

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-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 bar has 'Services' and 'Resource Groups' dropdowns.

The left sidebar is titled 'AWS services' and contains sections for 'Recently visited services' (Billing, IAM, EC2, EC2 Container Service, Elastic Beanstalk) and 'All services' (Compute, Developer Tools, Internet of Things, EC2, EC2 Container Service, Lightsail, Elastic Beanstalk, Lambda, Batch, Storage, Management Tools, Game Development, Mobile Services). Below the sidebar is a URL: <https://console.aws.amazon.com/billing/home?region=us-west-2>.

The right panel 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 (with a note about AWS Organizations for policy-based management of multiple AWS accounts). A red box highlights the 'My Organization' link and the 'Create an organization' button.

The 'What's new?' section highlights 'Announcing Amazon Chime' and 'Introducing Elastic Volumes for Amazon EBS', each with a 'Learn more' link.

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 dashboard, 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. A large blue 'Create Alarm' button is prominently displayed.

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 section 'When my total AWS charges for the month exceed: \$ 10 USD send a notification to: name@email.com'. A reminder note states: '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 'Additional settings' section includes a dropdown 'Treat missing data as : missing' and links to 'show simple options' and 'show advanced'. To the right of the dialog is an 'Alarm Preview' chart titled 'EstimatedCharges > 10' showing a blue line above a red horizontal line at the value of 10. The Y-axis ranges from 0 to 12.5, and the X-axis shows dates from 4/04 to 4/08. Below the chart is a 'More resources' section with links to 'AWS Billing console', 'Getting started with billing alarms', 'More help with billing alarms', and 'AWS Billing FAQs'. At the bottom of the dialog 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
Total	\$28.31

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

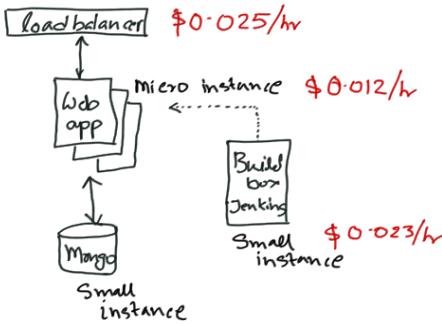
VIA AMAZON CLOUD ON AWS

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.

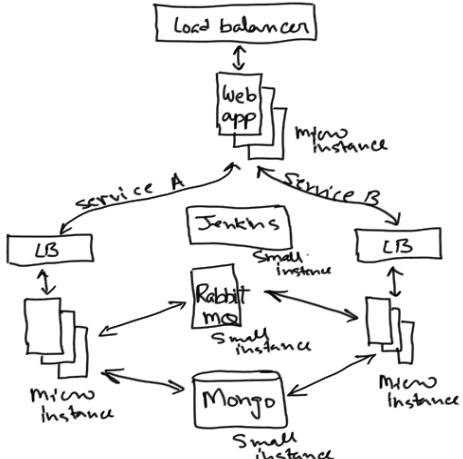
Instance Type	vCPU	ECU	Memory (GiB)	Instance Storage (GB)	Linux/UNIX Usage
t2.nano	1	Variable	0.5	EBS Only	\$0.0059 per Hour
t2.micro	1	Variable	1	EBS Only	\$0.012 per Hour
t2.small	1	Variable	2	EBS Only	\$0.023 per Hour
t2.medium	2	Variable	4	EBS Only	\$0.047 per Hour
t2.large	2	Variable	8	EBS Only	\$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 Documentation

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

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 infrastructure are you comparing against?
What kind of server do you currently have?

Services
AWS provides many services to its customers.
Compute
Storage

You could save 69% a year by moving your infrastructure to AWS.
Your three year total savings equals to \$ 654,304

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 in the top right corner 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**.

	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. The URL is displayed in a blue box with a 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."

Details

- Groups
- Users
- Roles
- Policies
- Identity Providers
- Account Settings
- Credential Report

Encryption Keys

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.amazonaws.com

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

The screenshot shows the AWS IAM Management Console with the URL <https://console.aws.amazon.com/iam/home?region=ap-southeast-1#home>. A modal dialog box titled "Manage MFA Device" is displayed, instructing the user to activate a virtual MFA device by installing an AWS MFA-compatible application on their device. It includes a "Don't show me this dialog box again." checkbox and "Cancel", "Previous", and "Next Step" buttons. The background shows the IAM dashboard with sections like "Welcome to Identity and Access Management", "IAM users sign-in link", and "Manage MFA Device". A video player for "Introduction to AWS IAM" is also visible.

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.

The "Quick Start" sidebar lists categories: My AMIs, AWS Marketplace, Community AMIs, and a checkbox for Free tier only. The main list shows three AMI options:

- Amazon Linux AMI 2015.09.1 (HVM), SSD Volume Type - ami-f0091d91**
Free tier eligible
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 (64-bit)
- Red Hat Enterprise Linux 7.1 (HVM), SSD Volume Type - ami-4dbf9e7d**
Free tier eligible
Red Hat Enterprise Linux version 7.1 (HVM), EBS General Purpose (SSD) Volume Type
Root device type: ebs Virtualization type: hvm
Select button (64-bit)
- SUSE Linux Enterprise Server 12 (HVM), SSD Volume Type - ami-d7450be7**
Free tier eligible
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
Select button (64-bit)

A message at the bottom states: "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.

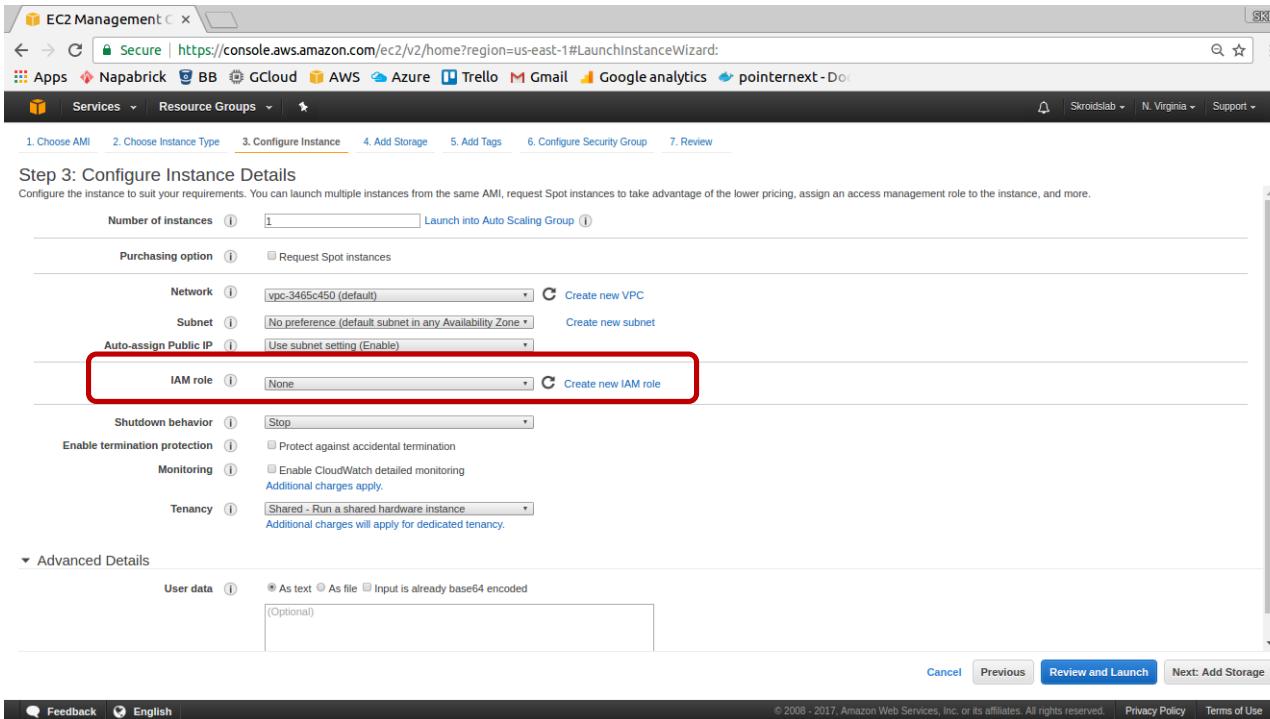
Advanced Details

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, there are "Cancel", "Previous", "Review and Launch", and "Next: Add Storage" buttons.

Important! What happens if you miss adding a role?

Activity - EC2 launch instance

EC2 Management Console SKL

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

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

Skroidslab 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 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

General Purpose (SSD)
General Purpose (SSD)
Provisioned IOPS (SSD)
Magnetic

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: Tag Instance

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 path 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

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 (which is highlighted), and 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 set to "Create a new key pair", a text input field with the value "nirmallya", 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 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". 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 success message: "Your instances are now launching. The following instance launches have been initiated: i-0749a28555320dbf7" with a "View launch log" link. Below this is a blue info message: "Get notified of estimated charges. Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier)." Under "How to connect to your instances", it says: "Your instances are launching, and it may take a few minutes until they are in the running state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances. Click [View Instances](#) to monitor your instances' status. Once your instances are in the running state, you can [connect](#) to them from the Instances screen. [Find out](#) how to connect to your instances." A section titled "Here are some helpful resources to get you started" lists links: "How to connect to your Linux instance" (Amazon EC2: User Guide), "Learn about AWS Free Usage Tier" (Amazon EC2: Discussion Forum). At the bottom, it says: "While your instances are launching you can also" with links: "Create status check alarms", "Create and attach additional EBS volumes", and "Manage security groups". A "View Instances" button is located 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

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation includes: EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES (with Instances selected), Spot Requests, Reserved Instances, Commands, Dedicated Hosts, IMAGES (with AMIs selected), Bundle Tasks, ELASTIC BLOCK STORE (with Volumes and Snapshots selected), and NETWORK & SECURITY (with Security Groups selected). The main content area displays the details for an instance named "Http Server" (i-48072c8c). The instance is running, t2.micro type, in us-west-2b availability zone, with a public DNS of ec2-54-201-208-132.us-west-2.compute.amazonaws.com and a public IP of 54.201.208.132. It has a private DNS of ip-172-31-44-93.us-west-2.compute.internal and a private IP of 172.31.44.93. The instance is associated with a security group named "launch-wizard-1". A modal window titled "Security Groups associated with i-48072c8c" lists the rule: "Ports 22, Protocol tcp, Source 0.0.0.0/0, Destination launch-wizard-1". The bottom footer includes links for Feedback, English, Privacy Policy, and Terms of Use.

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

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-west-2.compute.amazonaws.com 54.201.208.132

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, view rules

Secondary private IPs

VPC ID vpc-51238934

Subnet ID subnet-fa921f9f

Network interfaces eth0

Source/dest. check True

Ports Protocol Source Destination

22 tcp 0.0.0.0/0 launch-wizard-1

Key pair name nirmallya

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 bar includes links for Instances, Spot Requests, Reserved Instances, Commands, 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 SECURITY GROUPS section is currently selected. The main content area displays a 'Create Security Group' dialog box. The dialog box fields are as follows:

- Security group name:** port-80
- Description:** Open port 80
- VPC:** vpc-51238934 (172.31.0.0/16) *

A note below the VPC field states: "* denotes default VPC".

The dialog box also contains a 'Security group rules:' section with tabs for **Inbound** and **Outbound**. Under the Inbound tab, there is a table with columns: Type, Protocol, Port Range, and Source. A single rule is listed:

Type	Protocol	Port Range	Source
HTTP	TCP	80	Anywhere

An **Add Rule** button is located below the table.

At the bottom right of the dialog box 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. The "Networking" option is highlighted. 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). To the right of the instance details, security group information is shown, including Public DNS (ec2-54-201-208-132.us-west-2.compute.amazonaws.com), Public IP (54.201.208.132), Elastic IP (-), Availability zone (us-west-2b), Security groups (launch-wizard-1, view rules), 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. On the left, there's a navigation sidebar with links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances (which is 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 has a title "Change Security Groups" and displays instance details: Instance ID: i-48072c8c and Interface ID: eni-49e0a430. Below this, a table lists security groups to associate with the instance. The table has columns: Security Group ID, Name, and Description. Three groups are listed: default (unchecked), sg-a76855c3 (checked), and sg-1b665b7f (checked). At the bottom right of the dialog are "Cancel" and "Assign Security Groups" buttons. The background shows a list of security groups on the right side of the screen.

Security Group ID	Name	Description
<input type="checkbox"/> sg-05123160	default	default VPC security group
<input checked="" type="checkbox"/> sg-a76855c3	launch-wizard-1	launch-wizard-1 created 2015-12-13T17:02:39.635+05:30
<input checked="" type="checkbox"/> sg-1b665b7f	port-80	Open port 80

Cancel **Assign Security Groups**

Network interfaces eth0
Source/dest. check True
IAM role -
Key pair name nirmalya

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	Copy to new
sg-32750e48	open-8080	Open port 8080 for tomcat to go through	Copy to new
sg-0f64b-74	open-port-22	Open SSH	Copy to new
sg-e866f993	open-port-80	Open HTTP	Copy to new
sg-bd00f0c7	open-rdp	Open port 3389 for remote desktop for Windows	Copy to new
sg-4c465436	open-ssh	Open port 22 for SSH	Copy to new
sg-bc83bfc1	rds-launch-wizard	Created from the RDS Management Console	Copy to new
sg-d47159af	rds-launch-wizard-2	Created from the RDS Management Console	Copy to new

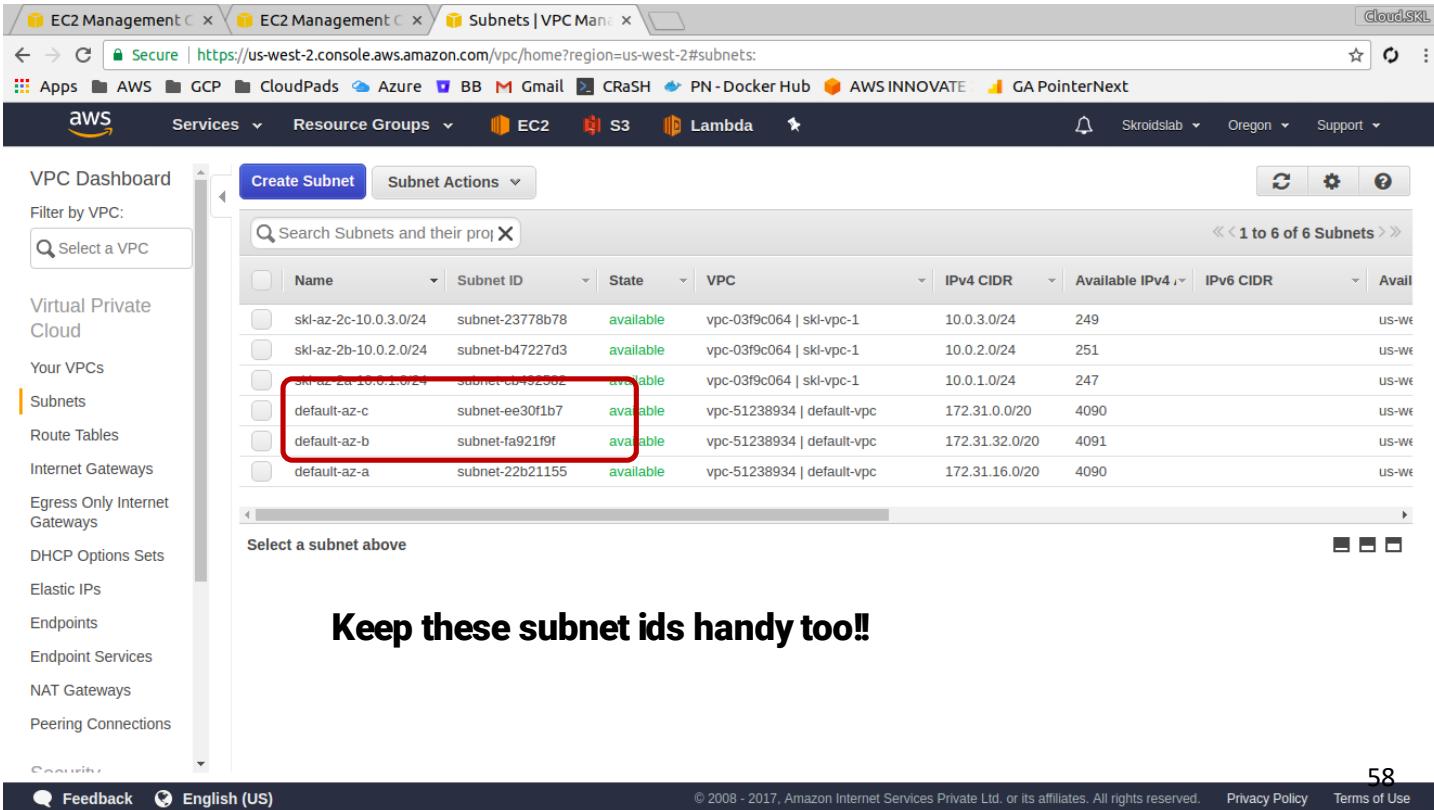
Select a security group above to view its inbound rules.

Keep these SG ids handy!

Buttons: Cancel, Previous, Review and Launch.

Footer: 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), and other AWS services.

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
default-az-c	subnet-ee30f1b7	available	vpc-51238934 default-vpc	172.31.0.0/20	4090		US-West
default-az-b	subnet-fa9219f	available	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) 58 © 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use Proprietary content. ©Great Learning. All Rights Reserved. Unauthorized use or distribution prohibited

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.

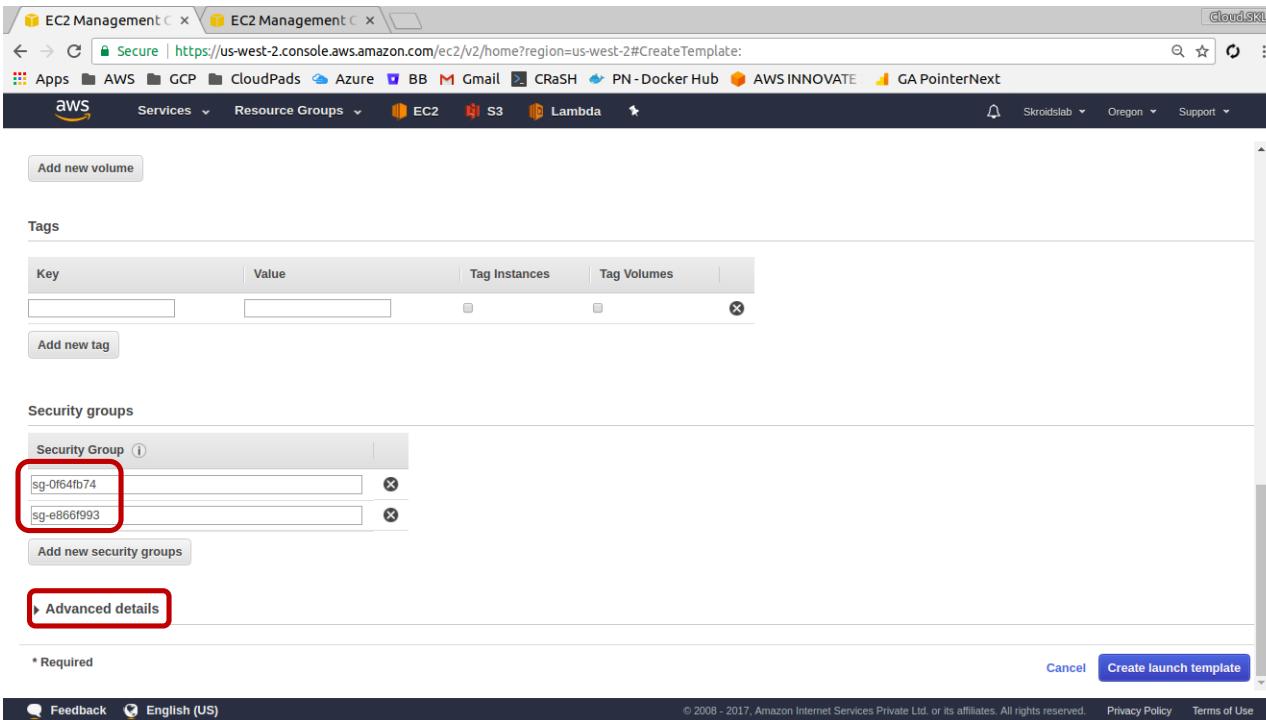
AMI ID

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 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 area displays the 'Create Template' wizard. Under the 'Tags' section, there is a table with columns for Key, Value, Tag Instances, and Tag Volumes. A button 'Add new tag' is visible. Below the tags is a 'Security groups' section. It contains a table with a column for 'Security Group'. Two entries are listed: 'sg-0f64fb74' and 'sg-e8661993'. Both entries have a red rectangular box drawn around them. A button 'Add new security groups' is present. At the bottom of the section is a button 'Advanced details' with a red rectangular box around it. A note at the bottom left says '* Required'. On the right side, there are 'Cancel' and 'Create launch template' buttons. 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.

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 template'.

Form fields visible:

- 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)

Buttons at the bottom:

- * Required
- Cancel
- Create launch template

Page footer:

- 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 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), 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" and is described as being for HTTP, HTTPS, and TCP. A "Create" button is also present here. 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 warning message in an orange box states: '⚠ Improve your load balancer's security. Your load balancer is not using any secure listener.' It advises users to use the HTTPS protocol for secure connections and provides links to 'Basic Configuration' and 'Next: Configure Security Groups'.

At the bottom of the page, there are 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 - 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 shows the "Step 3: Configure Security Groups" page of the ELB wizard. The steps are numbered 1. Configure Load Balancer, 2. Configure Security Settings, 3. Configure Security Groups (which is highlighted), 4. Configure Routing, 5. Register Targets, and 6. Review. A note below the steps says: "Step 3: Configure Security Groups. 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". The "Select an existing security group" option is selected and has a red box around it. A table lists existing security groups with columns for Security Group ID, Name, Description, and Actions. One row, "sg-e866f993", has a blue box around its checkbox and a red box around the entire row. The table has a filter bar at the top right labeled "Filter [VPC security groups]". At the bottom of the page are buttons for "Cancel", "Previous", and "Next: Configure Routing".

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

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 top 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 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.

An "Add to registered" dialog box is open, showing the port as 80. A search bar is present above the list of instances. The list of instances is identical to the registered targets table.

Add to registered	on port 80					
Search Instance	X					
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 at the bottom right include "Cancel", "Previous", and "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 'Basic Configuration':

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 copyright information: © 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.

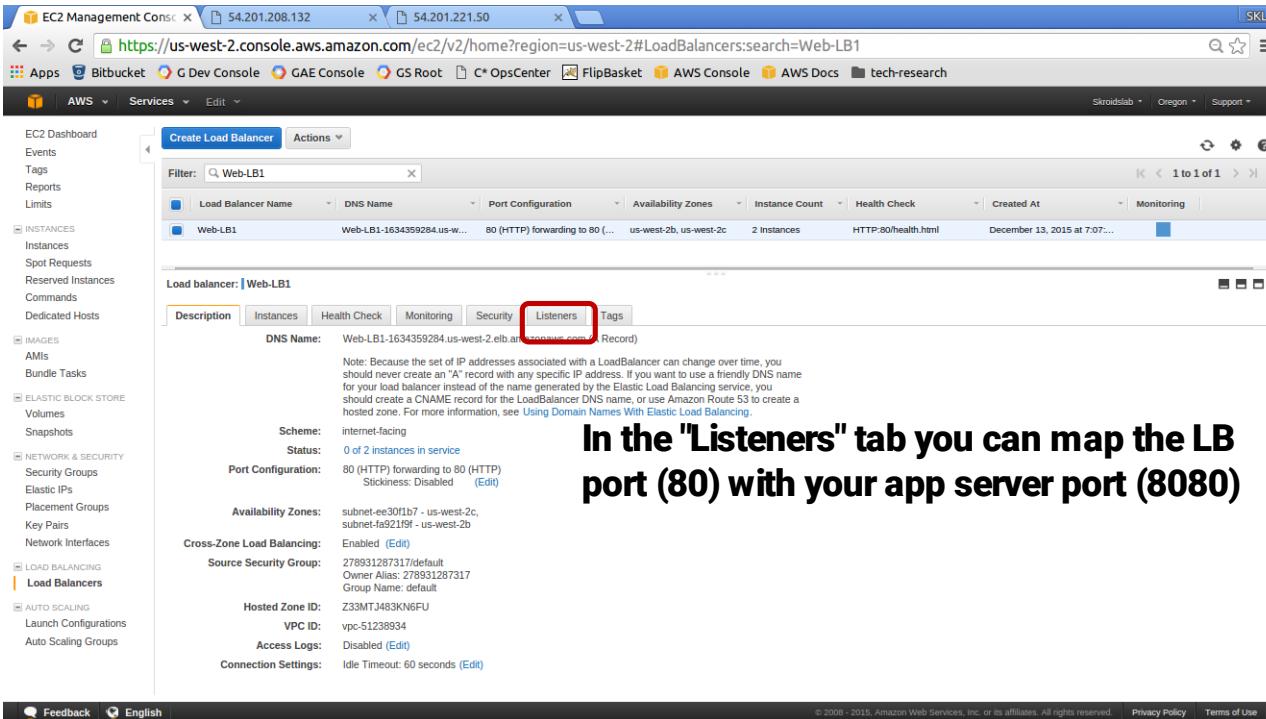
VPC: vpc-51238934 (172.31.0.0/16)

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)



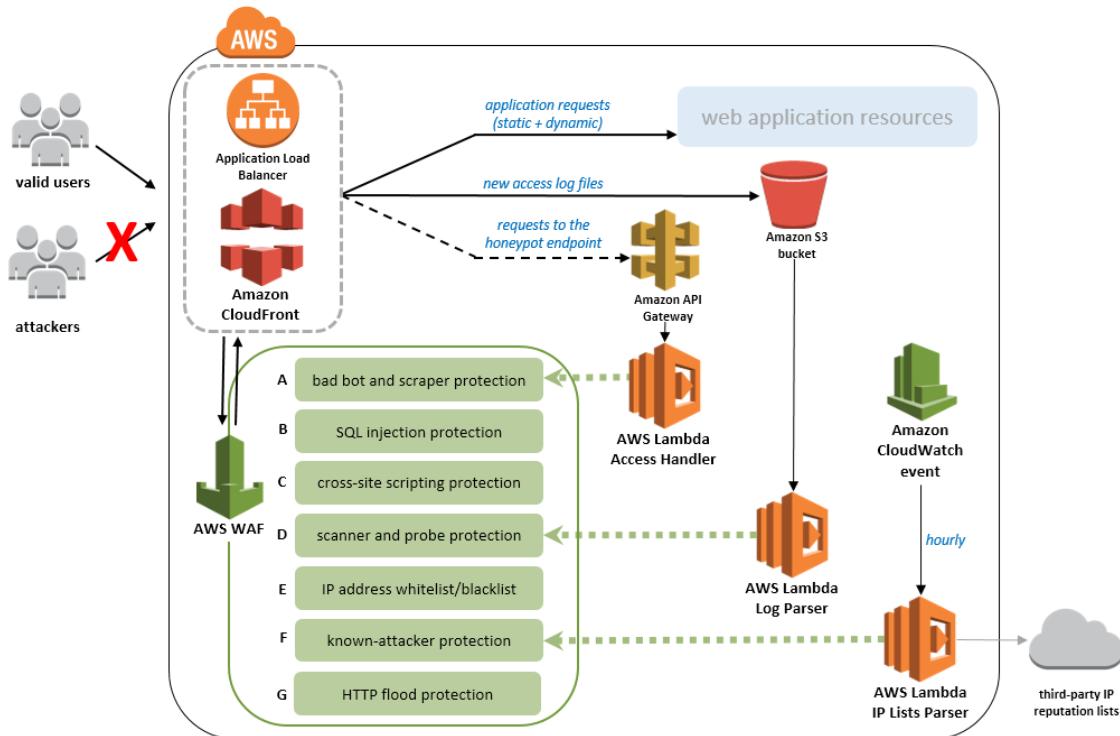
Compute - Part I

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 home page. At the top, there's a large green download icon with the text "AWS WAF and AWS Shield". Below it, a sub-headline reads "AWS WAF and AWS Shield help protect your AWS resources from web exploits and DDoS attacks". The main content area is divided into three sections: "AWS WAF" (represented by a wall icon), "AWS Shield" (represented by a shield icon), and "AWS Firewall Manager" (represented by a circular icon with arrows). Each section has a brief description and a "Go to AWS WAF", "Go to AWS Shield", or "Go to AWS Firewall Manager" button at the bottom.

AWS WAF

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.

[Go to AWS WAF](#)

AWS Shield

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.

[Go to AWS Shield](#)

AWS Firewall Manager

AWS Firewall Manager simplifies your AWS WAF administration and maintenance tasks across multiple accounts and resources.

[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 features the "AWS WAF" logo and a brief description: "AWS WAF is a web application firewall service that helps protect the websites and web apps that you deliver with Amazon CloudFront and ELB Application Load Balancers. Create web access control lists (web ACLs) that define which HTTP and HTTPS requests to allow, block, or count." A "Learn more" link and a "Configure web ACL" button are also present.

Three main sections are displayed:

- Web traffic filtering with custom rules**: Shows a diagram of a traffic flow through a filter. Description: "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**: Shows a computer monitor with a shield icon. Description: "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**: Shows a computer monitor with a chart icon. Description: "Review details about the web requests that AWS WAF allows, blocks, or counts, and update rules to thwart new attacks."

Footer links include Feedback, English (US), © 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 Create XSS match condition 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 Create condition 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

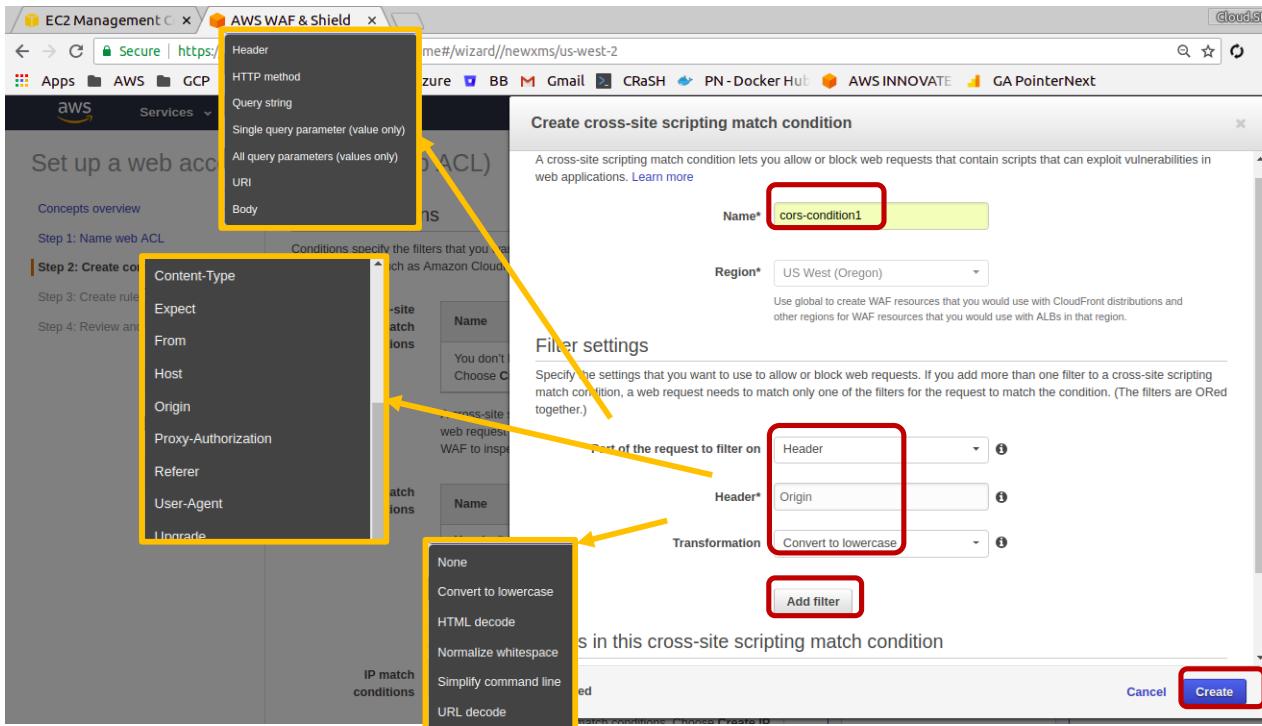
- Rule 1, Bad User-Agents, then block
 - IP match condition
Suspicious IPs
 - and
 - String match condition
Bad bots

or if requests match

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

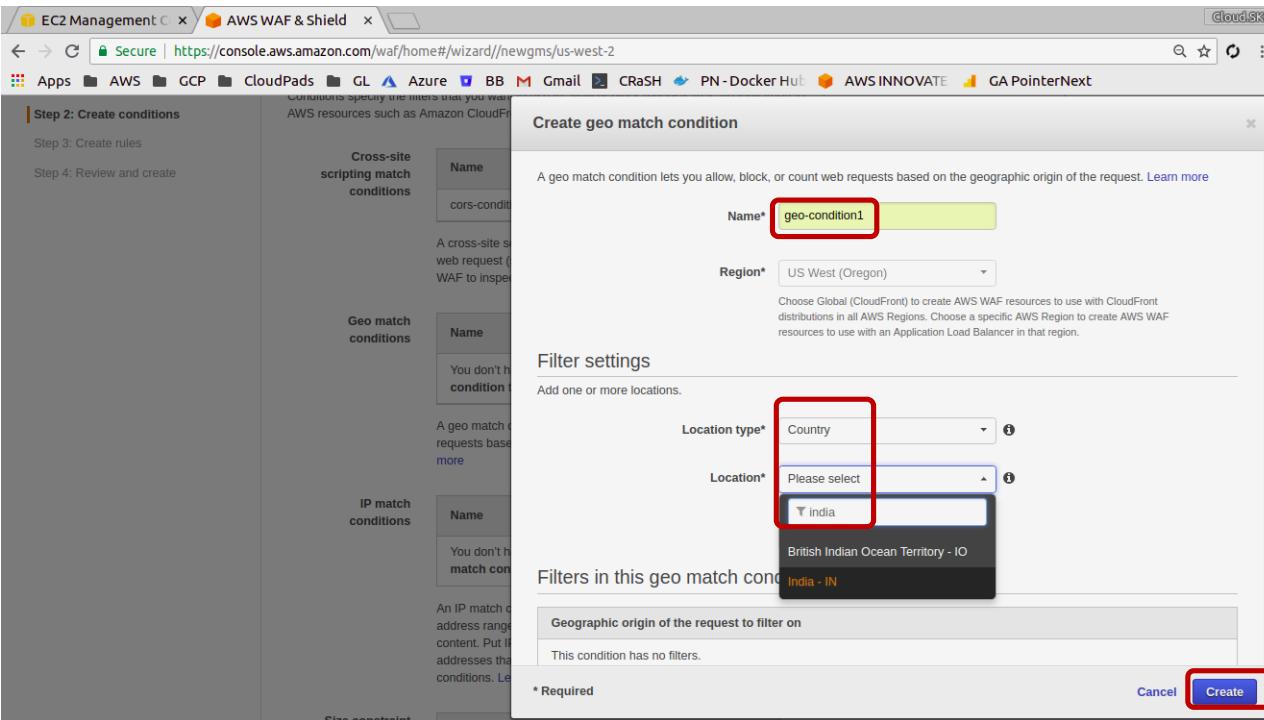
Create multiple conditions by clicking on the appropriate "Create condition" button which will show an "overlay" window

WAF - CORS condition



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

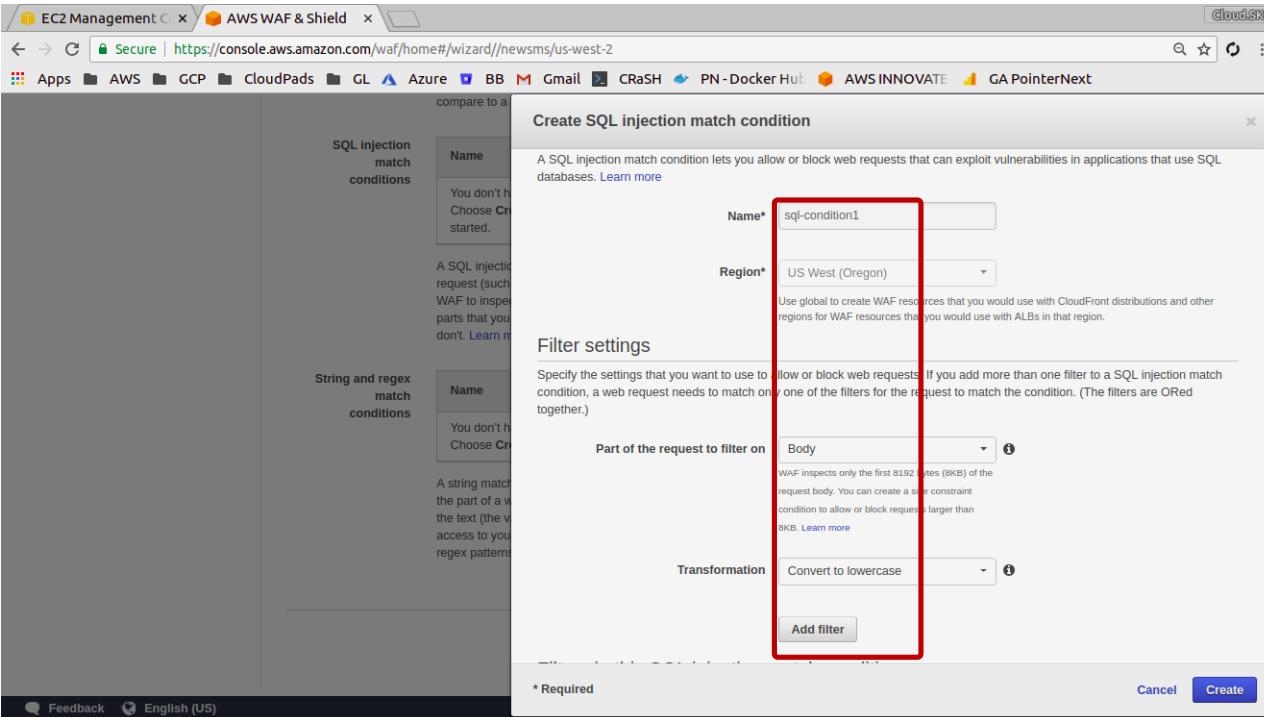
Cancel Create

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

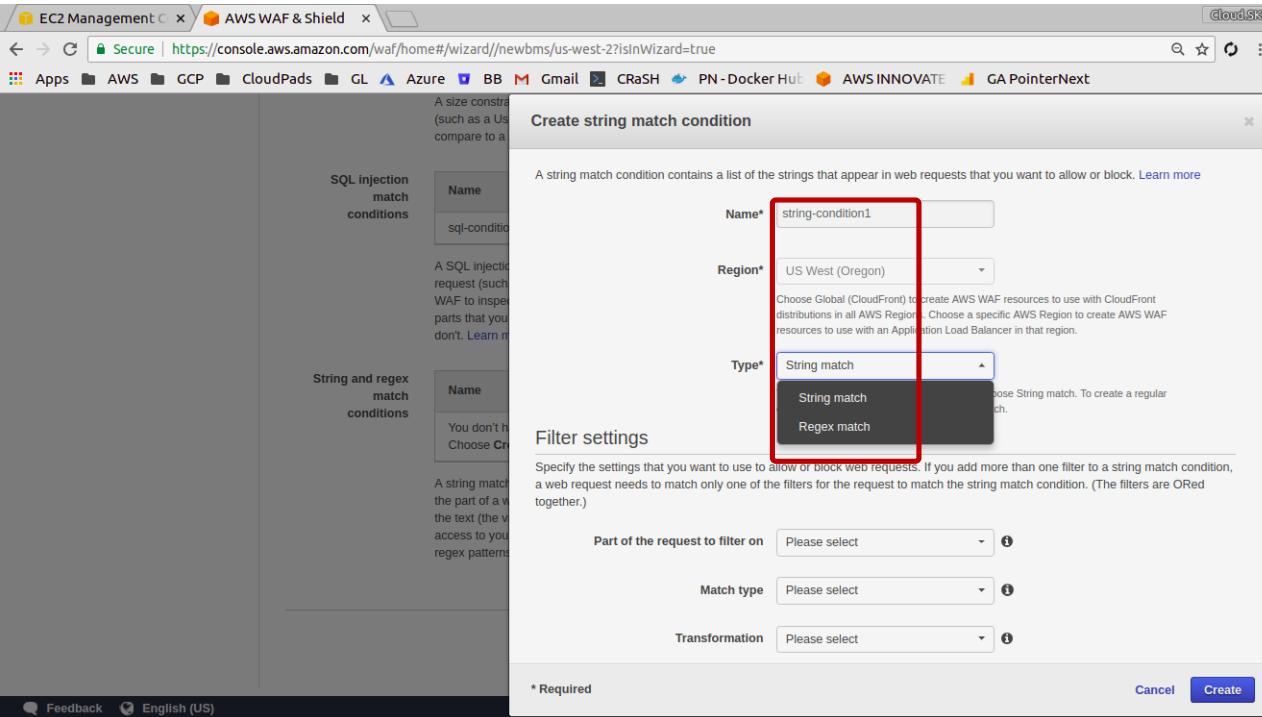
WAF - Size check condition

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 the following 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 'fraud string'. A tooltip for this field says: "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."

Annotations on the right side of the dialog highlight specific details:

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

At the bottom of the dialog, there are 'Cancel' and 'Create' buttons, and a note: '* Required'.

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 these conditions can be used in a rule:

- 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***: A dropdown menu is open, showing 'Regular rule' (highlighted with a red box) and 'Rate-based rule'.
- Region***: A dropdown menu is open, showing 'us-east-1' and 'us-west-2'.

Below these fields, a section titled 'Add conditions' is visible, containing a sub-section 'When a request' with a dropdown set to 'does' and a filter condition 'match at least one of the filters in the cross-site scripting match condition'. There is also a note about choosing a cross-site scripting match condition and an 'Add condition' 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. The dialog has the following structure:

- When a request
- ipmatch-condition1** (highlighted with a red box)
- IP Addresses in ipmatch-condition1:
122.179.50.121/32
-

At the bottom of the dialog, there are "Required" and "Cancel" buttons, and a "Create" button on the right.

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:

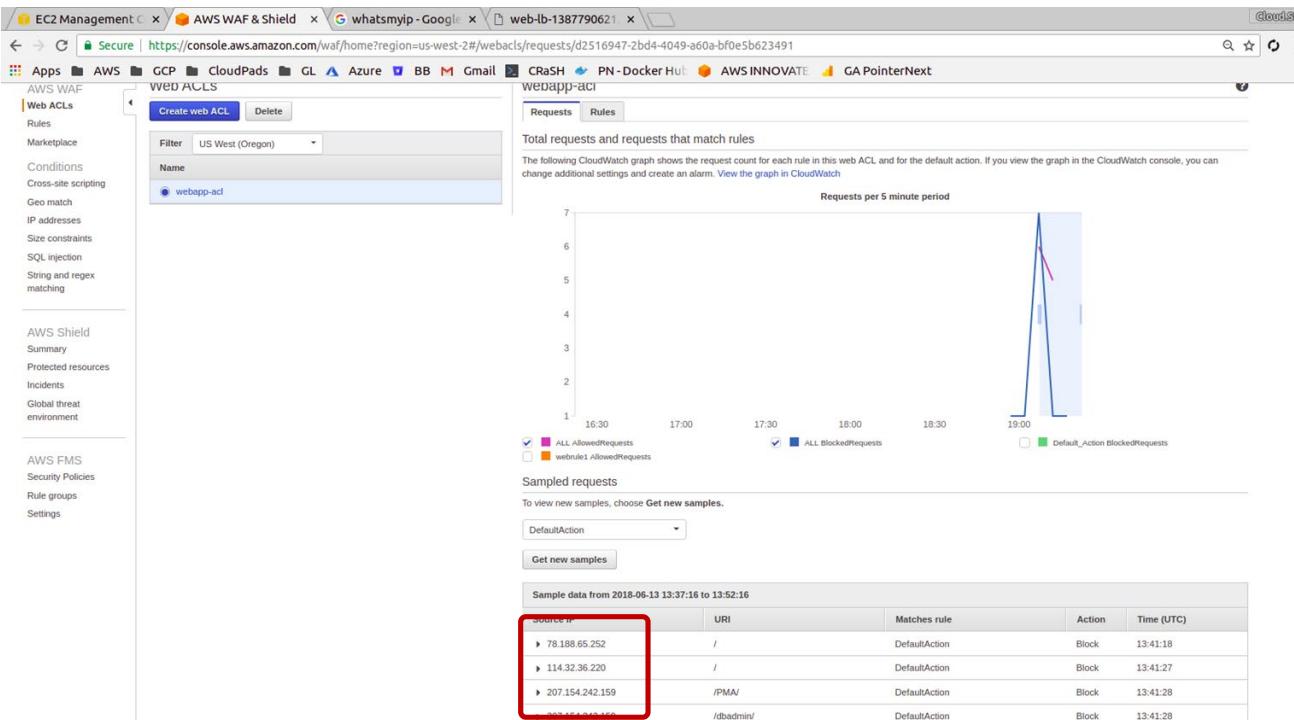
Order	Rule	Type	Action
1	webrule1	Regular	Allow requests
2	webrule1	Regular	Block requests

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 lists "AWS resources using this web ACL" with one entry: "Resource: web-lb, Type: Application load balancer". A red box highlights the "Action" column in the rule table.

**\$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#/webacl/requests/d2516947-2bd4-4049-a60a-bf0e5b623491>. The page displays a table of sample log 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 section 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
Client information: 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
Client information: 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
Client information: 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.

Buttons at the bottom right include 'Cancel' and 'View 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 the benefits of Scheduled Instances and provides links to purchase or learn more.

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 the 'Welcome to Dedicated Hosts' page. It features a central box titled 'My Dedicated Host' containing four buttons labeled 'My Instance 1', 'My Instance 2', 'My Instance 3', and 'Launch Instance Here'. Below this, a descriptive text explains what a Dedicated Host is, mentioning it's a physical server with dedicated EC2 instance capacity. It highlights features like visibility over utilization, determining socket and core counts, and addressing corporate compliance and regulatory requirements. A blue 'Allocate a Host' button is located at the bottom of this section. At the very bottom of the page, there are links for 'Feedback', 'English', and legal notices: '© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.', 'Privacy Policy', and 'Terms of Use'.

Compute - Part II

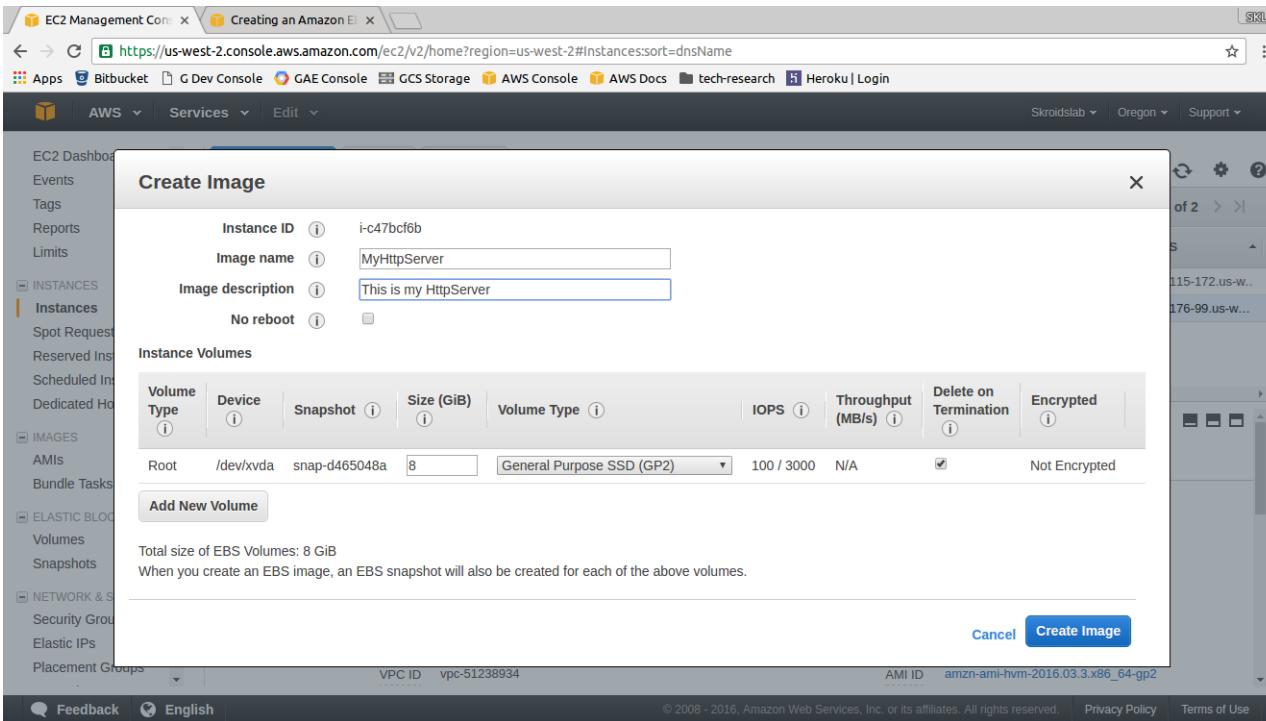
AMI

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's a table with various configuration parameters.

Parameter	Value
Instance ID	i-c47bcf6b
Public DNS	ec2-52-41-176-99.us-west-2.compute.amazonaws.com
Public IP	52.41.176.99
Elastic IPs	
Availability zone	us-west-2b
Instance state	running
Instance type	t2.micro
Private DNS	ip-172-31-45-229.us-west-2.compute.internal
Private IPs	172.31.45.229
Secondary private IPs	
VPC ID	vpc-51238934
Security groups	launch-wizard-1, view rules
Scheduled events	No scheduled events
AMI ID	amzn-ami-hvm-2016.03.3.x86_64-gp2

Activity - AMI



Activity - AMI (auto snapshot created)

greatlearning

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, AMIs, Bundle Tasks, Elastic Block Store, Volumes, Snapshots (which is currently selected), and Network & Security. The main content area displays a table titled "Create Snapshot" with one item listed: "Owned By Me". The table columns are Name, Snapshot ID, Size, Description, Status, and Started. The single entry is "snap-3ffc6f79", 8 GiB, "Created by CreateImage(i-c47bcf6b) for ami-93488bf3 from vol-d04ce659", completed, and started on 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 details:

Snapshot ID	snap-3ffc6f79
Status	completed
Volume	vol-d04ce659
Started	July 12, 2016 at 1:05:47 PM UTC+5:30
Owner	278931287317
Product codes	-
Description	Created by CreateImage(i-c47bcf6b) for ami-93488bf3 from vol-d04ce659

On the right side of the main content area, there are status indicators: Progress 100%, Capacity 8 GiB, Encrypted Not Encrypted, KMS Key ID, KMS Key Aliases, and KMS Key ARN.

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 top navigation bar shows the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Images:sort=name>. The main content area displays a table of owned AMIs, with one entry for 'MyAMI'. The details page for 'MyAMI' shows the following information:

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

Below the table, there are tabs for Details, Permissions, and Tags, with the Details tab selected. An 'Edit' button is located in the top right corner of the details section.

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 highlighted, showing the AMI details for "MyHttpServerAMI".

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

Below the table, the details for the selected AMI ("Image: ami-e1889480") are shown in two columns:

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 contains the following information:

- This image is currently:** Public Private
- AWS Account Number:** [Input field]
- This image currently has no permissions.**
- Add Permission:** Add "create volume" permissions to the following associated snapshots when creating permissions:
 - snap-b1b72bea
- Buttons:** Cancel, Save

Below the dialog, the table of AMIs displays the following data:

Name	Description
1287317/MyHttpServerAMI	This is my http server AMI
Linux	one

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)

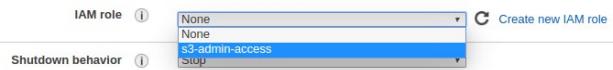
Activity - CLI

- "\$ 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 from the Oregon 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 lists the following AMI options:

- 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 (highlighted)
64-bit
- 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
64-bit
- 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
64-bit
- Ubuntu Server 14.04 LTS (HVM), SSD Volume Type - ami-5189a661**
Select button

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 - 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, there is a filter section with "Filter by:" dropdowns set to "All instance types" and "Current generation". A "Show/Hide Columns" button is also present.

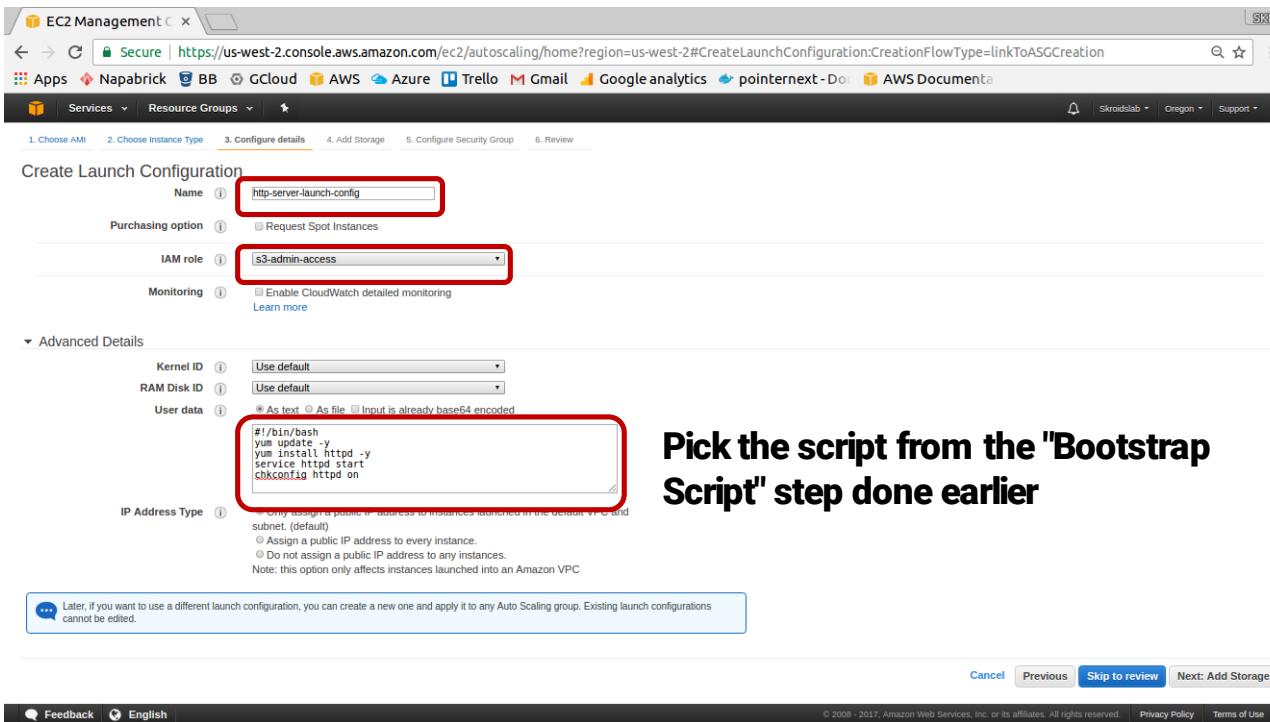
The main table lists various instance types under the "Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)" row. The columns are: Family, Type, vCPUs, Memory (GiB), Instance Storage (GB), EBS-Optimized Available, and Network Performance.

	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	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 other AWS services like Gmail and Google Analytics. It also contains copyright information: "© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved." and links to 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 - Doc, AWS Documenta, Services, Resource Groups, and various AWS regions like Skroidslab, Oregon, and Support.

The main content area displays the "Create Launch Configuration" wizard, 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. Step 4 is currently selected.

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

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 footer with Feedback, English, Copyright notice (© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.), Privacy Policy, and 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" 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	Copy to new
sg-5724b72e	docker-machine	vpc-51238934	Docker Machine	Copy to new
sg-a52f18de	open-port-22	vpc-51238934	Open SSH	Copy to new
<input checked="" type="checkbox"/> sg-5722f82c	open-port-80	vpc-51238934	Open port 80 for http traffic	Copy to new
sg-2538ae42	rds-launch-wizard	vpc-51238934	Created from the RDS Management Console	Copy to new

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

Type <i>(i)</i>	Protocol <i>(i)</i>	Port Range <i>(i)</i>	Source <i>(i)</i>
HTTP	TCP	80	0.0.0.0/0

Cancel Previous Review

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 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 steps are numbered 1. Choose AMI through 6. Review, with step 5. Configure Security Group currently selected.

AMI Details:

- Amazon Linux AMI 2017.03.0 (HVM), SSD Volume Type - ami-8ca83fec
- Free tier eligible
- Root device type: ebs
- Virtualization Type: hvm

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: No
- Monitoring: No
- IAM role: s3-admin-access
- Tenancy: Shared tenancy (multi-tenant hardware)
- Kernel ID: Use default
- RAM Disk ID: Use default
- User data: `iyEvYmlmL2Jhc2gkexVlIHwZGF0ZSAleQp5dW0gaw5zdGFsbCBodHRwZCAleQpzZXJ2aWhlGh0dIBkiHhN0YXJ0CmNoa2NvbmtZp2yBodHRwZCBvbgo=`
- 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 at the bottom include: Cancel, Previous, Create launch configuration, Feedback, English, and links to Privacy Policy and Terms of Use.

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 'Create Auto Scaling Group' wizard on the AWS Management Console. The current step is '2. Configure scaling policies'. A red box highlights the 'Add new alarm' button in the 'Increase Group Size' policy configuration section.

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 by 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](#)

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 with scaling policies based on CPU Utilization. A modal window titled 'Create Alarm' is overlaid, allowing the configuration of a CloudWatch alarm for CPU Utilization. The alarm settings include:

- Name: Increase Group Size
- Execute policy when: CPU>80%
- Take the action: Add [0] instances
- Instances need: 500 seconds to warm up after each step
- Send a notification to: SKL-Admin (skrodraslab@gmail.com)
- Whenever: Average of CPU Utilization
- Is: <= 10 Percent
- For at least: 2 consecutive period(s) of 5 Minutes
- Name of alarm: awsec2-ProdScaleGroup-High-CPU-Utilization

At the bottom of the modal, there are 'Cancel' and 'Create Alarm' buttons.

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 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=lc;launchConfigurationName=awseb-e-z15h>. The page is titled "Create Auto Scaling Group". It is the third step in a five-step process, indicated by the tabs at the top: 1. Configure Auto Scaling group details, 2. Configure scaling policies, 3. Configure Notifications (which is highlighted), 4. Configure Tags, and 5. Review.

Create Auto Scaling Group
Configure your Auto Scaling group to send notifications to a specified endpoint, such as an email address, whenever a specified event takes place, including: successful launch of an instance, failed instance launch, instance termination, and failed instance termination.

If you created a new topic, check your email for a confirmation message and click the included link to confirm your subscription. Notifications can only be sent to confirmed addresses.

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

Whenever instances:

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

[Add notification](#)

[Cancel](#) [Previous](#) [Review](#) [Next: Configure Tags](#)

[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 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 navigation bar includes 'Services' and 'Resource Groups'. The main content is the 'Create Auto Scaling Group' wizard, step 4: Configure Tags. It displays a table with one row: Key 'Name' and Value 'auto-scale-group-http-server'. There is a checkbox labeled 'Tag New Instances' which is checked. Below the table is a button 'Add tag' and the text '49 remaining'. At the bottom are buttons for 'Cancel', 'Previous', and 'Review'.

Activity - Auto scale group

The screenshot shows the AWS Auto Scaling Group creation wizard at step 5: Review. The page displays the configuration details for the Auto Scaling Group, including group name, size, policies, and notifications.

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-fa9219ff, 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

Cancel Previous Create Auto Scaling group

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

Activity - Auto scale group

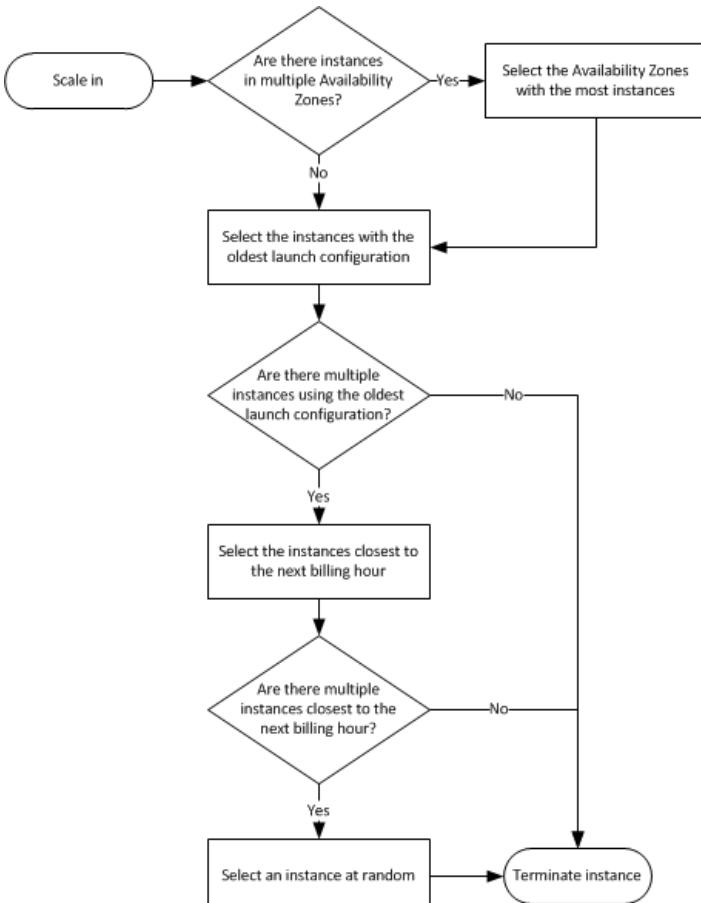
The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation includes 'EC2 Dashboard', 'Events', 'Tags', 'Reports', 'Limits', 'INSTANCES' (selected), 'Instances', 'Spot Requests', 'Reserved Instances', 'Commands', 'Dedicated Hosts', 'IMAGES', 'AMIs', 'Bundle Tasks', 'ELASTIC BLOCK STORE', 'Volumes', 'Snapshots', 'NETWORK & SECURITY', 'Security Groups', 'Elastic IPs', 'Placement Groups', and 'Key Pairs'. The main content area displays a 'Create launch configuration' button, a 'Create Auto Scaling group' button, and an 'Actions' dropdown. A 'Launch Configuration' table shows one entry: 'awseb-e-zl5hc...' with 'ami-63cdd902' as the AMI ID, 't1.micro' as the Instance Type, and a creation time of 'December 16, 2015 11:16:47 A...'. Below the table, the 'Launch Configuration: awseb-e-zl5hc4mezj-stack-AWSEBAutoScalingLaunchConfiguration-LBMY3OYJMZ4N' is detailed. The 'Details' tab is selected, showing the following configuration:

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

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

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: 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. An 'Actions' dropdown menu is open over this row, showing options: 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 in a card format. The card includes fields for 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.

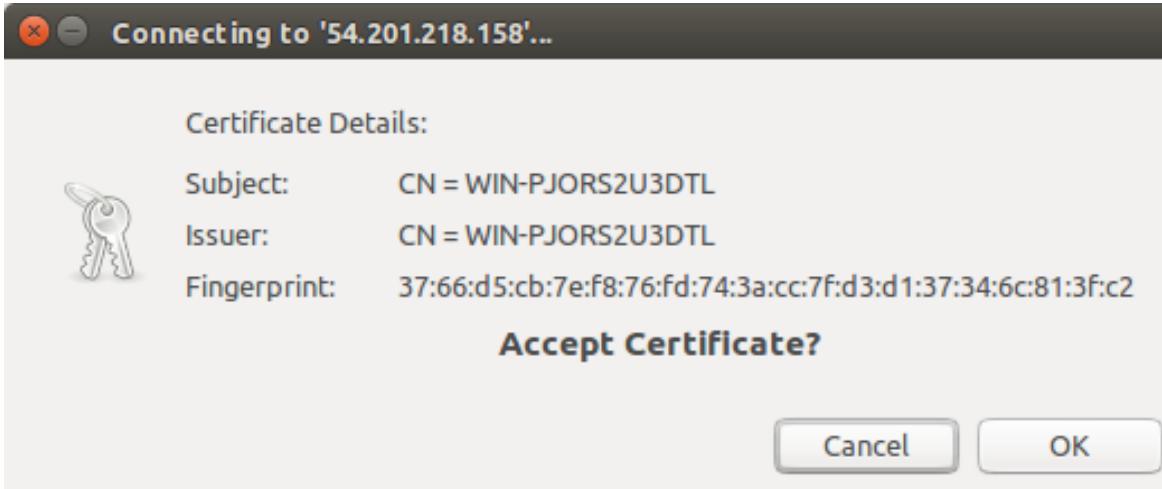
Activity - Windows EC2 instance

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 with status "Public" and IP 54.201.

Activity - Windows EC2 instance

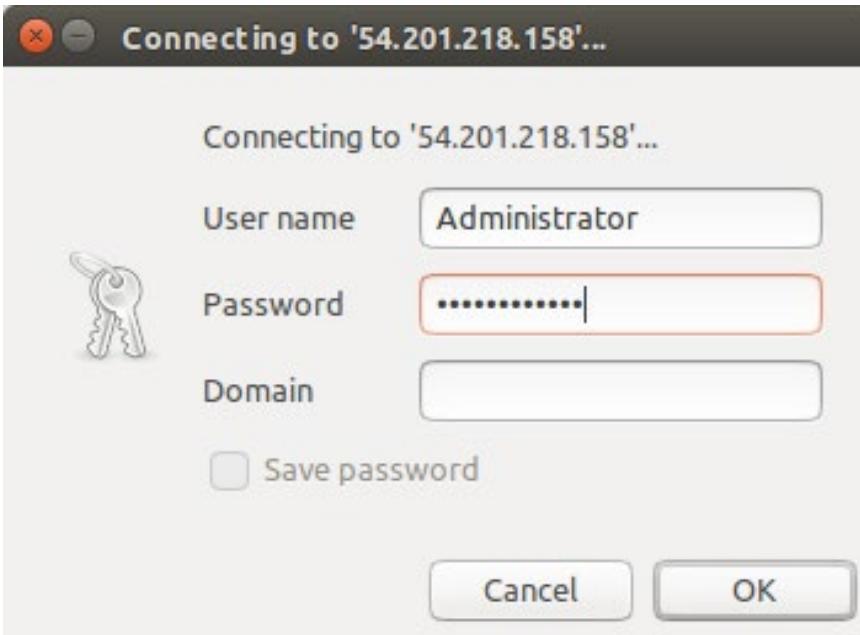
The screenshot shows the AWS EC2 Management Console interface. On the left, the navigation menu includes options like EC2 Dashboard, Instances, AMIs, and Network & Security. The main content area displays a list of instances, with one instance selected. A modal dialog box titled "Retrieve Default Windows Administrator Password" is open in the center. The dialog contains two sections: a green box stating "Password Decryption Successful" followed by the message "The password for instance i-71af84b5 (Windows12) was successfully decrypted." Below this, an orange box contains a warning message: "Password change recommended" with the text "We recommend that you change your default password. Note: If a default password is changed, it cannot be retrieved through this tool. It's important that you change your password to one that you will remember." At the bottom of the dialog, there is a section for remote connection information: "Public IP 54.201.218.158", "User name administrator", and "Password%tSNkbw8sF". A "Close" button is located at the bottom right of the dialog. The background shows a list of three instances with their public DNS names and IP addresses.

Activity - Windows EC2 instance

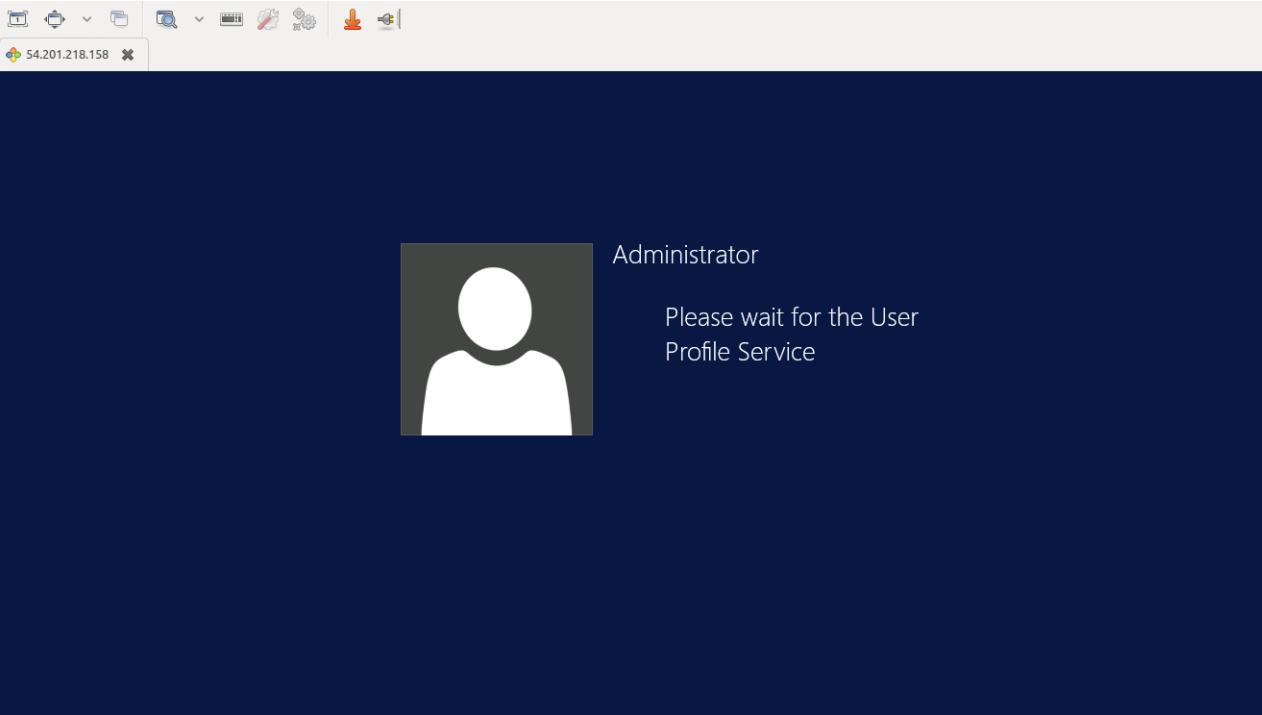


Total 0 items.

Activity - Windows EC2 instance



Activity - Windows EC2 instance



Activity - Windows EC2 instance

