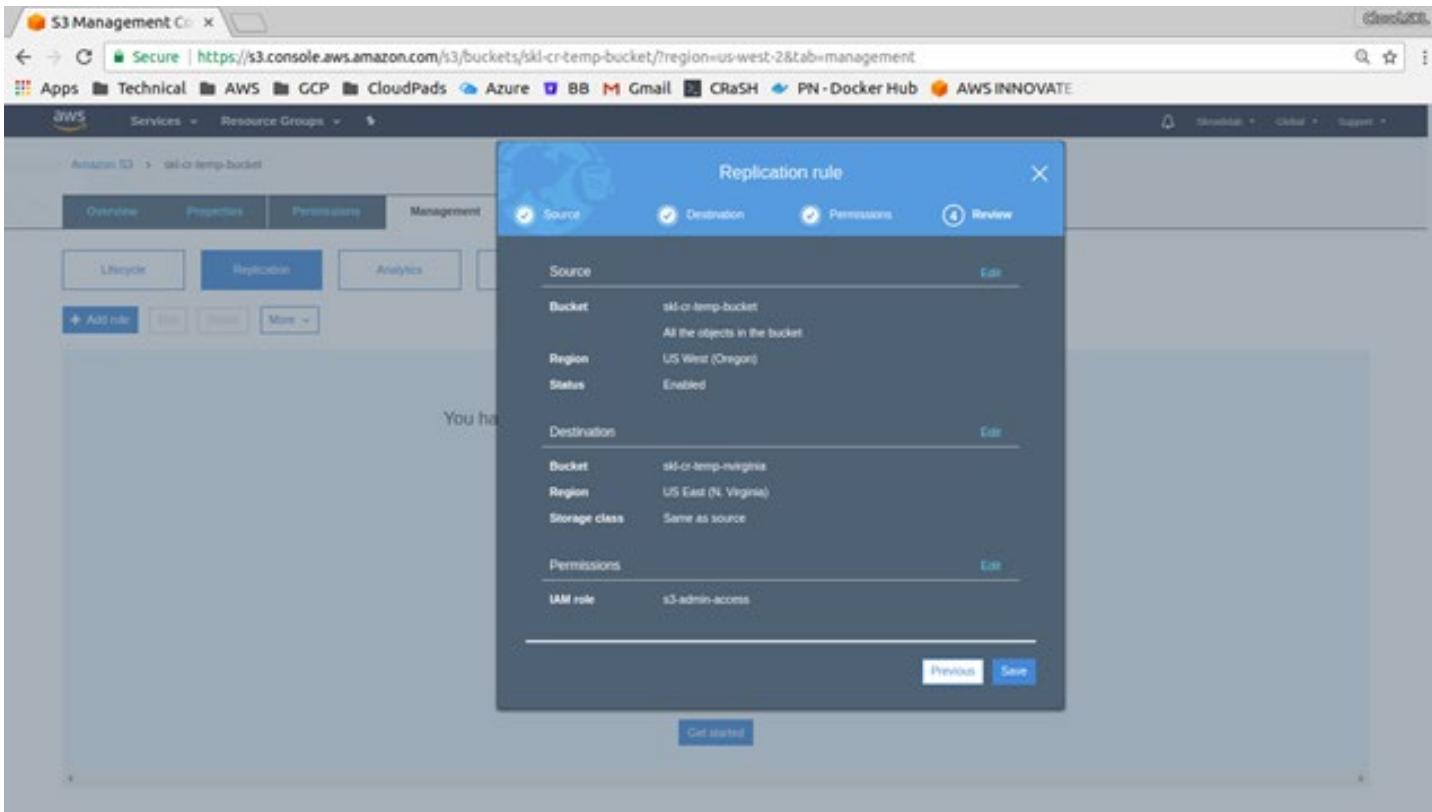
# Activity - S3 Cross region replica



# 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 labeled '+ Add lifecycle rule' which is also highlighted with a red box. Below this, a message states: 'There is no lifecycle rule applied to this bucket. Here is how to get started.' Three cards provide information on managing objects:

- 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 'Edit'.
- Automate transition to tiered storage**: Shows an icon of three stacked cylinders with gears. Text: 'Lifecycle rules enable you to automatically transition objects to the Standard - IA and/or the Amazon Glacier storage class.' Buttons: 'Learn more' and 'Edit'.
- 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 'Edit'.

At the bottom, a summary bar shows: Operations (0 In progress, 1 Success, 1 Error).

# Activity - S3 lifecycle

The screenshot shows the AWS S3 Management Console for the 'ski-videos' bucket. A modal window titled 'Lifecycle rule' is open, showing the first step: 'Name and scope'. The rule name is set to 'Recycle-1'. Below it, there's a section for 'Add filter to limit scope to prefix/tag' with a placeholder 'Type to add prefix/tag filter'. At the bottom of the modal are 'Cancel' and 'Next' buttons. The background shows the S3 console interface with tabs for Objects, Properties, Permissions, and Management, and a 'Lifecycle' tab selected. To the right of the modal, there's a large icon of a trash can labeled 'Expire your objects'.

# 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 contains the following configuration:

- Configure transition**:
  - Current version
  - Previous versions
- For current version of objects**:
  - Object creation: Transition to Standard-IA after 30 days
  - Days after object creation: 30
  - Transition to Amazon Glacier after 60 days
  - Days after object creation: 60
- For previous versions of objects**: You don't have any transitions set up for previous versions of objects.

At the bottom of the modal are 'Previous' and 'Next' buttons. The background of the console shows a large trash can icon and the text 'Expire your objects'.

# 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 modal contains the following configuration:

- 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 of the modal states: "You cannot enable clean up expired object delete markers if you enable Expiration."

Below the modal, the main S3 Management interface shows a summary of operations: 0 In progress, 1 Success, 1 Error. It also includes links for Feedback and 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 indicators: 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/ski-videos?region=us-east-1&tab=management>. The top navigation bar includes links for Apps (Napabrick, BB, GCloud, AWS, Azure, Trello, Gmail, Google analytics, pointernext), Services (selected), Resource Groups, and various AWS services like Lambda, CloudWatch, and CloudFront.

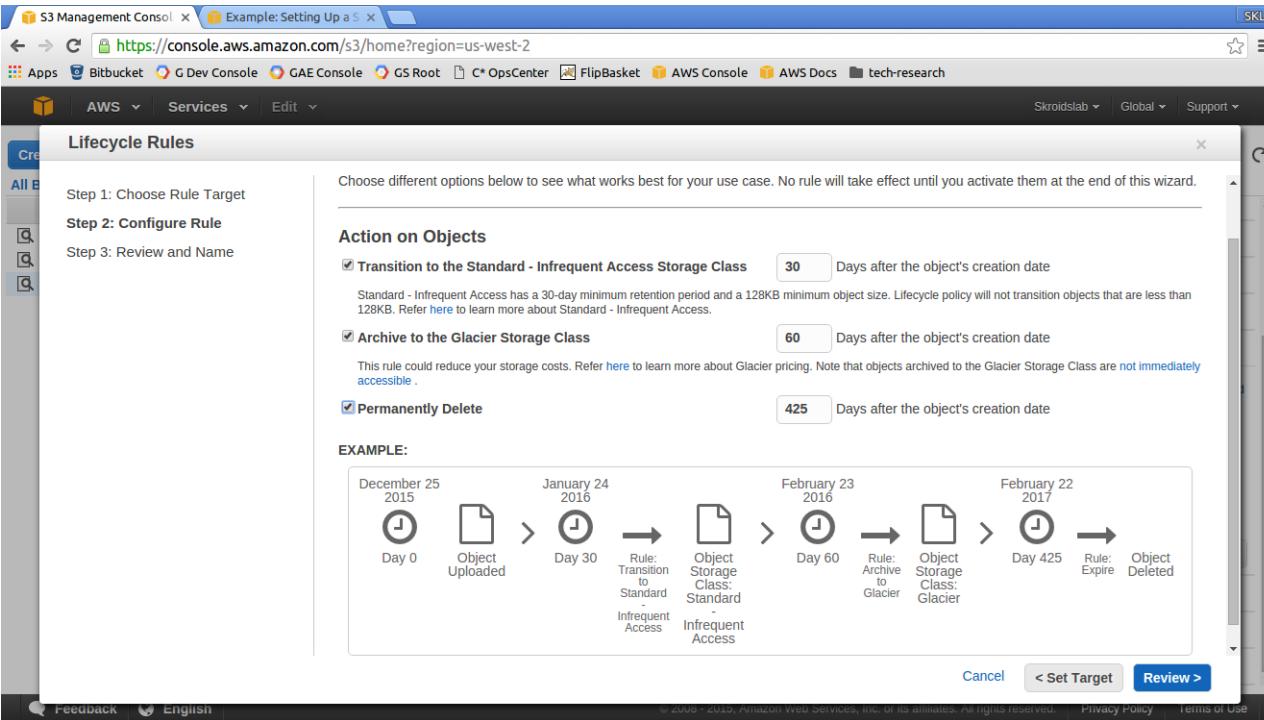
The main content area shows the 'Management' tab selected under the 'Lifecycle' section. There are tabs for Objects, Properties, Permissions, and Management. Below these are tabs for Lifecycle, Analytics, Metrics, and Inventory. A button to '+ Add Lifecycle rule' is visible.

A table displays a single lifecycle rule named 'Recycle-1'. The rule is applied to the 'Whole bucket' and defines transitions for both current and previous versions. For the current version, it moves from Standard-IA to Amazon Glacier and then to Expire. For previous versions, it moves from Standard-IA to Amazon Glacier and then to Permanent Delete.

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 / Permanent Delete

At the bottom, a progress bar indicates 0 In progress, 1 Success, and 1 Error operations.

# 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**

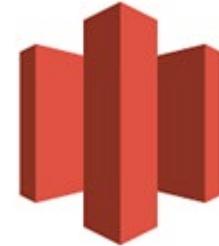
Transition to the Standard - Infrequent Access Storage Class  Days after becoming a previous version  
Standard - Infrequent Access has a 30-day minimum retention period and a 128KB minimum object size. Lifecycle policy will not transition objects that are less than 128KB. Refer [here](#) to learn more 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 search bar labeled 'Filter By Name:' is present. The main table has columns: 'Name', 'Inventory Last Updated', 'Size (as of last inventory)', and '# of Archives (as of last inventory)'. One row is visible: 'SKLVideosArchiva', 'Not updated yet', '...', and '...'. Below the table, a modal window is open for the 'SKLVideosArchiva' vault. It shows tabs for 'Details', 'Notification', 'Permissions', 'Vault Lock', and 'Tags', with 'Details' selected. Under 'Details', information includes: 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, and 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: ...'.

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

Vault Name: SKLVideosArchiva

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

Vault Details as of the last inventory update:

Size: ...

# 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 policy options, 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](#)".

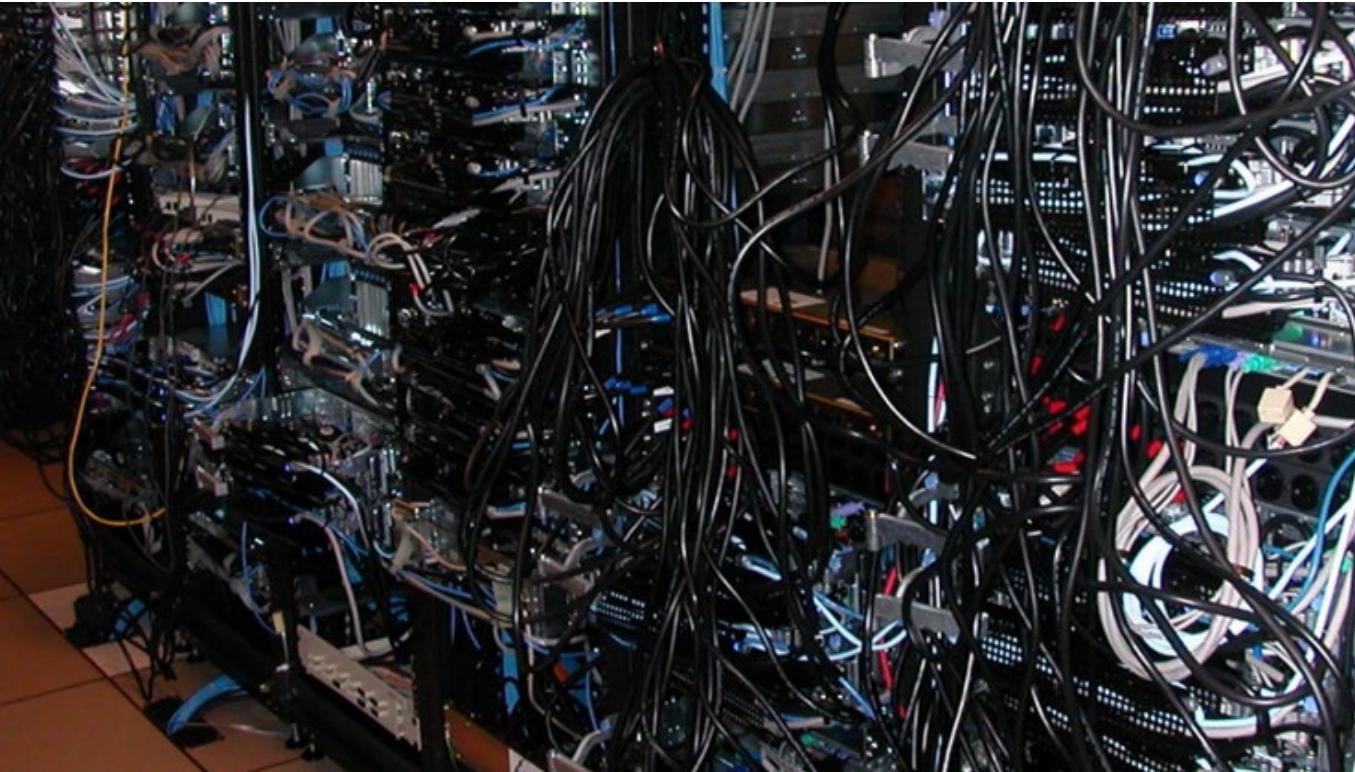
At the bottom right of the dialog box are "Cancel" and "Save" buttons.



# Networking

VPC

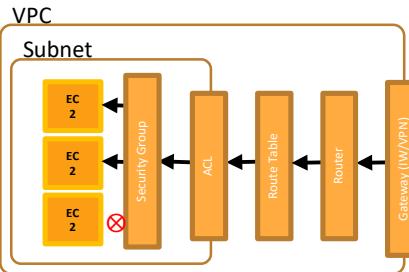
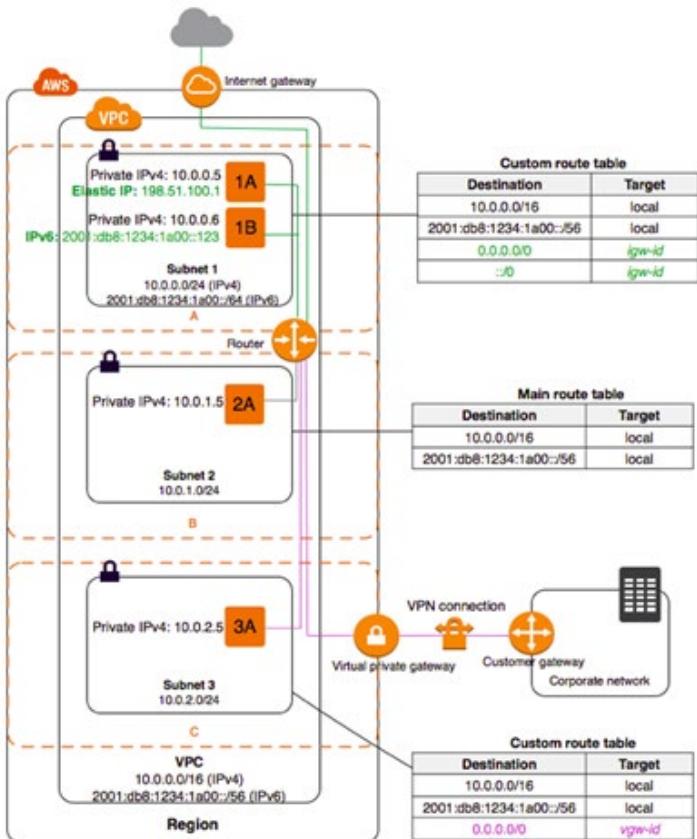
Let's talk about this ...



# 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

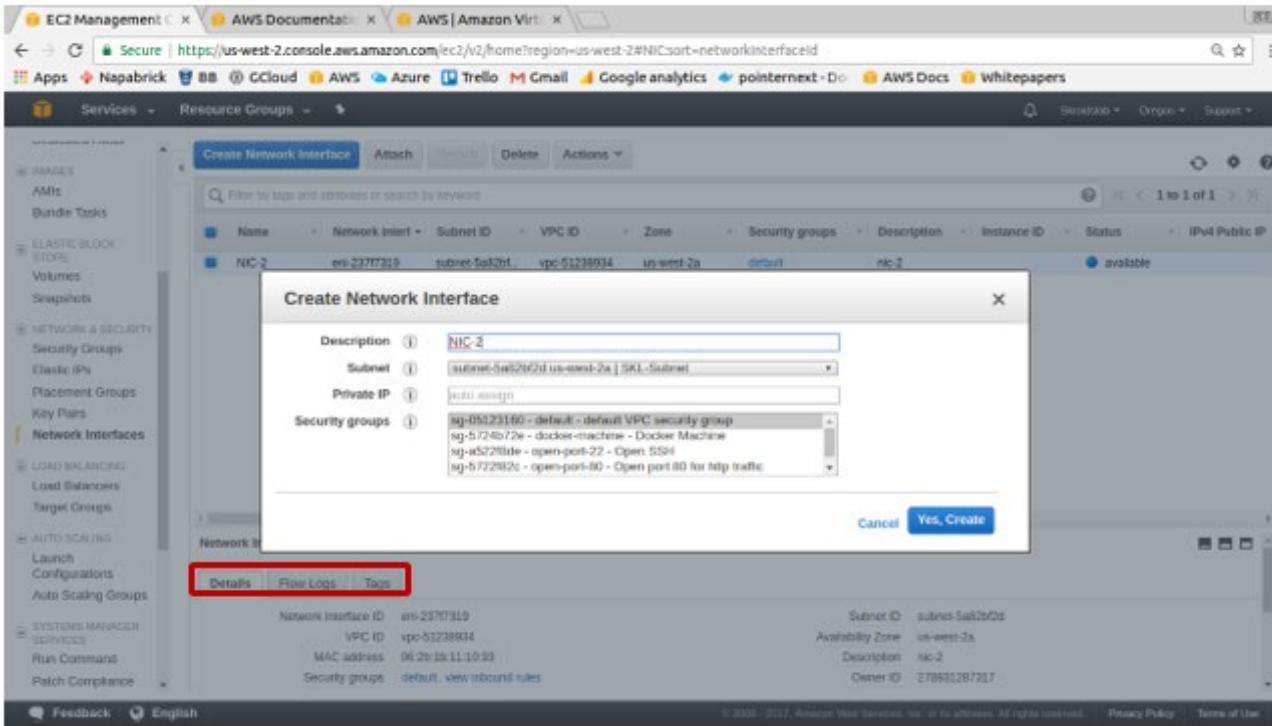


- AWS provides two features that you can use to increase security in your VPC**
  - Security groups control inbound and outbound traffic for your instances (stateful)**
  - Network ACLs control inbound and outbound traffic for your subnets (stateless)**
- Every subnet that you create is automatically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

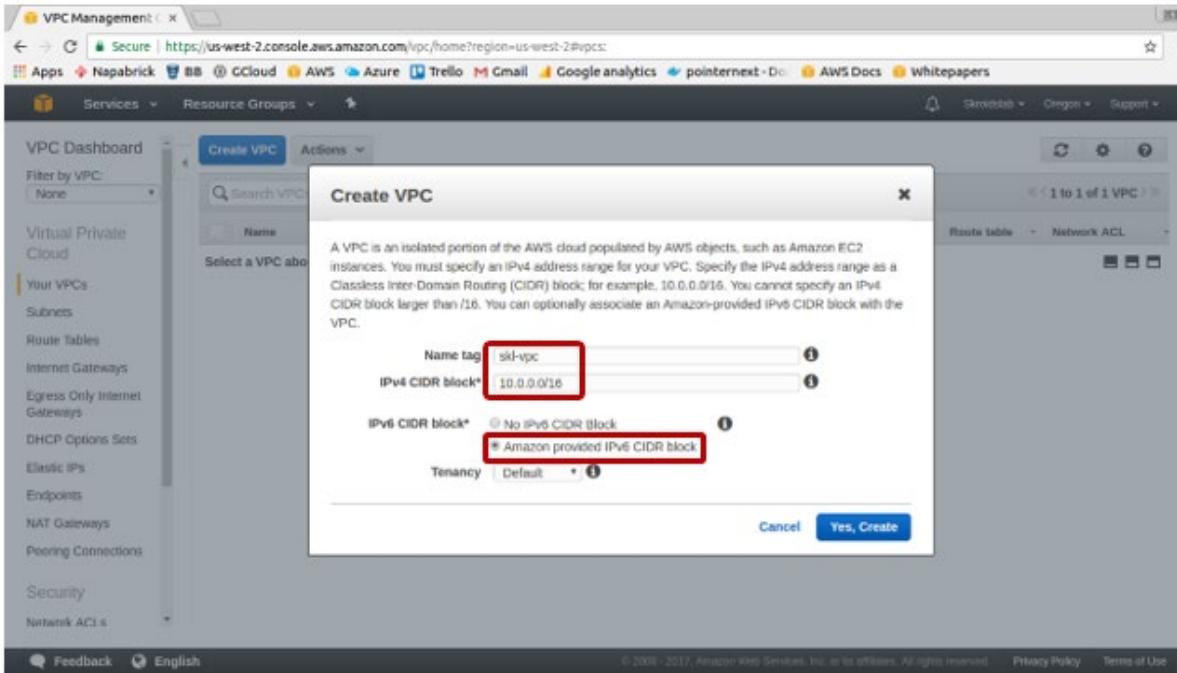
**Service Health**

Current Status	Details
<span style="color: green;">●</span> Amazon VPC - US West (Oregon)	Service is operating normally
<span style="color: green;">●</span> Amazon EC2 - US West (Oregon)	Service is operating normally

**Additional Information**

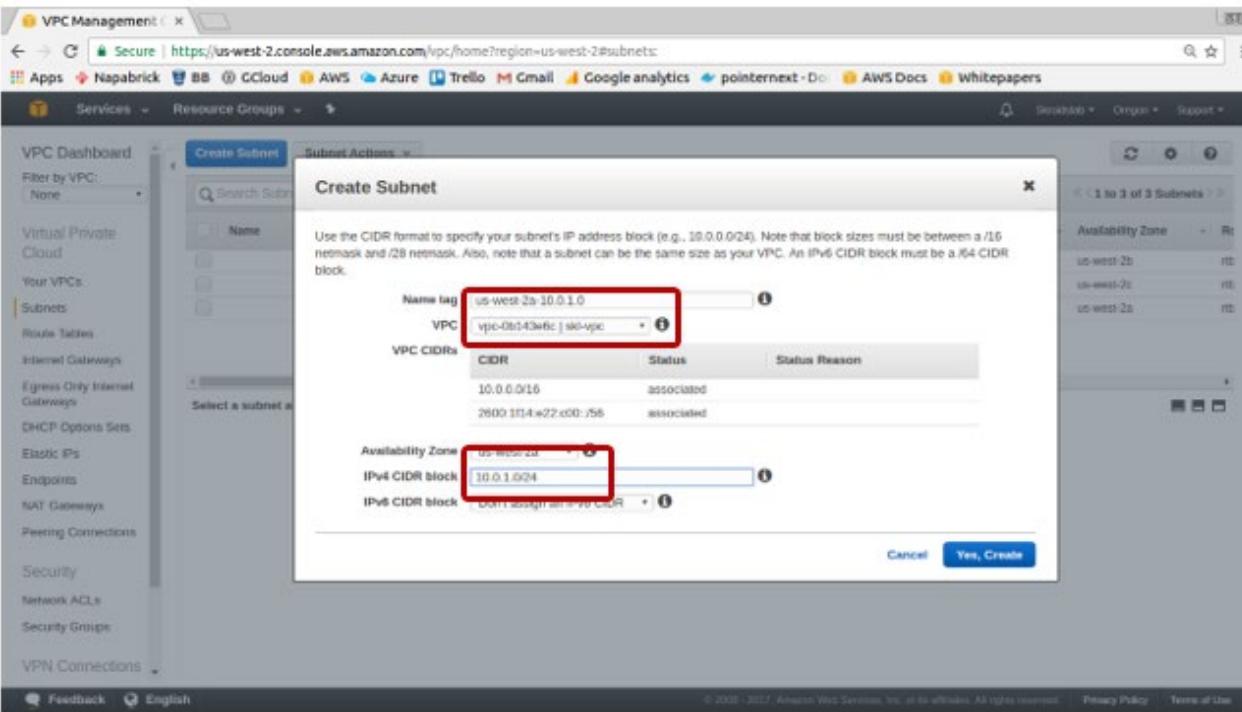
- VPC Documentation
- All VPC Resources
- Forum
- Report an issue

# 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:

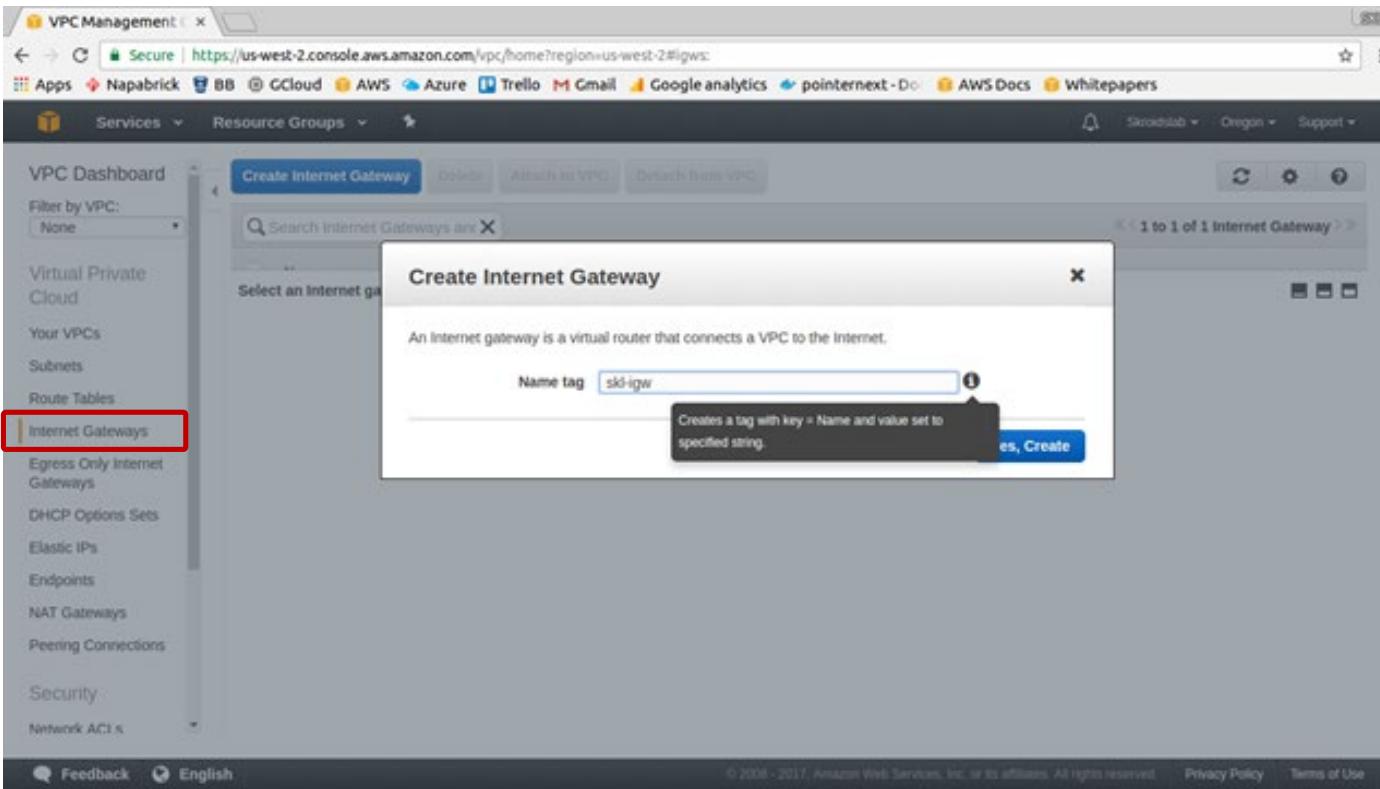
Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Region
us-west-2b-10.0.2.0	subnet-58d99f3f	available	vpc-0b143e6c   sk8-vpc	10.0.2.0/24	251		us-west-2b	US West (Oregon)
us-west-2a-10.0.1.0	subnet-28990181	available	vpc-0b143e6c   sk8-vpc	10.0.1.0/24	251		us-west-2a	US West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

Below the table, details for the selected subnet (`subnet-58d99f3f | us-west-2b-10.0.2.0`) are shown:

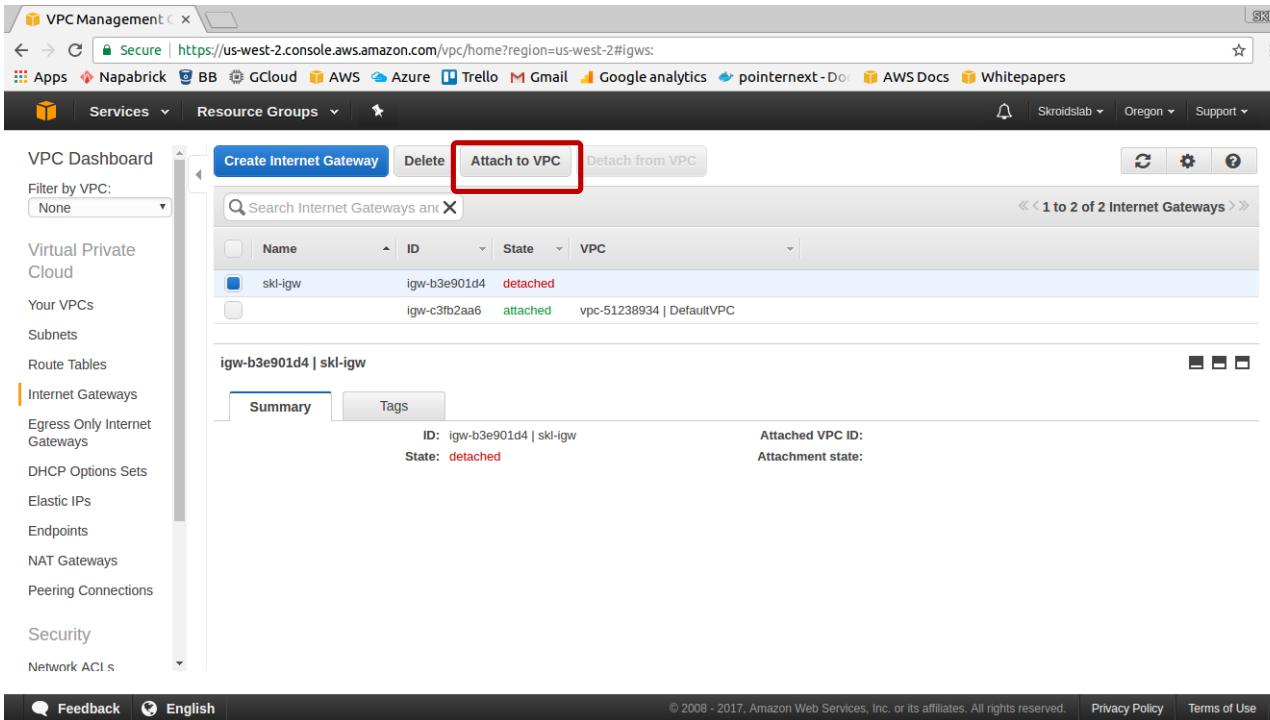
- Summary tab: Subnet ID: `subnet-58d99f3f | us-west-2b-10.0.2.0`, Availability Zone: `us-west-2b`.
- Route Table tab: IPv4 CIDR: `10.0.2.0/24`, IPv6 CIDR: `2002:10:1000::/32`, State: `available`, VPC: `vpc-0b143e6c | sk8-vpc`, Available IPs: `251`.
- Network ACL tab: Network ACL: `acl-d98f505f`, Default subnet: `no`.
- Flow Logs tab: Auto-assign Public IP: `no`, Auto-assign IPv6 address: `no`.
- Tags tab: None.

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 is collapsed, and the main content area displays the Internet Gateways page. The 'Attach to VPC' button for the 'skl-igw' gateway is highlighted with a red box.

**Internet Gateways Table:**

Name	ID	State	VPC
skl-igw	igw-b3e901d4	detached	
	igw-c3fb2aa6	attached	vpc-51238934   DefaultVPC

**igw-b3e901d4 | skl-igw (Selected):**

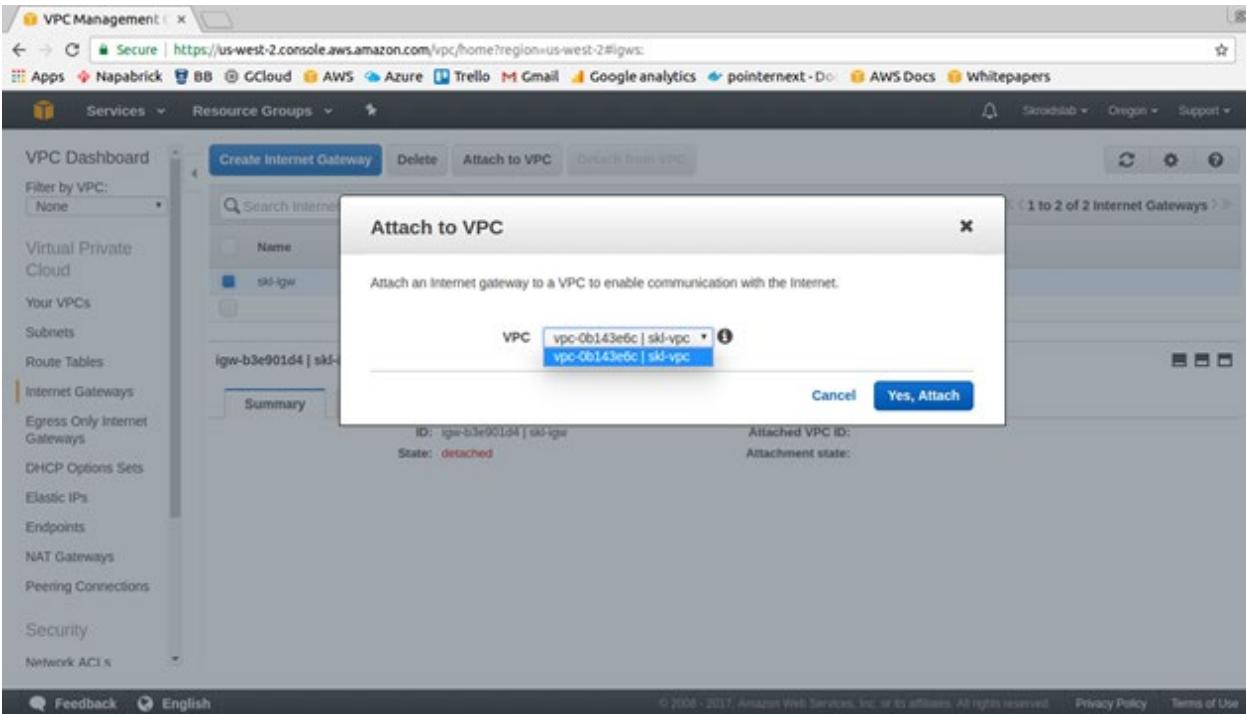
**Summary Tab:**

- ID: igw-b3e901d4 | skl-igw
- State: detached
- Attached VPC ID: vpc-51238934
- Attachment state:

**Tags Tab:**

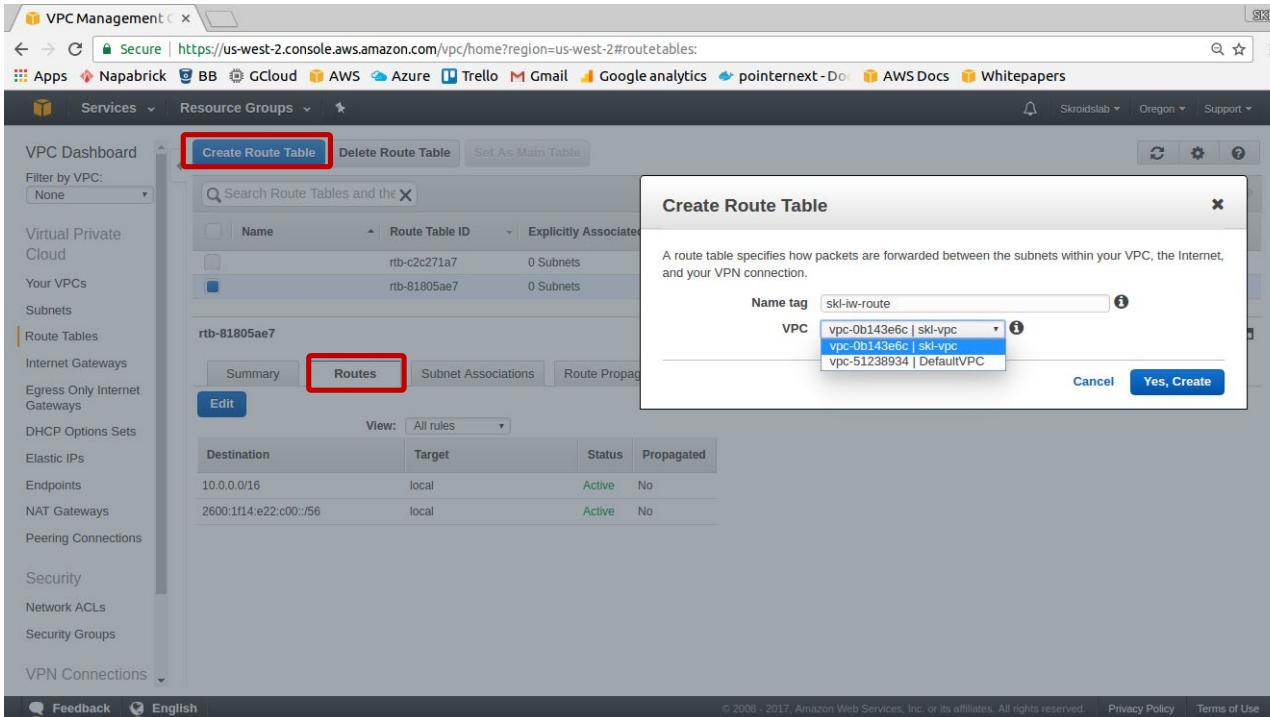
None

# 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	
<b>rtb-84ba60e2   skl-lw-route</b>	0 Subnets	No	vpc-0b143e6c   skl-vpc	

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

Summary	Routes	Subnet Associations	Route Propagation	Tags
<b>Edit</b>				

**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 in the first route table row.

**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
<b>rtb-B4ba60e2   skj-lw-route</b>	<b>rtb-B4ba60e2</b>	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 with their CIDR ranges:

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	<a href="#">igw-b3e901d4</a>

# 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-d98f5c0f	No	No	No
11.0/24	us-west-2a	rtb-84ba60e2   sk...   rtb-84ba60e2   sk...	aci-d98f5c0f	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

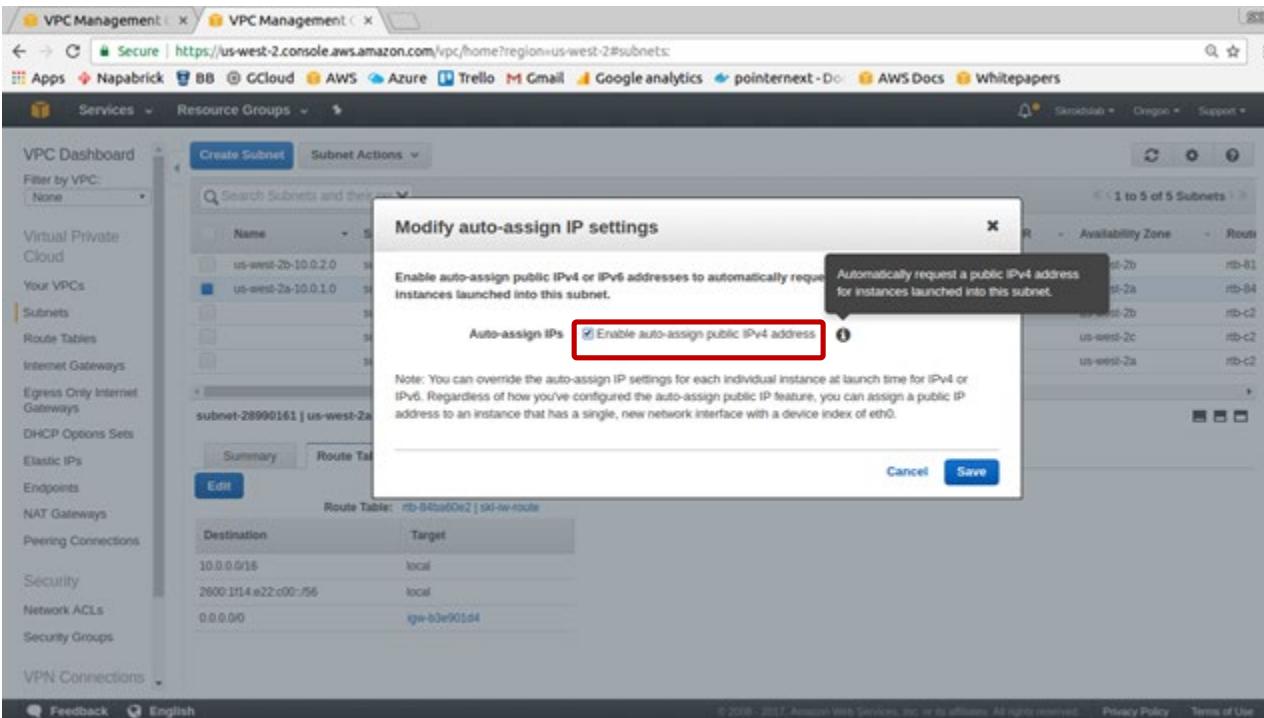
Summary    Route Table    Network ACL    Flow Logs    Tags    Edit

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

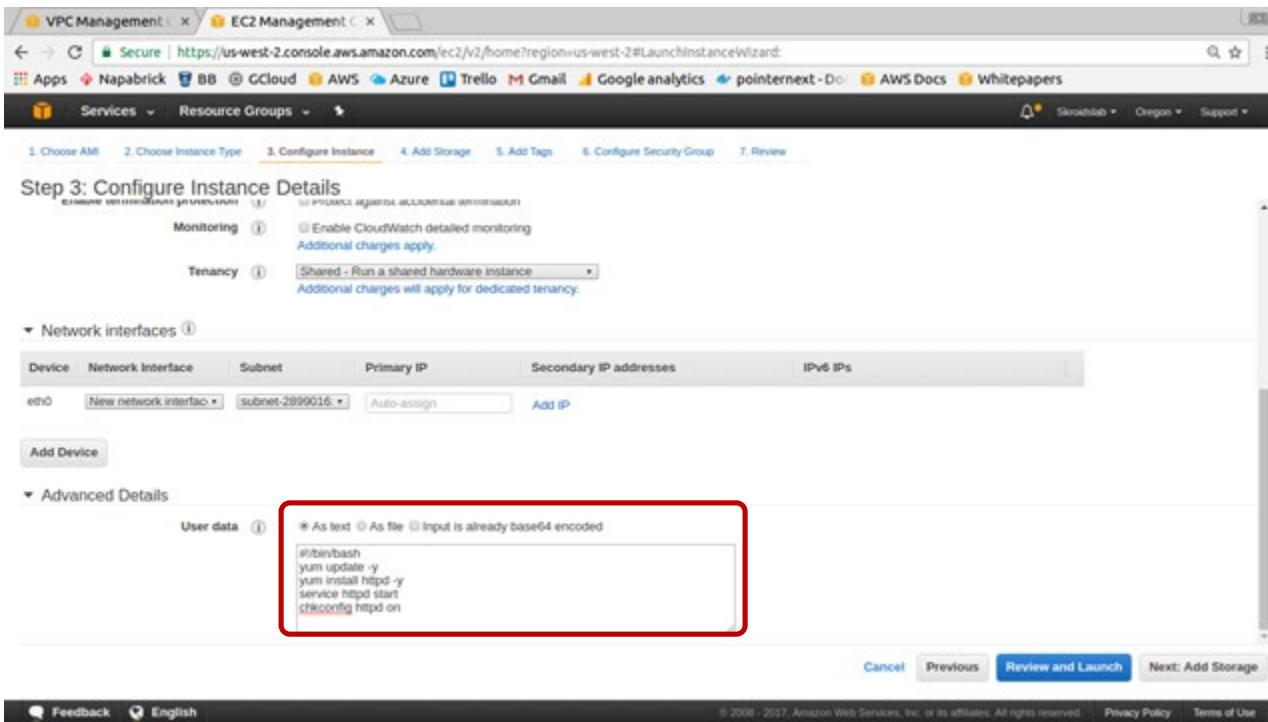
Enable termination protection:  Protect against accidental termination

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 navigation sidebar with sections like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, AMIs, Elastic Block Store, Volumes, Snapshots, Network & Security, Security Groups, Elastic IPs, Placement Groups, Key Pairs, and Network Interfaces. The main area displays the 'Launch Instance' button and a search bar. Below that is a table showing one instance: 'web-server-1' (Instance ID: i-0ff2413c64ce6aec7, Instance Type: t2.micro, Availability Zone: us-west-2a, Status: running). The Public DNS (IPv4) is listed as 52.36.8.194. A detailed view of this instance is shown below, including fields like Instance ID, Instance state, Instance type, Elastic IPs, Availability zone, Security groups, Scheduled events, AMI ID, Platform, IAM role, Key pair name, Owner, Launch time, Public DNS (IPv4), IPv4 Public IP, IPv6 IPs, Private DNS, Private IP, Secondary private IPs, VPC ID, Subnet ID, Network interfaces, Sourcedest check, EBS-optimized, and Root device type.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
web-server-1	i-0ff2413c64ce6aec7	t2.micro	us-west-2a	running	2/2 checks ...	None	52.36.8.194	52.36.8.194

Instance: i-0ff2413c64ce6aec7 (web-server-1) Public IP: 52.36.8.194

Description Status Checks Monitoring Tags

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

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

# Activity - Test the IG+RT

VPC Management EC2 Management

Secure | https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#routetables:

Apps Napabrick BB GCloud AWS Azure Trello Gmail Google analytics pointernext-Doc AWS Docs Whitepapers

Services Resource Groups

VPC Dashboard Filter by VPC: None

Virtual Private Cloud Your VPCs Subnets

Route Tables (highlighted with a red box)

Internet Gateways

Egress Only Internet Gateways DHCP Options Sets Elastic IPs Endpoints NAT Gateways Peering Connections Security Network ACLs Security Groups VPN Connections

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and the X

1 to 3 of 3 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-lw-route	rtb-84ba60e2	1 Subnet	No	vpc-0b143e6c   skl-vpc

rtb-84ba60e2 | skl-lw-route

Summary Routes Subnet Associations Route Propagation Tags

Cancel Save View: All rules

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	igw-b3e901d4	Active	No	

Add another route

Feedback English

© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

**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:

Description:

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

**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.**

Proprietary content. ©Great Learning. All Rights Reserved. Unauthorized use or distribution prohibited

# 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 instance's configuration details. The 'Status Checks' tab indicates 2/2 checks passed. The 'Tags' tab is also present. At the bottom of the instance view, there are tabs for EBS Unattached and Extra.

**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

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

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
	Instance state: running	IPv6 IPs: -
	Instance type: t2.micro	Private DNS: ip-10-0-1-152.us-west-2.compute.internal
	Elastic IPs: -	Private IPs: 10.0.1.152
Availability zone	us-west-2a	Secondary private IPs: -
Security groups	skl-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 for the selected instance are shown, including its elastic IP, availability zone (us-west-2a), security groups (sk8-port-combo, view inbound rules), scheduled events (No scheduled events), AMI ID (amzn-ami-vpc-nat-hvm-2016.09.rc-0.20160910-x86\_64-ena (ami-11kd0e71)), private DNS (ip-20-0-1-152.us-west-2.compute.internal), private IP (10.0.1.152), secondary private IP, VPC ID (vpc-0b143e6c), and subnet ID (subnet-28990161). The bottom of the screen features a footer with links for Feedback, English, Privacy Policy, and Terms of Use.

# 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

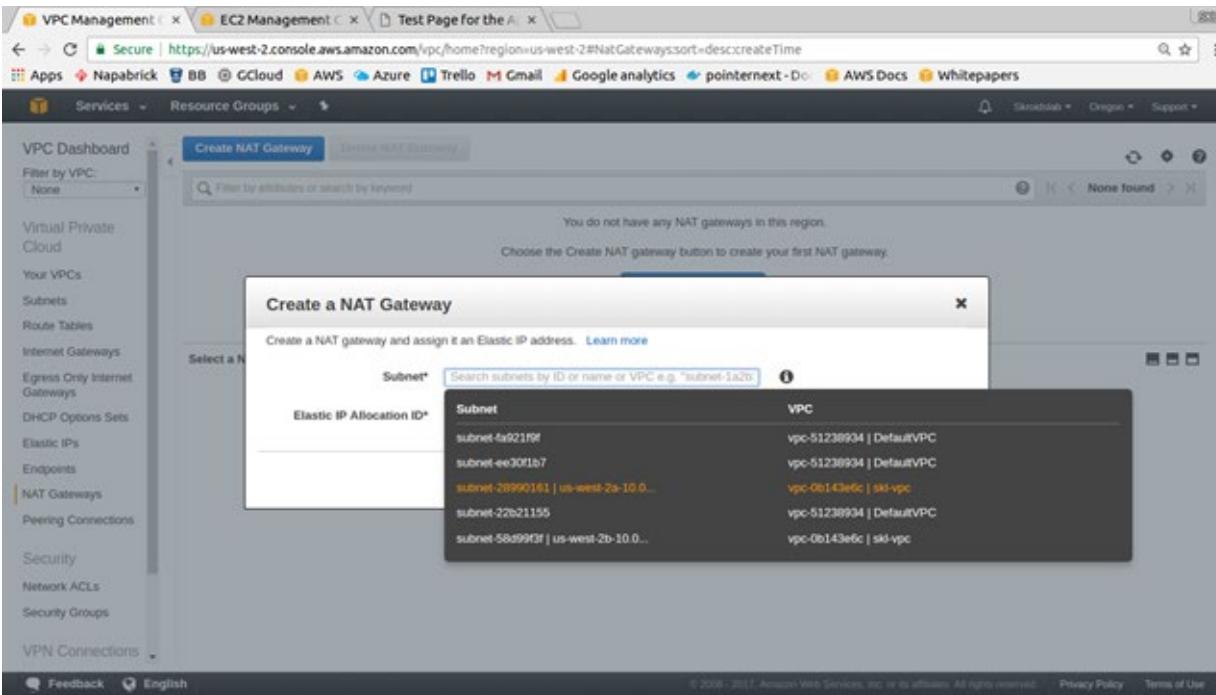
For the 'skl-main-rt' table, the 'Routes' tab is active, showing one route entry:

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'.

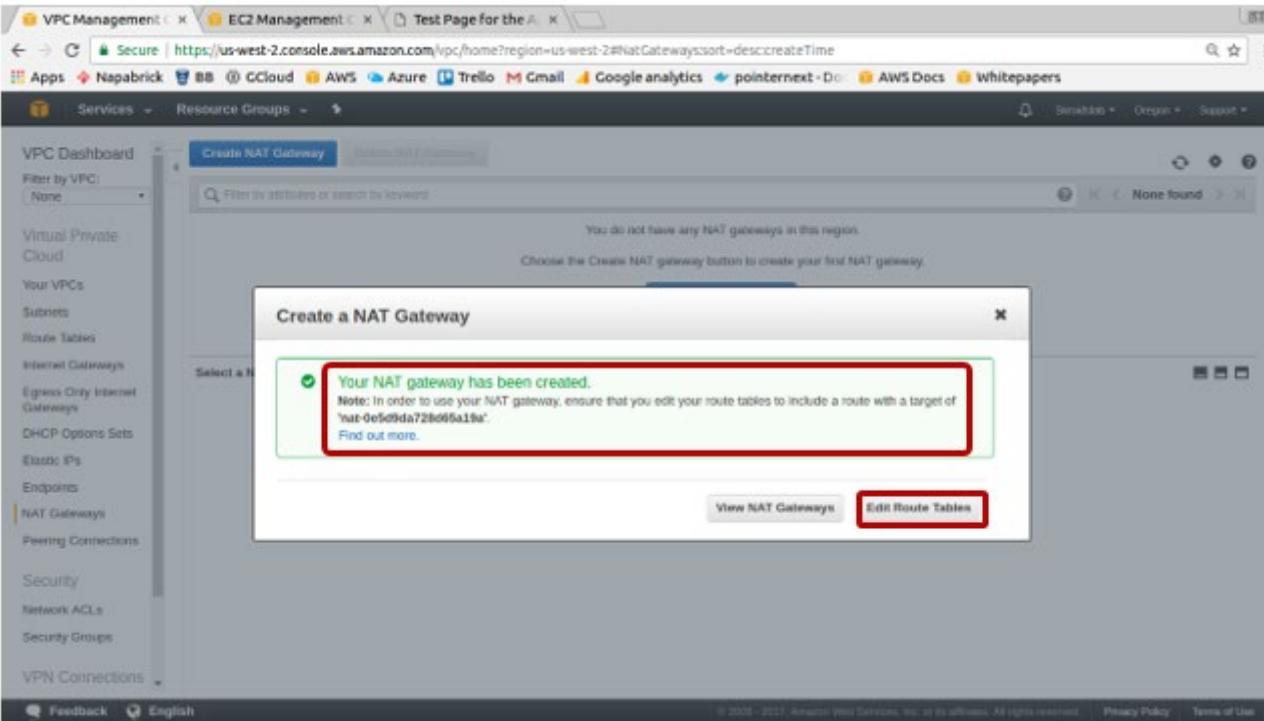
Go to the terminal window of db (that is already open) and try  
# yum install mysql -y

# 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

greatlearning

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-0c5d943e729d05a19a	Active	No	<input type="radio"/>
2600::/48	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 of the main content area, 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 bold text at the bottom center states: "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. A dropdown menu shows 'Cloud Rocker 100' (selected), 'Oregon', and 'Support'.

The main form is titled 'Create Peering Connection'. It has a 'Peering connection name tag' input field containing 'def-skl-peer', which is highlighted with a red box. Below it is a section titled 'Select a local VPC to peer with'. A dropdown menu for 'VPC (Requester)' shows 'vpc-25648043' selected. A sub-menu for 'CIDRs' lists two entries: 'vpc-25648043' and 'cross-default-vpc'. The entry 'vpc-25648043' is also highlighted with a red box. At the bottom, there's a section 'Select another VPC to peer with' with an 'Account' dropdown showing '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**, **Cancel**, and a large blue **Create Peering Connection** button, which is also highlighted with a red box.

# Activity - Peering

The screenshot shows a browser window for the AWS EC2 Management console. 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". Below it, a green box indicates "Success" with the message: "A VPC peering connection (pcx-88d8ede1) has been requested." It lists the details of the peering connection:

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	-

A blue "OK" button is at the bottom right of the message box.

At the bottom of the page, there are 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

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

Left sidebar navigation:

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

Bottom 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	-	10.0.0.0/16
new-hadoopdb	Pending Acceptance by 837466521382	-	-	-	-

# Activity - Peering

The screenshot shows the AWS VPC Peering Connections page. On the left, there's a sidebar with various VPC-related options like Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Endpoint Services, NAT Gateways, and Peering Connections (which is currently selected). 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, detailed information for 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 associated with '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". To the right of the input field is a dropdown menu with the value "pxc-08d8ede1 | def-sil-peer".

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

**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:

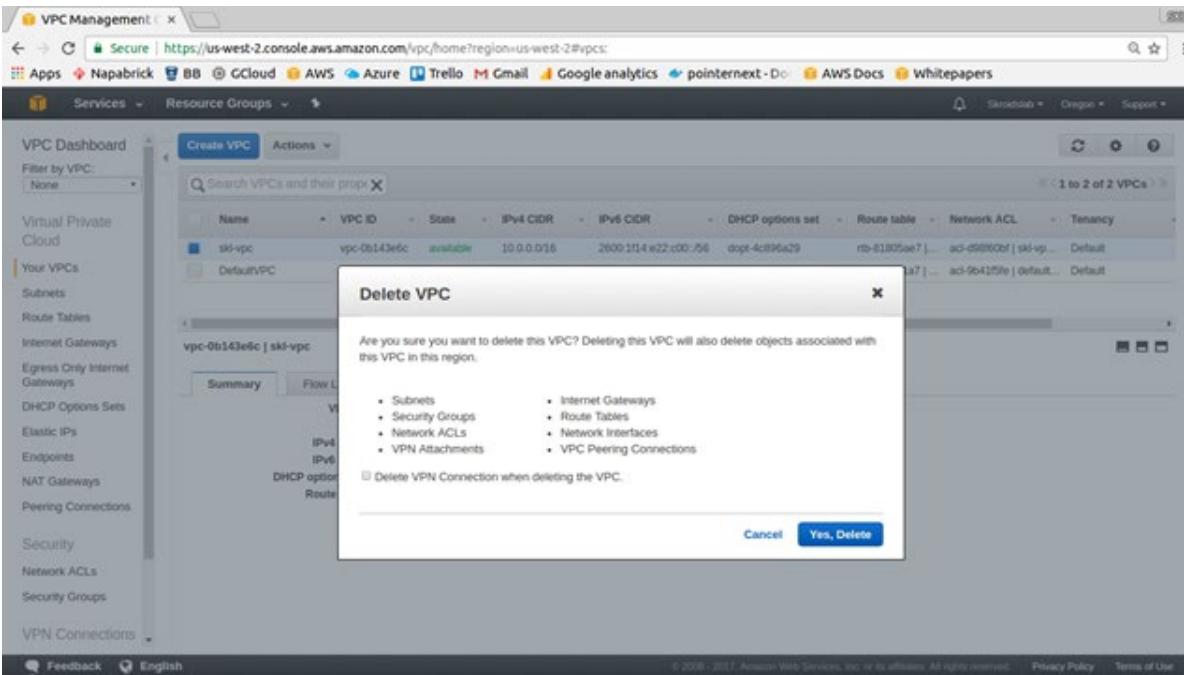
Name	Peering Connection ID	Status	Requester VPC	Acceptor VPC	Requester CIDRs	Acceptor CIDRs
def-sm-peer	pcx-80d8ede1	Active	vpc-25648043   cr...	vpc-e20fb9b   skl...	172.31.0.0/16	10.0.0.0/16
peer	pcx-d2eedfbd	Deleted	vpc-25648043   cr...	vpc-e20fb9b   skl...	-	-

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

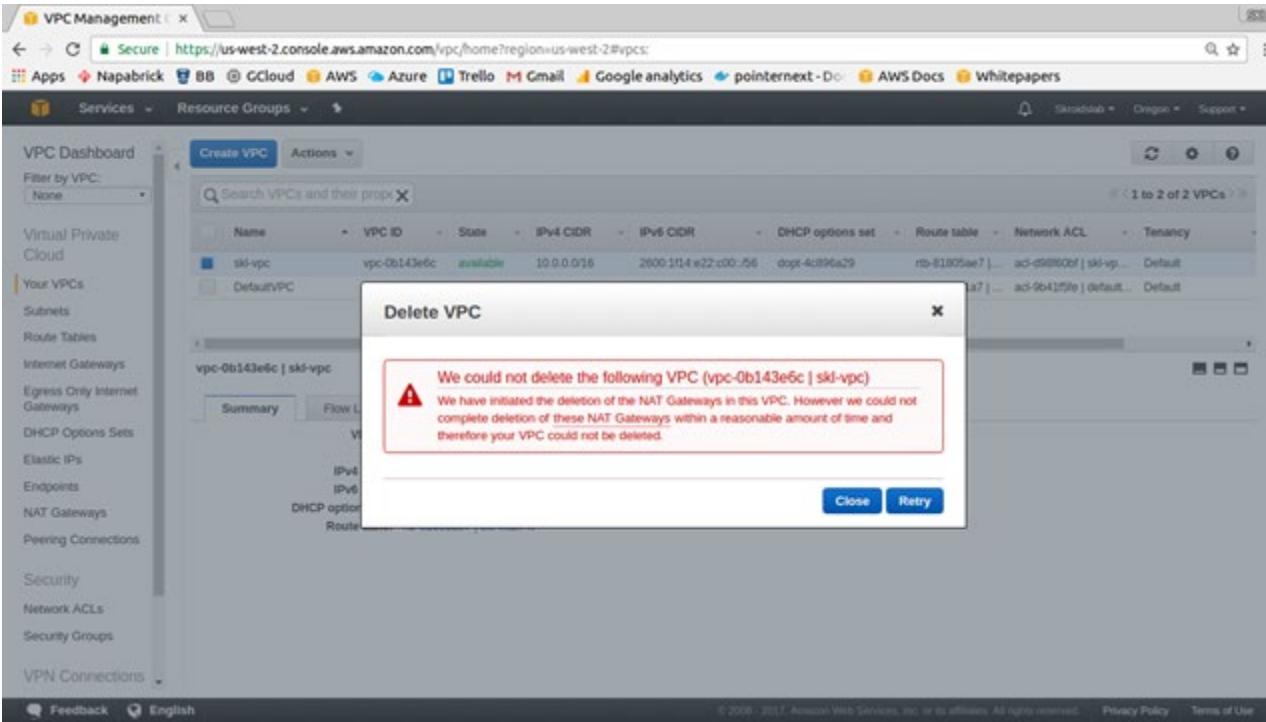
**Verify that both VPCs have the RT updated with each other's CIDR blocks. Now go back to the terminal window and ping the EC2 instance in the custom VPC from the default VPC and ping will respond back!**

# 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, there's a sidebar with 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 area has a title bar with 'Create Hosted Zone' and buttons for 'Go to Record Sets' and 'Delete Hosted Zone'. Below this is a search bar and a table displaying two existing hosted zones:

Domain Name	Type	Record Set Count	Comment	Hosted Zone ID
pointernext.click	Public	2	HostedZone created by Route53 R...	Z200ZPM07PBATU
pointer.next.com	Public	2	PointerNext dot com	Z263051G6406RR

To the right, a modal window titled 'Create Hosted Zone' is open. It contains a red-bordered box with instructions: '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.' Below this are fields for 'Domain Name' (set to 'example.com'), 'Comment' (empty), and 'Type' (set to 'Public Hosted Zone'). A note below says 'A public hosted zone determines how traffic is handled for your resources.' At the bottom of the modal 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` under the 'Registered domains' section. It displays the 'Name servers' field, which contains four entries: `ns-172.awsdns-00.com`, `ns-177.awsdns-32.net`, `ns-1296.awsdns-34.org`, and `ns-3385.awsdns-02.co.uk`. A red box highlights this field. The bottom view is for the same domain under the 'Hosted zones' section. It shows the 'NS' record set, which lists the same four name server entries. A red box highlights this record set. A large red arrow points from the highlighted 'Name servers' field in the top window to the highlighted 'NS' record set in the bottom window. The text 'Must match!' is overlaid in red between the two windows.

Registered domains > pointernext.click

Name servers:

- ns-172.awsdns-00.com
- ns-177.awsdns-32.net
- ns-1296.awsdns-34.org
- ns-3385.awsdns-02.co.uk

NS record set:

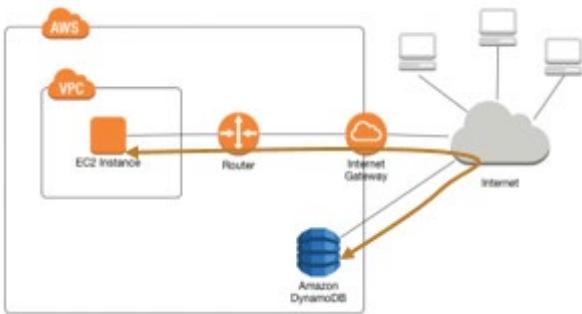
Name	Type	Value
pointernext.click.	NS	ns-172.awsdns-00.com ns-177.awsdns-32.net ns-1296.awsdns-34.org ns-3385.awsdns-02.co.uk

Must match!

# 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

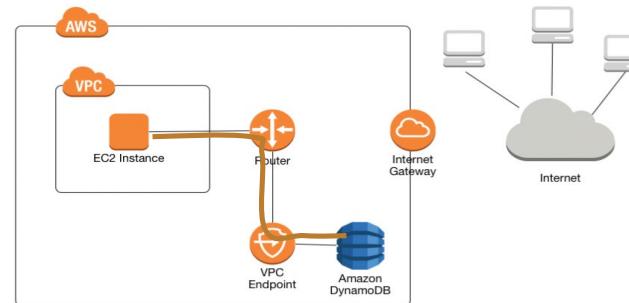
# Activity - VPC Endpoints



## 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>