

Amazon

Web Services

C3 SCHOOLS

MANOJ ENTERPRISES & XEROX

All soft ware institute materials, spiral-binding,

Printouts & stationery also available ..,

Contact:8125378496

Add: Plot No.40, Gayatri Nagar, Behind HUDA, mithrivannam, HYD.



|| C3 SCHOOLS

How-to Create a New EC2 Instance Key Pair

1. Use the below URL for login to AWS account.

<http://aws.amazon.com/>

The screenshot shows the AWS homepage. At the top, there's a navigation bar with 'Menu', the AWS logo, and links for 'Products', 'Solutions', 'Pricing', 'Software', 'More', 'English', 'My Account', and 'Create an AWS Account'. Below the navigation, there's a large graphic of a server rack inside a cloud. To the left, text reads 'Get started with Amazon EC2 for Microsoft Windows Server' and 'Register for free hands-on lab ». To the right, there's a box titled 'Get Started with AWS for Free' with a 'Create a Free Account' button, information about Amazon RDS and Amazon EBS, and a link to 'View AWS Free Tier Details »'.

2. Login to your AWS account.

A large, stylized blue graphic spelling 'AWS CRUNCH!' contains the AWS logo at its center. The 'A' is on the left, the 'W' is on the right, and the 'S' is on the far right.

Sign In or Create an AWS Account

What is your e-mail or mobile number?

E-mail or mobile number:

mohan.solaris0606@gmail.com

I am a new user.

I am a returning user
and my password is:

[Sign in using our secure server](#)

[Forgot your password?](#)

New AWS Accounts Include:

12 months of access to the AWS Free Tier

Amazon EC2: 750 hrs/month of Windows and Linux t2.micro instance usage
Amazon S3: 5GBs of Storage
Amazon RDS: 750 hrs/month of Micro DB Instance usage
Amazon DynamoDB: 25 GB of storage, up to 200 million requests/month

AWS Basic Support Features

Customer Service: 24x7x365
Support Forums
Documentation, White Papers, and Best Practice Guides

Visit aws.amazon.com/free for full offer terms.

Learn more about [AWS Identity and Access Management](#) and [AWS Multi-Factor Authentication](#), features that provide additional security for your AWS Account. View full [AWS Free Usage Tier](#) offer terms.

3. Go to AWS Management console:-



|| C3 SCHOOLS

5. Select EC2 from above mentioned services.

6. Select any of the regions from the left hand side drop down. E.g. we have selected 'US-West (Oregon)'.

The screenshot shows the AWS EC2 Dashboard. The left sidebar lists navigation options: EC2 Dashboard, Events, Tags, Reports, Limits, Instances (with sub-options Instances, Spot Requests, Reserved Instances), Images (with sub-options AMIs, Bundle Tasks), and Elastic Block Store (with sub-options Volumes, Snapshots). The main content area is titled 'Resources' and displays the following summary for the US West (Oregon) region:

0 Running Instances	0 Elastic IPs
0 Volumes	0 Snapshots
1 Key Pairs	0 Load Balancers
0 Placement Groups	1 Security Groups

A callout box at the bottom of this section says: "Automate application deployments to EC2 with [CodeDeploy](#)." There is a 'Hide' link next to it. Below this is a 'Create Instance' section with a 'Launch Instance' button. A note below the button states: "To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance." To the right of this is a 'Service Health' section and a 'Scheduled Events' section. The 'Service Status' table shows "US West (Oregon)" operating normally. The 'Scheduled Events' table shows "No events".

7. It will list summary of all EC2 activities like number of running instances, EBS volumes, ElasticIPs etc.



|| C3 SCHOOLS

S Services ▾ Edit ▾ dxd at edureka ▾ Oregon ▾ Help ▾

EC2 Dashboard

Events

Tags

Reports

INSTANCES

Instances

Spot Requests

Reserved Instances

IMAGES

AMIs

Bundle Tasks

ELASTIC BLOCK STORE

Volumes

Snapshots

NETWORK & SECURITY

Security Groups

Elastic IPs

Placement Groups

Available Tags

Resources

You are using the following Amazon EC2 resources in the US West (Oregon) region.

0 Running Instances 0 Elastic IPs 0 Snapshots
0 Volumes 20 Key Pairs 0 Load Balancers
0 Placement Groups 15 Security Groups

Optimize your resources' cost, performance and security with [AWS Trusted Advisor](#) Hide

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-cfab8aa7

Additional Information

Getting Started Guide

Documentation

All EC2 Resources

Forums

Pricing

Contact Us

Popular AMIs on AWS Marketplace

Vyatta Virtual Router/Firewall/VPN
Provided by Vyatta, Inc.
Rating **★★★★★**
Pay by the hour for software and AWS

Feedback

© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

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

8. Select “Key Pairs” from left menu. (EC2 Dashboard). Here will appear all your AWS existing key pairs. If none click to create the first.



|| C3 SCHOOLS

The screenshot shows the AWS Management Console with the 'Services' menu open. Under the 'Compute' section, 'Key Pairs' is selected. On the right, a table lists existing key pairs. A blue box highlights the 'Create Key Pair' button at the top of the table.

Key pair name	Fingerprint
rk	cb:3c:b0:af:0f:5f:eb:20:51:e6:95:8b:7c:f6:04:ea:dc:80:bc:9b

9. Click on 'Create Key Pair' button. Enter the logical name of **key pair you want to create**.

The screenshot shows the 'Create Key Pair' dialog box. The 'Key pair name' field contains 'MNAWS'. The 'Create' button is highlighted with a blue oval.

MNAWS

Create

Key Pair
Key pair name rk Fingerprint cb:3c:b0:af:0f:5f:eb:20:51:e6:95:8b:7c:f6:04:ea:dc:80:bc:9b

10. AWS will create a new key-pair with name 'MNAWS' and it will ask you to download the newly generated private key file (here MNAWS.pem).



|| C3 SCHOOLS

The screenshot shows the AWS Management Console with the 'Key Pairs' section selected in the sidebar. A key pair named 'MNAWS' is listed with its fingerprint. To the right, a file explorer window shows a file named 'MNAWS.pem' in the 'Downloads' folder, which is highlighted with a blue oval.

Key pair name	Fingerprint
MNAWS	22:fd:11:11:5a:8e:7f:54:b4:3e:c7:9b:25:81:d2:d3:cf:0d:cf:31
rk	cb:3c:b0:af:0f:5f:eb:20:51:e6:95:8b:7c:f6:04:ea:dc:80:bc:9b

Key Pair: MNAWS

Key pair name: MNAWS
Fingerprint: 22:fd:11:11:5a:8e:7f:54:b4:3e:c7:9b:25:81:d2:d3:cf:0d:cf:31

NOTE:

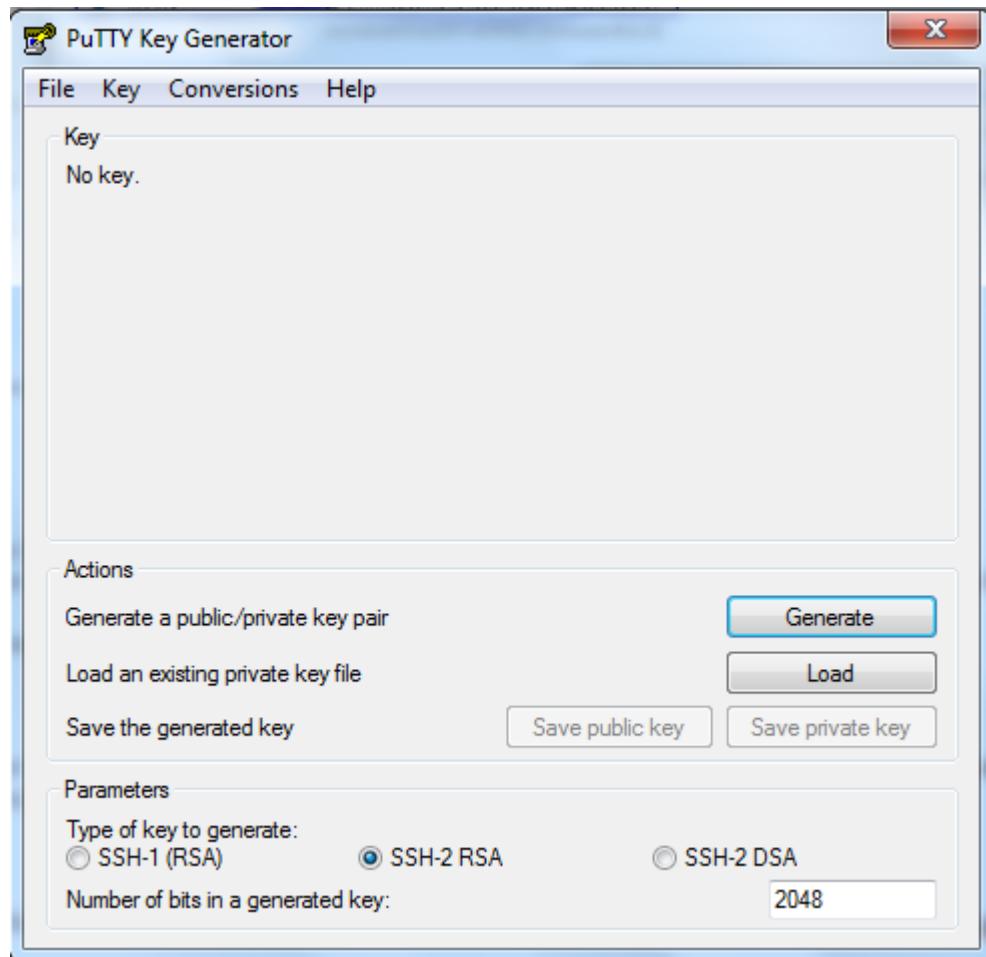
1. If you lose the key you will never be able to get it back.
2. If you have launched an instance with a key pair and by mistake you lost the key, you will not be able to login to the same instance using same key.

11. As shown above you have created the key-pair file which can be used when you want to make secure instance launch.

12. To windows instance or for windows machine, we need to convert it from .pem format to .ppk format using puttygen.



|| C3 SCHOOLS



How to Manage a Security Group on AWS Cloud

1. Go to the AWS Console through the URL <http://aws.amazon.com/console>. Select the EC2 service.



|| C3 SCHOOLS

AWS | Services | Edit

Amazon Web Services

Compute

- EC2 Virtual Servers in the Cloud
- Lambda Run Code in Response to Events
- EC2 Container Service Run and Manage Docker Containers

Storage & Content Delivery

- S3 Scalable Storage in the Cloud
- Elastic File System PREVIEW Fully Managed File System for EC2
- Storage Gateway Integrates On-Premises IT Environments with Cloud Storage
- Glacier Archive Storage in the Cloud
- CloudFront Global Content Delivery Network

Database

- RDS MySQL, Postgres, Oracle, SQL Server, and Amazon Aurora
- DynamoDB Predictable and Scalable NoSQL Data Store
- ElastiCache In-Memory Cache
- Redshift Managed Petabyte-Scale Data Warehouse Service

Administration & Security

- Directory Service Managed Directories in the Cloud
- Identity & Access Management Access Control and Key Management
- Trusted Advisor AWS Cloud Optimization Expert
- CloudTrail User Activity and Change Tracking
- Config Resource Configurations and Inventory
- CloudWatch Resource and Application Monitoring
- Service Catalog Personalized Catalog of AWS Resources

Application Services

- SQS Message Queue Service
- SWF Workflow Service for Coordinating Application Components
- AppStream Low Latency Application Streaming
- Elastic Transcoder Easy-to-use Scalable Media Transcoding
- SES Email Sending Service
- CloudSearch Managed Search Service
- API Gateway Build, Deploy and Manage APIs

Deployment & Management

- Elastic Beanstalk AWS Application Container
- OpsWorks DevOps Application Management Service
- CloudFormation Templated AWS Resource Creation
- CodeDeploy Automated Deployments
- CodeCommit Managed Git Repositories
- CodePipeline Continuous Delivery

Mobile Services

- Cognito User Identity and App Data Synchronization
- Device Farm Test Android, Fire OS, and iOS apps on real devices in the Cloud
- Mobile Analytics Collect, View and Export App Analytics
- SNS Push Notification Service

Enterprise Applications

- WorkSpaces Desktops in the Cloud

2. Select security groups from the EC2 dashboard.

AWS | Services | Edit

Resources

You are using the following Amazon EC2 resources in the US West (Oregon) region:

0 Running Instances	0 Elastic IPs
0 Volumes	0 Snapshots
1 Key Pairs	0 Load Balancers
0 Placement Groups	1 Security Groups

Automate application deployments to EC2 with [CodeDeploy](#). Hide

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

Availability Zone Status:

- us-west-2a: Availability zone is operating normally

Scheduled Events

US West (Oregon):
No events



|| C3 SCHOOLS

3. The Security Group console shows all the existing security groups of that region. Click on the “Create Security Group” button.

The screenshot shows the AWS Management Console with the AWS logo at the top left. The navigation bar includes 'AWS', 'Services' (with a dropdown arrow), 'Edit', and user information ('Mohan N', 'Oregon', 'Support'). On the left, a sidebar lists 'Reserved Instances', 'AMIs', 'Bundle Tasks', 'Elastic Block Store' (with 'Volumes' and 'Snapshots'), and 'NETWORK & SECURITY' (with 'Security Groups' selected, 'Elastic IPs', 'Placement Groups', 'Key Pairs', and 'Network Interfaces'). The main content area displays a table titled 'Security Groups'. The table has columns: Name, Group ID, Group Name, VPC ID, and Description. One row is visible: 'sg-f3fde396', 'default', 'vpc-7ba5281e', and 'default VPC security group'. Below the table is a search bar with placeholder text 'Filter by tags and attributes or search by keyword'. At the top right of the main content area are icons for refresh, settings, and help.

4. Provide the name of the security group and the description. If the user is launching the instance in VPC then select “VPC”, or else select “No VPC”. Click on “Yes, Create”.

The screenshot shows the 'Create Security Group' dialog box. At the top, it says 'Create Security Group' and has a close button 'X'. The form fields are:

- Security group name:** Test MN
- Description:** SG Lab
- VPC:** vpc-7ba5281e (172.31.0.0/16) *

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

Security group rules:

Under 'Inbound' (which is selected), there are tabs for 'Type', 'Protocol', 'Port Range', and 'Source'. A note below the tabs says 'This security group has no rules'. There is a 'Add Rule' button.

At the bottom right of the dialog are 'Cancel' and 'Create' buttons.

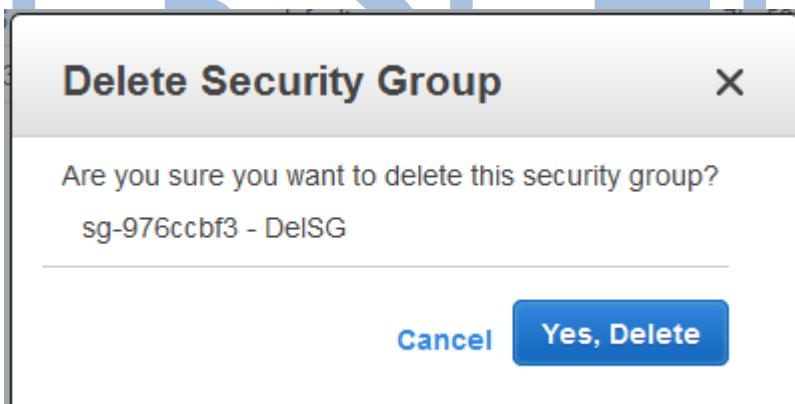


|| C3 SCHOOLS

5. The security group will be created and available in the Security Group console. To delete a security group, select the security group, go to actions and click on “Delete Security Group”.

Name	Group ID	Group Name	VPC ID	Description
sg-976ccbf3	DelSG	vpc-7ba5281e	For Deleting	
sg-f3fde396	default	vpc-7ba5281e	default VPC security group	
sg-f76ccb93	Test MN	vpc-7ba5281e	SG Lab	

6. AWS will ask for a confirmation before deleting the security group. Click on “Yes, Delete”.



7. The group will be deleted immediately and removed from the AWS Security group listing.

Name	Group ID	Group Name	VPC ID	Description
sg-f3fde396	default	vpc-7ba5281e	default VPC security group	
sg-f76ccb93	Test MN	vpc-7ba5281e	SG Lab	

8. If a security group is assigned to some instance, AWS will not allow for deleting that security group.



|| C3 SCHOOLS

Delete Security Groups

Note that the following security groups **cannot be deleted**:

These security groups are **associated with one or more instances**. Terminate the instances, or associate them with different security groups (VPC only). [View your associated instances](#).

sg-f76ccb93 - Test MN

[Cancel](#) [Yes, Delete](#)

How to Launch an Amazon AWS EC2 Instance

1. Login to your [AWS Console](#) and select the EC2 Service. It launches the EC2 dashboard. The dashboard shows the current running instances, the available elastic IPs, volumes, snapshots and other details. Click on “**Launch Instance**” to launch the EC2 instance.

The screenshot shows the AWS EC2 Dashboard. The left sidebar lists navigation options: EC2 Dashboard, Events, Tags, Reports, Limits, Instances (with sub-options Instances, Spot Requests, Reserved Instances), Images (with sub-options AMIs, Bundle Tasks), Elastic Block Store (with sub-options Volumes, Snapshots), and Network & Security (with sub-options Security Groups, Elastic IPs, Placement Groups). The main content area is titled "Resources" and displays statistics for the US West (Oregon) region: 0 Running Instances, 0 Elastic IPs, 0 Volumes, 0 Snapshots, 1 Key Pairs, 0 Load Balancers, 0 Placement Groups, and 2 Security Groups. A callout box suggests automating deployments with CodeDeploy. Below this is a "Create Instance" section with a "Launch Instance" button. A note states that instances will launch in the US West (Oregon) region. The "Service Health" and "Scheduled Events" sections show normal service status and no scheduled events respectively.

2. Select the AMI. The AWS Launch screen provides multiple options to select AMI. The user can select the AMIs provided by AWS (Standard OS), Select “My AMIs” to launch the instance from the user’s existing AMIs or select community AMIs to launch the instance from various providers (may or may not be authorized by AWS).



|| C3 SCHOOLS

AWS | Services | Edit | Mohan N | Oregon | Support

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

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					1 to 22 of 22 AMIs	
<input type="checkbox"/> My AMIs	Amazon Linux AMI 2015.03 (HVM), SSD Volume Type - ami-e7527ed7	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.			<input type="button" value="Select"/>	64-bit
<input type="checkbox"/> AWS Marketplace	Red Hat Enterprise Linux 7.1 (HVM), SSD Volume Type - ami-4dbf9e7d	Red Hat Enterprise Linux version 7.1 (HVM), EBS General Purpose (SSD) Volume Type			<input type="button" value="Select"/>	64-bit
<input type="checkbox"/> Community AMIs	SUSE Linux Enterprise Server 12 (HVM), SSD Volume Type - ami-d7450be7	SUSE Linux Enterprise Server 12 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.			<input type="button" value="Select"/>	64-bit
<input type="checkbox"/> Free tier only						

3. The various instance types are shown in the figure given below. Select the t2 Micro and click on the “Next configuration setting” button.

AWS | Services | Edit | Mohan N | 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 2: Choose an Instance Type

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

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
<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
<input type="checkbox"/>	General purpose	m4.xlarge	4	16	EBS only	Yes	High

4. Provide IAM role None and click on Next:Add Storage.



|| C3 SCHOOLS

AWS Services Edit Mohan N 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	1
Purchasing option	<input type="checkbox"/> Request Spot Instances
Network	vpc-7ba5281e (172.31.0.0/16) (default)
Subnet	No preference (default subnet in any Availability Zone)
Auto-assign Public IP	Use subnet setting (Enable)
IAM role	None
Shutdown behavior	Stop
Enable termination protection	<input type="checkbox"/> Protect against accidental termination
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring

Cancel **Previous** **Review and Launch** **Next: Add Storage**

5. Provide the storage related information. Click on “Add New Volume” to Add new Volume and can Delete by Cross button.

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-bfb086e1	8	General Purpose (SSD)	24 / 3000	<input checked="" type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	Search (case-insensitive)	8	General Purpose (SSD)	24 / 3000	<input type="checkbox"/>	Not Encrypted

Add New Volume

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

6. Provide the Root Volume Size (cannot be less than 8 GB for Linux) and Volume Type Standard.

7. Provide the tags for the AWS instance. Tagging is very useful when the user wants to track the cost of a particular instance / service.



|| C3 SCHOOLS

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key	(127 characters maximum)	Value	(255 characters maximum)
Name		TestLab	X

Create Tag (Up to 10 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

8. For the security of the instance, select the existing key-pair.

For Existing Key-Pair

Assign a security group: Create a new security group Select an existing security group

Security Group ID	Name	Description	Actions
sg-f3fde396	default	default VPC security group	Copy to new
sg-f76ccb93	Test MN	SG Lab	Copy to new

Inbound rules for sg-f76ccb93

Type	Protocol	Port Range	Source
This security group has no rules			

Cancel Previous Review and Launch

9. Select the security group. The security group provides the virtual firewall for the user's instance. Open only the ports for the specific IPs as per the user's requirement. Click on "Review and Launch".



|| C3 SCHOOLS

AWS | Services | Edit | Mohan N | 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 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 ID	Name	Description	Actions
sg-f3fde396	default	default VPC security group	Copy to new
sg-f76ccb93	Test MN	SG Lab	Copy to new

Inbound rules for sg-f76ccb93 (Selected security groups: sg-f76ccb93)

Type	Protocol	Port Range	Source
This security group has no rules			

Cancel | Previous | **Review and Launch**

10. Review all the details and click on “Launch”.

AWS | Services | Edit | Mohan N | 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 7: Review Instance Launch

AMI Details

Amazon Linux AMI 2015.03 (HVM), SSD Volume Type - ami-e7527ed7
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.
Free tier eligible
Root Device Type: ebs Virtualization type: hvm

Instance Type

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

Security Groups

Security Group ID	Name	Description
sg-f76ccb93	Test MN	SG Lab

All selected security groups inbound rules

Cancel | Previous | **Launch**

11. AWS will launch the instance and provide the user with the ID of the instance.



|| C3 SCHOOLS

Select an existing key pair or create a new key pair

X

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

Select a key pair

MNAWS

I acknowledge that I have access to the selected private key file (MNAWS.pem), and that without this file, I won't be able to log into my instance.

Cancel

Launch Instances



Launch Status

[Get notified or 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).

How to connect to your instances

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.

▼ Here are some helpful resources to get you started

- [How to connect to your Linux instance](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: User Guide](#)
- [Amazon EC2: Discussion Forum](#)

While your instances are launching you can also

- [Create status check alarms](#) to be notified when these instances fail status checks. (Additional charges may apply)
- [Create and attach additional EBS volumes](#) (Additional charges may apply)
- [Manage security groups](#)

[View Instances](#)



|| C3 SCHOOLS

12. Go to the AWS EC2 console and it will display the new instance. The instance will be first in a running State. **It is advisable to connect to** the instance once the status checks are in “2/2 Checks”.

The screenshot shows the AWS EC2 Instances page. The navigation bar at the top includes 'AWS', 'Services', 'Edit', and user information 'Mohan N | Oregon | Support'. On the left, a sidebar lists 'EC2 Dashboard', 'Events', 'Tags', 'Reports', 'Limits', 'INSTANCES' (with 'Instances' selected), 'Spot Requests', and 'Reserved Instances'. The main content area has tabs 'Launch Instance', 'Connect', and 'Actions'. A search bar says 'Filter by tags and attributes or search by keyword'. Below is a table with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, and Public DNS. One row is shown: 'TestLab' (i-852da840, t2.micro, us-west-2b, running, 2/2 checks, None, ec2-52-26-159-46.us-w...).

13. Previously, it was showing 0 running instance on EC2 Dashboard. Now it is showing running instance 1.

The screenshot shows the AWS EC2 Dashboard. The navigation bar at the top includes 'AWS', 'Services', 'Edit', and user information 'Mohan N | Oregon | Support'. On the left, a sidebar lists 'EC2 Dashboard' (selected), 'Events', 'Tags', 'Reports', 'Limits', 'INSTANCES' (with 'Instances' selected), 'Spot Requests', 'Reserved Instances', 'IMAGES' (with 'AMIs' selected), 'Bundle Tasks', 'ELASTIC BLOCK STORE' (with 'Volumes' selected), 'NETWORK & SECURITY' (with 'Security Groups' selected). The main content area has sections 'Resources' (showing 1 Running Instances, 0 Elastic IPs, etc.), 'Create Instance' (with 'Launch Instance' button), 'Service Health' (with 'Service Status' and 'Availability Zone Status' sections), and 'Scheduled Events' (showing 'US West (Oregon)' with 'No events').



|| C3 SCHOOLS

How to Connect to AWS Linux Instance from a Windows Machine

1. Launch a new Linux Instance.

The screenshot shows the AWS Quick Start interface for launching a new instance. The top navigation bar includes 'AWS', 'Services', 'Edit', 'Mohan N', 'Oregon', and 'Support'. Below the navigation is a step-by-step progress bar: '1. Choose AMI' (highlighted in orange), '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 on the right. The main area is titled 'Step 1: Choose an Amazon Machine Image (AMI)'. It says, '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.' On the left is a 'Quick Start' sidebar with 'My AMIs', 'AWS Marketplace', 'Community AMIs', and a 'Free tier only' checkbox. The main list shows three AMI options:

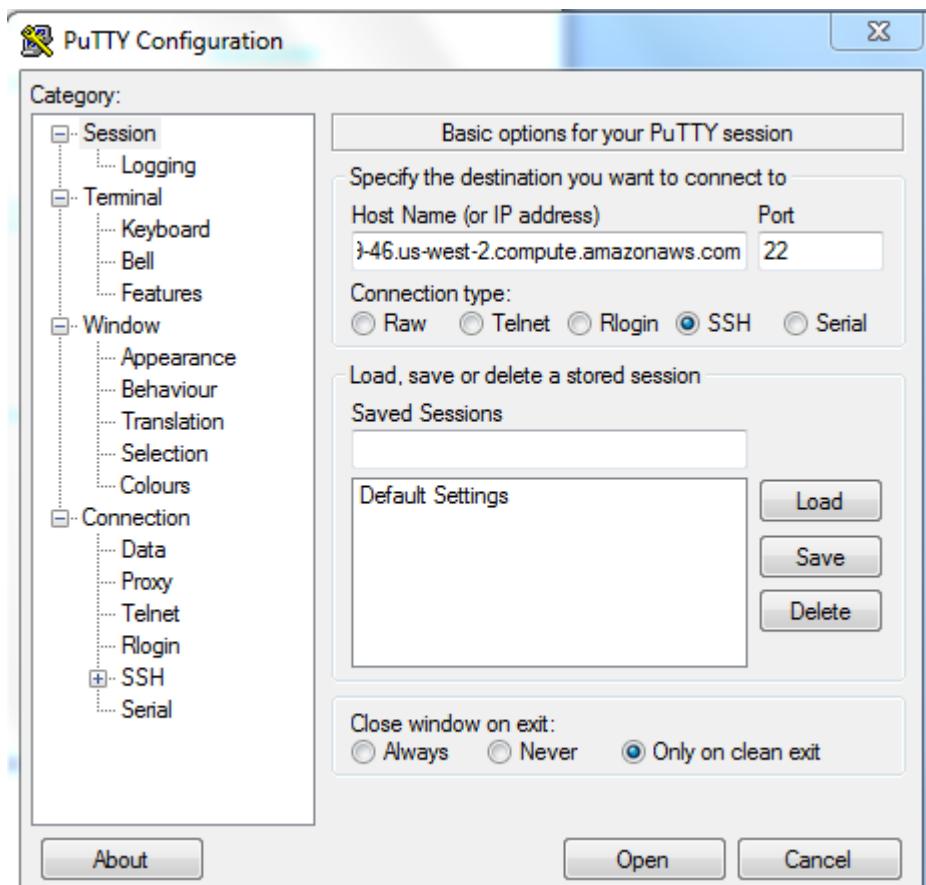
AMI Name	Description	Action	Architecture
Amazon Linux	Amazon Linux AMI 2015.03 (HVM), SSD Volume Type - ami-e7527ed7	Select	64-bit
Red Hat	Red Hat Enterprise Linux 7.1 (HVM), SSD Volume Type - ami-4dbf9e7d	Select	64-bit
SUSE Linux	SUSE Linux Enterprise Server 12 (HVM), SSD Volume Type - ami-d7450be7	Select	64-bit

2. Ensure that you have opened the SSH port 22 for connecting to Linux.

3. Start PuTTy by running **putty.exe**. Enter the public DNS you got in step #4 in the **Host name/IP address** field. Keep the port as 22.



|| C3 SCHOOLS

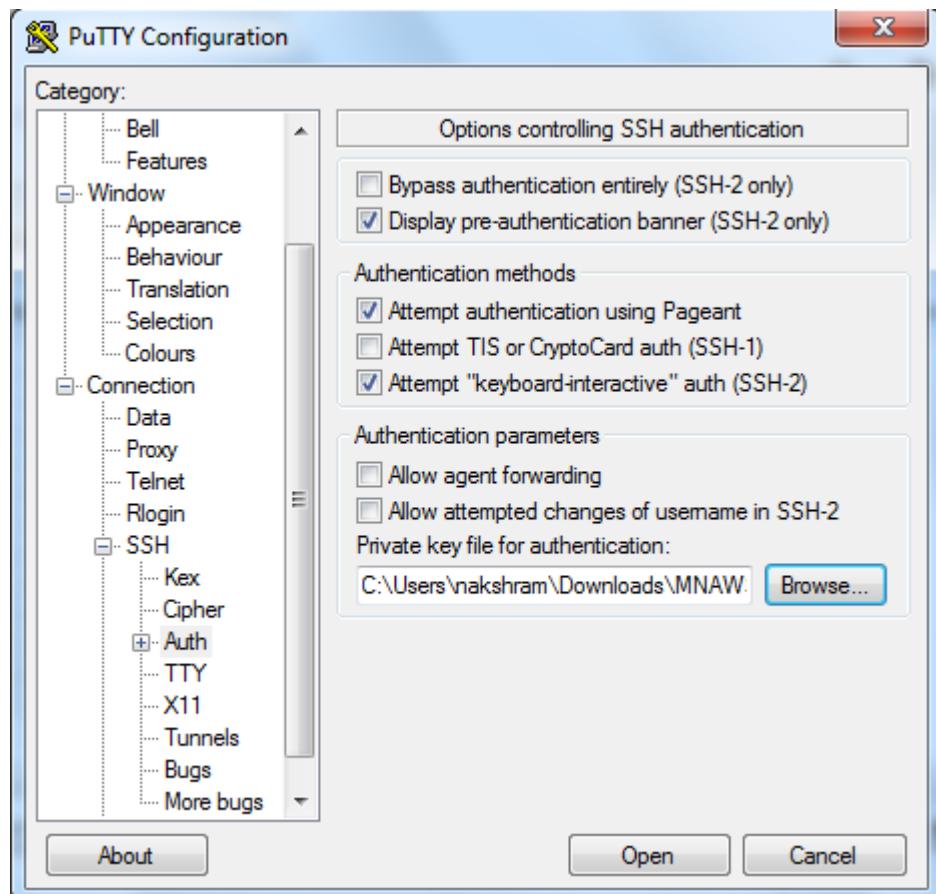


C3 SCHOOLS

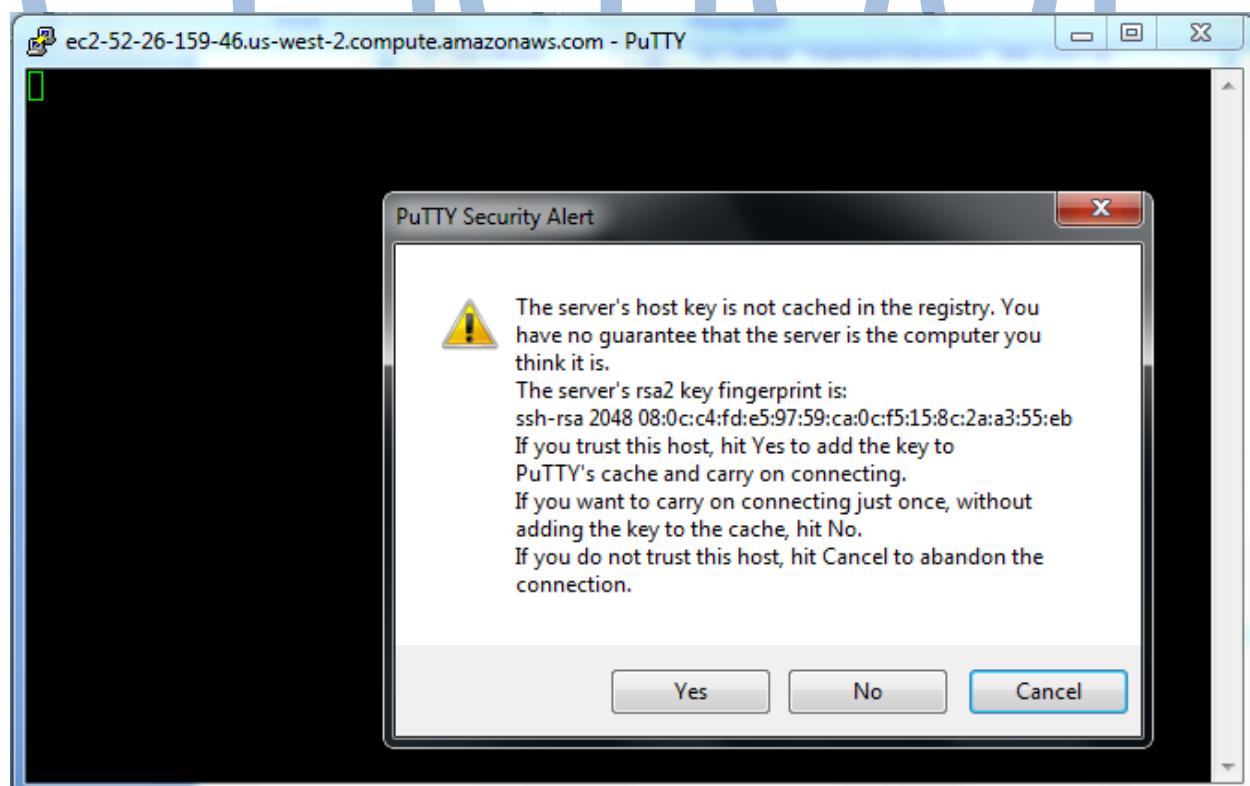
4. In the Category tree, select **SSH >Auth** and then provide the key-pair file we used in launching the instance to connect to the instance.



|| C3 SCHOOLS



5. Click Open. The command window (telnet) is launched to connect to the AWS instance.



6. Click Yes. You are prompted to log in.

7. For an AWS Linux instance, enter **ec2-user** as the username. (Based on your operating system, the



|| C3 SCHOOLS

username might be different.)

```
ec2-user@ip-10-252-26-242:~  
login as: ec2-user  
Authenticating with public key "imported-openssh-key"  
[ec2-user@ip-10-252-26-242 ~]$ [REDACTED]
```

The screenshot shows a terminal window titled "ec2-user@ip-10-252-26-242:~". It displays a successful SSH login with the message "Authenticating with public key 'imported-openssh-key'". Below this, it shows the Amazon Linux AMI logo and a link to the release notes: "https://aws.amazon.com/amazon-linux-ami/2012.03-release-notes/". It also indicates there are 10 security updates available out of 16 total. The command "[ec2-user@ip-10-252-26-242 ~]\$ [REDACTED]" is shown at the bottom.

If you have given the correct IP address, the Linux prompt is displayed as shown above.

Now you can install and manage your application on the server as required.

How to Associate and Disassociate an Elastic IP to an EC2 Instance

1. Go to the [AWS Console](#) and select the EC2 Service. It will list the AWS dashboard. It lists the current running instances, snapshots and elastic IPs. Click on the “Running Instance” link or the “Instances” link in the left navigation menu.

The screenshot shows the AWS EC2 Dashboard. On the left, there is a navigation menu with links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, Elastic Block Store, Network & Security, Load Balancing, Auto Scaling, Commands, and Help. The main content area is titled "Resources" and shows the following statistics for the US West (Oregon) region:

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

Below this, there is a "Create Instance" section with a "Launch Instance" button. To the right, there are sections for "Account Attributes" (Supported Platforms: VPC, Default VPC: none), "Additional Information" (Getting Started Guide, Documentation, All EC2 Resources, Forums, Pricing, Contact Us), and "AWS Marketplace" (Tableau Server (10 users), SAP HANA One 244GB, TIBCO Spotfire® Analytics Platform (Hourly)). At the bottom, there are sections for "Service Health" (US West (Oregon) status: operating normally) and "Scheduled Events" (US West (Oregon): No events).



|| C3 SCHOOLS

2. The [EC2 Instances](#) dashboard displays all the instances of that region. When the instance is launched, AWS assigns a public IP to the instance.

The screenshot shows the AWS EC2 Instances details page for an instance named 'i-0de2e9dc82db04140 (AWSchefserver)'. The Public DNS is highlighted in a red box and is shown as 'ec2-54-169-156-93.ap-southeast-1.compute.amazonaws.com'. The instance is running an t2.micro instance type with a private IP of 172.31.28.64 and a public IP of 54.169.156.93. It is located in the ap-southeast-1a availability zone and belongs to the 'sngsg' security group. The instance was launched using the 'amzn-ami-hvm-2016.03.3.x86_64-gp2 (ami-a59b49c6)' AMI. The instance has a VPC ID of vpc-30f4f655 and a subnet ID of subnet-15789363. The network interface is eth0 and the source/dest check is set to True. There are no scheduled events or IAM roles assigned.

Attribute	Value
Instance ID	i-0de2e9dc82db04140
Instance state	running
Instance type	t2.micro
Private DNS	ip-172-31-28-64.ap-southeast-1.compute.internal
Private IPs	172.31.28.64
Secondary private IPs	
VPC ID	vpc-30f4f655
Subnet ID	subnet-15789363
Network interfaces	eth0
Source/dest check	True
Public DNS	ec2-54-169-156-93.ap-southeast-1.compute.amazonaws.com
Public IP	54.169.156.93
Elastic IPs	-
Availability zone	ap-southeast-1a
Security groups	sngsg, view rules
Scheduled events	No scheduled events
AMI ID	amzn-ami-hvm-2016.03.3.x86_64-gp2 (ami-a59b49c6)
Platform	-
IAM role	-
Custom name	awschef

C3 SCHOOLS



|| C3 SCHOOLS

3. Go to Elastic IP dashboard by clicking on the “Elastic IP” in step#1. It lists all the Elastic IPs of that region. Select an elastic IP to be assigned to the instance and click on the “Associate Address” button.

The screenshot shows the AWS Elastic IP dashboard. At the top, there are buttons for "Allocate New Address" and "Actions". A dropdown menu is open under "Actions" with options: "Allocate New Address", "Release Addresses", and "Associate Address" (which is highlighted with a blue border). Below the menu, there is a search bar labeled "Filter by attributes or see" and two rows of results. The first row has a checkbox for "Elastic IP" and the value "52.76.175.104". The second row has a checkbox for "Disassociate Address" and the value "eipalloc-5d77ee38". To the right of these rows are dropdown menus for "Instance" and "Private IP Address".

4. It asks for the instance which will be associated with this IP. Select the instance from the list and click on “Yes, Associate”.

Select the instance OR network interface to which you wish to associate this IP address (52.76.175.104)

Instance i-0de2e9dc82db04140

Or

Network Interface

Search network interface ID or Name tag

Private IP Address

172.31.28.64* - 54.169.156.93

Reassociation

(i)

(i)



Warning

If you associate an Elastic IP address with your instance, your current public IP address is released. Learn more about [public IP addresses](#).

[Cancel](#) [Associate](#)

5. It will associate the elastic IP to that instance. Go to Instance dashboard and select the instance. The IP of the instance is updated to the elastic IP.

The screenshot shows the AWS Instance dashboard for instance i-0de2e9dc82db04140. At the top, it says "Instance: i-0de2e9dc82db04140 (AWSchefserver)" and "Elastic IP: 52.76.175.104". Below this, there are tabs for "Description", "Status Checks", "Monitoring", and "Tags". The "Description" tab is selected. It displays various instance details in a table format:

Instance ID	i-0de2e9dc82db04140	Public DNS	ec2-52-76-175-104.ap-southeast-1.compute.amazonaws.com
Instance state	running	Public IP	52.76.175.104
Instance type	t2.micro	Elastic IPs	52.76.175.104*
Private DNS	ip-172-31-28-64.ap-southeast-1.compute.internal	Availability zone	ap-southeast-1a
Private IPs	172.31.28.64	Security groups	sngsg, view rules
Secondary private IPs		Scheduled events	No scheduled events
VPC ID	vpc-30f4f655	AMI ID	amzn-ami-hvm-2016.03.3.x86_64-gp2 (a59b49c6)
Subnet ID	subnet-15789363	Platform	-
Network interfaces	eth0	IAM role	-
Source/dest. check	True	Key pair name	sngkey

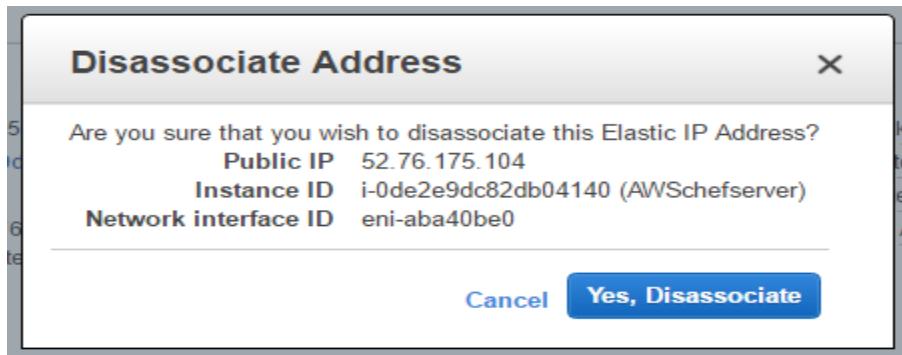


|| C3 SCHOOLS

6. To disassociate the instance, Go to Elastic IP dashboard by clicking on the “Elastic IP” in step#1. It lists all the Elastic IPs of that region. Select an elastic IP to be the instance and click on “Disassociate Address” from the Actions menu.

The screenshot shows the AWS Elastic IP dashboard. In the top left, there's a blue button labeled "Allocate New Address". Below it, a search bar says "Filter by attributes or service name". On the right, there's a "Actions" dropdown menu with options: "Allocate New Address", "Release Addresses", "Associate Address", and "Disassociate Address". The "Disassociate Address" option is highlighted with a blue box. The main table lists one item: "Elastic IP" (checkbox), "52.76.175.104" (IP address), "eipalloc-5d77ee38" (Allocation ID), "i-0de2e9dc82db04140 (AWSchefserver)" (Instance ID), and "172.31.28.64" (Private IP Address).

7. AWS will ask for a confirmation before disassociating the address. Click on “Yes, Disassociate”.



8. The elastic IP address associated with the instance will be disassociated. The above mentioned IP can be reassigned to any other instance. If the IP address is unassigned, it will cost the user. Release the IP address if the user does not require it.

The figure given below demonstrates the instance with the new public IP after the elastic IP has been disassociated.



|| C3 SCHOOLS

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	Pub
AWSchefser...	i-0de2e9dc82db04140	t2.micro	ap-southeast-1a	running	2/2 checks ...	None	ec2-54-169-235-239....	54.1

Instance: i-0de2e9dc82db04140 (AWSchefserver) Public DNS: ec2-54-169-235-239.ap-southeast-1.compute.amazonaws.com

Description Status Checks Monitoring Tags

Instance ID	i-0de2e9dc82db04140	Public DNS	ec2-54-169-235-239.ap-southeast-1.compute.amazonaws.com
Instance state	running	Public IP	54.169.235.239
Instance type	t2.micro	Elastic IPs	
Private DNS	ip-172-31-28-64.ap-southeast-1.compute.internal	Availability zone	ap-southeast-1a
Private IPs	172.31.28.64	Security groups	sngsg, view rules
Secondary private IPs		Scheduled events	No scheduled events
VPC ID	vpc-30f4f655	AMI ID	amzn-ami-hvm-2016.03.3.x86_64-gp2 (ami-a59b49c6)

How to Manage a Security Group on AWS Cloud

1. Go to the AWS Console through the URL <http://aws.amazon.com/console>. Select the EC2 service.



|| C3 SCHOOLS

AWS | Services | Edit

Amazon Web Services

Compute EC2 Virtual Servers in the Cloud Lambda Run Code in Response to Events EC2 Container Service Run and Manage Docker Containers	Administration & Security Directory Service Managed Directories in the Cloud Identity & Access Management Access Control and Key Management Trusted Advisor AWS Cloud Optimization Expert CloudTrail User Activity and Change Tracking Config Resource Configurations and Inventory CloudWatch Resource and Application Monitoring Service Catalog Personalized Catalog of AWS Resources	Application Services SQS Message Queue Service SWF Workflow Service for Coordinating Application Components AppStream Low Latency Application Streaming Elastic Transcoder Easy-to-use Scalable Media Transcoding SES Email Sending Service CloudSearch Managed Search Service API Gateway Build, Deploy and Manage APIs
Storage & Content Delivery S3 Scalable Storage in the Cloud Elastic File System <small>PREVIEW</small> Fully Managed File System for EC2 Storage Gateway Integrates On-Premises IT Environments with Cloud Storage Glacier Archive Storage in the Cloud CloudFront Global Content Delivery Network	Deployment & Management Elastic Beanstalk AWS Application Container OpsWorks DevOps Application Management Service CloudFormation Templated AWS Resource Creation CodeDeploy Automated Deployments CodeCommit Managed Git Repositories CodePipeline Continuous Delivery	Mobile Services Cognito User Identity and App Data Synchronization Device Farm Test Android, Fire OS, and iOS apps on real devices in the Cloud Mobile Analytics Collect, View and Export App Analytics SNS Push Notification Service
Database RDS MySQL, Postgres, Oracle, SQL Server, and Amazon Aurora DynamoDB Predictable and Scalable NoSQL Data Store ElastiCache In-Memory Cache Redshift Managed Petabyte-Scale Data Warehouse Service		Enterprise Applications WorkSpaces Desktops in the Cloud

2. Select security groups from the EC2 dashboard.



|| C3 SCHOOLS

Spot Requests
Reserved Instances

IMAGES
AMIs
Bundle Tasks

ELASTIC BLOCK STORE
Volumes
Snapshots

NETWORK & SECURITY
Security Groups (circled)
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces

LOAD BALANCING
Load Balancers

AUTO SCALING
Launch
Configurations
Auto Scaling Groups

Resources

You are using the following Amazon EC2 resources in the US West (Oregon) region:

0 Running Instances	0 Elastic IPs
0 Volumes	0 Snapshots
1 Key Pairs	0 Load Balancers
0 Placement Groups	1 Security Groups (circled)

Automate application deployments to EC2 with [CodeDeploy](#). Hide

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 **Scheduled Events**

Service Status:
 US West (Oregon): This service is operating normally

Availability Zone Status:
 us-west-2a: Availability zone is operating normally

US West (Oregon):
No events

C3 SCHOOLS

3. The Security Group console shows all the existing security groups of that region. Click on the "Create Security Group" button.

AVS Services Edit

Mohan N Oregon Support

Reserved Instances

IMAGES
AMIs
Bundle Tasks

ELASTIC BLOCK STORE
Volumes
Snapshots

NETWORK & SECURITY
Security Groups (highlighted)
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces

Create Security Group

Actions

Filter by tags and attributes or search by keyword

Name	Group ID	Group Name	VPC ID	Description
sg-f3fde396	default	vpc-7ba5281e	default VPC security group	



|| C3 SCHOOLS

4. Provide the name of the security group and the description. If the user is launching the instance in VPC then select “VPC”, or else select “No VPC”. Click on “Yes, Create”.

Create Security Group

Security group name	Test MN
Description	SG Lab
VPC	vpc-7ba5281e (172.31.0.0/16) *

* denotes default VPC

Security group rules:

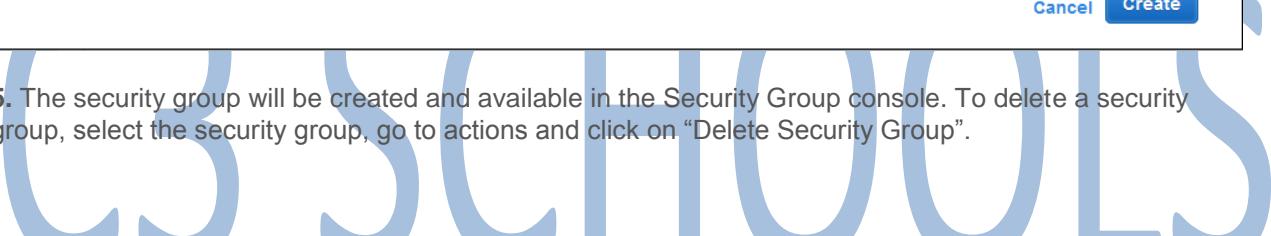
Inbound Outbound

Type	Protocol	Port Range	Source
------	----------	------------	--------

This security group has no rules

Add Rule Cancel Create

5. The security group will be created and available in the Security Group console. To delete a security group, select the security group, go to actions and click on “Delete Security Group”.



Actions				
Create Security Group				
Filter by tags and attributes or search by keyword				
Name	Group ID	Group Name	VPC ID	Description
<input checked="" type="checkbox"/>	sg-976ccbf3	DelSG	vpc-7ba5281e	For Deleting
<input type="checkbox"/>	sg-f3fde396	default	vpc-7ba5281e	default VPC security group
<input type="checkbox"/>	sg-f76ccb93	Test MN	vpc-7ba5281e	SG Lab

6. AWS will ask for a confirmation before deleting the security group. Click on “Yes, Delete”.

Delete Security Group

Are you sure you want to delete this security group?

sg-976ccbf3 - DelSG

Cancel Yes, Delete

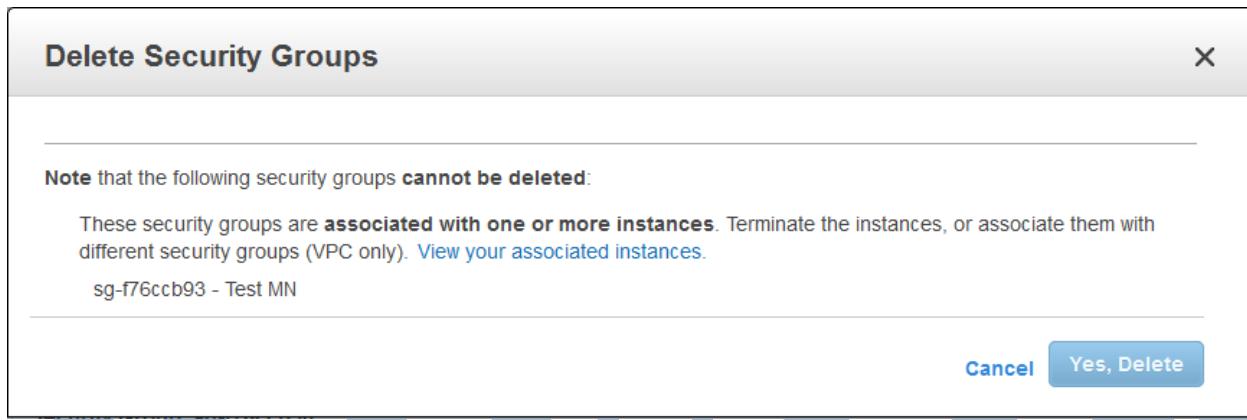


|| C3 SCHOOLS

7. The group will be deleted immediately and removed from the AWS Security group listing.

Filter by tags and attributes or search by keyword				
	Name	Group ID	Group Name	VPC ID
<input type="checkbox"/>	sg-f3fde396		default	vpc-7ba5281e
<input type="checkbox"/>	sg-f76ccb93		Test MN	vpc-7ba5281e

8. If a security group is assigned to some instance, AWS will not allow for deleting that security group.





|| C3 SCHOOLS

How to Launch an Amazon AWS EC2 Instance

1. Login to your [AWS Console](#) and select the EC2 Service. It launches the EC2 dashboard. The dashboard shows the current running instances, the available elastic IPs, volumes, snapshots and other details. Click on “Launch Instance” to launch the EC2 instance.

The screenshot shows the AWS EC2 Dashboard. On the left, there's a navigation sidebar with links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, Elastic Block Store, and Network & Security. The main area is titled "Resources" and displays the following statistics for the US West (Oregon) region:

Category	Value
Running Instances	0
Volumes	0
Key Pairs	1
Placement Groups	0
Elastic IPs	0
Snapshots	0
Load Balancers	0
Security Groups	2

Below the stats, there's a callout for "CodeDeploy" and a note about launching instances in the US West (Oregon) region. The "Create Instance" section has a prominent blue "Launch Instance" button. At the bottom, there are sections for "Service Health" (with a green checkmark for "US West (Oregon): This service is operating normally") and "Scheduled Events" (showing "No events").

2. Select the AMI. The AWS Launch screen provides multiple options to select AMI. The user can select the AMIs provided by AWS (Standard OS), Select “My AMIs” to launch the instance from the user’s existing AMIs or select community AMIs to launch the instance from various providers (may or may not be authorized by AWS).



|| C3 SCHOOLS

AWS Services Edit Mohan N Oregon Support

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

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

Category	AMI Name	Description	Root device type	Virtualization type	Select	Architecture
My AMIs	Amazon Linux AMI 2015.03 (HVM), SSD Volume Type - ami-e7527ed7	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.	ebs	hvm	Select	64-bit
AWS Marketplace	Red Hat Enterprise Linux 7.1 (HVM), SSD Volume Type - ami-4dbf9e7d	Red Hat Enterprise Linux version 7.1 (HVM), EBS General Purpose (SSD) Volume Type	ebs	hvm	Select	64-bit
Community AMIs	SUSE Linux Enterprise Server 12 (HVM), SSD Volume Type - ami-d7450be7	SUSE Linux Enterprise Server 12 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.	ebs	hvm	Select	64-bit

3. The various instance types are shown in the figure given below. Select the t2 Micro and click on the “Next configuration setting” button.

AWS Services Edit Mohan N 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 2: Choose an Instance Type

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

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
<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
<input type="checkbox"/>	General purpose	m4.xlarge	4	16	EBS only	Yes	High

Cancel Previous Review and Launch Next: Configure Instance Details

4. Provide IAM role None and click on Next:Add Storage.



|| C3 SCHOOLS

AWS Services Edit Mohan N 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	1	
Purchasing option	<input type="checkbox"/> Request Spot Instances	
Network	vpc-7ba5281e (172.31.0.0/16) (default)	<input type="button" value="Create new VPC"/>
Subnet	No preference (default subnet in any Availability Zone)	<input type="button" value="Create new subnet"/>
Auto-assign Public IP	Use subnet setting (Enable)	
IAM role	None	<input type="button" value="Create new IAM role"/>
Shutdown behavior	Stop	
Enable termination protection	<input type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring	

Cancel **Previous** **Review and Launch** **Next: Add Storage**

5. Provide the storage related information. Click on “Add New Volume” to Add new Volume and can Delete by Cross button.

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-bfb086e1	8	General Purpose (SSD)	24 / 3000	<input checked="" type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	Search (case-insensitive)	8	General Purpose (SSD)	24 / 3000	<input type="checkbox"/>	Not Encrypted <input type="button" value="X"/>

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.

6. Provide the Root Volume Size (cannot be less than 8 GB for Linux) and Volume Type Standard.

7. Provide the tags for the AWS instance. Tagging is very useful when the user wants to track the cost of a particular instance / service.



|| C3 SCHOOLS

Step 5: Tag Instance

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key	(127 characters maximum)	Value	(255 characters maximum)
Name		TestLab	X

Create Tag (Up to 10 tags maximum)

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

8. For the security of the instance, select the existing key-pair.

For Existing Key-Pair

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 ID	Name	Description	Actions
sg-f3fde396	default	default VPC security group	Copy to new
sg-f76ccb93	Test MN	SG Lab	Copy to new

Inbound rules for sg-f76ccb93

Type	Protocol	Port Range	Source
This security group has no rules			

Cancel Previous **Review and Launch**

9. **Select the security group.** The security group provides the virtual firewall for the user's instance. Open only the ports for the specific IPs as per the user's requirement. Click on "Review and Launch".



|| C3 SCHOOLS

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

Security Group ID	Name	Description	Actions
sg-f3fde396	default	default VPC security group	Copy to new
sg-f76ccb93	Test MN	SG Lab	Copy to new

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

Inbound rules for sg-f76ccb93 (Selected security groups: sg-f76ccb93)

Type	Protocol	Port Range	Source
This security group has no rules			

Cancel Previous Review and Launch

10. Review all the details and click on “Launch”.

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

Step 7: Review Instance Launch

AMI Details



Amazon Linux AMI 2015.03 (HVM), SSD Volume Type - ami-e7527ed7

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

Edit AMI

Instance Type

Edit instance type

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

Security Groups

Edit security groups

Security Group ID	Name	Description
sg-f76ccb93	Test MN	SG Lab

All selected security groups inbound rules

Cancel Previous Launch



|| C3 SCHOOLS

11. AWS will launch the instance and provide the user with the ID of the instance.

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

Select a key pair

MNAWS

I acknowledge that I have access to the selected private key file (MNAWS.pem), and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

Launch Status

Get notified or 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).

How to connect to your instances

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.

Here are some helpful resources to get you started

- [How to connect to your Linux instance](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: User Guide](#)
- [Amazon EC2: Discussion Forum](#)

While your instances are launching you can also

- [Create status check alarms](#) to be notified when these instances fail status checks. (Additional charges may apply)
- [Create and attach additional EBS volumes](#) (Additional charges may apply)
- [Manage security groups](#)

[View Instances](#)

12. Go to the AWS EC2 console and it will display the new instance. The instance will be first in a running State. **It is advisable to connect to the instance once the status checks are in “2/2 Checks”.**



|| C3 SCHOOLS

The screenshot shows the AWS EC2 Dashboard. The left sidebar has links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances (which is selected), Spot Requests, and Reserved Instances. The main 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, and Public DNS. One row is shown: TestLab, i-852da840, t2.micro, us-west-2b, running, 2/2 checks ..., None, ec2-52-26-159-46.us-w...

13. Previously, it was showing 0 running instance on EC2 Dashboard. Now it is showing running instance 1.

The screenshot shows the AWS EC2 Dashboard. The left sidebar includes EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, Elastic Block Store, and Network & Security. The main area displays "Resources" with a summary: 1 Running Instances, 0 Elastic IPs, 2 Volumes, 0 Snapshots, 2 Key Pairs, 0 Load Balancers, 0 Placement Groups, and 2 Security Groups. It also features a "Create Instance" section with a "Launch Instance" button and a note about launching in the US West (Oregon) region. Below this are sections for Service Health (with Service Status: US West (Oregon) operating normally and Availability Zone Status: us-west-2a operating normally) and Scheduled Events (with no events listed).

How to Connect to AWS Linux Instance from a Windows Machine

1. Launch a new Linux Instance.



|| C3 SCHOOLS

AWS Services Edit

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

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.

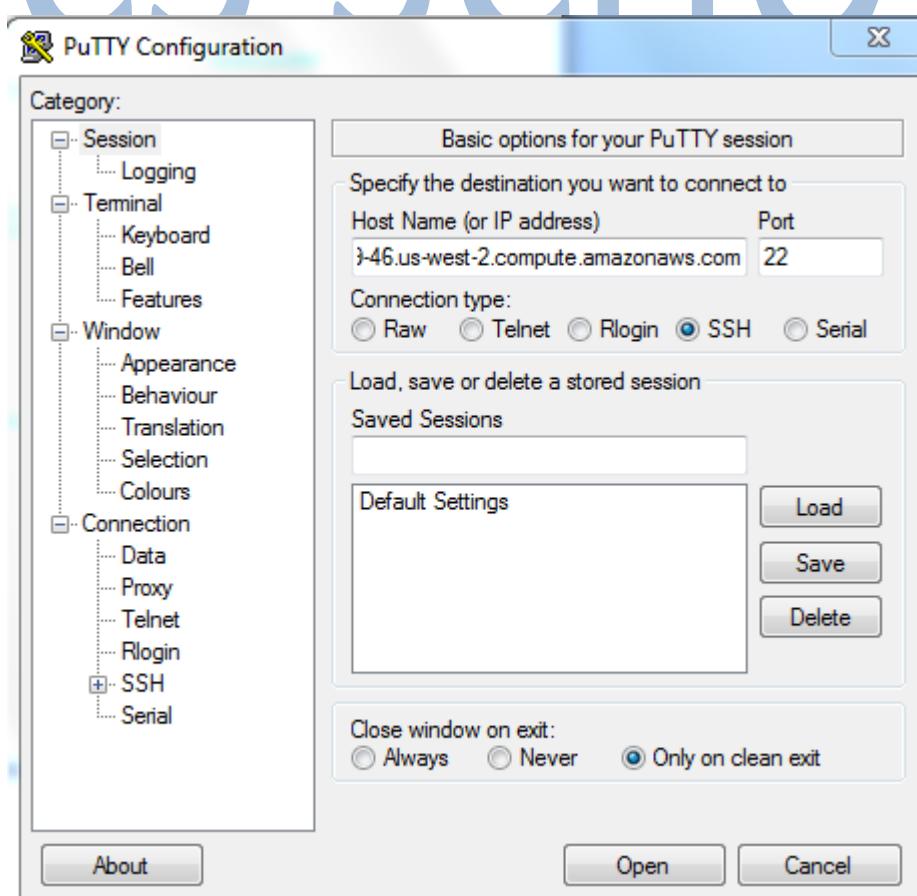
Quick Start

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

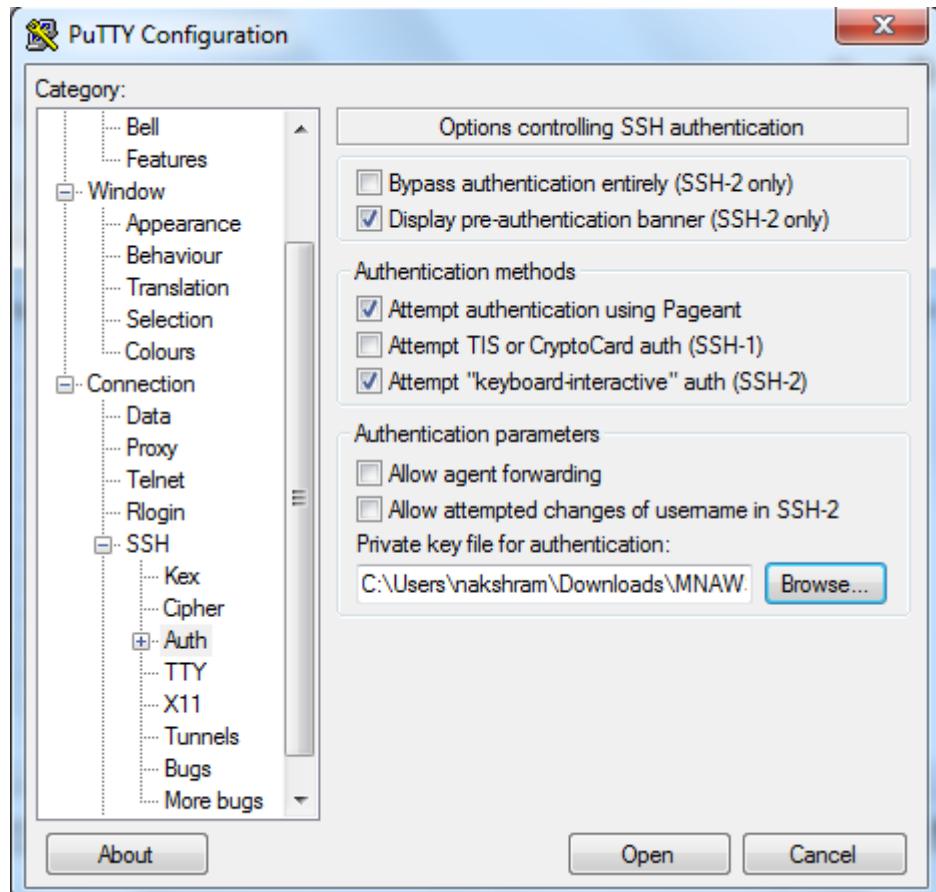
AMI Name	Description	Root device type	Virtualization type	Select	64-bit
Amazon Linux AMI 2015.03 (HVM), SSD Volume Type - ami-e7527ed7	The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.	ebs	hvm	Select	64-bit
Red Hat Enterprise Linux 7.1 (HVM), SSD Volume Type - ami-4dbf9e7d	Red Hat Enterprise Linux version 7.1 (HVM), EBS General Purpose (SSD) Volume Type	ebs	hvm	Select	64-bit
SUSE Linux Enterprise Server 12 (HVM), SSD Volume Type - ami-d7450be7	SUSE Linux Enterprise Server 12 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.	ebs	hvm	Select	64-bit

2. Ensure that you have opened the SSH port 22 for connecting to Linux.

3. Start PuTTy by running **putty.exe**. Enter the public DNS you got in step #4 in the **Host name/IP address** field. Keep the port as 22.



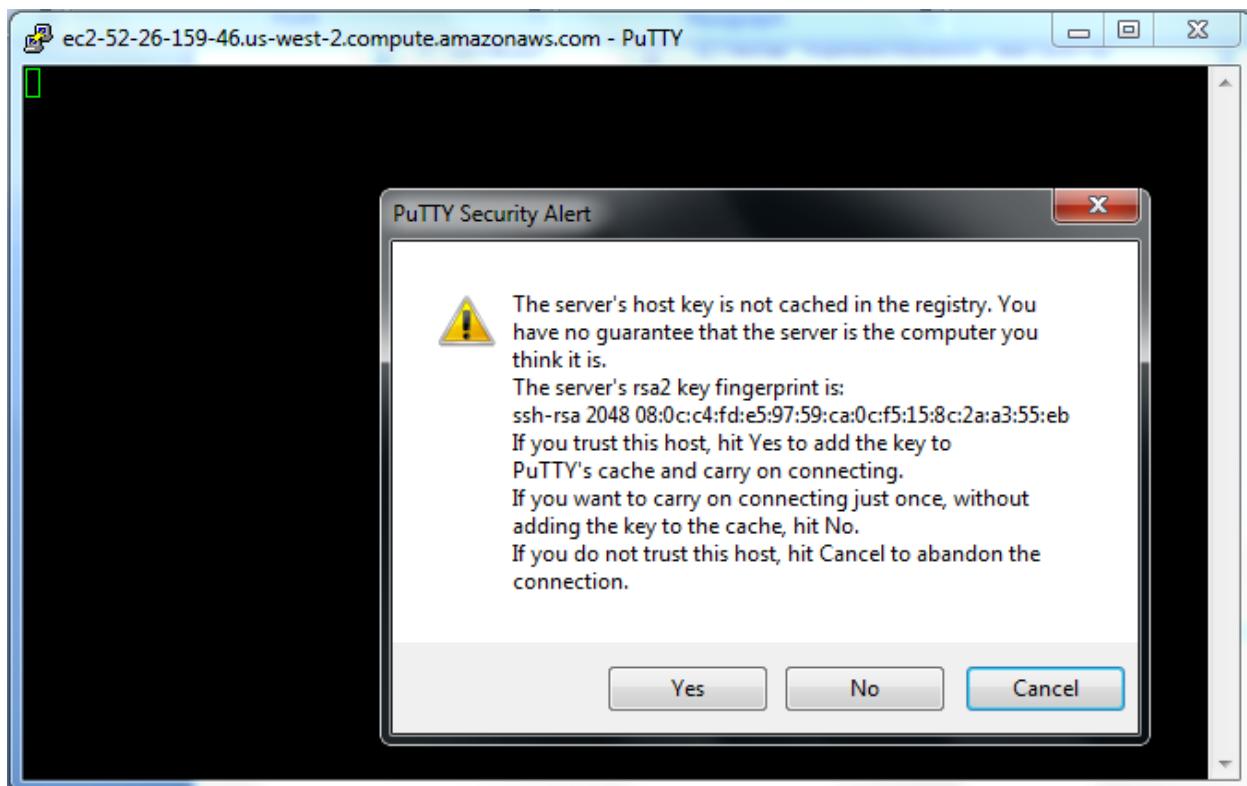
4. In the Category tree, select **SSH >Auth** and then provide the key-pair file we used in launching the instance to connect to the instance.



5. Click **Open**. The command window (telnet) is launched to connect to the AWS instance.



|| C3 SCHOOLS



6. Click **Yes**. You are prompted to log in.

7. For an AWS Linux instance, enter **ec2-user** as the username. (Based on your operating system, the username might be different.)

```
ec2-user@ip-10-252-26-242:~$ login as: ec2-user
Authenticating with public key "imported-openssh-key"
[ec2-user@ip-10-252-26-242 ~]$
```

The terminal session shows the user logging in as "ec2-user" and authenticating with a public key. The prompt then displays the Amazon Linux AMI logo and a link to the release notes. It also indicates there are 10 security updates available out of 16 total.

If you have given the correct IP address, the Linux prompt is displayed as shown above.



|| C3 SCHOOLS

Now you can install and manage your application on the server as required.

How to Associate and Disassociate an Elastic IP to an EC2 Instance

9. Go to the [AWS Console](#) and select the EC2 Service. It will list the AWS dashboard. It lists the current running instances, snapshots and elastic IPs. Click on the “Running Instance” link or the “Instances” link in the left navigation menu.

The screenshot shows the AWS EC2 Instances dashboard. On the left, there's a sidebar with various navigation links like EC2 Dashboard, Instances, and Load Balancing. The main area has sections for Resources (listing 0 Running Instances, 0 Dedicated Hosts, etc.), Create Instance (with a Launch Instance button), Service Health (showing US West (Oregon) is operating normally), and Scheduled Events (no events). To the right, there are Account Attributes and Additional Information sections, along with a Marketplace sidebar listing products like Tableau Server and SAP HANA One.

10. The [EC2 Instances](#) dashboard displays all the instances of that region. When the instance is launched, AWS assigns a public IP to the instance.

This screenshot shows the details for a specific EC2 instance (i-0de2e9dc82db04140). The top bar shows the instance ID and Public DNS. Below, there are tabs for Description, Status Checks, Monitoring, and Tags. The Description tab is active, displaying detailed information about the instance, including its state (running), type (t2.micro), and network settings (Public DNS: ec2-54-169-156-93.ap-southeast-1.compute.amazonaws.com, Private DNS: ip-172-31-28-64.ap-southeast-1.compute.internal, Private IP: 172.31.28.64, Subnet ID: subnet-15789363, Network interface: eth0, and Source/dest check: True). Other tabs show Status Checks, Monitoring, and Tags.



|| C3 SCHOOLS

11. Go to Elastic IP dashboard by clicking on the “Elastic IP” in step#1. It lists all the Elastic IPs of that region. Select an elastic IP to be assigned to the instance and click on the “Associate Address” button.

The screenshot shows the AWS Elastic IP dashboard. At the top, there are buttons for "Allocate New Address" and "Actions ▾". A dropdown menu is open under "Actions", showing options: "Allocate New Address", "Release Addresses", and "Associate Address" (which is highlighted with a blue border). Below the menu, there is a search bar labeled "Filter by attributes or see" and a table with two rows. The first row has columns "Elastic IP" and "52.76.175.104". The second row has columns "Disassociate Address" and "eipalloc-5d77ee38". To the right of the table are dropdown menus for "Instance" and "Private IP Address".

12. It asks for the instance which will be associated with this IP. Select the instance from the list and click on “Yes, Associate”.

Select the instance OR network interface to which you wish to associate this IP address (52.76.175.104)

Instance Or
Network Interface
Private IP Address ⓘ
 Reassociation ⓘ



Warning

If you associate an Elastic IP address with your instance, your current public IP address is released. Learn more about [public IP addresses](#).

[Cancel](#) [Associate](#)

13. It will associate the elastic IP to that instance. Go to Instance dashboard and select the instance. The IP of the instance is updated to the elastic IP.



|| C3 SCHOOLS

Instance: i-0de2e9dc82db04140 (AWSchefserver)		Elastic IP: 52.76.175.104
Description		
Status Checks		
Monitoring		
Tags		
Instance ID: i-0de2e9dc82db04140		
Instance state: running		
Instance type: t2.micro		
Private DNS: ip-172-31-28-64.ap-southeast-1.compute.internal		
Private IPs: 172.31.28.64		
Secondary private IPs:		
VPC ID: vpc-30f4f655		
Subnet ID: subnet-15789363		
Network interfaces: eth0		
Source/dest. check: True		
Public DNS: ec2-52-76-175-104.ap-southeast-1.compute.amazonaws.com		
Public IP: 52.76.175.104		
Elastic IPs: 52.76.175.104*		
Availability zone: ap-southeast-1a		
Security groups: sngsg, view rules		
Scheduled events: No scheduled events		
AMI ID: amzn-ami-hvm-2016.03.3.x86_64-gp2 (a59b49c6)		
Platform: -		
IAM role: -		
Key pair name: sngkey		

C3 SCHOOLS

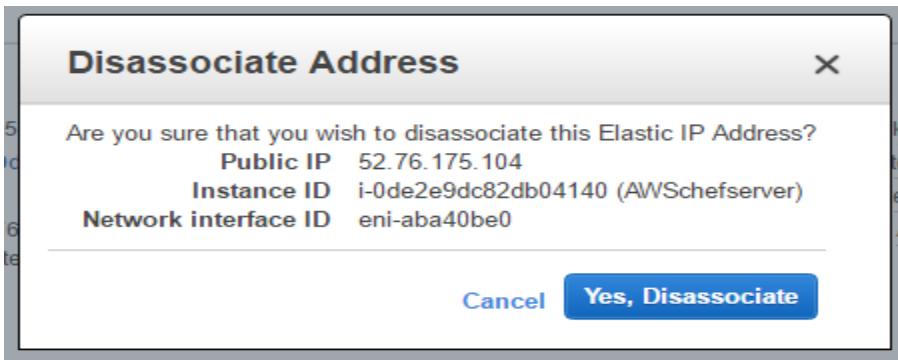


|| C3 SCHOOLS

14. To disassociate the instance, Go to Elastic IP dashboard by clicking on the “Elastic IP” in step#1. It lists all the Elastic IPs of that region. Select an elastic IP to be the instance and click on “Disassociate Address” from the Actions menu.

The screenshot shows the AWS Elastic IP dashboard. At the top, there are buttons for "Allocate New Address" and "Actions". A dropdown menu is open under "Actions" with the following options: "Allocate New Address", "Release Addresses", "Associate Address", and "Disassociate Address". The "Disassociate Address" option is highlighted with a blue border. Below the menu, a table lists an elastic IP entry: "Elastic IP" (checkbox), "52.76.175.104" (IP address), "eipalloc-5d77ee38" (Allocation ID), "i-0de2e9dc82db04140 (AWSchefserver)" (Instance ID), and "172.31.28.64" (Private IP Address). The entire interface has a light gray background with blue and white UI elements.

15. AWS will ask for a confirmation before disassociating the address. Click on “Yes, Disassociate”.



16. The elastic IP address associated with the instance will be disassociated. The above mentioned IP can be reassigned to any other instance. If the IP address is unassigned, it will cost the user. Release the IP address if the user does not require it.

The figure given below demonstrates the instance with the new public IP after the elastic IP has been disassociated.



|| C3 SCHOOLS

[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	Pub
AWSchefser...	i-0de2e9dc82db04...	t2.micro	ap-southeast-1a	running	2/2 checks...	None	ec2-54-169-235-239....	54.1

Instance: i-0de2e9dc82db04140 (AWSchefserver) Public DNS: ec2-54-169-235-239.ap-southeast-1.compute.amazonaws.com

Description Status Checks Monitoring Tags

Instance ID	i-0de2e9dc82db04140	Public DNS	ec2-54-169-235-239.ap-southeast-1.compute.amazonaws.com
Instance state	running	Public IP	54.169.235.239
Instance type	t2.micro	Elastic IPs	
Private DNS	ip-172-31-28-64.ap-southeast-1.compute.internal	Availability zone	ap-southeast-1a
Private IPs	172.31.28.64	Security groups	sngsg, view rules
Secondary private IPs		Scheduled events	No scheduled events
VPC ID	vpc-30f4f655	AMI ID	amzn-ami-hvm-2016.03.3.x86_64-gp2 (ami-a59b49c6)

How to Share your Local Drive with an AWS Windows Instance

1. Launch a new Windows Instance.

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

Step 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit [Select](#) 64-bit

Ubuntu Server 14.04 LTS (HVM), SSD Volume Type - ami-21d30f42 <small>Free tier eligible</small>	Ubuntu Server 14.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services). Root device type: ebs Virtualization type: hvm	Select 64-bit
Microsoft Windows Server 2012 R2 Base - ami-d6f32ab5 <small>Free tier eligible</small>	Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English] Root device type: ebs Virtualization type: hvm	Select 64-bit
Microsoft Windows Server 2012 R2 with SQL Server Express - ami-c9fd24aa <small>Windows</small>	Microsoft Windows Server 2012 R2 Standard edition, 64-bit architecture, Microsoft SQL Server 2016 Express edition. [English] Root device type: ebs Virtualization type: hvm	Select 64-bit
Microsoft Windows Server 2012 R2 with SQL Server Web - ami-75fd2416 <small>Windows</small>	Microsoft Windows Server 2012 R2 Standard edition, 64-bit architecture, Microsoft SQL Server 2016 Web edition. [English] Root device type: ebs Virtualization type: hvm	Select 64-bit
Microsoft Windows Server 2012 R2 with SQL Server Standard - ami-eefb228d <small>Windows</small>	Microsoft Windows Server 2012 R2 Standard edition, 64-bit architecture, Microsoft SQL Server 2016 Standard edition. [English] Root device type: ebs Virtualization type: hvm	Select 64-bit

2. Ensure that you have opened the RDP port 3389 for connecting to Windows. In this example we opened it for all IP addresses but this is not best practice. create a new group or select existing one



|| C3 SCHOOLS

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

launch-wizard-1

Description:

launch-wizard-1 created 2016-09-15T14:07:42.979+05:30

Type <i>(i)</i>	Protocol <i>(i)</i>	Port Range <i>(i)</i>	Source <i>(i)</i>
RDP	TCP	3389	Anywhere <i>(i)</i> 0.0.0.0/0

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.

3. Verify all of the launch details

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

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

⚠ Improve your instances' security. Your security group, launch-wizard-1, is open to the world.

Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

AMI Details



Microsoft Windows Server 2012 R2 Base - ami-d6f32ab5

Microsoft Windows 2012 R2 Standard edition with 64-bit architecture, [English]

Root Device Type: ebs Virtualization type: hvm

If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the [License Mobility Form](#). Don't show me this again

Instance Type

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

Security Groups

Security group name:
Description:

launch-wizard-1
launch-wizard-1 created 2016-09-15T14:07:42.979+05:30

Type <i>(i)</i>	Protocol <i>(i)</i>	Port Range <i>(i)</i>	Source <i>(i)</i>
RDP	TCP	3389	0.0.0.0/0

Instance Details

Storage

Tags

4. Once you confirm the details, the instance is launched and displayed in the console as shown below. Make note of the public DNS of the instance.



|| C3 SCHOOLS

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
Win Ins	i-0b708d0f899ca0...	t2.micro	ap-southeast-1a	running	Initializing	None	ec2-52-221-223-133....	52.221.223.133
AWSchefser...	i-0de2e9dc82db04...	t2.micro	ap-southeast-1a	stopped	None			

Instance: i-0b708d0f899ca023e (Win Ins) Public DNS: ec2-52-221-223-133.ap-southeast-1.compute.amazonaws.com

Description Status Checks Monitoring Tags

Instance ID	i-0b708d0f899ca023e	Public DNS	ec2-52-221-223-133.ap-southeast-1.compute.amazonaws.com
Instance state	running	Public IP	52.221.223.133
Instance type	t2.micro	Elastic IPs	
Private DNS	ip-172-31-25-158.ap-southeast-1.compute.internal	Availability zone	ap-southeast-1a
Private IPs	172.31.25.158	Security groups	launch-wizard-1, view rules
Secondary private IPs		Scheduled events	No scheduled events
VPC ID	vpc-30f4f655	AMI ID	Windows_Server-2012-R2_RTM-English-64Bit-Build-2016.08.11 (ami-d6f32ab5)
Subnet ID	subnet-15789363	Platform	windows
Network interfaces	eth0	IAM role	-
Source/dest. check	True	Key pair name	sngkey
EBS-optimized	False	Owner	076828422820
		Launch time	September 15, 2016 at 2:35:03 PM UTC+5:30 (less than one hour)

Next you will need to generate the password for this windows instance. This requires the .pem file that was created earlier and that was used to launch this instance.

C3 SCHOOLS



|| C3 SCHOOLS

5. Right-click the instance and select **Get Windows Password**. or click on action button and then select **Get Windows Password**

The screenshot shows the AWS Management Console interface for EC2 instances. A context menu is open over an instance named 'Windows'. The menu items include 'Connect', 'Get Windows Password' (which is highlighted with a blue box), 'Launch More Like This', 'Instance State', 'Instance Settings', 'Image', 'Networking', and 'CloudWatch Monitoring'. The main pane displays two instances: 'Windows' (running) and 'db04...' (stopped). The 'Windows' instance details are shown in a large table on the right.

	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS	Public IP
1	Windows	i-0ca0...	t2.micro	ap-southeast-1a	running	2/2 checks ...	None	ec2-52-221-223-133....	52.221.223.133
2	db04...	i-0db04...	t2.micro	ap-southeast-1a	stopped		None		

Instance Details:

- Public DNS: ec2-52-221-223-133.ap-southeast-1.compute.amazonaws.com
- Public IP: 52.221.223.133
- Elastic IPs: None
- Availability zone: ap-southeast-1a
- Security groups: launch-wizard-1, view rules
- Scheduled events: No scheduled events
- AMI ID: Windows_Server-2012-R2_RTM-English-64Bit-Basic-2016.08.11 (ami-d6f32ab5)
- Platform: windows
- IAM role: -
- Key pair name: sngkey
- Owner: 076828422820
- Launch time: September 15, 2016 at 2:35:03 PM UTC+5:30 (less than one hour)

Secondary private IPs:

- VPC ID: vpc-30f4f655
- Subnet ID: subnet-15789363
- Network interfaces: eth0
- Source/dest. check: True

EBS-optimized: False

6. You are prompted to provide the details of your .pem file. Open your .pem file in notepad, copy all of the content (including ----- BEGIN RSA and ----- END RSA lines). or choose file from location and open the file then click Decrypt Passwod



|| C3 SCHOOLS

Retrieve Default Windows Administrator Password

To access this instance remotely (e.g. Remote Desktop Connection), you will need your Windows Administrator password. A default password was created when the instance was launched and is available encrypted in the system log.

To decrypt your password, you will need your key pair for this instance. Browse to your key pair, or copy and paste the contents of your private key file into the text area below, then click Decrypt Password.

The following Key Pair was associated with this instance when it was created.

Key Name: sngkey

In order to retrieve your password you will need to specify the path of this Key Pair on your local machine:

Key Pair Path: sngkey.pem

Or you can copy and paste the contents of the Key Pair below:

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEowIBAAKCAQEAkZm0l6JMod5YiJgjyYcRPb6T2c0veY8KnJLzn2QsfBXqovmxFou/pLeidIZ  
C36ZIKyUJVJlf+QHGN7SZA60gQ6CzU3KcT0bA0nFTswgmbBzfaUhzeVDhjctJnrJFudw/TBxK1RP  
56SMgDPxRVE/+6p1WtanNPdABVSL9X4DclLfIORVnuosJGS+4nEyk6WITEq14UKQpQL3IpvfDTbb  
tHKn7oXnwuu+s/KifKB3k1ZV/d9gbq9bVeNRzz+Rn8CSO/kIBs5q4eG3GfPgiwrKPWbjur+EbsTK
```

C3 SCHOOLS



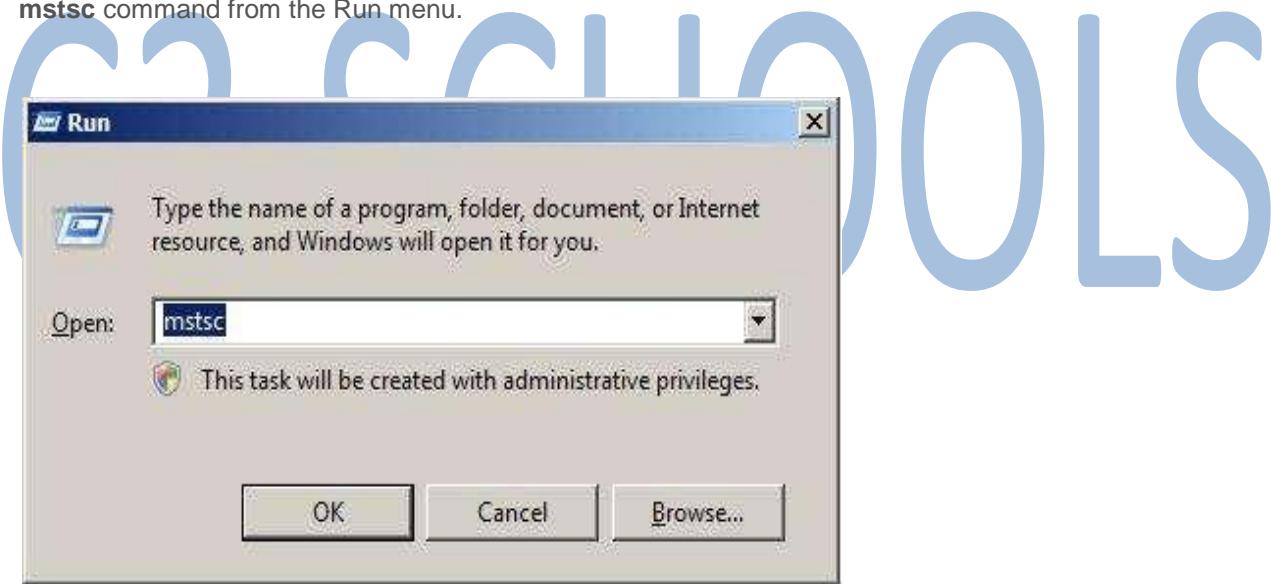
|| C3 SCHOOLS

7. Click **Decrypt Password**. The decrypted password is displayed; you can use this password to connect to the Windows instance.



8. Store the password in a safe place, you will need to use it whenever you connect to the instance.

9. Now start the RDP (Remote Desktop Service) from the Windows machine as shown below. Run the **mstsc** command from the Run menu.



The Remote Desktop Connection window is displayed.



|| C3 SCHOOLS



C3 SCHOOLS



|| C3 SCHOOLS

10. Click the **Options** button and then select the **Local Resources** tab.



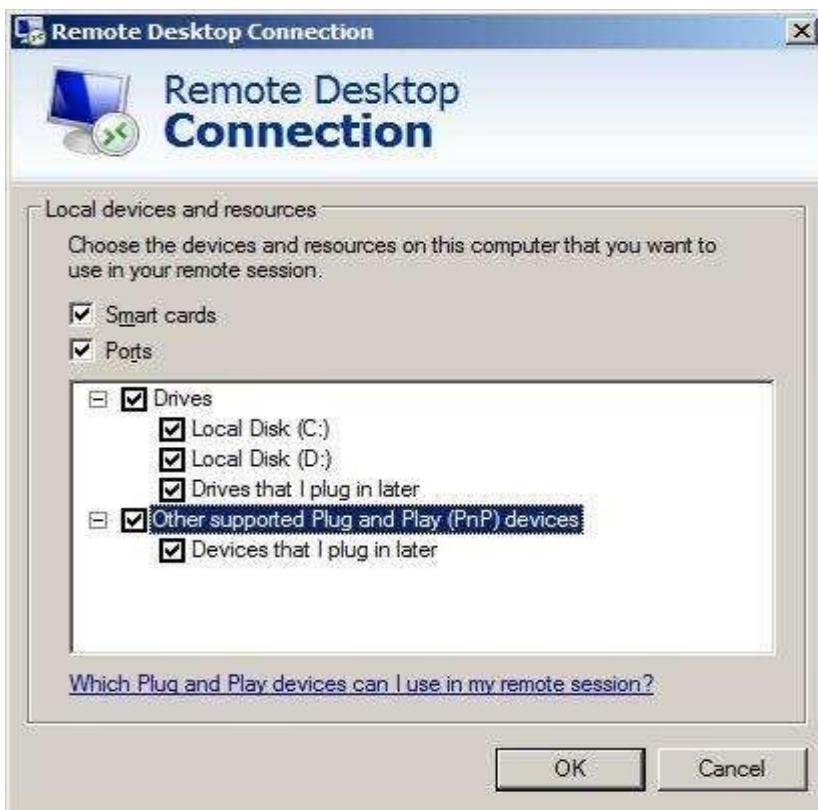
11. In the Remote audio area, select **Settings** to configure the audio settings of your instance.





|| C3 SCHOOLS

12. In the **Local Resource** tab, in the **Local devices and resources** area, click **More**. All the plug and play devices that can be available through network in the AWS EC2 server instance are listed, as well as the disk drives.



13. Select the devices and drives that you want to access from the Remote AWS EC2 server.

14. Once you have completed the above settings, provide the public DNS IP of your instance (obtained in step #4).

In the **Username** field, enter administrator.





|| C3 SCHOOLS

15. Click **Connect**.



16. When prompted for confirmation, click **Connect** again. The process of connecting to the Remote Desktop (your EC2 instance running in AWS) begins. Once connected, you are prompted for the password.





|| C3 SCHOOLS

17. Provide the password you got in step#7. When you click **OK**, the password is verified and you are connected to your Windows instance.



C3 SCHOOLS

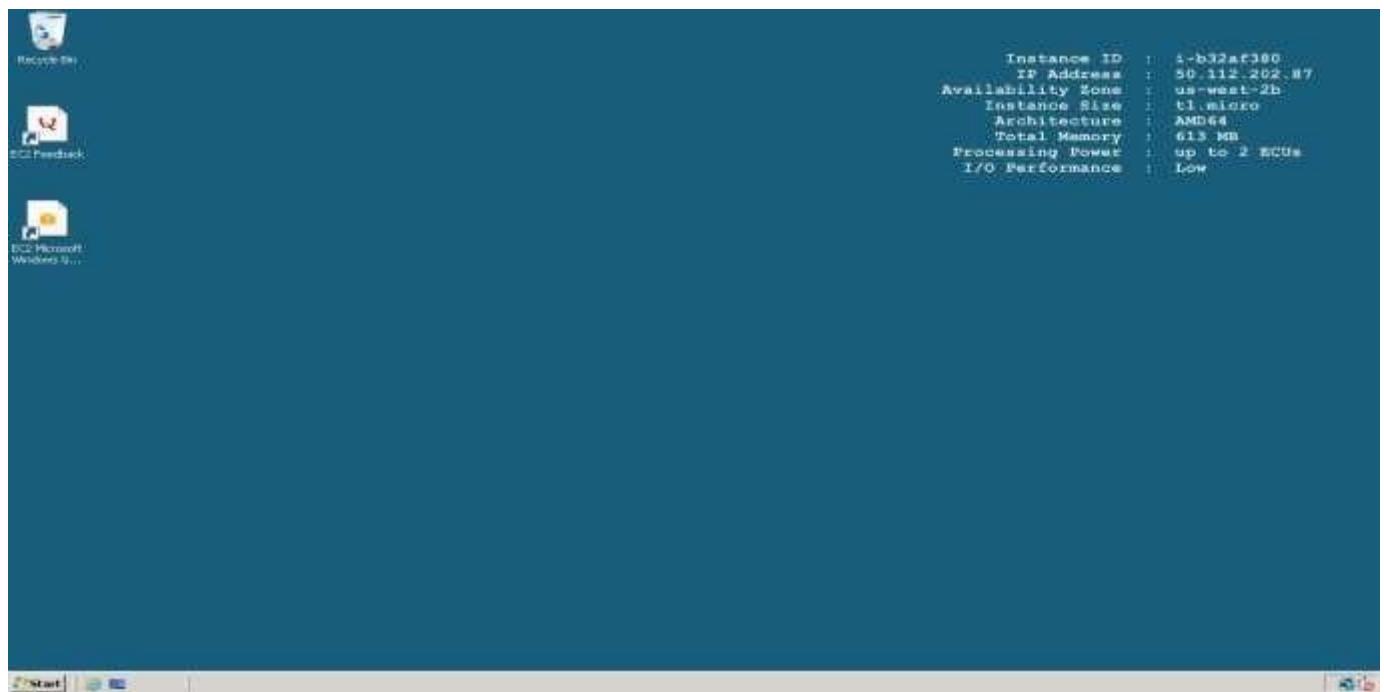
18. On first time usage, your desktop is automatically set up when you connect.





|| C3 SCHOOLS

19. Once connected and setup, the desktop resembles the following:

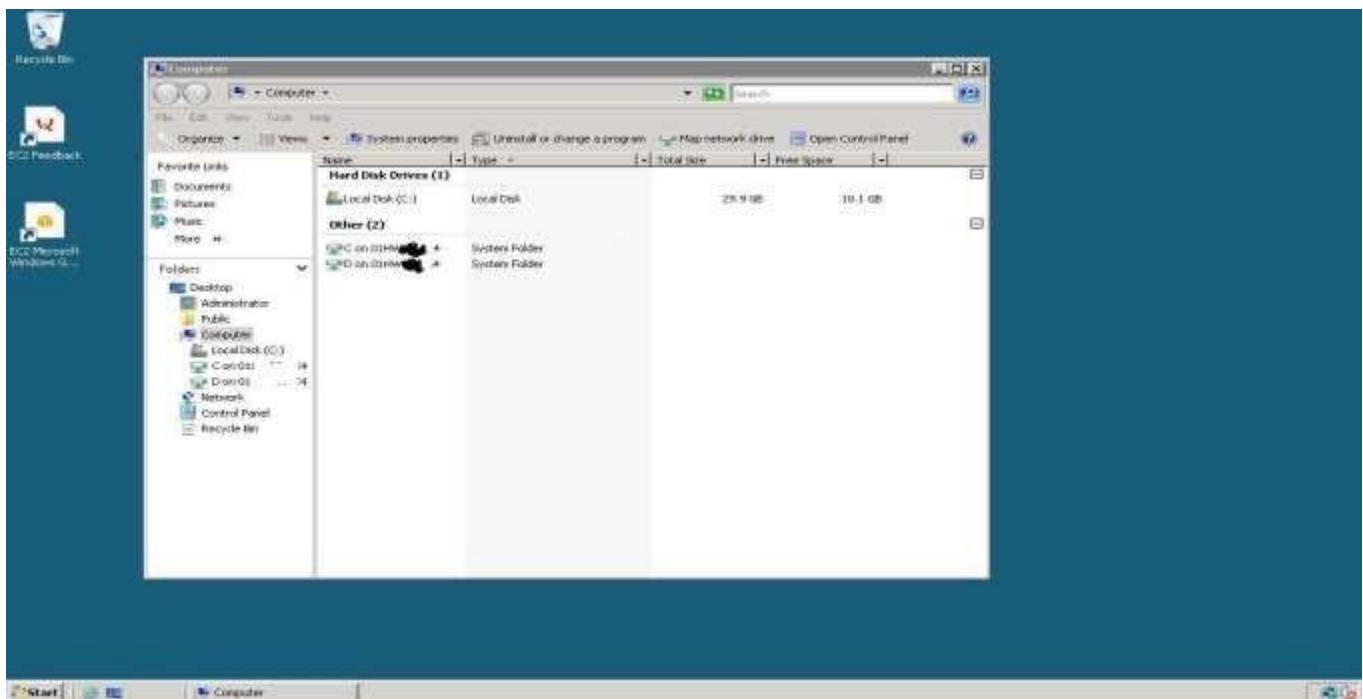




|| C3 SCHOOLS

20. Open the Windows Explorer or My Computer.

The local hard disk of your desktop/laptop in the EC2 server instance is listed.



C3 SCHOOLS

As shown above, in Windows Explorer will show both the "C" & "D" drives of your local machine. (We have masked some characters for security reasons).

How to access the Instance metadata:

1. Enter your AWS account Console, launch a linux instance and connect to it.
2. To get the Instance metadata run: **GET <http://169.254.169.254/latest/meta-data/>**
3. Run the Linux command **/usr/bin/curl -s <http://169.254.169.254/latest/meta-data/>**



|| C3 SCHOOLS

4. It will list the available metadata. If you want specific metadata like ami-id, public-ip or local ip run commands as shown in below image.

```
[ec2-user@ip-10-252-39-116 ~]$ /usr/bin/curl -s http://169.254.169.254/latest/meta-data/  
ami-id  
ami-launch-index  
ami-manifest-path  
block-device-mapping/  
hostname  
instance-action  
instance-id  
instance-type  
kernel-id  
local-hostname:  
local-ipv4  
mac  
metrics/  
network/  
placement/  
profile  
public-hostname  
public-ipv4  
public-keys/  
reservation-id  
security-groups[ec2-user@ip-10-252-39-116 ~]$ /usr/bin/curl -s http://169.254.169.254/latest/meta-data/ami-id  
ami-46da5576[ec2-user@ip-10-252-39-116 ~]$  
[ec2-user@ip-10-252-39-116 ~]$ /usr/bin/curl -s http://169.254.169.254/latest/meta-data/ami-id  
ami-46da5576[ec2-user@ip-10-252-39-116 ~]$  
[ec2-user@ip-10-252-39-116 ~]$ /usr/bin/curl -s http://169.254.169.254/latest/meta-data/local-ipv4  
10.252.39.116[ec2-user@ip-10-252-39-116 ~]$  
[ec2-user@ip-10-252-39-116 ~]$ /usr/bin/curl -s http://169.254.169.254/latest/meta-data/public-ipv4  
54.245.7.36[ec2-user@ip-10-252-39-116 ~]$
```



|| C3 SCHOOLS

5. A few more samples like get availability zone (here us-west-2b), instance-type (here micro), mac, security group, public host name of running instance is shown below.

C3 SCHOOLS



|| C3 SCHOOLS

A screenshot of a terminal window titled "ec2-user@ip-10-252-39-116:~". The window displays several curl commands being run against the EC2 metadata endpoint at `http://169.254.169.254/latest/meta-data/`. The commands are:

- `/placement/availability-zone` (redacted)
- `/instance-type` (redacted)
- `/mac` (redacted)
- `/security-groups` (redacted)
- `/public-hostname` (redacted)

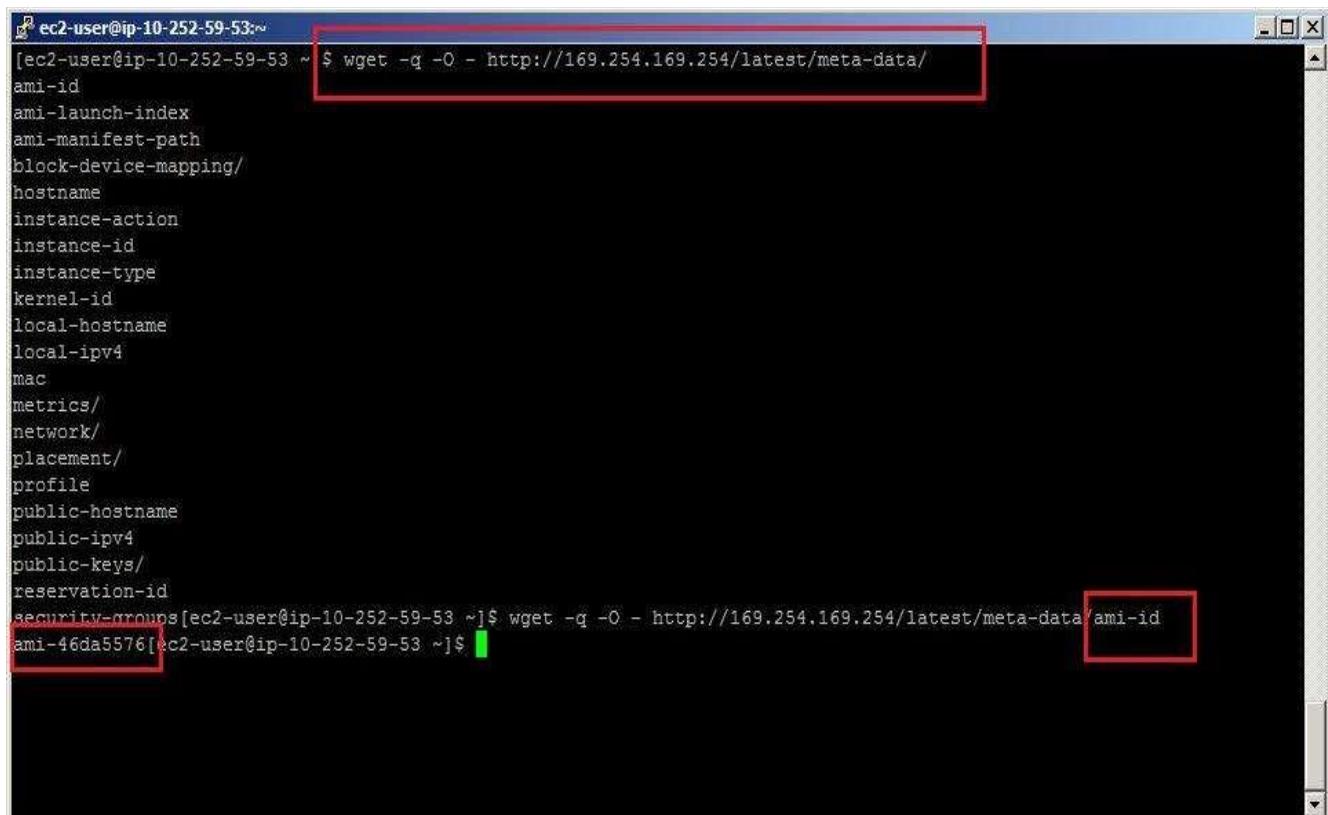
The output shows the instance type as "t1.micro" and the public hostname as "ec2-54-245-7-36.us-west-2.compute.amazonaws.com".

6. You can also run command wget instead of curl to get the instance metadata. Run command `wget -q -o - http://169.254.169.254/latest/meta-data/`.

7. For example if you want to get ami-id using wget, run command `wget -q -o - http://169.254.169.254/latest/meta-data/ami-id` to get AMI id.



|| C3 SCHOOLS



A screenshot of a terminal window titled "ec2-user@ip-10-252-59-53:~". The window displays the output of the command \$ wget -q -O - http://169.254.169.254/latest/meta-data/. The output lists various AWS metadata keys such as ami-id, ami-launch-index, ami-manifest-path, block-device-mapping/, hostname, instance-action, instance-id, instance-type, kernel-id, local-hostname, local-ipv4, mac, metrics/, network/, placement/, profile, public-hostname, public-ipv4, public-keys/, reservation-id, security-groups, and user-data. The "ami-id" key is highlighted with a red box. The entire command line is also highlighted with a red box.

```
[ec2-user@ip-10-252-59-53 ~]$ wget -q -O - http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
instance-action
instance-id
instance-type
kernel-id
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups[ec2-user@ip-10-252-59-53 ~]$ wget -q -O - http://169.254.169.254/latest/meta-data/ami-id
ami-46da5576[ec2-user@ip-10-252-59-53 ~]$
```

C3 SCHOOLS



|| C3 SCHOOLS

8. If you are in windows, you can run the command as SOAP call in browser or call from the AWS SDK / API.

9. If you type in the browser <http://169.254.169.254/latest/meta-data/>, it will return all the instance metadata.

The screenshot shows a Windows Internet Explorer window with the URL <http://169.254.169.254/latest/meta-data/>. The page displays a list of metadata keys, each preceded by a red box. The keys listed are:

- ami-id
- ami-launch-index
- ami-manifest-path
- block-device-mapping/
- hostname
- instance-action
- instance-id
- instance-type
- local-hostname
- local-ipv4
- mac
- metrics/
- network/
- placement/
- profile
- public-hostname
- public-ipv4
- public-keys/
- reservation-id
- security-groups

10. Now if you want to query particular data send in the URL that metadata. E.g. If you want to know local IP of instance, type in the browser <http://169.254.169.254/latest/meta-data/local-ipv4>.

The screenshot shows a Windows Internet Explorer window with the URL <http://169.254.169.254/latest/meta-data/local-ipv4>. The page displays the value "10.252.47.166", which is highlighted with a red box.



|| C3 SCHOOLS

How to add your own metadata to an instance and get it from instance -

12. When you launch an instance, it asks to provide the metadata.

13. If it is an EBS backed instance, you can stop the instance and provide the metadata.

The screenshot shows the AWS Management Console with the 'Instances' service selected. A context menu is open over an instance named 'Win Ins'. The 'Actions' menu is expanded, and the 'Instance Settings' option is selected. A sub-menu under 'Instance Settings' is open, showing options like 'View/Change User Data', 'Change Shutdown Behavior', and 'Get System Log'. The main instance details table is visible in the background.

Attribute	Value
Name	i-0b708d0f899ca023e
Instance State	stopped
Image	Windows Server 2012-R2 RTM English 64-bit Base - 2016.08.11 (ami-d6f32ab5)
Networking	None
CloudWatch Monitoring	None
Add/Edit Tags	None
Attach to Auto Scaling Group	None
Change Instance Type	None
Change Termination Protection	None
View/Change User Data	None
Change Shutdown Behavior	None
Get System Log	None
Get Instance Screenshot	None
Modify Instance Placement	None

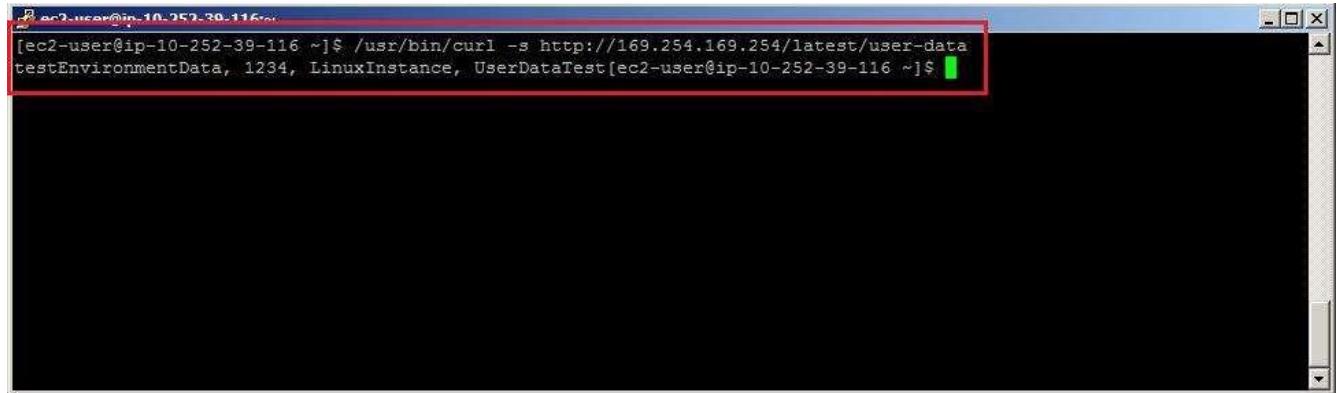
We can view or modify user data here

The screenshot shows the 'View/Change User Data' dialog box. It displays the instance ID 'i-0b708d0f899ca023e' and a large text area for 'User Data'. Below the text area are two radio buttons: 'Plain text' (selected) and 'Input is already base64 encoded'. At the bottom right are 'Cancel' and 'Save' buttons. The background shows the same instance details table as the previous screenshot.



|| C3 SCHOOLS

15. In order to get the metadata of Linux instance run the following command -
`/usr/bin/curl -s http://169.254.169.254/latest/meta-data/user-data.`



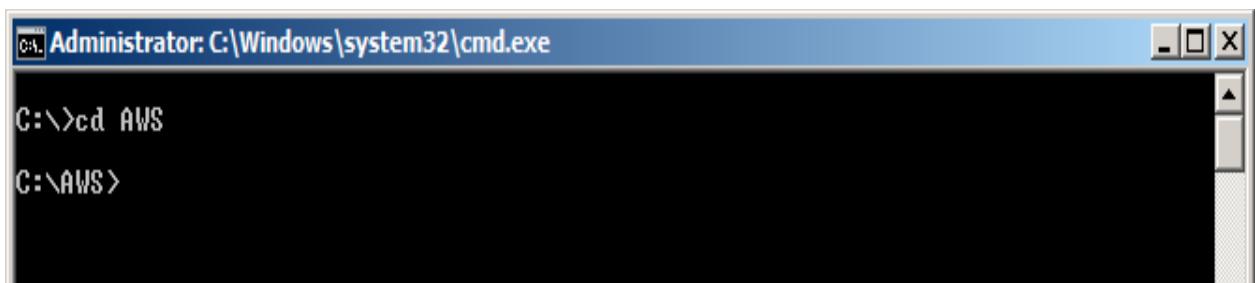
```
[ec2-user@ip-10-252-39-116 ~]$ /usr/bin/curl -s http://169.254.169.254/latest/meta-data/user-data
testEnvironmentData, 1234, LinuxInstance, UserDataTest[ec2-user@ip-10-252-39-116 ~]$
```

As shown above either you can get instance metadata or your own metadata in the instance. This option is very useful when you want to pass boot parameters or pass some instructions during instance boot. Also when you have to configure DB connection / register your instance with monitoring tool or some configuration management tool the metadata is very handful.

How to Install AWS CLI to Windows

A) Downloading SDK APIs

1. Create a folder to store your APIs in your local drive. E.g. C:AWS



```
C:\Administrator: C:\Windows\system32\cmd.exe
C:\>cd AWS
C:\AWS>
```

2. Download the Amazon AWS SDK API tools for Windows (.zip) file from the following link.

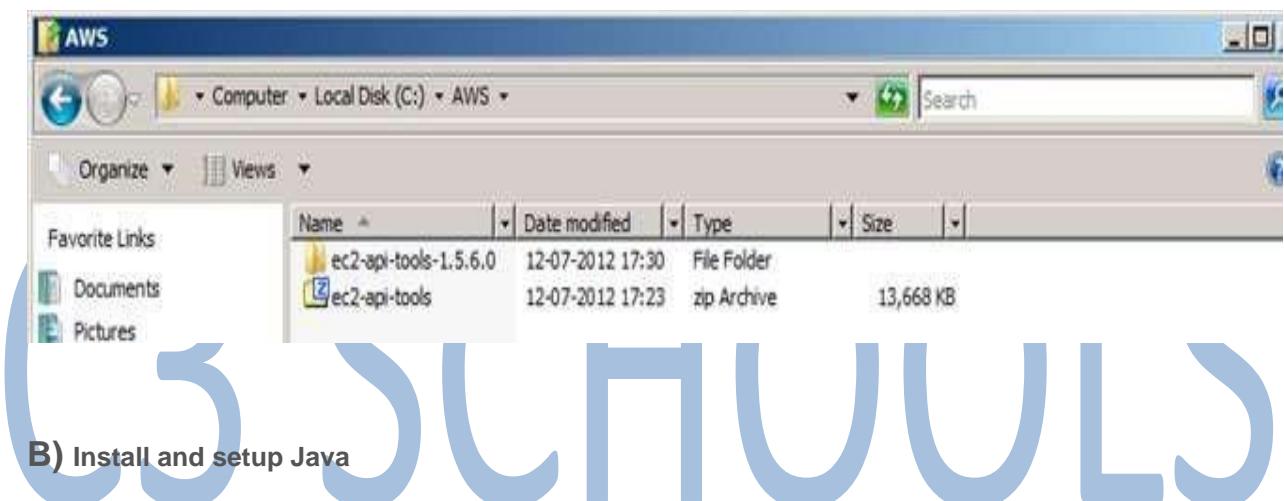
<http://s3.amazonaws.com/ec2-downloads/ec2-api-tools.zip> and save in the folder created in step#1.



|| C3 SCHOOLS

3. Unzip the file and Extract it to local drive

```
C:\>cd AWS  
C:\AWS>cd ec2-api-tools-1.5.6.0  
C:\AWS\ec2-api-tools-1.5.6.0>_
```



1. If JDK / JRE is not installed and environment variables are not set please follow below steps else jump to section 'C'

2. Install and download JDK 5 or above. The JDK download is free and JDK 7 is available for download
at <http://www.oracle.com/technetwork/java/javase/downloads/index.html>

3. Set environment variable as following

i. JAVA_HOME=<JRE / JDK PATH>

ii. PATH=%PATH%;<JAVA_HOME>bin

iii. CLASSPATH=%PATH%;<JAVA_HOME>lib

4. Run command java –version and check if it displays the correct version of your



|| C3 SCHOOLS

JDK / JRE.

```
Administrator: C:\Windows\system32\cmd.exe
C:\AWS\ec2-api-tools-1.5.6.0>SET JAVA_HOME=C:\Sun\SDK\jdk
C:\AWS\ec2-api-tools-1.5.6.0>SET PATH=%PATH%;C:\Sun\SDK\jdk\bin\
C:\AWS\ec2-api-tools-1.5.6.0>SET CLASSPATH=%CLASSPATH%;C:\Sun\SDK\jdk\lib\
C:\AWS\ec2-api-tools-1.5.6.0>java -version
java version "1.6.0_22"
```

5. If you setup above commands through command window it will be valid for the session of this command window only.

6. Please set all above parameters through Environment Variables. You can access Environment variables through for windows 7 / Vista: MyComputer -> Right Click and Select Properties. -> select “Advanced System Settings” from left menu and go to Environment variables.

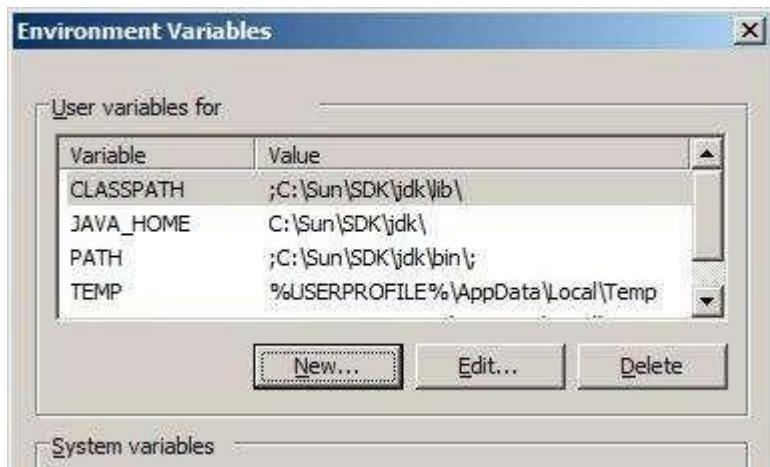
For Windows XP Right Click on Computer -> Select Properties -> Select Advanced Tab and click -> Environment variables.

C3 SCHOOLS



|| C3 SCHOOLS

7. Set the variables as shown below



C) Download and set AWS Certificate File and Private Keys. (Some of the data is masked or removed in the screen for confidentiality purpose).

1. Go to AWS Account section. <http://aws.amazon.com/account>
2. in the left menu click on “Security Credentials” as selected below:

C3 SCHOOLS



|| C3 SCHOOLS

[Sign Up](#)[My Account / Console](#)

English

[AWS Products & Solutions](#)[AWS Product Information](#)[Developers](#)[Support](#)**Account:**

- [Account Activity](#)
- [AWS Identity and Access Management](#)
- [AWS Management Console](#)
- [Consolidated Billing](#)
- [DevPay](#)
- [Manage Your Account](#)
- [Payment Method](#)
- [Personal Information](#)
- [Security Credentials](#)**
- [Usage Reports](#)
- [Billing Alerts](#)
- [Billing Preferences](#)

This page allows you to manage the root account credentials for your AWS Account. To manage IAM Users, their permissions, and security credentials, use the AWS Management Console.

Welcome D1 | Sign Out
Account Number 0-1-182-1B10-A

Access to applications and services within AWS cloud is secure and protected in multiple ways. Accessing those applications and services requires the use of special credentials that are associated with your account. There are three types of credentials currently offered by AWS. If you know which security credentials you need, simply select one of the links below:

- [Access Credentials: Your Access Keys, X.509 Certificates, and Key Pairs](#)
- [Sign-In Credentials: Your E-mail Address, Password, and AWS Multi-Factor Authentication Device](#)
- [Account Identifiers: Your AWS Account ID and Canonical User ID](#)

If you are not sure which security credentials you should use, the link below will help you identify the credentials you need for the task you want to accomplish:

[Find out which AWS Security Credentials you need](#)

CLOUD COMPUTING



|| C3 SCHOOLS

3. Go to Access Credentials – > X.509

Access Credentials

There are three types of access credentials used to authenticate your requests to AWS services: (a) access keys, (b) X.509 certificates, and (c) key pairs. Each access credential type is explained below.

X.509 Certificates

Use X.509 certificates to make secure SOAP protocol requests to AWS service APIs.

Exceptions: Amazon S3 and Amazon Mechanical Turk instead require your Access Keys for SOAP requests.

Created	X.509 Certificate	Status
July 13, 2010	cert-7QDOSUR (Download) QOBHTUF VH3EYBHM.pem	Action (Make Inactive)

[Create a New Certificate](#) | [Upload Your Own Certificate](#)

View Your Deleted Certificates

For your protection, AWS doesn't ask for your private key or retain it on file. You should also never share your private key with anyone. In addition, industry best practice recommends frequent certificate rotation.

[Learn more about X.509 Certificates](#)

4. It will show all existing active / Inactive certificates.

OLS



|| C3 SCHOOLS

5. Create a new Certificate by clicking “Create a new Certificate”. It will show screen as below:



6. Download your private key file and X.509 to local folder. (E.g. C: AWSkeys).
7. If you fail to save Private Key file, AWS does not store it for you and you will lose it permanently.
8. If the case #7 happens, delete the new created certificate and follow steps #1 – #6 to save the file again.



|| C3 SCHOOLS

9. Store the downloaded pk & cert file into local directory (e.g c: AWSkeys)

C3 SCHOOLS



|| C3 SCHOOLS

10. Set the AWS Keys in environment as below: (For going to Environment variable follow step#6 of section 'B')

i. EC2_HOME= < <path where you have downloaded ec2 tools extracted as section 'A'>, e.g. C:AWSec2-api-tools-1.5.6.0

ii. EC2_CERT=<fully qualified path where cert-xxxxxx.pem file placed>

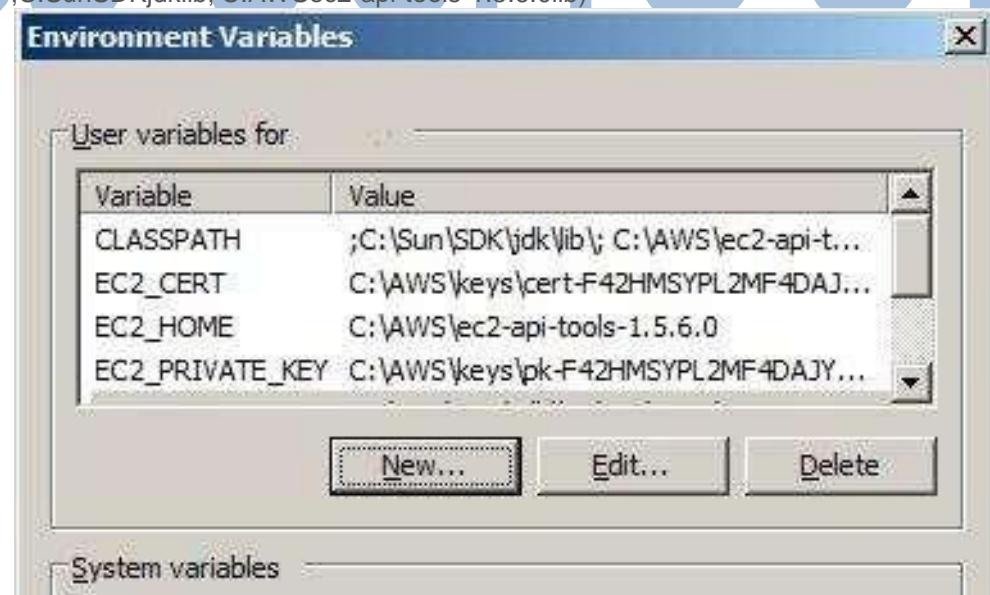
e.g. EC2_CERT= c:AWSkeys cert-F42xxxxxxxxxAR2xxxxxxUBA438xxxxD.pem

iii. EC2_PRIVATE_KEY=<fully qualified path where pk-xxxxx.pem file placed>

e.g. EC2_PRIVATE_KEY= c:Cloudkeys pk-F42xxxxxxxxxAR2xxxxxxUBA438xxxxD.pem

iv. PATH=; <JAVA_HOME>bin;< EC2_HOME >bin (e.g. PATH=:C:SunSDKjdbin;C:AWSec2-api-tools-1.5.6.0bin)

v. CLASSPATH= ; <JAVA_HOME>lib; < EC2_HOME >lib (e.g. CLASSPATH=:C:SunSDKjdklib; C:AWSec2-api-tools-1.5.6.0lib)





|| C3 SCHOOLS

11. Test your setup by executing following command in command line. ec2-run- instances or

ec2-describe-images –o amazon (Lists all public AMIs of Amazon)

```
C:\Administrator:C:\Windows\system32\cmd.exe
C:\AWS>ec2-run-instances
Required parameter 'AMI' missing (-h for usage)

C:\AWS>ec2-describe-images -o amazon | more
IMAGE aki-d4ca2dbd    aki-linux-2.6.18.92-92.el5xen-xfs/vmlinuz-2.6.18.92-92.e
l5xen.i386.aki.manifest.xml      amazon available   public          i386
kernel                          instance-store paravirtual    xen
IMAGE aki-46e7002f    aki-linux-2.6.21.7-2.fc8xen-xfs/vmlinuz.manifest.xml
amazon available   public          i386   kernel
instance-store paravirtual    xen
IMAGE ami-32dc075b    amazon/.NET Beanstalk HostManager v1.0.0.3      amazon
available   public          x86_64 machine        windows ebs
hvm     xen
BLOCKDEVICEMAPPING      /dev/sda1           snap-96ebaeb  35
IMAGE ami-6c9c3105    amazon/.NET Beanstalk HostManager v1.0.0.4      amazon
available   public          x86_64 machine        windows ebs
hvm     xen
BLOCKDEVICEMAPPING      /dev/sda1           snap-608be71e  30
IMAGE ami-cbd47ba2    amazon/Amazon Elastic MapReduce 2012-07-09-23-50-37 pvm/
ebs     amazon available   public          x86_64 machine aki-4e7d9527
ebs     paravirtual    xen
BLOCKDEVICEMAPPING      /dev/sda           snap-9c817ded  10
IMAGE ami-e9d27d80    amazon/Amazon Elastic MapReduce 2012-07-10-00-42-47 pvm/
ebs     amazon available   public          x86_64 machine aki-4e7d9527
ebs     paravirtual    xen
BLOCKDEVICEMAPPING      /dev/sda           snap-180bf769  10
IMAGE ami-8bb21de2    amazon/Amazon Elastic MapReduce 2012-07-10-16-56-36 pvm/
ebs     amazon available   public          x86_64 machine aki-4e7d9527
ebs     paravirtual    xen
BLOCKDEVICEMAPPING      /dev/sda           snap-ce28eebf  10
```

If it shows above output your setup of AWS API is complete.

How to Create or Delete an Amazon EBS Volume

The Amazon Elastic Block Store (Amazon EBS) offers persistent storage for Amazon EC2 instances. Amazon EBS volumes provide a scalable storage service, which persists independently of the instance life. An EBS volume is cheaper and scalable.

1. Go to the AWS console through the URL <http://aws.amazon.com/console>. Select the EC2 service. From the EC2 dashboard, select EBS Volumes or Volumes.



|| C3 SCHOOLS

EC2 Dashboard

Events

Tags

Reports

Limits

INSTANCES

Instances

Spot Requests

Reserved Instances

Dedicated Hosts

IMAGES

AMIs

Bundle Tasks

ELASTIC BLOCK STORE

Volumes

Snapshots

NETWORK & SECURITY

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

LOAD BALANCING

Load Balancers

Target Groups

Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Singapore) region:

0 Running Instances	0 Elastic IPs
0 Dedicated Hosts	0 Snapshots
2 Volumes	0 Load Balancers
2 Key Pairs	3 Security Groups
0 Placement Groups	

Build and run distributed, fault-tolerant applications in the cloud with [Amazon Simple Workflow 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 Asia Pacific (Singapore) region

Service Health

Service Status:

- ✓ Asia Pacific (Singapore): This service is operating normally

Availability Zone Status:

- ✓ ap-southeast-1a: Availability zone is operating normally
- ✓ ap-southeast-1b: Availability zone is operating normally

Scheduled Events

Asia Pacific (Singapore): No events

2. The EBS Volumes dashboard lists all the volumes available in that region. Click on “Create Volume”.

EC2 Dashboard

Events

Tags

Reports

Limits

INSTANCES

Instances

Spot Requests

Reserved Instances

Dedicated Hosts

IMAGES

AMIs

Bundle Tasks

ELASTIC BLOCK STORE

Volumes

Snapshots

Create Volume

Actions ▾

Filter by tags and attributes or search by keyword

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone	State
vol-23e205a7	30 GiB	gp2	100 / 3000	snap-098db55d...	September 15, 2016...	ap-southeast-1a	in-use	
vol-0653ed82	8 GiB	gp2	100 / 3000	snap-efff61911	September 4, 2016 ...	ap-southeast-1a	in-use	



|| C3 SCHOOLS

3. In the Create Volume dialog, select the volume types. AWS provides two types of volumes. A standard EBS volume generally provides about 100 IOPS on an average. However, in comparison AWS offers a new type of volume called Provisioned IOPS, which provides for a performance of up to 2000 IOPS.

The screenshot shows the AWS Management Console interface for creating a new EBS volume. The main window displays a list of existing volumes, while a modal dialog box titled "Create Volume" is open in the foreground. The "Volume Type" dropdown menu is open, showing several options: General Purpose SSD (GP2), General Purpose SSD (GP2) (selected), Provisioned IOPS SSD (IO1), Magnetic, Throughput Optimized HDD (ST1), and Cold HDD (SC1). Other fields in the dialog include "Size (GiB)" (set to 30 GiB), "Availability Zone" (set to ap-southeast-1a), and an "Encryption" checkbox. At the bottom right of the dialog are "Cancel" and "Create" buttons.

C3 SCHOOLS



|| C3 SCHOOLS

4. For the standard volume, provide the value for the volume size and select the availability zone and snapshot. The availability zone is very important as a volume can be attached to only an instance in the same availability zone. Click on “Yes, Create”.

Create Volume

Volume Type: Standard

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

IOPS: (Max: 4000 IOPS)

Availability Zone: us-west-2a

Snapshot: --- No Snapshot ---

! A volume type must be selected.

Cancel Yes, Create

C3 SCHOOLS

5. The volume will be created and available in the EBS dashboard. Since it has not been assigned to any instance it will be in the “available” state.

Name	Volume ID	Capacity	Volume Type	Snapshot	Created	Zone	State	Alarm Status	Attachment Information
empty	vol-eb382fe9	10 GB	standard	-	2014-03-05T10:02:33	us-west-2a	available	none	



|| C3 SCHOOLS

6. Select “Provisioned IOPS” in step#3, if the user wants to create a provisioned IOPS volume. Provide the value for IOPS, the size (GB) and select the availability zone. Click on “Yes, Create”.

C3 SCHOOLS



|| C3 SCHOOLS

Create Volume

Volume Type: Provisioned IOPS (io1)

Size: 500 GiB (Min: 1 GiB, Max: 1TiB)

IOPS: 800 (Max: 4000 IOPS)

Availability Zone: us-west-2a

Snapshot: --- No Snapshot ---

Cancel Yes, Create

7. The resultant volume type will be io1. It will display the IOPS in brackets.

empty	vol-eb382fe9	10 GB	standard	-	2014-03-05T10:02:33	us-west-2a	available	none
empty	vol-3d26313f	500 GB	io1 (800)	-	2014-03-05T10:12:30	us-west-2a	available	none

8. To delete a volume, select the volume and right click..Select “Delete Volume”.

Create Volume Actions

Viewing: All Volumes

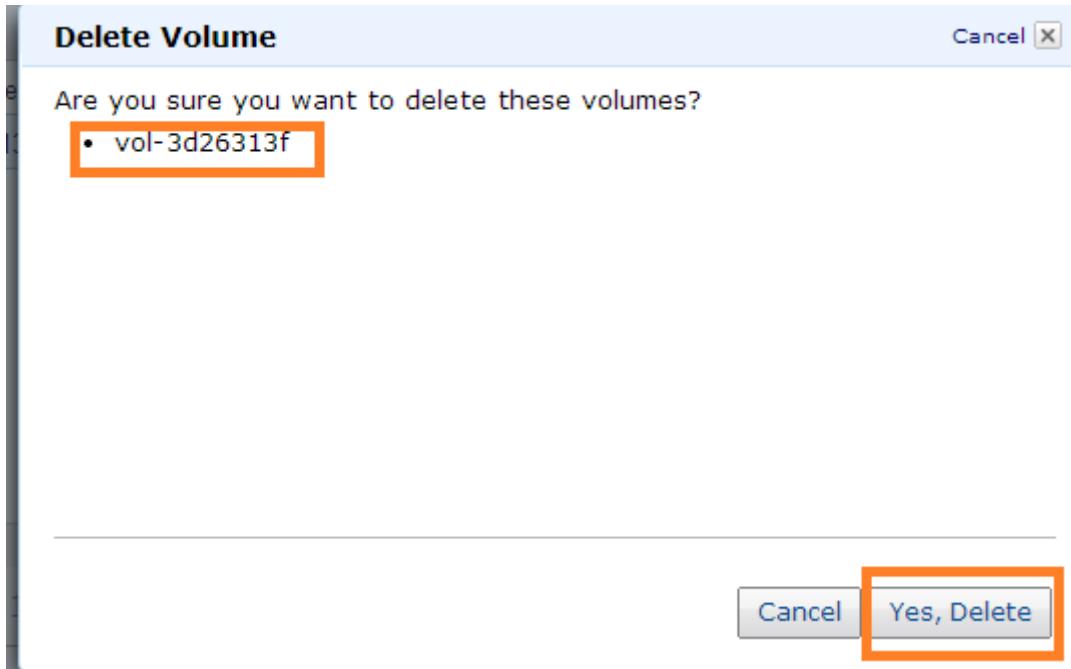
- Delete Volume
- Attach Volume
- Detach Volume
- Force Detach
- Create Snapshot
- Change Auto-Enable IO Setting

Name	Type	Snapshot	Created	Zone	State	Alarm Status	Attachment Information
empty	standard	-	2014-03-05T10:02:33	us-west-2a	available	none	
empty	io1 (800)	-	2014-03-05T10:12:30	us-west-2a	available	none	



|| C3 SCHOOLS

9. AWS will confirm before deleting the volume. Click on “Yes, Delete”.



10. The volume has been deleted, now it looks like as below.

Name	Volume ID	Capacity	Volume Type	Snapshot	Created	Zone	State	Alarm Status	Attachment Information
empty	vol-eb382fe9	10 GB	standard	-	2014-03-05T10:02:33	us-west-2a	available	none	

How to Create an AMI for Amazon EBS Backed Instances

This demonstrates how to create an Amazon EBS-backed AMI from a running Amazon EBS-backed instance.

1. Go to the AWS console through the URL <http://aws.amazon.com/console>. Select the EC2 service. From the EC2 dashboard, click on the Running Instances or the Instance link.



|| C3 SCHOOLS

Servies | Edit | Help | cloud at edureka | Oregon | Help |

EC2 Dashboard

- Events
- Tags
- Reports

INSTANCES

- Instances
- Spot Requests
- Reserved Instances

IMAGES

- AMI
- Bundle Tasks

ELASTIC BLOCK STORE

- Volumes
- Snapshots

NETWORK & SECURITY

- Security Groups
- Elastic IPs
- Placement Groups
- Load Balancers
- Virtual Private Cloud

Resources

You are using the following Amazon EC2 resources in the US West (Oregon) Region:

1 Running Instance	0 Elastic IPs
2 Volumes	0 Snapshots
19 Key Pairs	0 Load Balancers
0 Placement Groups	15 Security Groups

Focus on application development and offload database management to AWS – Try Amazon RDS Now! Hide

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

Scheduled Events

Popular AMIs on AWS Marketplace

© 2006 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use <https://aws.amazon.com/s2/privacy/usage-terms/> Feedback

2. Select the EBS backed running instance or launch an EBS backed instance.

Servies | Edit | Help | cloud at edureka | Oregon | Help |

EC2 Dashboard

- Events
- Tags
- Reports

INSTANCES

Instances

- Spot Requests
- Reserved Instances

IMAGES

ELASTIC BLOCK STORE

- Volumes
- Snapshots

NETWORK & SECURITY

- Security Groups
- Elastic IPs
- Placement Groups
- Load Balancers
- Key Pairs
- Network Interfaces

Actions ▾

Filter: EBS root device ▾ All instance types ▾ Search instances 1 to 1 of 1 Instances

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS	Public IP
i-957b1fc	i-957b1fc	t1.micro	us-west-2b	running	2/2 checks	None	ec2-54-186-55-223.us-west-2.compute.amazonaws.com	54.186.55.223

Instance: i-957b1fc Public DNS: ec2-54-186-55-223.us-west-2.compute.amazonaws.com

Description Status Checks Monitoring Tags

Instance ID: i-957b1fc Public DNS: ec2-54-186-55-223.us-west-2.compute.amazonaws.com

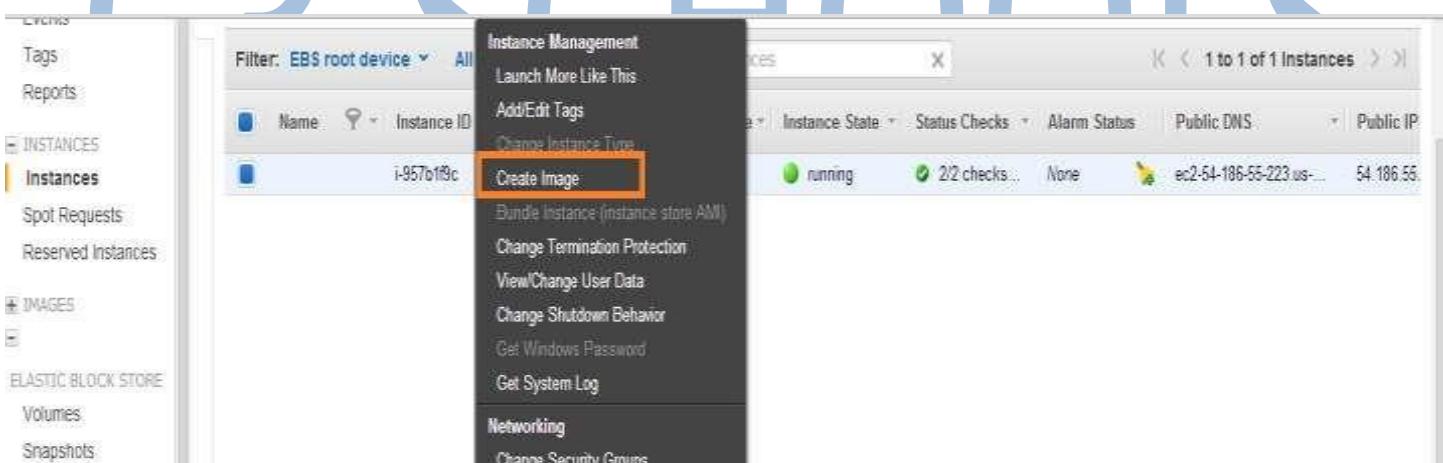
Instance state: running Public IP: 54.186.55.223

3. An AMI serves as the basic unit of deployment for services delivered using EC2. Thus, when the user launches an instance from an AMI, it will have all the software installed or available data of the current running instance.

4. Configure the instance with any random data / install some software or create some temporary files or directories, as shown below.

```
[ec2-user@ip-10-254-9-56 ~]$ sudo mkdir test1
[ec2-user@ip-10-254-9-56 ~]$ sudo mkdir test2
[ec2-user@ip-10-254-9-56 ~]$ sudo vi testFile.txt
[ec2-user@ip-10-254-9-56 ~]$ ls
test1  test2  testFile.txt
[ec2-user@ip-10-254-9-56 ~]$ sudo cat testFile.txt
Hi This is Test File
[ec2-user@ip-10-254-9-56 ~]$
```

5. Select the instance and click on the “Actions” menu, as shown in step#2. Click on “Create Image (EBS AMI)”.



6. The AMI creation wizard will ask for the AMI name, description, and the other required parameters. Provide details, such as the AMI Name, and AMI description.

a. By default when the AMI is created, EC2 shuts down the instance. Next, it takes the snapshots of any attached volumes and finally creates and registers the AMI. After this, EC2 reboots the instance. The instance may not respond or be available temporarily during this process. Select the option “No Reboot” if the user does not want to reboot the instance. If the “No Reboot” option is selected, then AWS does not guarantee the file system integrity of the created image.



|| C3 SCHOOLS

- b. The user can also modify the root volume. Select the root volume tab. The user can modify the volume size or volume type. Click on “Save” to save the changes made on the root volume.

C3 SCHOOLS



|| C3 SCHOOLS

Create Image

Instance ID	i-957b1f9c
Image name	TestEBSAMICreation
Image description	Test EBS backend AMI Creation
No reboot	<input type="checkbox"/>

Instance Volumes

Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination
Root	/dev/sda1	snap-6415a45a	10	Standard	N/A	<input checked="" type="checkbox"/>

Total size of EBS Volumes: 10 GiB
When you create an EBS image, an EBS snapshot will also be created for each of the above volumes.

[Cancel](#) [Create Image](#)

7. To add an additional EBS volume while launching an instance, configure it by using the EBS Volumes tab. First select the EBS Volumes tab.



|| C3 SCHOOLS

Create Image X

Instance ID: i-957b1f9c

Image name: TestEBSAMICreation

Image description: Test EBS backend AMI Creation

No reboot:

Instance Volumes

Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination
Root	/dev/sda1	snap-6415a45a	10	Standard	N/A	<input checked="" type="checkbox"/>
EBS	/dev/sdb	Search (case sensitive)	8	Standard	N/A	<input type="checkbox"/> X

Add New Volume

Total size of EBS Volumes: 10 GiB
When you create an EBS image, an EBS snapshot will also be created for each of the above volumes.

[Cancel](#) **Create Image**

C3 SCHOOLS



|| C3 SCHOOLS

8. Fill in details, such as the Device, Snapshot, Size and Volume type and click on the Add button. When an AMI is configured with an additional EBS volume, and an instance is launched with this new AMI, the additional volumes are automatically attached to the instance

Create Image

Instance ID: i-957b1f9c

Image name: **TestEBSAMICreation**

Image description: **Test EBS backend AMI Creation**

No reboot:

Instance Volumes

Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination
Root	/dev/sda1	snap-6415a45a	10	Provisioned IOPS	100	<input checked="" type="checkbox"/>

Add New Volume

Total size of EBS Volumes: 8 GiB
When you create an EBS image, an EBS snapshot will also be created for each of the above volumes.

Create Image

9. To add an instance store volume, click on Instance Store Volumes, select the Instance Store and Device, and click on Add. When the user launches an instance from the new AMI, the additional volumes are automatically initialized and mounted. The data in an instance store volume is not persistent. Thus, it must be used only for temporary data storage. This option is available for all the instance types except the micro instance.

Click on the “Create Image” button after configuring all the parameters.



|| C3 SCHOOLS

10. AWS will provide a confirmation about the AMI creation request. It provides the AMI ID. Click on the “View pending image ami-..” link or close button.

Create Image

✓ Create Image request received.

[View pending image ami-72adc242](#)

Any snapshots backing your new EBS image can be managed on the [snapshots screen](#) after successful image creation.

Close

11. The View pending image link will take the user to the AMI console. It displays that the AMI creation is in progress.

Filter: Owned by me ▾ All images ▾ All platforms ▾ X | < 1 to 1 of 1 Images > ▾

Name	AMI Name	AMI ID	Source	Owner	Visibility	Status	Platform	Root Device	Virtualization
	TestEBSAMIC...	ami-72adc242	835988942473/T...	835988942473	Private	pending	Other Linux	ebs	paravirtual

12. Once the AMI has been created, it will be in an available state.

Launch Actions ▾

Filter: Owned by me ▾ All images ▾ All platforms ▾ X | < 1 to 1 of 1 Images > ▾

Name	AMI Name	AMI ID	Source	Owner	Visibility	Status	Platform	Root Device	Virtualization
	TestEBSAMIC...	ami-72adc242	835988942473/T...	835988942473	Private	available	Other Linux	ebs	paravirtual



|| C3 SCHOOLS

13. If a new instance is launched from this AMI, it will show the output as given below. The reason for the additional volumes or the ephemeral storage is because the user configured it.

Viewing: All Volumes Search | < < 1 to 2 of 2 Items > >

Name	Volume ID	Capacity	Volume Type	Snapshot	Created	Zone	State	Alarm Status	Attachment Information
empty	vol-eb382fe9	10 GiB	standard	--	2014-03-05T10:02:33	us-west-2a	available	none	
empty	vol-139ba51d	8 GiB	standard	snap-6415a45a	2014-03-07T07:11:12	us-west-2b	in-use	none	i-957b19c:/dev/sda1 (attach)

Steps to create an EBS Snapshot:

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.

The screenshot shows the Amazon EC2 Management Console interface. On the left, there's a navigation sidebar with links like EC2 Dashboard, Events, Tags, Instances, Spot Requests, Reserved Instances, AMIs, Bundle Tasks, Volumes, Snapshots, Security Groups, Elastic IPs, Placement Groups, Load Balancers, and Key Pairs. The main content area has several sections: 'Resources' which lists 2 Running Instances, 4 Volumes, 7 Key Pairs, 0 Placement Groups, 1 Elastic IP, 1 Snapshot, 0 Load Balancers, and 4 Security Groups; 'Create Instance' with a 'Launch Instance' button; 'Service Health' showing 'US West (Oregon)' is operating normally; 'Scheduled Events' showing 'No events'; and a sidebar for 'Account Attributes' and 'Additional Information'. A note at the bottom says 'Note: Your instances will launch in the US West (Oregon) region.'

There are two ways to create an EBS Snapshot, either go to the Snapshot option directly from the EC2 Dashboard or as stated in Step



|| C3 SCHOOLS

2. Click **Snapshots** in the navigation pane.

The console displays a list of current snapshots if created any.

You do not have any snapshots stored.
Click the Create Snapshot button to back up a volume.

Create Snapshot

3. Click **Create Snapshot**.

The Create Snapshot dialog box appears.

You do not have any snapshots stored.
Click the Create Snapshot button to back up a volume.

Create Snapshot

Volume: Select Volume

Name:

Description:

Cancel Create



|| C3 SCHOOLS

4. Select the volume to create a snapshot for and click **Create**.

The screenshot shows the AWS EC2 Management Console with the 'Schemas' tab selected. On the left, a sidebar lists services: EC2 Dashboard, Events, Tags, Instances, AMIs, Bundle Tasks, Elastic Block Storage, Volumes, Snapshots, Network & Security, Security Groups, Elastic IPs, Placement Groups, Load Balancers, and Key Pairs. The 'Snapshots' section is currently active. At the top, there are buttons for 'Create Snapshot', 'Delete', 'Permissions', 'Create Volume', 'Create Image', and 'Copy'. Below these buttons, a search bar says 'Viewing: Owned By Me' and a 'Search' button. A message '1 to 1 of 1 items' is displayed. A table lists one item:

Name	Snapshot ID	Capacity	Description	Status	Started	Progress
host_wordpress	snap-c0d8ef	8 GB	trial_snapshot	Pending	2013-07-31 15:43 GMT+053	

At the bottom of the page, a message says '0 Elastic Block Store Volume Snapshots selected' and 'Select a snapshot above'. The footer includes links for 'Feedback', 'Privacy Policy', and 'Terms of Use', along with a copyright notice: '© 2006 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved.' The bottom right corner shows the date and time: '13:43 31-07-2013'.

Amazon EC2 begins creating the snapshot.

5. Or you can go to the Elastic Block Storage Volumes.
 6. Select the volume that you want to create a snapshot for.
 7. Go to the 'Actions' menu and Select 'Create Volume'.
- This will begin creating the Snapshot for your EBS Volume.



|| C3 SCHOOLS

The screenshot shows the AWS EC2 Management console with the 'Volumes' section selected. A context menu is open over a volume named 'empty' (Volume ID: vol-1dfe4674). The 'Create Snapshot' option is highlighted in blue. The main table lists four volumes, each with a snapshot attached:

Name	Type	Snapshot	Created	Zone	State	Alarm Status	Attachment Information		
empty	standard	snap-708e8348	2013-07-31T06:51:46	us-west-2a	in-use	none	i-51e62c2 (linux_tna111)		
empty	standard	snap-f23ec1c8	2013-07-31T08:56:22	us-west-2c	in-use	none	i-04ab2c33 (tna1_windows)		
empty	standard	snap-098f8231	2013-07-29T09:43:35	us-west-2b	in-use	none	i-5424c1 (host):/dev/sda1		
empty	8 GB	vol-1dfe4674	standard	snap-7f891947	2013-07-29T10:38:11	us-west-2b	in-use	none	i-c78501ff (host_wordpres)

At the bottom of the screenshot, there is a status bar with icons and text: "© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Feedback".

The yellow pending button becomes green and percentage of the completion is shown.



|| C3 SCHOOLS

The screenshot shows the AWS EC2 Management console interface. On the left, there's a sidebar with navigation links like EC2 Dashboard, Instances, Images, and Elastic Block Store. The main area has tabs for Create Snapshot, Delete, Permissions, Create Volume, Create Image, and Copy. A search bar is at the top right. Below it, a table lists a single snapshot entry:

Name	Snapshot ID	Capacity	Description	Status	Started	Progress
host_wordpress	snap-c5dbaeff	8 GB	trial_snapshot	completed	2013-07-31 15:43 GMT+0530	available (100%)

A modal window is open over the table, titled "Elastic Block Store Volume Snapshot selected". It displays detailed information about the snapshot:

Description		Tags	
Snapshot ID:	snap-c5dbaeff	Status:	completed
Volume:	vol-1dfe4674	Capacity:	8 GB
Owner:	039988942473	Started:	2013-07-31 15:43 GMT+0530
Description:	trial_snapshot	Product Codes:	

At the bottom of the page, there's a footer with copyright information and a feedback link.

When the green button shows 100% , it means snapshot is now created.

You can also create a copy of this snapshot, delete it and add permissions to it.



|| C3 SCHOOLS

How to Create an EBS Volume from a Snapshot

Amazon Elastic Block Store (Amazon EBS) offers persistent storage for the Amazon EC2 instances through the EBS volumes. Snapshots can be used to create new Amazon EBS volumes, which will have all the available data snapped during the point-in snapshots.

This demonstrates how to create a volume from a snapshot:

1. Go to the AWS console through the URL <http://aws.amazon.com/console>. Select the EC2 service. From the EC2 dashboard, select EBS Snapshots or Snapshots.

The screenshot shows the AWS EC2 Dashboard. On the left, there's a navigation menu with options like Services, Instances, Images, and Network & Security. The main area is titled 'Resources' and displays the following data:

Category	Value
Running Instances	1
Volumes	2
Key Pairs	19
Placement Groups	0
Elastic IPs	0
Snapshots	1
Load Balancers	0
Security Groups	15

A callout box highlights the '1 Snapshot' entry. Below the resources, there's a 'Create Instance' section with a 'Launch Instance' button, and a 'Service Health' section showing 'Service Status: US West (Oregon)' and 'Availability Zone Status: us-west-2a'. On the right side, there are sections for 'Account Attributes' (Supported Platforms: VPC, Default VPC: vpc-ctab8aa7), 'Additional Information' (Getting Started Guide, Documentation, All EC2 Resources, Forums, Pricing, Contact Us), and 'Popular AMIs on AWS Marketplace' (Vyatta Virtual Router/Firewall/VPN, provided by Vyatta, Inc., rating 5 stars, pay-by-the-hour usage, view all networking software).



|| C3 SCHOOLS

2. The snapshot dashboard lists all the snapshots owned by the user in that region. Select a snapshot from which the user wants to create the volume. Click on the “Create Volume” button.

C3 SCHOOLS



|| C3 SCHOOLS

The screenshot shows the AWS EC2 Dashboard with the 'Schemas' section selected. Under 'ELASTIC BLOCK STORE', 'Schemas' is also selected. A table lists snapshots, with one row highlighted by a red box. The highlighted row contains the following information:

Name	Snapshot ID	Capacity	Description	Status	Started	Progress
empty	snap-98a6bf69	8 GB	Created by CreateImage(i-057b19c) for ami-7	completed	2014-03-07 14:53 GMT+053	available (100%)

Below the table, a modal window titled 'Elastic Block Store Volume Snapshot selected' displays the details of the selected snapshot:

Description	Tags
Snapshot ID: snap-98a6bf69	
Status: completed	Progress: 100%
Volume: vol-139ba51d	Capacity: 8 GB

At the bottom of the page, there is a copyright notice: "© 2006 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved." and links to "Privacy Policy" and "Terms of Use".

3. Select the volume type, size of the volume, IOPS (if volume type is Provisioned IO), and the availability zone. The snapshot ID will automatically be selected based on the snapshot selected in step#2.

Click on the “Yes, Create” button.

Create Volume

Snapshot: snap-98a6bf69 -- Created by CreateImage(i... vol-139ba51d)

Volume Type: Provisioned IOPS (io1)

Size: 100 GiB (Min: 8 GiB, Max: 1TiB)

IOPS: 100 (Max: 4000 IOPS)

Availability Zone: us-west-2a

Cancel **Yes, Create**



|| C3 SCHOOLS

4. The new volume from the snapshot will be created and be in an available state as it is not attached to any instance.

Name	Volume ID	Capacity	Volume Type	Snapshot	Created	Zone	State	Alarm Status	Attachment Information
empty	vol-eb382fe9	10 GB	standard	-	2014-03-05T10:02:33	us-west-2a	available	none	
empty	vol-ea3c2de8	100 GB	io1 (100)	snap-98a6bf69	2014-03-07T10:05:14	us-west-2a	available	none	
empty	vol-139ba51d	8 GiB	standard	snap-6415a45a	2014-03-07T07:11:12	us-west-2b	in-use	none	i-957b1f9c/dev/sda1 (attai)

How to Attach an EBS Volume with an AWS EC2 Windows Instance

Amazon EBS volumes provide a scalable storage service, which persists independently of the instance life. A user can attach an EBS volume to an EC2 instance. It is mandatory that both the volume as well as the instance be in the same availability zone. The user can assign a maximum of 16 EBS volumes to an instance.

A user has to specify the device name while attaching an EBS volume to an EC2 instance. When a volume is attached to a Windows instance, it is recommended to format the device and mount it as a drive.

1. Go to the AWS Console and select the EC2 Service. From the EC2 dashboard, Click on the 'Running Instances'.



|| C3 SCHOOLS

EC2 Dashboard
Events
INSTANCES
Instances
Spot Requests
Reserved Instances
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Load Balancers
Key Pairs
Network Interfaces

Getting Started

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 region.

Service Health

Service Status

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

[View complete service health details](#)

Availability Zone Status

Current Status	Details
✓ us-west-2a	Availability zone is operating normally
✓ us-west-2b	Availability zone is operating normally
✓ us-west-2c	Availability zone is operating normally

My Resources

You are using the following Amazon EC2 resources in the region:

1 Running Instance

0 Elastic IPs

1 EBS Volume

2 EBS Snapshots

2 Key Pairs

0 Load Balancers

0 Placement Groups

1 Security Group

Events

✓ US West (Oregon): No events

Related Links

- [Getting Started Guide](#)
- [Documentation](#)
- [All EC2 Resources](#)
- [Find software on AWS Marketplace](#)
- [Forums](#)
- [Feedback](#)
- [Report an Issue](#)

C3 SCHOOLS



|| C3 SCHOOLS

2. Launch a Windows instance.

The screenshot shows the AWS Instances page. At the top, there are buttons for "Launch Instance" and "Actions". Below that, a search bar and filters for "Viewing: Running Instances" and "All Instance Types". On the right, there are navigation icons. The main table lists one instance:

Name	Instance	AMI ID	Root Device	Type	State	Status Checks	Alarm Status	Monitoring	Security Group
<input checked="" type="checkbox"/> Windows Instance	i-caca71f8	ami-167af226	ebs	t1.micro	running	2/2 checks	none	basic	default

3. Go to Volumes and check the currently attached volume information. Create an additional volume in the same zone where the instance is running.

The screenshot shows the AWS Volumes page. The table lists three volumes:

<input type="checkbox"/>	empty	vol-852eb2bc	8 GiB	standard	snap-921bb2b4	2013-01-25T12:59:45	us-west-2a	in-use	none	i-44de6576 (Te)
<input checked="" type="checkbox"/>	empty	vol-bcb72885	20 GiB	standard	--	2013-01-25T18:11:12	us-west-2b	available	none	
<input type="checkbox"/>	empty	vol-fe23bfc7	30 GiB	standard	snap-94f7a8b2	2013-01-25T13:48:23	us-west-2b	in-use	none	i-caca71f8 (Wi)

4. Select the volume to be attached. From the “Actions” menu, select “Attach Volume”.

The screenshot shows the AWS Volumes page with the "Actions" dropdown open. The dropdown menu includes "Delete Volume" and "Attach Volume". The "Attach Volume" option is highlighted with a red box. The main table lists three volumes:

Name	Vol	Detach Volume	Snapshot	Created	Zone	State
<input type="checkbox"/>	empty		snap-921bb2b4	2013-01-25T12:59:45	us-west-2a	in-use
<input checked="" type="checkbox"/>	empty		--	2013-01-25T13:59:34	us-west-2b	available
<input type="checkbox"/>	empty		snap-94f7a8b2	2013-01-25T13:48:23	us-west-2b	in-use



|| C3 SCHOOLS

5. AWS will ask for the EC2 instance, where the EBS volume will be attached. The device name should also be provided.

Click on "Yes, Attach".



6. The volume will be attached to the instance and the instance information will be displayed in the volume attachment information.

<input type="checkbox"/>	empty	vol-852eb2bc	8 GiB	standard	snap-921bb2b4	2013-01-25T12:59:45	us-west-2a	in-use	none	i-44de6576 (Test)/dev/sc
<input type="checkbox"/>	empty	vol-fe23bfc7	30 GiB	standard	snap-94f7a8b2	2013-01-25T13:48:23	us-west-2b	in-use	none	i-caca71f8 (Windows Inst)
<input checked="" type="checkbox"/>	empty	vol-bcb72885	20 GiB	standard	-	2013-01-25T18:11:12	us-west-2b	in-use	none	i-caca71f8 (Windows Inst)

7. When the user checks the instance information, as explained in step#2, the two devices will be displayed. The newly attached device is shown as xvdf.

<input checked="" type="checkbox"/>	Name	Instance	AMI ID	Root Device	Type	State	Status Checks	Alarm Status	Monitoring	Security
<input checked="" type="checkbox"/>	Windows Instance	i-caca71f8	ami-167af226	ebs	t1.micro	running	Loading...	none	basic	default

RAM Disk ID:	-	Platform:	windows
Key Pair Name:	-	Kernel ID:	-
Monitoring:	basic	AMI Launch Index:	0
Elastic IP:	-	Root Device:	sda1
Root Device Type:	ebs	Tenancy:	default
IAM Role:	-	Lifecycle:	normal
EBS Optimized:	false		
Block Devices:	<input type="checkbox"/> sda1 <input type="checkbox"/> xvdf		



|| C3 SCHOOLS

- When the user clicks on the xvdf device, the device information will be displayed.



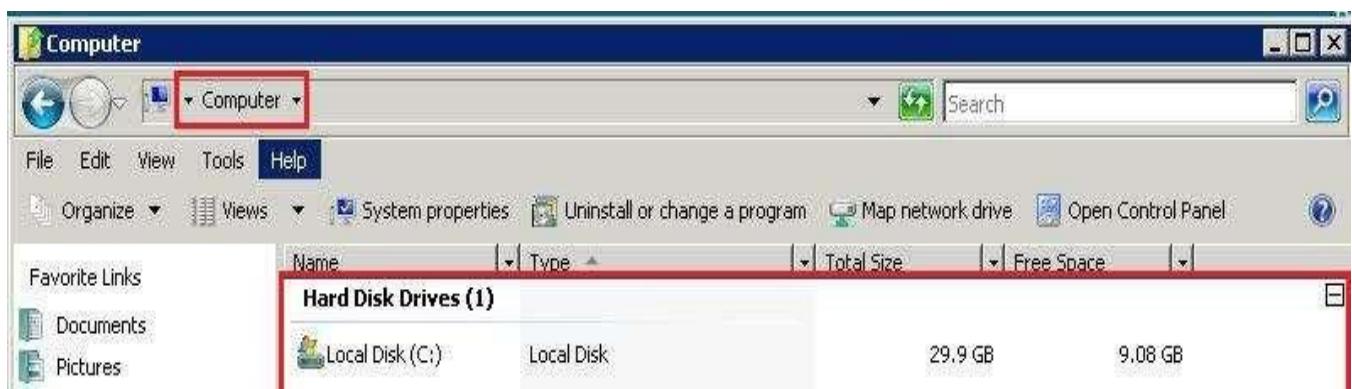
- The user is required to format the attached device before using it.

The Amazon Elastic Block Store (Amazon EBS) offers persistent storage for the Amazon EC2 instances. We saw that an EBS volume can be attached to AWS Windows instance for vertical scalability.

This demonstrates how to format an EBS volume attached to a Windows instance:

- Create an EBS volume and attach it to Windows Instance.

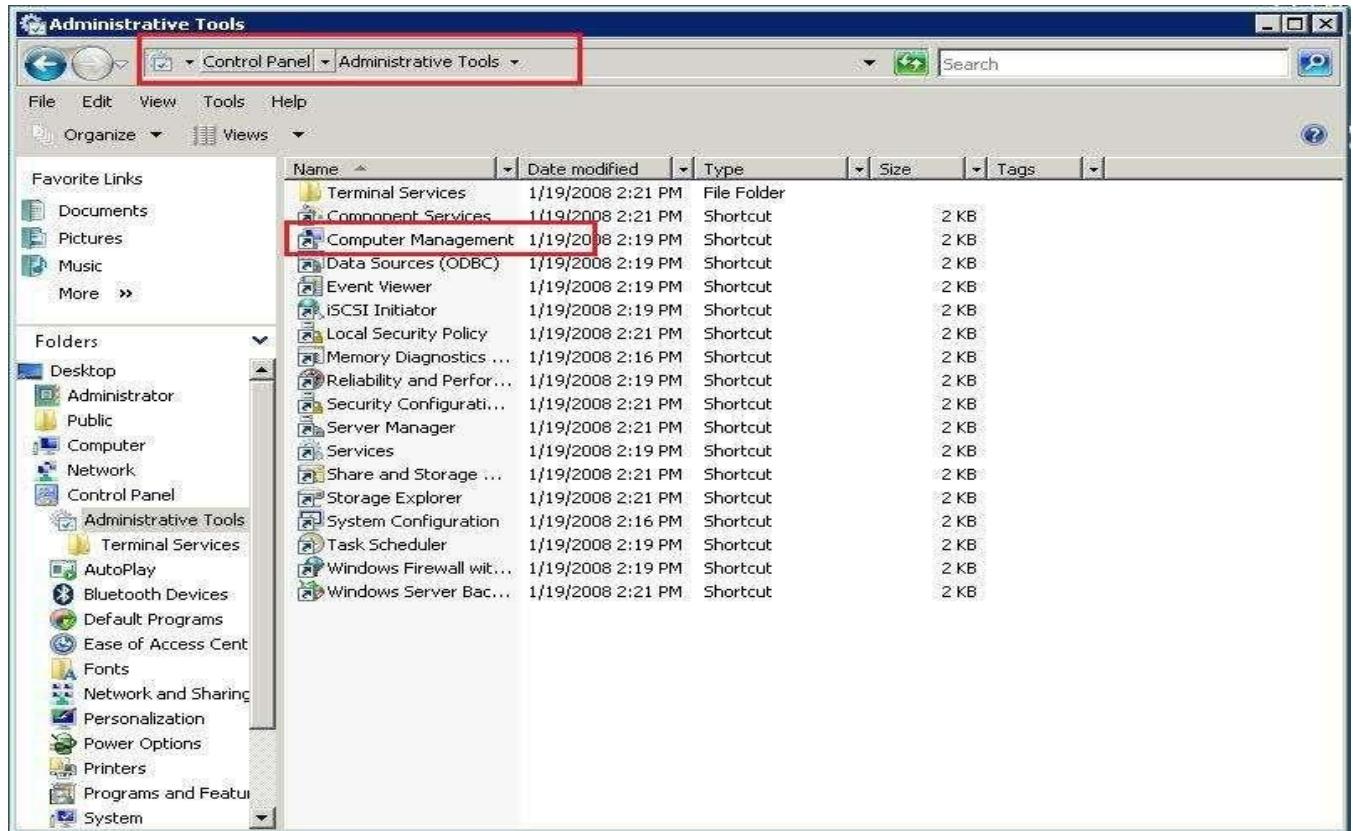
- Login to the Windows instance. Currently only one disk drive (C Drive) is available in the instance. The new device (volume), which is mounted, is still not available in the instance.





|| C3 SCHOOLS

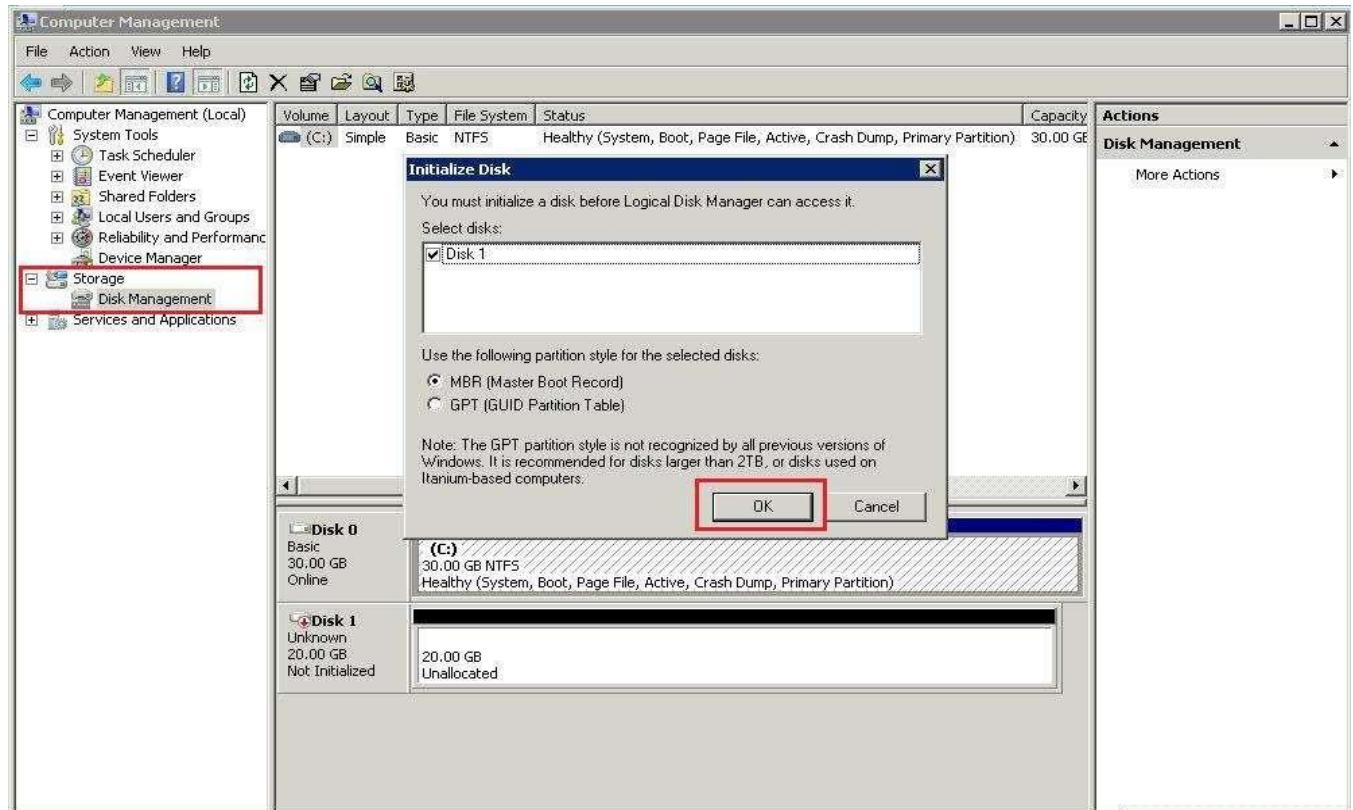
3. Go to the Control Panel -> Administrative Tools.Click on Computer Management.





|| C3 SCHOOLS

4. Click "Disk Storage". If Windows asks to initialize the disk, click on the "OK" button.

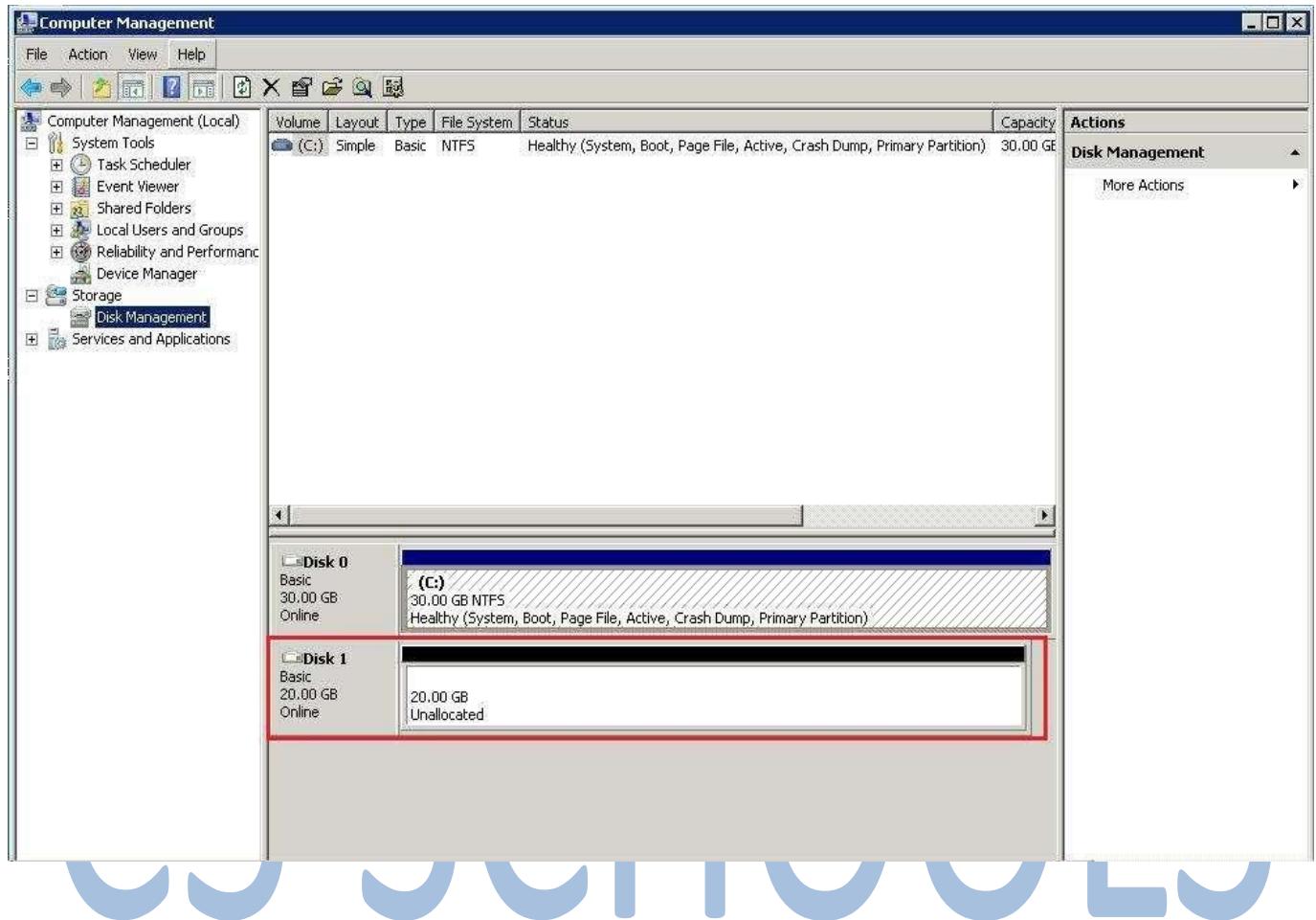


CS SUMMERS

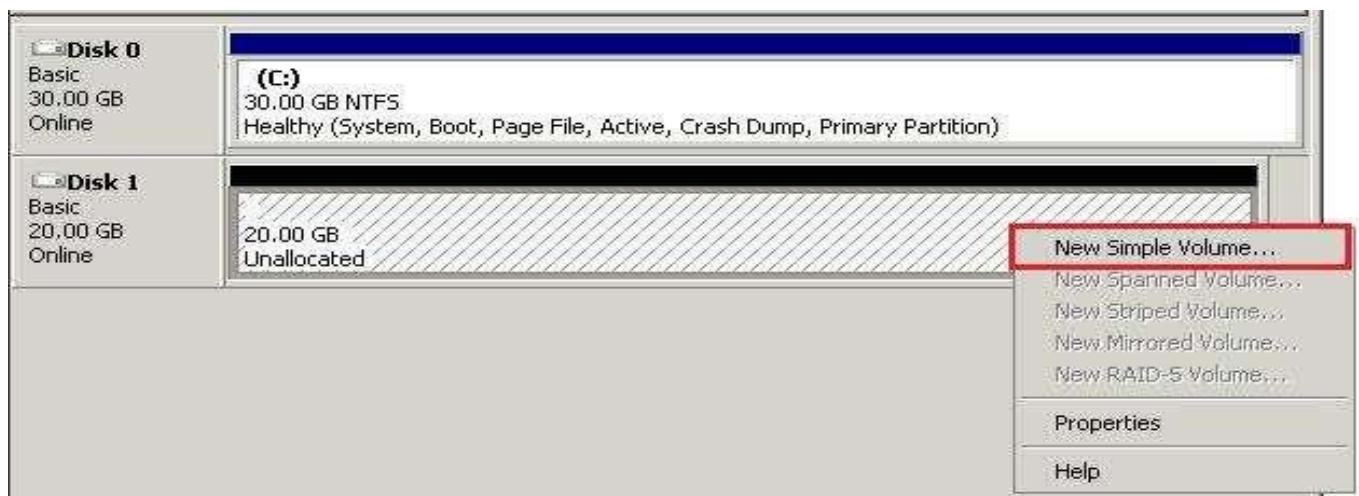


|| C3 SCHOOLS

5. The new attached volume will be displayed as "Disk1". It is still unallocated.



6. Right click on "Disk 1" and select "New Simple Volume".





|| C3 SCHOOLS

7. Windows will show the New Simple Volume Wizard. The user can select the default options or the options, such as the drive, and size as per requirement.





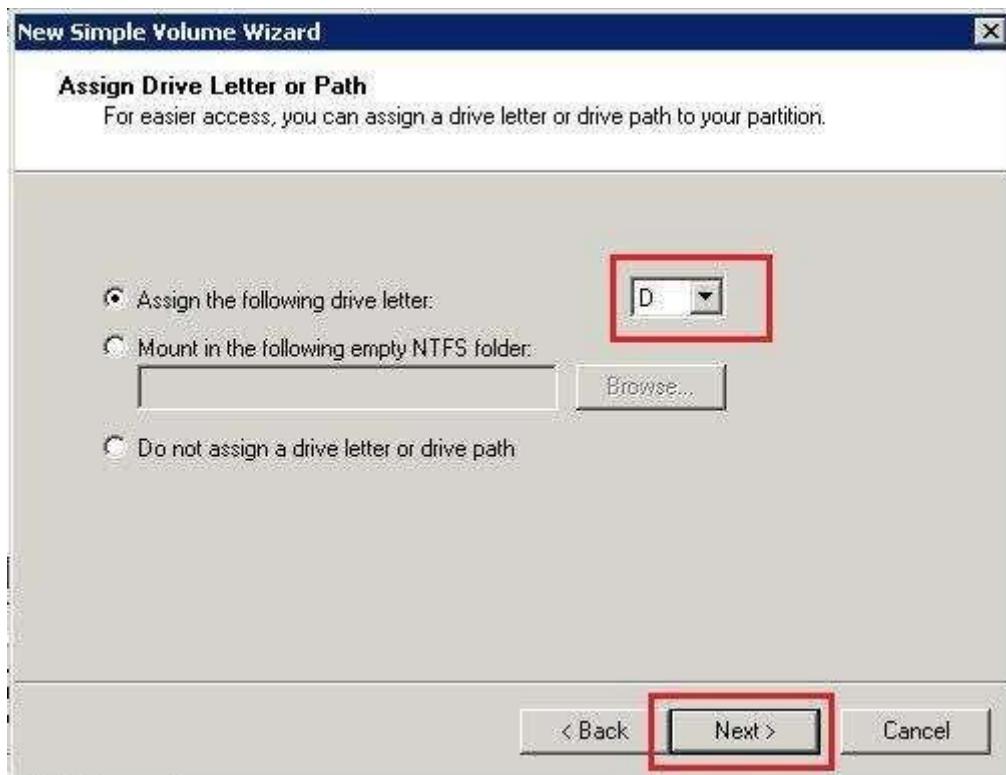
|| C3 SCHOOLS



C3 SCHOOLS



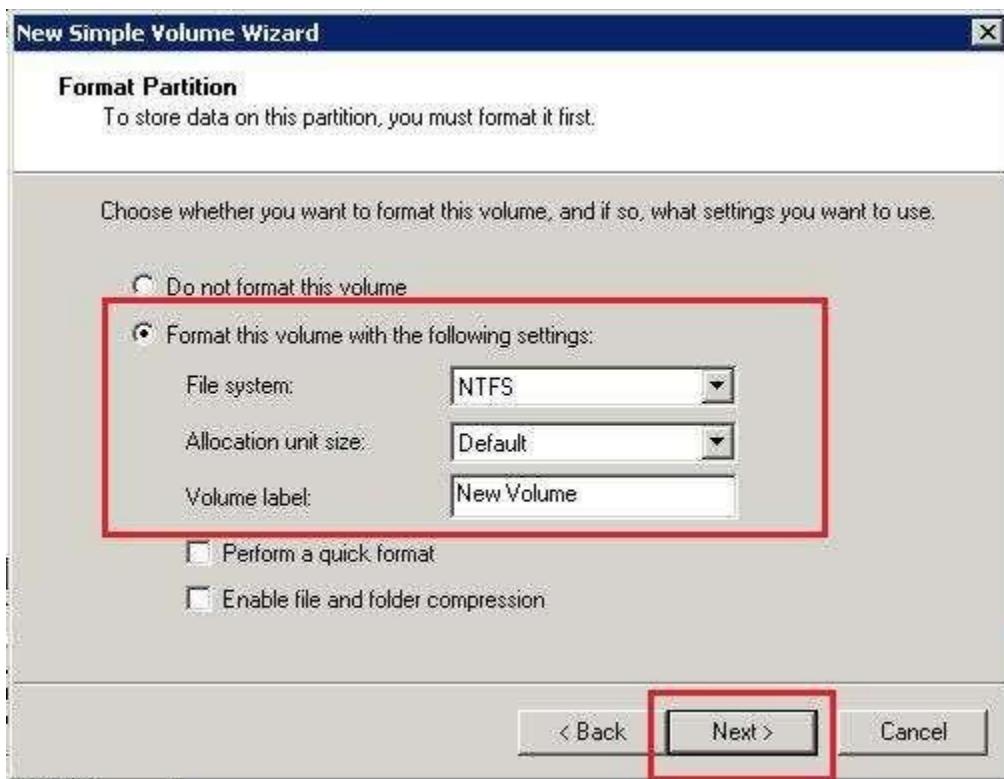
|| C3 SCHOOLS



C3 SCHOOLS



|| C3 SCHOOLS

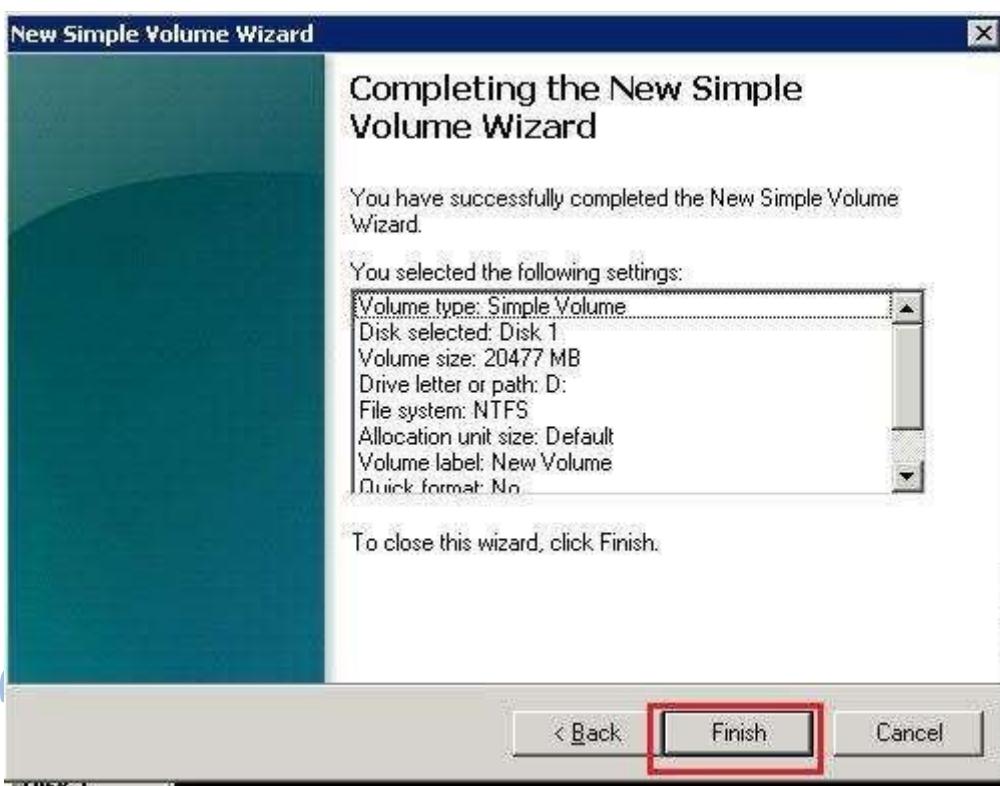


C3 SCHOOLS

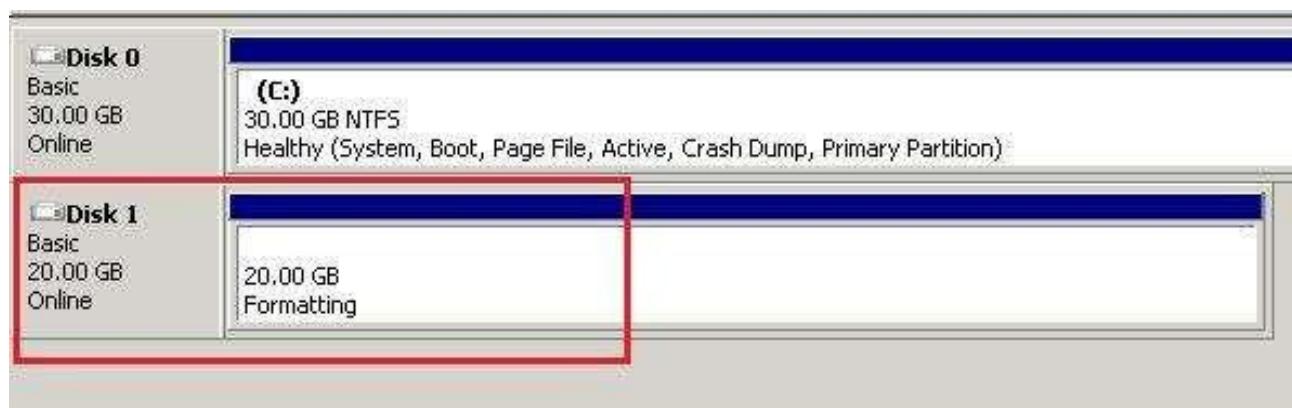


|| C3 SCHOOLS

8. On completion of the above mentioned steps, the New Simple Volume Wizard will show the summary of all the steps for review. Click on the “Finish” button.



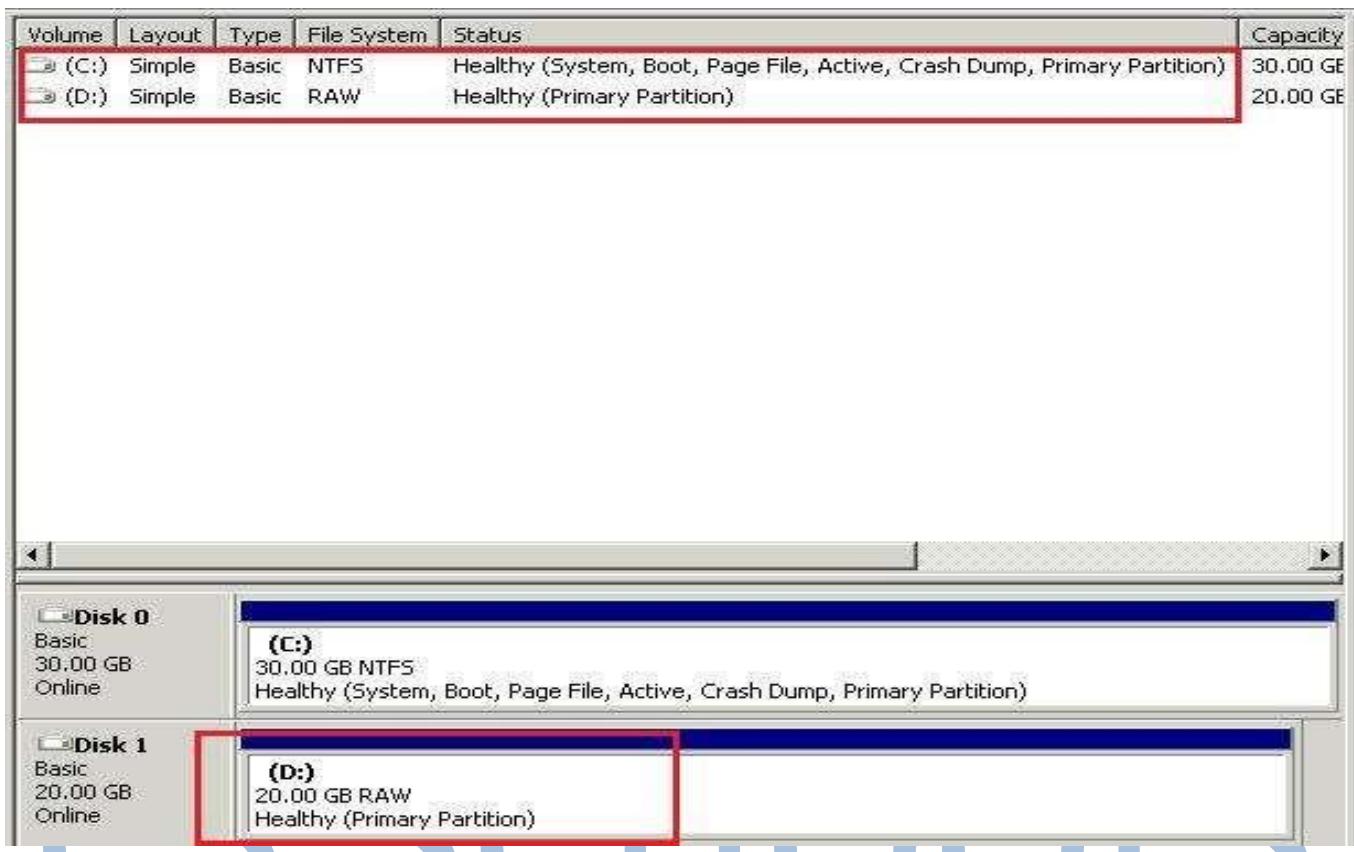
9. On completion of the above mentioned steps, the volume will be formatted.





|| C3 SCHOOLS

10. The new volume will be available after formatting as “D Drive”.



11. The new device will now be available in the computer.

Hard Disk Drives (2)				
	Local Disk (C:)	Local Disk	29.9 GB	9.08 GB
	Local Disk (D:)	Local Disk	19.9 GB	19.9 GB



|| C3 SCHOOLS

How to Launch an EBS Optimized EC2 Instance with a Provisioned IOPS Volume

This demonstrates how to launch an EBS-Optimized EC2 Linux Instance using the provisioned IOPS volume.

A standard EC2 EBS (Elastic Block Store) volume will generally provide about 100 IOPS on an average. However, in comparison AWS has offered a new type of volume called Provisioned IOPS, which provides for a performance of up to 2000 IOPS.

An EBS-Optimized instance is provisioned with dedicated throughput to EBS. Use the EBS optimized instance for maximum performance and full utilization of the IOPS provisioned on an EBS volume.

C3 SCHOOLS
Login to your AWS console.

1. Select the EC2 Service. It launches the EC2 dashboard. Go to the Instances section and click on “Launch Instance” to launch an EC2 instance.

The screenshot shows the AWS EC2 Instances dashboard. At the top, there is a navigation bar with 'Launch Instance' and 'Actions' dropdown menus. Below the navigation bar, there is a search bar labeled 'Viewing: Running Instances' and a 'Search' button. To the right of the search bar are navigation icons. The main area displays a table header with columns: Name, Instance, AMI ID, Root Device, Type, State, Status Checks, Alarm Status, Monitoring, and Security Group. A message at the bottom of the table says 'No Instances found.'



|| C3 SCHOOLS

2. The Launch wizard has multiple options, such as “Classic Wizard”, “Quick Launch” and “AWS Marketplace”. Quick Launch contains pre-configured steps, whereby it will skip some steps and launch with the default configurations. AWS Marketplace is used to launch the instance from the AWS online store.

Select “Classic Wizard” and click on “Continue”.

Create a New Instance

Select an option below:

Classic Wizard

Launch an On-Demand or Spot instance using the classic wizard with fine-grained control over how it is launched.

Quick Launch Wizard

Launch an On-Demand instance using an editable, default configuration so that you can get started in the cloud as quickly as possible.

AWS Marketplace

AWS Marketplace is an online store where you can find and buy software that runs on AWS. Launch with 1-Click and pay by the hour.

Launch with the Classic Wizard

Request Instances Wizard

Choose an Amazon Machine Image (AMI) from one of the tabbed lists below by clicking its Select button.

Quick Start | My AMIs | Community AMIs

AMI Name	Description	AMI ID	Region	Actions
Basic 32-bit Amazon Linux AMI 2011.02.1 Beta (AMI ID: ami-8c1fce6)	Amazon Linux AMI Base 2011.02.1, EBS boot, 32-bit architecture with Amazon EC2 AMI Tools.	ami-8c1fce6	US West (Oregon)	<input checked="" type="button"/> Selected
Basic 64-bit Amazon Linux AMI 2011.02.1 Beta (AMI ID: ami-8c1fce7)	Amazon Linux AMI Base 2011.02.1, EBS boot, 64-bit architecture with Amazon EC2 AMI Tools.	ami-8c1fce7	US West (Oregon)	<input type="button"/> Select
Red Hat Enterprise Linux 6.1 32 bit (AMI ID: ami-0cb64265)	Red Hat Enterprise Linux version 6.1, EBS-boot, 32-bit architecture, Root Device Size: 7.0GB	ami-0cb64265	US West (Oregon)	<input type="button"/> Select
Red Hat Enterprise Linux 6.1 64 bit (AMI ID: ami-5e937037)	Red Hat Enterprise Linux version 6.1, EBS-boot, 64-bit architecture, Root Device Size: 6.0GB	ami-5e937037	US West (Oregon)	<input type="button"/> Select
SUSE Linux Enterprise Server 11 64-bit (AMI ID: ami-e9x3578d)	SUSE Linux Enterprise Server 11 Service Pack 1 basic install, EBS boot, 64-bit architecture with Amazon EC2 AMI Tools preinstalled; Apache 2.2, MySQL 5.0, PHP 5.3, Ruby 1.8.7, and Java 2.3; Root Device Size: 15.0GB	ami-e9x3578d	US West (Oregon)	<input type="button"/> Select

*Free tier eligible if used with a micro instance. See [AWS free tier](#) for complete details and terms.

Continue >



|| C3 SCHOOLS

3. Select the AMI (Amazon Machine Image). The AWS Launch screen provides multiple options to select AMI. The user can select the AMIs provided by AWS (Standard OS). Select “My AMIs” to launch the instance from the user’s existing AMIs or select community AMIs to launch the instance from various providers (may or may not be authorized by AWS).

Request Instances Wizard

CHOOSE AN AMI INSTANCE DETAILS CREATE KEY PAIR CONFIGURE FIREWALL REVIEW

Choose an Amazon Machine Image (AMI) from one of the tabbed lists below by clicking its **Select** button.

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

Amazon Linux AMI 2012.09
The Amazon Linux AMI 2012.09 is an EBS-backed, PV-GRUB image. It includes Linux 3.2, AWS tools, and repository access to multiple versions of MySQL, PostgreSQL, Python, Ruby, and Tomcat.
Root Device Size: 8 GB 64 bit 32 bit

Red Hat Enterprise Linux 6.3
Red Hat Enterprise Linux version 6.3, EBS-boot.
Root Device Size: 7 GB 64 bit 32 bit

SUSE Linux Enterprise Server 11
SUSE Linux Enterprise Server 11 Service Pack 2 basic install, EBS boot with Amazon EC2 AMI Tools preinstalled; Apache 2.2, MySQL 5.0, PHP 5.3, and Ruby 1.8.7.
Root Device Size: 10 GB 64 bit 32 bit

Ubuntu Server 12.04.1 LTS
Ubuntu Server 12.04.1 LTS, with support available from Canonical (<http://www.ubuntu.com/cloud/services>).
Root Device Size: 8 GB 64 bit 32 bit

Ubuntu Server 11.10
Ubuntu Server 11.10 with support available from Canonical
 Free tier eligible if used with a micro instance. See [AWS free tier](#) for complete details and terms.



|| C3 SCHOOLS

4. Provide the instance details, such as the Instance Type, Availability Zone and Number of Instances. The availability zone depends on the current region. If the user is launching an EBS Optimized Instance, select the checkbox. The checkbox will be enabled only for the selected instance types.

Request Instances Wizard

Cancel X

CHOOSE AN AMI INSTANCE DETAILS CREATE KEY PAIR CONFIGURE FIREWALL REVIEW

Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances.

Number of Instances: **Instance Type:**

Launch as an EBS-Optimized instance (additional charges apply): Not supported for this instance type

Launch Instances
EC2 Instances let you pay for compute capacity by the hour with no long term commitments. This transforms what are commonly large fixed costs into much smaller variable costs.
Launch into: EC2 VPC
Availability Zone:

Request Spot Instances

< Back Continue ➤



|| C3 SCHOOLS

5. Select the Large instance type and the checkbox will be enabled. Select the checkbox to launch an instance as an EBS Optimized Instance.

Click on "Continue".

Request Instances Wizard

CHOOSE AN AMI INSTANCE DETAILS CREATE KEY PAIR CONFIGURE FIREWALL REVIEW Cancel

Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances.

Number of Instances: **Instance Type:**

Launch as an EBS-Optimized instance (additional charges apply):

Launch Instances
EC2 Instances let you pay for compute capacity by the hour with no long term commitments. This transforms what are commonly large fixed costs into much smaller variable costs.
Launch into: EC2 VPC
Availability Zone:

Request Spot Instances

[« Back](#) **Continue**



|| C3 SCHOOLS

6. Provide the Kernel ID and RAM Disk ID.

Request Instances Wizard

Cancel

CHOOSE AN AMI INSTANCE DETAILS CREATE KEY PAIR CONFIGURE FIREWALL REVIEW

Number of Instances: 1 **Availability Zone:** No Preference

Advanced Instance Options

Here you can choose a specific kernel or RAM disk to use with your instances. You can also choose to enable CloudWatch Detailed Monitoring or enter data that will be available from your instances once they launch.

Kernel ID: **RAM Disk ID:**

Monitoring: Enable CloudWatch detailed monitoring for this instance
(additional charges will apply)

User Data:

as text (Use shift+enter to insert a newline)
 as file base64 encoded

Termination Protection: Prevention against accidental termination. **Shutdown Behavior:**

IAM Role:

< Back **Continue**

CD JCTIOLC



|| C3 SCHOOLS

7. Provide the storage related information. In order to launch an EBS optimized instance with a Provisioned IOPS EBS volume, click on "Edit" to modify the volume type and size.

Request Instances Wizard

CHOOSE AN AMI INSTANCE DETAILS CREATE KEY PAIR CONFIGURE FIREWALL REVIEW

Number of Instances: 1

Availability Zone: No Preference

Storage Device Configuration

Your instance will be launched with the following storage device settings. Edit these settings to add EBS volumes, instance store volumes, or edit the settings of the root volume.

Type	Device	Snapshot ID	Size	Volume Type IOPS	Delete on Termination
Root	/dev/sda1	snap-921bb2b4	8	standard	true

0 EBS Volumes 0 Ephemerals

Edit

< Back Continue ➤

CD OUTPUTS



|| C3 SCHOOLS

8. Select the volume type as “Provisioned IOPS” and provide the IOPS from 100-2000. The IOPS optimized EBS volume size should be a minimum of 10 GB for a Linux Instance. Provide the Root Volume Size (more than 10 GB). If the user wants the root volume to be deleted on instance termination, select “Delete On termination”. Save all the changes made and Click on “Continue”.

Request Instances Wizard

CHOOSE AN AMI INSTANCE DETAILS CREATE KEY PAIR CONFIGURE FIREWALL REVIEW Cancel

Number of Instances: 1

Availability Zone: No Preference

Storage Device Configuration

Your instance will be launched with the following storage device settings. Edit these settings to add EBS volumes, instance store volumes, or edit the settings of the root volume.

Root Volume EBS Volumes Instance Store Volumes

Optional edit the the root volume of your instance and then click Save.

Volume Size: GiB **Volume Type:** **IOPS:**

Device: /dev/sda1 **Delete on Termination:**

Volume size must be at least 10GiB

Type	Device	Snapshot ID	Size	Volume Type	IOPS	Delete on Termination
Root	/dev/sda1	snap-921bb2b4	8	standard		true

0 EBS Volumes 0 Ephemerals

[< Back](#) **Continue**



|| C3 SCHOOLS

9. Provide the tags for the AWS instance. Tagging is very useful when the user wants to track the cost of a particular instance / service. Click on “Continue”.

Request Instances Wizard

CHOOSE AN AMI INSTANCE DETAILS CREATE KEY PAIR CONFIGURE FIREWALL REVIEW

Add tags to your instance to simplify the administration of your EC2 infrastructure. A form of metadata, tags consist of a case-sensitive key/value pair, are stored in the cloud and are private to your account. You can create user-friendly names that help you organize, search, and browse your resources. For example, you could define a tag with key = Name and value = Webserver. You can add up to 10 unique keys to each instance along with an optional value for each key. For more information, go to Using Tags in the *EC2 User Guide*.

Key (127 characters maximum)	Value (255 characters maximum)	Remove
Name	EBS Optimized Instance	X
		X

Add another Tag. (Maximum of 10)

Back Continue

10. For the security of the instance, select the existing key-pair or create a new key-pair. Continue once the key pair has been created / selected.

Request Instances Wizard

CHOOSE AN AMI INSTANCE DETAILS CREATE KEY PAIR CONFIGURE FIREWALL REVIEW

Public/private key pairs allow you to securely connect to your instance after it launches. For Windows Server Instances, a Key Pair is required to set and deliver a secure encrypted password. For Linux Server Instances, a key pair will allow you to SSH into your instance.

To create a key pair, enter a name and click **Create & Download your Key Pair**. You will then be prompted to save the private key to your computer. Note, you only need to generate a key pair once - not each time you want to deploy an Amazon EC2 instance.

Choose from your existing Key Pairs

Your existing Key Pairs*:

Create a new Key Pair

Proceed without a Key Pair

Back Continue



|| C3 SCHOOLS

11. Select the security group. The security group provides the virtual firewall for the instance. Click on “Continue”.

Request Instances Wizard

CHOOSE AN AMI INSTANCE DETAILS CREATE KEY PAIR **CONFIGURE FIREWALL** REVIEW

Security groups determine whether a network port is open or blocked on your instances. You may use an existing security group, or we can help you create a new security group to allow access to your instances using the suggested ports below. Add additional ports now or update your security group anytime using the Security Groups page.

Choose one or more of your existing Security Groups

`sg-0c1c933c - default`

(Selected groups: sg-0c1c933c)

Create a new Security Group

< Back **Continue**

12. Review all the details and click on “Launch”.

Request Instances Wizard

CHOOSE AN AMI INSTANCE DETAILS CREATE KEY PAIR CONFIGURE FIREWALL **REVIEW**

Please review the information below, then click **Launch**.

AMI: Amazon Linux AMI ID ami-2a31bf1a (x86_64)

Name: Amazon Linux AMI 2012.09

Description: The Amazon Linux AMI 2012.09 is an EBS-backed, PV-GRUB image. It includes Linux 3.2, AWS tools, and repository access to multiple versions of MySQL, PostgreSQL, Python, Ruby, and Tomcat. [Edit AMI](#)

Number of Instances: 1

Availability Zone: No Preference

Instance Type: M1 Large (m1.large)

Instance Class: On Demand [Edit Instance Details](#)

EBS-Optimized: Yes [Edit Instance Details](#)

Monitoring: Disabled **Termination Protection:** Disabled

Tenancy: Default **Shutdown Behavior:** Stop

Kernel ID: Use Default **RAM Disk ID:** Use Default

Network Interfaces:

Secondary IP Addresses:

User Data:

IAM Role:

< Back **Launch**



|| C3 SCHOOLS

13. AWS will launch the instance and provide the user with the ID of the instance.

Launch Instance Wizard

Your instances are now launching.

Instance ID(s): **i-385c8c0a**

Note: Your instances may take a few minutes to launch, depending on the software you are running.

Note: Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

You can perform the following tasks while your instances are launching:

- **Create Status Check Alarms**
- You can use status check alarms to be notified if these instances fail status checks (additional charges may apply).
- **Create EBS Volumes** (Additional charges may apply.)
- **View your instances on the Instances page**

Close

14. Go to the AWS EC2 console and it will display the new instance. The instance will be first in a pending state until it boots completely. It is advisable to connect to the instance once the status checks are in “2/2 Checks”.

Viewing: Running Instances All Instance Types											< < 1 to 1 of 1 Instances > >	
Name	Instance	AMI ID	Root Device	Type	State	Status Checks	Alarm Status	Monitoring	Security Gro	Key Pair Na		
<input type="checkbox"/> empty	i-385c8c0a	ami-2a31bf1a	ebs	m1.large	running	2/2 checks	none	basic	default			

15. Go to Volumes from the EBS Dashboard. It will list the newly created IOPS Volume.

Name	Volume ID	Capacity	Volume Type	Snapshot	Created	Zone	State	Alarm Status	Attachmen
<input type="checkbox"/> empty	vol-17...0003	8 GiB	standard	snap-921bb2b4	2013-01-01T13:44:52	us-west-2a	in-use	none	i-f818c8ca
<input type="checkbox"/> empty	vol-d3862aea	10 GiB	io1 (100)	snap-921bb2b4	2013-01-01T18:22:15	us-west-2a	in-use	none	i-1e5d8d2c
<input type="checkbox"/> empty	vol-17...000a	30 GiB	standard	snap-94f7a8b2	2012-12-17T13:14:00	us-west-2c	in-use	none	i-e29f5bd0

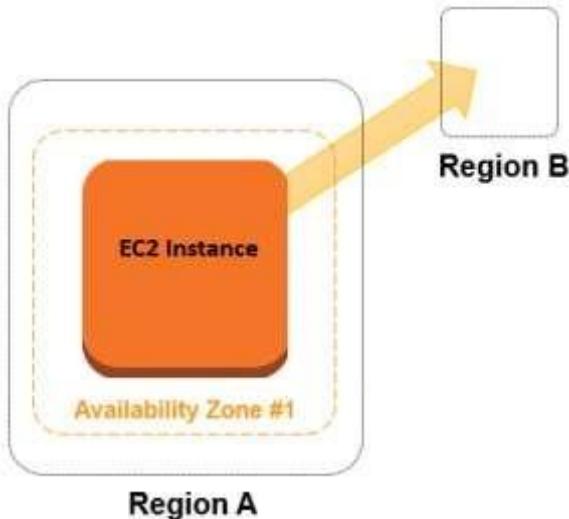


|| C3 SCHOOLS

How to Migrate (Copy) an EC2 Instance between Amazon AWS Regions

AWS has the functionality to copy snapshots across regions. Replicating snapshots across availability zones (AZs) and regions will enable you to deploy your online services across AZs and regions. Doing so will protect your cloud from damage and ensure availability during an outage.

This demonstrates how to copy a snapshot of a Linux based instance to another region as well as attach a volume to a new instance to complete the instance data migration across regions.



HOOOLS



|| C3 SCHOOLS

1. Go to the [AWS Console](#) and select the EC2 Service. Go to the EC2 running instance dashboard and select the running Linux instance. It displays the instance metadata. Note the volume details of the instance. The instance is currently running in the US-West-2 (Oregon) region.

The screenshot shows the AWS EC2 Instances dashboard. At the top, there are buttons for 'Launch Instance' and 'Actions'. The region is set to 'Oregon'. Below the header, there are dropdown menus for 'Viewing' (set to 'All Instances'), 'Instance Types' (set to 'All Instance Types'), and a search bar. A status bar at the bottom indicates '1 to 2 of 2 Instances'.

Name	Instance	AMI ID	Root Device	Type	State	Status Checks	Alarm Status	Monitoring	Security Gro
[]	i-e29f5bd0	ami-167af226	ebs	t1.micro	stopped		none	basic	
<input checked="" type="checkbox"/> Test Linux	i-b8b77b8a	ami-2a31bf1a	ebs	t1.micro	running	initializing	none	basic	default

Below the table, a detailed view of the 'Test Linux' instance is shown. The 'RAM Disk ID' is listed as 'sda1'. The 'Platform' section shows the AMI ID as 'aki-fc37bacc'. Other details include:

- Key Pair Name:** []
- Monitoring:** []
- Elastic IP:** []
- Root Device Type:** ebs
- Attachment time:** 2012-12-22T17:58:12.000Z
- Block device status:** attached
- Delete on termination:** Yes
- EBS Optimized:** []
- Snapshot ID:** snap-921bb2b4
- Block Devices:** []
- Network Interfaces:** []
- Public DNS:** ec2-50-112-206-42.us-west-2.compute.amazonaws.com
- Private DNS:** []

2. Login to the Linux instance, as explained in [Connecting to AWS linux instance from a Windows machine](#). List the data of the instance.

```
[ec2-user@ip-10-252-195-157 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-252-195-157 ~]$ ls
aws-scripts-mon  snapcopyDir  test2.txt  test.txt
[ec2-user@ip-10-252-195-157 ~]$ sudo cat test.txt
hi
[ec2-user@ip-10-252-195-157 ~]$
```



|| C3 SCHOOLS

3. Go to Snapshot in the EC2 console and select “Create Snapshot”.

Provide the snapshot name, description and select the volume of the instance identified in step #1. Click on the “Create” button.



4. The snapshot has been created and is available in the Snapshot console.

Name	Snapshot ID	Capacity	Description	Status	Started	Progress
<input type="checkbox"/> Copy-Snapshot-Region	snap-8c5746aa	8 GiB	Copy Snapshot from One Region	completed	2012-12-31 17:28	available (100%)
<input type="checkbox"/> EBS-Copy	snap-ca5243ec	8 GiB	Test Snapshot Copy	completed	2012-12-31 17:23	available (100%)

5. Select the snapshot that the user wants to move to the other region. Right click on the snapshot and select the “copy snapshot” option.



|| C3 SCHOOLS

Screenshot of the AWS Snapshot Management interface showing the 'Copy' button highlighted.

Viewing: Owned By Me

Name	Snapshot ID	Capacity	Description
<input checked="" type="checkbox"/> Copy-Snapshot-Region	snap-8c5746aa	8 GiB	Copy Snapshot from One Region
<input type="checkbox"/> EBS-Copy	snap-0	Delete Snapshot Snapshot Permissions Create Volume from Snapshot Create Image from Snapshot Add/Edit Tags Copy Snapshot	shot Copy

6. Provide the target region and the description for the snapshot. Click on the button "Yes, Copy".

C3 SCHOOLS

Copy Snapshot

Snapshot: snap-8c5746aa -- Copy Snapshot from One Region

Destination region: EU (Ireland)

Description: [Copied snap-8c5746aa from us-west-2] Copy Snapshot from One Region

Cancel Yes, Copy

7. The snapshot copy process will now commence. AWS will display the acknowledgement for the same and provide a link to go to the snapshot console of the target region. Click on the link or manually change the region to go to the target region snapshot console.



|| C3 SCHOOLS

Copy Snapshot

Snapshot copy operation has been initiated. Visit the [Snapshots](#) page in EU (Ireland) to check on the progress of the copy operation.

[Close](#)

Cancel X

C3 SCHOOLS



|| C3 SCHOOLS

8. In the target region (EU-Ireland), the copy process is in progress. AWS will display the progress of the process.

Name	Snapshot ID	Capacity	Description	Status	Started	Progress
empty	snap-08953961	10 GiB		completed	2012-12-31 17:36:43	available (100%)
empty	snap-ce8cb8e7	8 GiB	[Copied snap-8c5746aa from us-west-2] Copy Snapshot from One Region	pending	2012-12-31 17:36:43	5%

9. After the process is complete, the snapshot will be available in the target region.

Name	Snapshot ID	Capacity	Description	Status	Started	Progress
empty	snap-08953961	10 GiB		completed	2012-12-31 17:36:43	available (100%)
empty	snap-ce8cb8e7	8 GiB	[Copied snap-8c5746aa from us-west-2] Copy Snapshot from One Region	completed	2012-12-31 17:36:43	available (100%)

10. Create the volume from the snapshot.

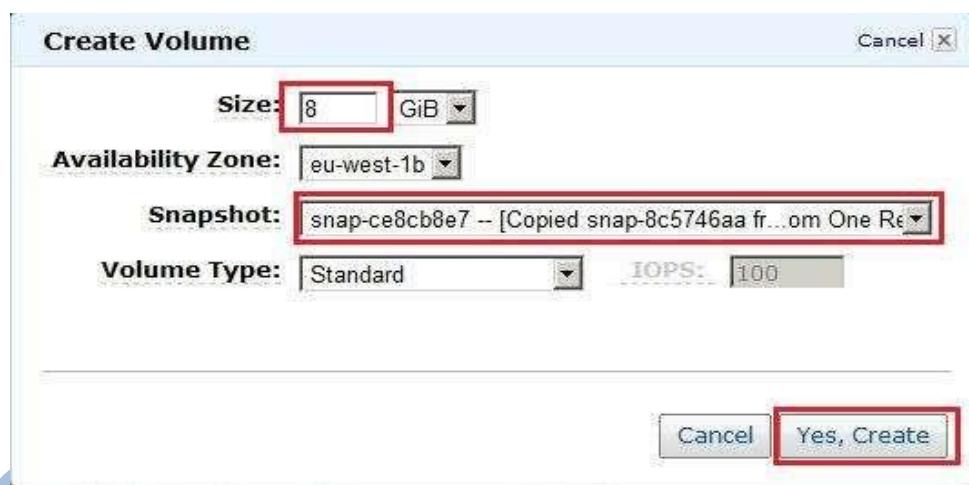
Create Snapshot	Delete	Permissions	Create Volume	Create Image	Copy	
Viewing: Owned By Me	Search					
Name	Snapshot ID	Capacity	Description	Status	Started	Progress
empty	snap-08953961	10 GiB				
<input checked="" type="checkbox"/> empty	snap-ce8cb8e7	8 GiB	[Copied snap-8c5746aa from us-west-2] Copy Snapshot from One Region			

- Delete Snapshot
- Snapshot Permissions
- Create Volume from Snapshot**
- Create Image from Snapshot
- Add/Edit Tags
- Copy Snapshot



|| C3 SCHOOLS

11. Select the zone where the volume will be created and provide the remaining details. Click on the button "Yes, Create" to create the volume.



12. Launch a Linux instance (as explained in [How to launch an Amazon AWS EC2 instance](#)) in the same zone where the volume from the snapshot has been created.

1 EC2 Instance selected.

EC2 Instance: EU Instance (i-757c753e) running
ec2-46-137-139-23.eu-west-1.compute.amazonaws.com

Description	Status Checks	Monitoring	Tags
AMI: amzn-ami-pv-2012.09.0.x86_64-ebs (ami-c37474b7)	Alarm Status: none		
Zone: eu-west-1b	Security Groups: default, view rules		



|| C3 SCHOOLS

13. Stop the instance, as explained in [How to reboot an EC2 instance](#). Detach the root volume of the new instance.

Name	Volume ID	Capacity	Volume Type	Snapshot	Created	Zone	State
<input type="checkbox"/> empty	vol-7cfbd856	8 GiB	standard	snap-ce8cb8e7	2013-01-01T04:39:36	eu-west-1b	available
<input checked="" type="checkbox"/> empty	vol-1af4d730	8 GiB	standard	snap-981540ce	2013-01-01T04:34:31	eu-west-1b	in-use

Detach Volume
Force Detach
Create Snapshot
Change Auto-Enable IO Setting

14. Once the root volume has been detached, attach the volume created in step #11 to the instance.

Name	Volume ID	Capacity	Volume Type	Snapshot	Created	Zone	State
<input type="checkbox"/> empty	vol-1af4d730	8 GiB	standard	snap-981540ce	2013-01-01T04:34:31	eu-west-1b	available
<input checked="" type="checkbox"/> empty	vol-7cfbd856	8 GiB	standard	snap-ce8cb8e7	2013-01-01T04:39:36	eu-west-1b	available

Delete Volume
Attach Volume
Create Snapshot
Change Auto-Enable IO Setting

15. Attach the volume as the root volume by mounting on /dev/sda1.

Attach Volume

Volume: vol-7cfbd856 in eu-west-1b

Instances: i-757c753e - EU Instance (stopped) in eu-west-1b

Device: /dev/sda1

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

Cancel Yes, Attach



|| C3 SCHOOLS

16. Start the Linux instance and login to the instance. The instance will display the content similar to the US-West-2 Linux instance, as shown in step #2.

```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Mon Dec 31 11:52:40 2012 from 14.97.140.73

[ec2-user@ip-10-226-87-234 ~]$ cd /root
[ec2-user@ip-10-226-87-234 ~]$ ls
Amazon Linux AMI

https://aws.amazon.com/amazon-linux-ami/2012.09-release-notes/
There are 3 security update(s) out of 43 total update(s) available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-226-87-234 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-226-87-234 ~]$ ls
aws-scripts-mon  snapcopyDir  test2.txt  test.txt
[ec2-user@ip-10-226-87-234 ~]$ sudo cat test.txt
hi
[ec2-user@ip-10-226-87-234 ~]$
```

17. The above process completes the migration of the user's instance from one region to another.
[Amazon Cloud S3 Bucket Creation Policies and Guidelines](#)

When naming an AWS S3 bucket, it has to be a unique name not only for your account but for all buckets existing on S3. The main reason for that is the fact that S3 buckets can be accessed on the internet as

<http://<bucketName>.s3.amazonaws.com> and if two buckets have the same name it means they will have the same internet URL.

Below is the policy to be followed while creating Amazon AWS buckets:

1. One AWS account can have max 100 buckets at a time.

2. One bucket can have unlimited objects inside it.

To create a bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Click **Create Bucket**.
3. In the Create Bucket dialog box, in the Bucket Name box, type a name for your bucket. and select region.



|| C3 SCHOOLS

- Can contain lowercase letters, numbers, periods (.), and hyphens (-).
- Must start with a number or letter.
- Must be between 3 and 63 characters long.
- Must not be formatted as an IP address (e.g., 192.168.5.4).
- Must not contain underscores (_).
- Must not end with a hyphen.
- Cannot contain two, adjacent periods.
- Cannot contain dashes next to periods (e.g., my.-bucket.com and my.-bucketare invalid).

Create a Bucket - Select a Bucket Name and Region Cancel

A bucket is a container for objects stored in Amazon S3. When creating a bucket, you can choose a Region to optimize for latency, minimize costs, or address regulatory requirements. For more information regarding bucket naming conventions, please visit the [Amazon S3 documentation](#).

Bucket Name:

Region: ▼

Set Up Logging > Create Cancel

- i. The above is a valid name and will create a bucket in the US Region



|| C3 SCHOOLS

Create Bucket Actions ▾

All Buckets (5)

Name
awsaugust
awstestbucketus
cf-templates-2tsqo9p6j1q-ap-southeast-1
devopsaugust
testsngdevops

Bucket: awstestbucketus X

Bucket: awstestbucketus
Region: US Standard
Creation Date: Sat Sep 17 13:28:33 GMT+530 2016
Owner: mohan.nagula

Permissions

Static Website Hosting

Logging

Events

Versioning

Lifecycle

Cross-Region Replication

Tags

Requester Pays

How to Manage an AWS S3 Cloud Storage Bucket

A bucket is a container for objects stored in Amazon S3. Every object is contained in a bucket and can be accessed through internet.

1. Login to your AWS account console and enter the AWS S3 Simple Storage section.



|| C3 SCHOOLS

Create Bucket Actions ▾

All Buckets (5)

Name
awsaugust
awstestbucketus
cf-templates-2tsqo9pb6jqg-ap-southeast-1
devopsaugust
testsngdevops

Bucket: awstestbucketus X

Bucket: awstestbucketus
Region: US Standard
Creation Date: Sat Sep 17 13:28:33 GMT+530 2016
Owner: mohan.nagula

Permissions
Static Website Hosting
Logging
Events
Versioning
Lifecycle
Cross-Region Replication
Tags
Requester Pays

2. Select a bucket on the left menu bar; the main screen will show a list all folders and objects that bucket contains.
Click the button `Create Bucket`.
3. The wizard dialog window will open with the new bucket properties: Name and Region.

Create a Bucket - Select a Bucket Name and Region

A bucket is a container for objects stored in Amazon S3. When creating a bucket, you can choose a Region to optimize for latency, minimize costs, or address regulatory requirements. For more information regarding bucket naming conventions, please visit the [Amazon S3 documentation](#).

Bucket Name: awstestbucketus

Region: US Standard

[Set Up Logging >](#) [Create](#) [Cancel](#)

Note that AWS S3 bucket can be deployed in a region (and not in zones such as the EC2 instance) .



|| C3 SCHOOLS

All buckets names should have unique name across all AWS S3 users' buckets. There is a direct mapping between Amazon S3 buckets and the sub domains of s3.amazonaws.com. Objects stored in Amazon S3 are addressable under the domain **bucketname.s3.amazonaws.com**.

When you name a bucket, it is possible that same name might have been used by some other AWS user will not be available. Also AWS implements certain rules for creating a bucket in AWS. The rule for creating bucket in standard US (US-East) region is different than all other regions.

id Bucket Name	Ment
sbucket	t name cannot start with a period (.).
bucket.	t name cannot end with a period (.).
xamplebucket	can only be one period between labels.

4. Follow the above policy and enter your new bucket's name. Enable bucket transactions recording by clicking the button 'Setup logging'. The logging feature allows you to generate access log files for the operations that are performed on the bucket you own. These log files will be stored in a bucket (possibly different) that you own.
5. Click 'Create' will create the new S3 bucket and will add the new bucket as a new item on the console left menu bar.
6. Once your bucket is created, you can click the drop down to view the different options as show below

The screenshot shows the AWS S3 'All Buckets' page. A dropdown menu is open over the 'Actions' button, listing options like Open, Download, Create Folder..., Upload, Make Public, Rename, Delete, Initiate Restore, Cut, Copy, Paste, and Properties. To the right, the details for the bucket 'tarun-nov14' are displayed, including its creation date and owner. A sidebar on the right lists various management options: Permissions, Static Website Hosting, Logging, Notifications, Versioning, Lifecycle, Tags, and Requester Pays.

Name	Size	Last Modified
AWS S3.jpg	10.3 KB	Sat Nov 01 07:36:53 GMT+530 2014
AWS.jpg	7.6 KB	Sat Nov 01 07:36:54 GMT+530 2014
index.html	188 bytes	Sat Nov 01 07:36:55 GMT+530 2014

Bucket: tarun-nov14

Bucket: tarun-nov14
Region: US Standard
Creation Date: Sat Nov 01 07:35:08 GMT+530 2014
Owner: Me

Permissions
Static Website Hosting
Logging
Notifications
Versioning
Lifecycle
Tags
Requester Pays



7. We will create a folder in bucket, select option 'Create Folder'.

A screenshot of the AWS S3 console. At the top, there are buttons for "Upload" and "Create Folder", with "Create Folder" being highlighted. Next to it is an "Actions" dropdown menu. Below the header, the path "All Buckets / awstestbucket" is shown. A search bar and filter buttons for "None", "Properties", and "Transfers" are also present. The main area displays a table with one row, labeled "Name", under the "Actions" column. A tooltip message "The bucket 'awstestbucketus' is empty" is visible. The "Actions" menu is open, showing options like "Open", "Download", "Create Folder...", "Upload", "Make Public", "Rename", "Delete", "Initiate Restore", "Cut", "Copy", "Paste", and "Properties". The "Create Folder..." option is highlighted with a dark background and white text.

8. Name the folder, the folder name should be unique for the specific bucket only. Once the folder created it will list in the bucket.

9. Explore the bucket's properties by selecting the property option tab. Below for example we selected the 'Permission tab', that specify the user(grantee) and his specific permissions.



|| C3 SCHOOLS

Create Bucket Actions ▾

All Buckets (5)

Name
awsaugust
awstestbucketus
c-templates-2tsq7ip61og-ap-southeast-1
devopsaugust
testingdevops

Bucket: awstestbucketus

Bucket: awstestbucketus
Region: US Standard
Creation Date: Sat Sep 17 13:28:33 GMT+530 2016
Owner:

Permissions

You can control access to the bucket and its contents using access policies. Learn more.

Grantee: devop List Upload/Delete View Permissions X Edit Permissions

Grantee: Everyone List Upload/Delete View Permissions X Edit Permissions

Add more permissions Add bucket policy Add CORS Configuration

Save Cancel

C3 SCHOOLS



|| C3 SCHOOLS

10. Select the `Logging tab` , it will list if logging is enabled for the bucket. You can store logs of the S3 bucket inside it or in some other.

▼ Logging

You can enable logging to track requests for access to your bucket. [Learn more.](#)

Enabled: <input checked="" type="checkbox"/>
Target Bucket: awstestbucketuslogs
Target Prefix: logs/

Save **Cancel**

11. Select `Notifications` tab, to enable notification generated by AWS SNS when object is lost.

Events

Event Notifications enable you to send alerts or trigger workflows. Notifications can be sent via Amazon Simple Notification Service (SNS) or Amazon Simple Queue Service (SQS) or to a Lambda function (depending on the bucket location).

Name	1234	i
Events	ObjectCreated (All)	i
Prefix	e.g. images/	i
Suffix	e.g. jpg	i
Send To	<input checked="" type="radio"/> SNS topic <input type="radio"/> SQS queue <input type="radio"/> Lambda function	i

You don't own any SNS topics in this region.

Enter the Amazon Resource Name (ARN) of an SNS topic. S3 must have permission to publish to the topic from this source bucket. See the [Developer Guide](#).

SNS topic ARN

Save **Cancel**

12. **S3 Versioning Service** allows you to preserve, retrieve, and restore every version of every object stored in this bucket.



|| C3 SCHOOLS

Versioning allows you to preserve, retrieve, and restore every version of every object stored in this bucket. This provides an additional level of protection by providing a means of recovery for accidental overwrites or expirations. Versioning-enabled buckets store all versions of your objects by default.

You can use lifecycle rules to manage all versions of your objects as well as their associated costs. Lifecycle rules enable you to automatically archive your objects to the Glacier Storage Class and/or remove them after a specified time period.

Once enabled, Versioning cannot be disabled, only suspended.

Versioning is currently not enabled on this bucket.

[Enable Versioning](#)

C3 SCHOOLS



|| C3 SCHOOLS

13. Cross-Region Replication a bucket-level feature that enables automatic, asynchronous copying of objects across buckets in different AWS regions.

▼ Cross-Region Replication

Cross-Region Replication replicates every future upload of every object in this bucket to another bucket. Cross-Region Replication is designed for use in conjunction with Versioning. You will be required to enable Versioning on this bucket and the target bucket. [Learn More](#)

Versioning is currently not enabled on this bucket.

[Enable Versioning](#)

14. Select the ‘Transfers’ option will show all the ongoing or recent transfers or updates. If you upload new object or delete some bucket / object, the event and its status will be shown in transfer window.

[How to Generate S3 Policies and Manage S3 Bucket Permissions](#)

Bucket policies define access rights for Amazon S3 resources. Only a bucket owner can write bucket policies. The S3 bucket policy enables you to set permissions such as “Allow/deny bucket-level permissions” and “Deny permission on any objects in the bucket”.

To grant permissions to a specific user, you need the canonical ID of that user. You can get the canonical ID from the AWS account.

1. Enter your AWS account console.
2. Select the bucket and select properties for that bucket. The permissions for that bucket are listed.



|| C3 SCHOOLS

The screenshot shows the AWS S3 console. In the top navigation bar, 'AWS' is selected. Below the navigation, there are tabs for 'Create Bucket', 'Actions', 'None', 'Properties', and 'Transfers'. The main area shows 'All Buckets (2)'. A table lists two buckets: 'elasticbeanstalk-ap-southeast-1-076828422820' and 'tempbuck135'. The 'tempbuck135' row is selected. On the right, a detailed view for 'Bucket: tempbuck135' is displayed. It shows the bucket name, region (Mumbai), creation date (Fri Sep 23 07:17:31 GMT+530 2016), and owner (f5ab03db69048b107e456ece29c7fae84c90b48f73961716e864f036df078eca). A 'Permissions' section is expanded, showing grants for 'me' and 'Everyone'. Under 'Everyone', 'List', 'Upload/Delete', and 'View Permissions' are checked. Buttons for 'Edit Permissions', 'Add more permissions', 'Add bucket policy', and 'Add CORS Configuration' are visible. At the bottom are 'Save' and 'Cancel' buttons.

You add permissions to a grantee. A grantee can be an AWS account or one of the predefined Amazon S3 groups. You grant permission to an AWS account according to the email address or the canonical user ID.

The next steps describe how to generate a policy and apply it to an S3 bucket using the **Add Bucket Policy** link as marked above.

3. Go to the [Amazon S3 policy generator tool](#) and generate a new policy.



|| C3 SCHOOLS



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies. You can submit your samples (Enter 'AWS Policy Examples' in the Library Title field).

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy and an SQS Queue Policy.

Select Type of Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect Allow Deny

Principal

AWS Service All Services ('*')

Actions AbortMultipartUpload CreateBucket DeleteBucket DeleteBucketPolicy DeleteBucketWebsite DeleteObject

Amazon Resource Name (ARN) Invalid. You must enter a valid ARN.

4. Specify the principal. The principal is one or more people who receive or are denied permissions according to the policy. The principal must be specified using the principal's AWS ID.
5. Specify the actions for which the principal will have control. Once all data is selected, click **Add Statement**.



|| C3 SCHOOLS

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies. You can submit your samples (Enter 'AWS Policy Examples' in the Library Title field).

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy and an SQS Queue Policy.

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies. You can submit your samples (Enter 'AWS Policy Examples' in the Library Title field).

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy and an SQS Queue Policy.

Select Type of Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect Allow Deny

Principal

Multiple values are comma limited

AWS Service All Services (*)

Use multiple statements to add permissions for more than one service.

Actions All Actions (*)

Amazon Resource Name (ARN)

ARN should follow the following format: arn:aws:s3:::<bucket_name>/<key_name>,
Multiple values are comma limited.

Add Conditions (Optional)

W J P U V L J



|| C3 SCHOOLS

6. The statement is added and displayed as shown below.

Principal(s)	Effect	Action	Resource	Conditions
• C	Allow	• s3:CreateBucket	arn:aws:s3:::s3buckettst07072012	None

Step 3: Generate Policy

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

Generate Policy **Start Over**

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided *as is* without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.
An [amazon.com](#) company

7. Note that the policy is not yet generated. Click the **Generate Policy** button to display the policy.



|| C3 SCHOOLS

The screenshot shows the AWS Policy Generator interface. At the top, there are fields for 'Principal' (a dropdown menu) and 'AWS Service' (set to 'Amazon S3'). A checkbox for 'All Services (*)' is also present. Below these, a note says 'Use multiple statements to add permissions for more than one service.' A large modal window titled 'Policy JSON Document' contains the following JSON code:

```
{  
  "Id": "Policy1342969334059",  
  "Statement": [  
    {  
      "Sid": "Stmt1342969286660",  
      "Action": [  
        "s3:CreateBucket"  
      ],  
      "Effect": "Allow",  
      "Resource": "arn:aws:s3:::s3buckettst07072012",  
      "Principal": [  
        "(any principal)"  
      ]  
    }  
  ]  
}
```

Below the JSON code, there is a 'Close' button. At the bottom of the main window, there is a note about the AWS Policy Generator's terms and conditions, followed by a copyright notice: '©2010, Amazon Web Services LLC or its affiliates. All rights reserved. An [amazon.com](#) company'.

C3 SCHOOLS



|| C3 SCHOOLS

8. Copy the content of the new policy and add it to a bucket policy.

The screenshot shows the AWS S3 Bucket Policy Editor dialog box. The policy document is as follows:

```
{ "Statement": [ { "Sid": "AddCannedAcl", "Effect": "Allow", "Principal": { "AWS": ["*"] }, "Action": ["s3:PutObject", "s3:PutObjectAcl"], "Resource": ["arn:aws:s3:::s3buckettst07072012/*"], "Condition": { "StringEquals": { "s3:x-amz-acl": "public-read" } } } ] }
```

Below the dialog box, the AWS Policy Generator and Sample Bucket Policies links are visible. At the bottom right of the dialog are Save, Delete, and Close buttons. To the right of the dialog, there are checkboxes for View Permissions and Edit Permissions, and buttons for Add more permissions, Remove selected permissions, and Add bucket policy. The Save button is highlighted.

9. Click **Save** to add the policy to the bucket.



|| C3 SCHOOLS

S | Services ▾ | Edit Shortcut ▾ | Help ▾

Buckets

Create Bucket Actions ▾

s3bucketst07072012

tests3aminvm070712

Objects and Folders

Upload Create Folder Actions ▾ Refresh Properties Transfers Help

s3bucketst07072012

Name	Size	Last Modified
Sample1.txt	33 bytes	Sun Jul 22 22:14:22 GMT+530 2012
TestFolder	--	--
new folder	--	--

Properties

Name: s3bucketst07072012

Region: Oregon

Creation Date: Sun Jul 22 00:48:34 GMT+530 2012

Owner: Me

Versioning: Not Enabled

Permissions Website Logging Notifications Lifecycle

Grantee: [] List Upload/Delete View Permissions Edit Permissions x

Grantee: Authenticated Users List Upload/Delete View Permissions Edit Permissions x

Add more permissions Remove selected permissions Edit bucket policy

Save Cancel

© 2008 - 2012, Amazon Web Services LLC or its affiliates. All rights reserved. | Feedback | Support | Privacy Policy | Terms of Use | An [amazon.com](#) company

C3 SCHOOLS



|| C3 SCHOOLS

10. Click **Edit Bucket** policy and verify that the policy is listed.

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with 'Services' dropdown, 'Edit Shortcut', and 'Help'. Below it, the 'Buckets' section lists several buckets, and the 'Properties' section shows details for the selected bucket ('s3bucketst07072012'): Name, Region (Oregon), Creation Date (Sun Jul 22 00:48:34 GMT+530 2012), Owner (Me), and Versioning (Not Enabled). The main area is titled 'Bucket Policy Editor' for the bucket 's3bucketst07072012'. It contains a text area with a JSON policy document:

```
"Version": "2008-10-17",
"Statement": [
    {
        "Sid": "AddCannedAcl",
        "Effect": "Allow",
        "Principal": {

        },
        "AWS": "arn:aws:iam::000000000000:root",
        "Action": [
            "s3:PutObjectAcl",
            "s3:PutObject"
        ],
        "Resource": "arn:aws:s3:::s3bucketst07072012/*",
        "Condition": {
            "StringEquals": {
                "aws:SourceIdentity": "arn:aws:sts::000000000000:assumed-role/S3FullAccess/AmazonS3FullAccess"
            }
        }
]
```

Below the policy editor are buttons for 'Save', 'Delete', and 'Close'. Further down are sections for 'View Permissions' and 'Edit Permissions', and buttons for 'Add more permissions', 'Remove selected permissions', and 'Edit bucket policy'. The 'Edit bucket policy' button is highlighted with a red box. At the bottom of the page, there's a footer with links to 'Feedback', 'Support', 'Privacy Policy', 'Terms of Use', and 'An amazon.com company'.

You can either set permissions directly by selecting grantee as 'everyone' or 'me'. If you want to specify specific permission for a selected AWS account ID, you can use policy to define permission according to the AWS accounts/canonical IDs.

[How to Manage AWS Simple Storage Service \(S3\) Objects](#)

1. First go to the AWS S3 Console home and select the bucket for which you want to view and create objects.



|| C3 SCHOOLS

Name	Storage Class	Size	Last Modified
test.txt	Standard	83 bytes	Fri Sep 23 07:39:48 GMT+530 2016

2. To upload an object in the bucket, click the **Upload** button.

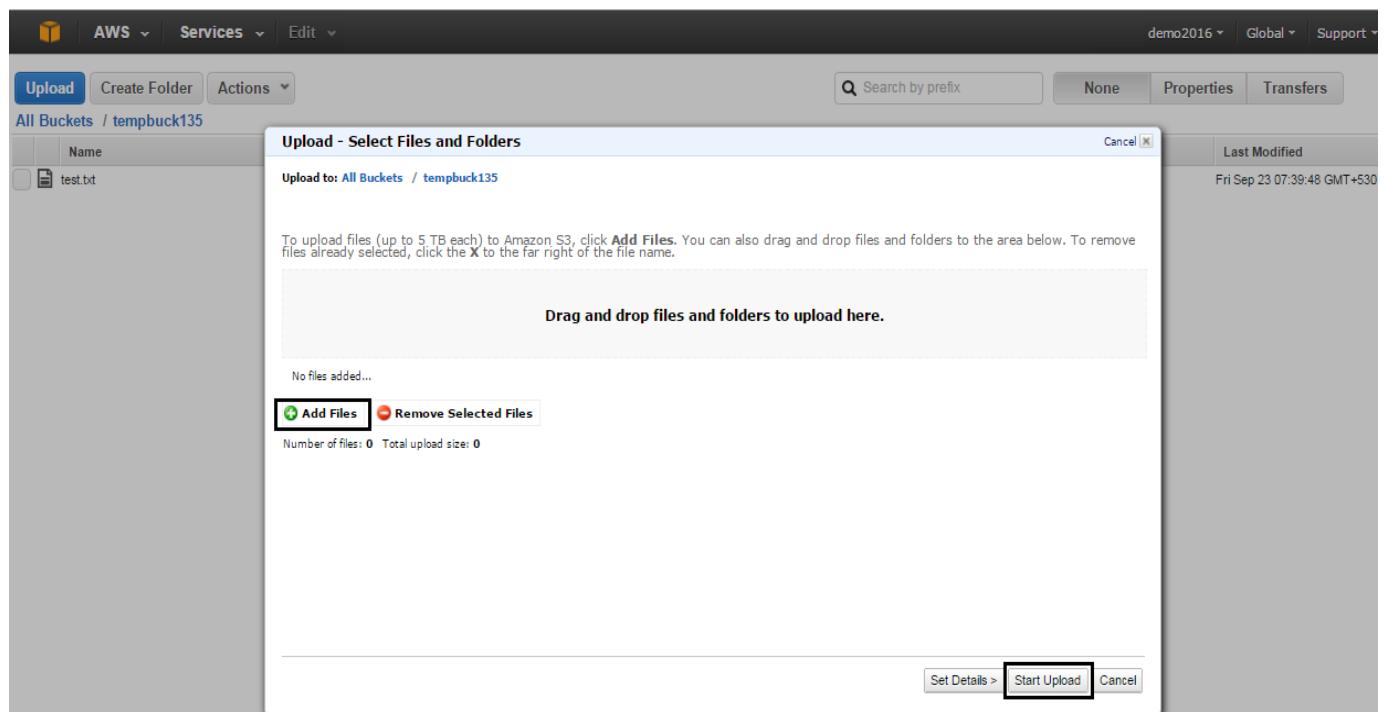
- Upload
- Create Folder
- Actions
- Open
- Download
- Create Folder...
- Upload**
- Make Public
- Rename
- Delete
- Initiate Restore
- Cut
- Copy
- Paste
- Properties



|| C3 SCHOOLS

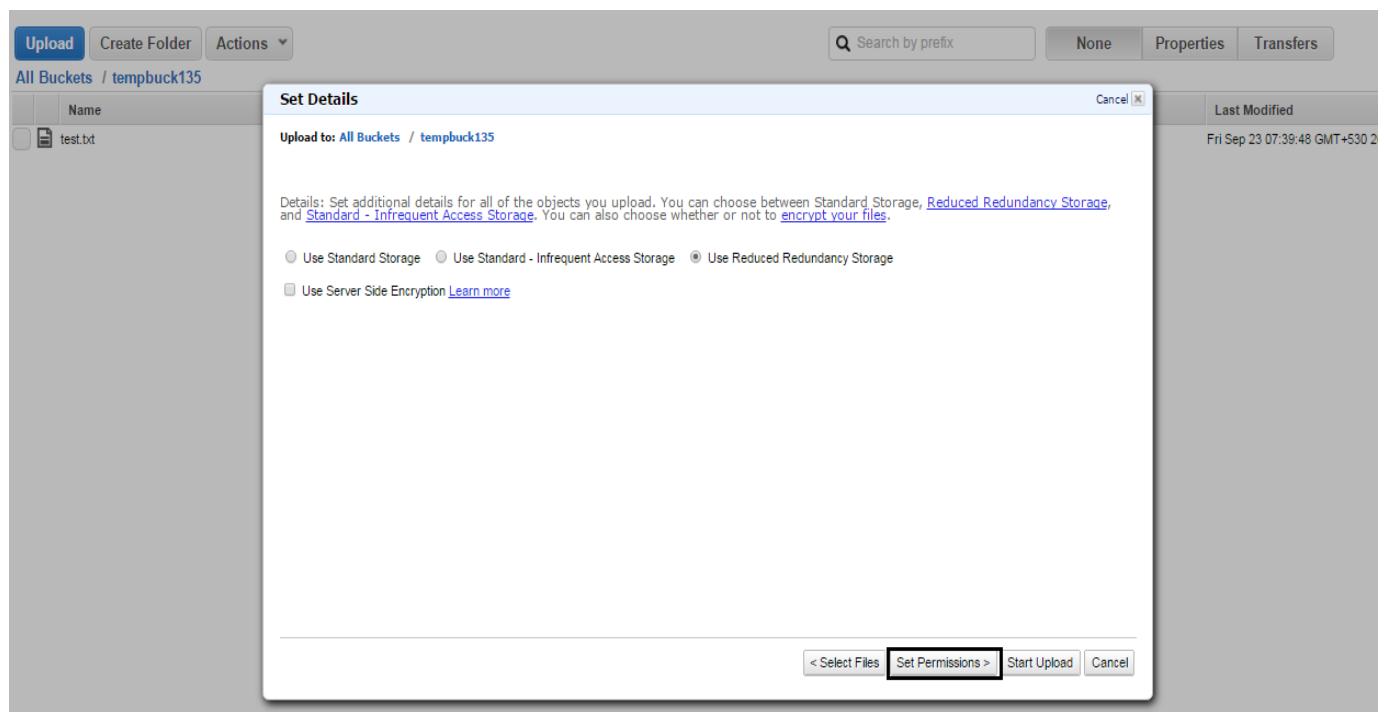
3. In the dialog box, click the **Add files** button.

4. When prompted, select the files from your machine or network. All selected files will be displayed in the dialog box.



The screenshot shows the AWS S3 console interface. A modal dialog box titled "Upload - Select Files and Folders" is open. Inside the dialog, there is a list of files in the background, including "test.txt". Below this is a large text input field with the placeholder "Drag and drop files and folders to upload here.". At the bottom of the dialog, there are two buttons: "Add Files" and "Remove Selected Files". The "Add Files" button is highlighted with a black border. Below the buttons, it says "Number of files: 0 Total upload size: 0". At the very bottom of the dialog, there are three buttons: "Set Details >" (highlighted with a black border), "Start Upload", and "Cancel".

5. If you want to set specific properties for the object before uploading it, click the **Set Details** button.



The screenshot shows the AWS S3 console interface. A modal dialog box titled "Set Details" is open. Inside the dialog, there is a section for "Details" which says: "Set additional details for all of the objects you upload. You can choose between Standard Storage, [Reduced Redundancy Storage](#), and [Standard - Infrequent Access Storage](#). You can also choose whether or not to [encrypt your files](#)". There are three radio buttons: "Use Standard Storage" (selected), "Use Standard - Infrequent Access Storage", and "Use Reduced Redundancy Storage". Below these, there is a checkbox "Use Server Side Encryption" with the link "Learn more". At the bottom of the dialog, there are four buttons: "< Select Files", "Set Permissions >" (highlighted with a black border), "Start Upload", and "Cancel".



|| C3 SCHOOLS

6. For testing, select the **Reduced Redundancy Storage** option and click the **Set Permissions** button. Grant read/write permissions to a grantee.

The screenshot shows the AWS Management Console interface for setting permissions on an object named 'test.txt' located in the bucket 'tempbuck135'. The 'Set Permissions' dialog is open, displaying the following details:

- Upload to:** All Buckets / tempbuck135
- Permissions:** Grant or remove permissions for specific accounts. By default, you are granted full control of all objects you upload to Amazon S3 using the AWS Management Console.
- Grantee:** Everyone
- Permissions:** Open/Download (checked)
- Buttons:** Add more permissions, Remove selected permissions, < Set Details, Set Metadata >, Start Upload, Cancel

7. Next, we will set the metadata for this object. By default, **Figure out content types automatically** is checked.



|| C3 SCHOOLS

S | Services ▾ Edit Shortcut ▾ Help ▾

Buckets Objects and Folders

Create Bucket Actions ▾ Upload Create Folder Actions ▾ Refresh Properties Transfers Help

Set Metadata

Upload to: s3buckettst07072012

Metadata: Add metadata to all of the objects you upload. You can specify common HTTP headers, such as Content-Type and Content-Disposition, as well as custom metadata for these.

Figure out content types automatically

Key: Cache-Control Value: Newvem

Add more metadata Remove selected metadata

< Set Permissions Start Upload Cancel

© 2008 - 2012, Amazon Web Services LLC or its affiliates. All rights reserved. | Feedback | Support | Privacy Policy | Terms of Use | An [amazon.com](#) company





|| C3 SCHOOLS

8. When you have set all the above properties, you can start the file upload by clicking the **Start Upload** button.

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with icons for AWS, Services, Edit, demo2016, Global, and Support. Below the navigation bar, there are buttons for Upload, Create Folder, Actions, and search fields for Search by prefix, None, Properties, and Transfers. The main area shows a list of files in the bucket 'tempbuck135'. There are two files listed: 'Solutions-Architect-Associate.png' (Reduced Redundancy, 6.2 KB, last modified Sat Sep 24 00:15:04 GMT+530 2016) and 'test.txt' (Standard, 83 bytes, last modified Fri Sep 23 07:39:48 GMT+530 2016). To the right of the file list is a 'Transfers' section with a checkbox for 'Automatically clear finished transfers'. Below this is a progress bar for an upload, showing a green checkmark icon and the text 'Done'. Underneath the progress bar, it says 'Upload: Uploading Solutions-Architect-Associate.png to tempbuck135'.

The files (objects) are uploaded to the bucket as shown above. The transfer window shows the status of upload.

9. Now we will see the properties of an object. Select the object and click the **Properties** button. The properties are listed as shown below.

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with icons for AWS, Services, Edit, demo2016, Global, and Support. Below the navigation bar, there are buttons for Upload, Create Folder, Actions, and search fields for Search by prefix, None, Properties, and Transfers. The main area shows a list of files in the bucket 'tempbuck135'. There are two files listed: 'Solutions-Architect-Associate.png' (Reduced Redundancy, 6.2 KB, last modified Sat Sep 24 00:15:04 GMT+530 2016) and 'test.txt' (Standard, 83 bytes, last modified Fri Sep 23 07:39:48 GMT+530 2016). To the right of the file list is a detailed view for the selected object 'Solutions-Architect-Associate.png'. The details show the following properties:

Bucket:	tempbuck135
Name:	Solutions-Architect-Associate.png
Link:	https://s3.ap-south-1.amazonaws.com/tempbuck135/Solutions-Architect-Associate.png
Size:	6442
Last Modified:	Sat Sep 24 00:15:04 GMT+530 2016
Owner:	f5ab03db69048b107e456ece29c7fae84c90b48f73961716e864f036df078eca
ETag:	96395b1ce7b4863378ff2cdd55a23a92
Expiry Date:	None
Expiration Rule:	N/A

Below the properties, there are sections for Details, Storage Class (radio buttons for Standard, Standard - Infrequent Access, Reduced Redundancy), Server Side Encryption (radio buttons for None, AES-256), and Buttons for Save and Cancel. At the bottom, there are links for Permissions and Metadata.



|| C3 SCHOOLS

10.In the details tab, you can see the URL of this object.

http://s3-us-west-2.amazonaws.com/s3buckettst07072012/Sample1.txt.txt

Hi,
This is Sample1 for AWS S3

11.Click the **Permission** tab. You can see that the permission for this object is set as “Open” for all users. If the permission was not set for the public, it will show ‘a “Page not found” error.

AWS Services Edit demo2016 Global Support

Upload Create Folder Actions

All Buckets / tempbuck135

	Name	Storage Class	Size	Last Modified
	Solutions-Architect-Associate.png	Reduced Redundancy	6.2 KB	Sat Sep 24 00:15:04 GMT+530 2016
	test.txt	Standard	83 bytes	Fri Sep 23 07:39:48 GMT+530 2016

Object: Solutions-Architect-Associate.png

Bucket: tempbuck135
Name: Solutions-Architect-Associate.png
Link: <https://s3.ap-south-1.amazonaws.com/tempbuck135/Solutions-Architect-Associate.png>
Size: 6442
Last Modified: Sat Sep 24 00:15:04 GMT+530 2016
Owner: f5ab03db69046b107e456ece29e7fae84c90b48f73961716e864f036df078eca
ETag: 96395b1ce7b4863378ff2cdd55a23a92
Expiry Date: None
Expiration Rule: N/A

Details

Permissions

You can control access to the bucket and its contents using access policies. Learn more.

Grantee: Everyone Open/Download View Permissions Edit Permissions X

Grantee: Me Open/Download View Permissions Edit Permissions X

Add more permissions

Save Cancel



|| C3 SCHOOLS

The next steps describe how to work with folders stored in a S3 bucket. You cannot create a bucket inside a bucket. To make better file structure, you can create folders inside a bucket.

12. Select the folder and click **Properties**.

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with 'AWS', 'Services', 'Edit', and user information 'demo2016'. Below the navigation bar, there are buttons for 'Upload', 'Create Folder', 'Actions', a search bar 'Search by prefix', and filters for 'None', 'Properties', and 'Transfers'. The main area shows a list of objects in the 'tempbuck135' bucket. One object, 'test1', is selected and highlighted in blue. On the right, a detailed view of the selected folder 'test1' is shown. The folder details include the bucket name 'tempbuck135' and the folder name 'test1'. Below the folder details, there's a section for 'Details' where users can change storage class (Standard, Standard - Infrequent Access, Reduced Redundancy) and server-side encryption (None, AES-256). At the bottom right of the details panel are 'Save' and 'Cancel' buttons.

Name	Storage Class	Size	Last Modified
Solutions-Architect-Associate.png	Reduced Redundancy	6.2 KB	Sat Sep 24 00:15:04 GMT+530 2016
test.txt	Standard	83 bytes	Fri Sep 23 07:39:48 GMT+530 2016
test1	--	--	--

Folder: test1

Bucket: tempbuck135
Name: test1

▼ Details

For all selected items:

Storage Class: Standard Standard - Infrequent Access Reduced Redundancy
Existing values will remain unchanged

Server Side Encryption: None AES-256
Existing values will remain unchanged

Save **Cancel**

The details show folder storage type as well encryption.

13. Create a new object in this folder. Double-clicking on the folder will list all the objects in this folder (currently empty).



|| C3 SCHOOLS

AWS Services Edit demo2016 Global Support

Upload Create Folder Actions Search by prefix None Properties Transfers

All Buckets / tempbuck135 / test1

	Name	Storage Class	Size	Last Modified
The folder 'test1' is empty				

Folder: test1 X

Bucket: tempbuck135
Name: test1

▼ Details

For all selected items:

Storage Class: Standard Standard - Infrequent Access Reduced Redundancy
Existing values will remain unchanged

Server Side Encryption: None AES-256
Existing values will remain unchanged

Save **Cancel**

C3 SCHOOLS



|| C3 SCHOOLS

14. Upload an object as mentioned in steps #3 -8.

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with 'AWS', 'Services', 'Edit', and dropdowns for 'demo2016', 'Global', and 'Support'. Below the navigation bar, there are buttons for 'Upload', 'Create Folder', and 'Actions'. A search bar says 'Search by prefix' and filter buttons for 'None', 'Properties', and 'Transfers'. The main area shows 'All Buckets / tempbuck135 / test1'. A table lists one object: 'webnieri.txt' (Standard storage class, 69 bytes, last modified Sat Sep 24 00:33:15 GMT+530 2016). To the right of the table is a detailed view for 'Object: webnieri.txt'. It shows properties like Bucket: tempbuck135, Folder: test1, Name: webnieri.txt, Link: https://s3.ap-south-1.amazonaws.com/tempbuck135/test1/webnieri.txt, Size: 69, Last Modified: Sat Sep 24 00:33:15 GMT+530 2016, Owner: f5ab03db69048b107e456ece29c7fae84c90b48f73961716e864f036df078eca, ETag: 5b59698b57722020b48a50fe8847e20b, Expiry Date: None, and Expiration Rule: N/A. Below the properties are sections for 'Details' and 'Permissions'. Under 'Permissions', it says 'You can control access to the bucket and its contents using access policies. Learn more.' There are two permission entries: one for 'Me' (Grantee: Me, Open/Download checked, View Permissions checked, Edit Permissions checked) and another for 'Everyone' (Grantee: Everyone, Open/Download checked, View Permissions checked, Edit Permissions checked). A 'Save' button is at the bottom right.

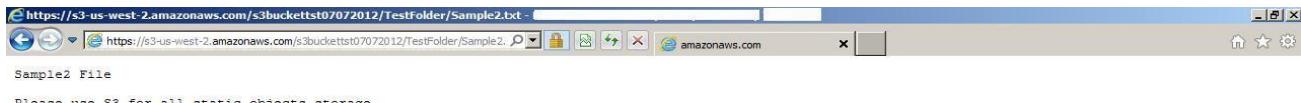
This uploads the same object as you uploaded to bucket. The object will have same properties as the object had in the bucket. The only difference will be the access URL. The access URL includes the folder name as indicated above.

15. You can share this object with everyone so that they can access/view from the internet.

16. You can access the object from the internet as shown below.



|| C3 SCHOOLS



How to Host a Static Website on AWS S3

A static website includes only static content, and might contain client-side scripts such as JavaScript or static content references. Hosting both the website and data on Amazon S3 helps simplify the management of your website and decrease the hosting costs. You can store all your static content files (images, videos, JavaScript files, Style sheets, etc.) on AWS S3 Storage, make references to them in your static HTML page and access them from internet as an ordinary website.

You must configure your Amazon S3 bucket as a website and reference its content using the appropriate website endpoint to access your html page from the internet.

1. Enter the [AWS S3 console home](#) and select the bucket for which you want to list the objects.
2. Upload **index.html** in the bucket and the .jpg file in the images folder as shown below.



|| C3 SCHOOLS

	Name	Storage Class	Size	Last Modified
<input type="checkbox"/>	Solutions-Architect-Associate.png	Reduced Redundancy	6.2 KB	Sat Sep 24 00:15:04 GMT+530 2015
<input checked="" type="checkbox"/>	index.html	Reduced Redundancy	8 bytes	Sat Sep 24 00:46:19 GMT+530 2015
<input type="checkbox"/>	test.txt	Standard	83 bytes	Fri Sep 23 07:39:48 GMT+530 2015
<input type="checkbox"/>	test1	--	--	--

3. In the `Permissions` tab, grant permissions for the bucket to everyone so that the objects can be accessible from internet.

Object: index.html

Bucket:	tempbuck135
Name:	index.html
Link:	https://s3.ap-south-1.amazonaws.com/tempbuck135/index.html
Size:	8
Last Modified:	Sat Sep 24 00:46:19 GMT+530 2015
Owner:	f5ab03db69048b107e456ece29c7fae84c90b48f73961716e664f036df078eca
ETag:	fd33e2e8ad3cb1bdd3ea8f5633fcf5c7
Expiry Date:	None
Expiration Rule:	N/A

Details

Permissions

You can control access to the bucket and its contents using access policies. [Learn more](#).

Grantee: Me Open/Download View Permissions Edit Permissions X

Grantee: Everyone Open/Download View Permissions Edit Permissions X

Add more permissions

Save Cancel

4. In the `Website` tab, select `Enabled` to make the objects of this bucket available as static website content.



|| C3 SCHOOLS

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with 'AWS', 'Services', 'Edit', and user information ('demo2016', 'Global', 'Support'). Below the navigation is a toolbar with 'Create Bucket' and 'Actions' dropdown. A table lists 'All Buckets (2)' with columns for 'Name'. Two buckets are listed: 'elasticbeanstalk-ap-southeast-1-076828422820' and 'tempbuck135'. The 'tempbuck135' row is selected and highlighted in blue. To the right of the table, under 'Permissions', is a section for 'Static Website Hosting'. It contains a note about hosting a static website on Amazon S3, mentioning the endpoint 'tempbuck135.s3-website.ap-south-1.amazonaws.com'. There are three radio button options: 'Do not enable website hosting' (selected), 'Enable website hosting' (with 'Index Document' set to 'index.html' and 'Error Document' left blank), and 'Redirect all requests to another host name'. At the bottom right are 'Save' and 'Cancel' buttons.

5. Provide the index file name. Note the **index document** is the document Amazon S3 returns when requests are made to the root or the subfolder of your website. When configuring a bucket as a website, you must provide an index document name.

In this example, we have kept the Error Document as blank. Should an error occur, Amazon S3 returns an HTML error document. For 4XX class errors, you can optionally configure your own custom error document, enabling you to provide additional guidance to your users.

The bucket is hosted in the US standard region. To host the website and reference its content, we need the appropriate website endpoint. When you configure a bucket as a website, the website is available via the region-specific website endpoint. To get end points for all regions, refer to <http://docs.amazonwebservices.com/AmazonS3/latest/dev/WebsiteEndpoints.html>.

6. We have enabled the bucket as a website. Access the bucket through the URL given in website tab. The 403 forbidden error is displayed.



|| C3 SCHOOLS



403 Forbidden

- Code: AccessDenied
 - Message: Access Denied
 - RequestId: 2F9008D97E321683
 - HostId: 4wqxI6/TLjtMwME0GvBLoCNj3QHYFmlw6kK9bjj7VsK088+/Mw0vaOdyXMRwBwo
-

C3 SCHOOLS



|| C3 SCHOOLS

This is because we have made the bucket public but we have not defined the objects in the bucket as public.

Object: index.html

Bucket: tempbuck135
Link: <https://s3.ap-south-1.amazonaws.com/tempbuck135/index.html>

Last Modified: Sat Sep 24 00:46:19 GMT+530 2016
Owner: f5ab03db69048b107e458ete29c7fae84c90b48f73961716e864f036df078eca
ETag: fd33e2e8ad3cb1bdd3ea8f5633fcfc5c7
Expiry Date: None
Expiration Rule: N/A

Details

Permissions

You can control access to the bucket and its contents using access policies. Learn more.

Grantee: Me Open/Download View Permissions Edit Permissions

Grantee: Everyone Open/Download View Permissions Edit Permissions

Add more permissions

Save Cancel

7. Set the permissions for this bucket to **Open/download for everyone** as shown above.

8. Access the bucket again from internet as shown below -

The HTML page is displayed but it does not show the image file. We have not set the image as public, therefore it is not accessible from the internet.

9. Make the image file residing in image folder as public.



|| C3 SCHOOLS

AWS Services Edit demo2016 Global Support

Upload Create Folder Actions

All Buckets / tempbuck135

	Name	Storage Class	Size	Last Modified
	Solutions-Architect-Associate.png	Reduced Redundancy	6.2 KB	Sat Sep 24 00:15:04 GMT+530 2016
	test.txt	Standard	83 bytes	Fri Sep 23 07:39:48 GMT+530 2016

Object: Solutions-Architect-Associate.png

Solutions-Architect-Associate.png

Bucket: tempbuck135
Name: Solutions-Architect-Associate.png
Link: <https://s3.ap-south-1.amazonaws.com/tempbuck135/Solutions-Architect-Associate.png>
Size: 6442
Last Modified: Sat Sep 24 00:15:04 GMT+530 2016
Owner: f5ab03db69048b107e456ecc2967fae84c90b48f73961716e864f038df078eca
ETag: 96395b51ce7b4863378f22dd55a23a92
Expiry Date: None
Expiration Rule: N/A

Details

Permissions

You can control access to the bucket and its contents using access policies. Learn more.

Grantee: Everyone Open/Download View Permissions Edit Permissions X

Grantee: Me Open/Download View Permissions Edit Permissions X

Add more permissions

Save Cancel

C3 SCHOOLS

10. Access the bucket from internet again. Your HTML page is displayed with the image.

The difference between making bucket as website is shown below.

11. If I remove the website enabled flag in the **Website** tab, when you access the website as <http://hoststaticwebsites3.s3-website-us-east-1.amazonaws.com/>, the “404-Page Not found Error” is displayed.



|| C3 SCHOOLS

AWS Services Edit demo2016 Global Support

Upload Create Folder Actions All Buckets / tempbuck135

	Name	Storage Class	Size	Last Modified
	Solutions-Architect-Associate.png	Reduced Redundancy	6.2 KB	Sat Sep 24 00:15:04 GMT+530 2016
	index.html	Reduced Redundancy	8 bytes	Sat Sep 24 00:46:19 GMT+530 2016
	test.txt	Standard	83 bytes	Fri Sep 23 07:39:48 GMT+530 2016
	test1	--	--	--

Bucket: tempbuck135
Region: Mumbai
Creation Date: Fri Sep 23 07:17:31 GMT+530 2016
Owner: f5ab03db69048b107e456ece29c7fae84c90b48f73961716e864f036df078eca

Permissions

Static Website Hosting

You can host your static website entirely on Amazon S3. Once you enable your bucket for static website hosting, all your content is accessible to web browsers via the Amazon S3 website endpoint for your bucket.

Endpoint: tempbuck135.s3-website.ap-south-1.amazonaws.com

Each bucket serves a website namespace (e.g. "www.example.com"). Requests for your host name (e.g. "example.com" or "www.example.com") can be routed to the contents in your bucket. You can also redirect requests to another host name (e.g. redirect "example.com" to "www.example.com"). See our walkthrough for how to set up an Amazon S3 static website with your host name.

Do not enable website hosting

Enable website hosting

Redirect all requests to another host name

Save Cancel

Nonetheless, the bucket is still public and can be accessed through <https://s3.amazonaws.com/hoststaticwebsites3/>.

If you access the bucket using the above URL, the output is generated through SOAP and shows you the content of the bucket in XML format.

The difference is the end point. Because this is no longer a static website, it only shows content and does not parse your HTML page.

How to Use Reduced Redundancy Storage (RRS) to Store an Object

This guide shows you how to store objects in RRS.

1. Create a S3 bucket as explained. Select bucket "reduced-redundancy-mum", and then click the "Upload" button.



|| C3 SCHOOLS

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with 'AWS', 'Services', 'Edit', and user information ('demo2016', 'Global', 'Support'). Below the navigation is a toolbar with 'Upload', 'Create Folder', and 'Actions' dropdown. The 'Actions' dropdown is open, showing options like 'Open', 'Download', 'Create Folder...', 'Upload' (which is highlighted in orange), 'Make Public', 'Rename', 'Delete', 'Initiate Restore', 'Cut', 'Copy', 'Paste', and 'Properties'. To the right of the menu, a message says 'The bucket 'reduced-redundacy-mum' is empty'. The main area has a table header with columns 'Name', 'Storage Class', 'Size', and 'Last Modified'.

2. Select the objects to be uploaded.

The screenshot shows the 'Upload - Select Files and Folders' dialog box overlying the S3 console. The dialog has a title bar 'Upload - Select Files and Folders' with 'Cancel' and 'Last Modified' buttons. It displays the upload path 'Upload to: All Buckets / reduced-redundacy-mum'. Below this is a note: 'To upload files (up to 5 TB each) to Amazon S3, click Add Files. You can also drag and drop files and folders to the area below. To remove files already selected, click the X to the far right of the file name.' A large text area says 'Drag and drop files and folders to upload here.' Two files are listed: 'index.html (8 bytes)' and 'webniet.txt (69 bytes)'. At the bottom are buttons for 'Add Files' (with a green plus icon) and 'Remove Selected Files' (with a red minus icon). The status bar at the bottom shows 'Number of files: 2 Total upload size: 77 bytes'. At the very bottom are 'Set Details >', 'Start Upload', and 'Cancel' buttons, with 'Set Details >' being the one highlighted with a red box.



|| C3 SCHOOLS

3. Click the “Set Details” button.

Upload Create Folder Actions ▾

All Buckets / reduced-redundancy-mum

Name

Search by prefix

None Properties Transfers

Cancel X

Last Modified

Set Details

Upload to: All Buckets / reduced-redundancy-mum

Details: Set additional details for all of the objects you upload. You can choose between Standard Storage, [Reduced Redundancy Storage](#), and [Standard - Infrequent Access Storage](#). You can also choose whether or not to [encrypt your files](#).

Use Standard Storage Use Standard - Infrequent Access Storage Use Reduced Redundancy Storage

Use Server Side Encryption [Learn more](#)

< Select Files Set Permissions > Start Upload Cancel

4. Select the “Use Reduced Redundancy Storage” checkbox.
5. If you want to provide specific access permission or want to set Metadata, click the “Set Permissions” button; otherwise, click the “Start Upload” button.
6. All selected objects are uploaded to the bucket specified in RRS storage class.
7. Select any of the uploaded objects, and then click the “Properties” button near the top of the screen.



|| C3 SCHOOLS

Object: webnier.txt

Bucket: reduced-redundancy-mum
Name: webnier.txt
Link: <https://s3.ap-south-1.amazonaws.com/reduced-redundancy-mum/webnier.txt>
Size: 69
Last Modified: Sat Sep 24 01:32:04 GMT+530 2016
Owner: f5ab03db69048b107e456ece29c7fae84c90b48f73961716e864f036df078eca
ETag: 5b69698b57722020b48a50fe8847e20b
Expiry Date: None
Expiration Rule: N/A

▼ Details

Storage Class: Standard Standard - Infrequent Access Reduced Redundancy

Server Side Encryption: None AES-256

Save **Cancel**

8. In the Details tab, you can see that the object is stored in Reduced Redundancy Storage.
9. If an object has been uploaded to the Standard storage class (Standard is selected in the Details tab), and you want to change the storage class to Reduced Redundancy, simply select the “Reduced Redundancy” option and click “Save”.

Link: https://s3.amazonaws.com/costTrackingBucket_NV/elb-dg.pdf

Storage: Standard Reduced Redundancy

Server Side Encryption: None AES-256

Save **Cancel**

10. The object is transferred from Standard Storage to Reduced Redundancy Storage.



|| C3 SCHOOLS

The screenshot shows the AWS Transfer interface. At the top, there is a checkbox labeled "Automatically clear finished transfers". Below it, there are two completed transfer tasks: "Upload: Uploading 3 items to reduced_redundancy_NV" and "Use Reduced Redundancy Storage: elb-dg.pdf in costTrackingBucket_NV", both marked as "Done".

How to Move or Copy Objects between Regions

This shows how to move or copy objects between two S3 buckets in two different Amazon Cloud availability regions. Also includes explanation on how to delete an object or a folder from a bucket.

AWS Simple Storage Service (S3) buckets can be created in different regions. AWS S3 never copies the object from one region to another unless it is instructed to do so.

To illustrate how you can easily move or copy objects between regions using AWS S3 console:

- We have created the bucket “buckettocopy” in Singapore Region.

The screenshot shows the AWS S3 console. In the top navigation bar, "Services" is selected. On the left, under "All Buckets (3)", there are three buckets listed: "buckettocopy", "elasticbeanstalk-ap-southeast-1-076828422820", and "tempbuck135". A modal window titled "Bucket: buckettocopy" is open, prompting the user to "Create a Bucket - Select a Bucket Name and Region". The "Bucket Name" field contains "buckettocopy" and the "Region" dropdown is set to "Singapore". At the bottom of the modal are "Set Up Logging > Create" and "Cancel" buttons.

- We have created another bucket in US-Oregon Region named “copypasteobjectinto”.



|| C3 SCHOOLS

A screenshot of the AWS S3 console. At the top, there's a navigation bar with "AWS", "Services", "Edit", and dropdown menus for "demo2016", "Global", and "Support". Below the navigation is a toolbar with "Create Bucket" (highlighted in blue), "Actions", and buttons for "None", "Properties", and "Transfers". A table titled "All Buckets (4)" lists existing buckets: "buckettocopy", "copypasteobjectinto" (which is selected and highlighted in blue), "elasticbeanstalk-ap-southeast-1-076828422820", and "tempbuck135". To the right of the table, a modal dialog box is open with the title "Bucket: copypasteobjectinto". The dialog is titled "Create a Bucket - Select a Bucket Name and Region" and contains instructions about bucket creation. It has fields for "Bucket Name" (set to "copypasteobjectinto") and "Region" (set to "Oregon"). At the bottom of the dialog are "Set Up Logging >", "Create" (in a blue button), and "Cancel" buttons.

C3 SCHOOLS



|| C3 SCHOOLS

- We have uploaded some objects to the US Standard Region bucket, “buckettocopy”.

	Name	Storage Class	Size	Last Modified
<input type="checkbox"/>	Desert.jpg	Standard	826.1 KB	Sat Sep 24 01:52:24 GMT+530 2016
<input type="checkbox"/>	Hydrangeas.jpg	Standard	581.3 KB	Sat Sep 24 01:52:29 GMT+530 2016
<input type="checkbox"/>	Jellyfish.jpg	Standard	757.5 KB	Sat Sep 24 01:52:35 GMT+530 2016

- I created a folder a file into it. The folder “Folder1” has a file inside it. **The following describes how to move “Folder1” from US Oregon region to Singapore.**

1. Right-click “Folder1” and select **Cut**.

Bucket: buckettocopy
Name: Folder1



|| C3 SCHOOLS

2. Go to the target bucket, “copypasteobjectinto”, right-click it and select **Paste**.

The screenshot shows the AWS S3 console interface. At the top, there are buttons for Upload, Create Folder, and Actions (with a dropdown arrow). Below that is a search bar labeled "Search by prefix" and buttons for None, Properties, and Transfers. The main area displays a table with columns for Name, Storage Class, Size, and Last Modified. A message at the top right says "The bucket 'copypasteobjectinto' is empty". On the far left, there's a sidebar with navigation links like All Buckets, Home, and Help. The Actions menu is open, showing options like Open, Download, Create Folder..., Upload, Make Public, Rename, Delete, Initiate Restore, Cut, Copy, Paste (which is highlighted in orange), and Properties.

As shown below, the task progress status is displayed in the **Transfers** panel. When the folder and its object have been moved, the folder is displayed in the target bucket.

This screenshot shows the AWS S3 console with the Transfers panel open. The top navigation bar includes AWS, Services, Edit, demo2016, Global, and Support. The main area shows a table with columns for Name, Storage Class, Size, and Last Modified. In the Transfers panel, there's a checkbox for "Automatically clear finished transfers" and a "Done" status entry with a green checkmark. The entry details a copy operation: "Copy: Folder1 from buckettocopy to copypasteobjectinto".

3. Open the folder to display the file. The cut–paste operation moves all the files in the folder to the target bucket.



|| C3 SCHOOLS

The screenshot shows the AWS S3 console with the path "All Buckets / copypasteobjectinto / Folder1". A table lists an object named "Tulips.jpg" with details: Storage Class (Standard), Size (606.3 KB), and Last Modified (Sat Sep 24 02:08:36 GMT+530 2016). To the right, a "Transfers" section shows a "Done" status with a message: "Copy: Folder1 from buckettocopy to copypasteobjectinto".

	Name	Storage Class	Size	Last Modified
	Tulips.jpg	Standard	606.3 KB	Sat Sep 24 02:08:36 GMT+530 2016

The operation to copy the objects from the source bucket to target bucket is similar. As shown, the source bucket "buckettocopy" does not have "Folder" because we moved it to target bucket "copypasteobjectinto". In the source bucket, we will select two objects.

4. Right-click and select **Copy**.

The screenshot shows the AWS S3 console with the path "All Buckets / buckettocopy". A context menu is open over three selected objects: "Desert.jpg", "Hydrangeas.jpg", and "Jellyfish.jpg". The "Copy" option is highlighted in the menu. To the right, a summary indicates "2 items selected" and specifies the "Bucket: buckettocopy" and "Selected: 2".

	Name	Size	Last Modified
	Desert.jpg	826.1 KB	Sat Sep 24 01:52:24 GMT+530 2016
	Hydrangeas.jpg	581.3 KB	Sat Sep 24 01:52:29 GMT+530 2016
	Jellyfish.jpg	757.5 KB	Sat Sep 24 01:52:35 GMT+530 2016

5. Go to target bucket "copypasteobjectinto", right-click and select **Paste**.



|| C3 SCHOOLS

The screenshot shows the AWS S3 console interface. A context menu is open over a folder named 'Folder1'. The 'Actions' dropdown is expanded, and the 'Paste' option is highlighted in orange. The main pane displays a table of objects in the 'copypasteobj' bucket, including 'Desert.jpg' and 'Hydrangeas.jpg'. The right pane shows the 'Transfers' section with a 'Done' status message.

Name	Size	Last Modified
Desert.jpg	826.1 KB	Sat Sep 24 02:21:38 GMT+530 2016
Folder1	--	--
Hydrangeas.jpg	581.3 KB	Sat Sep 24 02:21:38 GMT+530 2016

6. Initially, there was only a folder inside the bucket. When the copy operation is completed, the objects will appear in the target bucket.

The screenshot shows the AWS S3 console interface. The 'copypasteobjectinto' bucket is selected. The main pane displays a table of objects in the 'copypasteobjectinto' bucket, including 'Desert.jpg', 'Folder1', and 'Hydrangeas.jpg'. The right pane shows the 'Transfers' section with two completed transfer messages: one for 'Folder1' and another for '2 items'.

Name	Storage Class	Size	Last Modified
Desert.jpg	Standard	826.1 KB	Sat Sep 24 02:21:38 GMT+530 2016
Folder1	--	--	--
Hydrangeas.jpg	Standard	581.3 KB	Sat Sep 24 02:21:38 GMT+530 2016

We have completed the moving as well as the copy-pasting of objects across regions. [To delete objects, follow the next steps.](#)

7. Go to the "buckettocopy" bucket. Select a couple of files, then right-click and select 'Delete'.



|| C3 SCHOOLS

The screenshot shows the AWS S3 console interface. In the center, there is a table listing three objects: 'Desert.jpg', 'Hydrangeas.jpg', and 'Jellyfish.jpg'. The 'Jellyfish.jpg' row has a context menu open, with the 'Delete' option highlighted. On the right side of the screen, there is a 'Transfers' panel showing two completed transfers: one for 'Folder1' and another for '2 items from buckettocopy'.

You are prompted to confirm the deletion.

The screenshot shows the AWS S3 console with a confirmation dialog box overlaid. The dialog asks if the user is sure they want to delete 'Desert.jpg' and 'Hydrangeas.jpg'. It also has a checkbox for 'Prevent this page from creating additional dialogs.' At the bottom of the dialog are 'OK' and 'Cancel' buttons, with 'OK' being highlighted. The background shows the same S3 bucket list and transfers panel as the previous screenshot.

8. Click **OK** to confirm and start the delete process. The progress of deleting is shown in the **Transfers** panel. When the delete operation is complete, the objects will no longer be displayed in the bucket.

The screenshot shows the AWS S3 console after the deletion of 'Desert.jpg' and 'Hydrangeas.jpg'. Only 'Jellyfish.jpg' remains in the bucket. The 'Transfers' panel on the right shows the completion of the deletion process, with a message indicating 'Deleting 2 objects from buckettocopy'.



|| C3 SCHOOLS

You can delete more than one object at a time. You can also delete a folder – but only if the folder is empty.

9. Delete the items in the folder, and then you can delete the folder.

The screenshot shows the AWS Management Console interface for the S3 service. On the left, the 'Buckets' sidebar lists several buckets, including 'copyobjectfromme', 'copypasteobjectintome' (which is selected), 'hoststaticwebsites3', 's3buckett07072012', and 'tests3aminvm070712'. The main 'Objects and Folders' pane displays the contents of the 'copypasteobjectintome' bucket, showing two objects: 'Sample1.txt.txt' (33 bytes, Last Modified: Tue Jul 24 15:13:27 GMT+530 2012) and 'Sample2.txt' (61 bytes, Last Modified: Tue Jul 24 15:13:27 GMT+530 2012). Below this, the 'Transfers' section shows a list of tasks: 'Delete: Deleting Folder1 from copypasteobjectintome', 'Delete: Deleting Sample3.txt from Folder1', 'Delete: Deleting Folder1 from copypasteobjectintome', 'Delete: Deleting Folder1 from copypasteobjectintome', 'Move: Folder1 from copypasteobjectintome to copyobjectfromme', and 'Delete: Deleting Folder1 from copyobjectfromme'. Several of these tasks have failed, with error status bars highlighted by red boxes. At the bottom of the page, there is a footer with links to 'Feedback', 'Support', 'Privacy Policy', 'Terms of Use', and 'An amazon.com company'.

You can delete a bucket in the same way, after ensuring that all objects and folders it contains have been deleted.

How to Encrypt AWS S3 Storage Objects

Amazon AWS supports two kinds of encryption:

- a. Server Side Encryption
- b. Client Side Encryption

This document explains how to achieve Server Side Encryption using AWS console.

Server side encryption of data encryption at rest can be achieved through AWS Management Console, using AWS S3 APIs or SDK. Amazon S3 encrypts your data as it writes it to disks in its data centers and decrypts it only when accessing it.

1. Create an S3 bucket. We created a sample bucket named serverside-encryption-test



|| C3 SCHOOLS

AWS | Services | Edit

Create Bucket Actions

All Buckets (5)

Name
autobucket135
cf-templates-2tsqo9p6j1qg-ap-south-1
elasticbeanstalk-ap-southeast-1-076828422820
serverside-encryption-test
techtrends

2. Create an Object in the bucket. Manage S3 storage objects. Start by clicking on the `Upload` button inside the Object panel and then select the objects to be uploaded to the bucket.

Upload - Select Files and Folders

Upload to: All Buckets / serverside-encryption-test

To upload files (up to 5 TB each) to Amazon S3, click **Add Files**. You can also drag and drop files and folders to the area below. To remove files already selected, click the X to the far right of the file name.

Drag and drop files and folders to upload here.

Aws.txt (0 bytes) chef class.txt (4.3 KB)

Add Files **Remove Selected Files**

Number of files: 2 Total upload size: 4.3 KB

Set Details > Start Upload Cancel



|| C3 SCHOOLS

3. Click on 'Select Details' as shown above.
4. Select 'User Server Side Encryption', there are two types master keys select accordingly and click on "start upload"

Set Details Cancel

Upload to: All Buckets / [serverside-encryption-test](#)

Details: Set additional details for all of the objects you upload. You can choose between Standard Storage, [Reduced Redundancy Storage](#), and [Standard - Infrequent Access Storage](#). You can also choose whether or not to [encrypt your files](#).

Use Standard Storage Use Standard - Infrequent Access Storage Use Reduced Redundancy Storage

Use Server Side Encryption [Learn more](#)

Use the Amazon S3 service master key
S3 will decrypt the object for anyone with permission to access this object.

Use an AWS Key Management Service master key
S3 will decrypt the object for anyone with permission to access this object and permission to use the master key.

[< Select Files](#) [Set Permissions >](#) Start Upload [Cancel](#)



|| C3 SCHOOLS

Set Details Cancel 

Upload to: All Buckets / serverside-encryption-test

Details: Set additional details for all of the objects you upload. You can choose between Standard Storage, [Reduced Redundancy Storage](#), and [Standard - Infrequent Access Storage](#). You can also choose whether or not to [encrypt your files](#).

Use Standard Storage Use Standard - Infrequent Access Storage Use Reduced Redundancy Storage

Use Server Side Encryption [Learn more](#)

Use the Amazon S3 service master key
S3 will decrypt the object for anyone with permission to access this object.

Use an AWS Key Management Service master key
S3 will decrypt the object for anyone with permission to access this object and permission to use the master key.

Master Key: arn:aws:kms:ap-south-1:076828422820:key/de0c0e64-9705-42dc-92cf-b385dff0cb76 ▼
Only keys in the same region as this bucket are available for encrypting objects in this bucket.

Description: Default master key that protects my EBS volumes when no other key is defined

Account: 076828422820 (this account)

Key ID: de0c0e64-9705-42dc-92cf-b385dff0cb76

[< Select Files](#) [Set Permissions >](#) **Start Upload** [Cancel](#)

5. The objects will be uploaded to the selected bucket.

6. Select one of the uploaded objects and click on the properties button to display the properties of that object.



|| C3 SCHOOLS

Upload Create Folder Actions ▾

All Buckets / serverside-encryption-test

	Name	Storage Class	Size	Last Modified
	Aws.txt	Standard	0 bytes	Thu Oct 27 14:05:40 GMT+530 2016
	chef class.txt	Standard	4.3 KB	Thu Oct 27 14:05:40 GMT+530 2016

Object: Aws.txt X

Bucket: serverside-encryption-test
Name: Aws.txt
Link: <https://s3.ap-south-1.amazonaws.com/serverside-encryption-test/Aws.txt>
Size: 0
Last Modified: Thu Oct 27 14:05:40 GMT+530 2016
Owner: 15ab03db69048b107e456ece29c7fae84c90b48f73961716e864f036d1078eca
ETag: d41d8cd98f00b204e9800998ecf8427e
Expiry Date: None
Expiration Rule: N/A

▼ Details

Storage Class: Standard Standard - Infrequent Access Reduced Redundancy

Server Side Encryption: None AES-256

Save Cancel



7. It will show that the object is “Server Side Encrypted” using ASE-256.

8. Amazon S3 Server Side Encryption employs strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 Server Side Encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.

9. Other way to achieve server side encryption is by using REST APIs.

There are two ways to achieve Client Side encryption:

a. Encrypting your data before sending it to Amazon S3. You can use any encryption mechanism you would prefer. You can check Porticor as an option for that matter.



|| C3 SCHOOLS

- b. Use AWS SDK for Java to encrypt data before sending it to S3. The AWS SDK for Java uses a process called envelope encryption. In envelope encryption, you provide your encryption key to the Amazon S3 encryption client and the client takes care of the rest of the process.

How to Install Command Line Tools (CLI) for Amazon AWS Cloud Watch

AWS CloudWatch is used to monitor AWS cloud resources and the applications customers run on AWS. It can monitor AWS resources as well metrics generated by custom applications and services hosted in AWS.

Part 1 - Downloading CLI from AWS S3

1. Create a folder to store your APIs in your local drive. E.g. C:\AWS\CloudWatch

The screenshot shows a Windows Command Prompt window with the title bar "Administrator: C:\Windows\system32\cmd.exe". The command line shows the user navigating to the "AWS" directory and then creating a new folder named "CloudWatch" using the command "cd AWS & cd CloudWatch & md CloudWatch". The output shows the folder has been created at "C:\AWS\CloudWatch".

C3 SCHOOLS

2. Download the Amazon [AWS Cloud Watch API tools for Windows](#) and save it in the folder created. [Get the latest version of Cloud Watch API](#).

3. Unzip the file and extract it to a local drive.



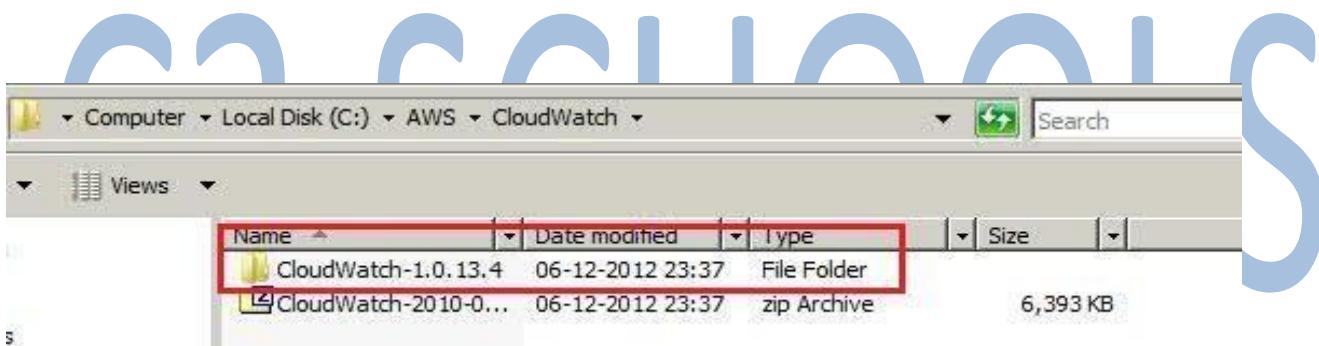
|| C3 SCHOOLS

```
C:\Administrator:C:\Windows\system32\cmd.exe
C:\>cd AWS\CloudWatch
C:\AWS\CloudWatch>cd CloudWatch-1.0.13.4
C:\AWS\CloudWatch\CloudWatch-1.0.13.4>dir
Volume in drive C has no label.
Volume Serial Number is 2262-EEA1

Directory of C:\AWS\CloudWatch\CloudWatch-1.0.13.4

06-12-2012 23:37 <DIR> .
06-12-2012 23:37 <DIR> ..
06-12-2012 23:37 <DIR> bin
17-09-2012 21:31 82 credential-file-path.template
06-12-2012 23:37 <DIR> lib
17-09-2012 21:31 5,111 license.txt
17-09-2012 21:31 1,813 notice.txt
17-09-2012 21:31 2,786 README.TXT
17-09-2012 21:32 1,908 RELEASENOTES.TXT
17-09-2012 21:31 83,461 THIRDPARTYLICENSE.TXT
       6 File(s)    95,161 bytes
      4 Dir(s)  7,535,304,704 bytes free

C:\AWS\CloudWatch\CloudWatch-1.0.13.4>
```



Part 2 – Install and setup Java

1. If JDK / JRE is not installed and the environment variables are not set please follow the steps below, otherwise skip to part 2 below.
2. [Download JDK 5 \(or above\)](#) and Install.
3. Set the environment variable as following:
 - i. JAVA_HOME=<JRE / JDK PATH>



|| C3 SCHOOLS

```
C:\>set JAVA_HOME=C:\Program Files\Java\jdk1.7.0_09
```

ii. PATH=%PATH%;<JAVA_HOME>\bin; C:\AWS\CloudWatch\CloudWatch-1.0.13.4\bin\;

iii. CLASSPATH=%PATH%;<JAVA_HOME>\lib; C:\AWS\CloudWatch\CloudWatch-1.0.13.4\lib\

> Note that we have added the bin folder of CloudWatch API also as part of the PATH.

```
C:\>set JAVA_HOME=C:\Program Files\Java\jdk1.7.0_09
C:\>set PATH=%PATH%;C:\AWS\CloudWatch\CloudWatch-1.0.13.4\bin\
C:\>set CLASSPATH=%CLASSPATH%;C:\AWS\CloudWatch\CloudWatch-1.0.13.4\lib;C:\Program Files\Java\jdk1.7.0_09\lib\
C:\AWS\CloudWatch\CloudWatch-1.0.13.4>
```

4. Run command java -version and verify that it displays the correct version of your JDK / JRE.

```
C:\>java -version
java version "1.7.0_09"
Java(TM) SE Runtime Environment (build 1.7.0_09-b05)
Java HotSpot(TM) Client VM (build 23.5-b02, mixed mode, sharing)
```

5. If you setup the above commands through the command window it will be valid for the session of the command window only.

6. Set all the above parameters through Environment Variables.

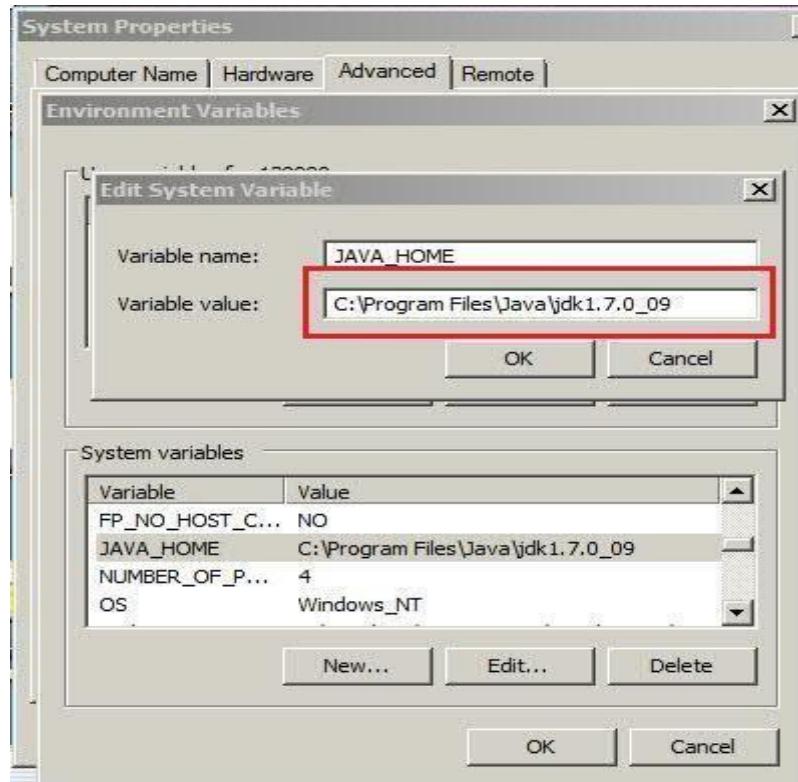
You can access Environment Variables for windows 7 / Vista at: MyComputer -> Right Click and Select Properties -> Select “Advanced System Settings” from the left menu and go to the Environment Variables.



|| C3 SCHOOLS

For Windows XP Right Click on Computer -> Select Properties -> Select Advanced Tab and click -> Environment Variables.

7. Set the variables as shown below.



TOOLS

Part 3 -- Download and set AWS Certificate File and Private Keys.

1. Enter your UI console.
2. On the left menu click "Security Credentials".



|| C3 SCHOOLS

The screenshot shows the AWS Account Management console. The left sidebar has a red box around the "Security Credentials" link under the "Account" category. The main content area contains text about managing root account credentials and three types of credentials: Access Credentials, Sign-In Credentials, and Account Identifiers. A blue link at the bottom right of the content area points to "Find out which AWS Security Credentials you need".

This page allows you to manage the root account credentials for your AWS Account. To manage IAM Users, their permissions, and security credentials, use the AWS Management Console.

Welcome D1 | Sign Out
Account Number 0 E - 82 18-0 .6

Access to applications and services within AWS cloud is secure and protected in multiple ways. Accessing those applications and services requires the use of special credentials that are associated with your account. There are three types of credentials currently offered by AWS. If you know which security credentials you need, simply select one of the links below:

↓ **Access Credentials:** Your Access Keys, X.509 Certificates, and Key Pairs
↓ **Sign-In Credentials:** Your E-mail Address, Password, and AWS Multi-Factor Authentication Device
↓ **Account Identifiers:** Your AWS Account ID and Canonical User ID

If you are not sure which security credentials you should use, the link below will help you identify the credentials you need for the task you want to accomplish:

Find out which AWS Security Credentials you need

C3 SCHOOLS



|| C3 SCHOOLS

3. Click "Access Credentials" and select the "X.509 Certificates" tab.

Access Credentials

There are three types of access credentials used to authenticate your requests to AWS services: (a) access keys, (b) X.509 certificates, and (c) key pairs. Each access credential type is explained below.

[Access Keys](#) | [**X.509 Certificates**](#) | [Key Pairs](#)

Use X.509 certificates to make secure SOAP protocol requests to AWS service APIs.

Exceptions: Amazon S3 and Amazon Mechanical Turk instead require your Access Keys for SOAP requests.

Created	X.509 Certificate	Status
July 13, 2010	cert-7QD6LR QOBN7UF VH3EYEIM.pem	Active (Make Inactive)

[Create a new Certificate](#) | [Upload Your Own Certificate](#)

[View Your Deleted Certificates](#)

For your protection, AWS doesn't ask for your private key or retain it on file. You should also never share your private key with anyone. In addition, industry best practice recommends frequent certificate rotation.

[Learn more about X.509 Certificates](#)

4. It will show you all the existing active / inactive certificates.

5. Click "Create a new Certificate". You will get the following screen:



|| C3 SCHOOLS



6. Download your private key file and the X.509 certificate to a local folder. (e.g. D:\Cloud\keys\).

7. If you fails to save the Private Key file, AWS will not store it and you will lose it permanently.

8. In that case, delete the new certificate and start the process again.

9. Store the downloaded .ppk & .cert file into a local directory (e.g D:\Cloud\keys\). Set the AWS Keys in environment as below :

i. EC2_CERT=<fully qualified path where cert-xxxxx.pem file placed>

e.g. EC2_CERT= D:\Cloud\keys\ cert-F42xxxxxxxxxAR2xxxxxxUBA438xxxxD.pem



|| C3 SCHOOLS



ii. EC2_PRIVATE_KEY=<fully qualified path where pk-xxxx.pem file placed>

e.g. EC2_PRIVATE_KEY= D:\Cloud\keys\ pk- F42xxxxxxxxxAR2xxxxxxUBA438xxxxD.pem



iii. AWS_CLOUDWATCH_HOME = C:\AWS\CloudWatch\CloudWatch-1.0.13.4\;



10. Check if all setup is done by checking the values using the following command:



|| C3 SCHOOLS

```
C:\Administrator: C:\Windows\system32\cmd.exe
C:\>set EC2_CERT
EC2_CERT=D:\Cloud\keys\cert-[REDACTED].pem

C:\>set EC2_PRIVATE_KEY
EC2_PRIVATE_KEY=D:\Cloud\keys\pk-[REDACTED].pem

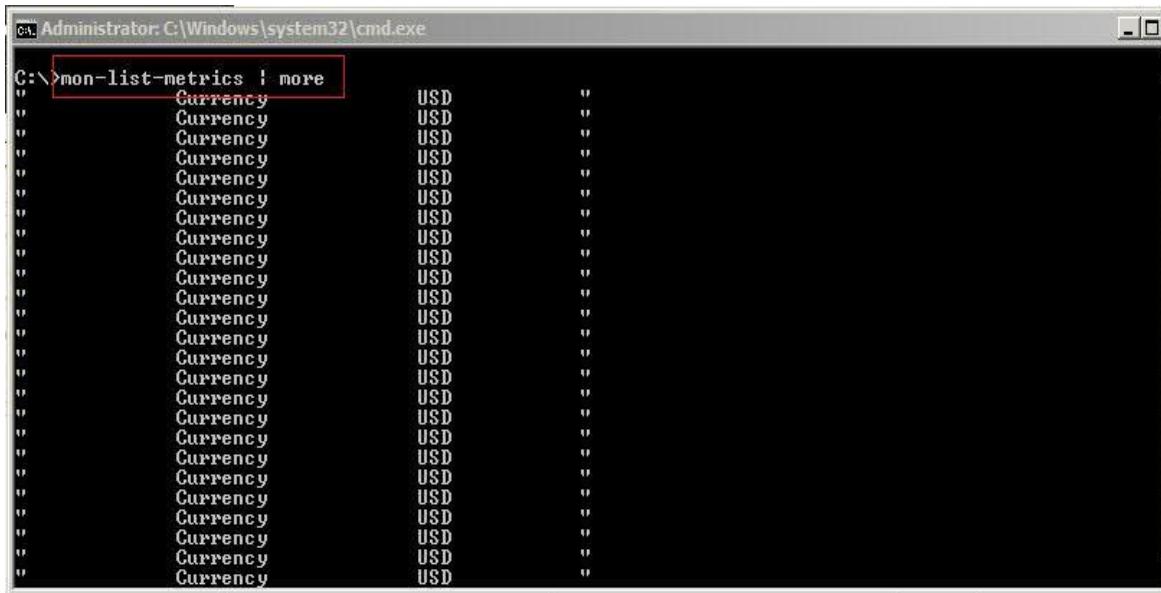
C:\>set EC2_HOME
EC2_HOME=D:\Cloud\Tools\ec2-api-tools-1.6.4

C:\>set JAVA_HOME
JAVA_HOME=C:\Program Files\Java\jdk1.7.0_09

C:\>set AWS_CLOUDWATCH_HOME
AWS_CLOUDWATCH_HOME=C:\AWS\CloudWatch\CloudWatch-1.0.13.4\
```

C3 SCHOOLS

11. Once the setup is done, run the CloudWatch commands to test whether CloudWatch APIs are set correctly or not.



```
C:\>mon-list-metrics | more
"Currency" "USD"
```

If you do not get an error and get an output like the above, it means that your setup for CloudWatch API is complete.

C3 SCHOOLS

IAM How-to: Setting up AWS IAM CLI Tool on Windows

A) Downloading AWS SDK APIs from AWS S3

1. Create a folder to store your APIs in your local drive. E.g. C:\AWS.

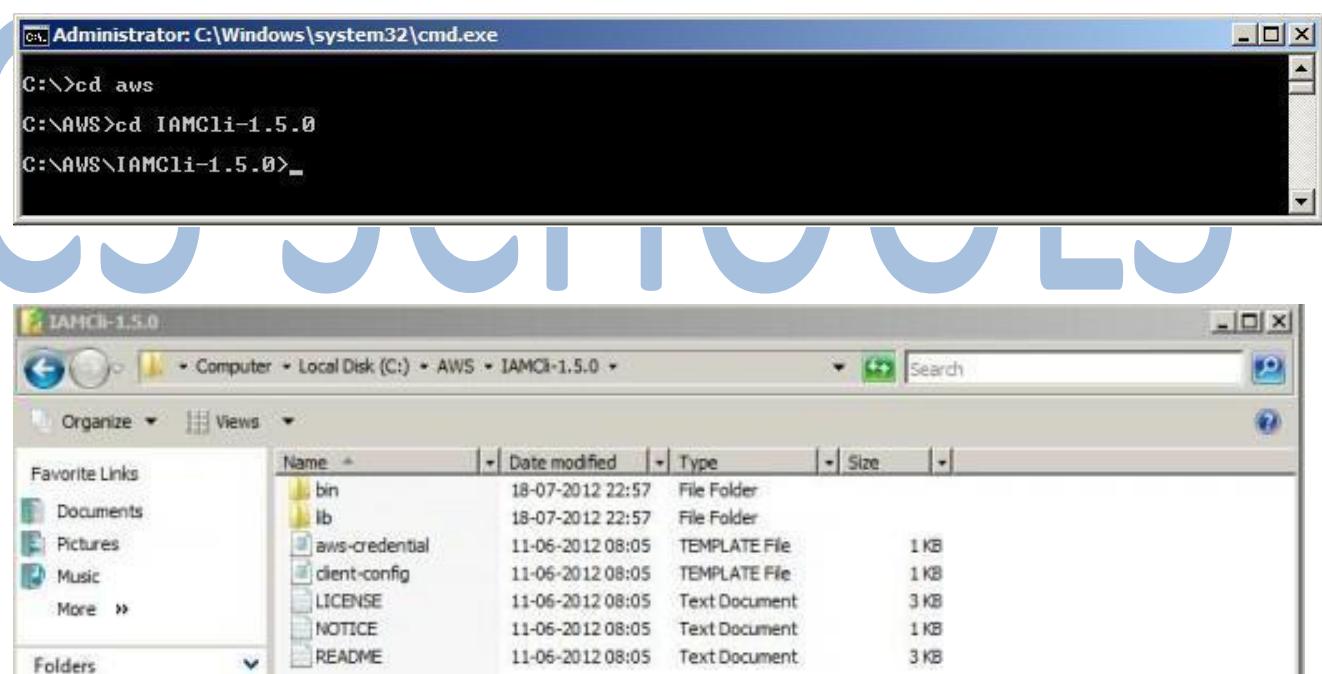


```
C:\>Administrator: C:\Windows\system32\cmd.exe
C:\>cd AWS
C:\AWS>
```

2. Download the Amazon AWS SDK API tools for Windows (.zip) file from the following

link <http://awsiammedia.s3.amazonaws.com/public/tools/cli/latest/IAMCli.zip> and save in the folder created in step#1.

3. Unzip the file and extract it to local drive.



B) Install and setup Java

1. If JDK / JRE is not installed and environment variables are not set please follow below steps, else jump to section 'C'.
2. Install and download JDK 5 or above. The JDK download is free and JDK 7 is available for

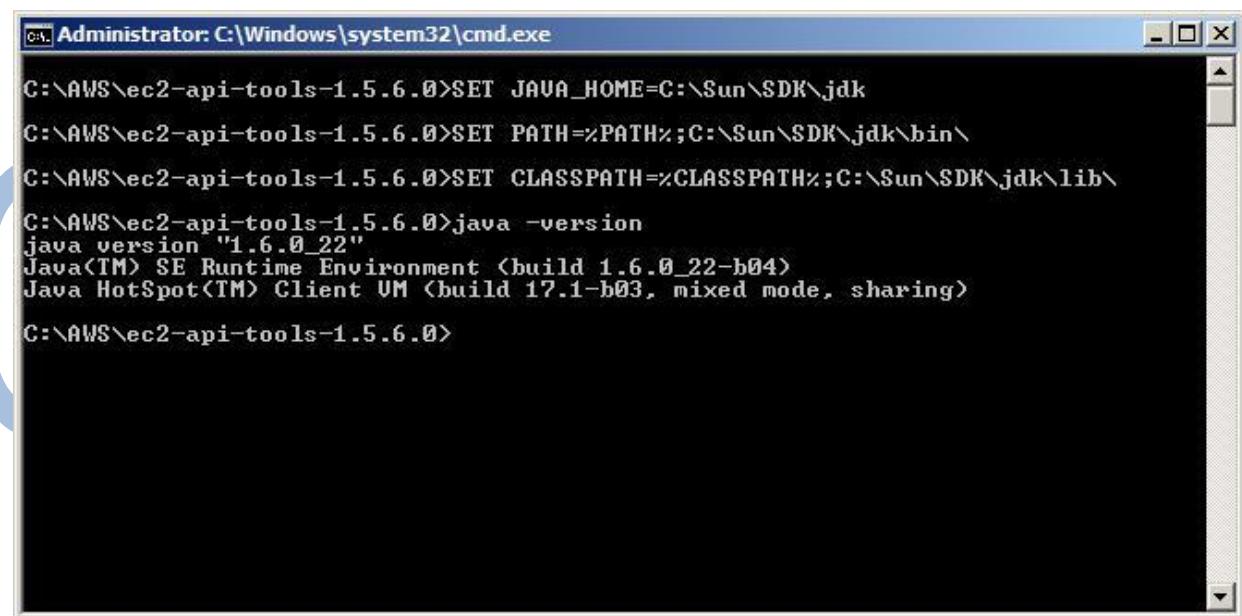
download at <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

C3 SCHOOLS

3. Set environment variable as following

- i. JAVA_HOME=<JRE / JDK PATH>
- ii. PATH=%PATH%;<JAVA_HOME>\bin\
- iii. CLASSPATH=%PATH%;<JAVA_HOME>\lib\

4. Run command **java -version** and check if it displays the correct version of your JDK / JRE.



The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window contains the following text:

```
C:\AWS\ec2-api-tools-1.5.6.0>SET JAVA_HOME=C:\Sun\SDK\jdk
C:\AWS\ec2-api-tools-1.5.6.0>SET PATH=%PATH%;C:\Sun\SDK\jdk\bin\
C:\AWS\ec2-api-tools-1.5.6.0>SET CLASSPATH=%CLASSPATH%;C:\Sun\SDK\jdk\lib\
C:\AWS\ec2-api-tools-1.5.6.0>java -version
java version "1.6.0_22"
Java(TM) SE Runtime Environment (build 1.6.0_22-b04)
Java HotSpot(TM) Client VM (build 17.1-b03, mixed mode, sharing)
C:\AWS\ec2-api-tools-1.5.6.0>
```

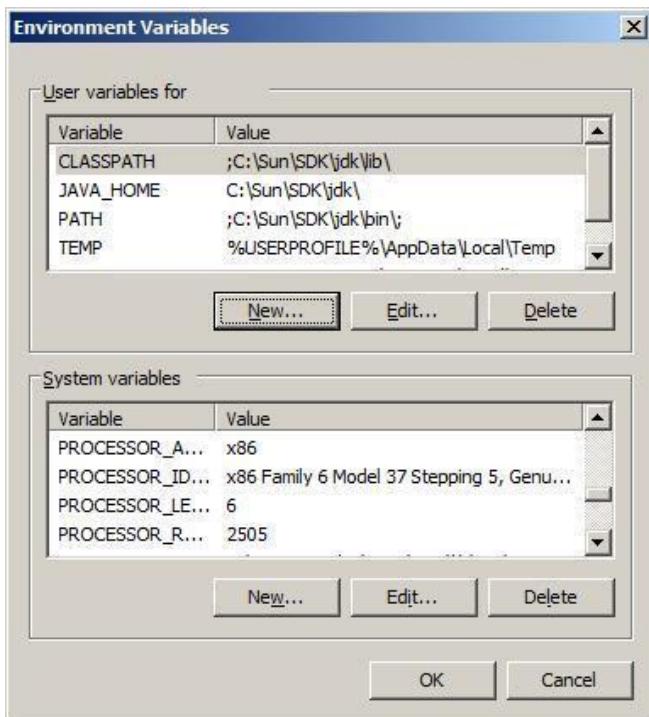
5. If you setup above commands though command window it will be valid for the session of this command window only.
6. Please set all above parameters through Environment Variables. You can access Environment variables,

For windows 7 / Vista through: MyComputer -> Right Click and Select Properties. -> select "Advanced System Settings" leftmenu and from goto Environment variables.

For Windows XP Right Click on Computer -> Select Properties -> Select Advanced Tab and click -> Environment variables.

C3 SCHOOLS

7. Set the variables as shown below.



C3 SCHOOLS

C) Download and set AWS Certificate File and Private Keys. (Some of the data is masked or removed in the screen for confidentiality purpose).



|| C3 SCHOOLS

1. Go to AWS Account section. <http://aws.amazon.com/account>.

2. In the left menu click on “Security Credentials” as selected below.

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with icons for Home, AWS, Services, Edit, demo2016 (username), Oregon (region), and Support. Below the navigation bar is the main content area titled "Amazon Web Services". The left sidebar contains several service categories: Compute (EC2, Lambda), Storage & Content Delivery (S3, CloudFront, Elastic File System, Glacier, Snowball, Storage Gateway), Database (RDS), and others like Developer Tools, Internet of Things, Game Development, Mobile Services, Application Services, and Security & Identity. On the right side, there's a user profile section for "IAM User: RaVi" and "Account: demo2016". A "Tag Editor" button is also present. A large blue watermark "C3 SCHOOLS" is overlaid across the entire screenshot.

3. Go to Access Credentials – > Access keys.

There are three types of access credentials used to authenticate your requests to AWS services: (a) access keys, (b) X.509 certificates, and (c) key pairs. Each access credential type is explained below.



The screenshot shows the AWS IAM Access Keys page. At the top, there are three tabs: "Access Keys" (selected), "X.509 Certificates", and "Key Pairs". Below the tabs, a note explains that access keys can be used to make secure REST or Query protocol requests to any AWS service API. It mentions that one is created automatically when the account is created. A "Your Access Keys" table lists a single key entry:

Created	Access Key ID	Secret Access Key	Status
December 15, 2009	AKIAITEDMZTXFAUQHLYQ	Show	Active (Make)

A "Create a new Access Key" button is located below the table. A modal dialog box titled "Secret Access Key" is displayed over the table, showing a long, randomly generated secret key value.

Below the table, a note cautions against sharing secret access keys with others and recommends frequent key rotation.

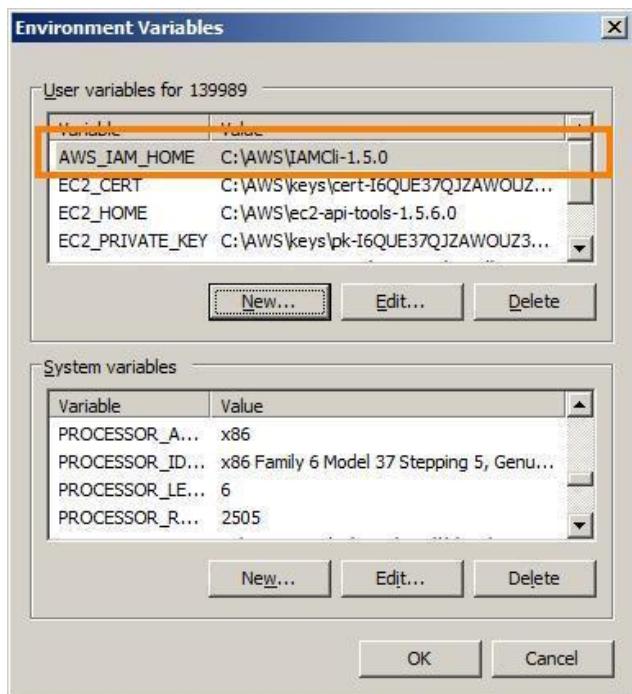
C3 SCHOOLS

4. Note down your access keys and secret access keys.

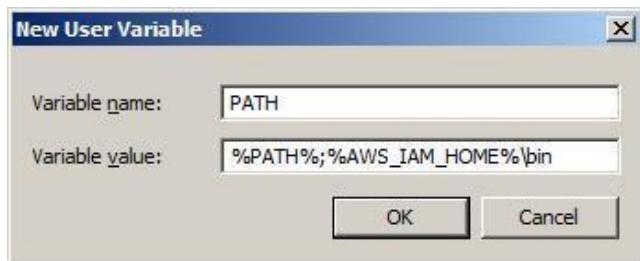
5. Set the AWS IAM Keys in environment as below: (You can access Environment variables through

For windows 7 / Vista: MyComputer -> Right Click and Select Properties. -> select “Advanced System Settings” from left menu and go to Environment variables.)

- i. set AWS_IAM_HOME=<path_to_cli> (Here C:\AWS\IAMCli-1.5.0).



ii. set Path=%AWS_IAM_HOME%\bin;%Path%

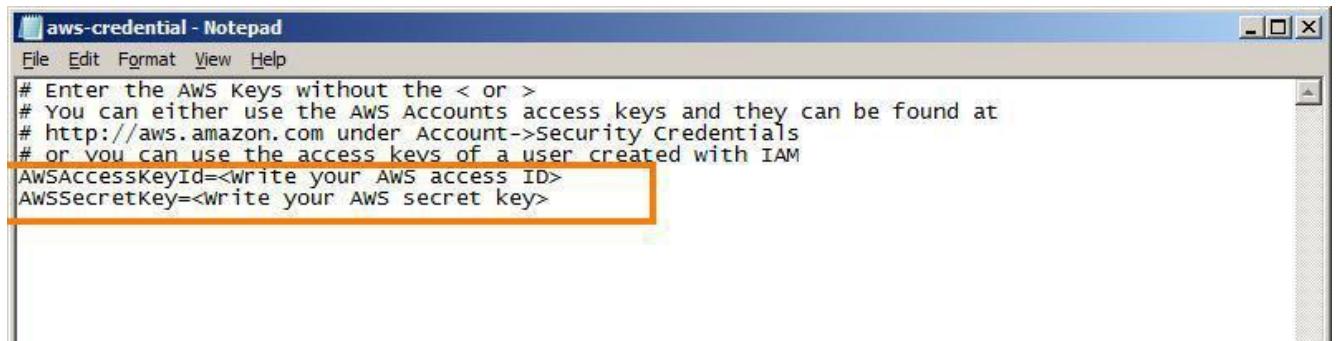


6. Now you need to set your access Key and secret access key, you downloaded in step#4.

7. Create a new file in IAM API folder which you created in step#3 of Section A (C:\AWS\IAMCli-1.5.0).

8. I named file 'aws-iam-credentials.txt'. Copy all the-credentialcontent.template'from'aws to new file.

9. In the new-iam'aws-credentials.txt', update your access key and secret acce you got in step#4.

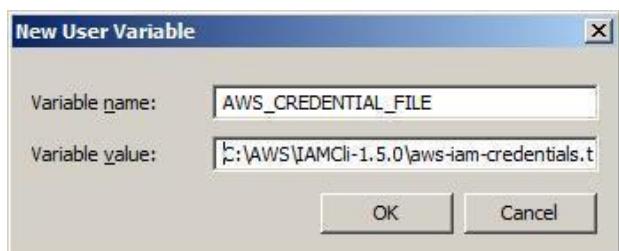


```

aws-credential - Notepad
File Edit Format View Help
# Enter the AWS Keys without the < or >
# You can either use the AWS Accounts access keys and they can be found at
# http://aws.amazon.com under Account->Security Credentials
# or you can use the access keys of a user created with IAM
AWSAccessKeyId=<write your AWS access ID>
AWSSecretKey=<write your AWS secret key>

```

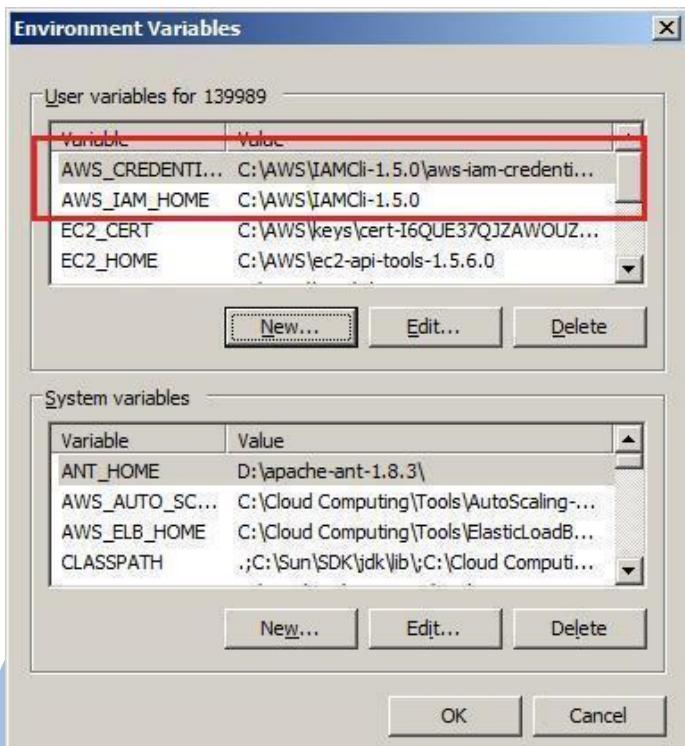
10. Now set this **aws-iam-credentials.txt** file in your environment variable.



C3 SCHOOLS

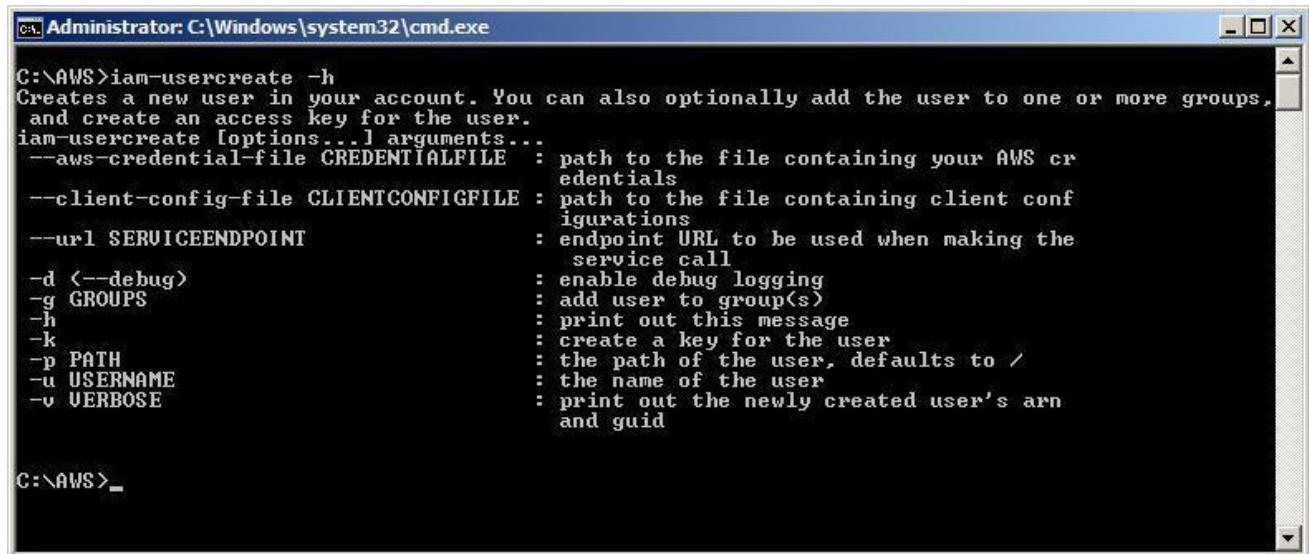
```
set AWS_CREDENTIAL_FILE=<path_and_filename_of_credential_file>
```

11. Once you set all above variable, your environment variable will have values as below.



C3 SCHOOLS

12. Now your command line tool API are set. Run the command **iam-usercreate -h** to verify.



```
C:\AWS>iam-usercreate -h
Creates a new user in your account. You can also optionally add the user to one or more groups,
and create an access key for the user.
iam-usercreate [options...] arguments...
--aws-credential-file CREENTIALFILE : path to the file containing your AWS cr
edentials
--client-config-file CLIENTCONFIGFILE : path to the file containing client conf
igurations
--url SERVICEENDPOINT : endpoint URL to be used when making the
service call
-d <--debug> : enable debug logging
-g GROUPS : add user to group(s)
-h : print out this message
-k : create a key for the user
-p PATH : the path of the user, defaults to /
-u USERNAME : the name of the user
-v VERBOSE : print out the newly created user's arn
and guid

C:\AWS>_
```

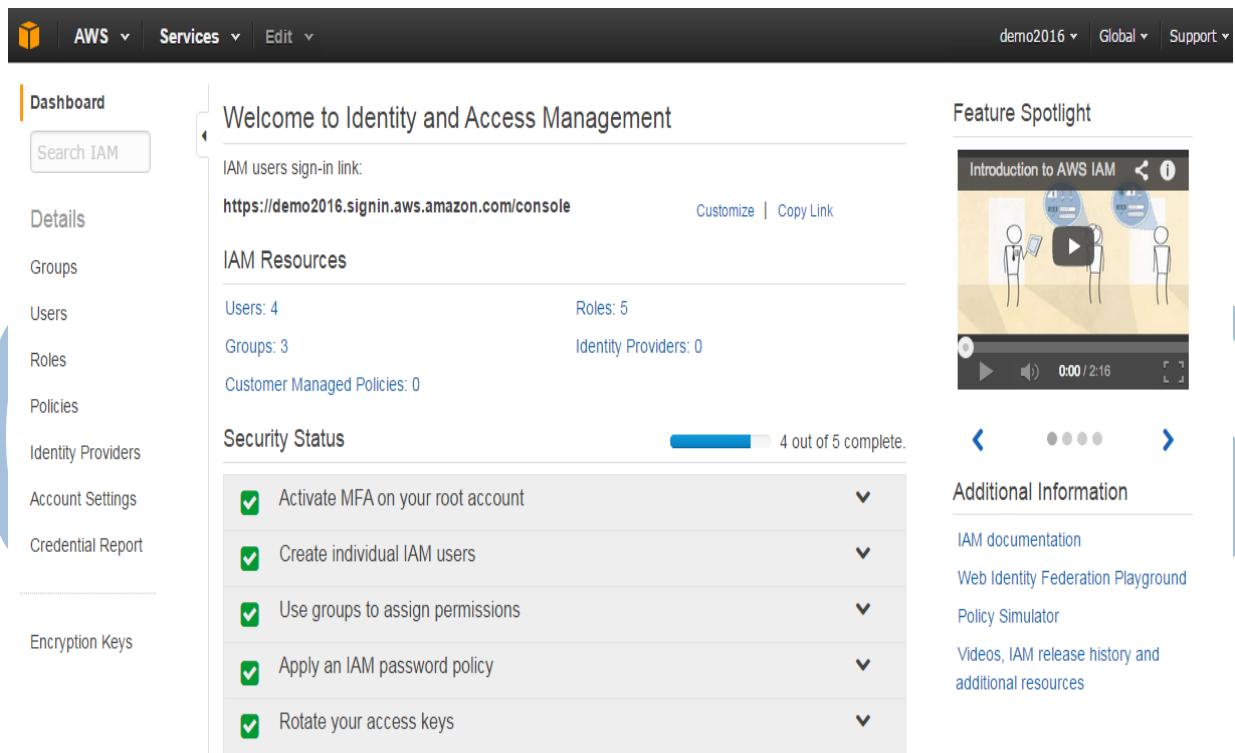
C3 SCHOOLS

13. Above output shows that your IAM command line tool is set correctly.

IAM How-to: Setup IAM Administrator Group

In this guide we will explain how to create an administrator group and grant the group the necessary permissions to access your AWS resources. IAM administrator group will have full access to all AWS services or products except AWS account section.

1. First login to your AWS account and enter the IAM console. There we see users, groups and others details.



The screenshot shows the AWS Identity and Access Management (IAM) console dashboard. The top navigation bar includes links for AWS, Services, Edit, demo2016, Global, and Support. On the left, a sidebar menu lists options: Dashboard (selected), Search IAM, Details, Groups, Users, Roles, Policies, Identity Providers, Account Settings, Credential Report, and Encryption Keys. The main content area displays the 'Welcome to Identity and Access Management' page. It features a 'IAM users sign-in link' (https://demo2016.signin.aws.amazon.com/console) with 'Customize' and 'Copy Link' buttons. Below this is the 'IAM Resources' section, which shows 4 Users, 5 Roles, 3 Groups, and 0 Identity Providers. The 'Customer Managed Policies' section shows 0 policies. The 'Security Status' section indicates 4 out of 5 items are complete. A list of five tasks with checkboxes is shown: 'Activate MFA on your root account', 'Create individual IAM users', 'Use groups to assign permissions', 'Apply an IAM password policy', and 'Rotate your access keys'. To the right, a 'Feature Spotlight' box displays a video thumbnail titled 'Introduction to AWS IAM' with a play button and a progress bar showing 0:00 / 2:16. Below the video are navigation arrows and a 'Additional Information' section with links to IAM documentation, Web Identity Federation Playground, Policy Simulator, and Videos, IAM release history and additional resources.

2. Go to **Groups** in dashboard Click on 'Create a New Group' to create new group for users



|| C3 SCHOOLS

AWS | Services | Edit | demo2016 | Global | Support

Create New Group Wizard

Step 1: Group Name

Step 2: Attach Policy

Step 3: Review

Set Group Name

Specify a group name. Group names can be edited any time.

Group Name:

mygroup

Example: Developers or ProjectAlpha

Maximum 128 characters

C3 SCHOOLS

C) Enter the name for administrator group. You can use only certain characters to name a group.

D) Click **Next Step** and select the policy. You need to use a policy to assign permissions to your administrator group. A policy is a document that formally states one or more permissions.

Create New Group Wizard | **Attach Policy**

Step 1: Group Name

Step 2: Attach Policy

Step 3: Review

Select one or more policies to attach. Each group can have up to 10 policies attached.

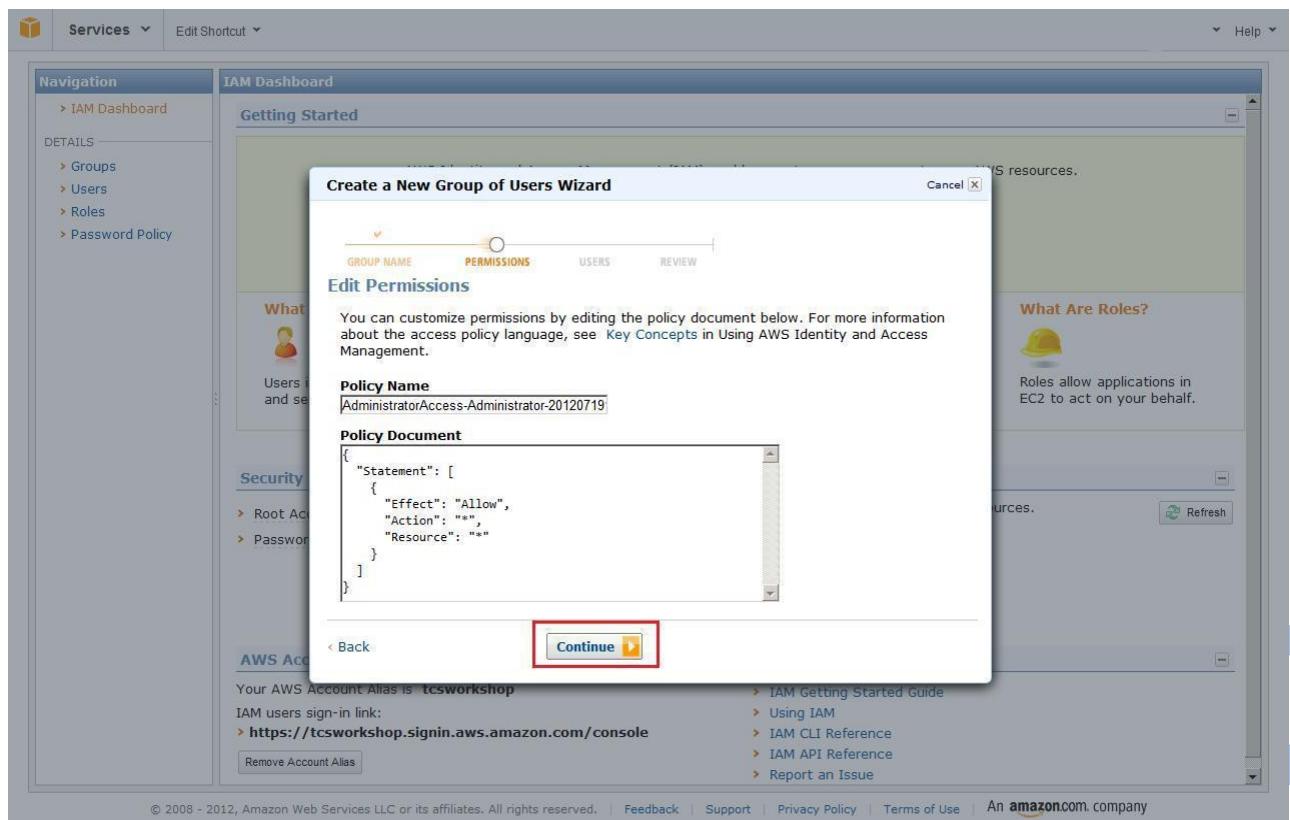
Filter: Policy Type ▾		Filter	Showing 204 results		
	Policy Name	Attached Entities	Creation Time	Edited Time	
<input type="checkbox"/>	AmazonS3FullAccess	3	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+...	
<input type="checkbox"/>	AdministratorAccess	2	2015-02-07 00:09 UTC+0530	2015-02-07 00:09 UTC+...	
<input type="checkbox"/>	AWSElasticBeanstalkEnhanc...	1	2016-02-09 04:47 UTC+0530	2016-08-23 01:58 UTC+...	
<input type="checkbox"/>	AWSElasticBeanstalkMulti...	1	2016-02-09 04:45 UTC+0530	2016-06-07 05:15 UTC+...	
<input type="checkbox"/>	AWSElasticBeanstalkService	1	2016-04-12 01:57 UTC+0530	2016-05-13 05:37 UTC+...	
<input type="checkbox"/>	AWSElasticBeanstalkWebTier	1	2016-02-09 04:38 UTC+0530	2016-03-08 05:05 UTC+...	
<input type="checkbox"/>	AWSElasticBeanstalkWorke...	1	2016-02-09 04:42 UTC+0530	2016-03-08 05:08 UTC+...	
<input type="checkbox"/>	CloudWatchActionsEC2Acc...	1	2015-07-07 05:30 UTC+0530	2015-07-07 05:30 UTC+...	
<input type="checkbox"/>	AmazonAPIGatewayAdmini...	0	2015-07-09 23:04 UTC+0530	2015-07-09 23:04 UTC+...	
<input type="checkbox"/>	AmazonAPIGatewayInvoke...	0	2015-07-09 23:06 UTC+0530	2015-07-09 23:06 UTC+...	

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

4. IAM provides several policy templates you can use to automatically assign permissions to the groups you create.

5. If you want to create your own policy or upload custom policy, select custom policy option. In this guide we selected default 'Administrator' It gives the 'administrator Access' group policy permission. to access all account resources, except your AWS account information.

7. On the next page you can modify the template of policy.



The screenshot shows the AWS IAM Dashboard with the 'Create a New Group of Users Wizard' dialog box open. The dialog has four tabs: GROUP NAME, PERMISSIONS, USERS, and REVIEW. The 'PERMISSIONS' tab is selected, showing a JSON policy document:

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

The 'Continue' button at the bottom of the dialog is highlighted with a red box. The background shows the IAM Dashboard with a sidebar containing 'Navigation' and 'DETAILS' sections, and a central area with 'Getting Started' and 'Edit Permissions' sections. A modal window titled 'What Are Roles?' is also visible in the background.



|| C3 SCHOOLS

8. If you do not want to modify the policy, press the 'Continue' button. The admin group will create

C3 SCHOOLS

9. Next, Go to Users Option to add users to the new admin group. These users will be created for IAM and since they are part of administrator group they will inherit the administrator group policy.

Dashboard

Search IAM

Details

Groups

Users

Roles

Policies

Identity Providers

Account Settings

Credential Report

Encryption Keys

Create New Users User Actions ▾

Filter Showing 4 results

User Name	Groups	Password	Password Last Used	Access Keys	Creation Time
MohaN	1	✓	2016-09-20 12:26 UTC+0530	1 active	2016-07-19 14:48 U...
RaVi	1	✓	2016-09-20 20:03 UTC+0530	1 active	2016-07-21 13:21 U...
test	1		N/A	1 active	2016-09-07 08:45 U...
user1	1	✓	Never	1 active	2016-09-17 08:31 U...

Create User

Enter User Names:

1.

2.

3.

4.

5.

Maximum 64 characters each

Generate an access key for each user

Users need access keys to make secure REST or Query protocol requests to AWS service APIs.

For users who need access to the AWS Management Console, create a password in the Users panel after completing this wizard.



10. Select the option to generate access key for the users. Access key is very important as if you

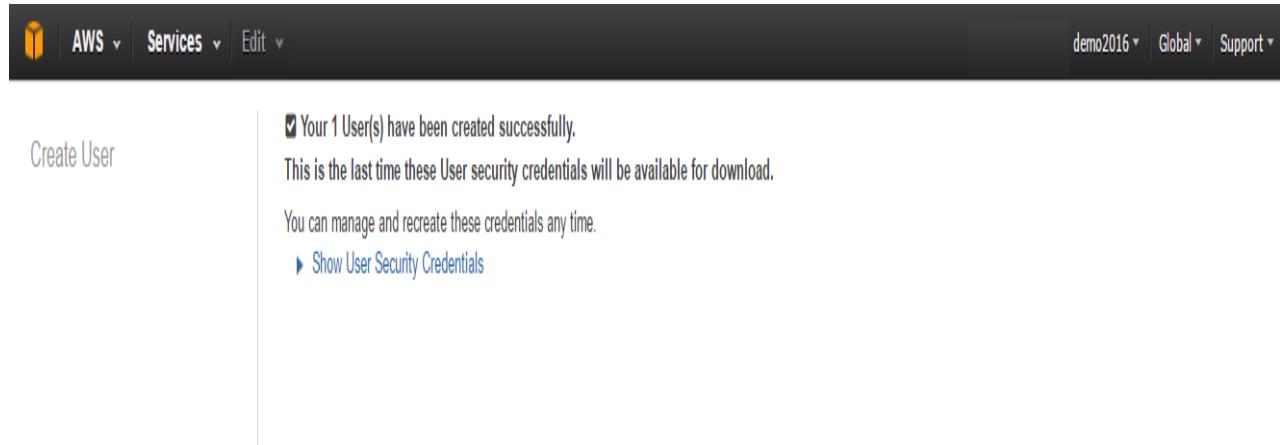
want to work with AWS IAM API's or use third party tools to work with access key and secret access keys.

11. If you want your IAM users to access AWS through AWS console, you would need passwords for them. Add existing users through ‘Add Existing Users’.

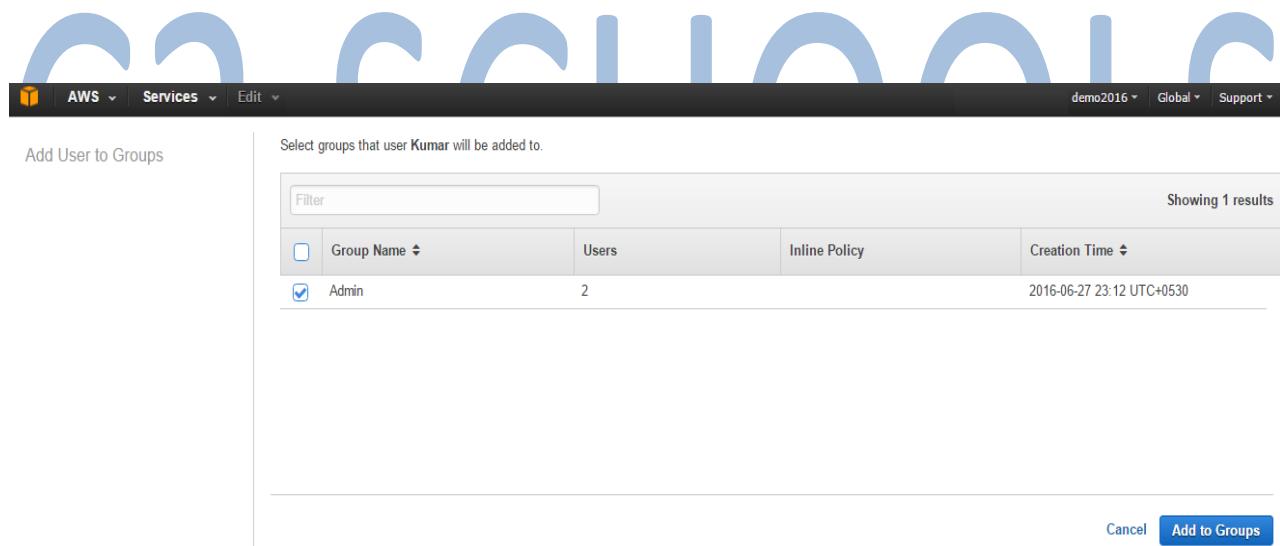
12. Review all the details you have provided and press **Finish**.

C3 SCHOOLS

13. Once all data is created it will show the success message page. In this part we will get the access key and secret access keys of user. If you press 'Show User Security Credentials', it will show the acc of user in same page.



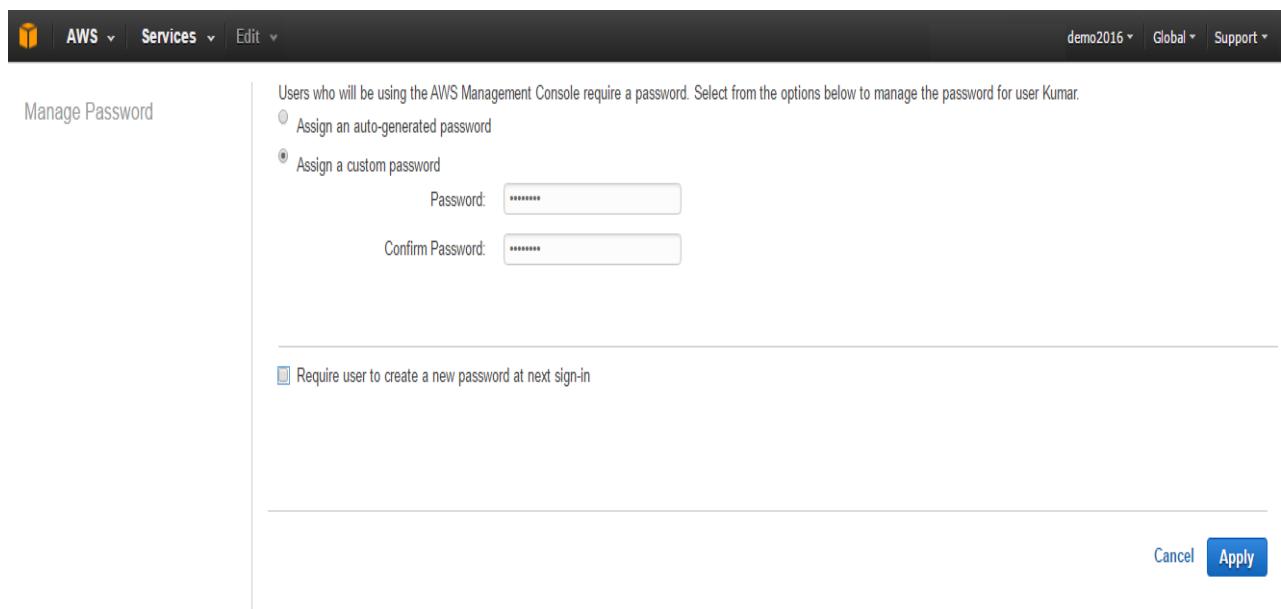
Your 1 User(s) have been created successfully.
This is the last time these User security credentials will be available for download.
You can manage and recreate these credentials any time.
[Show User Security Credentials](#)



Select groups that user Kumar will be added to.

Group Name	Users	Inline Policy	Creation Time
Admin	2		2016-06-27 23:12 UTC+0530

Add to Groups



The screenshot shows the 'Manage Password' section for a user named 'Kumar'. It includes fields for entering a custom password and confirming it, along with a checkbox for requiring a new password at next sign-in. At the bottom right are 'Cancel' and 'Apply' buttons.

14. If you press 'Download Credentials', it will generate csv file which secret access keys. Once you save the credentials, press **Close Window**.

15. Go to groups section in IAM dashboard console. It will list the new created group and user attached to group.

AWS Services Edit demo2016 Global Support

Dashboard Search IAM

Details Groups Users Roles Policies Identity Providers Account Settings Credential Report

Encryption Keys

IAM > Groups > Admin

Summary

Group ARN: arn:aws:iam::076828422820:group/Admin

Users (in this group): 3

Path: /

Creation Time: 2016-06-27 23:12 UTC+0530

Users Permissions Access Advisor

This view shows all users in this group: 3 Users

Remove Users from Group Add Users to Group

User	Actions
Kumar	Remove User from Group
RaVi	Remove User from Group
MohaN	Remove User from Group

16. To run the command line API tool, setup IAM command line API tool a Tool in Windows".
17. Run command **iam-group create -g admin Grp**, this will create group. called 'admin'
18. Run command **iam-grouplistbypath**, to check the created group.

Administrator: C:\Windows\system32\cmd.exe

```
C:\AWS\IAMCli-1.5.0\bin>iam-groupcreate -g adminGrp
C:\AWS\IAMCli-1.5.0\bin>iam-grouplistbypath
arn:aws:iam::[REDACTED]:group/adminGrp
arn:aws:iam::[REDACTED]:group/Administrator
arn:aws:iam::[REDACTED]:group/Admins
IsTruncated: false
```

19. Now to assign a policy to group, create a policy text file. E.g. AdminPolicy.txt contains following

{

```
"Statement":{
```

```
    "Effect":"Allow",
```

```
    "Action":"*",
```

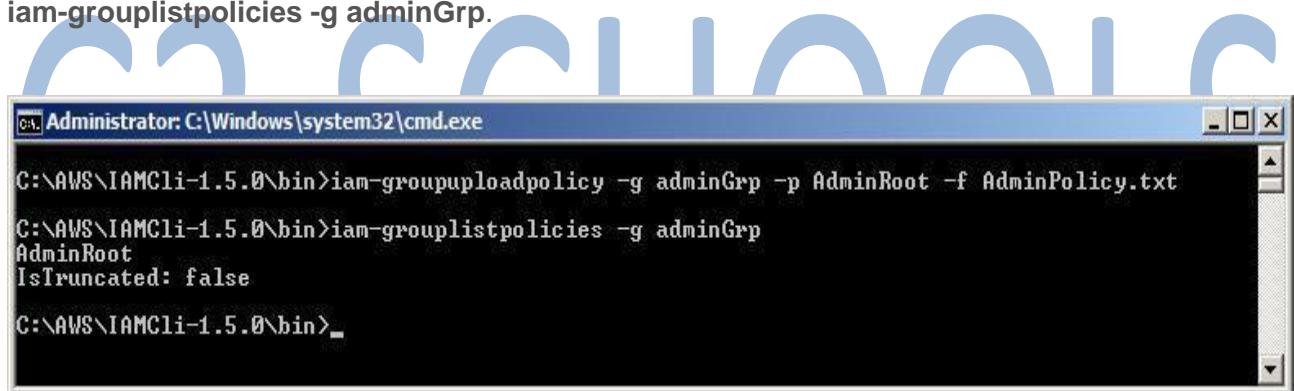
```
    "Resource":"*"
```

```
}
```

20. Run command **iam-groupuploadpolicy -g adminGrp -p AdminRoot -f AdminPolicy.txt**.

21. Type below command to confirm that admin policy is attached

```
iam-grouplistpolicies -g adminGrp.
```



```
C:\Administrator: C:\Windows\system32\cmd.exe
C:\AWS\IAMCli-1.5.0\bin>iam-groupuploadpolicy -g adminGrp -p AdminRoot -f AdminPolicy.txt
C:\AWS\IAMCli-1.5.0\bin>iam-grouplistpolicies -g adminGrp
AdminRoot
IsTruncated: false
C:\AWS\IAMCli-1.5.0\bin>
```

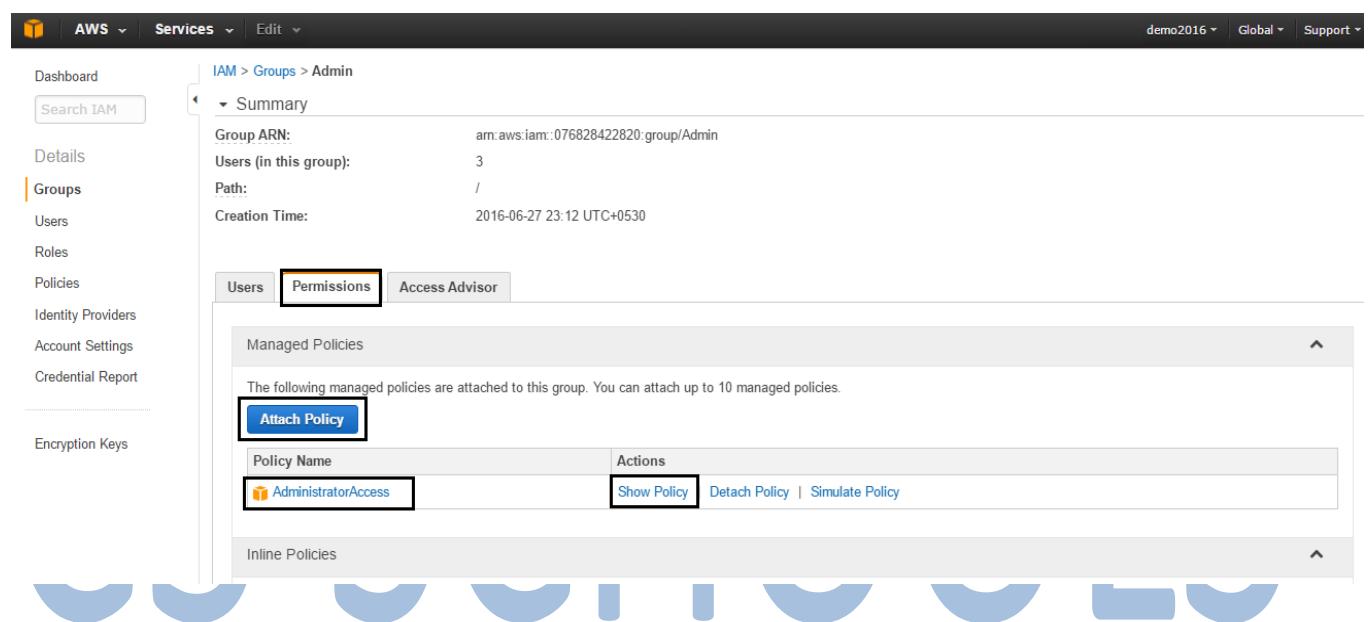
How to Manage IAM Security Policies

In this guide we will describe how to define, create Policy and is attach a policy used to grant access permission to user, group or role so to AWS resources based on specific rules. To give a particular IAM entity permission, you need to write a policy according to the access policy language IAM uses and then attach the policy to the related AWS entity. In case of a group the group users' inherits the you can group attach more than one policy to a group or user.

Let's start with setting a policy for a group:

E)Login to your AWS account and enter the IAM console.

F)Select the Group from left navigation *Permissions* menu. In' the admin group as shown select below'.



The screenshot shows the AWS IAM Groups page for the 'Admin' group. The left sidebar is collapsed, and the main content area displays the 'Summary' tab for the 'Admin' group. The summary includes the following details:

- Group ARN: arn:aws:iam::076828422820:group/Admin
- Users (in this group): 3
- Path: /
- Creation Time: 2016-06-27 23:12 UTC+0530

Below the summary, there are three tabs: 'Users' (disabled), 'Permissions' (selected), and 'Access Advisor'. The 'Permissions' tab shows the 'Managed Policies' section, which lists the 'AdministratorAccess' policy attached to the group. The 'AdministratorAccess' policy is highlighted with a red box. The 'Actions' column for this policy includes 'Show Policy' (also highlighted with a red box) and 'Detach Policy | Simulate Policy'.

3. The permission tab will list the existing policies attached to Group

AWS Services Edit demo2016 Global Support

Attach Policy

Attach Policy

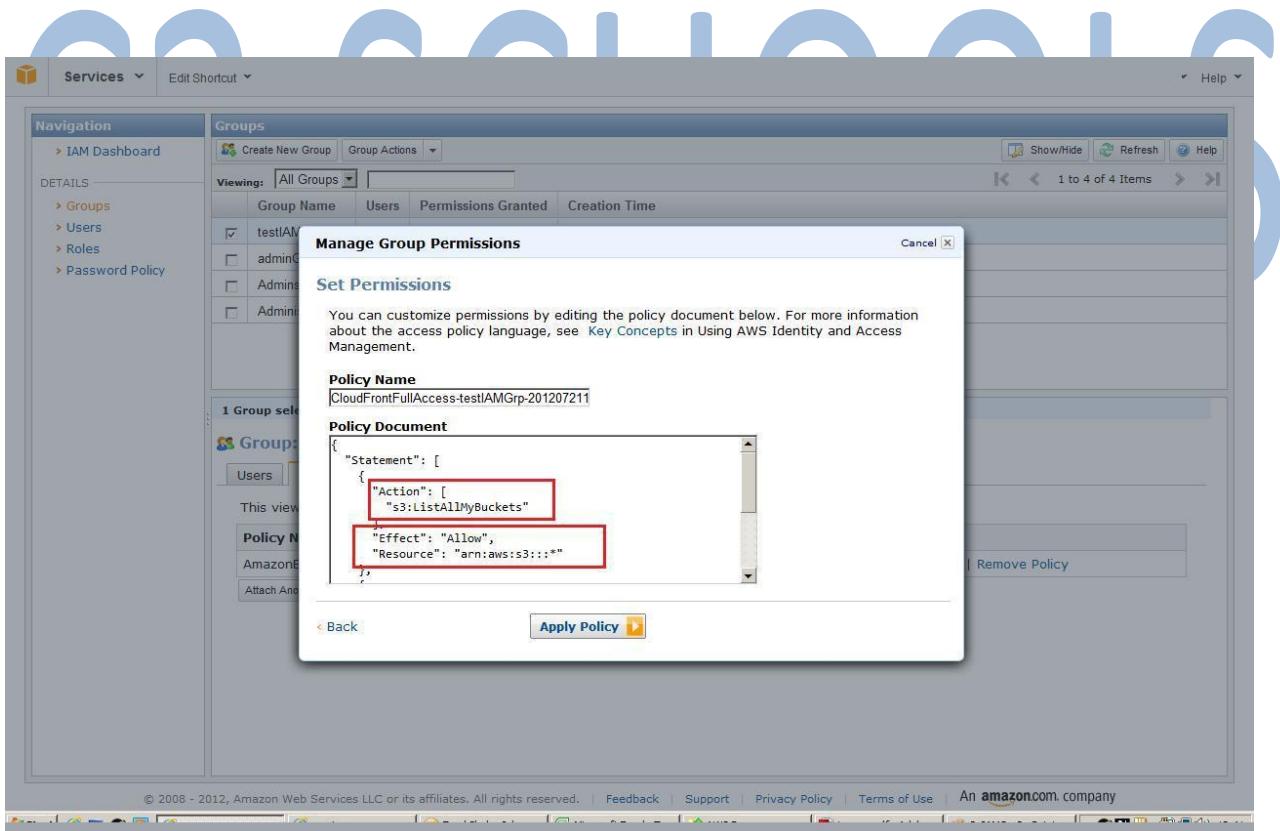
Select one or more policies to attach. Each group can have up to 10 policies attached.

	Policy Name	Attached Entities	Creation Time	Edited Time
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	0	2015-07-09 23:04 UTC+0530	2015-07-09 23:04 UTC+0530
<input type="checkbox"/>	AmazonAPIGatewayInvokeFullAccess	0	2015-07-09 23:06 UTC+0530	2015-07-09 23:06 UTC+0530
<input type="checkbox"/>	AmazonAPIGatewayPushToCloud...	0	2015-11-12 05:11 UTC+0530	2015-11-12 05:11 UTC+0530
<input type="checkbox"/>	AmazonAppStreamFullAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input type="checkbox"/>	AmazonAppStreamReadOnlyAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input type="checkbox"/>	AmazonCognitoDeveloperAuthentic...	0	2015-03-24 22:52 UTC+0530	2015-03-24 22:52 UTC+0530
<input type="checkbox"/>	AmazonCognitoPowerUser	0	2015-03-24 22:44 UTC+0530	2016-06-02 22:27 UTC+0530
<input type="checkbox"/>	AmazonCognitoReadOnly	0	2015-03-24 22:36 UTC+0530	2016-06-02 23:00 UTC+0530
<input type="checkbox"/>	AmazonDMSCloudWatchLogsRole	0	2016-01-08 05:14 UTC+0530	2016-01-08 05:14 UTC+0530
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	0	2016-04-20 22:35 UTC+0530	2016-04-20 22:35 UTC+0530

Showing 206 results

Cancel Attach Policy

4. Select the entity for which you want to grant access. In this example Access', this will list the JSON policy language. Definition Modify the policy as in needed



Services Edit Shortcut Help

Navigation > IAM Dashboard

Groups

Create New Group Group Actions Viewing: All Groups

Group Name Users Permissions Granted Creation Time

1 Group selected

Group Name

Group Actions

Viewing: All Groups

Group Name

Users

Permissions Granted

Creation Time

1 to 4 of 4 Items

Cancel

Manage Group Permissions

Set Permissions

You can customize permissions by editing the policy document below. For more information about the access policy language, see Key Concepts in Using AWS Identity and Access Management.

Policy Name CloudFrontFullAccess-testAMGrp-201207211

Policy Document

```
{
  "Statement": [
    {
      "Action": [
        "s3>ListAllMyBuckets"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::/*"
    }
  ]
}
```

Back Apply Policy

© 2008 - 2012, Amazon Web Services LLC or its affiliates. All rights reserved. | Feedback | Support | Privacy Policy | Terms of Use | An amazon.com company



|| C3 SCHOOLS

C3 SCHOOLS



|| C3 SCHOOLS

5. Select Apply policy once your policy is defined.

The screenshot shows the AWS IAM Groups Admin interface. On the left sidebar, 'Groups' is selected. In the main area, under the 'Permissions' tab, there is a table showing two attached managed policies:

Policy Name	Actions
CloudFrontFullAccess	Show Policy Detach Policy Simulate Policy
AdministratorAccess	Show Policy Detach Policy Simulate Policy

6. This will add another policy to group. As shown above, the Group testIAMGrp has now two policies. One for EC2 Read and one for Cloud front full access.
7. Now we will modify the policy for a user. A user normally inherits all the policy of the group it belongs to. As shown below, the user testIAMUser1, inherits group policy.



|| C3 SCHOOLS

AWS Services Edit demo2016 Global Support

Dashboard

Search IAM

Details

Groups

Users

Roles

Policies

Identity Providers

Account Settings

Credential Report

Encryption Keys

▼ Summary

User ARN: am:aws:iam::076828422820:user/RaVi

Has Password: Yes

Groups (for this user): 1

Path: /

Creation Time: 2016-07-21 13:21 UTC+0530

Groups Permissions Security Credentials Access Advisor

Managed Policies

There are no managed policies attached to this user.

Attach Policy

Group Policies

This view shows policies that are attached to groups that this user is in.

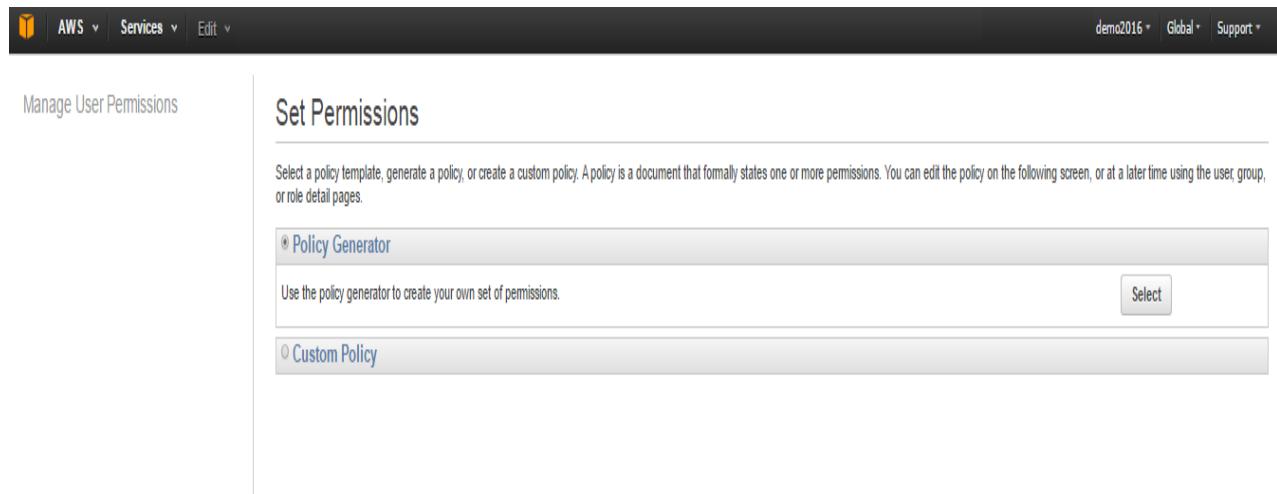
Policy Name	Group Name	Actions
CloudFrontFullAccess	Admin	Show Policy
AdministratorAccess	Admin	Show Policy

Inline Policies

W J U I T V V L J

8. We can assign the individual policy to a user. Select ‘Attach User Policy’ from ‘Permis a user.

9. It will ask to select the policy.



The screenshot shows the 'Set Permissions' page in the AWS IAM console. The top navigation bar includes 'AWS', 'Services', 'Edit', 'demo2016', 'Global', and 'Support'. On the left, there's a sidebar with 'Manage User Permissions'. The main area is titled 'Set Permissions' and contains instructions: 'Select a policy template, generate a policy, or create a custom policy. A policy is a document that formally states one or more permissions. You can edit the policy on the following screen, or at a later time using the user, group, or role detail pages.' Below this, two options are listed: 'Policy Generator' (selected, indicated by a radio button) and 'Custom Policy'. A 'Select' button is located next to the 'Policy Generator' section.

10. For the user we will use ‘Policy Generator’ instead of selecting from also attach your custom.

12. Select the AWS service for which you want to grant access. We have and ‘Associate Address’ policy for this user.

C3 SCHOOLS

AWS Services Edit demo2016 Global Support

Manage User Permissions

Edit Permissions

The policy generator enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see [Overview of Policies](#) in Using AWS Identity and Access Management.

Effect Allow Deny

AWS Service Amazon EC2

Actions 2 Action(s) Selected

All Actions (*)
AcceptVpcPeeringConnection
 AllocateAddress
 AllocateHosts
AllocatePrivateIpAddressRange

Amazon Resource Name (ARN)

Cancel Previous **Next Step**



13. Once you select the actions, press 'Add Statement'.

AWS Services Edit demo2016 Global Support

Manage User Permissions

Edit Permissions

The policy generator enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see Overview of Policies in Using AWS Identity and Access Management.

Effect: Allow Deny

AWS Service: Amazon EC2

Actions: 2 Action(s) Selected

Amazon Resource Name (ARN):

Add Conditions (optional)

Add Statement

Cancel Previous Next Step

14. It will add the two actions to the list of policies. As shown below. We will also select two more policies ‘Attach Volume’ & ‘Bundle Volume’.

AWS Services Edit demo2016 Global Support

Manage User Permissions

Edit Permissions

The policy generator enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see Overview of Policies in Using AWS Identity and Access Management.

Effect: Allow Deny

AWS Service: Amazon EC2

Actions: 2 Action(s) Selected

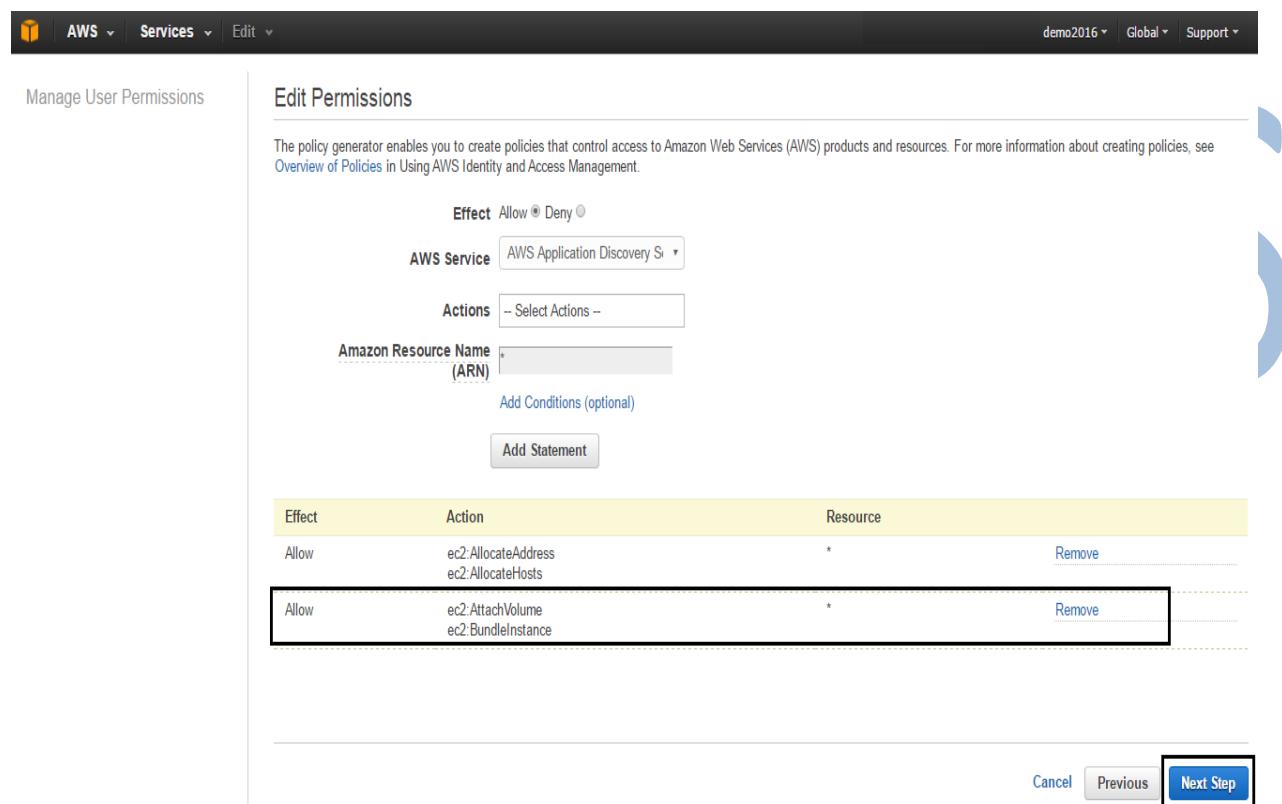
Amazon Resource Name (ARN):

AttachNetworkInterface
 AttachVolume
 AttachVpnGateway
 AuthorizeSecurityGroupEgress
 AuthorizeSecurityGroupIngress
 BundleInstance

Effect	Action	Resource	
Allow	ec2:AllocateAddress ec2:AllocateHosts	*	Remove

Cancel Previous Next Step

15. Once you select new actions add them to statement, Press **Continue**. It will list the policy definition. You can modify the policy in JSON language.



The screenshot shows the AWS IAM 'Edit Permissions' interface. At the top, there's a navigation bar with 'AWS Services' and 'Edit'. Below it, the main title is 'Edit Permissions'. A descriptive note says: 'The policy generator enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see Overview of Policies in Using AWS Identity and Access Management.' There are fields for 'Effect' (set to 'Allow'), 'AWS Service' (set to 'AWS Application Discovery Service'), 'Actions' (button to 'Select Actions'), and 'Amazon Resource Name (ARN)' (input field). Below these are buttons for 'Add Conditions (optional)' and 'Add Statement'. A table displays two policy statements:

Effect	Action	Resource	
Allow	ec2:AllocateAddress ec2:AllocateHosts	*	Remove
Allow	ec2:AttachVolume ec2:BundleInstance	*	Remove

At the bottom right, there are buttons for 'Cancel', 'Previous', and 'Next Step' (which is highlighted with a blue box).

16. Once you apply policy it will be added to user.



|| C3 SCHOOLS

AWS Services Edit demo2016 Global Support

Manage User Permissions

Review Policy

Customize permissions by editing the following policy document. For more information about the access policy language, see [Overview of Policies](#) in the [Using IAM](#) guide. To test the effects of this policy before applying your changes, use the [IAM Policy Simulator](#).

Policy Name

policygen-Ravi-201609221311

Policy Document

```
1 * {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Sid": "Stmt1474529674000",
6             "Effect": "Allow",
7             "Action": [
8                 "ec2:AllocateAddress",
9                 "ec2:AllocateHosts"
10            ],
11            "Resource": [
12                "*"
13            ]
14        },
15        {
16            "Sid": "Stmt1474529712000",
17            "Effect": "Allow",
18            "Action": [
19                "ec2:AttachVolume",
20                "ec2:BundleInstance"
21            ],
22            "Resource": [
23                "*"
24            ]
25        }
26    ]
27}
```

Use autoformatting for policy editing

Cancel Validate Policy Apply Policy

17. As shown below, the user has group policy as well individual policy. Press show policy to view the policy.

AWS Services Edit demo2016 Global Support

Dashboard

IAM > Users > Kumar

Summary

Details Groups **Users** Roles Policies Identity Providers Account Settings Credential Report

Encryption Keys

Managed Policies

There are no managed policies attached to this user.

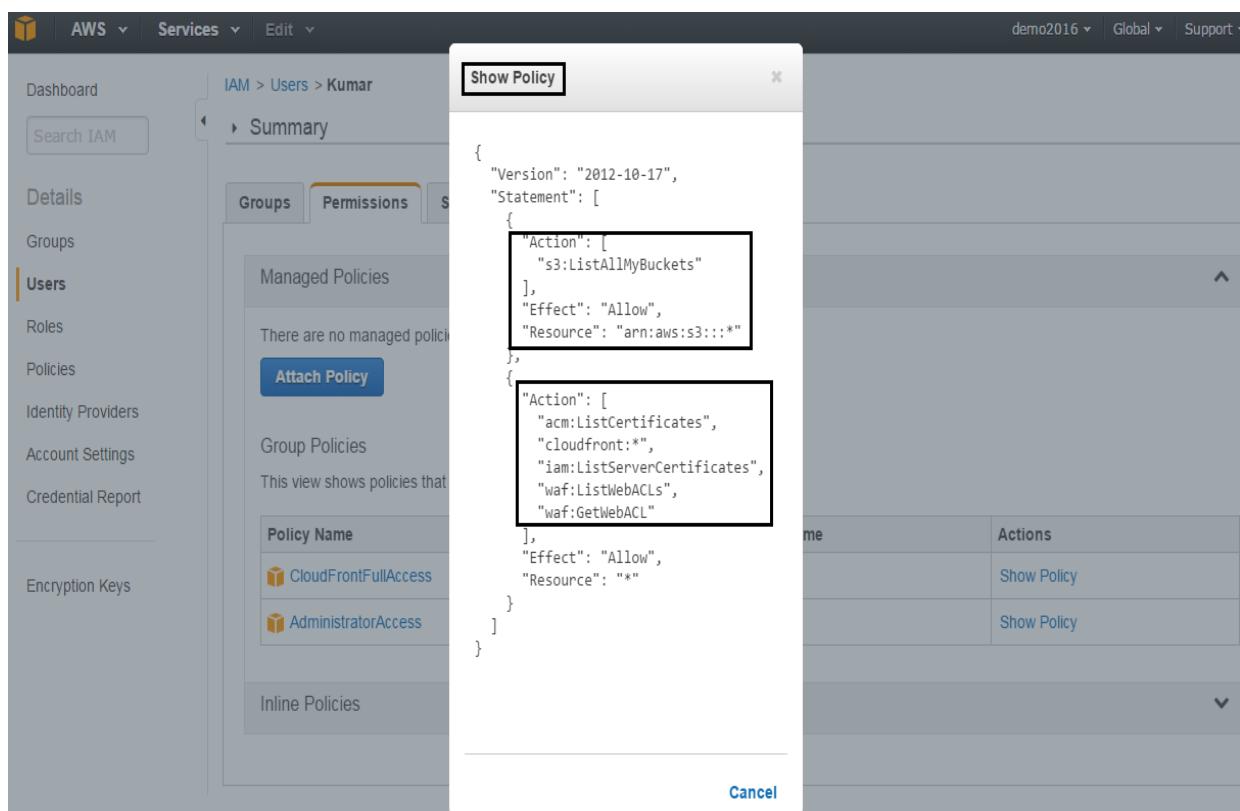
Attach Policy

Group Policies

This view shows policies that are attached to groups that this user is in.

Policy Name	Group Name	Actions
CloudFrontFullAccess	Admin	Show Policy
AdministratorAccess	Admin	Show Policy

Inline Policies

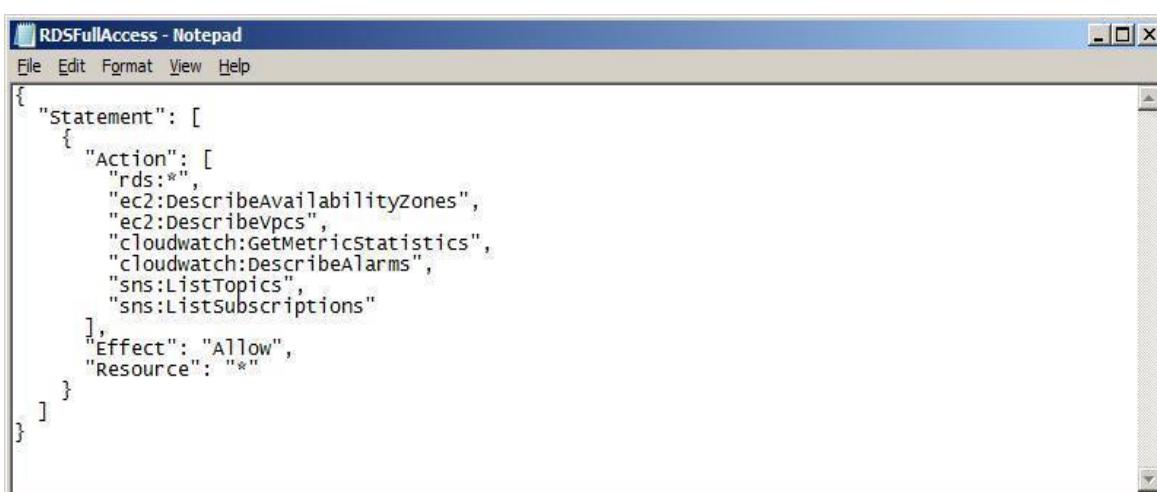


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3>ListAllMyBuckets"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::/*"
    },
    {
      "Action": [
        "acm>ListCertificates",
        "cloudfront:*",
        "iam>ListServerCertificates",
        "waf>ListWebACLs",
        "waf:GetWebACL"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

C3 SCHOOLS

18. The above displays the policy we defined in JSON language.**In the next steps we will attach policy through command line.**

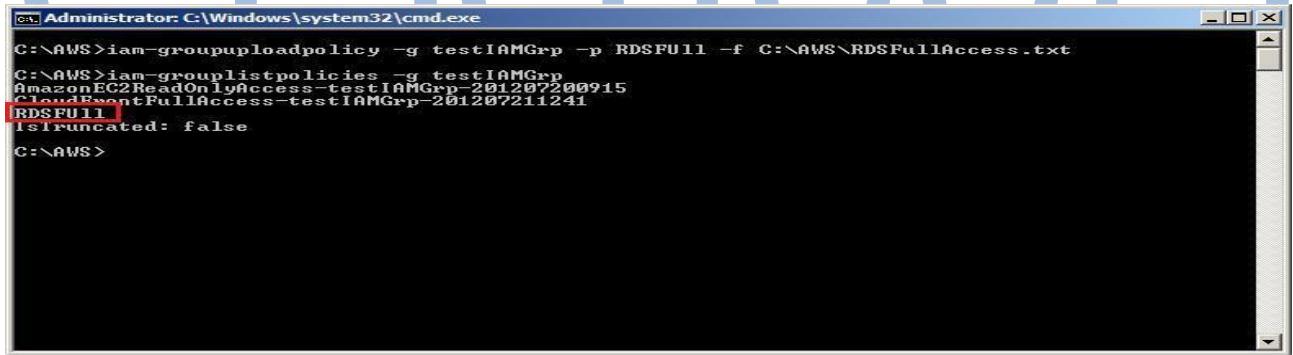
19. We need to create a policy in JSON format. We have defined the policy for full RDS access in JSON format. Name the file as RDSFullAccess.txt



```
{
  "Statement": [
    {
      "Action": [
        "rds:*",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarms",
        "sns>ListTopics",
        "sns>ListSubscriptions"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

20. Run the command **iam-group upload policy -g test IAM Grp -p RDS FULL -f C:\AWS\RDSFullAccess.txt**. This will add the policy defined in RDSFullAccess.txt to group test IAM Grp.

List the policy with **iam-grouplistpolicies -g testIAMGrp**.

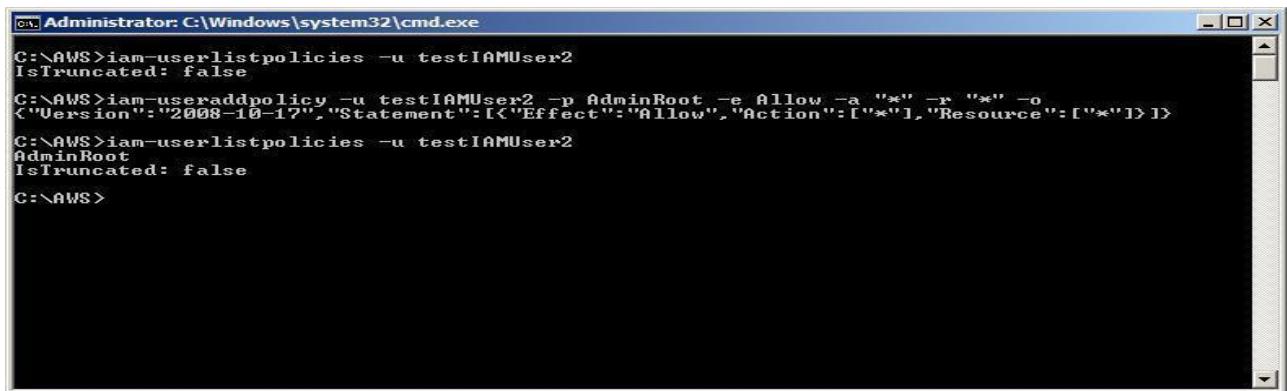


```
Administrator: C:\Windows\system32\cmd.exe
C:\AWS>iam-groupuploadpolicy -g testIAMGrp -p RDSFULL -f C:\AWS\RDSFullAccess.txt
C:\AWS>iam-grouplistpolicies -g testIAMGrp
AmazonEC2ReadOnlyAccess-testIAMGrp-2012072200915
CloudFrontFullAccess-testIAMGrp-201207211241
RDSFULL
IsTruncated: false
C:\AWS>
```

iv. Add policy to individual user. Let's define commandpolicyline only instead of creating a separate file.

```
iam-useraddpolicy -u testIAMUser2 -p AdminRoot -e Allow -a "*" -r "*" -o.
```

- v. List the policy assigned to user through **iam-userlistpolicies -u testIAMUser2**.



```
C:\Administrator:C:\Windows\system32\cmd.exe
C:>AWS>iam-userlistpolicies -u testIAMUser2
IsTruncated: false
C:>AWS>iam-useraddpolicy -u testIAMUser2 -p AdminRoot -e Allow -a "*" -r "*" -o
<"Version":"2008-10-17","Statement": [{"Effect": "Allow", "Action": ["*"], "Resource": ["*"]}]>
C:>AWS>iam-userlistpolicies -u testIAMUser2
AdminRoot
IsTruncated: false
C:>AWS>
```

C3 SCHOOLS

How to Create or Modify IAM User Group

In this guide we will show you how to create and update IAM users and groups including how to configure and attach a new policy to an existing IAM group. In this guide we will create the group 'testIAMGrp' without any policy at first.

1. Login to your AWS account console and enter the IAM section.

AWS Services Edit demo2016 Global Support

Dashboard

Search IAM

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://demo2016.signin.aws.amazon.com/console>

Customize | Copy Link

IAM Resources

Users: 3 Roles: 0

Groups: 1 Identity Providers: 0

Customer Managed Policies: 1

Security Status

5 out of 5 complete.

- Activate MFA on your root account
- Create individual IAM users
- Use groups to assign permissions
- Apply an IAM password policy
- Rotate your access keys

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

2. Click on 'Create a New Group of Users'. Enter group name then click next step

AWS Services Edit demo2016 Global Support

Create New Group Wizard

Step 1: Group Name

Step 2: Attach Policy

Step 3: Review

Set Group Name

Specify a group name. Group names can be edited any time.

Group Name: mygroup

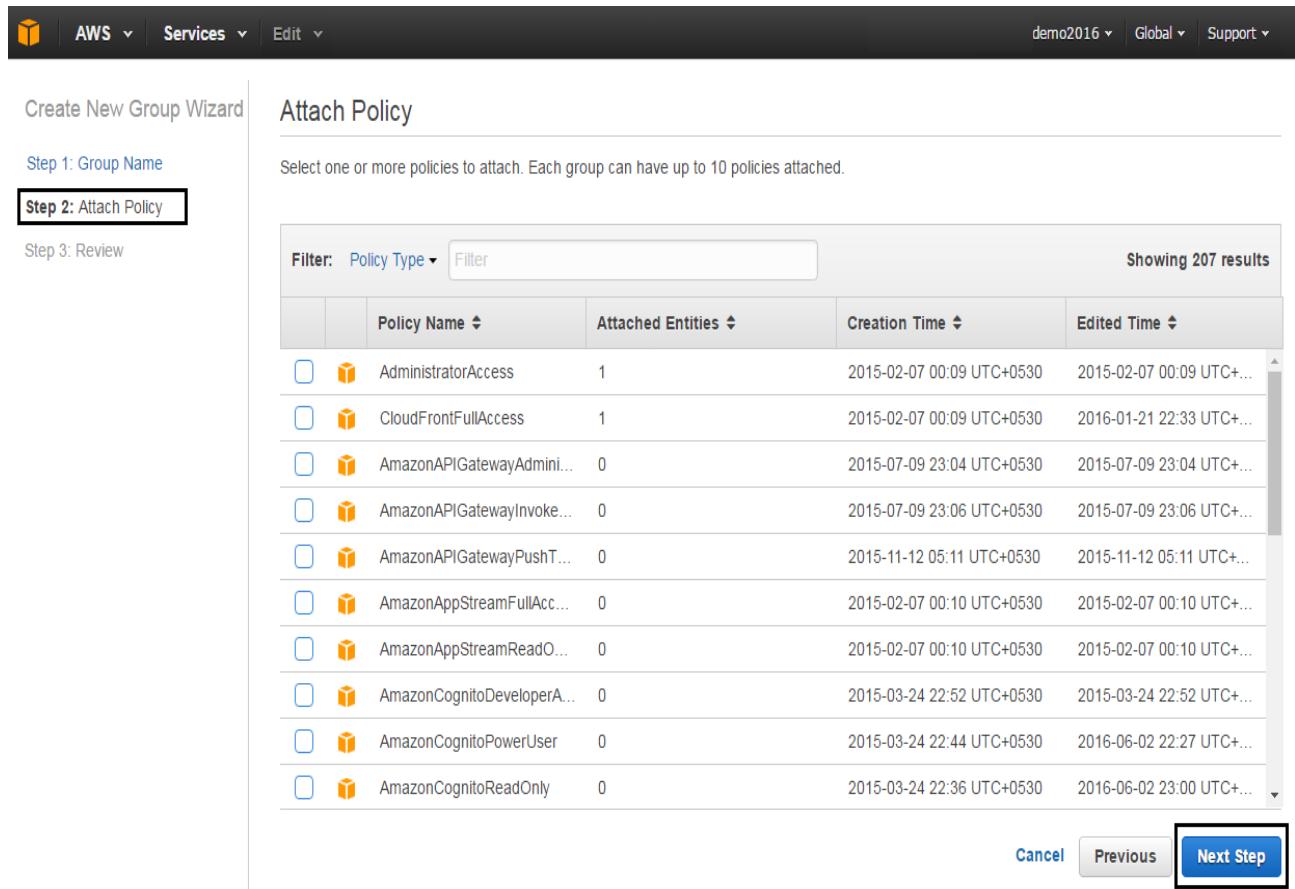
Example: Developers or ProjectAlpha

Maximum 128 characters

Cancel **Next Step**

3. Enter the name for the new IAM group. Note that you can use only certain amount of characters for the group name.

4. Click 'Continue' will select forward the wanted you policy to. The policy document contains several users' permission rules that will be assigned to your group.



The screenshot shows the 'Create New Group Wizard' in progress, specifically Step 2: Attach Policy. The interface includes a navigation bar with 'AWS', 'Services', 'Edit', and user information 'demo2016', 'Global', and 'Support'. On the left, a sidebar lists 'Step 1: Group Name', 'Step 2: Attach Policy' (which is highlighted with a black border), and 'Step 3: Review'. The main content area is titled 'Attach Policy' and contains a message: 'Select one or more policies to attach. Each group can have up to 10 policies attached.' Below this is a table titled 'Showing 207 results' with columns: 'Policy Name', 'Attached Entities', 'Creation Time', and 'Edited Time'. The table lists various AWS policies such as 'AdministratorAccess', 'CloudFrontFullAccess', and 'AmazonAPIGatewayAdmin...'. At the bottom right of the table are 'Cancel', 'Previous', and 'Next Step' buttons, with 'Next Step' being highlighted with a blue background.

	Policy Name	Attached Entities	Creation Time	Edited Time
<input type="checkbox"/>	AdministratorAccess	1	2015-02-07 00:09 UTC+0530	2015-02-07 00:09 UTC+...
<input type="checkbox"/>	CloudFrontFullAccess	1	2015-02-07 00:09 UTC+0530	2016-01-21 22:33 UTC+...
<input type="checkbox"/>	AmazonAPIGatewayAdmini...	0	2015-07-09 23:04 UTC+0530	2015-07-09 23:04 UTC+...
<input type="checkbox"/>	AmazonAPIGatewayInvoke...	0	2015-07-09 23:06 UTC+0530	2015-07-09 23:06 UTC+...
<input type="checkbox"/>	AmazonAPIGatewayPushT...	0	2015-11-12 05:11 UTC+0530	2015-11-12 05:11 UTC+...
<input type="checkbox"/>	AmazonAppStreamFullAcc...	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+...
<input type="checkbox"/>	AmazonAppStreamReadO...	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+...
<input type="checkbox"/>	AmazonCognitoDeveloperA...	0	2015-03-24 22:52 UTC+0530	2015-03-24 22:52 UTC+...
<input type="checkbox"/>	AmazonCognitoPowerUser	0	2015-03-24 22:44 UTC+0530	2016-06-02 22:27 UTC+...
<input type="checkbox"/>	AmazonCognitoReadOnly	0	2015-03-24 22:36 UTC+0530	2016-06-02 23:00 UTC+...

5. At first we will not assign any policy to the new group Press the next step 'Next Step'



|| C3 SCHOOLS

AWS | Services | Edit | demo2016 | Global | Support

Create New Group Wizard | Review

Step 1: Group Name | Step 2: Attach Policy | Step 3: Review

Review the following information, then click **Create Group** to proceed.

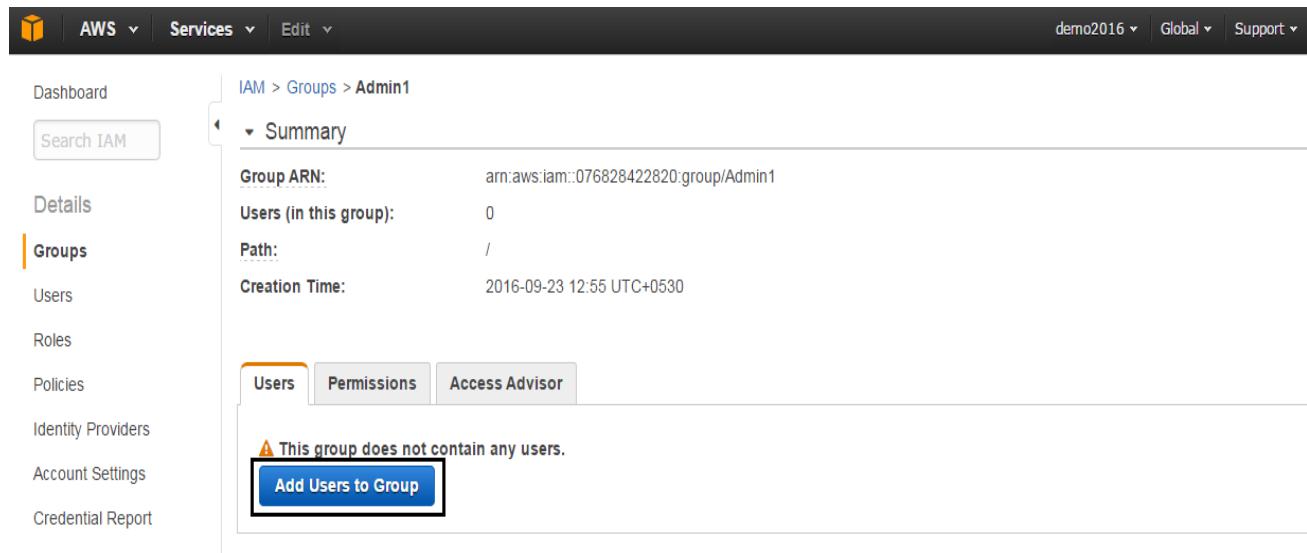
Group Name Admin1 | [Edit Group Name](#)

Policies | [Edit Policies](#)

[Cancel](#) | [Previous](#) | **Create Group**

C3 SCHOOLS

6. Add new or existing users to the new group. These users will be created for IAM and since they are part of testIAMGrp group they will inherit the group policy. Currently they will not have any access since no policy was assigned to the group.



IAM > Groups > Admin1

Summary

Group ARN: arn:aws:iam::076828422820:group/Admin1

Users (in this group): 0

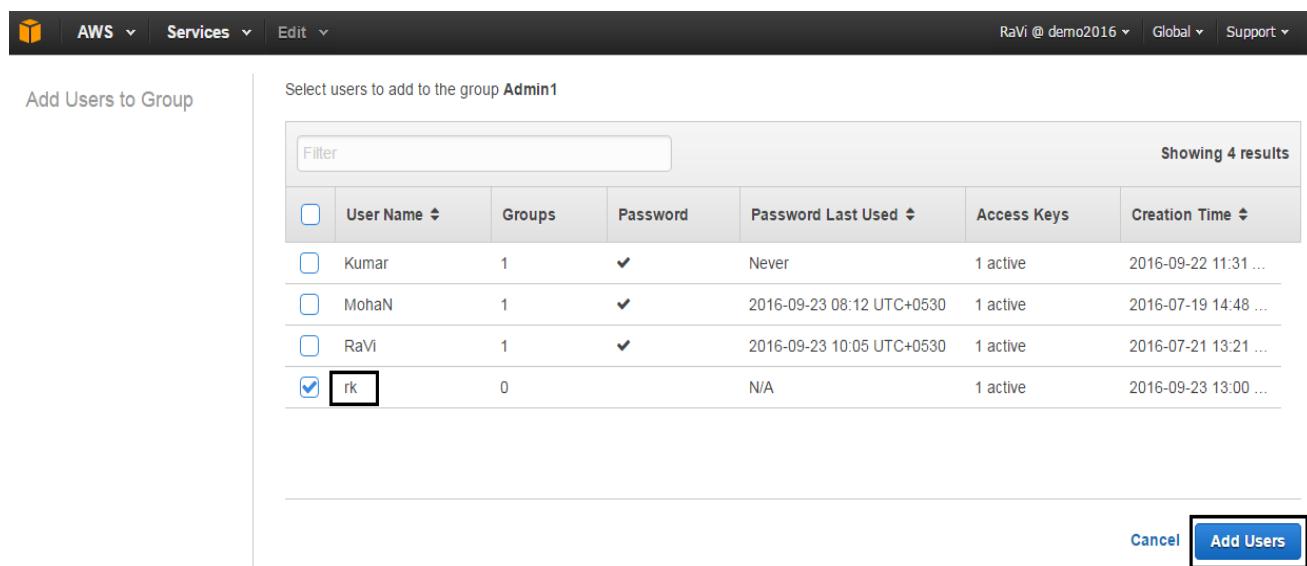
Path: /

Creation Time: 2016-09-23 12:55 UTC+0530

Users Permissions Access Advisor

Add Users to Group

7. Check the option to `Generate an access key for each user`. Access key enables you to work with AWS IAM APIs or use third party tools to work with AWS. Note that you can add existing users by clicking on the 'Add Existing Users' tab to view and select the relevant user



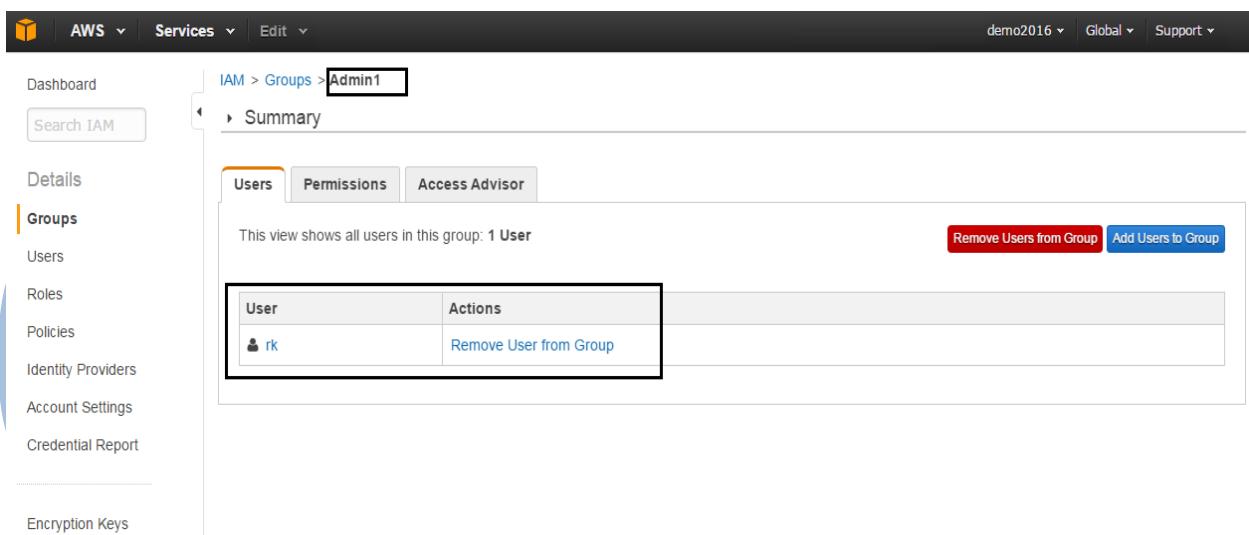
Select users to add to the group Admin1

User Name	Groups	Password	Password Last Used	Access Keys	Creation Time
Kumar	1	✓	Never	1 active	2016-09-22 11:31 ...
MohaN	1	✓	2016-09-23 08:12 UTC+0530	1 active	2016-07-19 14:48 ...
RaVi	1	✓	2016-09-23 10:05 UTC+0530	1 active	2016-07-21 13:21 ...
<input checked="" type="checkbox"/> rk	0		N/A	1 active	2016-09-23 13:00 ...

Add Users

8. If you want the newly created IAM users to access the AWS console, you might want to click on `Edit Users` and set passwords for them. You can also create new users in IAM.

9. The new IAM group created and users added to the group admin1



IAM > Groups > Admin1

Summary

Users Permissions Access Advisor

This view shows all users in this group: 1 User

User	Actions
rk	Remove User from Group

Remove Users from Group Add Users to Group

Details

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

11. Press to 'Show User Security Credentials', it will show the access user in dialog box. Note – Before closing the window we strongly suggest to copy and save the group keys for later use.

12. Pressing the 'Download Credentials', will generate csv file which will have secret access keys.

AWS Services Edit demo2016 Global Support

Dashboard IAM > Users > rk

Search IAM

Summary

Details Groups Security Credentials Access Advisor

Users

Access Keys

Use access keys to make secure REST or Query protocol requests to any AWS service API. For your protection, you should never share your secret keys with anyone. In addition, industry best practice recommends frequent key rotation. [Learn more about Access Keys](#)

Create Access Key

Access Key ID	Created	Last Used	Last Used Service	Last Used Region	Status	Actions
AKIAJHA7RU4LQFF3ITRA	2016-09-23 13:00 UTC+0530	N/A	N/A	N/A	Active	Make Inactive Delete

Sign-In Credentials

SSH keys for AWS CodeCommit

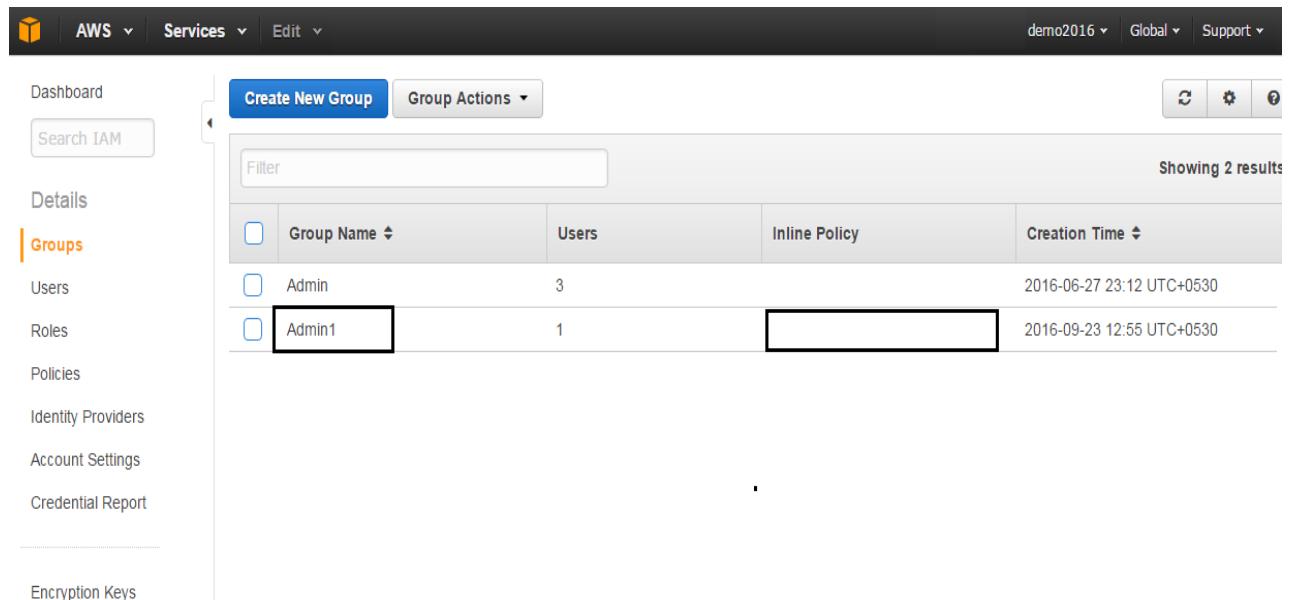
Feedback English © 2008 - 2016, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

credentials (1).csv Show all

13. Once you save the credentials, press 'Close Window'.

15. Click the left pane on the `Groups` item to view your and IAM the recent groups' new entries

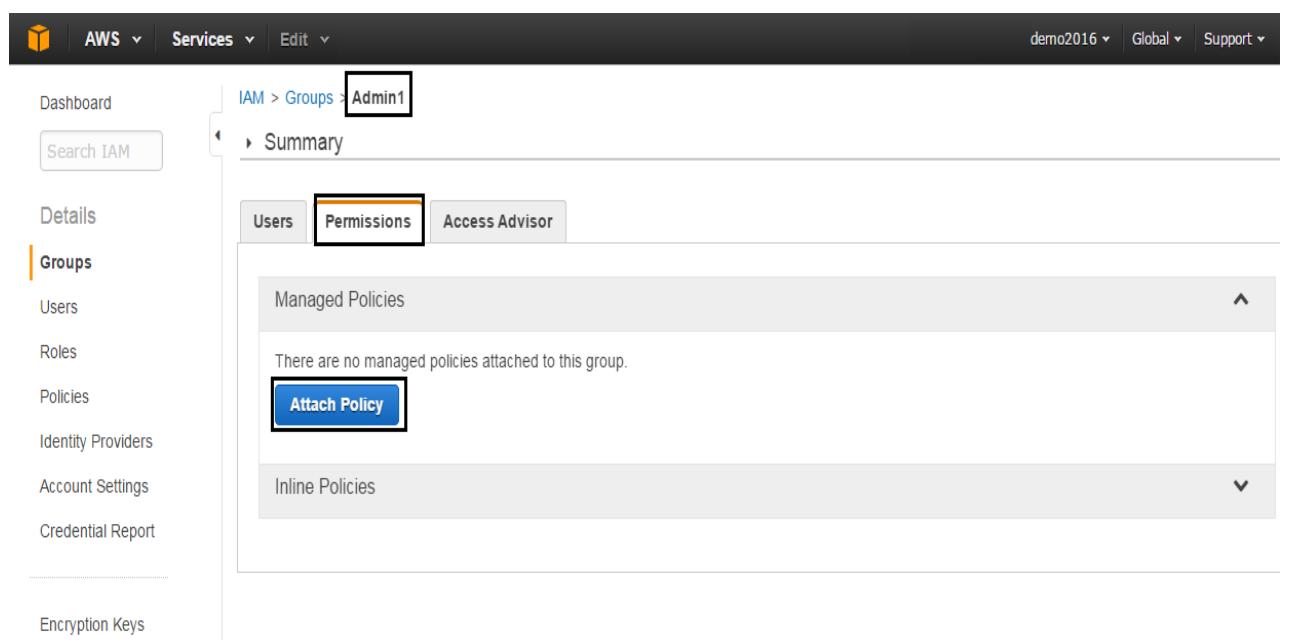
`Admin1`. Click the specific group to view its assigned users and configured preferences.



The screenshot shows the AWS IAM Groups page. On the left sidebar, 'Groups' is selected. The main content area displays a table with two rows:

	Group Name	Users	Inline Policy	Creation Time
<input type="checkbox"/>	Admin	3		2016-06-27 23:12 UTC+0530
<input type="checkbox"/>	Admin1	1		2016-09-23 12:55 UTC+0530

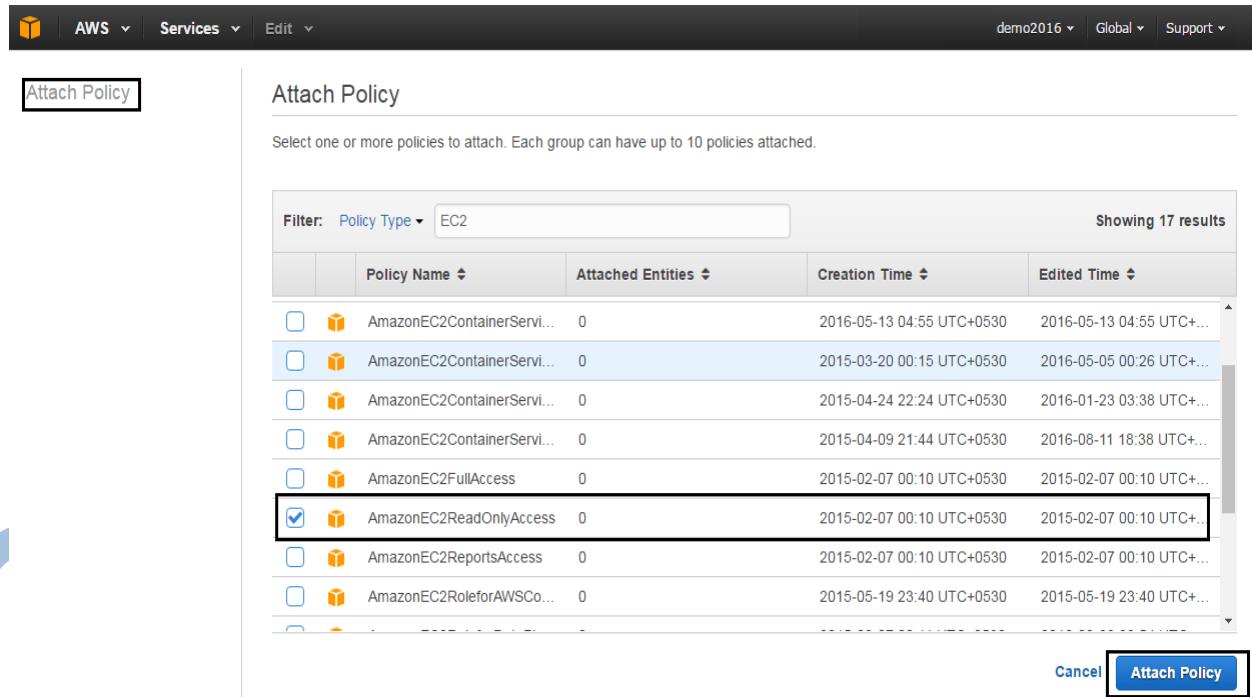
16. Select the `Permissions` for the group and click on 'Attach Policy'. The Manage Permissions Dialog appears.



The screenshot shows the AWS IAM Groups page for the 'Admin1' group. The navigation path is 'IAM > Groups > Admin1'. The 'Permissions' tab is selected. The 'Managed Policies' section indicates there are no managed policies attached to this group, with a prominent 'Attach Policy' button. The 'Inline Policies' section is also visible.

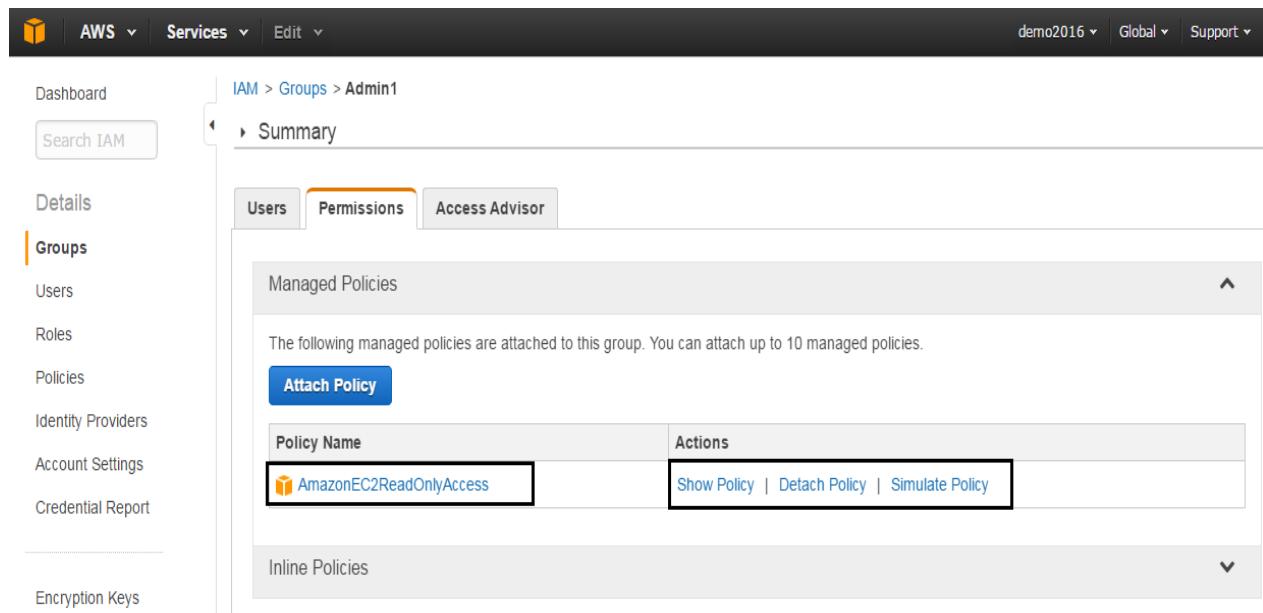
17. Check out the IAM policy ready-made templates and select the one that fit your needs. Here we

Selected “EC2 Read Only Access” policy.



The screenshot shows the AWS IAM Attach Policy interface. At the top left, there is a navigation bar with icons for Home, AWS, Services, Edit, demo2016, Global, and Support. On the left, a sidebar has 'Attach Policy' highlighted. The main area is titled 'Attach Policy' and contains the instruction 'Select one or more policies to attach. Each group can have up to 10 policies attached.' Below this is a table with a filter set to 'Policy Type: EC2'. The table shows 17 results, with the 'AmazonEC2ReadOnlyAccess' policy selected (indicated by a checked checkbox). Other policies listed include AmazonEC2ContainerService, AmazonEC2FullAccess, and AmazonEC2ReportsAccess. At the bottom right of the table are 'Cancel' and 'Attach Policy' buttons.

18. Press ‘Attach Policy’ and you will see Confirmation page.

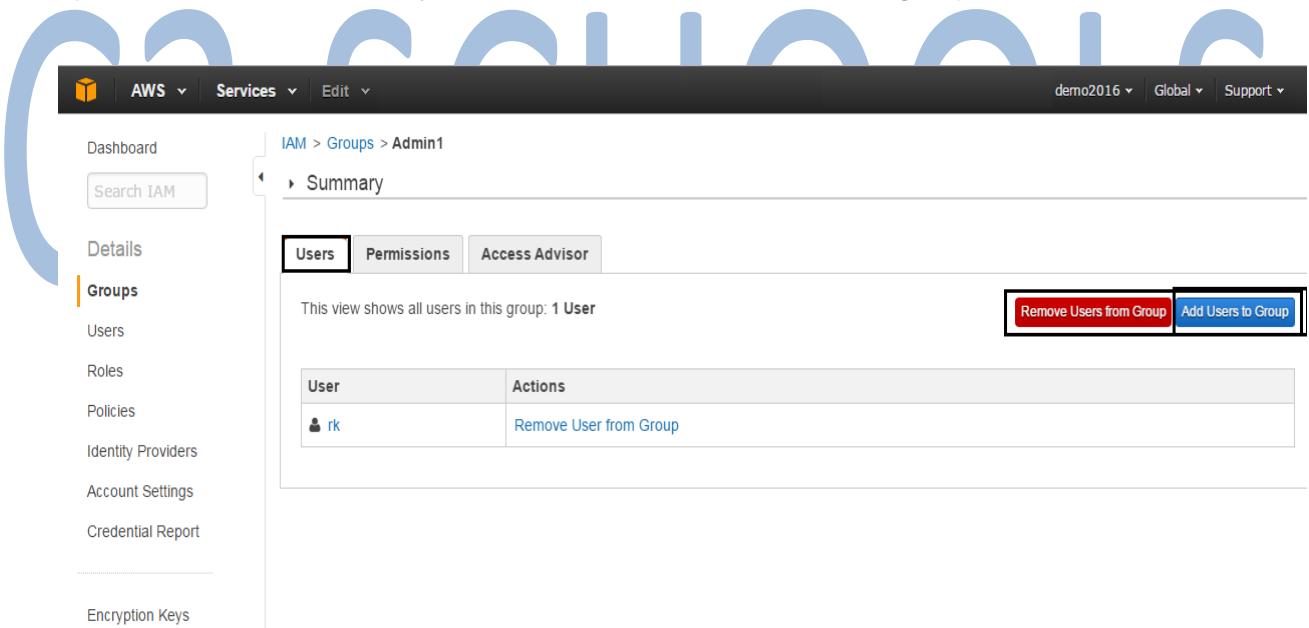


The screenshot shows the AWS IAM Groups Summary page for the 'Admin1' group. The left sidebar includes 'Dashboard', 'Search IAM', 'Details', 'Groups' (which is selected), 'Users', 'Roles', 'Policies', 'Identity Providers', 'Account Settings', 'Credential Report', and 'Encryption Keys'. The main content area shows the 'IAM > Groups > Admin1' path and the 'Summary' tab. Under the 'Permissions' tab, the 'Managed Policies' section lists the 'AmazonEC2ReadOnlyAccess' policy. The 'Actions' column for this policy includes 'Show Policy', 'Detach Policy', and 'Simulate Policy'. The 'Inline Policies' section is currently empty.

19. Apply the policy. Later on you will be able to modify the assigned policy.

G) You can also attach new policy by selecting 'Attach Another Policy'

H) Select the `Users` tab if you want to add or remove user to a group.



The screenshot shows the AWS IAM Groups page. The navigation bar at the top includes 'AWS', 'Services', 'Edit', 'demo2016', 'Global', and 'Support'. On the left, a sidebar menu lists 'Dashboard', 'Search IAM', 'Details', 'Groups' (which is selected and highlighted in orange), 'Users', 'Roles', 'Policies', 'Identity Providers', 'Account Settings', 'Credential Report', and 'Encryption Keys'. The main content area shows the 'Admin1' group summary. It has tabs for 'Users' (selected), 'Permissions', and 'Access Advisor'. A message states 'This view shows all users in this group: 1 User'. Below this is a table:

User	Actions
rk	Remove User from Group

At the bottom right of the table are two buttons: 'Remove Users from Group' (red) and 'Add Users to Group' (blue).

22. You can also manage the assigned group of a user directly from the `Users` section in the IAM section as shown below. Go to IAM Users page by selecting users from left navigation menu.



|| C3 SCHOOLS

AWS Services Edit demo2016 Global Support

Dashboard Search IAM

Details Groups Roles Policies Identity Providers Account Settings Credential Report

Encryption Keys

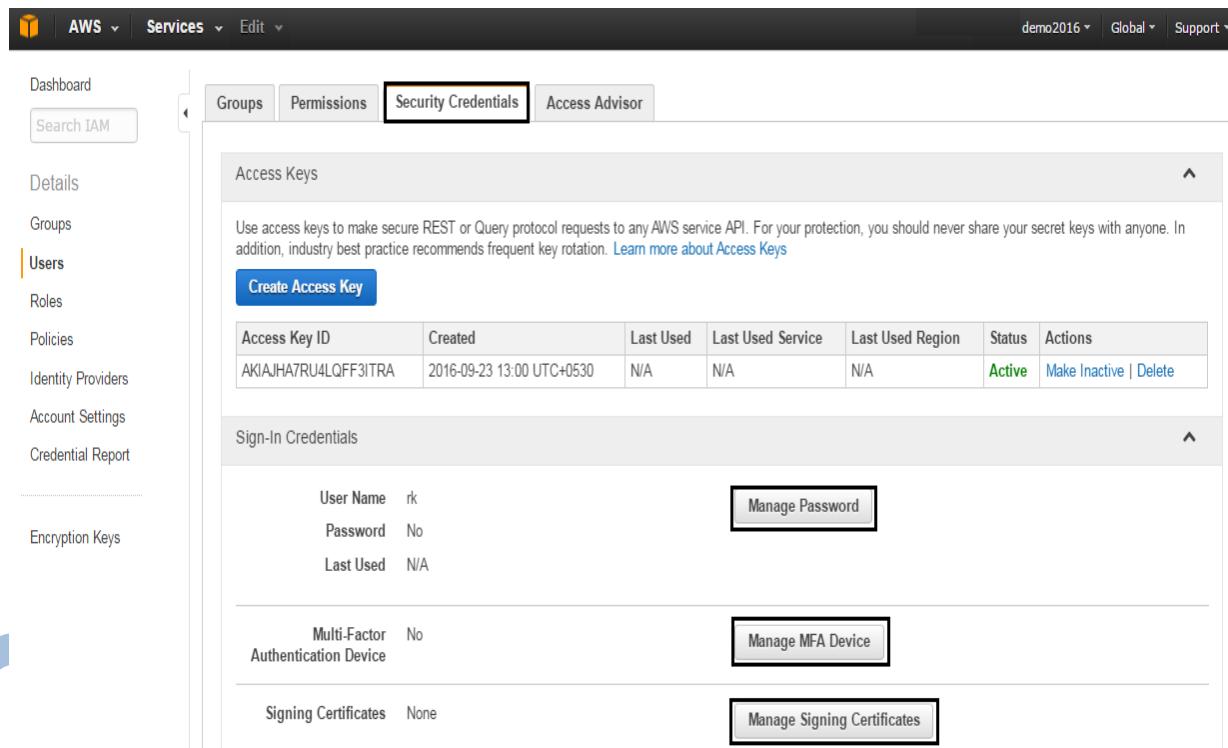
Create New Users User Actions

Filter Showing 4 results

User Name	Groups	Password	Password Last Used	Access Keys	Creation Time
Kumar	1	✓	Never	1 active	2016-09-22 11:31 U...
MohaN	1	✓	2016-09-23 08:12 UTC+0530	1 active	2016-07-19 14:48 U...
RaVi	1	✓	2016-09-23 10:05 UTC+0530	1 active	2016-07-21 13:21 U...
<input checked="" type="checkbox"/> rk	1		N/A	1 active	2016-09-23 13:00 U...

C3 SCHOOLS

- I) Select the Security Credentials tab.



Access Keys

Use access keys to make secure REST or Query protocol requests to any AWS service API. For your protection, you should never share your secret keys with anyone. In addition, industry best practice recommends frequent key rotation. [Learn more about Access Keys](#)

Create Access Key

Access Key ID	Created	Last Used	Last Used Service	Last Used Region	Status	Actions
AKIAJHA7RU4LQFF3ITRA	2016-09-23 13:00 UTC+0530	N/A	N/A	N/A	Active	Make Inactive Delete

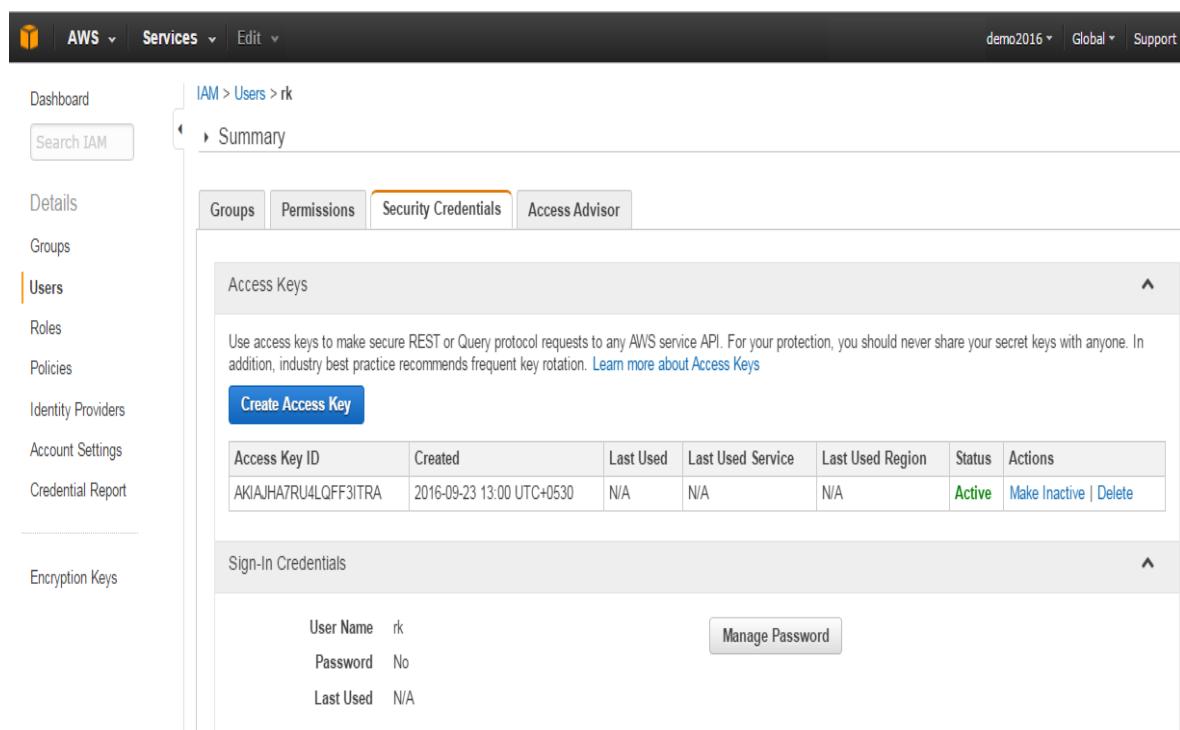
Sign-In Credentials

User Name	rk	Manage Password
Password	No	
Last Used	N/A	

Multi-Factor Authentication Device	No	Manage MFA Device
------------------------------------	----	--------------------------

Signing Certificates	None	Manage Signing Certificates
----------------------	------	------------------------------------

24. Select 'create or Manage Access Keys' to manage your access keys.



IAM > Users > rk

Summary

Access Keys

Use access keys to make secure REST or Query protocol requests to any AWS service API. For your protection, you should never share your secret keys with anyone. In addition, industry best practice recommends frequent key rotation. [Learn more about Access Keys](#)

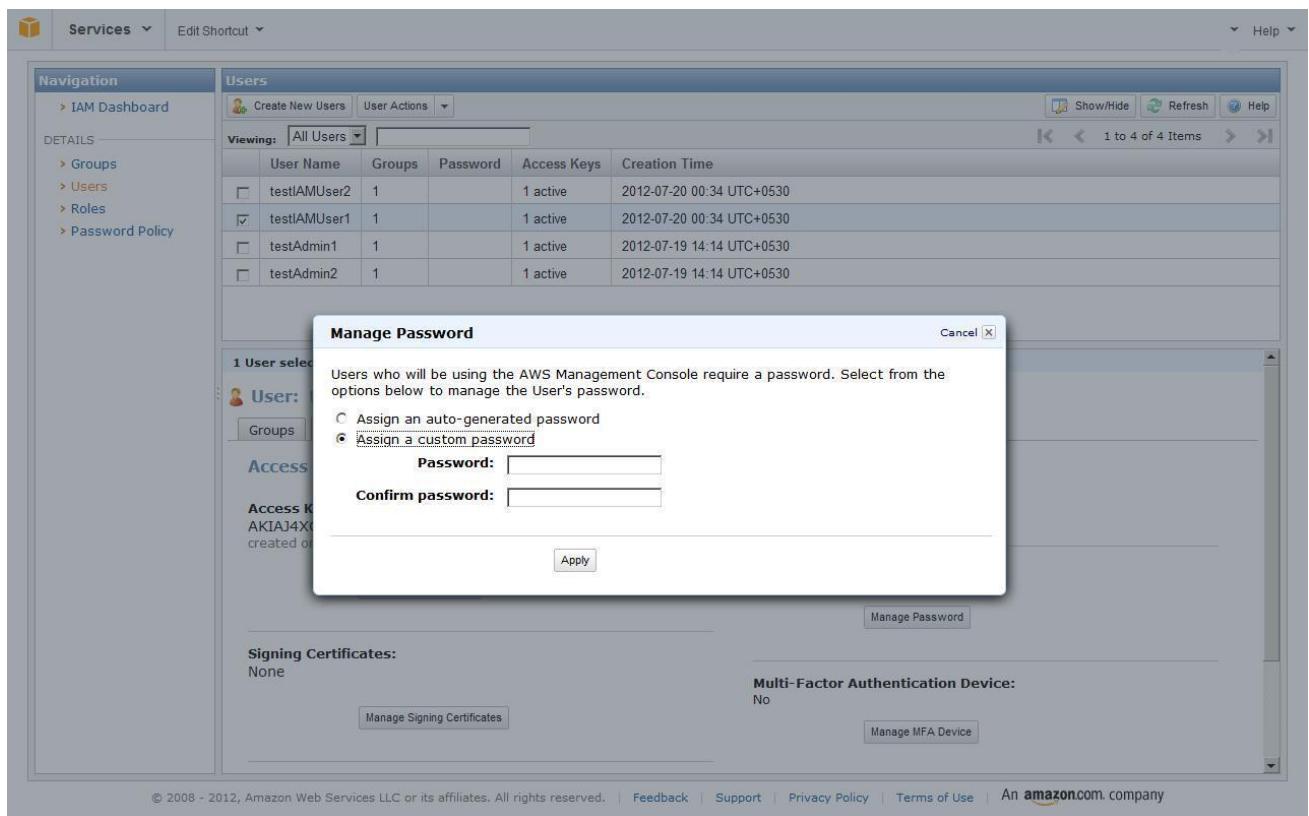
Create Access Key

Access Key ID	Created	Last Used	Last Used Service	Last Used Region	Status	Actions
AKIAJHA7RU4LQFF3ITRA	2016-09-23 13:00 UTC+0530	N/A	N/A	N/A	Active	Make Inactive Delete

Sign-In Credentials

User Name	rk	Manage Password
Password	No	
Last Used	N/A	

25. Select 'Manage Password' from Sescreenurityto manage Credentials your password.



The screenshot shows the AWS IAM Management Console. On the left, there's a navigation sidebar with 'IAM Dashboard' selected. Under 'DETAILS', there are links for Groups, Users, Roles, and Password Policy. The main area is titled 'Users' and shows a table of users:

User Name	Groups	Password	Access Keys	Creation Time
testIAMUser2	1	1 active	2012-07-20 00:34 UTC+0530	
testIAMUser1	1	1 active	2012-07-20 00:34 UTC+0530	
testAdmin1	1	1 active	2012-07-19 14:14 UTC+0530	
testAdmin2	1	1 active	2012-07-19 14:14 UTC+0530	

A modal dialog box titled 'Manage Password' is open over the user list. It contains instructions: 'Users who will be using the AWS Management Console require a password. Select from the options below to manage the User's password.' There are two radio buttons: 'Assign an auto-generated password' (unchecked) and 'Assign a custom password' (checked). Below the radio buttons are two input fields: 'Password:' and 'Confirm password:', both currently empty. At the bottom of the dialog is an 'Apply' button. In the background, under 'User:', there's a section for 'Access Keys' showing 'AKIAJ4X...' and 'created on 2012-07-20'. Below that, there's a 'Signing Certificates:' section stating 'None' and a 'Multi-Factor Authentication Device:' section stating 'No'.

How to Manage AWS IAM Roles

An IAM (the AWS Identity and Management layer) role is an entity that contains set of permissions that applied on other entities. IAM roles enable your and manage users'a and appli secure access to AWS computing resources.

The AWS IAM roles allows an instance to have access to certain resources using API credentials (access key, secret key and security token). This AWS feature provides the ability to have read-only and more importantly write-only access to data service such as AWS SQS, S3, SimpleDB and more.

For example if you grant S3 full read access permission and launch instance while specify the role during the launch process, any application running on the instance can access the S3 resources without any keys or certificates.

Follow the instructions below and learn how-to create and manage an IAM role:

> Using the AWS UI Console

AWS IAM console.

J) Login to AWS IAM console.

K) Select 'Roles' from left navigation menu.

AWS | Services | Edit | demo2016 | Global | Support

Dashboard Create New Role Role Actions

Search IAM

Details Filter Showing 0 result

Groups

Users

Roles

Policies

Identity Providers

Account Settings

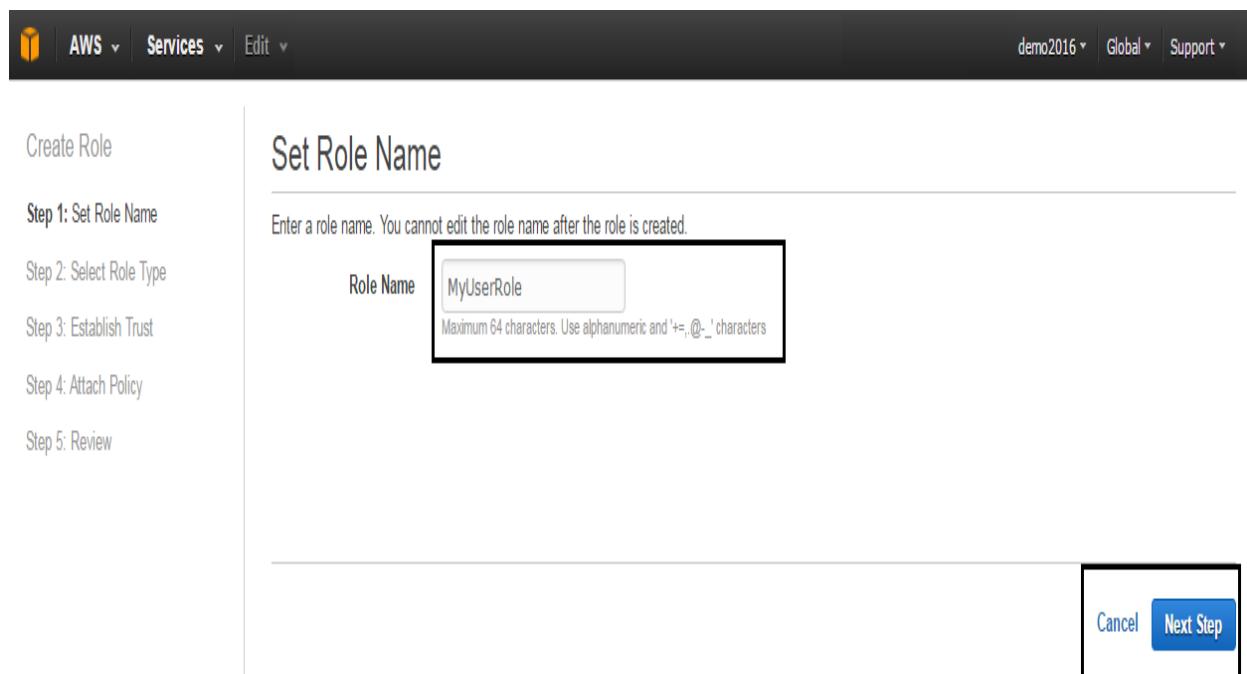
Credential Report

Encryption Keys



C3 SCHOOLS

- L) Click the create button.



AWS Services Edit demo2016 Global Support

Create Role

Step 1: Set Role Name

Step 2: Select Role Type

Step 3: Establish Trust

Step 4: Attach Policy

Step 5: Review

Set Role Name

Enter a role name. You cannot edit the role name after the role is created.

Role Name

Maximum 64 characters. Use alphanumeric and '+,-,_.' characters

Cancel Next Step

4. Provide role name and press Continue. Select Role Type and Establish Trust
- 



|| C3 SCHOOLS

AWS Services Edit demo2016 Global Support

Create Role

Step 1: Set Role Name

Step 2: Select Role Type

Step 3: Establish Trust

Step 4: Attach Policy

Step 5: Review

Select Role Type

AWS Service Roles

› Amazon EC2

Allows EC2 instances to call AWS services on your behalf.

Select

› AWS Directory Service

Allows AWS Directory Service to manage access for existing directory users and groups to AWS services.

Select

› AWS Lambda

Allows Lambda Function to call AWS services on your behalf.

Select

› Amazon Redshift

Allows Amazon Redshift Clusters to call AWS services on your behalf.

Select

› Amazon API Gateway

Allows API Gateway to call AWS resources on your behalf.

Select

Role for Cross-Account Access

Role for Identity Provider Access

Cancel

Previous

Next Step



|| C3 SCHOOLS

8. Select the access policy as per resource. Here we have select Amazon S3 Full Access. Press Next Step button

Attach Policy

Select one or more policies to attach. Each role can have up to 10 policies attached.

	Policy Name	Attached Entities	Creation Time	Edited Time
<input type="checkbox"/>	AmazonRoute53ReadOnlyAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input checked="" type="checkbox"/>	AmazonS3FullAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input type="checkbox"/>	AmazonSESFullAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSESReadOnlyAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSNSSFullAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSNSSReadOnlyAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSNSRole	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSQSFullAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSQSReadOnlyAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSSMFullAccess	0	2015-05-29 23:09 UTC+0530	2016-03-08 02:39 UTC+0530
<input type="checkbox"/>	AmazonSSMReadOnlyAccess	0	2015-05-29 23:14 UTC+0530	2015-05-29 23:14 UTC+0530

Showing 207 results

Cancel Previous **Next Step**

9. Review the policy and modify as needed.

Review

Review the following role information. To edit the role, click an edit link, or click Create Role to finish.

Role Name	MyUserRole	Edit Role Name
Role ARN	arn:aws:iam:076828422820:role/MyUserRole	
Trusted Entities	The identity provider(s) ds.amazonaws.com	
Policies	arn:aws:iam::aws:policy/AmazonS3FullAccess	Change Policies

Cancel Previous **Create Role**



|| C3 SCHOOLS

7. Review all details and press 'Create list the new created Role 'role. In AWS It will IAM console.

IAM > Roles > MyUserRole

Summary

Role ARN: arn:aws:iam::076828422820:role/MyUserRole

Instance Profile ARN(s):

Path: /

Creation Time: 2016-09-23 21:55 UTC+0530

Permissions Trust Relationships Access Advisor Revoke Sessions

Managed Policies

The following managed policies are attached to this role. You can attach up to 10 managed policies.

Attach Policy

Policy Name	Actions
AmazonS3FullAccess	Show Policy Detach Policy Simulate Policy

Inline Policies

8. Modify or add policy from the bottom console pane

9. Grant additional cloud resource access by choosing the relevant policy.



|| C3 SCHOOLS

The screenshot shows the 'Attach Policy' section of the AWS IAM console. It displays a table of available policies, each with a checkbox, a policy name, the number of attached entities, creation time, and edited time. The 'AmazonSESFullAccess' policy is selected, indicated by a checked checkbox. The table has four columns: Policy Name, Attached Entities, Creation Time, and Edited Time. A filter bar at the top left allows filtering by Policy Type. A message at the top says 'Select one or more policies to attach. Each role can have up to 10 policies attached.' At the bottom right of the table area, there are 'Cancel' and 'Attach Policy' buttons.

	Policy Name	Attached Entities	Creation Time	Edited Time
<input type="checkbox"/>	AmazonRoute53FullAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input type="checkbox"/>	AmazonRoute53ReadOnlyAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input checked="" type="checkbox"/>	AmazonSESFullAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSESReadOnlyAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSNSFullAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSNSReadOnlyAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSNSRole	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSQSFullAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSQSReadOnlyAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSSMFullAccess	0	2015-05-29 23:09 UTC+0530	2016-03-08 02:39 UTC+0530
<input type="checkbox"/>	AmazonSSMReadOnlyAccess	0	2015-05-29 23:14 UTC+0530	2015-05-29 23:14 UTC+0530
<input type="checkbox"/>	AmazonVPCFullAccess	0	2015-02-07 00:11 UTC+0530	2015-12-17 22:55 UTC+0530

Attach Policy

Attach Policy

Select one or more policies to attach. Each role can have up to 10 policies attached.

Showing 205 results				
	Policy Name	Attached Entities	Creation Time	Edited Time
<input type="checkbox"/>	AmazonRoute53FullAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input type="checkbox"/>	AmazonRoute53ReadOnlyAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input checked="" type="checkbox"/>	AmazonSESFullAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSESReadOnlyAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSNSFullAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSNSReadOnlyAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSNSRole	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSQSFullAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSQSReadOnlyAccess	0	2015-02-07 00:11 UTC+0530	2015-02-07 00:11 UTC+0530
<input type="checkbox"/>	AmazonSSMFullAccess	0	2015-05-29 23:09 UTC+0530	2016-03-08 02:39 UTC+0530
<input type="checkbox"/>	AmazonSSMReadOnlyAccess	0	2015-05-29 23:14 UTC+0530	2015-05-29 23:14 UTC+0530
<input type="checkbox"/>	AmazonVPCFullAccess	0	2015-02-07 00:11 UTC+0530	2015-12-17 22:55 UTC+0530

Cancel Attach Policy

CS SCHUULS

11. Once your role is created you can assign it to an instance while launching. Select the role on instance launch dialog as shown below.



|| C3 SCHOOLS

Step 3: Configure Instance Details

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

Number of instances: 1

Purchasing option: Request Spot Instances

Network: vpc-6d584d09 (10.0.0.0/16) | MyVPC

Subnet: subnet-3f85b85b(10.0.1.0/24) | subnetuswest-2a | 251 IP Addresses available

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

IAM role: S3 FullAccess

Shutdown behavior: Stop

Enable termination protection: Protect against accidental termination

Monitoring: Enable CloudWatch detailed monitoring
Additional charges apply.

Buttons: Cancel, Previous, **Review and Launch**, Next: Add Storage

> Create and view IAM roles using the AWS UI Command Line -

1. Run the command **iam-rolecreate -r testRole2 -p / -s ec2.amazonaws.com -v** to create a new role. Here in the command ‘-p’ is path which is‘-defaults’indicating the‘/’service.. Note that currently only ec2 is supported.

```
Administrator: C:\Windows\system32\cmd.exe
C:\AWS>iam-rolecreate -r testRole2 -p / -s ec2.amazonaws.com -v
arn:aws:iam::9[REDACTED]:role/testRole2
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Service": "ec2.amazonaws.com"
        }
    ],
    "Action": [
        "sts:AssumeRole"
    ]
}
C:\AWS>
```



|| C3 SCHOOLS

2. The command `iam-rolelistbypath` returns the roles' list.

```
C:\>Administrator: C:\Windows\system32\cmd.exe
C:\>AWS>iam-rolelistbypath
arn:aws:iam::900000000000:role/testRole2
arn:aws:iam::900000000000:role/testRoleName
IsTruncated: false
C:\>AWS>
```

How to Use Amazon CloudWatch to View Your AWS Cloud Metrics

1. Login to your AWS UI management console and enter the AWS Cloud Watch service page.

2. If your First Time CloudWatch Page will be as follows...

The screenshot shows the AWS CloudWatch Metrics service page. The top navigation bar includes 'AWS', 'Services', 'Edit', 'CloudWatch', 'Dashboards', 'Alarms', 'ALARM', 'INSUFFICIENT', 'OK', 'Billing', 'Events', 'Rules', 'Logs', and 'Metrics NEW'. A sidebar on the left lists 'CloudWatch', 'Dashboards', 'Alarms', 'ALARM', 'INSUFFICIENT', 'OK', 'Billing', 'Events', 'Rules', 'Logs', and 'Metrics NEW'. The main content area features a 'Metric Summary' section with a message about extended retention and a link to 'Go to Amazon EC2'. It also includes sections for 'Alarm Summary' (with a note about no alarms created) and 'Service Health' (showing a single entry for 'Amazon CloudWatch Service' with status 'Service is operating normally'). On the right, there's an 'Additional Info' sidebar with links to 'Getting Started Guide', 'Monitoring Scripts Guide', 'Overview and Features', 'Documentation', 'Forums', and 'Report an Issue'.

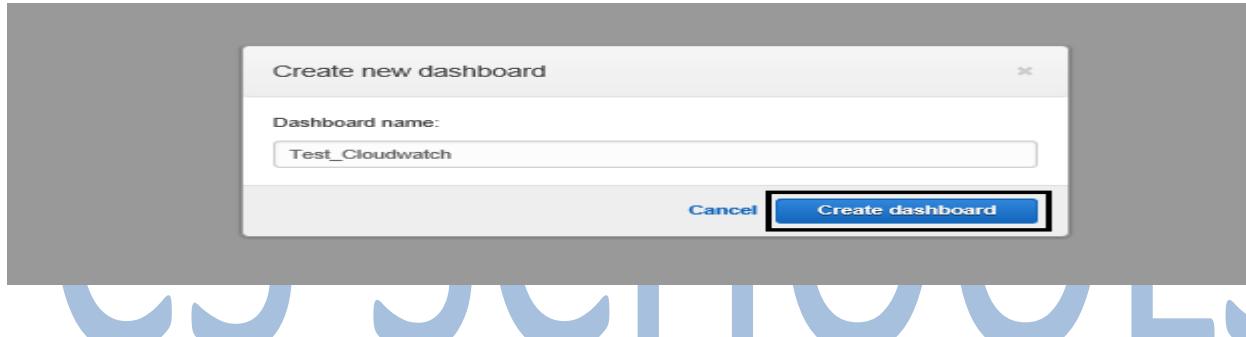


|| C3 SCHOOLS

3. In the navigation pane, choose **Dashboards**. Choose **Create dashboard**. Then Pop Up box will Appear Enter Name For Dashboard...

The screenshot shows the AWS CloudWatch Dashboards interface. On the left, there's a navigation sidebar with links like CloudWatch, Dashboards, Alarms, ALARM, INSUFFICIENT, OK, Billing, Events, Rules, Logs, and Metrics (NEW). The 'Dashboards' link is currently selected. The main area has a heading 'Dashboards' and a large 'Create dashboard' button, which is also highlighted with a blue box. Below it is a 'Name' input field containing 'Test_Cloudwatch'. A message says, 'You have no CloudWatch dashboards. Please [create a dashboard](#)'. On the right side, there's an 'Additional Information' section with links to 'Getting Started Guide', 'Documentation', 'Forums', and 'Report an Issue'. At the top, there are AWS navigation links for 'AWS', 'Services', 'Edit', and account information 'demo2016', 'Mumbai', and 'Support'.

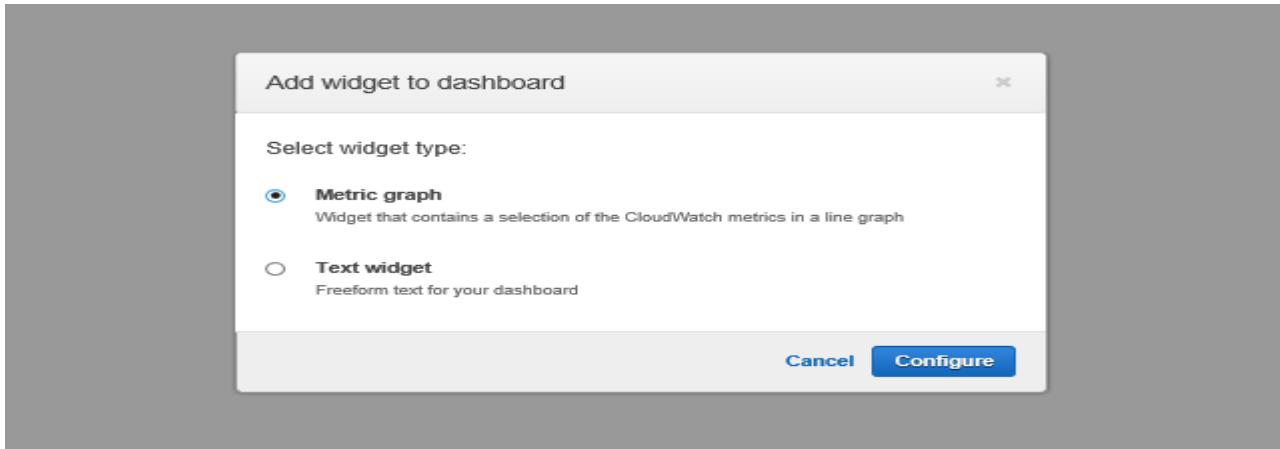
Then Click On Create Dashboard.



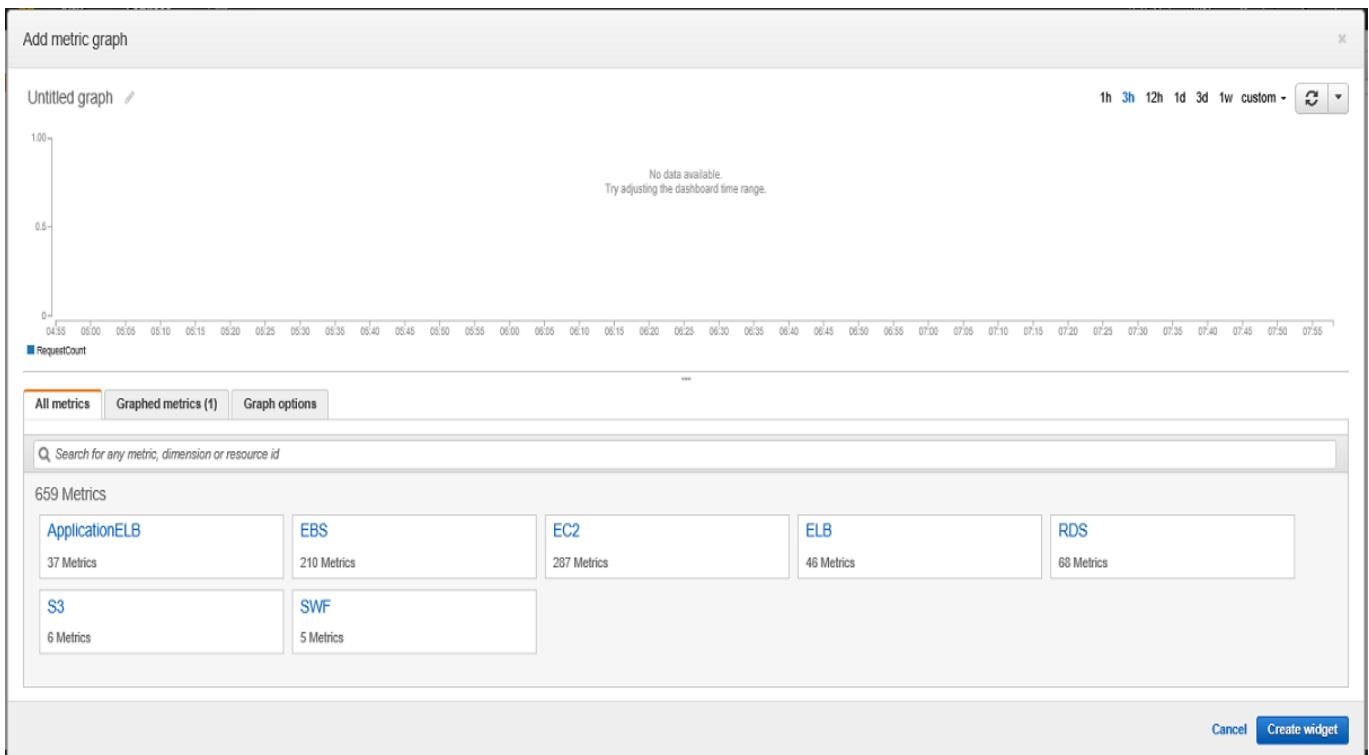


|| C3 SCHOOLS

4. To add a graph to your dashboard, choose **Metric graph** and then choose **Configure**



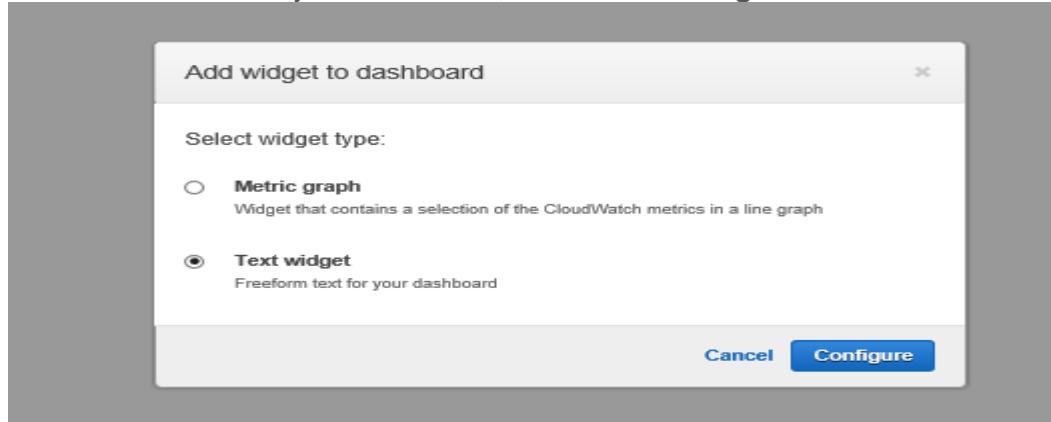
5. Then, in the **Add metric graph** dialog box, select the metrics to graph, and then choose **Create widget**.



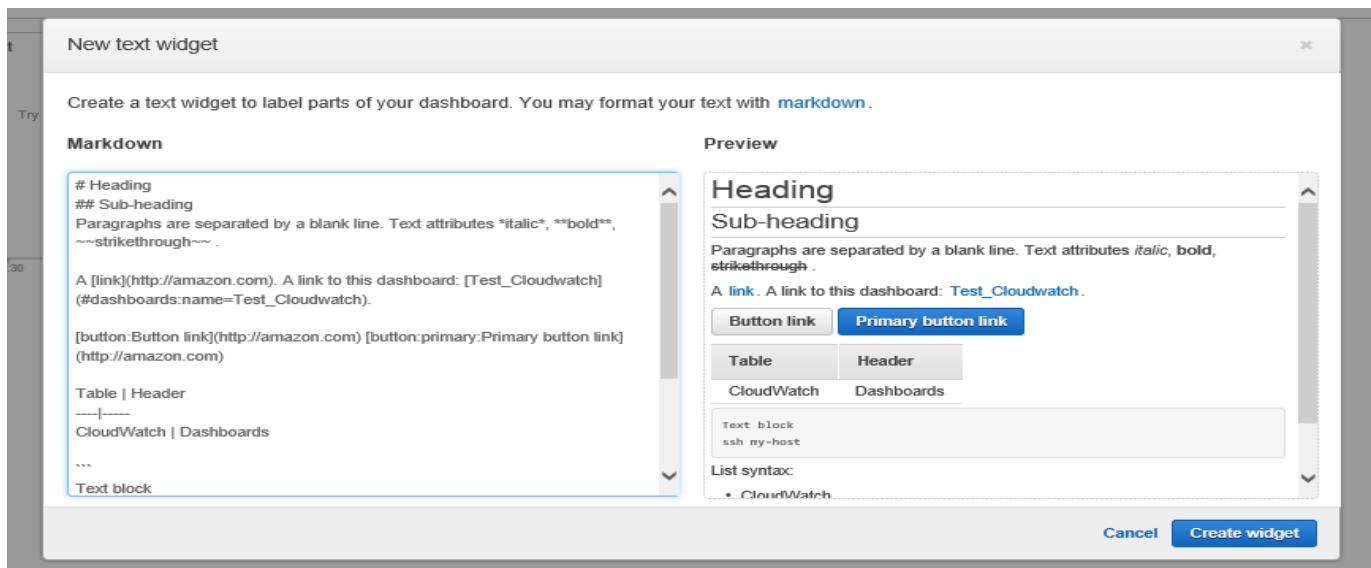


|| C3 SCHOOLS

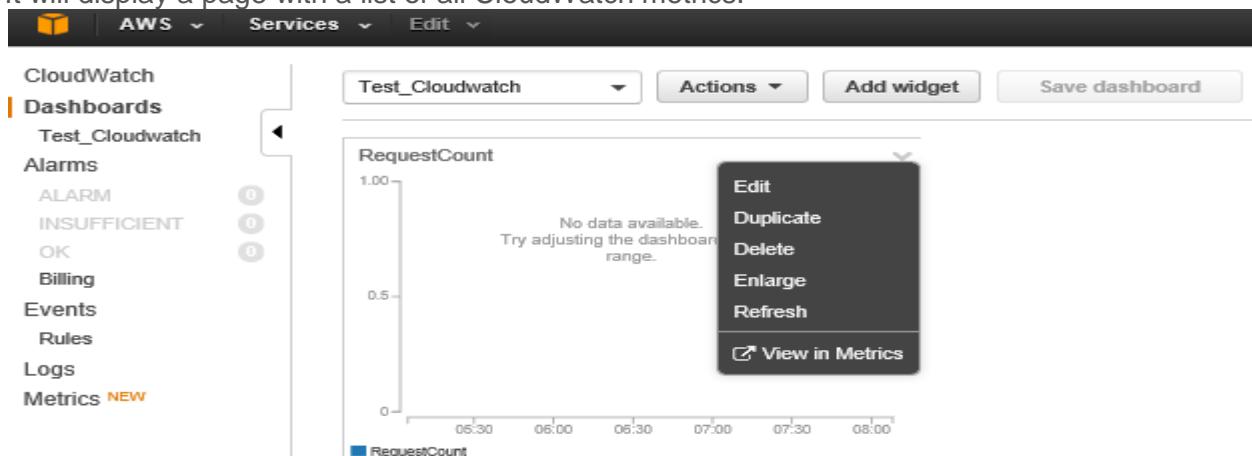
6. To add a text block to your dashboard, choose **Text widget** and then choose **Configure**.



7. Then, in the **New text widget** dialog box, for **Markdown**, add and format your text using [Markdown](#), and then choose **Create widget**.

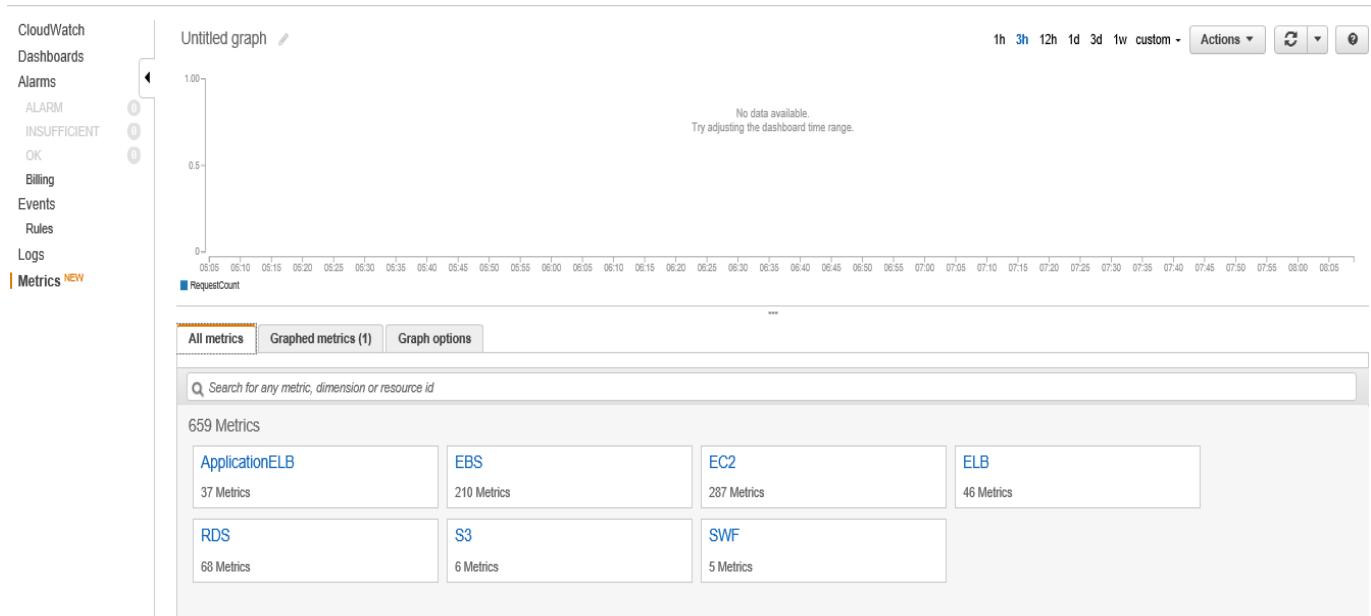


8. It will display a page with a list of all CloudWatch metrics.

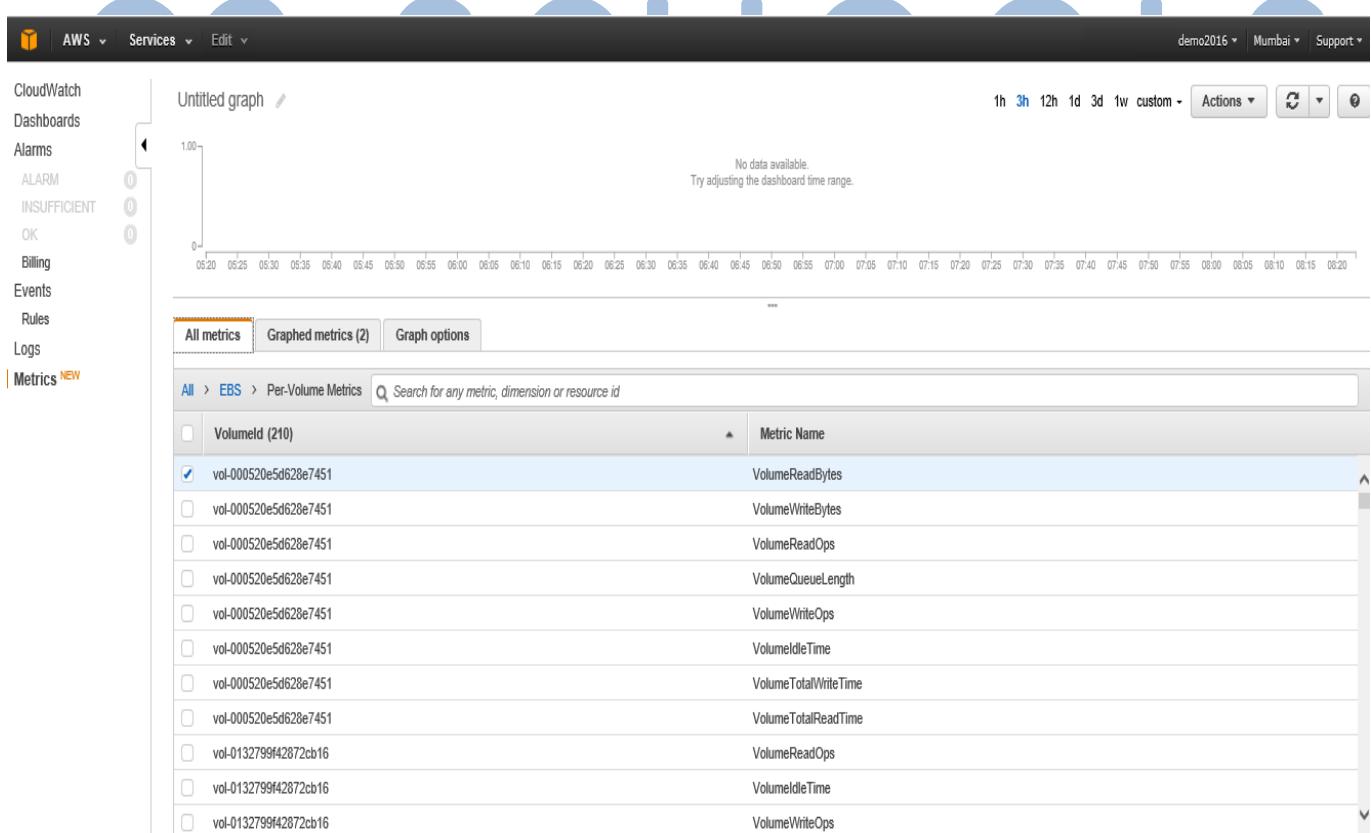




|| C3 SCHOOLS



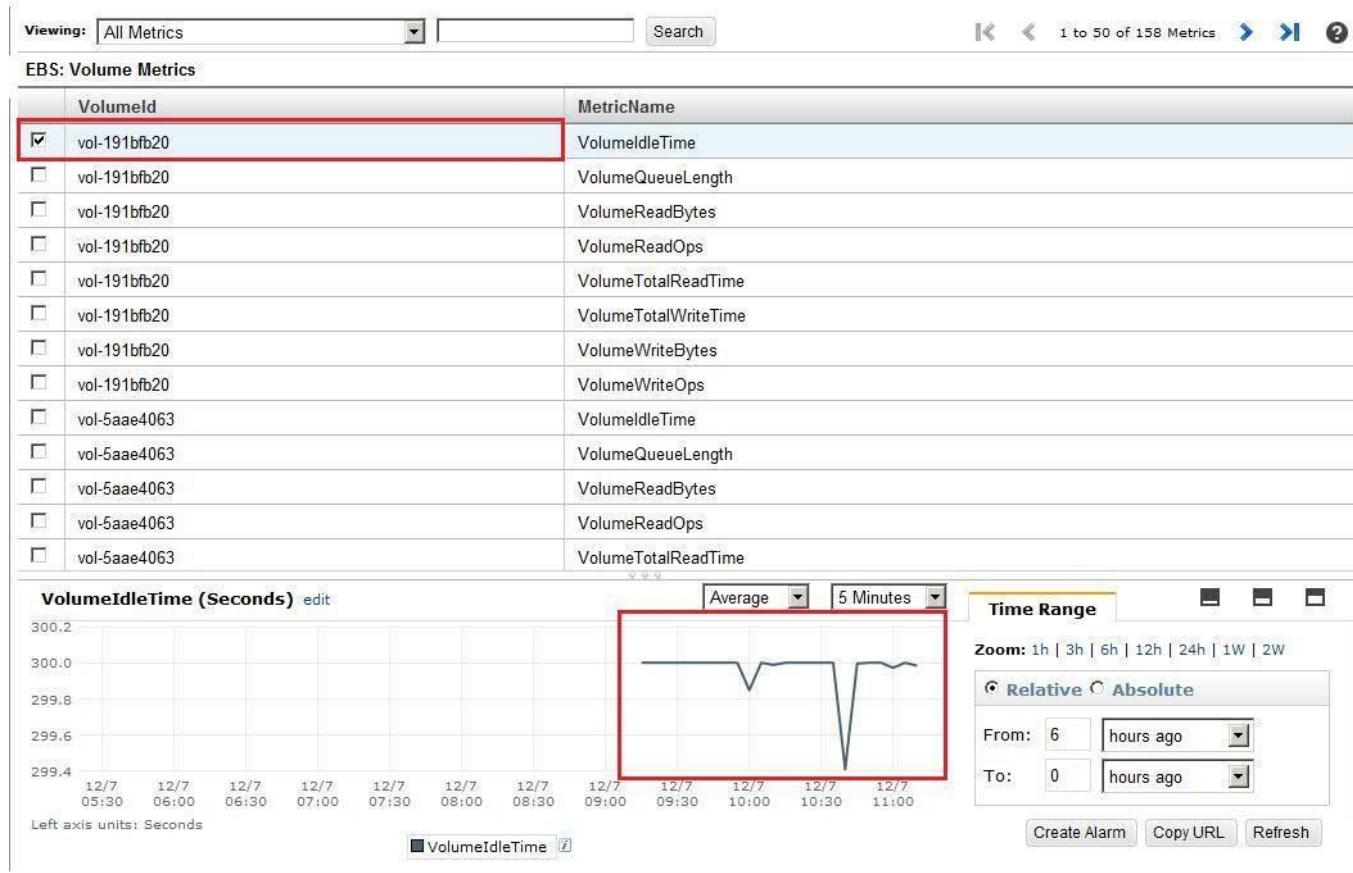
9. It will display a page with a list of all CloudWatch metrics. The first listing is for volumes. Select any metric of a volume.



10. It will list metrics collected for that resource during the last 6 hours.



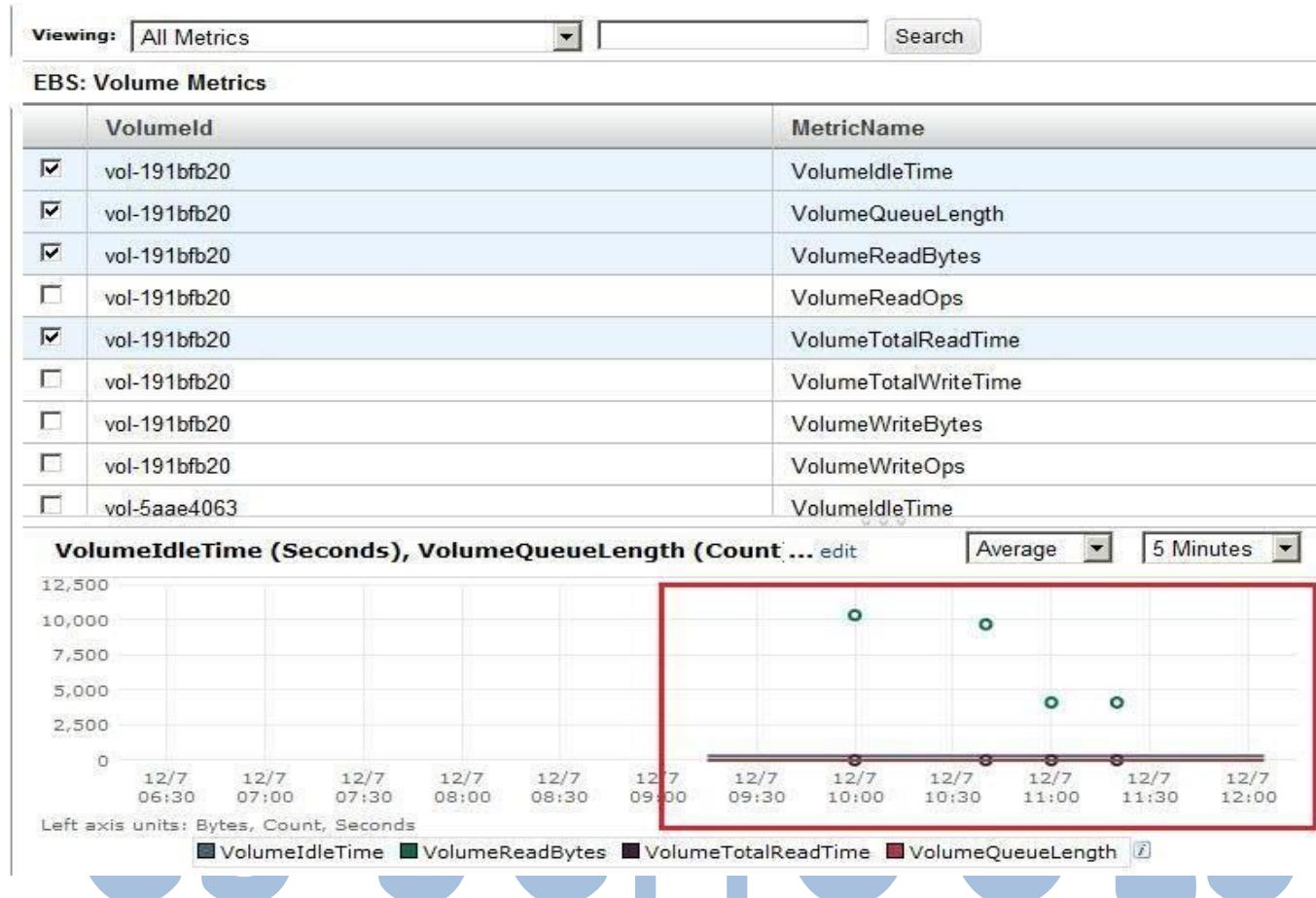
|| C3 SCHOOLS





|| C3 SCHOOLS

11. If you select multiple metrics they all will be displayed in the same graph.



Use Amazon CloudWatch CLI to View Your AWS Cloud Metrics

1. If you want to list your metrics through the command line tool first [install the AWS Cloud Watch CLI](#).

2. Run the commands below -

Setting the Region for CloudWatch:

```
set AWS_CLOUDWATCH_URL=https://monitoring.us-west-2.amazonaws.com
```

Run the command:



|| C3 SCHOOLS

Mon-list-metrics --headers

It will list all the metrics. Use pipe command to load data page wise.

C3 SCHOOLS



|| C3 SCHOOLS

3. The output of the above commands -

4. Load more metrics:

InstanceType	t1.micro	"
InstanceType	t1.micro	"
LoadBalancerName	AWSHttpsELB	"
LoadBalancerName	ELBConfigureSSL	"
VolumeId	vol-191bfhb20	"

How to Enable CloudWatch Detailed Monitoring

1 . Enter your AWS Account console then Enter the EC2 section and select the relevant instance.



|| C3 SCHOOLS

The screenshot shows the AWS EC2 Instances page. On the left sidebar, under 'INSTANCES', 'Instances' is selected. In the main content area, a single instance named 'Test_Server' is listed. The instance ID is i-09e4e5bd1c78686f1, it's an t2.micro type running in ap-south-1b. The public DNS is ec2-35-154-24-53.ap-south-1.compute.amazonaws.com. The instance state is running. The monitoring tab is selected at the bottom.

2. At the bottom pane of the instance details select the `Monitoring` tab.

The screenshot shows the same AWS EC2 Instances page as above, but the 'Monitoring' tab is now selected at the bottom. The instance details remain the same. The CloudWatch metrics section is visible, showing four graphs for CPU Utilization, Disk Reads, Disk Read Operations, and Disk Writes over the last hour. The graphs show minimal activity.



|| C3 SCHOOLS

3. In order to increase the monitoring resolution we will enable detailed monitoring at every minute. Click "Enable Detailed Monitoring" and Confirm it for the specific instance selected.

Enable Detailed Monitoring

Enable detailed monitoring for your instance to get these metrics at 1-minute frequency. [Learn more](#)

Are you sure you want to enable detailed monitoring for the following instances? [\(Additional charges apply.\)](#)

i-09e4e5bd1c78686f1 (Test_Server)

CPU Utilization (Percent)

Disk Reads (Bytes)

Disk Read Operations (Operations)

Disk Writes (Bytes)

Cancel Yes, Enable

Enable Detailed Monitoring

Detailed monitoring has been enabled.

Close

4. Once it is enabled it will show data as below and the parameters will refresh at every minute.



|| C3 SCHOOLS

AWS Services Edit

EC2 Dashboard

Events

Tags

Reports

Limits

INSTANCES

Instances

Spot Requests

Reserved Instances

Dedicated Hosts

IMAGES

AMIs

Bundle Tasks

ELASTIC BLOCK STORE

Volumes

Snapshots

NETWORK & SECURITY

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

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 Key

Test_Server i-09e4e5bd1c7868f1 (Test_Server) i2.micro ap-south-1b running 2/2 checks... None ec2-35-154-24-53.ap-south-1.compute.amazonaws.com 35.154.24.53 Mumbai

Instance: i-09e4e5bd1c7868f1 (Test_Server) Public DNS: ec2-35-154-24-53.ap-south-1.compute.amazonaws.com

Description Status Checks Monitoring Tags

CloudWatch alarms: No alarms configured Create Alarm

No alarms created. You can create an alarm using the Create Alarm button above.

CloudWatch metrics: Detailed monitoring. Disable Detailed Monitoring Showing data for: Last Hour

CPU Utilization (Percent)

Time	Value
11/8 08:00	0.041
11/8 08:30	0.011

Disk Reads (Bytes)

Time	Value
11/8 08:00	0.75
11/8 08:30	0.25

Disk Read Operations (Operations)

Time	Value
11/8 08:00	0.75
11/8 08:30	0.25

Disk Writes (Bytes)

Time	Value
11/8 08:00	0.75
11/8 08:30	0.25

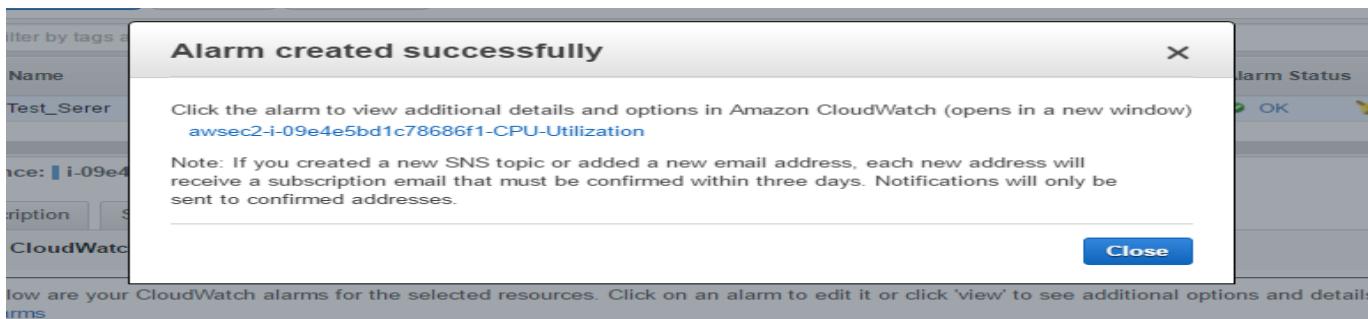
Below are your CloudWatch metrics for the selected resources (a maximum of 10). Click on a graph to see an expanded view. All times shown are in UTC. View all CloudWatch metrics



|| C3 SCHOOLS

5. Press “Create Alarm” to a new alarm or “View all CloudWatch Alarms” to get the list of all your CloudWatch alarms. Note that – AWS cloud free tier include 10 CloudWatch alarms, each additional will cost you \$0.10 per alarm per month.

The screenshot shows the 'Create Alarm' dialog box. In the 'Send a notification to:' field, 'Test_Alarm' is entered. Below it, 'awsAccount@domain.com' is listed under 'With these recipients:'. Under 'Take the action:', there are four options: 'Recover this instance', 'Stop this instance', 'Terminate this instance', and 'Reboot this instance'. A warning message 'You have to select an action.' is displayed. The 'Whenever:' dropdown is set to 'Maximum' of 'CPU Utilization', with 'Is:' set to '>= 80 Percent'. 'For at least:' is set to '1 consecutive period(s) of 5 Minutes'. The 'Name of alarm:' field contains 'awsec2-i-09e4e5bd1c78686f1-CPU-Utilization'. To the right, a chart titled 'CPU Utilization Percent' shows a red horizontal line at 80% across three time periods: 11/8 04:00, 11/8 06:00, and 11/8 08:00. The chart area includes the identifier 'i-09e4e5bd1c78686f1'. At the bottom right are 'Cancel' and 'Create Alarm' buttons.



6. To disable the “detailed monitoring”, select the instance and select “Instance Action” as shown below.



|| C3 SCHOOLS

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Dedicated Hosts, Images (AMIs), and Elastic Block Store (Volumes, Snapshots). The main area displays a table of instances. One instance, 'Test_Server' (ID: i-09e4e5bd1c78686f1), is selected. A context menu is open over this instance, with 'CloudWatch Monitoring' highlighted. Sub-options under 'CloudWatch Monitoring' include 'Enable Detailed Monitoring' (disabled) and 'Disable Detailed Monitoring' (enabled). Other options in the menu are 'Connect', 'Get Windows Password', 'Launch More Like This', 'Instance State', 'Instance Settings', 'Image', and 'Networking'. Below the instance table, there's a section for CloudWatch alarms, showing one alarm named 'awsec2-i-09e4e5bd1c78686f1-CPU-Utilization' in OK state, with a 'view' link.

State	Name	More Options
OK	awsec2-i-09e4e5bd1c78686f1-CPU-Utilization	view

C3 SCHOOLS



|| C3 SCHOOLS

7. Confirm the action.

The screenshot shows the AWS CloudWatch Metrics console. A modal dialog box titled "Disable Detailed Monitoring" is centered. It contains a message asking if the user is sure they want to disable detailed monitoring for the instance i-09e4e5bd1c78686f1 (Test_Server). Below the message is a table showing one CloudWatch alarm named "awsec2-i-09e4e5bd1c78686f1-CPU-Utilization" with a status of "OK". At the bottom of the dialog are two buttons: "Cancel" and "Yes, Disable". The background of the console shows the instance details for "Test_Server" (i-09e4e5bd1c78686f1) including its state as "running" and its public IP as 35.154.24.53.

The screenshot shows the AWS CloudWatch Metrics console after the monitoring has been disabled. The modal dialog box now displays a green-bordered message box containing the text "Detailed monitoring has been disabled." There is a single "Close" button at the bottom right of the dialog. The background shows the same instance details as the previous screenshot, but the CloudWatch alarm table is no longer present.

How to Get Statistics on AWS EC2 Using Amazon CloudWatch

1. To access the AWS CloudWatch console go to [AWS console](#) and select the AWS CloudWatch service.
2. The AWS CloudWatch dashboard lists your present alarms as well as an overview of your AWS resources. Click “View Metrics”.



|| C3 SCHOOLS

AWS Services Edit

CloudWatch Dashboards Test_Cloudwatch Alarms Events Rules Logs Metrics NEW

Test_Cloudwatch Actions Add widget Save dashboard

RequestCount
1.00
0.5
0
No data available.
Try adjusting the dashboard range.

Edit Duplicate Delete Enlarge Refresh View in Metrics

CloudWatch Dashboards Alarms Events Rules Logs Metrics NEW

Untitled graph / Actions 1h 3h 12h 1d 3d 1w custom ▾

No data available.
Try adjusting the dashboard time range.

All metrics Graphed metrics (1) Graph options

Search for any metric, dimension or resource id

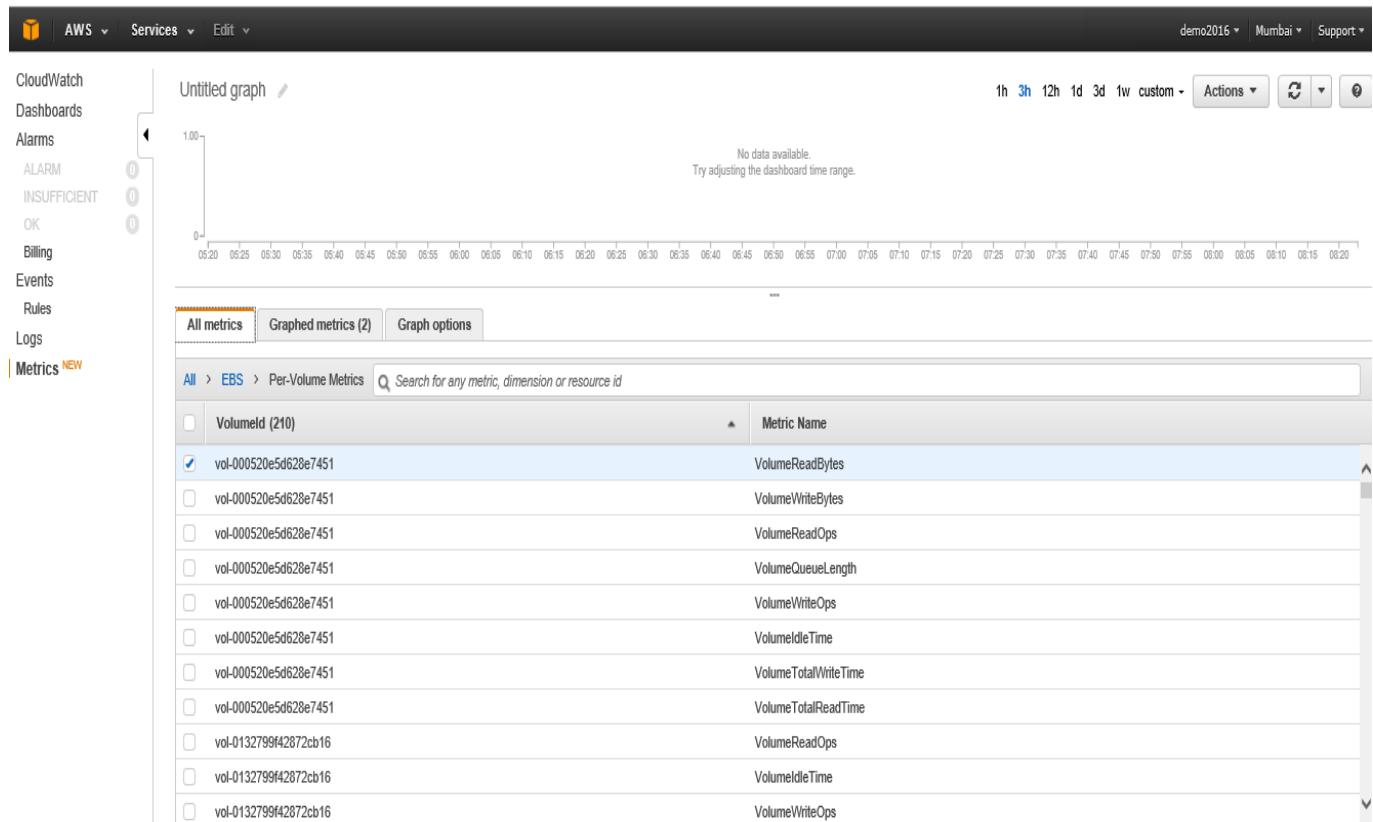
659 Metrics

ApplicationELB 37 Metrics	EBS 210 Metrics	EC2 287 Metrics	ELB 46 Metrics
RDS 68 Metrics	S3 6 Metrics	SWF 5 Metrics	

3. It will display a page with a list of all CloudWatch metrics. The first listing is for volumes. Select any metric of a volume.



|| C3 SCHOOLS



4. It displays a page which has the list of all CloudWatch metrics. In the “Viewing” dropdown menu, select “EC2:Instance Metrics”.

This screenshot shows a list of CloudWatch metrics. The 'Viewing:' dropdown is set to 'EBS: Volume Metrics'. A dropdown menu is open under 'EBS: Vol' showing options: 'All Metrics', 'EBS: Volume Metrics', 'EC2: Aggregated Across Instances', 'EC2: Aggregated by Image (AMI) Id', 'EC2: Instance Metrics' (which is selected and highlighted in blue), 'EC2: Aggregated by Instance Type', 'ELB: Aggregated Across All Load Balancers', 'ELB: Aggregated by Availability Zone', and 'ELB: Load Balancers By Availability Zone'. The main table lists metrics with their names:

	MetricName
<input type="checkbox"/> vol-000520e5d628e7451	VolumeldTime
<input type="checkbox"/> vol-191fbfb20	VolumeQueueLength
<input type="checkbox"/> vol-191fbfb20	VolumeReadBytes
<input type="checkbox"/> vol-191fbfb20	VolumeReadOps
<input type="checkbox"/> vol-191fbfb20	VolumeTotalReadTime
<input type="checkbox"/> vol-191fbfb20	VolumeTotalWriteTime
<input type="checkbox"/> vol-5aaee4063	VolumeWriteBytes
<input type="checkbox"/> vol-5aaee4063	VolumeWriteOps
<input type="checkbox"/> vol-5aaee4063	VolumeldTime

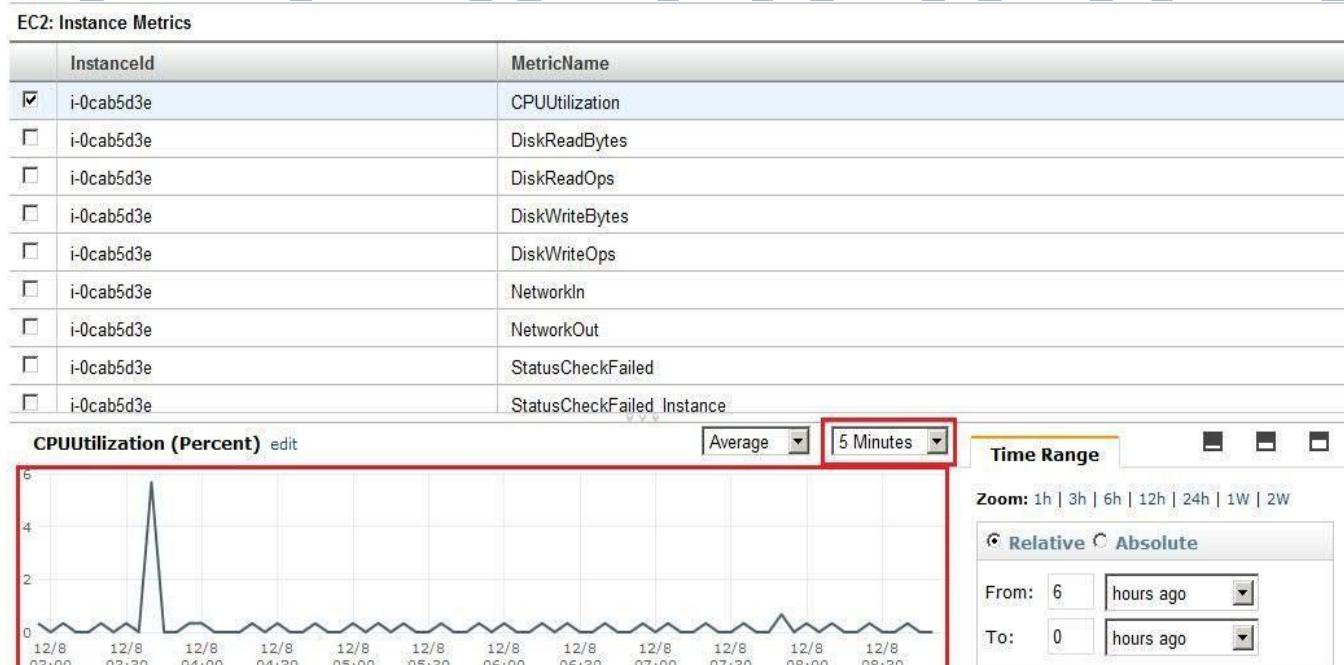


|| C3 SCHOOLS

5. It will list all the metrics available for all the instances of that region. Scroll down to select the metric for a specific instance or select “CPU Utilization” for the marked instance.

EC2: Instance Metrics	
InstanceId	MetricName
<input type="checkbox"/> i-0cab5d3e	CPUUtilization
<input type="checkbox"/> i-0cab5d3e	DiskReadBytes
<input type="checkbox"/> i-0cab5d3e	DiskReadOps
<input type="checkbox"/> i-0cab5d3e	DiskWriteBytes
<input type="checkbox"/> i-0cab5d3e	DiskWriteOps
<input type="checkbox"/> i-0cab5d3e	NetworkIn
<input type="checkbox"/> i-0cab5d3e	NetworkOut
<input type="checkbox"/> i-0cab5d3e	StatusCheckFailed
<input type="checkbox"/> i-0cab5d3e	StatusCheckFailed_Instance

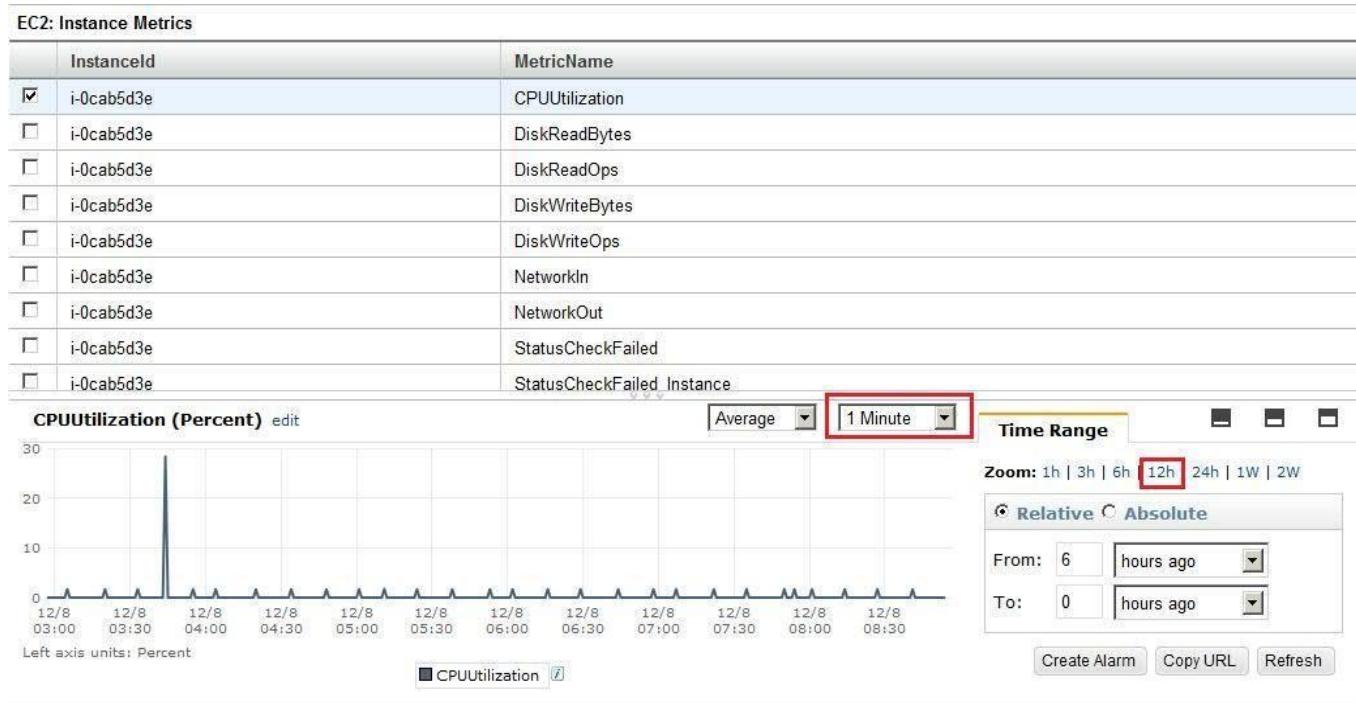
6. It will list CPU Utilization data of the selected instance over the last 6 hours. Currently it shows the basic monitoring data at every 5 minutes.





|| C3 SCHOOLS

7. If detailed monitoring is enabled for this instance, select “1 Minute” from the dropdown. It will list more detailed CPU Utilization statistics at every minute for this instance.



C3 SCHOOLS

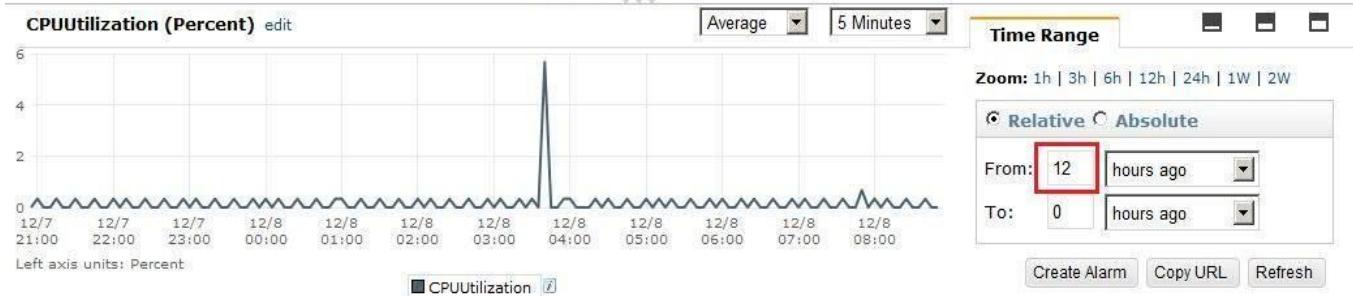
8. If you want to see the metrics for the last 12 hours, select 12h in “Time Range”. It will list records of the last 12 hours. The maximum range can be of 14 days.



|| C3 SCHOOLS

EC2: Instance Metrics

InstanceId	MetricName
<input checked="" type="checkbox"/> i-0cab5d3e	CPUUtilization
<input type="checkbox"/> i-0cab5d3e	DiskReadBytes
<input type="checkbox"/> i-0cab5d3e	DiskReadOps
<input type="checkbox"/> i-0cab5d3e	DiskWriteBytes
<input type="checkbox"/> i-0cab5d3e	DiskWriteOps
<input type="checkbox"/> i-0cab5d3e	NetworkIn
<input type="checkbox"/> i-0cab5d3e	NetworkOut
<input type="checkbox"/> i-0cab5d3e	StatusCheckFailed
<input type="checkbox"/> i-0cab5d3e	StatusCheckFailed_Instance

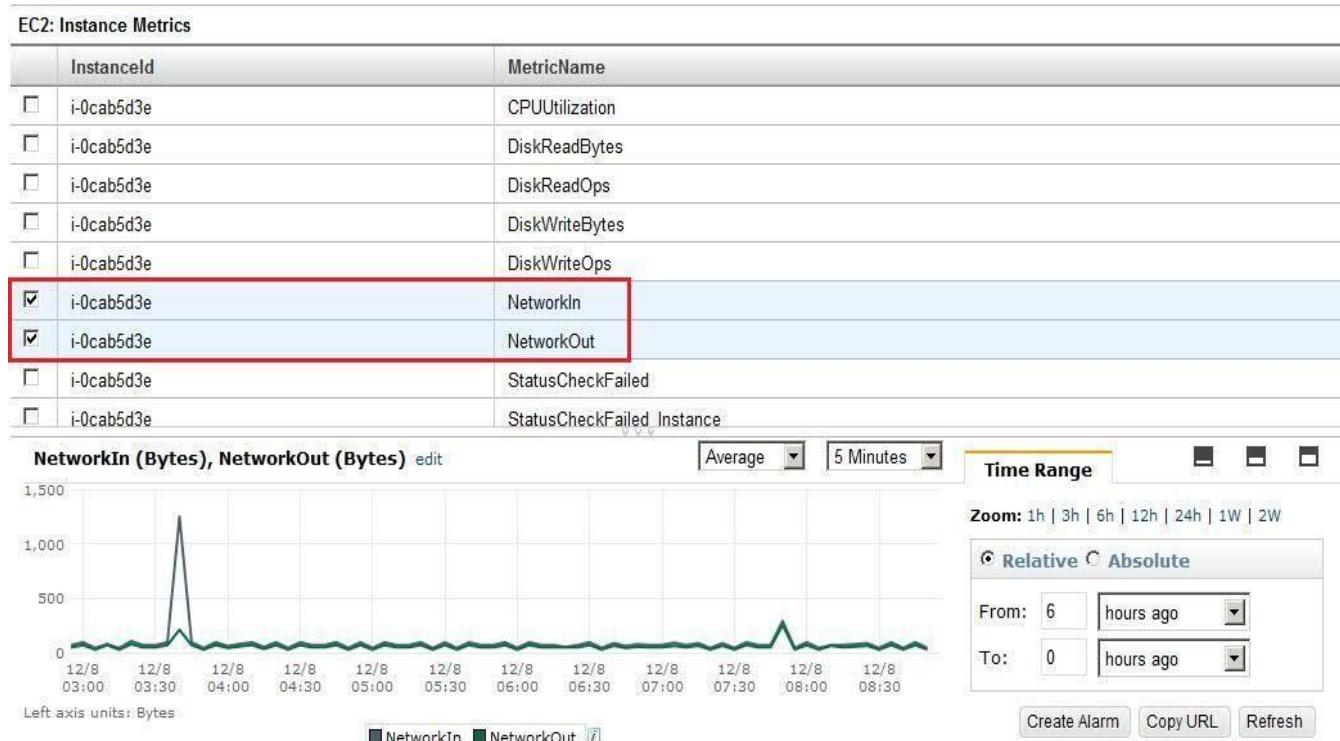


C3 SCHOOLS



|| C3 SCHOOLS

9. To view multiple metrics of the same instance, select those metrics.



C3 SCHOOLS

How to View AWS CloudWatch Aggregated Metrics Data for Multiple Instances

CloudWatch also provides APIs to get the aggregated data of multiple instances for which detailed monitoring is enabled. Instances that use basic monitoring are not included in the aggregates.

The following steps show how to view aggregated metrics data for detailed monitoring enabled [EC2 instances](#).



|| C3 SCHOOLS

10. Select “EC2: Aggregated Across Instances” from the “Viewing” drop down menu.

Screenshot of the AWS CloudWatch Metrics console showing the “Viewing” dropdown menu. The dropdown is set to “EC2: Instance Metrics” and is expanded to show “EC2: Aggregated Across Instances” selected. A list of metrics follows:

	MetricName
<input checked="" type="checkbox"/> i-0	CPUUtilization
<input type="checkbox"/> i-0	DiskReadBytes
<input type="checkbox"/> i-0	DiskReadOps
<input type="checkbox"/> i-0	DiskWriteBytes
<input type="checkbox"/> i-0	DiskWriteOps
<input type="checkbox"/> i-0cab5d3e	NetworkIn
<input type="checkbox"/> i-0cab5d3e	NetworkOut
<input type="checkbox"/> i-0cab5d3e	StatusCheckFailed
<input type="checkbox"/> i-0cab5d3e	StatusCheckFailed_Instance

11. It will list all the metrics available for Aggregated Statistics.

Screenshot of the AWS CloudWatch Metrics console showing the “MetricName” list. The “CPUUtilization” checkbox is highlighted with a red box.

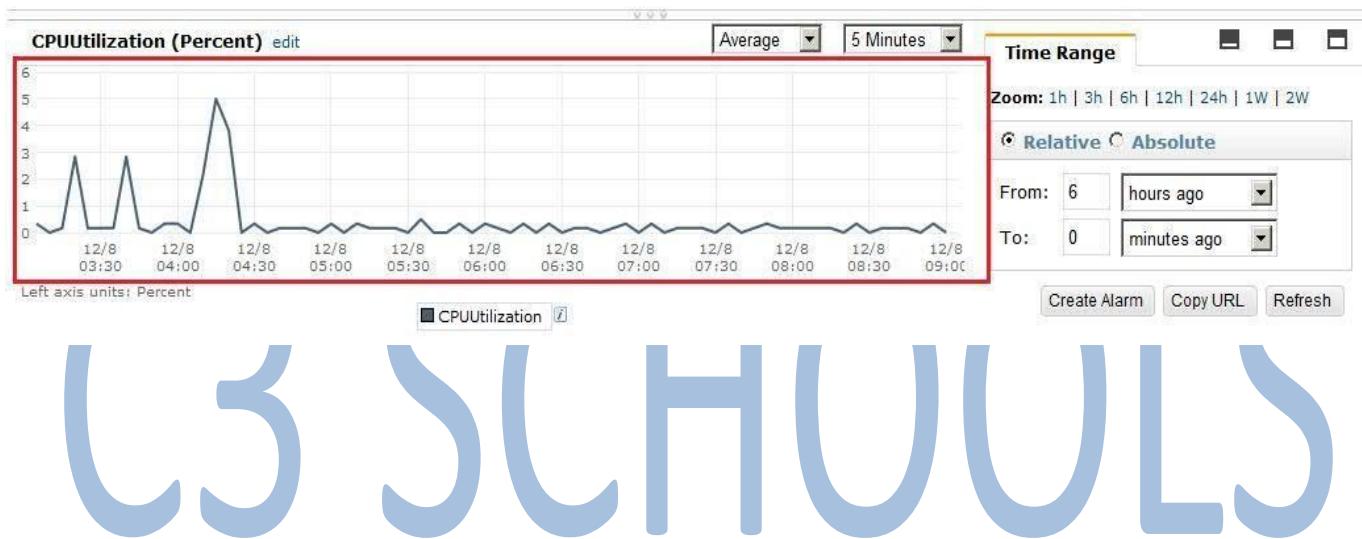
MetricName
<input type="checkbox"/> CPUUtilization
<input type="checkbox"/> DiskReadBytes
<input type="checkbox"/> DiskReadOps
<input type="checkbox"/> DiskWriteBytes
<input type="checkbox"/> DiskWriteOps
<input type="checkbox"/> NetworkIn
<input type="checkbox"/> NetworkOut



|| C3 SCHOOLS

12. If you select “CPUUtilization”, it will list the aggregated metrics collected for all the detailed monitoring enabled instances.

MetricName
<input checked="" type="checkbox"/> CPUUtilization
<input type="checkbox"/> DiskReadBytes
<input type="checkbox"/> DiskReadOps
<input type="checkbox"/> DiskWriteBytes
<input type="checkbox"/> DiskWriteOps
<input type="checkbox"/> NetworkIn
<input type="checkbox"/> NetworkOut



13. You can change the average time or Time Range as explained in steps #6 and #7.

14. As explained above, you can also get statistics for “Aggregated across ELB” ([Elastic Load Balancer](#)), “Aggregated by AutoScaling Group” (if auto scaling is created), “Aggregated by AMI” by selecting specific metrics from the drop down menu.



|| C3 SCHOOLS

Viewing:	EC2: Instance Metrics	Search
	All Metrics	
<input type="checkbox"/>	i-6 EBS: Volume Metrics	StatusCheckFailed
<input type="checkbox"/>	EC2: Aggregated Across Instances	StatusCheckFailed_Instance
<input type="checkbox"/>	i-6 EC2: Aggregated by Image (AMI) Id	StatusCheckFailed_System
<input type="checkbox"/>	i-6 EC2: Instance Metrics	CPUUtilization
<input type="checkbox"/>	EC2: Aggregated by Instance Type	DiskReadBytes
<input type="checkbox"/>	i-8 ELB: Aggregated Across All Load Balancers	DiskReadOps
<input type="checkbox"/>	ELB: Aggregated by Availability Zone	DiskWriteBytes
<input type="checkbox"/>	i-8 ELB: Load Balancers By Availability Zone	DiskWriteOps
<input type="checkbox"/>	ELB: Load Balancer Metrics	NetworkIn
<input type="checkbox"/>	i-81435db2	NetworkOut
<input type="checkbox"/>	i-81435db2	SlowQueryTime
<input type="checkbox"/>	i-81435db2	

C3 SCHOOLS



|| C3 SCHOOLS

15. If you want to get metrics statistics using the command line tool you will need to [install the CLI tools for CloudWatch](#).

Follow the steps and run the command below - First set the Region for the CloudWatch:

```
set AWS_CLOUDWATCH_URL=https://monitoring.us-west-2.amazonaws.com  
Run the command:
```

```
mon-get-stats CPUUtilization --start-time 2012-12-08T03:04:00 --end-time 2012-12-08T09:04:00 --  
-period 360 --namespace "AWS/EC2" --statistics "Maximum" --dimensions "InstanceId=i-0cab5d3e"
```

The above command shows the metrics collected during the last 6 hours for the specified instance. This is the same as we showed in step#5 through AWS graphic user interface console.



A screenshot of a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window contains the following text:

```
C:\>set AWS_CLOUDWATCH_URL=https://monitoring.us-west-2.amazonaws.com  
C:\>mon-get-stats CPUUtilization --start-time 2012-12-08T03:04:00 --end-time 2012-12-08T09:04:00 --  
-period 360 --namespace "AWS/EC2" --statistics "Maximum" --dimensions "InstanceId=i-0cab5d3e" --header  
Time Maximum Unit  
2012-12-08 03:04:00 1.67 Percent  
2012-12-08 03:10:00 0.0 Percent  
2012-12-08 03:16:00 1.67 Percent  
2012-12-08 03:22:00 0.0 Percent  
2012-12-08 03:28:00 1.67 Percent  
2012-12-08 03:34:00 0.0 Percent  
2012-12-08 03:40:00 28.33 Percent  
2012-12-08 03:46:00 0.0 Percent  
2012-12-08 03:52:00 1.67 Percent  
2012-12-08 03:58:00 0.0 Percent  
2012-12-08 04:04:00 1.67 Percent  
2012-12-08 04:10:00 0.0 Percent  
2012-12-08 04:16:00 1.64 Percent  
2012-12-08 04:22:00 0.0 Percent  
2012-12-08 04:28:00 0.0 Percent  
2012-12-08 04:34:00 1.67 Percent  
2012-12-08 04:40:00 0.0 Percent  
2012-12-08 04:46:00 1.64 Percent  
2012-12-08 04:52:00 0.0 Percent  
2012-12-08 04:58:00 1.67 Percent  
2012-12-08 05:04:00 0.0 Percent  
2012-12-08 05:10:00 1.69 Percent  
2012-12-08 05:16:00 0.0 Percent  
2012-12-08 05:22:00 1.64 Percent  
2012-12-08 05:28:00 0.0 Percent  
2012-12-08 05:34:00 1.64 Percent  
2012-12-08 05:40:00 0.0 Percent  
2012-12-08 05:46:00 0.0 Percent
```



|| C3 SCHOOLS

16. To get the aggregated data as shown in step #11 run the following command.

```
mon-get-stats CPUUtilization --start-time 2012-12-08T03:04:00 --end-time 2012-12-08T09:04:00 --period 360 --namespace "AWS/EC2" --statistics "Average,SampleCount" -headers
```

It will output the below -



```
C:\Administrator: C:\Windows\system32\cmd.exe
C:\>set AWS_CLOUDWATCH_URL=https://monitoring.us-west-2.amazonaws.com
C:\>mon-get-stats CPUUtilization --start-time 2012-12-08T03:04:00 --end-time 2012-12-08T09:04:00 --period 360 --namespace "AWS/EC2" --statistics "Average,SampleCount" --headers
time           SampleCount   Average          Unit
2012-12-08  03:04:00    12.0    0.2783333333333333 Percent
2012-12-08  03:10:00    12.0    0.1391666666666666 Percent
2012-12-08  03:16:00    12.0    0.1391666666666666 Percent
2012-12-08  03:22:00    12.0    2.2225 Percent
2012-12-08  03:28:00    12.0    0.2758333333333333 Percent
2012-12-08  03:34:00    12.0    0.1391666666666666 Percent
2012-12-08  03:40:00    12.0    2.360833333333333 Percent
2012-12-08  03:46:00    12.0    0.1391666666666666 Percent
2012-12-08  03:52:00    12.0    0.2783333333333333 Percent
2012-12-08  03:58:00    12.0    0.0 Percent
2012-12-08  04:04:00    12.0    0.2799999999999997 Percent
2012-12-08  04:10:00    12.0    2.625 Percent
2012-12-08  04:16:00    12.0    5.15083333333334 Percent
2012-12-08  04:22:00    12.0    1.38 Percent
2012-12-08  04:28:00    12.0    0.1391666666666666 Percent
2012-12-08  04:34:00    12.0    0.1391666666666666 Percent
2012-12-08  04:40:00    12.0    0.1408333333333334 Percent
2012-12-08  04:46:00    12.0    0.1366666666666666 Percent
2012-12-08  04:52:00    12.0    0.1408333333333334 Percent
2012-12-08  04:58:00    12.0    0.2758333333333333 Percent
2012-12-08  05:04:00    12.0    0.0 Percent
2012-12-08  05:10:00    12.0    0.2816666666666667 Percent
2012-12-08  05:16:00    12.0    0.1391666666666666 Percent
2012-12-08  05:22:00    12.0    0.1366666666666666 Percent
2012-12-08  05:28:00    12.0    0.1391666666666666 Percent
2012-12-08  05:34:00    12.0    0.4150000000000004 Percent
2012-12-08  05:40:00    12.0    0.0 Percent
2012-12-08  05:46:00    12.0    0.1391666666666666 Percent
2012-12-08  05:52:00    12.0    0.1391666666666666 Percent
```

Creating an Amazon CloudWatch Alarm

The following steps will instruct you on how to create an Amazon CloudWatch Alarm:

1) Firstly, you are required to select a metric for your alarm. To do so:

- You need to open the Amazon CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
- Now, in the “Navigation” pane, you should select Alarms.



|| C3 SCHOOLS

The screenshot shows the AWS CloudWatch Alarms interface. On the left, a sidebar lists various monitoring services: CloudWatch, Dashboards, Alarms (selected), ALARM (with 1 item), INSUFFICIENT (with 1 item), OK (with 1 item), Billing, Events, Rules, Logs, and Metrics (NEW). The main area has tabs for 'Create Alarm', 'Modify', 'Copy', and 'Delete'. A search bar at the top right says 'Search Alarms'. Below it is a table header with columns 'State', 'Name', 'Threshold', and 'Config Status'. A message 'No records found.' is displayed.

- Click on “Create Alarm”.
- On the “SELECT METRIC” page of the “Create Alarm Wizard”, you need to select “EC2: Aggregated by Auto Scaling Group” from the “Viewing” drop-down menu.

The screenshot shows the “Create Alarm” wizard, Step 1: Select Metric. The left pane lists metrics for “AutoScalingGroupName: myAS”, including CPUUtilization, CPUCreditBalance, CPUCreditUsage, DiskReadBytes, and DiskReadOps. The “CPUUtilization” metric is selected. The right pane contains a graph titled “CPUUtilization” with “Average” and “5 Minutes” settings. The graph displays a message: “No data available. Try adjusting the dashboard time range.”. The right pane also includes sections for “Update Graph”, “Time Range” (set to “Relative” from “12 hours ago” to “0 hours ago”), and “Left Y-axis” with “Limits” set to “Min: Auto” and “Max: Auto”. At the bottom are “Cancel”, “Previous”, “Next”, and “Create Alarm” buttons.



|| C3 SCHOOLS

- Now, you are required to click on the “**MyAutoScalingGroup/CPU Utilization**” row.
- Click on the “**Next**” button.

The “**DEFINE ALARM**” page of the “**Create Alarm Wizard**” will appear.

2) In this next step you will need to define the alarm.

- On the “**DEFINE ALARM**” page of the “**Create Alarm Wizard**”, type “MyHighCPUAlarm” in the “**Name**” box.
- Now, you are required to type a description in the “**Description**” box.
- In the “**Define Alarm Threshold**” section, you should select CPU Utilization \geq and type 60 in the box, and for 3 consecutive period.
- In Actions Where “**Whenever this alarm**” from drop-down menu Select “**State is INSUFFICIENT**”
- Where “**Send Notification to**” Create a New list or Select one from drop-down menu.
- Now, you will need to type a topic name in the “**Topic**” box, and an email address in the “**Emails List**” box.
- Select “**Period**” from drop-down menu accordingly, Then Select “**Statistic**” from drop-down menu Accordingly.

C3 SCHOOLS



|| C3 SCHOOLS

Create Alarm

1. Select Metric 2. Define Alarm

Alarm Threshold

Provide the details and threshold for your alarm. Use the graph on the right to help set the appropriate threshold.

Name: MyHighCPUAlarm

Description: CPU Utility Testing Alarm

Whenever: CPUUtilization

is: \geq 60

for: 3 consecutive period(s)

Actions

Define what actions are taken when your alarm changes state.

Notification

Whenever this alarm: State is INSUFFICIENT

Send notification to: CPUUtilization [Select list](#)

Email list: xxxxxxxx@outlook.in

[+ Notification](#) [+ AutoScaling Action](#) [+ EC2 Action](#)

Alarm Preview

This alarm will trigger when the blue line goes up to or above the red line for a duration of 15 minutes

CPUUtilization ≥ 60

Namespace: AWS/EC2

AutoScaling-
GroupName: myAS

Metric Name: CPUUtilization

Period: 5 Minutes

Statistic: Average

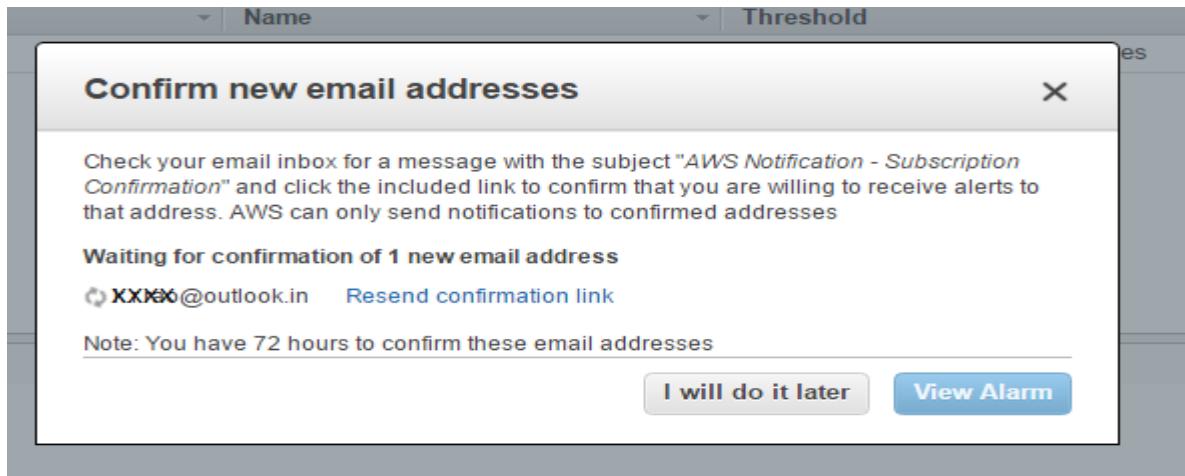
[Cancel](#) [Previous](#) [Next](#) **Create Alarm**

- 3) Click on the “Create Alarm” button.



|| C3 SCHOOLS

- 4) A confirmation window will appear, Once we confirm our *AWS Notification - Subscription Confirmation* and click the included link to confirm that you are willing to receive alerts to that address.



- 5) Click on the “View Alarm” button.

The confirmation window will close, and you will be returned to the CloudWatch page. Your new alarm will now appear on the list.

How to Send Alert Emails Based on Your AWS Instance CPU Usage Alarm

The following steps will instruct you on how to create an Amazon CloudWatch Alarm:

- 6) Firstly, you are required to select a metric for your alarm. To do so:

- You need to open the Amazon CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
- Now, in the “Navigation” pane, you should select Alarms.



|| C3 SCHOOLS

The screenshot shows the AWS CloudWatch Alarms interface. On the left, a sidebar lists various monitoring services: CloudWatch, Dashboards, Alarms (selected), ALARM (with 1 item), INSUFFICIENT (with 1 item), OK (with 1 item), Billing, Events, Rules, Logs, and Metrics (NEW). The main area has tabs for 'Create Alarm', 'Modify', 'Copy', and 'Delete'. A search bar at the top right says 'Search Alarms'. Below it is a table header with columns 'State', 'Name', 'Threshold', and 'Config Status'. A message 'No records found.' is displayed.

- Click on “Create Alarm”.
- On the “SELECT METRIC” page of the “Create Alarm Wizard”, you need to select “EC2: Aggregated by Auto Scaling Group” from the “Viewing” drop-down menu.

The screenshot shows the “Create Alarm” wizard, Step 1: Select Metric. The left pane lists metrics for “myAS”: CPUCreditBalance, CPUCreditUsage, CPUUtilization (selected), DiskReadBytes, and DiskReadOps. The right pane shows a graph titled “CPUUtilization” with “Average” and “5 Minutes” metrics. The graph displays a single data series “CPUUtilization” with a value of 0.00. A message “No data available. Try adjusting the dashboard time range.” is shown. The right side also includes “Update Graph” and “Time Range” controls.



|| C3 SCHOOLS

- Now, you are required to click on the “**MyAutoScalingGroup/CPU Utilization**” row.
- Click on the “**Next**” button.

The “**DEFINE ALARM**” page of the “**Create Alarm Wizard**” will appear.

7) In this next step you will need to define the alarm.

- On the “**DEFINE ALARM**” page of the “**Create Alarm Wizard**”, type “MyHighCPUAlarm” in the “**Name**” box.
- Now, you are required to type a description in the “**Description**” box.
- In the “**Define Alarm Threshold**” section, you should select CPU Utilization \geq and type 60 in the box, and for 3 consecutive period.
- In **Actions Where "Whenever this alarm"** from drop-down menu Select "**State is INSUFFICIENT**".
- Where "**Send Notification to**" Create a New list or Select one from drop-down menu.
- Now, you will need to type a topic name in the “**Topic**” box, and an email address in the “**Emails List**” box.
- Select "**Period**" from drop-down menu accordingly, Then Select "**Statistic**" from drop-down menu Accordingly.

C3 SCHOOLS



|| C3 SCHOOLS

Create Alarm

1. Select Metric 2. Define Alarm

Alarm Threshold

Provide the details and threshold for your alarm. Use the graph on the right to help set the appropriate threshold.

Name: MyHighCPUAlarm

Description: CPU Utility Testing Alarm

Whenever: CPUUtilization

is: \geq 60

for: 3 consecutive period(s)

Actions

Define what actions are taken when your alarm changes state.

Notification

Whenever this alarm: State is INSUFFICIENT

Send notification to: CPUUtilization [Select list](#)

Email list: xxxxxxxx@outlook.in

[+ Notification](#) [+ AutoScaling Action](#) [+ EC2 Action](#)

Alarm Preview

This alarm will trigger when the blue line goes up to or above the red line for a duration of 15 minutes

CPUUtilization ≥ 60

Namespace: AWS/EC2

AutoScaling-
GroupName: myAS

Metric Name: CPUUtilization

Period: 5 Minutes

Statistic: Average

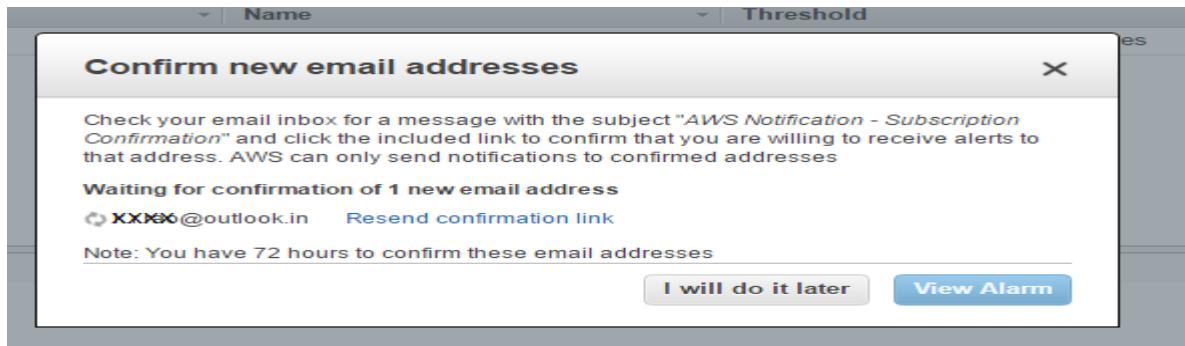
[Cancel](#) [Previous](#) [Next](#) **Create Alarm**

- 8) Click on the “Create Alarm” button.

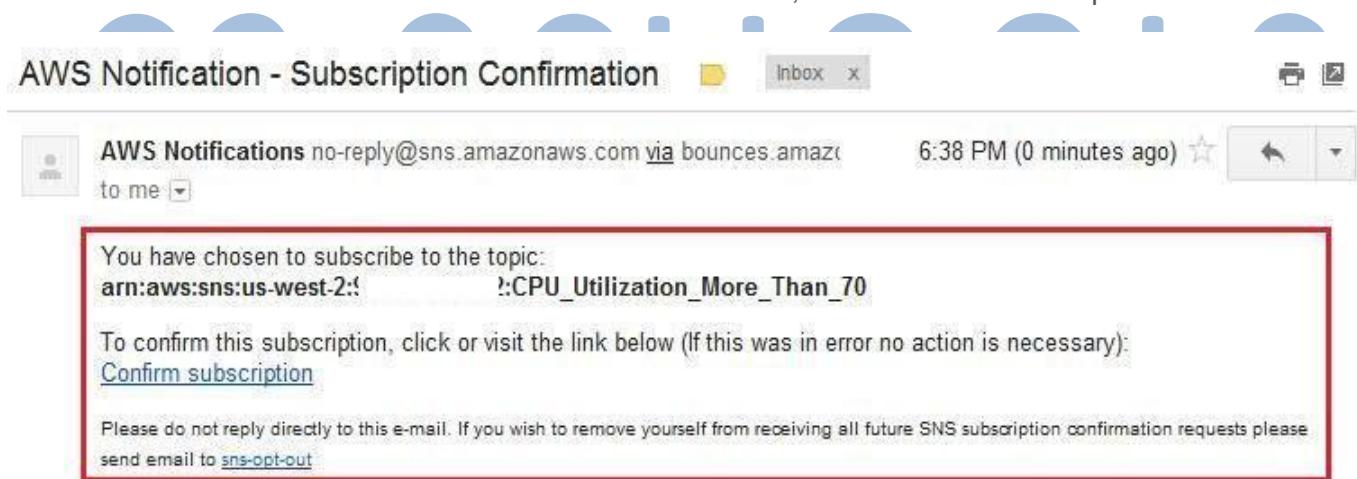


|| C3 SCHOOLS

- 9) A confirmation window will appear. Once we confirm our *AWS Notification - Subscription Confirmation* and click the included link to confirm that you are willing to receive alerts to that address.



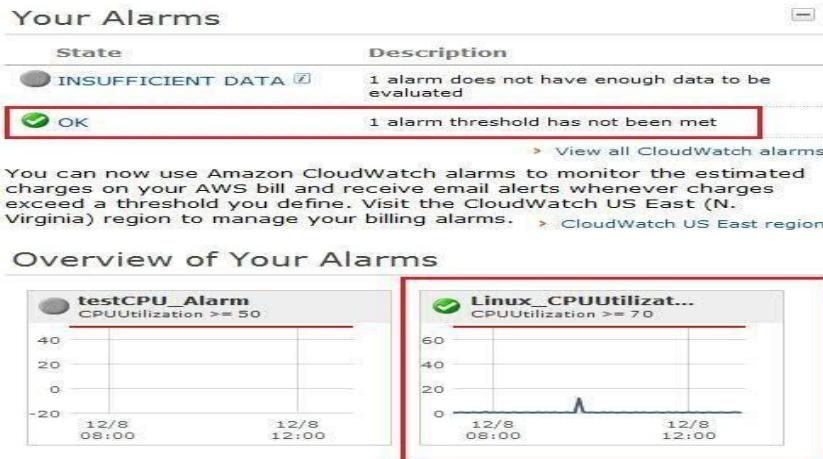
- 10) Click on the “View Alarm” button.
- 11) When the alarm is created and it is configured to send the email for any state, CloudWatch will send a confirmation mail to that email ID for verification. To confirm, click “Confirm Subscription”.



- 12) Click on CloudWatch dashboard inside the CloudWatch console. It will list the new alert as well as the current state of the alarm.



|| C3 SCHOOLS



- 13) If you want to set an alarm for some other metric other than CPU Utilization, select that metric instead of CPU Utilization in step#1 and configure the alarm as explained above.

Add a CloudWatch Alert Using the CLI Tools

1. If you want to add an alert using command line tool you need to [install CLI](#). You will also need the ARN ID of your SNS topic.

2. Run the commands below.

First set the Region for CloudWatch:

```
set AWS_CLOUDWATCH_URL=https://monitoring.us-west-2.amazonaws.com
```

Run command:

```
mon-put-metric-alarm --alarm-name cpu-monitor --alarm-description "Alarm sends Email when CPU exceeds 70" --metric-name CPUUtilization --namespace AWS/EC2 --statistic Average --period 60 --threshold 70 --comparison-operator GreaterThanThreshold --dimensions "InstanceId=i-06ab5d3e" --evaluation-periods 2 --unit Percent --alarm-actions arn:aws:sns:us-west-2:
```

The above command creates an alarm for CPU Utilization. If you want to change the state of the alarm manually try the following command:



|| C3 SCHOOLS

```
mon-set-alarm-state cpu-monitor --state-reason "initializing" --state-value OK
```

The above command changes the state of the alert to “OK”.

```
mon-set-alarm-state cpu-monitor --state-reason "testing" --state-value ALARM
```

The above command changes the state of the alert to “ALARM”.

3. The actual output of the above commands is shown below.



```
C:\>Administrator: C:\Windows\system32\cmd.exe
C:\>set AWS_CLOUDWATCH_URL=https://monitoring.us-west-2.amazonaws.com
C:\>mon-put-metric-alarm --alarm-name cpu-monitor --alarm-description "Alarm sends Email when CPU exceeds 70" --metric-name CPUUtilization --namespace AWS/EC2 --statistic Average --period 60 --threshold 70 --comparison-operator GreaterThanThreshold --dimensions "InstanceId=i-06ab5d3e" --evaluation-periods 2 --unit Percent --alarm-actions arn:aws:sns:us-west-2:████████:CPU_Utilization_More_Than_70
OK-Created Alarm
C:\>mon-set-alarm-state cpu-monitor --state-reason "initializing" --state-value OK
OK-Set alarm state value
C:\>
C:\>mon-set-alarm-state cpu-monitor --state-reason "testing" --state-value ALARM
OK-Set alarm state value
C:\>
```

We observed that sometimes although your syntax is correct the CloudWatch API throws an error message saying that the syntax is incorrect.

Check your environment variable through the set command. If it has any ARGV variable set, reset it with command

```
Set ARGV=
```

Note : We did provide a blank value to ARGV to reset it.

[How to Send Emails Alert Based on AWS Elastic Load Balancer Alarms](#)



|| C3 SCHOOLS

[Amazon CloudWatch](#) is used for basic monitoring of several AWS products. It monitors various services based on available [AWS cloud metrics](#).

This shows how to send an email based on an [ELB \(Elastic Load Balancer\)](#) metrics. Login to your AWS UI console and follow the next steps:

1. Go to the [AWS EC2](#) console and get the [Load Balancer details](#). Write down the [ELB Name](#).

The screenshot shows the AWS EC2 Load Balancers page. On the left, there's a sidebar with navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances (with sub-links for Instances, Spot Requests, Reserved 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 has tabs for Create Load Balancer, Actions, Filter (Search, 1 to 1 of 1), and a table of load balancers. The table shows one entry: MyTestELB, with details: DNS name: MyTestELB-1743859104.ap-south-1.elb.amazonaws.com, VPC ID: vpc-c2699dab, Availability Zones: ap-south-1b, ap-south-1a, Type: classic, and Created: November 11, 2016 at 1:51:16 PM UTC+5:30. Below the table, there's a section for Basic Configuration with fields: Name (MyTestELB), Creation time (November 11, 2016 at 1:51:16 PM UTC+5:30), Hosted zone (ZP97RAFLXTNZK), Status (2 of 2 instances in service), and VPC (vpc-c2699dab). Another section shows Port Configuration with a Port Configuration table (Port 80 (HTTP) forwarding to 80 (HTTP), Stickiness: Disabled) and an Edit stickiness button.



|| C3 SCHOOLS

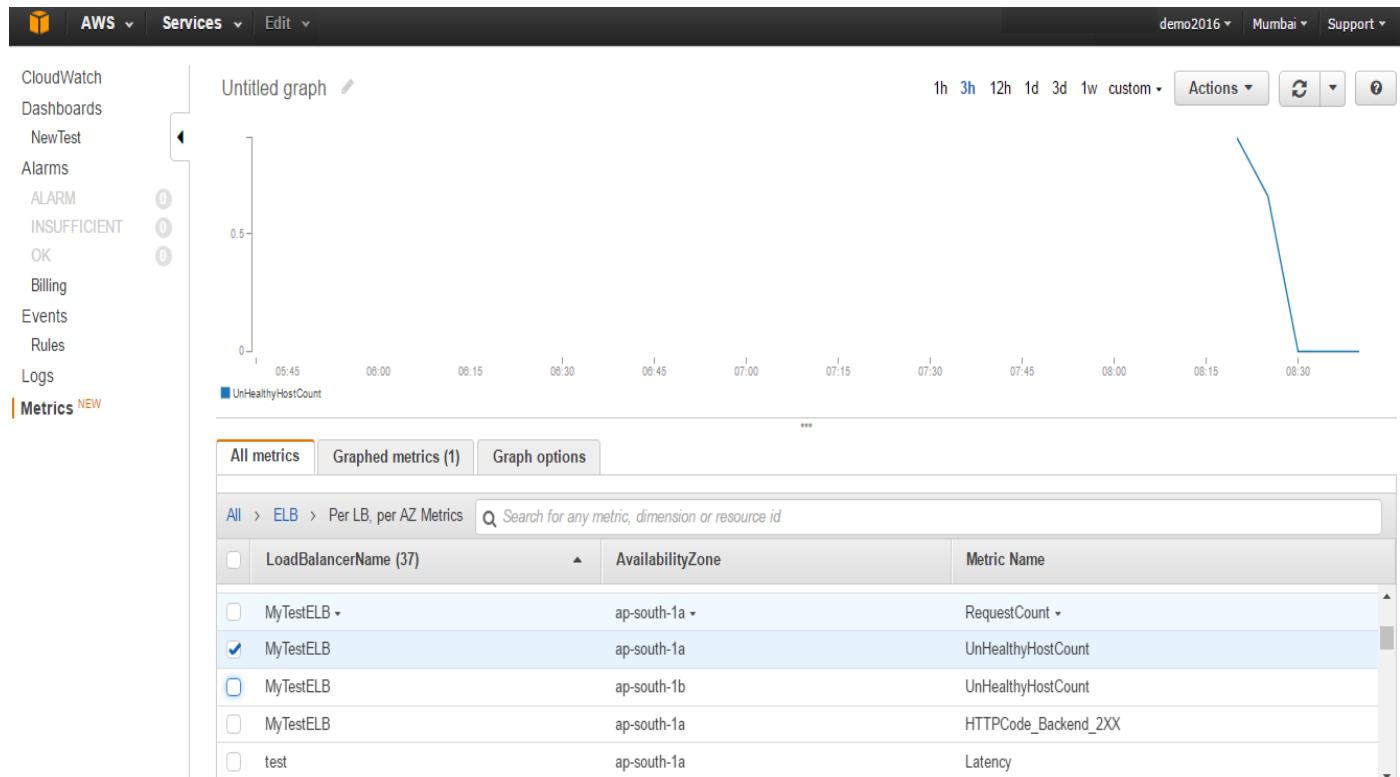
2. Enter the AWS CloudWatch console and select the AWS CloudWatch service. The dashboard list your present alarms as well as an overview of your AWS resources alarms. Click on “Browse Metrics”.

The screenshot shows the AWS CloudWatch Metrics Summary dashboard. At the top, there's a navigation bar with icons for Home, AWS, Services, Edit, demo2016, Mumbai, and Support. On the left, a sidebar menu under 'CloudWatch' includes options like Dashboards, NewTest, Alarms, ALARM (with 0 notifications), INSUFFICIENT (with 0 notifications), OK (with 0 notifications), Billing, Events, Rules, Logs, and Metrics (marked as NEW). The main content area has three sections: 'Metric Summary', 'Alarm Summary', and 'Service Health'. The 'Metric Summary' section displays a message about monitoring operational and performance metrics for AWS resources and applications, mentioning 1,132 metrics available in the Asia Pacific (Mumbai) region. It includes a 'Browse Metrics' button and a search bar. The 'Alarm Summary' section states that no alarms are created in the region and provides a 'Create Alarm' button. The 'Service Health' section shows a table with one row for the 'Amazon CloudWatch Service', indicating it is operating normally. Below the table, there are several blue semi-circular progress bars.

3. The metrics available with CloudWatch will be loaded. Select “ELB: Load Balancer Metrics” from the “Given Viewing List” .
4. The metrics available for all the ELBs in the current AWS region will be loaded. Select the ELB Name and any of its related metrics. It will show the graph of the selected metric at the Top.



|| C3 SCHOOLS



Click "Create Alarm" to set a new alarm for the selected ELB metric.

C3 SCHOOLS



|| C3 SCHOOLS

Click on Next after selecting required options....

5. Provide the metadata for defining the alert. Provide the Name and Description. In “Define Alarm Threshold”, provide the threshold value and period to have the alarm on.

In the case below we configured that if the ELB Unhealthy Host Count is more than 3 for 1 minutes the state of the alert will change to ALARM.

6. Configure the action for that alert. CloudWatch sends emails using the SNS service. Any CloudWatch alert has three stages,

1. State is ALARM,
2. State is OK
3. State is Insufficient.

You can set an action for each of the states. To send an email when the state is set to ALARM, select the state as “State is ALARM”, then in “Action” specify “Sending Email” in “Topic”, then click on New List.



|| C3 SCHOOLS

7. It will ask you for the email address which will receive the message. Provide one or multiple email IDs (comma separated). Click “Continue”.

Create Alarm

1. Select Metric 2. Define Alarm

Name: ELBInstanceUnhealthy

Description: Send Email when ELB Instance Unhealthy

Whenever: UnHealthyHostCount
is: \geq 3
for: 2 consecutive period(s)

Actions

Define what actions are taken when your alarm changes state.

Notification

Whenever this alarm: State is ALARM

Send notification to: Sending Mail Select list

Invalid notification list name, allowed characters are letters (a-z, A-Z), numbers (0-9), and underscore (_).

Email list:

+ Notification + AutoScaling Action + EC2 Action

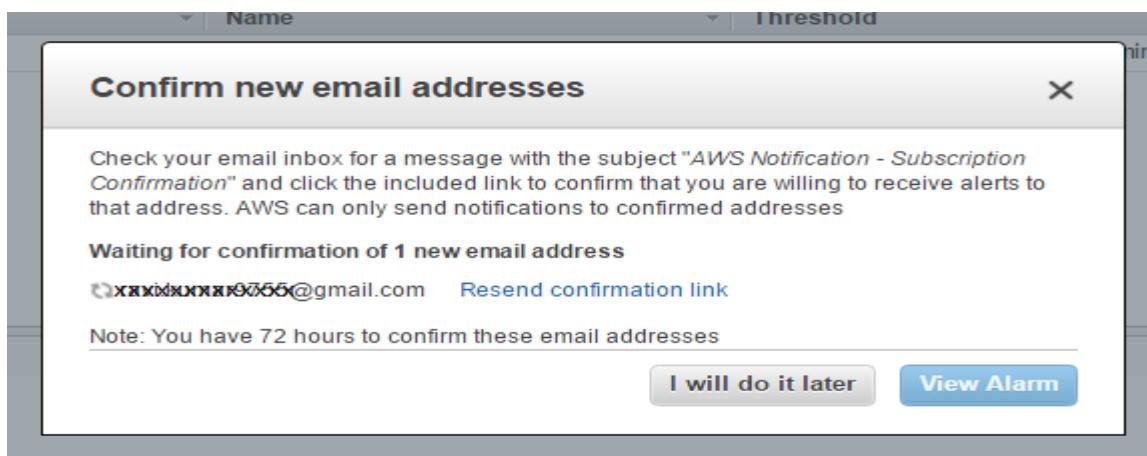
Namespace: AWS/ELB
Availability-Zone: ap-south-1a
LoadBalancer-Name: MyTestELB
Metric Name: UnHealthyHostCount
Period: 1 Minute
Statistic: Average

Cancel Previous Next **Create Alarm**

8. Review all the parameters you provided in the previous screen. If all the parameters are correct click “Create Alarm”. On the confirmation page click “I Will do it later” or after confirming email link it will show view Alarm button then click on it.



|| C3 SCHOOLS



- Click on “Alarms” in left menu of the CloudWatch console. Your new alert will be shown with its current state.

State	Name	Threshold
OK	ELBInstanceUnhealthy	UnHealthyHostCount >= 3 for 2 minutes

- When the alarm is created and configured to send emails for any state, CloudWatch sends a confirmation email verification to the assigned email. Acknowledge by clicking “Confirm Subscription”.



|| C3 SCHOOLS

AWS Notification - Subscription Confirmation Inbox

AWS Notifications no-reply@sns.amazonaws.com via bounces.amazonaws.com to me 11:46 PM (0 minutes ago)

You have chosen to subscribe to the topic:
arn:aws:sns:us-west-2:t-----2:SendEmail

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
[Confirm subscription](#)

Please do not reply directly to this e-mail. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send email to [sns-opt-out](#).

11. Once you confirmed the subscription, you will be forwarded to the following screen.

Subscription confirmed!

You have subscribed [youremail@gmail.com](#) to the topic:
SendEmail.

Your subscription's id is:
arn:aws:sns:us-west-2:t-----2:SendEmail:475d084d-d49b-40cb-a28d-beff6ab056fe

If it was not your intention to subscribe, [click here to unsubscribe](#).

12. If you want to set alarm an for any other metric than Unhealthy Host Count, select that metric instead of Unhealthy Host Count in step#4 and configure the alarm as shown above. [Check the list of all the available metrics for any AWS service](#)

Generate Emails Alerts Based on AWS ELB Alarms using the AWS CLI (command line tools)

13. If you want to add an alert using the command line tool you need to [install CLI](#). You will also need to get the ARN ID of your SNS topic.

14. Run the commands below.

Start by setting the Region for CloudWatch:

```
set AWS_CLOUDWATCH_URL=https://monitoring.us-west-2.amazonaws.com
```

Run the command:



|| C3 SCHOOLS

```
mon-put-metric-alarm --alarm-name elb-unhelathy --alarm-description "Alarm sends Email when ELB Unhealthy Count Increases" --metric-name UnHealthyHostCount --namespace AWS/ELB --statistic Average --period 120 --threshold 3 --comparison-operator GreaterThanThreshold --dimensions "LoadBalancerName=CloudWatchAlarm" --evaluation-periods 2 --unit Count --alarm-actions arn:aws:sns:us-west-2:xxxxxxxxxxxx:SendEmail
```

The above command creates an alarm for CPU Utilization. If you want to change the state of the alarm manually, try the following command:

```
mon-set-alarm-state elb-unhelathy --state-reason "initializing" --state-value OK
```

The above command changes the state of the alert to “OK”.

```
mon-set-alarm-state elb-unhelathy --state-reason "testing" --state-value ALARM
```

The above command changes the state of the alert to “ALARM”.

15. The actual output of all the above commands is shown below.

The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The user has run several commands related to CloudWatch Metrics and Alarms:

- Set the environment variable `AWS_CLOUDWATCH_URL` to `https://monitoring.us-west-2.amazonaws.com`.
- Created a metric alarm named `elb-unhelathy` with the following configuration:
 - Alarm description: "Alarm sends Email when ELB Unhealthy Count Increases"
 - Metric name: `UnHealthyHostCount`
 - Namespace: `AWS/ELB`
 - Statistic: `Average`
 - Period: 120
 - Threshold: 3
 - Comparison operator: `GreaterThanThreshold`
 - Dimensions: "LoadBalancerName=CloudWatchAlarm"
 - Evaluation periods: 2
 - Unit: Count
 - Actions: `arn:aws:sns:us-west-2:xxxxxxxxxxxx:SendEmail`
- Set the state of the alarm to "OK" with reason "initializing".
- Set the state of the alarm to "ALARM" with reason "testing".
- Described the alarm `elb-unhelathy`, showing it is in state `OK` and has the specified configuration.

We observed that sometimes although your syntax is correct the CloudWatch API throws an error message saying that the syntax is incorrect.

Check your environment variable through the set command. If it has any ARGV variable set, reset it with command:

```
Set ARGV=
```

Note : We did not provide a blank value to ARGV to reset it.



|| C3 SCHOOLS

16. If the Alarm state gets changed to ALERT it will send an email to to email ID configured in the SNS topic or mentioned in step#7 as shown below.

AWS Notifications no-reply@sns.amazonaws.com via bounces.amazonaws.com to me 12:13 AM (15 hours ago)

You are receiving this email because your Amazon CloudWatch Alarm "elb-unhelathy" in the US-West-2 region has entered the ALARM state, because "testing" at "Monday 10 December, 2012 18:43:29 UTC".

View this alarm in the AWS Management Console:
<https://console.aws.amazon.com/cloudwatch/home?region=us-west-2#s=Alarms&alarm=elb-unhelathy>

Alarm Details:

- Name:	elb-unhelathy
- Description:	Alarm sends Email when ELB Unhealthy Count Increases
- State Change:	OK -> ALARM
- Reason for State Change:	testing
- Timestamp:	Monday 10 December, 2012 18:43:29 UTC

How to Monitor Estimated AWS Charges and Create Billing Alarms

Amazon Web Services charge you on a pay as you go model. AWS will charge you for different AWS services based on the usage hours, data transfer or data storage.

This guide shows how to enable billing monitoring and to create a billing alarm.

1. Go to [AWS Account](#) section. Click “Account Activity” in the left navigation menu.



|| C3 SCHOOLS

[Sign Up](#)[My Account / Console](#)[English](#)[AWS Products & Solutions](#)[AWS Product Information](#)[Developers](#)[Support](#)

Account

- [Account Activity](#)
- [AWS Identity and Access Management](#)
- [AWS Management Console](#)
- [Consolidated Billing](#)
- [DevPay](#)
- Manage Your Account**
- [Payment Method](#)
- [Personal Information](#)
- [Security Credentials](#)
- [Usage Reports](#)
- [Billing Alerts](#)
- [Billing Preferences](#)

Cost Allocation Report

- [Manage Cost Allocation Report](#)

Manage Your Account

Welcome
Account Number | Sign Out

Services You're Signed Up For

Amazon CloudFormation	Amazon Simple Queue Service (SQS)
Amazon CloudFront	Amazon Simple Storage Service (S3)
Amazon CloudSearch	Amazon Simple Workflow Service (SWF)
Amazon CloudWatch	Amazon SimpleDB
Amazon DynamoDB	Amazon Virtual Private Cloud (VPC)
Amazon Elastic Compute Cloud (EC2)	Auto Scaling
Amazon Elastic MapReduce	AWS Direct Connect
Amazon ElastiCache	AWS Elastic Beanstalk
Amazon Glacier	AWS Import/Export
Amazon Mechanical Turk	AWS Storage Gateway
Amazon Relational Database Service (RDS)	Consolidated Billing
Amazon Route 53	Elastic Block Store (EBS)
Amazon Simple Email Service (SES)	Elastic Load Balancing
Amazon Simple Notification Service (SNS)	Product Advertising API

2. Click "Enable Now" to begin setting the alarm on exceeded usage.

[AWS Products & Solutions](#)[AWS Product Information](#)[Developers](#)[Support](#)

Account

- Account Activity**
- [AWS Identity and Access Management](#)
- [AWS Management Console](#)
- [Consolidated Billing](#)
- [DevPay](#)
- Manage Your Account**
- [Payment Method](#)
- [Personal Information](#)

Account Activity

Welcome
Account Number | Sign Out

You are eligible for the AWS Free Usage Tier. See the Getting Started Guide AWS Free Usage Tier to learn how to get started with the free usage tier.

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

3. When you enable the monitoring of your estimated charges for the first time, it takes about 15 minutes before you can view the billing data and set the billing alarms using the Amazon CloudWatch console.

Once it becomes available, click "Set your first billing alert".



|| C3 SCHOOLS

Account

- Account Activity
- AWS Identity and Access Management
- AWS Management Console
- Consolidated Billing

Account Activity

Welcome

| Sign Out

Account Number

Your account is enabled for monitoring estimated charges. Set your first billing alert to receive an e-mail when charges reach a threshold you define. Learn More

4. It will show the confirmation page explaining that you will receive an alert via email once the usage is more than the specified limit. Click 'Create Alarm'.



5. On the "Create Alarm" page, specify the AWS SNS Topic Name (can be any name), email address to receive the alert email, the threshold limit for billing usage and the name of the alarm. Here we specified that when billing exceeds \$5000, it should send an email to the specified email address. [\[xxxxx@gmail.com\]](mailto:xxxxx@gmail.com).

On the right side it shows the current as well as the estimated charge (\$5000) graph. The blue line is the actual usage while the red line shows the estimated amount specified. [\$5000]. Click "Create Alarm".



|| C3 SCHOOLS

Create Billing Alarm

Create an Amazon CloudWatch alarm to receive alerts via e-mail whenever estimated charges on your AWS bill exceed a threshold you define. The actual charges you will be billed in this statement period may differ from the charges shown on the notification. [Learn more.](#)

To create an alarm, first choose whom to notify and then define when the notification should be sent

Send a notification to:

Notifications use Amazon Simple Notification Service (SNS) topics that you can use for this and other alarms. Keep the default topic, or select or create your own.

With these recipients:

List up to 10 email addresses, separated by commas, to subscribe to this topic.

Whenever charges for:

Exceed:

Last statement period: USD 5537.30 - AWS Service Charges (total)

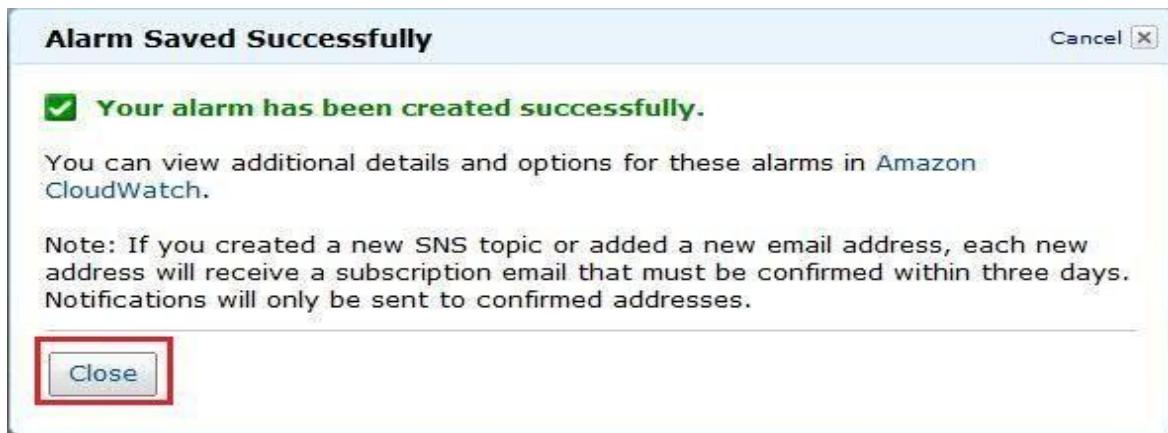
Name this alarm:

C3 SCHOOLS



|| C3 SCHOOLS

6. The alarm will be created and AWS will show the acknowledgement page. Click “Close” after you read the information.



7. It will show the Alarm details. Click “Close”.

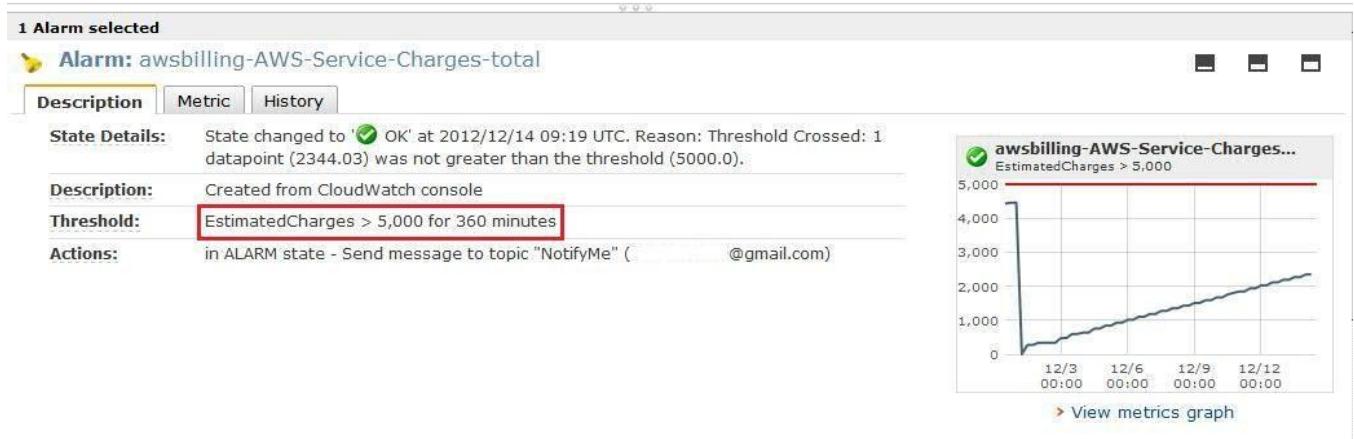


8. Go to the AWS CloudWatch console. Click on “Alerts”. It will list the new Billing Alert along with the existing alarms. When creating a new Alert, CloudWatch selects 6 Hours (360 minutes) as the default period. You should not change it.



C3 SCHOOLS

State	Name	Threshold
<input checked="" type="checkbox"/> OK	awsbilling-AWS-Service-Charges-tot	EstimatedCharges > 5,000 for 360 minutes



9. On the creation of the alert, it will send an email to the user acknowledging the subscription.

AWS Notification - Subscription Confirmation Inbox X

AWS Notifications no-reply@sns.amazonaws.com via bounces.amazon.com to me 2:49 PM (1 minute ago) Star Print Email

You have chosen to subscribe to the topic:
arn:aws:sns:us-east-1:-----?NotifyMe

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
[Confirm subscription](#)

Please do not reply directly to this e-mail. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send email to [sns-opt-out](#)

10. Click "Confirm subscription".



The screenshot shows an email from Amazon Web Services confirming a subscription. The subject is "Subscription confirmed!". The body of the email states: "You have subscribed [REDACTED]@gmail.com to the topic: [NotifyMe](#). Your subscription's id is: arn:aws:sns:us-east-1:a91f-48d1-8b00-1a10098b7cff". It also includes a link to unsubscribe: "If it was not your intention to subscribe, [click here to unsubscribe](#)".

11. When your estimated charge exceeds \$5000, it will send an email to the email address confirmed in step#10.

Autoscaling LAMP in AWS series, let's discuss how to create autoscaling launch configuration, autoscaling groups and how to verify the setup autoscaling.

Autoscale Implementation

Autoscale configuration is now available in console. AWS command lines are no longer needed for implementation.

Complete the following steps in order to set up autoscaling :

- Configure AMI to launch the Instances.
- Configure Instance type to launch the instances. (T2.micro)
- Configure KeyPair Name to access the machines.
- Configure Security Group to allow the Instances to communicate with other components.
- Keep the ELB name readily available.
- Keep your availability zones ready. (Example: us-east-1a, us-east-1b).



|| C3 SCHOOLS

- Set the minimum number of instances for Maximum and Desired Capacity. (Start with zero).
- Set Health Check Type. (ELB).
- Set Region.
- Change Capacity Cooldown time.
- Adjust for scale up and scale down.

1. Create the Autoscaling Launch Config

Log in to the AWS console and navigate to Services-> EC2-> Launch Configuration.



Click on "Create Autoscaling Group".

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.

On the next screen, click on "Create Launch Configuration".



|| C3 SCHOOLS

Create Auto Scaling Group

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 additional instances will be terminated if required.

Cancel Create launch configuration

Create a new launch configuration. The name of the launch configuration must be unique within the scope of the client's AWS account.

Choose AMI: Go to My AMIs and select the LAMP AMI created.

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

Cancel and Exit

Create Launch Configuration

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 Search my AMIs

AWS Marketplace

Community AMIs

Ownership

Owned by me

Shared with me

Architecture

LAMP_AMI_v1.0_29092013 - ami-a04ea6d7

LAMP_AMI_v1.0_29092013

Root device type: ebs Virtualization type: paravirtual Owner: 547978464708

Select

64-bit

Choose Instance Type: We've selected a micro instance for our example.



|| C3 SCHOOLS

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

Create Launch Configuration

Currently selected: t1 micro (up to 2 ECUs, 1 vCPUs, 0.613 GB memory, EBS only)

All instance types	Micro instances						
Micro instances							
General purpose	Size	ECUs	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
Memory optimized	t1.micro	up to 2	1	0.613	EBS only	-	Very Low
Storage optimized							
Compute optimized							

Micro instances are eligible for the AWS free usage tier. For the first 12 months following your AWS sign-up date, you get up to 750 hours of micro instances each month. When your free usage tier expires or if your usage exceeds the free tier restrictions, you pay standard, pay-as-you-go service rates.

Learn more about free usage tier eligibility and restrictions

Cancel Previous Next: Configure details

Configure Details: Give a name for the Launch Configuration

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

Create Launch Configuration

Name: lamp-launch-1

Purchasing option: Request Spot Instances

IAM role: None

Monitoring: Enable CloudWatch detailed monitoring

Advanced Details: 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

Add Storage: Keep the values on default.

Configure the Security Group: Select the Security group to launch the autoscaling instances. Review the details and create the Launch Configuration.



C3 SCHOOLS

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

Create Launch Configuration

Root device type: ebs Virtualization Type: paravirtual

Instance Type

Instance Type	ECUs	vCPUs	Memory GiB	Instance Storage (GiB) GiB	EBS-Optimized Available	Network Performance
t1.micro	up to 2	1	0.613	EBS only	-	Very Low

Launch configuration details

Name	lamp-launch-1	Edit details	
Purchasing option	On demand		
EBS Optimized	No		

Cancel Previous Create launch configuration

In the next window, select "KeyPair" to access the instances.

2. Create the Auto Scaling Group

Create a new Auto Scaling group with a specified name and other attributes. When you make the creation request, the Auto Scaling group is ready for use in other calls.

Navigate to EC2-> Auto Scaling Groups-> Create Autoscaling Group.

Select the existing Launch Configuration (lamp-launch-1) and go to "Next Step".

Create Auto Scaling Group

Cancel and Exit

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.

Create a new launch configuration

Create an Auto Scaling group from an existing launch configuration

Filter launch configurations... 1 to 1 of 1 Launch Configurations

Name	AMI ID	Instance Type	Spot Price	Security Groups
lamp-launch-1	ami-a04ea6d7	t1.micro		sg-f0eaa7b7

Cancel Next Step

Configure Autoscaling Group Details:

Give a name to the Auto Scaling Group.



Group Size: Start with zero instances in order to avoid the immediate creation of instances. The exact number of required instances can be set after these steps are completed, but just set cost optimization values to 0 for now.

Availability Zones:

Choose 2 availability zones in order to maintain high availability.

In "Advanced Details" choose the values as shown below.

1. Configure Auto Scaling group details 2. Configure scaling policies 3. Configure Notifications 4. Review

Create Auto Scaling Group

Launch Configuration (i) lamp-launch-1

Group name (i)

Group size (i) Start with instances

Network (i) Do not launch into a VPC C Create new VPC

Availability Zone(s) (i) eu-west-1a x eu-west-1b x

▼ Advanced Details

Load Balancing (i) Receive traffic from Elastic Load Balancer(s)

Health Check Type (i) ELB EC2

Health Check Grace Period (i) seconds

Monitoring (i) Amazon EC2 Detailed Monitoring metrics, which are provided at 1 minute frequency, are not enabled for the launch configuration lamp-launch-1. Instances launched from it will use Basic Monitoring metrics, provided at 5 minute frequency.
[Learn more](#)

Configure Scaling Policies: Keep minimum and maximum instances count to zero.

Increase Group Size: Keep the name at default.

Execute Policy: Click on "Add new alarm".



|| C3 SCHOOLS

The screenshot shows the 'Create Auto Scaling Group' wizard at step 2. The 'Increase Group Size' policy is selected. The 'Add new alarm' button is highlighted with a red box.

A popup window will appear for creating a "Cloud Watch Alarm".

The screenshot shows the 'Create Alarm' dialog box. The 'Whenever' section is highlighted with a red box. The 'Name of alarm' field contains 'awsec2-lamp-asg-1-High-CPU-Utilization'. On the right, there's a chart titled 'CPU Utilization Percent' showing data for 'lamp-asg-1' from 12/25 14:00 to 18:00. The 'Create Alarm' button is highlighted with a red box.

For this example, we chose CPU Load average as the autoscaling trigger. Whenever the average CPU load of app servers goes beyond 75% for 5 minutes, autoscaling will trigger the auto-scale-up-policy to launch the 1 instance and attach to load balancer. The application here is CPU intensive and requires more computing power, so we chose the CPU Load Average as the autoscale triggering event.

You can choose any Cloudwatch metric to trigger the autoscaling policy. For example, Disk read/writes, Network In/Out, ELB request count, ELB latency, etc.

Decrease Group size:



Create Alarm

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define. To edit an alarm, first choose whom to notify and then define when the notification should be sent.

Send a notification to: No SNS topics found...

Whenever: Average of CPU Utilization
Is: <= 45 Percent

For at least: 1 consecutive period(s) of 5 Minutes

Name of alarm: awsec2-lamp-asg-1-High-CPU-Utilizatio

CPU Utilization Percent

12/25 12/25 12/25
14:00 16:00 18:00

Cancel

Configure Notifications: If you've already created notifications, select one to receive the notifications of Autoscaling events, else skip this step for now.

Review the details and click on "Create Autoscaling Group".

Auto Scaling evaluates the health of each Amazon EC2 instance in the Auto Scaling Group and automatically replaces unhealthy instances in order to keep the Auto Scaling Group size fixed. That ensures that the application is getting the expected compute capacity.

In this example, we've chosen to scale down the environment when the average CPU load lowers to 40% for 5 minutes.

Verify Autoscaling

After completing the previous steps, it's time to test autoscaling.

1. Update the Autoscaling group minimum and maximum instances count to 2 and 4. You can change these later to fit your specific requirements.

Navigate to EC2-> Auto Scaling Group- > lamp-asg-1.

Right click on "lamp-asg-1" and select "Edit".

In the "Details" tab, update Desired Min and Max values to 1, and then save.



C3 SCHOOLS

Auto Scaling Group: lamp-asg-1

Launch Configuration: lamp-launch-1

Load Balancers: lamp-lb

Desired: 1

Min: 1

Max: 1

Health Check Type: ELB

Health Check Grace Period: 300

Termination Policies: Default

Creation Time: Thu Dec 26 01:10:26 GMT+530 2013

Availability Zone(s): eu-west-1a x eu-west-1b x

Default Countdown: 300

Placement Group:

Suspended Processes:

Enabled Metrics:

Save

Now, navigate to Services->EC2->Instances.

You can see that a new instance has been launched and attached to ELB.

Launch Instance Connect Actions

Filter: All instances All instance types Search instances

Name	Instance ID	Instance Type	Availability Zone	Status Checks	Alarm Status	Public DNS	Public IP	Key Name	Launch Time	Security G
i-cae6bb85	t1.micro	eu-west-1b	running	Initializing	none	elb-54-229-21-96.eu...	54.229.21.96	LAMP_KEY	2013-12-26T...	LAMP_SG

1 Load Balancer selected

Load Balancer: lamp-lb

Description Instances Health Check Monitoring Security Listeners

Instances

Instance	Name	Availability Zone	Status	Actions
i-cae6bb85	empty	eu-west-1b	Out of Service (why?)	Remove from Load Balancer

Availability Zones

Availability Zone	Instance Count	Healthy?	Actions
eu-west-1a	0	No (why?)	-

If your health check is configured properly, the instance status will turn into "In Service" rather quickly. Always have a minimum of 2 instances running in order to maintain high availability.

2. How to Update Launch Configuration: It's not possible to update the existing Launch configuration, so you'll have to create a new Launch configuration and edit the Autoscaling Group to use that new configuration.



Auto Scaling Group: lamp-asg-1

Details Scaling History Scaling Policies Instances Notifications Cancel

Launch Configuration: lamp-launch-2

Load Balancers: lamp-lb

Desired: 1

Min: 1

Max: 1

Health Check Type: ELB

Health Check Grace Period: 300

Termination Policies: Default

Creation Time: Thu Dec 26 01:10:26 GMT+530 2013

Availability Zone(s): eu-west-1a, eu-west-1b

Default Cooldown: 300

Placement Group:

Suspended Processes:

Enabled Metrics:

Now, start the application load run and find out the minimum and maximum instances required for your application to handle the load. Then update the AutoScaling Group to meet your needs.

Amazon Route 53

Hands On

We can use Amazon Route 53 to register new domains, transfer existing domains, route traffic for your domains to your AWS and external resources, and monitor the health of your resources.

Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service. Amazon Route 53 performs three main functions:

- **Domain registration** – Amazon Route 53 helps lets you register domain names such as example.com.
- **Domain Name System (DNS) service** – Amazon Route 53 translates friendly domains names like www.example.com into IP addresses like 192.0.2.1. Amazon Route 53 responds to DNS queries using a global network of authoritative DNS servers, which reduces latency.
- **Health checking** – Amazon Route 53 sends automated requests over the Internet to your application to verify that it's reachable, available, and functional.

1. Go to Amazon Web Services Console then Click on Route 53 under Networking you will see Route 53 page like below if you haven't created or entered this page. Click on Get Started Now under DNS Management



|| C3 SCHOOLS

AWS Services Edit demo2016 Global Support



Amazon Route 53

You can use Amazon Route 53 to register new domains, transfer existing domains, route traffic for your domains to your AWS and external resources, and monitor the health of your resources.


DNS management

If you already have a domain name, such as example.com, Route 53 can tell the Domain Name System (DNS) where on the Internet to find web servers, mail servers, and other resources for your domain.
[Learn More](#)

[Get started now](#)


Traffic management

Route 53 traffic flow provides a visual tool that you can use to create and update sophisticated routing policies to route end users to multiple endpoints for your application.
[Learn More](#)

[Get started now](#)


Availability monitoring

Route 53 can monitor the health and performance of your application as well as your web servers and other resources. Route 53 can also redirect traffic to healthy resources.
[Learn More](#)

[Get started now](#)

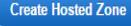

Domain registration

If you need a domain name, you can find an available name and register it by using Route 53. You can also make Route 53 the registrar for existing domains that you registered with other registrars.
[Learn More](#)

[Get started now](#)

2. After Clicking we will see Route 53 Page as Below

AWS Services Edit demo2016 Global Support

 Go to Record Sets Delete Hosted Zone


Amazon Route 53 is an authoritative Domain Name System (DNS) service. DNS is the system that translates human-readable domain names (example.com) into IP addresses (192.0.2.0). With authoritative name servers in data centers all over the world, Route 53 is reliable, scalable, and fast.

If you already have a domain name, such as example.com, Route 53 can tell the Domain Name System (DNS) where on the Internet to find web servers, mail servers, and other resources for your domain.
[Learn More](#)

[Create Hosted Zone](#)



C3 SCHOOLS

- Creates a new public hosted zone, used to specify how the Domain Name System (DNS) routes traffic on the Internet for a domain, such as example.com, and its sub domains. To create new hosted zone click on the Hosted zones in the Dashboard then "Create Hosted Zone"

Enter Domain Name in the field given, write comment if necessary, and select Type of Zone Required...

then Click on "Create"

The screenshot shows the AWS CloudFront service dashboard. On the left, there's a sidebar with links like Dashboard, Hosted zones (which is selected and highlighted in orange), Health checks, Traffic flow, Traffic policies, Policy records, Domains, Registered domains, and Pending requests. The main content area has a header with 'Create Hosted Zone', 'Go to Record Sets', and 'Delete Hosted Zone'. Below that is a search bar and a filter section with dropdowns for 'Domain Name', 'Type', 'Record Set Count', and 'Comment', and a 'Hosted Zone ID' dropdown. A message says 'You have no hosted zones'. On the right, a modal window titled 'Create Hosted Zone' is open. It contains a description: 'A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.' Below it are input fields: 'Domain Name' (with placeholder 'Example: example.com'), 'Comment' (an empty text area), and 'Type' (a dropdown set to 'Public Hosted Zone'). A note below the type dropdown says 'A public hosted zone determines how traffic is routed on the Internet.' At the bottom of the modal is a blue 'Create' button.

- Now Hosted zone created with a name getitresolve.com, With Every Hosted zone there are 4 different name server's created and associated with the hosted zone. Here there is one SOA (start of Authority) which shown the main Name server which most of the traffic is allowed

The screenshot shows the AWS CloudFront console interface. On the left, a sidebar menu includes options like Dashboard, Hosted zones, Health checks, Traffic flow, Traffic policies, Policy records, Domains, Registered domains, and Pending requests. The 'Hosted zones' option is selected. The main content area displays a table of record sets for the domain 'getitresolve.com'. One row is highlighted, showing an NS record type with values for multiple name servers. To the right of the table is a detailed 'Edit Record Set' panel. This panel contains fields for 'Name' (set to 'getitresolve.com.'), 'Type' (set to 'NS – Name server'), and 'Value' (containing the names of the four Amazon Web Services name servers: ns-1055.awsdns-03.org., ns-65.awsdns-08.com., ns-1897.awsdns-45.co.uk., and ns-954.awsdns-42.net.). There are also fields for 'Alias' (set to 'No'), 'TTL (Seconds)' (set to 172800), and a dropdown menu for selecting different TTL options (1m, 5m, 1h, 1d). Below these fields is a note about entering multiple name servers on separate lines, followed by an example: ns1.amazon.com, ns2.amazon.org, ns3.amazon.net, ns4.amazon.co.uk. At the bottom right of the panel is a blue 'Save Record Set' button.

5. Now, To Create or Purchase our Own Domain Name we go to <https://in.godaddy.com/>, then sign up to create Domain Name.



|| C3 SCHOOLS

The screenshot shows a web browser window with the URL <https://in.godaddy.com>. The GoDaddy homepage is displayed, featuring a prominent banner for a hosting sale. On the left, there's a sidebar with various service categories like Apps, DevOps, and AWS. The main content area includes a 'Get Started' button for WordPress and a large image of a person working on a laptop and a phone.

6. Since I already have an account which will show you all the registered domain name which I registered

Click On getitresolve.com to Manage Domain name's details

The screenshot shows the GoDaddy Domains management interface. At the top, there's a navigation bar with links for 'Domains', 'Buy & Sell', 'DNS', 'Settings', and 'Help'. On the right, there are user profile and notification icons. Below the navigation is a green header bar with the same menu items. The main content area is titled 'Domains' and displays a grid of domain records. The columns include 'Domain Name', 'Expires', 'Status', 'Auto-Renew', 'Lock', 'Privacy', and 'Certified Domain'. A yellow row highlights the first domain, 'GETITRESOLVE.CO.IN', which expires on 12-05-2017 and is active. The 'Lock' and 'Privacy' checkboxes are checked. There are 'Edit' and 'Add' buttons for this row. Other domains listed include 'getitresolve.co.in', 'GETITRESOLVE.IN', 'GETITRESOLVE.INFO', 'GETITRESOLVE.NET', 'GETITRESOLVE.ORG', 'GETONLINECLASSES.IN', and 'GETRESULTS.CO.IN', all with similar status and lock/privacy settings. At the bottom of the page, there's a copyright notice: 'Copyright © 1999 - 2016 GoDaddy Operating Company, LLC. All Rights Reserved.' and a link to 'Privacy Policy'.

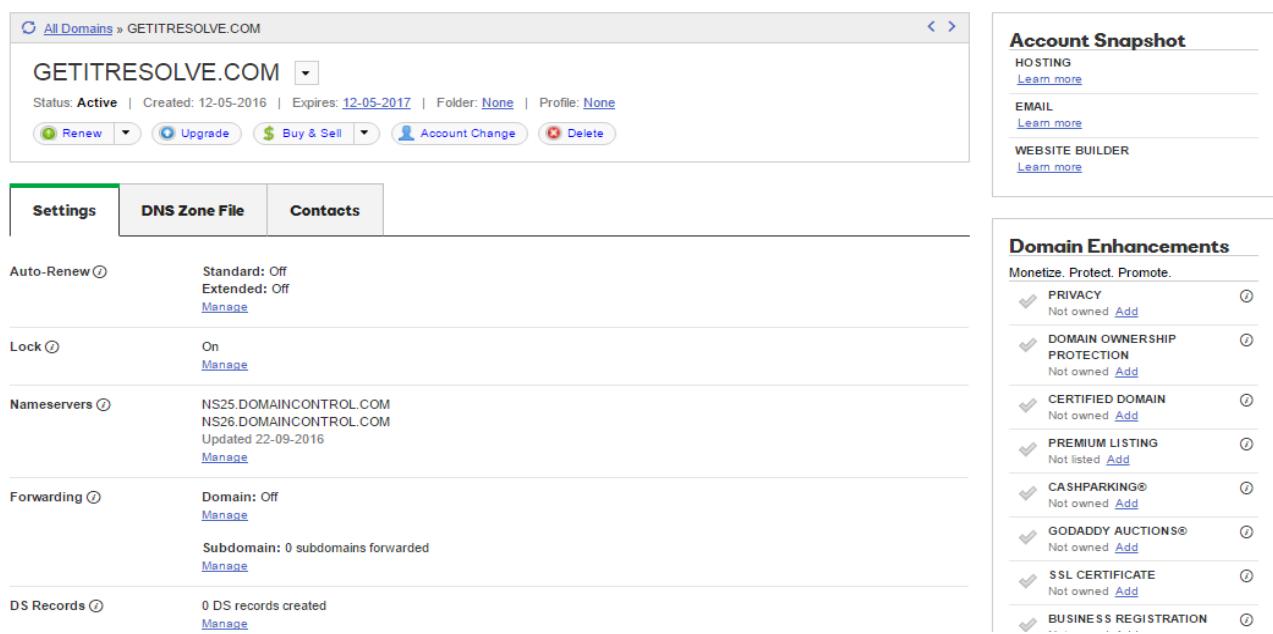
Domain Name	Expires	Status	Auto-Renew	Lock	Privacy	Certified Domain
GETITRESOLVE.CO.IN	12-05-2017	Active				Add
getitresolve.co.in	12-05-2017	Active		✓		
GETITRESOLVE.IN	12-05-2017	Active		✓		
GETITRESOLVE.INFO	12-05-2017	Active		✓		
GETITRESOLVE.NET	12-05-2017	Active		✓		
GETITRESOLVE.ORG	12-05-2017	Active		✓		
GETONLINECLASSES.IN	12-05-2017	Active		✓		
GETRESULTS.CO.IN	12-05-2017	Active		✓		

7. Here click where name servers to manage because to enter our hosted zone name server update here in the godday.com



|| C3 SCHOOLS

Domain Details



The screenshot shows the GoDaddy domain management interface for the domain GETITRESOLVE.COM. The top navigation bar includes links for All Domains, Home, and Help. Below the domain name, it shows the status as Active, creation date as 12-05-2016, expiration date as 12-05-2017, folder as None, and profile as None. Action buttons include Renew, Upgrade, Buy & Sell, Account Change, and Delete.

The main content area has tabs for Settings (selected), DNS Zone File, and Contacts. Under Settings, there are sections for Auto-Renew (Standard: Off, Extended: Off), Lock (On), Nameservers (NS25.DOMAINCONTROL.COM, NS26.DOMAINCONTROL.COM, Updated 22-09-2016), Forwarding (Domain: Off, Subdomain: 0 subdomains forwarded), and DS Records (0 DS records created). Each section has a Manage link.

On the right side, there's an Account Snapshot section with links for HOSTING, EMAIL, and WEBSITE BUILDER. Below that is a Domain Enhancements section titled "Monetize. Protect. Promote." with various options like Privacy, Domain Ownership Protection, Certified Domain, Premium Listing, Cashparking®, Godaddy Auctions®, SSL Certificate, and Business Registration, each with an Add link.

8. After Clicking Manage Dialogue box will appear there we select "Custom" to enter our created name server details here by clicking "Add Name Server", after enter all 4 domain name server names click "Save". To update server it will take around 30 minutes, in the mean time create instances in two different regions and create an ELB so that we can we can create Record Set



C3 SCHOOLS

Nameservers point your domain to where it is located.

Setup type:

Standard
Go Daddy hosting, forwarding, and parked domains.
 Custom
Customizable nameserver settings.

#	Nameserver	Status
1	NS-1055.AWSDNS-03.ORG	(
2	NS-65.AWSDNS-08.COM	(
3	NS-1897.AWSDNS-45.CO.UK	(
4	NS-854.AWSDNS-42.NET	(

Add Nameserver **Save** **Cancel**

Enhancements

- CloudFront Promote
- CloudFront Add
- IN OWNERSHIP EDITION
- IN OWNERSHIP Add
- FED DOMAINS ADD
- FED DOMAINS Add
- PARKING ADD
- ADD AUCTIONS Add
- CERTIFICATE ADD
- CERTIFICATE Add
- LESS REGISTRATION ADD
- LESS REGISTRATION Add
- IN APPRAISAL APPRAISED
- IN APPRAISAL Add
- DOMAIN BUNDLE AVAILABLE
- DOMAIN BUNDLE Add

9. Here we are creating instances in two different regions and an ELB for Route 53 Lab. To test different test cases I am creating 3 Instances in 2 different AZ in a single Region.

While creating instance we go to " Configure Instance there go to Advanced Details then select "As text" write "Code" as follows in the below.

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

IAM role

Shutdown behavior

Enable termination protection Protect against accidental termination

Monitoring Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy

Advanced Details

User data As text As file Input is already base64 encoded

```
#!/bin/bash
yum install httpd -y
service httpd start
yum update -y
echo "Hello Every one This is for Demo" > /var/www/html/index.html
```

Cancel **Previous** **Review and Launch** **Next: Add Storage**



|| C3 SCHOOLS

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Spot Requests, Reserved Instances, Dedicated Hosts, Images, AMIs, and Elastic Block Store. The main 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, and Public DNS. Three instances are listed: Primary (i-019cafa374d258..., t2.micro, ap-southeast-1a), Secondary (i-035964fbca0bc3..., t2.micro, ap-southeast-1b), and Test Server (i-050c148c7b6385..., t2.micro, ap-southeast-1a). All instances are shown as green dots indicating they are running. The "Secondary" and "Test Server" rows are highlighted with red boxes. At the bottom of the table area, it says "Select an instance above" and shows three small square icons.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
Primary	i-019cafa374d258...	t2.micro	ap-southeast-1a	running	2/2 checks...	None	ec2-54-254-227-198
Secondary	i-035964fbca0bc3...	t2.micro	ap-southeast-1b	running	2/2 checks...	None	ec2-54-179-185-155
Test Server	i-050c148c7b6385...	t2.micro	ap-southeast-1a	running	2/2 checks...	None	ec2-52-220-146-177

10. Here we are creating one instance in a different regions other than above, To test different test cases.



C3 SCHOOLS

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with navigation links: EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES (with Instances selected), SPOT REQUESTS, Reserved Instances, Dedicated Hosts, IMAGES (with AMIs selected), Bundle Tasks, ELASTIC BLOCK STORE (with Volumes and Snapshots), and NETWORK & SECURITY (with Security Groups and Elastic IP). The main content area has tabs: Launch Instance, Connect, Actions, and a search bar. A table lists instances, with one row highlighted: Name (Test Server), Instance ID (i-05689a56ce17c9c0d), Instance Type (t2.micro), Availability Zone (ap-south-1b), Status (running), Status Checks (2/2 checks...), Alarm Status (None), and Public DNS (ec2-52-66-142-223.ap-s...). Below the table, a detailed view for the 'Test Server' instance shows fields like Instance ID, Instance state, Instance type, Private DNS, Private IPs, Public DNS, Public IP (highlighted with a red box), Elastic IPs, Availability zone, and Security groups.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
Test Server	i-05689a56ce17c9c0d	t2.micro	ap-south-1b	running	2/2 checks...	None	ec2-52-66-142-223.ap-s...

Instance: i-05689a56ce17c9c0d (Test Server) Public DNS: ec2-52-66-142-223.ap-south-1.compute.amazonaws.com

Description Status Checks Monitoring Tags

Instance ID: i-05689a56ce17c9c0d	Public DNS: ec2-52-66-142-223.ap-south-1.compute.amazonaws.com
Instance state: running	Public IP: 52.66.142.223
Instance type: t2.micro	Elastic IPs:
Private DNS: ip-172-31-1-132.ap-south-1.compute.internal	Availability zone: ap-south-1b
Private IPs: 172.31.1.132	Security groups: MumSG. view rules

11. Here we are going to do few things. Copy and Paste Public IP Address Each Instance in the Browser, check whether it is showing index html or not. If not then login into your instances and check httpd service status and If the httpd service stopped then start the service. then try Refresh in the Browser to see index.html page.
12. Now We are going to Create an ELB for Route 53 Test cases. In the ELB creation Select Same "Security Group", then add two or more instance accordingly to ELB then add tag name and finally review and launch our ELB.



C3 SCHOOLS

The screenshot shows the AWS Management Console with the 'Services' menu selected. The left sidebar lists various services: Elastic Block Store, Network & Security, Load Balancing (with 'Load Balancers' highlighted by a red box), Auto Scaling, and Commands. The main content area shows a table of load balancers with one row selected ('MyELB'). Below the table, under the 'Load balancer: MyELB' heading, is a tab navigation bar with 'Description', 'Instances' (which is active and highlighted by a red box), 'Health Check', 'Listeners', 'Monitoring', and 'Tags'. A message indicates 'Connection Draining: Enabled, 300 seconds (Edit)'. Below this is an 'Edit Instances' button. A table lists two instances: 'Secondary' (Instance ID: i-035964fbca0bc3792) and 'Primary' (Instance ID: i-019cfa374d258a76). Both instances are in 'InService' status and have a 'Remove from Load Balancer' action button.

Instance ID	Name	Availability Zone	Status	Actions
i-035964fbca0bc3792	Secondary	ap-southeast-1b	InService ⓘ	Remove from Load Balancer
i-019cfa374d258a76	Primary	ap-southeast-1a	InService ⓘ	Remove from Load Balancer

13. Here we create a Record Set for our Name Server. There are two ways those are with alias name or without it.

- Without Alias name by selecting IP Address Type and Value here is Public IP Or Elastic IP if you're using Permanent web server , Select Routing Policy Accordingly here i have selected "Simple" then click on Create



C3 SCHOOLS

AWS Services Edit demo2016 Global Support

Dashboard Hosted zones Health checks Traffic flow Traffic policies Policy records Domains Registered domains Pending requests

Back to Hosted Zones Create Record Set Import Zone File Delete Record Set Test Record Set

Record Set Name: Any Type Aliases Only Weighted Only

Displaying 1 to 2 out of 2 Record Sets

Name	Type	Value	Evaluate Target Health	Health Check ID
getitresolve.com.	NS	ns-1055.awsdns-03.org. ns-65.awsdns-08.com. ns-1897.awsdns-45.co.uk. ns-854.awsdns-42.net.	-	1
getitresolve.com.	SOA	ns-1055.awsdns-03.org. awsdns-hostmaster.amazonaws.com.	-	9

Create Record Set

Name: www.getitresolve.com.

Type: A - IPv4 address

Alias: Yes No

TTL (Seconds): 300 1m 5m 1h 1d

Value: 52.220.146.128

IPv4 address. Enter multiple addresses on separate lines.
Example:
192.0.2.235
198.51.100.234

Routing Policy: Simple

Route 53 responds to queries based only on the values in this record. Learn More

Create

b. With the Alias name here we are using Our ELB, Select Routing Policy Accordingly here i have selected "Simple" then click on Create

AWS Services Edit demo2016 Global Support

Dashboard Hosted zones Health checks Traffic flow Traffic policies Policy records Domains Registered domains Pending requests

Back to Hosted Zones Create Record Set Import Zone File Delete Record Set Test Record Set

Record Set Name: Any Type Aliases Only Weighted Only

Displaying 1 to 2 out of 2 Record Sets

Name	Type	Value	Evaluate Target Health	Health Check ID
getitresolve.com.	NS	ns-1055.awsdns-03.org. ns-65.awsdns-08.com. ns-1897.awsdns-45.co.uk. ns-854.awsdns-42.net.	-	1
getitresolve.com.	SOA	ns-1055.awsdns-03.org. awsdns-hostmaster.amazonaws.com.	-	9

Create Record Set

Name: www.getitresolve.com.

Type: A - IPv4 address

Alias: Yes No

Alias Target: dualstack.getresults-co-in-954540704.

Alias Hosted Zone ID: Z35SXDOTRQ7X7K

You can also type the domain name for the resource. Examples:
- CloudFront distribution domain name: d111111abcdef8.cloudfront.net
- Elastic Beanstalk environment CNAME: example.elasticbeanstalk.com
- ELB load balancer DNS name: example-1.us-east-1.elb.amazonaws.com
- S3 website endpoint: example.s3-website-us-east-1.amazonaws.com
- Resource record set in this hosted zone: www.example.com

Learn More

Routing Policy: Simple

Route 53 responds to queries based only on the values in this record. Learn More

Evaluate Target Health: Yes No

Create



C3 SCHOOLS

14. Record Set will create according to instruction given and it will display

The screenshot shows the AWS Route 53 Hosted Zones interface. The left sidebar has 'Hosted zones' selected, indicated by a red box. The main area displays a table of record sets for the domain 'getitresolve.com.'. Two specific records are highlighted with red boxes: one for 'getitresolve.com.' (Type A, Value 52.220.146.177) and another for 'www.getitresolve.com.' (Type A, Value ALIAS dualstack.myelb-1249638457.ap-southeast-1). On the right, a sidebar shows 'Selected resource records' with a table:

Name	Type
getitresolve.com.	A
www.getitresolve.com.	A



C3 SCHOOLS

Route 53 Test Cases

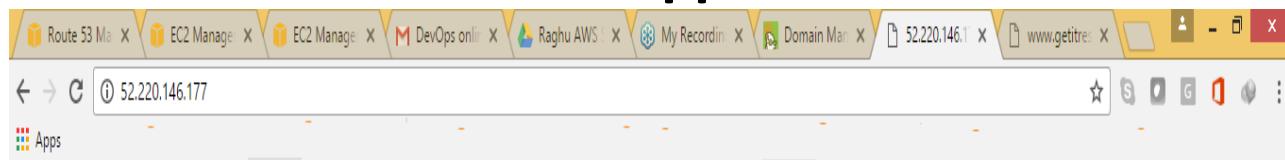
Case 1: Route 53 Single Web Server, In this we simply create a record set with Public IP or Elastic IP of our Web Server. Enter name "www", Type Select IP Address, Value Type or Paste IP Address of Web Server then Select Routing Policy as "Simple" for now after that click on "Create".

The screenshot shows the AWS Route 53 service console. On the left, there's a navigation sidebar with options like Dashboard, Hosted zones (which is selected), Health checks, Traffic flow, Traffic policies, Policy records, Domains, Registered domains, and Pending requests. The main area has tabs for Back to Hosted Zones, Create Record Set (which is highlighted with a red box), Import Zone File, Delete Record Set, and Test Record Set. Below these tabs, there's a search bar for 'Record Set Name' and filters for 'Any Type', 'Aliases Only', and 'Weighted Only'. A table lists existing record sets: one for 'getitresolve.com.' of type NS with values ns-1055.awsdns-03.org., ns-65.awsdns-08.com., ns-1897.awsdns-45.co.uk., and ns-854.awsdns-42.net.; another for 'getitresolve.com.' of type SOA with values ns-1055.awsdns-03.org. awsdns-hostmaster.amazon.com; and one for 'www.getitresolve.com.' of type A with value ALIAS dualstack.myelb-1249638457.ap-southeast-1. There's also a note about Route 53 responding based on record values. At the bottom right of the main area, the 'Create' button is highlighted with a red box.

After creating Record set go to web browser then check domain / web server displaying it's content or not



C3 SCHOOLS



Here if "Server Failed to connect" then there will be "no Backup".

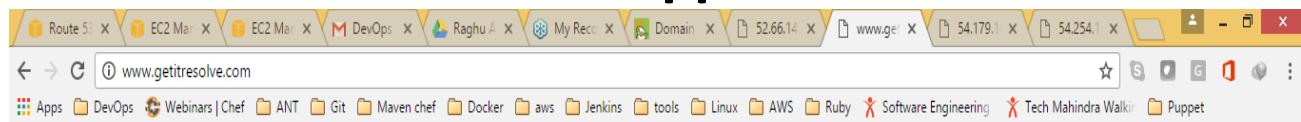
Case 2: Route 53 We use Two Web Server, In this we simply create a record set with Alias Target Address. Enter name "www", Type Select IP Address, Select Alias as "Yes", then go to Alias Target from the given choice we have our "ELB" Select it, Routing policy will be simple then click on Create.

The screenshot shows the AWS Route 53 service interface. On the left, there's a sidebar with navigation links like Dashboard, Hosted zones, Health checks, Traffic flow, Traffic policies, Policy records, Domains, Registered domains, and Pending requests. The main area has tabs for Back to Hosted Zones, Create Record Set (which is selected), Import Zone File, Delete Record Set, and Test Record Set. Below these tabs, there's a search bar for 'Record Set Name' and filters for 'Any Type', 'Aliases Only', and 'Weighted Only'. A table displays existing record sets for the domain 'getitresolve.com.' under three resource records (RRs): 'getitresolve.com.' (A type, value 52.220.146.177), 'getitresolve.com.' (NS type, values ns-1055.awsdns-03.org., ns-65.awsdns-08.com., ns-1897.awsdns-45.co.uk., ns-854.awsdns-42.net.), and 'getitresolve.com.' (SOA type, values ns-1055.awsdns-03.org., awsdns-hostmaster.amazon, awsdns-serial, awsdns-ttl). To the right, a 'Create Record Set' dialog box is open. It has fields for 'Name' (www.getitresolve.com.), 'Type' (A - IPv4 address), 'Alias' (radio button 'Yes' selected), 'Alias Target' (dropdown set to 'dualstack.MyELB-1249638457.ap-sou'), 'Alias Hosted Zone ID' (Z1LMS91P8CMLE5), and 'Routing Policy' (Simple). At the bottom of the dialog is a large blue 'Create' button.

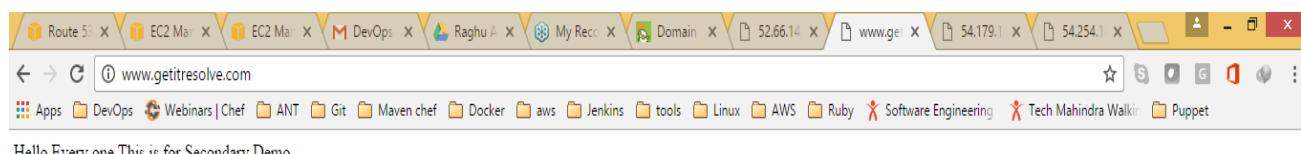
- In The Elastic Load Balancer (ELB) we have two Instances, by default Traffic will be shared if necessary, In Case if One Server is Down/ Failover then all the Traffic will be Routed to other Web server in the given ELB.



C3 SCHOOLS



In Case Failover Web Server



Case 3: Route 53 In Case Region Failover,

- We need to Create First Health Check for Region instances, For that Go to Route 53 Dash board Select Health Check then Click on Create Heath Check
- Select End Point so that we can check Results, Select End Point by IP Address, If End Point IP Address then write IP Address in the column, then Specify Path for Web server.
- Go to Advanced Configuration Select Request Interval, Failure Threshold accordingly then Click on Next



C3 SCHOOLS

Create health check

Step 1: Configure health check

Step 2: Get notified when health check fails

Configure health check

?

Route 53 health checks let you track the health status of your resources, such as web servers or mail servers, and take action when an outage occurs.

Name ⓘ

What to monitor Endpoint ⓘ

Status of other health checks (calculated health check)

State of CloudWatch alarm

Monitor an endpoint

Multiple Route 53 health checkers will try to establish a TCP connection with the following resource to determine whether it's healthy.
[Learn more](#)

Specify endpoint by IP address Domain name ⓘ

Protocol ⓘ

IP address * ⓘ

Host name ⓘ

Port * ⓘ

Path ⓘ

Advanced configuration

Request interval Standard (30 seconds) Fast (10 seconds) ⓘ

Failure threshold * ⓘ

String matching No Yes ⓘ

Latency graphs ⓘ

Invert health check status ⓘ

Health checker regions Customize Use recommended ⓘ

US East (N. Virginia)

US West (N. California)

US West (Oregon)

EU (Ireland)

Asia Pacific (Singapore)

Asia Pacific (Sydney)

Asia Pacific (Tokyo)

South America (São Paulo)

Health check type Basic + additional options: Fast Interval ([View Pricing](#))

* Required

Cancel

Next



|| C3 SCHOOLS

- In The Next Page Select Create Alarm "yes" If Necessary and specify Required Details otherwise Select No and Click on Create Health Check. After few minutes Health Check Status will be Healthy.

The screenshot shows the AWS CloudWatch interface for creating a health check. At the top, there's a navigation bar with icons for AWS, Services, Edit, demo2016, Global, and Support. The main title is "Create health check". Below it, there are two steps: "Step 1: Configure health check" (disabled) and "Step 2: Get notified when health check fails" (selected). The second step has a sub-section titled "Get notified when health check fails" with a question mark icon. It contains text about CloudWatch sending notifications via Amazon SNS when the health check status changes to unhealthy. A "Create alarm" section follows, with a radio button for "Yes" (selected) and one for "No". At the bottom, there are buttons for "Cancel", "Previous", and a prominent blue "Create health check" button.

- It will show us that Health Check is created Successfully. After few minutes Health Check Status will be Healthy



C3 SCHOOLS

The screenshot shows the AWS CloudFront Health Checks console. On the left, a sidebar lists navigation options: Dashboard, Hosted zones, Health checks (which is selected and highlighted in orange), Traffic flow, Traffic policies, Policy records, Domains, Registered domains, and Pending requests. At the top, there are AWS, Services, and Edit dropdown menus, along with demo2016, Global, and Support links. A success message box displays: "Health check with id 1b67e257-acba-4f32-9149-9133f23ae00f has been created successfully". Below the message is a table with columns: Name, Status, Description, Alarms, and ID. One row is visible: "Test Health Chk" (Status: Healthy, last checked 15 minutes ago, Description: http://52.220.146.177:80/index.html, Alarms: No alarms configured, ID: 1b67e257-acba-4f32-9149-9133f23ae00f). At the bottom of the table, tabs for Info, Monitoring, Alarms, Tags, Health checkers, and Latency are shown, with Info selected. A note below the table says "No health check selected."

- Next Step Go to Hosted Zones then Click on Create Record Set, There Write Record Name, Select Type, Select Alias as "No", as Value Enter Other Region Instance IP Address, Select Route Policy as Failover,

then select Associate with Heath Check as "Yes" then Select Health check we created Here and Click on Create Button.



C3 SCHOOLS

The screenshot shows the AWS Route 53 service console. On the left, there's a navigation sidebar with options like Dashboard, Hosted zones, Health checks, Traffic flow, Traffic policies, Policy records, Domains, Registered domains, and Pending requests. The 'Hosted zones' option is selected. In the main area, there's a table of existing record sets for the domain 'getitresolve.com.'. A 'Create Record Set' button is visible at the top right of this section. To the right of the table, a large form is displayed for creating a new record set. The 'Name' field is set to 'www2.getitresolve.com.', 'Type' is 'A - IPv4 address', and 'Value' is '52.66.142.223'. Other fields include 'TTL (Seconds)', 'Routing Policy' (set to 'Failover'), 'Failover Record Type' (set to 'Primary'), 'Set ID' ('www2-Primary'), 'Associate with Health Check' (set to 'Yes'), and 'Health Check to Associate' ('Test Health Chk'). The 'Create' button at the bottom of the form is highlighted with a red box.

- now go to Web Server and Check our <http://www2.getitresolve.com/> if our instance or working fine it will show primary instance servers web page otherwise it will show you Test server which is in different regions web server page will be shown.

To Delete Route 53, delete instances, ELB, Recorded sets, Health Check and Health Zone.

End of Route 53 Lab.