

Amazon EC2 Tutorial – For modified GUI

[Course tutorial and much more for extra reading]

Table of Contents

What is Amazon EC2?.....	4
Features of Amazon EC2.....	4
Sign Up for AWS.....	4
How Do I Get Started with the Free Usage Tier?.....	5
AWS Free Usage Tier (Per Month):	5
Elastic Compute Cloud (EC2)	5
Simple Storage Service (S3).....	6
CloudWatch	6
Instance Lifecycle	7
Instance Launch	7
Getting Started with Amazon EC2 Linux Instances.....	7
To launch an Amazon Linux instance in EC2:	8
Connect from Windows Using PuTTY	12
Amazon EC2 Key Pairs.....	16
Creating Your Key Pair Using Amazon EC2.....	16
Available Instance Types	17
Launch a Windows Instance.....	17
To connect to your Windows instance	20
Create an Elastic IP Address.....	21
To assign an Elastic IP address to your Windows instance	21
Instance Metadata and User Data [For additional reference]	22
Retrieving Instance Metadata [for additional reference].....	22
Examples of Retrieving Instance Metadata.....	22
Amazon Machine Images.....	26
Creating an Amazon EBS-Backed Linux AMI	26
Overview of the Creation Process for Amazon EBS-Backed AMIs.....	26
Copying an AMI	27
AMI Copy.....	27
Copying an Amazon EC2 AMI	28
Copying an AMI Using the Amazon EC2 Console	28
Instance Types.....	29
Spot Instances	29

Reserved Instances	30
Differences Between Reboot, Stop, and Terminate	30
Amazon Elastic Block Store (Amazon EBS).....	32
Amazon EBS Volumes - States	32
To create a new Amazon EBS volume	32
Attaching an Amazon EBS Volume to an Instance	33
Making an Amazon EBS Volume Available for Use.....	34
To detach an Amazon EBS volume	35
The volume is detached from the instance.....	36
For Windows Instances:.....	36
Make the Volume Available on Windows.....	36
To detach an Amazon EBS volume	38
Creating an Amazon EBS Snapshot	38
AWS Management Console	38
Public Data Set Concepts.....	40
Available Public Data Sets.....	41
Creating a Public Data Set Volume from a Snapshot	41
Attaching and Mounting the Public Data Set Volume	42
Installing the Amazon EC2 Command Line Interface Tools on Windows	42
[Separate document will be provided]	42
Elastic Load Balancing.....	43
Create a Basic Load Balancer in EC2-Classic	43
Configure Listeners for Your Load Balancer.....	43
Configure Health Check for Your Amazon EC2 Instances	44
Register Amazon EC2 Instances.....	46
Review Settings and Create Your Load Balancer	47
Verify the Creation of Your Load Balancer	48
Amazon S3: Simple Storage Service	51
Get Started With Amazon Simple Storage Service	51

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Amazon S3 Basics.....	51
Rules for Bucket Naming	51
Create a Bucket.....	52
Add an Object to a Bucket	54
View An Object	55
Using Reduced Redundancy Storage	55
Configure a Bucket for Website Hosting	56
Permissions Required for Website Access	58
Setting Up a Static Website in S3.....	59
Setting Up Notification of Bucket Events.....	60
Object Lifecycle Management	60
Lifecycle Configuration Rules	61
Manage Object Lifecycle Using the AWS Management Console.....	62
Using Versioning.....	63
Enabling Versioning	63
Suspending Versioning :	63
Restoring Previous Versions	64

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



What is Amazon EC2?

Amazon Elastic Compute Cloud (Amazon EC2) provides resizable computing capacity in the Amazon Web Services (AWS) cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage. Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.

Features of Amazon EC2

Amazon EC2 provides the following features:

- Virtual computing environments, known as *instances*
- **Pre-configured templates for your instances, known as *Amazon Machine Images (AMIs)***, that package the bits you need for your server (including the operating system and additional software)
- Various configurations of CPU, memory, storage, and networking capacity for your instances, known as ***instance types***
- Secure login information for your instances using ***key pairs*** (AWS stores the public key, and you store the private key in a secure place)
- Storage volumes for temporary data that's deleted when you stop or terminate your instance, known as ***instance store volumes***
- Persistent storage volumes for your data using Amazon Elastic Block Store (Amazon EBS), known as ***Amazon EBS volumes***
- Multiple physical locations for your resources, such as instances and Amazon EBS volumes, known as ***regions and Availability Zones***
- A firewall that enables you to specify the protocols, ports, and source IP ranges that can reach your instances using ***security groups***
- Static IP addresses for dynamic cloud computing, known as ***Elastic IP addresses***
- Metadata, known as ***tags***, that you can create and assign to your Amazon EC2 resources

Sign Up for AWS

When you sign up for Amazon Web Services (AWS), your AWS account is automatically signed up for all services in AWS, including Amazon EC2. You are charged only for the services that you use.

With Amazon EC2, you pay only for what you use. If you are a new AWS customer, you can get started with Amazon EC2 for free.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



If you have an AWS account already, skip to the next task. If you don't have an AWS account, use the following procedure to create one.

To create an AWS account

1. Go to <http://aws.amazon.com>, and then click **Sign Up**.
2. Follow the on-screen instructions.

How Do I Get Started with the Free Usage Tier?

When you create a new AWS account, you can test-drive some of the services and learn about AWS without charge. AWS calls this the [AWS Free Usage Tier](#).

You are eligible for the free tier for one year after you open your AWS account. After a year has passed, you will no longer be eligible for the free tier and will be charged any applicable fees for your AWS usage.

If you exceed the usage limits of the free tier or you use a service that is not on the free tier, you will be charged at the normal AWS billing rates.

To use AWS for free

1. [Use an AWS Account Created Less Than a Year Ago](#)
2. [Use Only Services That Offer a Free Usage Tier](#)
3. [Stay Within the Limits of the Free Usage Tier for the Services You Use](#)
4. [Create a Billing Alert to Warn You If Your Usage Exceeds the Free Usage Tier](#)

Unused capacity under the free tier does not roll over from month to month; it's a use-it-or-lose-it model

AWS Free Usage Tier (Per Month): Elastic Compute Cloud (EC2)

- 750 hours of [Amazon EC2](#) Linux† Micro Instance usage (613 MB of memory and 32-bit and 64-bit platform support) – enough hours to run continuously each month*
- 750 hours of [Amazon EC2](#) Microsoft Windows Server‡ Micro Instance usage (613 MB of memory and 32-bit and 64-bit platform support) – enough hours to run continuously each month*
- 750 hours of an [Elastic Load Balancer](#) plus 15 GB data processing*
- 30 GB of [Amazon Elastic Block Storage](#), plus 2 million I/Os and 1 GB of snapshot storage*

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Simple Storage Service (S3)

- 5 GB of [Amazon S3](#) standard storage, 20,000 Get Requests, and 2,000 Put Requests*

CloudWatch

- 10 [Amazon Cloudwatch](#) metrics, 10 alarms, and 1,000,000 API requests**

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

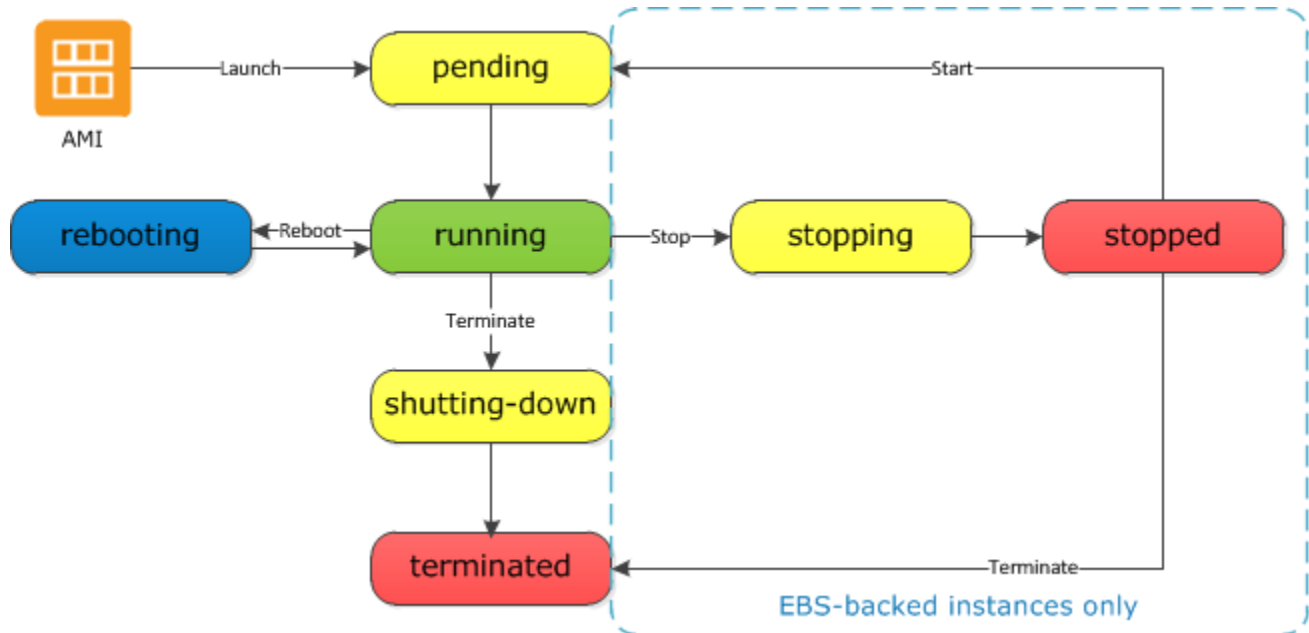
Chennai and Trivandrum , India



Instance Lifecycle

This topic describes the lifecycle of an Amazon EC2 instance, from the moment you launch it through its termination. By working with Amazon EC2 to manage your instance, you ensure that your customers have the best possible experience with the applications or sites that you host on your instance.

The following illustration represents the transitions between instance states.



Instance Launch

Getting Started with Amazon EC2 Linux Instances

- Let's get started with Amazon Elastic Compute Cloud (Amazon EC2) by launching, connecting to, and using a Linux instance. We'll use the AWS Management Console, a point-and-click web-based interface, to complete the example architecture shown in the following diagram:

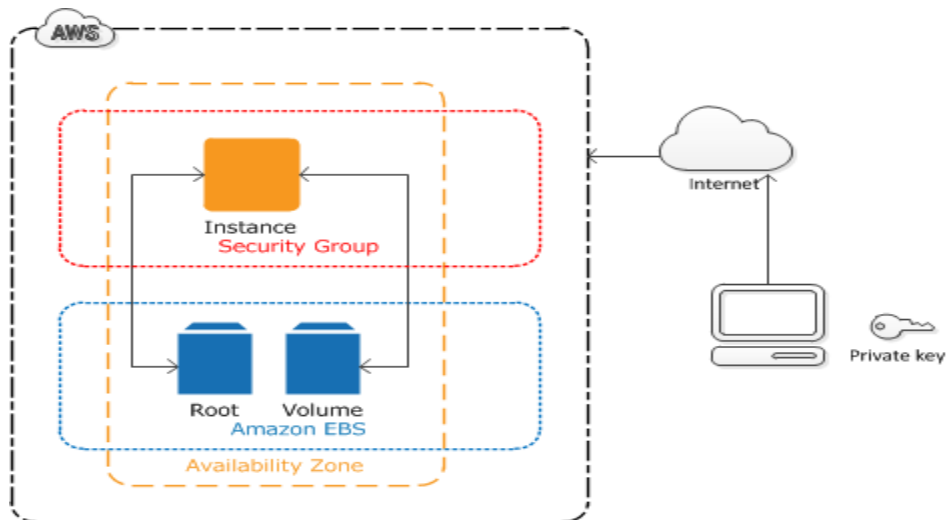
By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



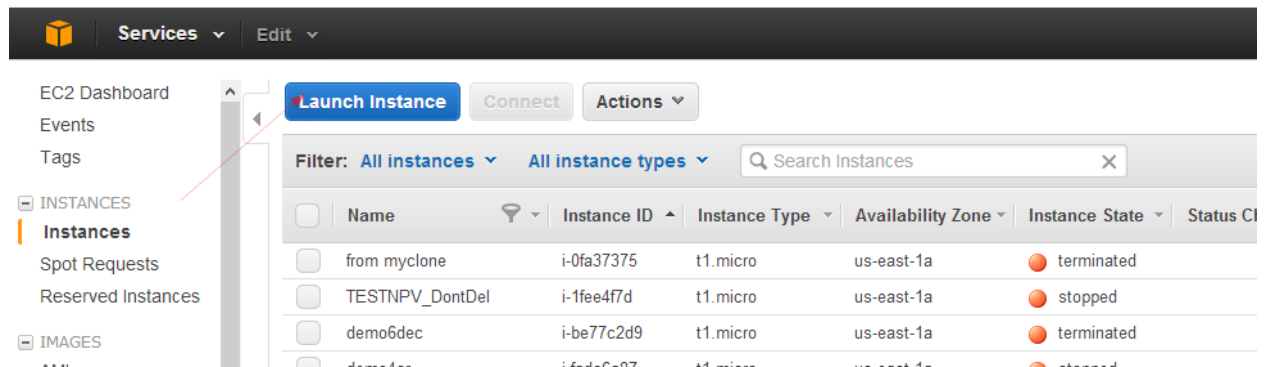
[Course tutorial and much more for extra reading]



4. The instance is an Amazon EBS-backed instance (meaning that the root volume is an Amazon EBS volume). We'll also create and attach an additional Amazon EBS volume. You can either specify the Availability Zone in which your instance runs, or let us select an Availability Zone for you. When you launch your instance, you secure it by specifying a key pair and security group. **(This exercise assumes that you created a key pair and a security group when getting set up;**

To launch an Amazon Linux instance in EC2:

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. From the console dashboard, click **Launch Instance**.



3. The **Select an Amazon Machine Image (AMI)** page displays a list of basic configurations called Amazon Machine Images (AMIs) that serve as templates for your instance. Select the 64-bit Amazon Linux AMI. Notice that this configuration is marked "Free tier eligible."

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Amazon EC2 Tutorial – For modified GUI


[Course tutorial and much more for extra reading]


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)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can see 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 ⓘ

**Amazon Linux AMI 2013.09.1** - ami-83e4bcea (64-bit) / ami-cde4bca4 (32-bit)
Free tier eligible
The Amazon Linux AMI is an EBS-backed, PV-GRUB image. It includes Linux 3.4, AWS tools, and repository access multiple versions of MySQL, PostgreSQL, Python, Ruby, and Tomcat.
Root device type: ebs Virtualization type: paravirtual

**Red Hat Enterprise Linux 6.4** - ami-a25415cb (64-bit) / ami-7e175617 (32-bit)
Free tier eligible
Red Hat Enterprise Linux version 6.4, EBS-boot.
Root device type: ebs Virtualization type: paravirtual

**SUSE Linux Enterprise Server 11** - ami-e8084981 (64-bit) / ami-b60948df (32-bit)
Free tier eligible
SUSE Linux Enterprise Server 11 Service Pack 3 basic install, EBS boot with Amazon EC2 AMI Tools preinstalled; Apache 2.2, MySQL 5.5, PHP 5.3, and Ruby 1.8.7 available
Root device type: ebs Virtualization type: paravirtual

4. On the **Select an Instance Type** page, you can select the hardware configuration of your instance. The **t1.micro** instance is selected by default. Click **Review and Launch** to let the wizard complete other configuration settings for you, so you can get started quickly.

Services Edit jayavel N. Virginia Help

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

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

All instance types
Micro instances
Free tier eligible
General purpose
Memory optimized
Storage optimized
Compute optimized

Currently selected: t1.micro (up to 2 ECUs, 1 vCPUs, 0.613 GiB memory, EBS only)
Micro instances
Micro instances are a low-cost instance option, providing a small amount of CPU resources. They are suited for lower throughput applications, and websites that require additional compute cycles periodically, but are not appropriate for applications that require sustained CPU performance. Popular uses for micro instances include low traffic websites or blogs, small administrative applications, bastion hosts, and free trials to explore EC2 functionality.

Size	ECUs ⓘ	vCPUs ⓘ	Memory (GiB)	Instance Storage (GiB) ⓘ	EBS-Optimized Available ⓘ	Network Performance ⓘ
t1.micro	up to 2	1	0.613	EBS only	-	Very Low

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 **Review and Launch** Next: Configure Instance Details
Go to PC settings to activate Windows Feedback

© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

5. On the **Review Instance Launch** page, you can review the settings for your instance.

Under **Security Groups**, you'll see that the wizard created and selected a security group for you. Instead, select the security group that you created when getting set up using the following steps:

- a. Click **Edit security groups**.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Amazon EC2 Tutorial – For modified GUI

[Course tutorial and much more for extra reading]

Services Edit

jayavel N. Virginia Help

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 [Edit AMI](#)

Amazon Linux AMI 2013.09.1 - ami-83e4bcea
The Amazon Linux AMI is an EBS-backed, PV-GRUB image. It includes Linux 3.4, AWS tools, and repository access to multiple versions of MySQL, PostgreSQL, Python, Ruby, and Tomcat.
Root Device Type: ebs Virtualization type: paravirtual

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
t1.micro	up to 2	1	0.613	EBS only	-	Very Low

Security Groups [Edit security groups](#)

Security group name launch-wizard-5
Description launch-wizard-5 created on Friday, December 6, 2013 12:47:35 PM UTC+5:30

Protocol	Type	Port Range (Code)	Source
----------	------	-------------------	--------

© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

Cancel Previous **Launch**

Activate Windows Go to PC settings to activate Windows

- b. If you have one, On the **Configure Security Group** page, ensure the **Select an existing security group** option is selected. If you don't have one, go to point "c"

Select your security group from the list of existing security groups, and click **Review and Launch**.

- c. If you do not have a security group, create a new one. Select the required **PORTS** by clicking "Add Rule" button.

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 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 below. [Learn more](#) about Amazon EC2 security groups.

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

Security group name:

Description:

Protocol	Type	Port Range (Code)	Source
SSH	TCP	22	Anywhere

Add Rule

6. In case of Linux instance the security group should have port 22 opened. For Windows instance port 3389(RDP) should be opened. In case of having a HTTP server in the instance port 80 should be opened.

Anywhere
means connect
from any IP.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

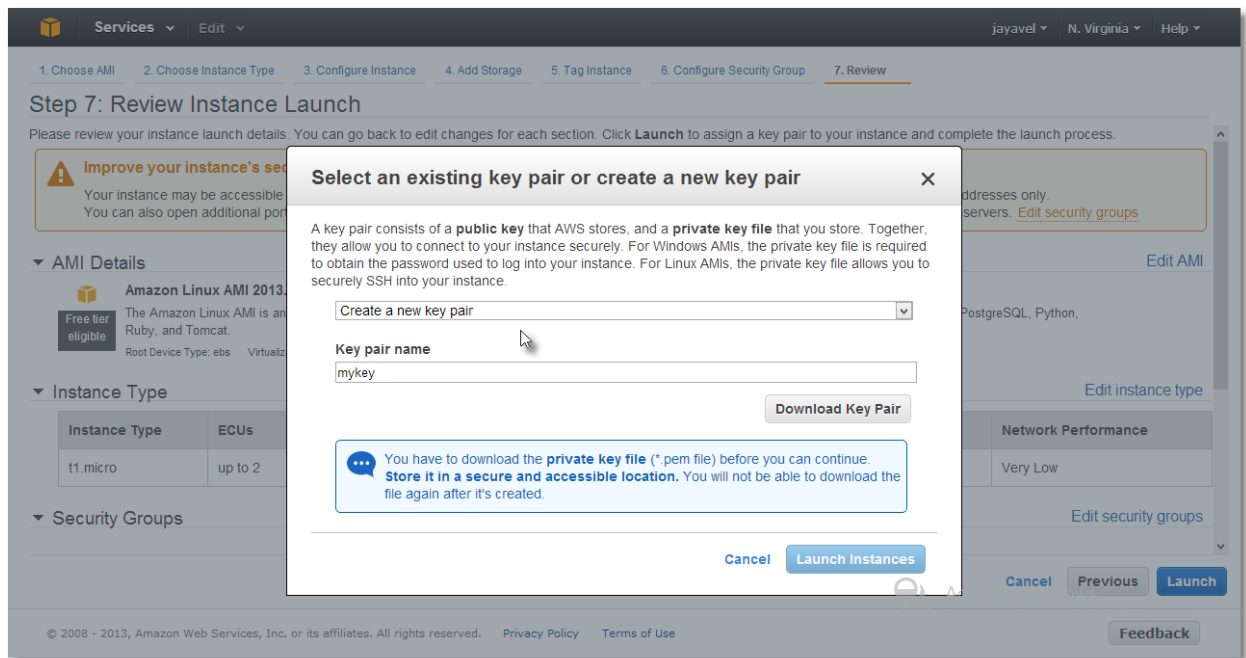
Chennai and Trivandrum, India



[Course tutorial and much more for extra reading]

- On the **Review Instance Launch** page, click **Launch**.
- In the **Select an existing key pair or create a new key pair** dialog box, select **Choose an existing key pair**, then select the key pair you created when getting set up.

Alternatively, you can create a new key pair. Select **Create a new key pair**, enter a name for the key pair, and then click **Download Key Pair**. This is the only chance for you to save the private key file, so be sure to download it. Save the private key file in a safe place. You'll need to provide the name of your key pair when you launch an instance and the corresponding private key each time you connect to the instance.



A key pair enables you to connect to a Linux instance through SSH. Therefore, don't select the **Proceed without a key pair** option. If you launch your instance without a key pair, then you can't connect to it.

When you are ready, select the acknowledgment check box, and then click **Launch Instances**.

- A confirmation page lets you know that your instance is launching. Click **View Instances** to close the confirmation page and return to the console.
- On the **Instances** screen, you can view the status of your instance. It takes a short time for an instance to launch. When you launch an instance, its initial state is `pending`. After the instance starts, its state changes to `running`, and it receives a public DNS name. (If the **Public DNS** column is hidden, click the **Show/Hide** icon and select **Public DNS**.)

Notes:

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Amazon EC2 Tutorial – For modified GUI

[Course tutorial and much more for extra reading]

EC2-Classic — Instances launched in EC2-Classic run in a flat network that you share with other customers. We assign each instance with a private IP address from a range of private IP addresses for the EC2-Classic network. EC2 also assigns a public IP address for your instance.

EC2-VPC — Instances launched in EC2-VPC run in an virtual private cloud (VPC) that is logically isolated in your AWS account. We assign each instance with a private IP address from the private IP address range of your VPC

Connect from Windows Using PuTTY

PuTTY doesn't use .pem files, it uses .ppk files. If you haven't already generated a .ppk file, do so now.

To connect to your Linux instance using PuTTY

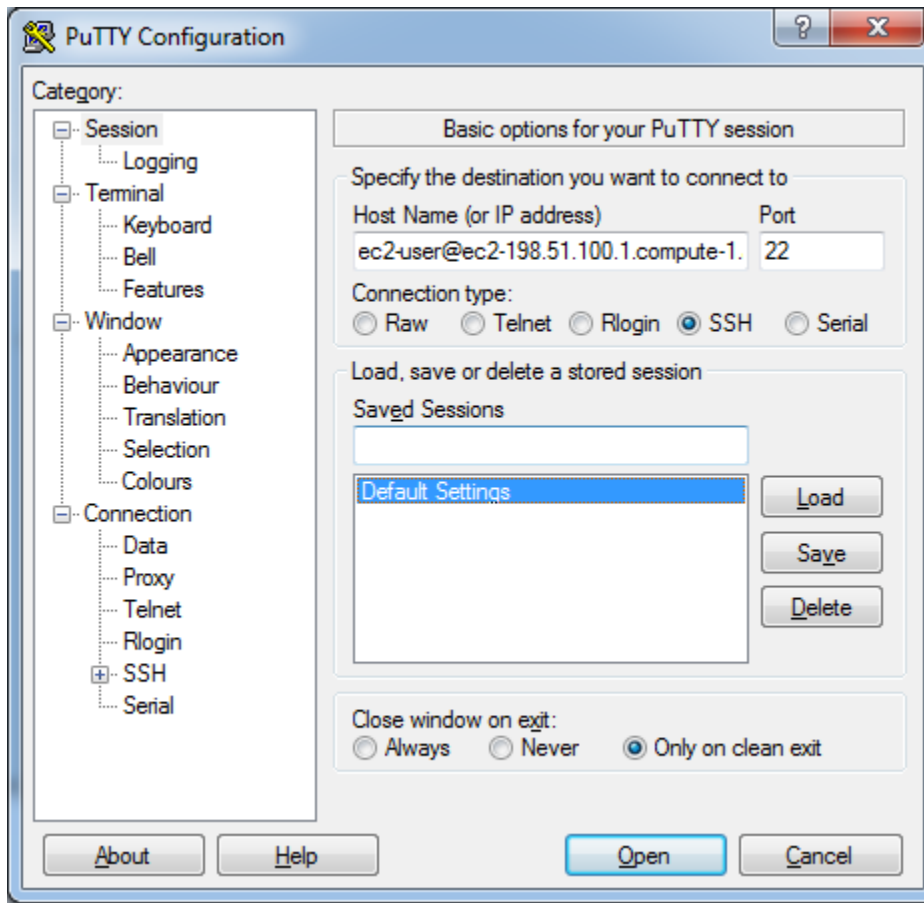
1. Start PuTTY (from the **Start** menu, click **All Programs > PuTTY > PuTTY**).
2. In the Category pane, select **Session** and complete the following fields:
 - a. In the **Host Name** box, enter `ec2-user@public_dns_name`.
 - b. Under **Connection type**, select **SSH**.
 - c. Ensure that **Port** is 22.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

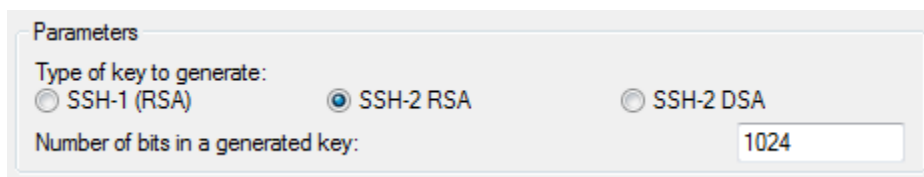
Chennai and Trivandrum , India





To prepare to connect to a Linux instance from Windows using PuTTY

3. Start PuTTYgen (for example, from the **Start** menu, click **All Programs > PuTTY > PuTTYgen**).
4. Under **Type of key to generate**, select **SSH-2 RSA**.



5. Click **Load**. By default, PuTTYgen displays only files with the extension .ppk. To locate your .pem file, select the option to display files of all types.

By ANIL KUMAR

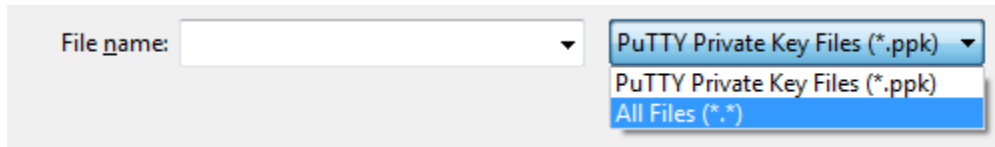
cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Amazon EC2 Tutorial – For modified GUI

[Course tutorial and much more for extra reading]



6. Select the private key file that you created in the previous procedure and click **Open**. Click **OK** to dismiss the confirmation dialog box.
7. Click **Save private key**. PuTTYgen displays a warning about saving the key without a passphrase. Click **Yes**.
8. Specify the same name for the key that you used for the key pair (for example, *your_user_name-key-pair-region_name*). PuTTY automatically adds the .ppkfile extension.

Back in Putty:

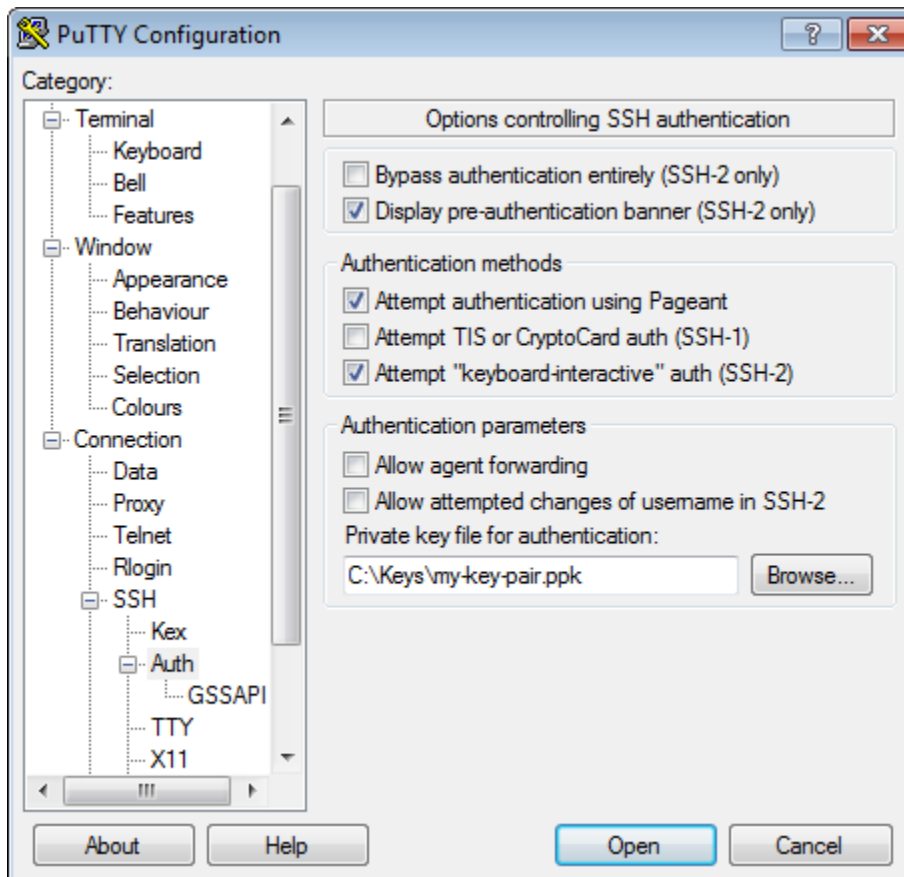
9. In the **Category** pane, expand **Connection**, expand **SSH**, and then select **Auth**. Complete the following:
 - a. Click **Browse**.
 - b. Select the .ppk file that you generated for your key pair, and then click **Open**.
 - c. Click **Open** to start the PuTTY session.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India





10. If this is the first time you have connected to this instance, PuTTY displays a security alert dialog box that asks whether you trust the host you are connecting to. Click **Yes**. A window opens and you are connected to your instance

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Amazon EC2 Key Pairs

Amazon EC2 uses public-key cryptography to encrypt and decrypt login information. Public-key cryptography uses a public key to encrypt a piece of data, such as a password, then the recipient uses the private key to decrypt the data. The public and private keys are known as a *key pair*.

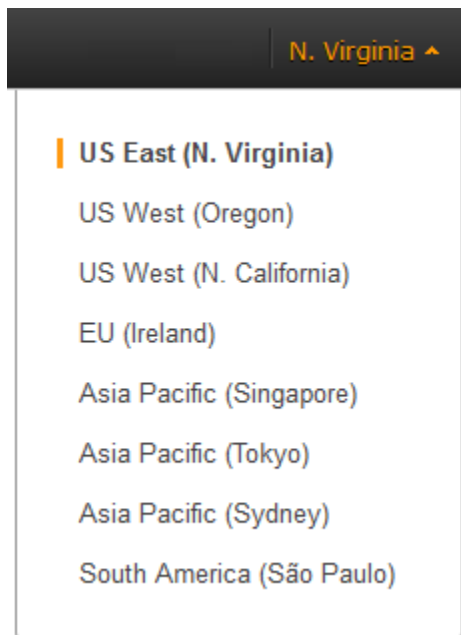
To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance. Linux/UNIX instances have no password, and you use a key pair to log in using SSH. With Windows instances, you use a key pair to obtain the administrator password and then log in using RDP.

Creating Your Key Pair Using Amazon EC2

Use the following steps to create a key pair using the Amazon EC2 console.

To have Amazon EC2 create your key pair

1. Open the Amazon EC2 console.
2. From the navigation bar, select a region for the key pair. You can select any region that's available to you, regardless of your location. This choice is important because some Amazon EC2 resources can be shared between regions, but key pairs can't. For example, if you create a key pair in the US West (Oregon) Region, you can't see or use the key pair in another region.



3. Click **Key Pairs** in the navigation pane.
4. Click **Create Key Pair**.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Amazon EC2 Tutorial – For modified GUI

[Course tutorial and much more for extra reading]

5. Enter a name for the new key pair in the **Key pair name** field of the **Create Key Pair** dialog box, and then click **Create**.
6. The private key file is automatically downloaded by your browser. The base file name is the name you specified as the name of your key pair, and the file name extension is `.pem`. Save the private key file in a safe place.

Important

This is the only chance for you to save the private key file. You'll need to provide the name of your key pair when you launch an instance and the corresponding private key each time you connect to the instance.

7. If you will use an SSH client on a Linux computer to connect to your Linux instance, use the following command to set the permissions of your private key file so that only you can read it.

```
$ chmod 400 my-key-pair.pem
```

Available Instance Types

Amazon EC2 provides the instance types listed in the following table.

Instance Family	Instance Types
General purpose	m1.small m1.medium m1.large m1.xlarge m3.xlarge m3.2xlarge
Compute optimized	c1.medium c1.xlarge c3.large c3.xlarge c3.2xlarge c3.4xlarge c3.8xlarge cc2.8xlarge
Memory optimized	m2.xlarge m2.2xlarge m2.4xlarge cr1.8xlarge
Storage optimized	hi1.4xlarge hs1.8xlarge
Micro instances	t1.micro
GPU instances	cg1.4xlarge g2.2xlarge

Launch a Windows Instance

You can launch a Windows instance using the AWS Management Console as described following. An instance is a virtual server in the AWS cloud. Amazon EC2 enables you to set up and configure the operating system and applications that run on your instance.

Important

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

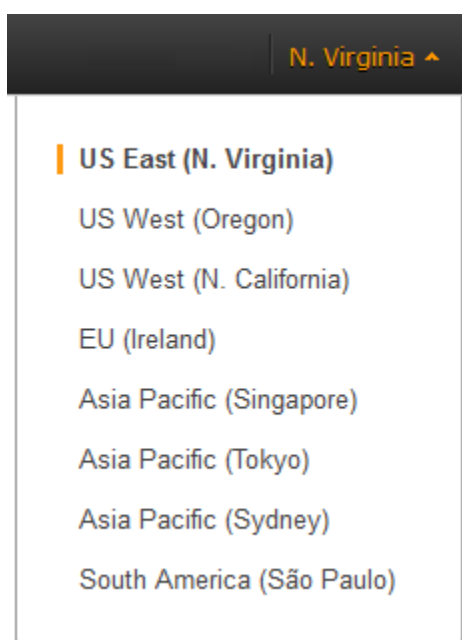
Chennai and Trivandrum , India



When you sign up for AWS, you can get started with Amazon EC2 for free using the [AWS Free Usage Tier](#). If you created your AWS account less than 12 months ago, and have not already exceeded the Free Usage Tier benefits for Amazon EC2 and Amazon EBS, it will not cost you anything to complete this tutorial, because we help you select options that are within the Free Usage Tier benefits. Otherwise, you'll incur the standard Amazon EC2 usage fees from the time that you launch the instance until you terminate the instance (which is the final task of this tutorial), even if it remains idle. The total charges to complete this tutorial outside the Free Usage Tier are minimal.

To launch an instance

1. Sign in to the AWS Management Console and open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. From the navigation bar, select the region for the instance. For this tutorial, you can use the default region. Otherwise, this choice is important because some Amazon EC2 resources can be shared between regions, while others can't. For example, if you'd like to connect your instance to an existing Amazon EBS volume, you must select the same region as the volume.



3. From the console dashboard, click **Launch Instance**.
4. The **Select an Amazon Machine Image (AMI)** page displays a list of basic configurations called Amazon Machine Images (AMIs) that serve as templates for your instance. Select the 64-bit version of Microsoft Windows Server 2008 R2. Notice that this configuration is marked 'Free tier eligible.'
5. On the **Select an Instance Type** page, you can select the hardware configuration for your instance. The **t1.micro** instance is selected by default. Click **Review and Launch** to let the wizard complete other configuration settings for you, so you can get started quickly.
6. On the **Review Instance Launch** page, you can review the settings for your instance.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



[Course tutorial and much more for extra reading]

Under **Security Groups**, you'll see that the wizard created and selected a security group for you. The security group includes basic firewall rules that enable you to connect your instance. For a Windows instance, you connect through Remote Desktop Protocol (RDP) on port 3389.

Caution

The security group the wizard creates authorizes all IP addresses to access your instance over the specified ports (for example, RDP). This is acceptable for the short exercise in this tutorial, but it's unsafe for production environments. In production, you'll authorize only a specific IP address or range of IP addresses to access your instance.

If you have an existing security group you'd prefer to use, you can click **Edit security groups**, and select your group on the **Configure Security Group** page. When done, click **Review and Launch** to return to the **Review Instance Launch** page.

7. Click **Launch**.
8. In the **Select an existing key pair or create a new key pair** dialog box, you can select **Choose an existing key pair**, to select a key pair you already created.

Alternatively, you can create a new key pair. Select **Create a new key pair**, enter a name for the key pair, and then click **Download Key Pair**. This is the only chance for you to save the private key file, so be sure to download it. Save the private key file in a safe place. You'll need to provide the name of your key pair when you launch an instance and the corresponding private key each time you connect to the instance.

Caution

Don't select the **Proceed without a key pair** option. If you launch your instance without a key pair, then you can't connect to it.

When you are ready, select the acknowledgement check box, and then click **Launch Instances**.

9. A confirmation page lets you know that your instance is launching. Click **View Instances** to close the confirmation page and return to the console.
10. On the **Instances** screen, you can view the status of the launch. It takes a short time for an instance to launch. When you launch an instance, its initial state is `pending`. After the instance starts, its state changes to `running` and it receives a public DNS name. (If the **Public DNS** column is hidden, click the **Show/Hide** icon in the top right corner of the Instances page and select **Public DNS**.)
11. Record the public DNS name for your instance because you'll need it for the next step.
12. (Optional) After your instance is launched, you can view its security group rules. From the Instances page, select the instance. In the **Description** tab, find **Security groups** and click **view rules**.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Security Groups associated with i-1a2b3c4d			
Ports	Protocol	Source	my-security-group
3389	tcp	0.0.0.0/0	✓

As you can see, if you used the security group the wizard created for you, it contains one rule that allows RDP traffic from any IP source to port 3389. If you launch a Windows instance running IIS and SQL, the wizard creates a security group that contains additional rules to allow traffic to port 80 for HTTP (for IIS) and port 1433 for MS SQL.

To connect to your Windows instance

1. In the Amazon EC2 console, select the instance, and then click **Connect**.
2. In the **Connect To Your Instance** dialog box, click **Get Password** (it will take a few minutes after the instance is launched before the password is available).
3. Click **Browse** and navigate to the private key file you created when you launched the instance. Select the file and click **Open** to copy the entire contents of the file into contents box.
4. Click **Decrypt Password**. The console displays the default administrator password for the instance in the **Connect To Your Instance** dialog box, replacing the link to **Get Password** shown previously with the actual password.
5. Record the default administrator password, or copy it to the clipboard. You need this password to connect to the instance.
6. Click **Download Remote Desktop File**. Your browser prompts you to either open or save the .rdp file. Either option is fine. When you have finished, you can click **Close** to dismiss the **Connect To Your Instance** dialog box.
7. If you opened the .rdp file, you'll see the **Remote Desktop Connection** dialog box. If you saved the .rdp file, navigate to your downloads directory, and double-click the .rdp file to display the dialog box. You may get a warning that the publisher of the remote connection is unknown. Click **Connect** to connect to your instance. You may get a warning that the security certificate could not be authenticated. Click **Yes** to continue.
8. Log in to the instance as prompted, using `Administrator` as the user name and the default administrator password that you recorded or copied previously. If the user name includes a domain (`domain\Administrator`), delete the text before `Administrator`.

After you connect, we recommend that you do the following:

- Change the Administrator password from the default value. You change the password while logged on to the instance itself, just as you would on any other Windows Server.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



- Create another user account with administrator privileges on the instance. Another account with administrator privileges is a safeguard if you forget the Administrator password or have a problem with the Administrator account.

Create an Elastic IP Address

By default, all Amazon EC2 instances launched into EC2-Classic or a default subnet are assigned two IP addresses at launch: a private (RFC 1918) address and a public address that is mapped to the private IP address through network address translation (NAT). Instances launched into a nondefault subnet do not get a public IP address by default, but can be assigned one at launch.

To connect to your instance, you use the public DNS name associated with the public IP address. However, this name is not static and can change, for example when an instance stops and restarts. If you want a persistent address to connect to, use an Elastic IP address.

Elastic IP addresses are static IP addresses designed for dynamic cloud computing. Additionally, Elastic IP addresses are associated with your account, not specific instances. Any Elastic IP addresses that you associate with your account remain associated with your account until you explicitly release them. Unlike traditional static IP addresses, however, Elastic IP addresses allow you to mask instance or Availability Zone failures by rapidly remapping your public IP addresses to any instance in your account.

To assign an Elastic IP address to your Windows instance

1. Click **Elastic IPs** in the navigation pane.
2. Click **Allocate New Address**.
3. In the **Allocate New Address** dialog box, if your account supports it, select whether you want to use the Elastic IP for EC2 or a VPC. Click **Yes, Allocate**.
4. Select the Elastic IP address you created, and then click **Associate Address**.
5. In the **Associate Address** dialog box, in the **Instance** list, select your instance and then click **Associate**.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Instance Metadata and User Data [For additional reference]

Instance metadata is data about your EC2 instance that you can use to configure or manage the running instance. Instance metadata is divided into categories.

user data : Used to specify parameters for configuring your instance during launch time (with cloud-init)

When you are adding user data, take note of the following:

- User data is treated as opaque data: what you give is what you get back. It is up to the instance to be able to interpret it.
- User data is limited to 16 KB. This limit applies to the data in raw form, not base64-encoded form.
- User data must be base64-encoded before being submitted to the API. The API command line tools perform the base64 encoding for you.

Retrieving Instance Metadata [for additional reference]

To view all categories of instance metadata from within a running instance, use the following URI:

```
http://169.254.169.254/latest/meta-data/
```

Note that you are not billed for HTTP requests used to retrieve instance metadata and user data.

On a Linux instance, you can use a tool such as cURL, or use the GET command, for example:

```
$ GET http://169.254.169.254/latest/meta-data/
```

You can also download the Instance Metadata Query tool, which allows you to query the instance metadata without having to type out the full URI or category names:

<http://aws.amazon.com/code/1825>

Examples of Retrieving Instance Metadata

The following are examples of requests and responses on a Linux instance.

This example gets the available versions of the instance metadata. These versions do not necessarily correlate with an Amazon EC2 API version. The earlier versions are available to you in case you have scripts that rely on the structure and information present in a previous version.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Amazon EC2 Tutorial – For modified GUI

[Course tutorial and much more for extra reading]

```
$ GET http://169.254.169.254/  
1.0  
2007-01-19  
2007-03-01  
2007-08-29  
2007-10-10  
2007-12-15  
2008-02-01  
2008-09-01  
2009-04-04  
2011-01-01  
2011-05-01  
2012-01-12  
latest
```

This example gets the top-level metadata items. Some items are only available for instances in a VPC.

```
$ GET 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  
network/  
placement/  
public-hostname  
public-ipv4  
public-keys/  
reservation-id  
security-groups
```

These examples get the value of some of the metadata items from the preceding example.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Amazon EC2 Tutorial – For modified GUI

[Course tutorial and much more for extra reading]

```
$ GET http://169.254.169.254/latest/meta-data/ami-id  
ami-2bb65342  
$ GET http://169.254.169.254/latest/meta-data/reservation-id  
r-fea54097  
$ GET http://169.254.169.254/latest/meta-data/hostname  
ec2-203-0-113-25.compute-1.amazonaws.com
```

This example gets the list of available public keys.

```
$ GET http://169.254.169.254/latest/meta-data/public-keys/  
0=my-public-key
```

This example shows the formats in which public key 0 is available.

```
$ GET http://169.254.169.254/latest/meta-data/public-keys/0  
openssh-key
```

This example gets public key 0 (in the OpenSSH key format).

```
$ GET http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key  
ssh-rsa MIICiTCcAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC  
VVMxCzAJBgNVBAGTAldBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6  
b24xFDASBgNVBASTC0lBTSBDb25zb2x1MRIwEAYDVQQDEw1UZXRhbnQ2YWMxH2Ad  
BgkqhkiG9w0BCQEWEG5vb25lQGFTYXpvcjE5b20wHhcNMTEwNDI1MjAONTIxWhcN  
MTIwNDI1MjAONTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAGTAldBMRAwDgYD  
VQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBASTC0lBTSBDb25z  
b2x1MRIwEAYDVQQDEw1UZXRhbnQ2YWMxH2AdBgkqhkiG9w0BCQEWEG5vb25lQGFT  
YXpvcjE5b20wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ  
21uUSfwfEvYSWtC2XADZ4nB+BLygVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T  
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE  
Ibb3OhjZnzcVQAaRHh1QWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4  
nUhVVxYUntned9+h8Mg9q6q+auNKyExzyLwax1Aoo7TJHidbtS4J5iNmZgXL0Fkb  
FFBjvSfpJi1J00zbnNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvJx79LjSTb  
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

This example shows the information available for a specific network interface (indicated by the MAC address) on an NAT instance in the EC2-Classical platform.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Amazon EC2 Tutorial – For modified GUI

[Course tutorial and much more for extra reading]

```
$ GET http://169.254.169.254/latest/meta-  
data/network/interfaces/macs/02:29:96:8f:6a:2d/  
device-number  
local-hostname  
local-ipv4s  
mac  
owner-id  
public-hostname  
public-ipv4s
```

This example gets the subnet ID for an EC2 instance launched into a VPC.

```
$ GET http://169.254.169.254/latest/meta-  
data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id  
subnet-be9b61d7
```

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India

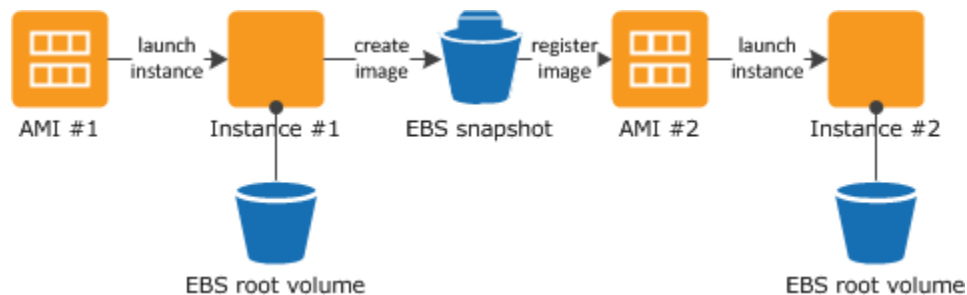


Amazon Machine Images

Creating an Amazon EBS-Backed Linux AMI

Overview of the Creation Process for Amazon EBS-Backed AMIs

The following diagram summarizes the creation process for Amazon EBS-backed AMIs.



First, launch an instance from an AMI that's similar to the AMI that you'd like to create. You can connect to your instance and customize it.

When the instance is set up the way you want it, it's best to stop the instance before you create an AMI to ensure data integrity.

Amazon EC2 powers down the instance before creating the AMI to ensure that everything on the instance is stopped and in a consistent state during the creation process.

If you're confident that your instance is in a consistent state appropriate for AMI creation, you can tell Amazon EC2 not to power down and reboot the instance. Some file systems, such as xfs, can freeze and unfreeze activity, making it safe to create the image without rebooting the instance.

It takes several minutes for the entire AMI creation process to complete. After the process completes, you have a new AMI and snapshot created from the root volume of the instance. When you launch an instance using the new AMI, we create a new EBS volume for its root volume using the snapshot. Both the AMI and the snapshot incur charges to your account until you delete them.

To create an AMI from an instance using the console

1. Open the Amazon EC2 console.
2. If you don't have a running instance that uses an Amazon EBS volume for the root device, you must launch one .
3. (Optional) Connect to the instance and customize it. For example, you can install software and applications, copy data, or attach additional EBS volumes.
4. In the navigation pane, click **Instances** and select your instance. Click **Actions** and then click **Create Image**.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



5. In the **Create Image** dialog box, specify the following, and then click **Create Image**.
 - a. A unique name for the image. **[Name the AMI using your name]**
 - b. (Optional) A description of the image, up to 255 characters.
 - c. By default, Amazon EC2 shuts down the instance, takes snapshots of any attached volumes, creates and registers the AMI, and then reboots the instance.
6. Click **AMIs** in the navigation pane to view the status of your AMI. While the new AMI is being created, its status is `pending`. This process typically takes a few minutes to finish, and then the status of your AMI is `available`.
7. (Optional) Click **Snapshots** in the navigation pane to view the snapshot that was created for the new AMI. When you launch an instance from this AMI, we use this snapshot to create its root device volume.

Copying an AMI

You can easily copy the Amazon Machine Images (AMIs) that you own to other AWS regions and scale your applications to take advantage of AWS's geographically diverse regions.

Copying your AMIs provides the following benefits:

- **Consistent global deployment:** You can copy an AMI from one region to another, enabling you to launch consistent instances based from the same AMI into different regions.
- **Scalability:** You can more easily design and build world-scale applications that meet the needs of your users, regardless of their location.
- **Performance:** You can increase performance by distributing your application, as well as locating critical components of your application in closer proximity to your users. You can also take advantage of region-specific features, such as instance types or other AWS services.
- **High availability:** You can design and deploy applications across AWS regions, to increase availability.

AMI Copy

You can copy both Amazon EBS-backed AMIs and instance-store-backed AMIs. You can copy an AMI to as many regions as you like. You can also copy an AMI to the same region. Each copy of an AMI results in a new AMI with its own unique AMI ID. When you launch an instance from an AMI, we launch it into the same region as the AMI you select, as shown in the following diagram.

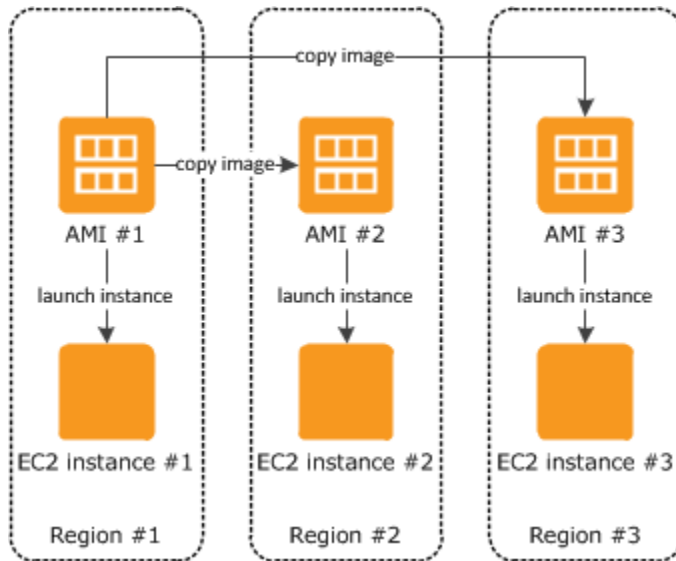
By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



[Course tutorial and much more for extra reading]



When you copy an AMI, the new AMI is fully independent of the source AMI; there is no link to the original (source) AMI. You can modify the new AMI without affecting the source AMI. The reverse is also true: you can modify the source AMI without affecting the new AMI. Therefore, if you make changes to the source AMI and want those changes to be reflected in the AMI in the destination region, you must recopy the source AMI to the destination region.

Copying an Amazon EC2 AMI

Prior to copying an AMI, you must ensure that the contents of the source AMI are updated to support running in a different region. For example, you should update any database connection strings or similar application configuration data to point to the appropriate resources. Otherwise, instances launched from the new AMI in the destination region may still use the resources from the source region, which can impact performance and cost.

You can copy an AMI using the AWS Management Console, the AWS CLI, the Amazon EC2 CLI, or the Amazon EC2 API.

Copying an AMI Using the Amazon EC2 Console

To copy an AMI using the console

1. Open the Amazon EC2 console.
2. From the navigation bar, select the region that contains the AMI to copy.
3. In the navigation pane, click **AMIs**.
4. Select the AMI to copy, click **Actions**, and then click **Copy AMI**.
5. In the **AMI Copy** page, set the following fields, and then click **Copy AMI**:

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



- **Destination region:** Select the region to which you want to copy the AMI.
 - **Name:** Specify a name for the new AMI.
 - **Description:** By default, the description includes information about the source AMI so that you can identify a copy from the original. You can change this description as necessary.
6. We display a confirmation page to let you know that the copy operation has been initiated and provide you with the ID of the new AMI.

To check on the progress of the copy operation immediately, click the provided link to switch to the destination region. To check on the progress later, click **Done**, and then when you are ready, use the navigation pane to switch to the destination region.

The initial status of the destination AMI is `pending` and the operation is complete when the status is `available`.

[Important Note : During Practice, If you copy an AMI do not forget to delete the AMI from source and destination]

Instance Types

When you launch an instance, the *instance type* that you specify determines the hardware of the host computer used for your instance. Each instance type offers different compute, memory, and storage capabilities. Select an instance type based on the requirements of the application or software that you plan to run on your instance.

Amazon EC2 provides each instance with a consistent and predictable amount of CPU capacity, regardless of its underlying hardware.

Spot Instances

If you have flexibility on when your application will run, you can bid on unused Amazon EC2 compute capacity, called Spot Instances, and lower your costs significantly. Set by Amazon EC2, the Spot price for these instances fluctuates periodically depending on the supply of and demand for Spot Instance capacity.

To use Spot Instances, you place a Spot Instance request (your bid) specifying the maximum price you are willing to pay per hour per instance. If the maximum price of your bid is greater than the current Spot price, your request is fulfilled and your instances run until you terminate them or the Spot price increases above your maximum price. Your instance can also be terminated when your bid price equals the market price, even when there is no increase in the market price. This can happen when demand for capacity rises, or when supply fluctuates.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Reserved Instances

Amazon Elastic Compute Cloud (Amazon EC2) Reserved Instances is a pricing model that enables you to reserve capacity for your EC2 instances and lowers your average instance cost. With Reserved Instances, you pay a low, one-time fee for the capacity reservation and then receive a significant discount on the hourly charge for your instances. When you want to use your reserved capacity, you launch an EC2 instance with the same configuration as the reserved capacity that you purchased. Amazon Web Services (AWS) will automatically apply the discounted hourly rate that is associated with your capacity reservation. You are charged the discounted hourly rate for your EC2 instance for as long as you own the Reserved Instance. When the term of your Reserved Instance ends, you can continue using the EC2 instance without interruption. However, you will now be charged at the On-Demand rate.

Reserved Instances can provide substantial savings over owning your own hardware or running only On-Demand instances, as well as help assure that the capacity you need is available to you when you require it.

To purchase an Amazon EC2 Reserved Instance, you must select an instance type (such as m1.small), platform (Linux/UNIX, Windows, or Windows with SQL Server), location (region and Availability Zone), and term (either one year or three years). If you want your Reserved Instance to run on a specific Linux/UNIX platform, you must identify that platform when you purchase the reserved capacity. Then, when you're ready to use the Reserved Instance that you purchased, you must choose an Amazon Machine Image (AMI) that runs that specific Linux/UNIX platform, along with any other specifications you identified during the purchase.

Differences Between Reboot, Stop, and Terminate

The following table summarizes the key differences between rebooting, stopping, and terminating your instance.

Characteristic	Reboot	Stop/start	Terminate
Host computer	The instance stays on the same host computer	The instance runs on a new host computer	None
Private and public IP addresses	These addresses stay the same	The instance gets new private and public IP addresses	None
Elastic IP addresses	The Elastic IP address remains associated with the instance	EC2-Classic: The Elastic IP address is disassociated from the instance EC2-VPC: The Elastic IP address remains associated with the instance	The Elastic IP address is disassociated from the instance
Instance store volumes	The data is preserved	The data is lost	The data is lost

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Amazon EC2 Tutorial - For modified GUI

[Course tutorial and much more for extra reading]

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India

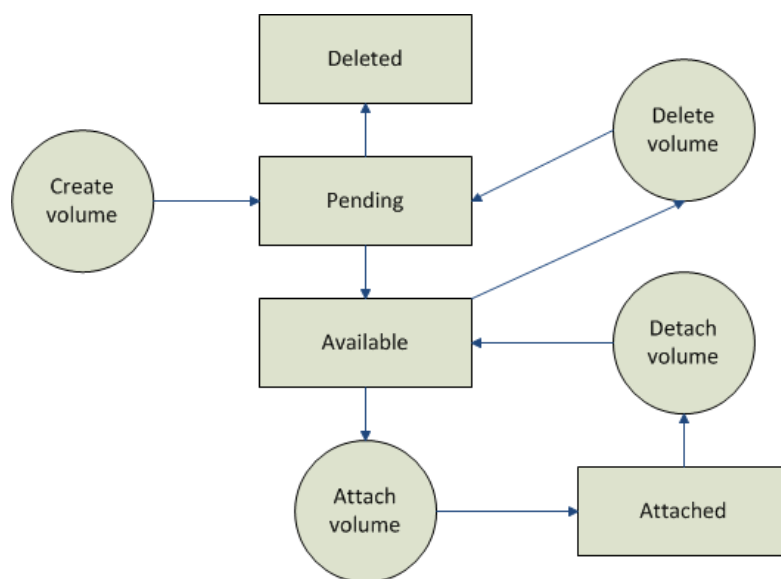


Amazon Elastic Block Store (Amazon EBS)

Amazon Elastic Block Store (Amazon EBS) provides block level storage volumes for use with Amazon EC2 instances. Amazon EBS volumes are highly available and reliable storage volumes that can be attached to any running instance that is in the same Availability Zone. Amazon EBS volumes that are attached to an Amazon EC2 instance are exposed as storage volumes that persist independently from the life of the instance. With Amazon EBS, you only pay for what you use.

Amazon EBS volumes behave like raw, unformatted block devices. You can create a file system on top of these volumes, or use them in any other way you would use a block device (like a hard drive). For more information on creating file systems and mounting volumes,

Amazon EBS Volumes - States



To create a new Amazon EBS volume

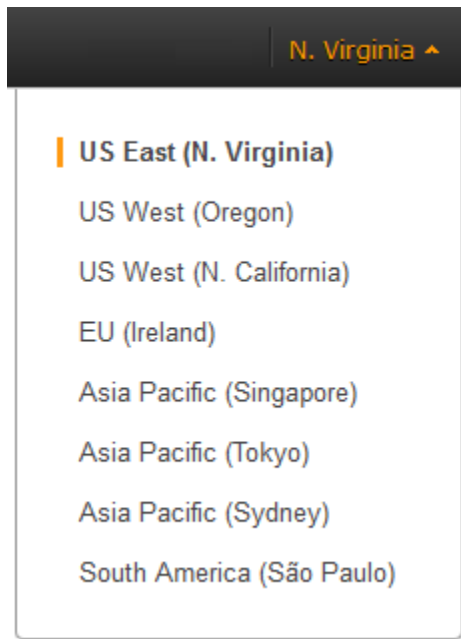
1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. From the navigation bar, select the region in which you would like to create your volume. This choice is important because some Amazon EC2 resources can be shared between regions, while others can't.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India





3. Click **Volumes** in the navigation pane.
4. Above the upper pane, click **Create Volume**.
5. In the **Create Volume** dialog box, in the **Volume Type** list, select **Standard** or **Provisioned IOPS**. [Default: choose Standard]

Note: With Amazon EBS provisioned IOPS (input/output operations per second) volumes, you can provision a specific level of I/O performance, up to 4000 IOPS per volume. This allows you to predictably scale to thousands of IOPS per Amazon EC2 instance

6. In the **Size** box and **GiB** list, select the size of the volume (in GiB or TiB).
7. For Provisioned IOPS volumes, in the **IOPS** box, enter the maximum number of input/output operations per second (IOPS) that the volume should support.
8. In the **Availability Zone** list, select the Availability Zone in which to create the volume.
9. Click **Yes, Create**.

Attaching an Amazon EBS Volume to an Instance

To attach an Amazon EBS volume to an instance

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. Click **Volumes** in the navigation pane.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



[Course tutorial and much more for extra reading]

The console displays a list of current volumes.

3. Select a volume and click **Attach Volume**.

The **Attach Volume** dialog box appears.

4. Select the instance to attach the volume to from the **Instance** list (only instances in the same Availability Zone as the volume are displayed).
5. Select how the device is exposed to the instance from the **Device** list.
6. Click **Attach** to attach the volume to the instance. The volume and instance must be in the same Availability Zone.

Making an Amazon EBS Volume Available for Use

1. Connect to your instance using SSH.
2. Depending on the block device driver of your instance's kernel, the device may be attached with a different name than what you specify. For example, if you specify a device name of `/dev/sdh`, your device may be renamed `/dev/xvdh` or `/dev/hdh` by the kernel; in some cases, even the trailing letter may also change (where `/dev/sda` could become `/dev/xvde`). Amazon Linux AMIs create a symbolic link from the renamed device path to the name you specify, but other AMIs may behave differently.
3. If you want to create a partition, following steps will help you. [Note: You can directly use the disk after formatting it with a ext3 or ext4 file system , without a partition]

sudo fdisk -l command is used to show details on disk partitions. To create a partition use **fdisk** with the device name

e.g:

sudo fdisk /dev/xvdh [or whatever the actual device name is]

following the portioning menu [only if required to create a partition]

n- new partition

p – Primary Partition

1 – first partition

t – Type of the Partition (83 for Linux)

w- Write the Partition to the disk

4. Use the following command to create an ext3 file system on the volume.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Caution

This step assumes that you're mounting an empty volume. If you're mounting a volume that already has data on it (for example, a volume that was restored from a snapshot), don't use **mkfs** before mounting the volume (skip to the next step instead). Otherwise, you'll format the volume and delete the existing data.

```
$ sudo mkfs -t ext3 device_name or partition name
e.g. sudo mkfs -t ext3 /dev/xvdh1
where /dev/xvdh1 is the name of the partition.
```

5. Use the following command to create the directory.

```
$ sudo mkdir volume_name
```

6. Use the following command to mount the volume.

```
$ sudo mount device_name volume_name
```

7. (Optional) To enable the instance to reconnect to an Amazon EBS volume on reboot, add the device to the fstab or create a script that automatically mounts the volume on startup.

To detach an Amazon EBS volume

1. First, unmount the volume.

For Linux/UNIX, use the following command to unmount the /dev/sdh device.

```
# umount -d /dev/sdh
```

For Windows, open **Disk Management**, right-click the volume to unmount, and select **Change Drive Letter and Path**. Then, select the mount point to remove and click **Remove**.

2. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
3. Click **Volumes** in the navigation pane.

The console displays a list of current volumes.

4. Select a volume and click **Detach Volume**.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



A confirmation dialog box appears.

5. Click **Yes, Detach**.

The volume is detached from the instance.

Caution

If your volume stays in the *detaching* state, you can force the detachment by clicking **Force Detach**. Forcing the detachment can lead to data loss or a corrupted file system. Use this option only as a last resort to detach a volume from a failed instance, or if you are detaching a volume with the intention of deleting it. The instance doesn't get an opportunity to flush file system caches or file system metadata. If you use this option, you must perform file system check and repair procedures.

If you've tried to force the volume to detach multiple times over several minutes and it stays in the *detaching* state, you can post a request for help to the [Amazon EC2 forum](#). To help expedite a resolution, include the volume ID and describe the steps that you've already taken.

For Windows Instances:

Make the Volume Available on Windows

To use an Amazon EBS volume

1. Log in to your instance using Remote Desktop.
2.
 - Windows Server 2012: Go to the Start screen.
 - Windows Server 2008: On the taskbar, click **Start**, and then click **Run**.
3. Type **diskmgmt.msc** and press **Enter**. The **Disk Management** utility opens.

Caution

If you're mounting a volume that already has data on it (for example, a public data set), make sure you don't reformat the volume and delete the existing data.

4. Select the disk that represents the new Amazon EBS volume.

By ANIL KUMAR

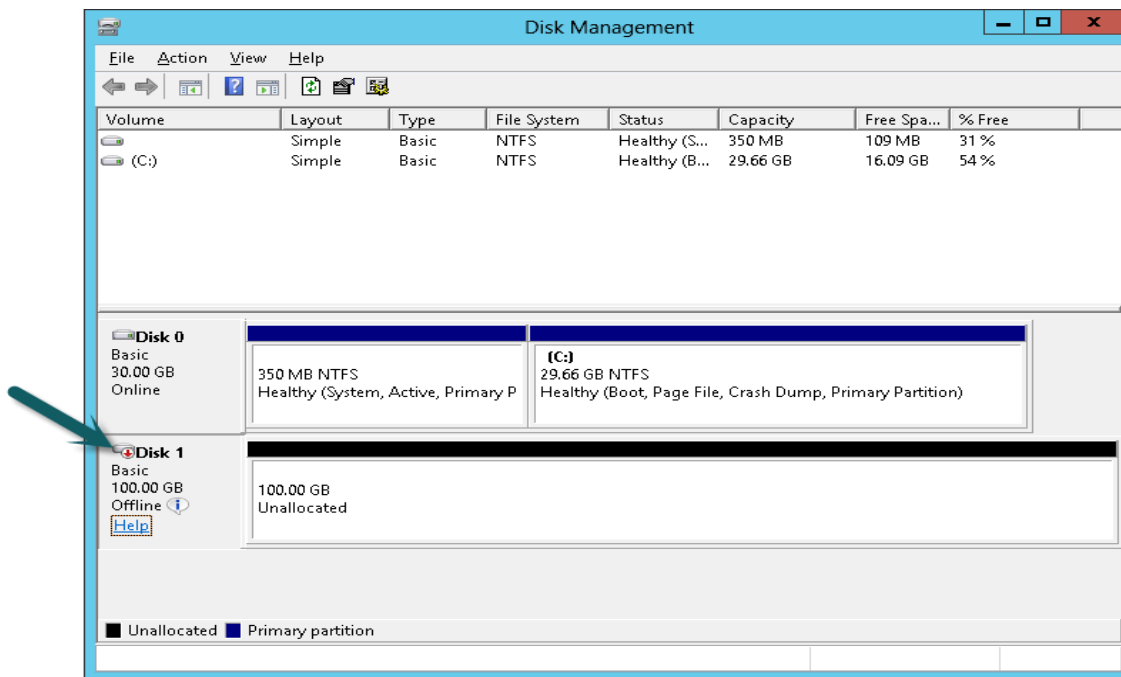
cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India

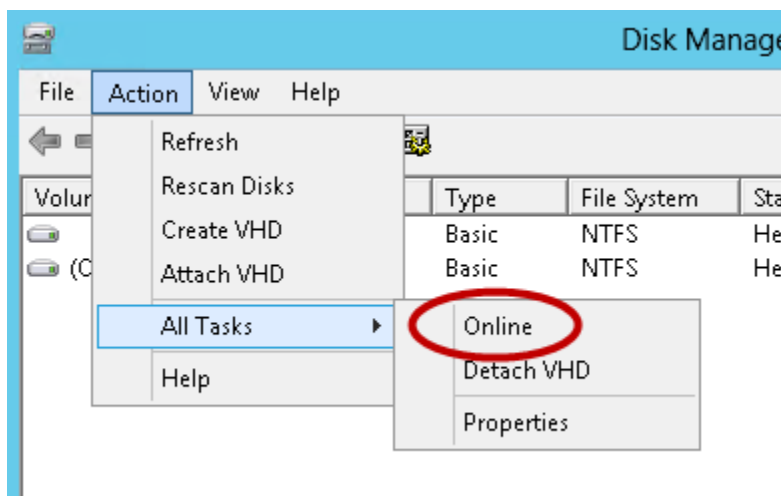


Amazon EC2 Tutorial – For modified GUI

[Course tutorial and much more for extra reading]



5. On the **Disk Management** menu, select **Action - All Tasks - Online**.



6. A new disk needs to be initialized before it can be used. To initialize the disk:
- In the Disk Management utility, select the new Amazon EBS volume disk.
 - On the **Disk Management** menu, select **Action - All Tasks - Initialize Disk**.
 - In the **Initialize Disk** dialog, select the disk to initialize, select the desired partition style, and press **OK**.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Your new Amazon EBS volume is now available for use. Any data written to this file system is written to the Amazon EBS volume and is transparent to applications using the device.

To detach an Amazon EBS volume

For Windows, open **Disk Management**, right-click the volume to unmount, and select **Change Drive Letter and Path**. Then, select the mount point to remove and click **Remove**.

Caution

If your volume stays in the *detaching* state, you can force the detachment by clicking **Force Detach**. Forcing the detachment can lead to data loss or a corrupted file system. Use this option only as a last resort to detach a volume from a failed instance, or if you are detaching a volume with the intention of deleting it. The instance doesn't get an opportunity to flush file system caches or file system metadata. If you use this option, you must perform file system check and repair procedures.

If you've tried to force the volume to detach multiple times over several minutes and it stays in the *detaching* state, you can post a request for help to the [Amazon EC2 forum](#). To help expedite a resolution, include the volume ID and describe the steps that you've already taken.

Creating an Amazon EBS Snapshot

AWS Management Console

To create a snapshot

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. Click **Snapshots** in the navigation pane.

The console displays a list of current snapshots.

3. Click **Create Snapshot**.

The Create Snapshot dialog box appears.

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

Amazon EC2 begins creating the snapshot.

To delete a snapshot

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. Click **Snapshots** in the navigation pane.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Amazon EC2 Tutorial – For modified GUI

[Course tutorial and much more for extra reading]

The console displays a list of current snapshots.

3. Select a snapshot and click **Delete Snapshot**.

A confirmation dialog box appears.

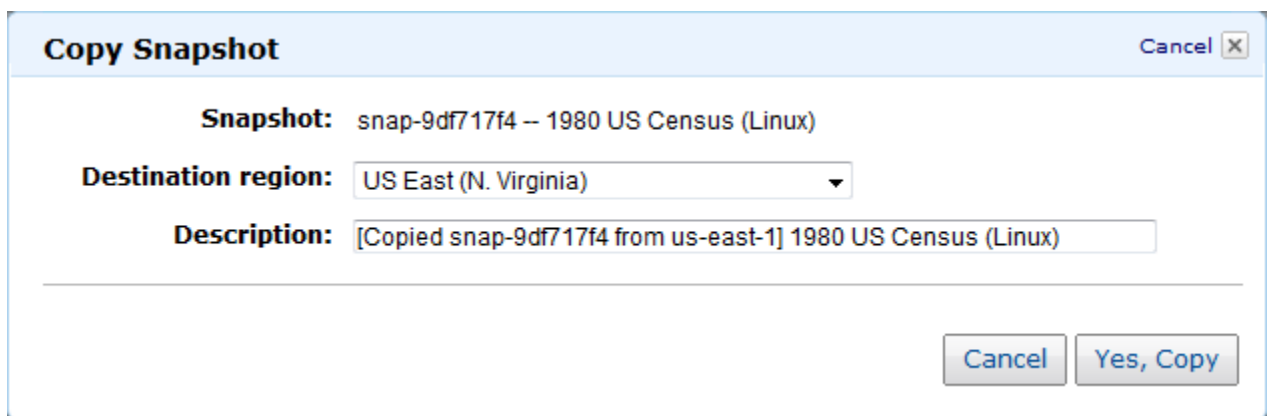
4. Click **Yes, Delete**.

The snapshot is deleted.

To copy a snapshot using the Amazon EC2 console

You can create a copy of an Amazon EBS snapshot using the Amazon EC2 console.

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, under **ELASTIC BLOCK STORE**, click **Snapshots**.
3. In the **EBS Snapshots** pane, right-click the snapshot to copy, and then click **Copy Snapshot**.
4. In the **Copy Snapshot** dialog box, update the following as necessary:
 - **Snapshot:** Select another snapshot, if appropriate.
 - **Destination region:** Select the region where you want to write the copy of the snapshot.
 - **Description:** By default, the description includes information about the source snapshot so that you can identify a copy from the original. You can change this description as necessary.
5. Click **Yes, Copy**.



Copy Snapshot Cancel X

Snapshot: snap-9df717f4 -- 1980 US Census (Linux)

Destination region: US East (N. Virginia) ▼

Description: [Copied snap-9df717f4 from us-east-1] 1980 US Census (Linux)

Cancel Yes, Copy

6. In the **Copy Snapshot** confirmation dialog box, you can click **Snapshots** to go to the **EBS Snapshots** pane in the region specified, or click **Close**.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Amazon EC2 Tutorial – For modified GUI

[Course tutorial and much more for extra reading]



To view the progress of the copy process later, switch the Amazon EC2 console to the destination region, and then refresh the **EBS Snapshots** pane. Copies in progress are listed at the top of the **EBS Snapshots** pane.

To modify snapshot permissions

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. Click **Snapshots** in the navigation pane.

The console displays a list of current snapshots and their status.

3. Select a snapshot and click **Permissions**.

The **Modify Snapshot Permissions** dialog box appears.

4. Choose whether to make the snapshot public or to share it with select AWS accounts:

Important

Making your snapshot public shares all snapshot data with everyone. Snapshots with AWS Marketplace product codes cannot be made public.

- To make the snapshot public, select **Public** and click **Save**.
- To expose the snapshot only to specific AWS accounts, select **Private**, enter the IDs of those AWS accounts, and click **Save**.

The console modifies permissions for the snapshot

Public Data Set Concepts

Amazon Web Services provides a repository of public data sets that can be seamlessly integrated into AWS cloud-based applications. Amazon stores the data sets at no charge to the community and, as with all AWS services, you pay only for the compute and storage you use for your own applications.

Previously, large data sets such as the mapping of the Human Genome and the US Census data required hours or days to locate, download, customize, and analyze. Now, anyone can access these data sets from an Amazon EC2 instance and start computing on the data within minutes. You can also leverage the entire AWS ecosystem and easily collaborate with other AWS users. For example, you can produce or use prebuilt server images with tools and applications to analyze the data sets. By hosting this important and useful data with cost-efficient services such as Amazon EC2, AWS hopes to provide researchers across a variety of disciplines and industries with tools to enable more innovation, more quickly.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Available Public Data Sets

Public data sets are currently available in the following categories:

- **Biology**—Includes Human Genome Project, GenBank, and other content.
- **Chemistry**—Includes multiple versions of PubChem and other content.
- **Economics**—Includes census data, labor statistics, transportation statistics, and other content.
- **Encyclopedic**—Includes Wikipedia content from multiple sources and other content.

Creating a Public Data Set Volume from a Snapshot

To use a public data set that is in Amazon EBS snapshot format, you create a new volume, specifying the snapshot ID of the public data set. You can create your new volume using the AWS Management Console as follows. If you prefer, you can use the [ec2-create-volume](#) command instead.

To create a public data set volume from a snapshot

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. From the navigation bar, select the region that your data set snapshot is located in.

Important

Snapshot IDs are constrained to a single region, and you cannot create a volume from a snapshot that is located in another region. In addition, you can only attach an Amazon EBS volume to an instance in the same Availability Zone. For more information, see [Resource Locations](#).

To create this volume in a different region, you can copy the snapshot to your required region and then restore it to a volume in that region. For more information, see [Copying an Amazon EBS Snapshot](#).

3. In the navigation pane, click **Volumes**.
4. Above the upper pane, click **Create Volume**.
5. In the **Create Volume** dialog box, in the **Volume Type** list, select **Standard** or **Provisioned IOPS**. For more information, see [Amazon EBS Volume Types](#).
6. In the **Snapshot** list, select the ID of the snapshot for your data set.

Note

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



[Course tutorial and much more for extra reading]

If the snapshot ID you are expecting to see does not appear, you may have a different region selected in the Amazon EC2 console.

7. In the **Size** field and **GiB** list, select the size of the volume (in GiB or TiB), or verify that the default size of the snapshot is adequate.

Note

If you specify both a volume size and a snapshot ID, the size must be equal to or greater than the snapshot size. When you select a volume type and a snapshot ID, minimum and maximum sizes for the volume are shown next to the **Size** list.

8. For Provisioned IOPS volumes, in the **IOPS** field, enter the maximum number of input/output operations per second (IOPS) that you want the volume to support.
9. In the **Availability Zone** list, select the Availability Zone in which to create the volume.

Important

Amazon EBS volumes can only be attached to instances in the same Availability Zone.

10. Click **Yes, Create**.

Important

If you created a larger volume than the default size for that snapshot (by specifying a size in Step 7), you need to extend the file system on the volume to take advantage of the extra space

Attaching and Mounting the Public Data Set Volume

After you have created your new data set volume, you need to attach it to an Amazon EC2 instance to access the data

Installing the Amazon EC2 Command Line Interface Tools on Windows

[Separate document will be provided]

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Elastic Load Balancing

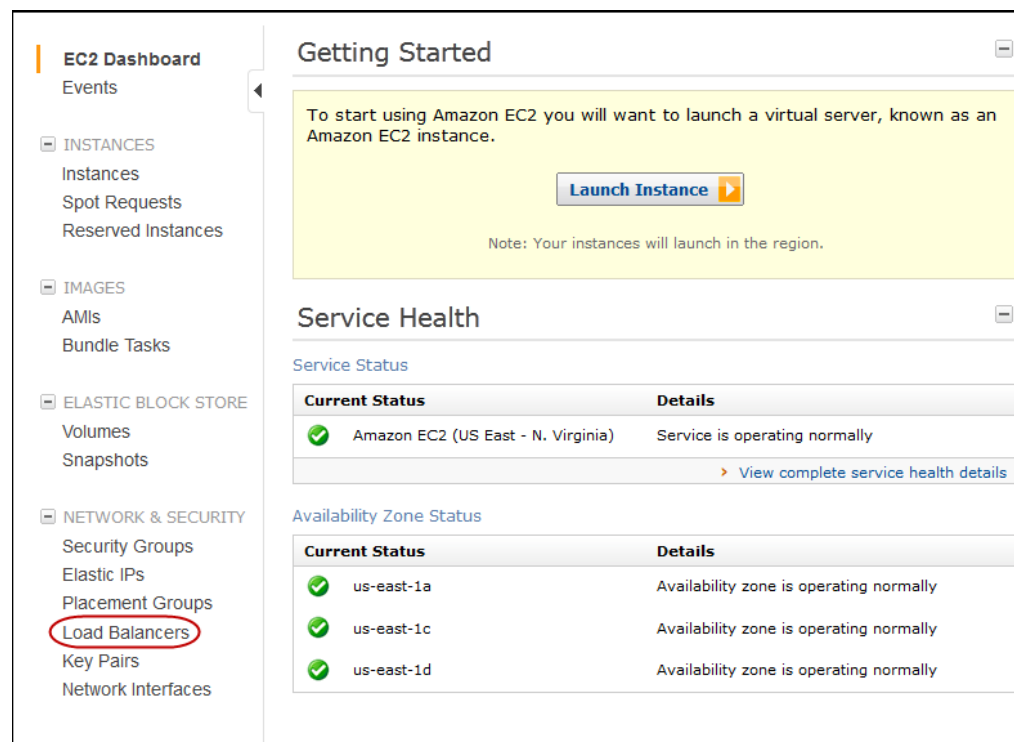
Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances. It enables you to achieve even greater fault tolerance in your applications, seamlessly providing the amount of load balancing capacity needed in response to incoming application traffic

Create a Basic Load Balancer in EC2-Classical

Configure Listeners for Your Load Balancer

To configure listeners for your load balancer

1. Sign in to the AWS Management Console and open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. Start the **Create Load Balancer** wizard:
 - a. On the Amazon EC2 console Getting Started page, in the **EC2 Dashboard** pane, under **NETWORK & SECURITY**, click **Load Balancers**.



- b. On the **Load Balancers** page, click **Create Load Balancers**.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



[Course tutorial and much more for extra reading]

3. On the **DEFINE LOAD BALANCER** page, make the following selections:
 - a. Enter a name for your load balancer (e.g., **my-test-loadbalancer**).
 - b. Leave **CreateLB inside** set to **EC2** for this tutorial.
 - c. Leave **Listener Configuration** set to the default value for this example.

Important

The default settings require that your Amazon EC2 HTTP servers are active and accepting requests on port 80.

Create a New Load Balancer Cancel X

DEFINE LOAD BALANCER CONFIGURE HEALTH CHECK ADD EC2 INSTANCES REVIEW

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

Load Balancer Name: my-test-loadbalancer

Create LB inside: EC2

Create an internal load balancer: ☐ (what's this?)

Listener Configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port	Actions
HTTP	80	HTTP	80	Remove
HTTP		HTTP		Save

Continue

- 4.
5. Click **Continue** to configure health check for your Amazon EC2 instances.

Configure Health Check for Your Amazon EC2 Instances

Elastic Load Balancing routinely checks the health of each load-balanced Amazon EC2 instance based on the configurations that you specify. If Elastic Load Balancing finds an unhealthy instance, it stops sending traffic to the instance and reroutes traffic to healthy instances.

To configure a health check for your Amazon EC2 instances

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



[Course tutorial and much more for extra reading]

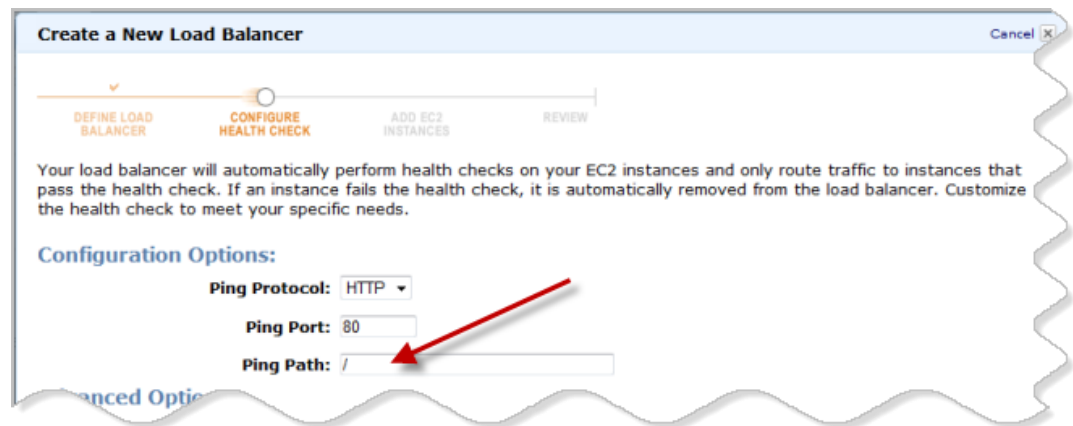
1. On the **CONFIGURE HEALTH CHECK** page of the **Create a New Load Balancer** wizard, set the following configurations:
 - a. Leave **Ping Protocol** set to its default value of `HTTP`.
 - b. Leave **Ping Port** set to its default value of `80`.

Elastic Load Balancing pings the port you choose (in this example, port 80) to send health check queries to your Amazon EC2 instances.

Important

Your Amazon EC2 instances must accept incoming traffic on the ping port. This example assumes that each of your instances has a working HTTP server that accepts incoming traffic on port 80.

- c. In the **Ping Path** field, replace the default value with a single forward slash ("/").



Elastic Load Balancing sends health check queries to the path you specify in **Ping Path**. This example uses a single forward slash so that Elastic Load Balancing sends the query to your HTTP server's default home page, whether that default page is named `index.html`, `default.html`, or a different name.

- d. Leave the **Advanced Options** set to their default values.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Amazon EC2 Tutorial – For modified GUI

[Course tutorial and much more for extra reading]

The screenshot shows the 'Create a New Load Balancer' wizard with four steps: DEFINE LOAD BALANCER, CONFIGURE HEALTH CHECK (current step), ADD EC2 INSTANCES, and REVIEW. A progress bar at the top indicates the current step. Below the progress bar, a text block explains that the load balancer will perform health checks on EC2 instances and only route traffic to those that pass. The 'Configuration Options' section includes a 'Ping Protocol' dropdown set to 'HTTP', a 'Ping Port' input field set to '80', and a 'Ping Path' input field set to '/'. The 'Advanced Options' section includes a 'Response Timeout' input field set to '5' seconds, a 'Health Check Interval' input field set to '0.5' minutes, an 'Unhealthy Threshold' slider set to '2', and a 'Healthy Threshold' slider set to '10'. To the right of these sliders, explanatory text describes each option: 'Time to wait when receiving a response from the health check (2 sec - 60 sec)', 'Amount of time between health checks (0.1 min - 5 min)', 'Number of consecutive health check failures before declaring an EC2 instance unhealthy', and 'Number of consecutive health check successes before declaring an EC2 instance healthy'. At the bottom, there are 'Back' and 'Continue' buttons.

Create a New Load Balancer Cancel

DEFINE LOAD BALANCER CONFIGURE HEALTH CHECK ADD EC2 INSTANCES REVIEW

Your load balancer will automatically perform health checks on your EC2 instances and only route traffic to instances that pass the health check. If an instance fails the health check, it is automatically removed from the load balancer. Customize the health check to meet your specific needs.

Configuration Options:

Ping Protocol: HTTP

Ping Port: 80

Ping Path: /

Advanced Options:

Response Timeout: 5 Seconds

Health Check Interval: 0.5 Minutes

Unhealthy Threshold: 2 3 4 5 6 7 8 9 10

Healthy Threshold: 2 3 4 5 6 7 8 9 10

Time to wait when receiving a response from the health check (2 sec - 60 sec).

Amount of time between health checks (0.1 min - 5 min)

Number of consecutive health check failures before declaring an EC2 instance unhealthy.

Number of consecutive health check successes before declaring an EC2 instance healthy.

[Back](#) [Continue](#)

2. Click **Continue** to register your Amazon EC2 instances with your load balancer.

Register Amazon EC2 Instances

Now that you've made your configuration choices you're ready to register your EC2 instances using the **ADD EC2 INSTANCES** page of the **Create Load Balancer** wizard.

To register your Amazon EC2 instances

1. On the **ADD EC2 INSTANCES** page, check the boxes in the **Select** column to add instances to your load balancer.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Create a New Load Balancer

Cancel

DEFINE LOAD BALANCER

CONFIGURE HEALTH CHECK

ADD EC2 INSTANCES

REVIEW

The table below lists all your running EC2 Instances that are not already behind another load balancer or part of an auto-scaling capacity group. Check the boxes in the Select column to add those instances to this load balancer.

Manually Add Instances to Load Balancer:

Select	Instance	Name	State	Security Groups	Availability Zone
<input checked="" type="checkbox"/>	i-67388616		running	default	us-east-1a
<input checked="" type="checkbox"/>	i-6b38861a		running	default	us-east-1a
<input checked="" type="checkbox"/>	i-4f318f3e		running	default	us-east-1d
<input checked="" type="checkbox"/>	i-31318f40		running	default	us-east-1d

[select all](#) | [select none](#)

Availability Zone Distribution:

2 instances in us-east-1a
2 instances in us-east-1d

< Back Continue

- Click **Continue** to review your settings and then create your load balancer.

Review Settings and Create Your Load Balancer

Now that you've registered your EC2 instances with your load balancer it's time to review the settings you have selected.

To review your settings

- On the **REVIEW** page of the **Create a New Load Balancer** wizard, check your settings. You can make changes by clicking the edit link for each setting.

Note

You can modify some of the settings even after you've created your load balancer. For example, you can modify the port configurations, health check configurations, and add or remove EC2 instances from your load balancer.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Amazon EC2 Tutorial – For modified GUI

[Course tutorial and much more for extra reading]

The screenshot shows the 'Create a New Load Balancer' wizard in the AWS Management Console, specifically the 'REVIEW' step. The wizard has four steps: DEFINE LOAD BALANCER, CONFIGURE HEALTH CHECK, ADD EC2 INSTANCES, and REVIEW. The 'REVIEW' step is currently active, indicated by a progress bar. The configuration details are as follows:

- Load Balancer Name:** my-test-loadbalancer
- Scheme:** internet-facing
- Port Configuration:** 80 (HTTP) forwarding to 80 (HTTP)
- Configure Health Check:**
 - Ping Target:** HTTP:80:/
 - Timeout:** 5
 - Interval:** 0.5
 - Unhealthy Threshold:** 2
 - Healthy Threshold:** 10
- Add EC2 Instances:** i-67388616, i-6b38861a, i-4f318f3e, i-31318f40
- VPC Information:**
 - VPC:**
 - Subnets:**

At the bottom, there is a '< Back' button and a 'Create' button with a right arrow. A note at the bottom right states: 'Please review your selections on this page. Clicking "Create" will launch your load balancer. Check the Amazon EC2 product page for load balancer pricing info.'

Red circles highlight the 'Edit Load Balancer Definition', 'Edit Health Check', and 'Edit EC2 Instance Selection' links.

2. Click **Create** to create your load balancer.

Verify the Creation of Your Load Balancer

Now that you've created your load balancer, you're ready to verify its settings.

To verify creation of your load balancer

1. After you click **Create** button in the **REVIEW** page, a confirmation window opens. Click **Close**.

The screenshot shows a confirmation window titled 'Create a New Load Balancer'. It contains a green checkmark and the text: 'Your load balancer has been created.' Below this, a note states: 'Note: It may take a few minutes for your instances to become active in the new load balancer.' and a link: '> View my load balancers and check their status.' At the bottom, there is a '< Back' button and a 'Close' button with a right arrow.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Amazon EC2 Tutorial – For modified GUI

[Course tutorial and much more for extra reading]

- When the confirmation window closes, the Load Balancers page opens. Your new load balancer now appears in the list.


Create Load Balancer

Delete

Viewing:

All Load Balancers

Search

<input type="checkbox"/>	Load Balancer Name	DNS Name	Port Configuration
<input type="checkbox"/>	 my-test-loadbalancer	my-test-loadbalancer-1367487779.us-east-1.elb.amazonaws.co	80 (HTTP) forwarding to 80 (HTTP)


- Select the check box next to your load balancer.

The Load Balancer selected pane displays the description of your load balancer. Verify that the descriptions match your specifications.


[Create Load Balancer](#) [Delete](#)

Viewing: All Load Balancers

☒ ☐

Load Balancer Name	DNS Name	Port Configuration
 my-test-loadbalancer	my-test-loadbalancer-1367487779.us-east-1.elb.amazonaws.co	80 (HTTP) forwarding to 80 (HTTP)

1 Load Balancer selected

 **Load Balancer: my-test-loadbalancer**

DescriptionInstancesHealth CheckSecurityListeners

DNS Name: [my-test-loadbalancer-1367487779.us-east-1.elb.amazonaws.com \(A Record\)](#)
ipv6.my-test-loadbalancer-1367487779.us-east-1.elb.amazonaws.com (AAAA Record)
dualstack.my-test-loadbalancer-1367487779.us-east-1.elb.amazonaws.com (A or AAAA Record)

Note: Because the set of IP addresses associated with a LoadBalancer can change over time, you should never create an "A" record with any specific IP address. If you want to use a friendly DNS name for your LoadBalancer instead of the name generated by the Elastic Load Balancing service, you should create a CNAME record for the LoadBalancer DNS name, or use Amazon Route 53 to create a hosted zone. For more information, see the [Using Domain Names With Elastic Load Balancing](#)

Scheme: internet-facing

Status: [0 of 4 instances in service](#)

Port Configuration: 80 (HTTP) forwarding to 80 (HTTP)
Stickiness: Disabled [\(edit\)](#)

Availability Zones: us-east-1a
us-east-1d

Source Security Group: amazon-elb/amazon-elb-sg
Owner Alias: amazon-elb
Group Name: amazon-elb-sg

Hosted Zone ID: Z3DZXE0Q79N41H

VPC ID: -

If the description in the **Status** row indicates that some of your instances are not in service, its probably because your instances are still in the registration process.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



Amazon EC2 Tutorial – For modified GUI

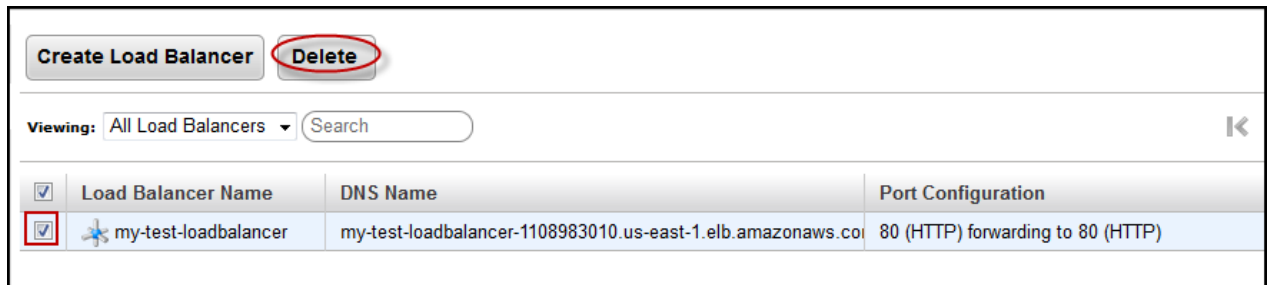
[Course tutorial and much more for extra reading]

4. You can test your load balancer after you've verified that at least one of your EC2 instances is *InService*. To test your load balancer, copy the **DNS Name** value that is listed in the **Description** tab and paste it into the address field of an Internet-connected web browser. If your load balancer is working, you will see the default page of your HTTP server.

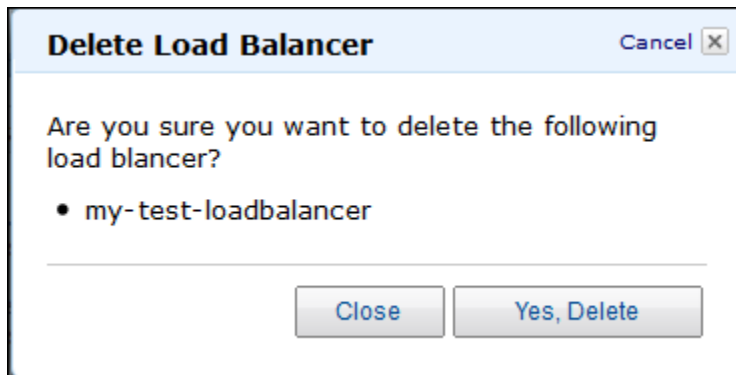
Congratulations! You've successfully created a basic load balancer.

To delete your load balancer

1. On the Amazon EC2 console [Getting Started](#) page, in the **EC2 Dashboard** pane, under **NETWORK & SECURITY**, click **Load Balancers**.
2. Select the check box next to the load balancer you want to delete, and then click **Delete**.



3. In the **Delete Load Balancer** window, click **Yes, Delete**.



By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India

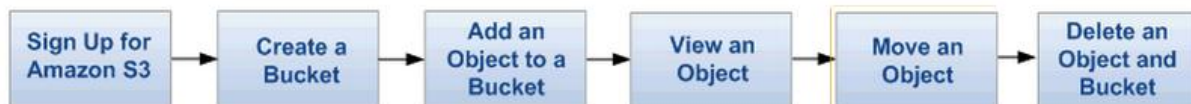


Amazon S3: Simple Storage Service

Get Started With Amazon Simple Storage Service

Amazon Simple Storage Service (Amazon S3) is storage for the internet. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere on the web. You can accomplish these tasks using the AWS Management Console , which is a simple and intuitive web interface.

Steps:



Amazon S3 Basics

To get the most out of Amazon S3, you need to understand a few simple concepts. Amazon S3 stores data as objects within buckets. An object is comprised of a file and optionally any metadata that describes that file.

To store an object in Amazon S3, you upload the file you want to store to a bucket. When you upload a file, you can set permissions on the object as well as any metadata.

Buckets are the containers for objects. You can have one or more buckets. For each bucket, you can control access to the bucket (who can create, delete, and list objects in the bucket), view access logs for the bucket and its objects, and choose the geographical region where Amazon S3 will store the bucket and its contents.

When using the AWS Management Console you can create folders to group objects. You can nest folders (create folders within folders).

Rules for Bucket Naming

In all regions except for the US Standard region, a bucket name must comply with the following rules. These rules result in a DNS-compliant bucket name.

- Bucket names must be at least 3 and no more than 63 characters long.
- Bucket names must be a series of one or more labels. Adjacent labels are separated by a single period (.). Bucket names can contain lowercase letters, numbers, and dashes. Each label must start and end with a lowercase letter or a number.
- Bucket names must not be formatted as an IP address (e.g., 192.168.5.4).

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



The following examples are valid bucket names:

- myawsbucket
- my.aws.bucket
- myawsbucket.1

The following examples are invalid bucket names:

Invalid Bucket Name	Comment
.myawsbucket	Bucket name cannot start with a period (.).
myawsbucket.	Bucket name cannot end with a period (.).
my..examplebucket	There can only be one period between labels.

If you want to access a bucket by using a virtual hosted-style request, for example, `http://mybucket.s3.amazonaws.com` over SSL, the bucket name cannot include a period (.).

The rules for bucket names in the US Standard region are similar but less restrictive:

- Bucket names can be as long as 255 characters.
- Bucket names can contain any combination of uppercase letters, lowercase letters, numbers, periods (.), dashes (-) and underscores (_)

These naming rules for US Standard region can result in a bucket name that is not DNS-compliant. For example, `MyAWSBucket` is a valid bucket name, even though it contains uppercase letters. If you try to access this bucket by using a virtual hosted-style request (`http://MyAWSBucket.s3.amazonaws.com/yourobject`), the URL resolves to the bucket `myawsbucket` and not the bucket `MyAWSBucket`. In response, Amazon S3 will return a bucket not found error

Create a Bucket

You are not charged for creating a bucket; you are only charged for storing objects in the bucket and for transferring objects in and out of the bucket

To create a bucket

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in


Chennai and Trivandrum , India



Amazon EC2 Tutorial – For modified GUI

[Course tutorial and much more for extra reading]

1. Sign into 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 a Bucket** dialog box, in the **Bucket Name** box, enter a bucket name.

The bucket name you choose must be unique across all existing bucket names in Amazon S3. One way to help ensure uniqueness is to prefix your bucket names with the name of your organization. Bucket names must comply with certain rules.

Note

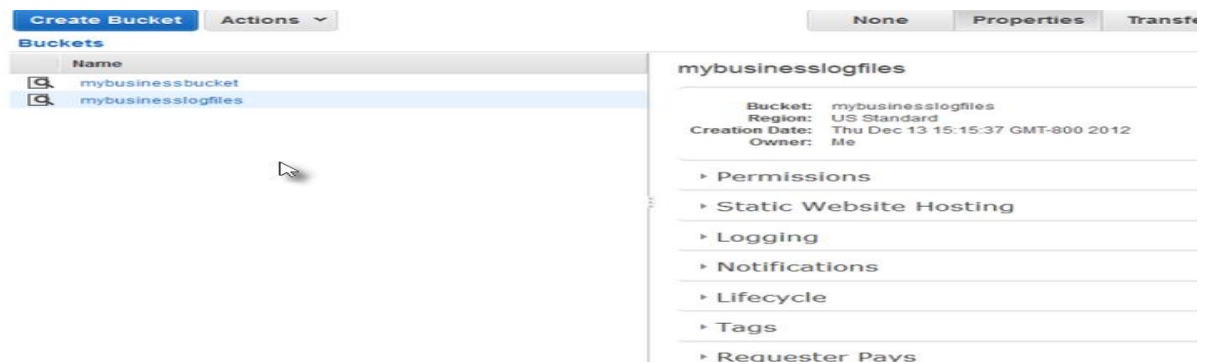
After you create a bucket, you cannot change its name. In addition, the bucket name is visible in the URL that points to the objects stored in the bucket. Ensure that the bucket name you choose is appropriate.

4. In the **Region** box, select a region. For this exercise, accept the default.

You can choose a region to optimize latency, minimize costs, or address regulatory requirements. Objects stored in a region never leave that region unless you explicitly transfer them to another region

5. Click **Create**.

When Amazon S3 successfully creates your bucket, the console displays your empty bucket in the Buckets panel.



By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

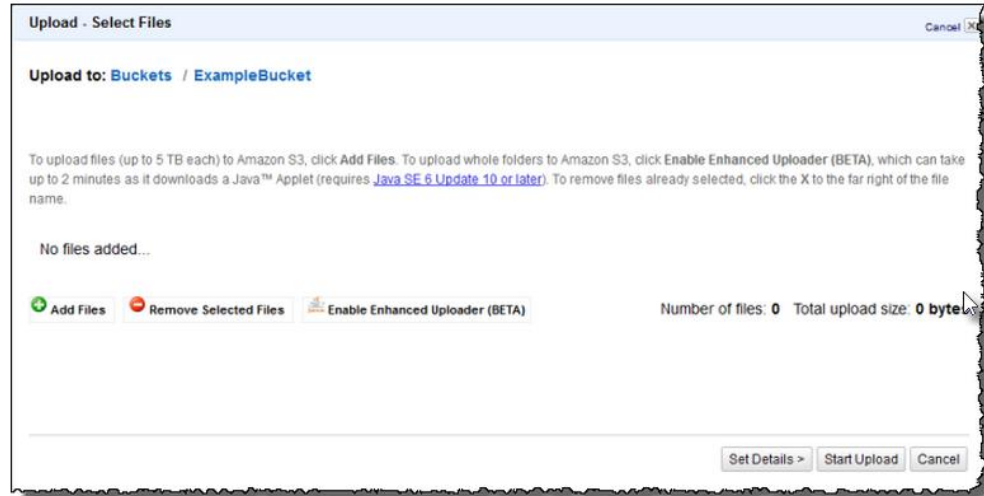
Chennai and Trivandrum , India



Add an Object to a Bucket

To upload an object

1. In the [Amazon S3 console](#), click the name of bucket where you want to upload an object and then click **Upload**.



2. In the **Upload - Select Files** wizard, if you want to upload an entire folder, you must click **Enable Enhanced Uploader** to install the necessary Java applet. You only need to do this once per console session.

Note

If you are behind a firewall you will need to install your organization's supported proxy client in order for the Java applet to work.

3. Click **Add Files**.

A file selection dialog box opens:

- If you enabled the advanced uploader in step 2, you see a Java dialog box titled **Select files and folders to upload**, as shown.
 - If not, you see the **File Upload** dialog box associated with your operating system.
4. Select the file that you want to upload and then click **Open**.
 5. Click **Start Upload**.

You can watch the progress of the upload from within the **Transfer** panel.

Tip

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



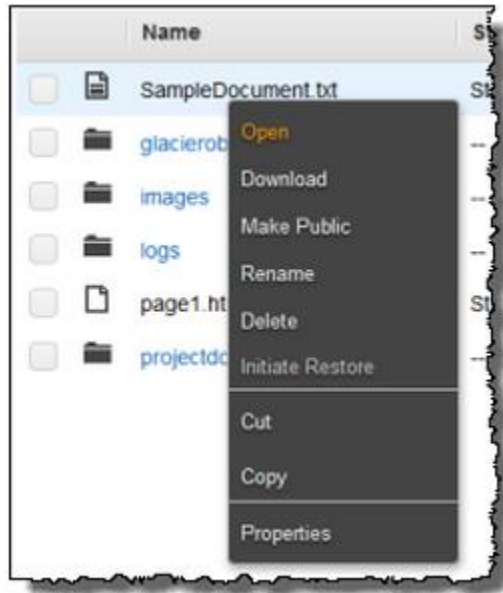
[Course tutorial and much more for extra reading]

To hide the **Transfer** dialog box, click the **Close** button at top right in the **Transfers** panel.
To open it again, click **Transfers**.

View An Object

Now that you've added an object to a bucket, you can open and view it in a browser. You can also download the object to your local computer.

To open or download an object



1. In the Amazon S3 console, in the Objects and Folders list, right-click the object or objects that you want to open or download, then click **Open** or **Download** as appropriate.
2. If you are downloading the object, specify where you want to save the downloaded object. The procedure for saving the object will depend on the browser and operating system that you are using.

Note

By default your Amazon S3 buckets and objects are private. To make an object viewable by using a URL, for example <https://s3.amazonaws.com/Bucket/Object>, you must make the object publicly readable

Using Reduced Redundancy Storage

In order to reduce storage costs, you can use reduced redundancy storage for noncritical, reproducible data at lower levels of redundancy than Amazon S3 provides with standard storage. The lower level of redundancy results in less durability and availability, but in many cases the lower costs can make reduced redundancy storage an acceptable storage solution. For example, reduced redundancy storage can be a cost-effective solution for sharing media content that is durably stored elsewhere. It

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



can also make sense if you are storing thumbnails and other resized images that can be easily reproduced from an original image.

Reduced redundancy storage is designed to provide 99.99% durability of objects over a given year. This durability level corresponds to an average annual expected loss of 0.01% of objects. For example, if you store 10,000 objects using the RRS option, you can, on average, expect to incur an annual loss of a single object per year (0.01% of 10,000 objects).

Note

This annual loss represents an expected average and does not guarantee the loss of less than 0.01% of objects in a given year.

Reduced redundancy storage stores objects on multiple devices across multiple facilities, providing 400 times the durability of a typical disk drive, but it does not replicate objects as many times as Amazon S3 standard storage. In addition, reduced redundancy storage is designed to sustain the loss of data in a single facility.

If an object in reduced redundancy storage has been lost, Amazon S3 will return a 405 error on requests made to that object. Amazon S3 also offers notifications for reduced redundancy storage object loss: you can configure your bucket so that when Amazon S3 detects the loss of an RRS object, a notification will be sent through Amazon Simple Notification Service (SNS). You can then replace the lost object.

Configure a Bucket for Website Hosting

To configure a bucket for static website hosting, you add a website configuration to your bucket. The configuration includes the following information:

- Index document

When you type a URL such as `http://example.com` you are not requesting a specific page. In this case the web server serves a default page, for the directory where the requested website content is stored. This default page is referred as index document, and most of the time it is named `index.html`. When you configure a bucket for website hosting, you must specify an index document. Amazon S3 returns this index document when requests are made to the root domain or any of the subfolders Error document

If an error occurs, Amazon S3 returns an HTML error document. For 4XX class errors, you can optionally provide your own custom error document, in which you can provide additional guidance to your users.

- Redirects all requests

If your root domain is `example.com` and you want to serve requests for both `http://example.com` and `http://www.example.com`, you can create two buckets named `example.com` and `www.example.com`, maintain website content in only one bucket, say, `example.com`, and configure the other bucket to redirect all requests to the `example.com` bucket.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

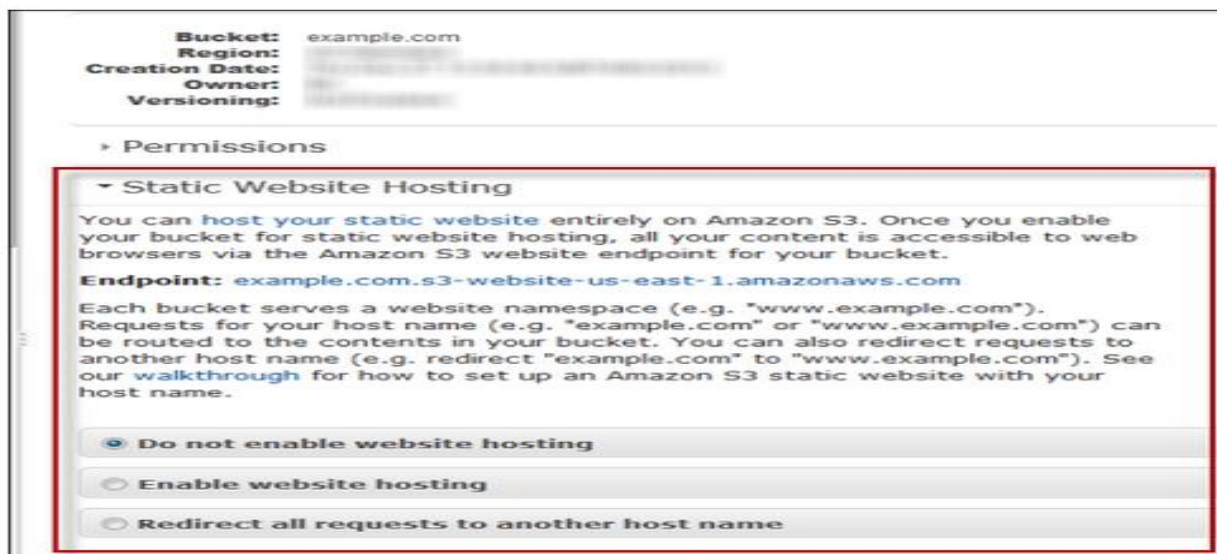
Chennai and Trivandrum , India



Amazon EC2 Tutorial – For modified GUI

[Course tutorial and much more for extra reading]

You can manage your buckets website configuration using the Amazon S3 console. The bucket **Properties** panel in the console enables you to specify the website configuration.



To host a static website on Amazon S3, you need only provide the name of the index document.



To redirect all requests to the bucket's website endpoint to another host, you only need to provide host name.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



[Course tutorial and much more for extra reading]



☐ Do not enable website hosting

☐ Enable website hosting

☒ Redirect all requests to another host name

To redirect requests to another bucket, enter the name of the target bucket below. If you are redirecting to a root domain address (e.g. example.com), see our [walkthrough](#) for configuring root domain website hosting.

Redirect all requests to:

Permissions Required for Website Access

When you configure a bucket as a website, you must make the objects that you want to serve publicly readable. To do so, you write a bucket policy that grants everyone `s3:GetObject` permission. On the website endpoint, if a user requests an object that does not exist, Amazon S3 returns HTTP response code 404 (Not Found). If the object exists but you have not granted read permission on the object, the website endpoint returns HTTP response code 403 (Access Denied). The user can use the response code to infer if a specific object exists or not. If you do not want this behavior, you should not enable website support for your bucket.

The following sample bucket policy grants everyone access to the objects in the specified folder. For more information on bucket policies.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "PublicReadGetObject",
    "Effect": "Allow",
    "Principal": {
      "AWS": "*"
    },
    "Action": ["s3:GetObject"],
    "Resource": ["arn:aws:s3:::example-bucket/*"]
  }]
}
```

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



```
]
}
```

Note

The bucket policy applies only to objects owned by the bucket owner. If your bucket contains objects not owned by the bucket owner, then public READ permission on those objects should be granted using the object ACL.

Setting Up a Static Website in S3

You can configure an Amazon S3 bucket to function like a website. This example walks you through the steps of hosting a website on Amazon S3. In the following procedure, you will use the AWS Management Console to perform the necessary tasks:

1. Create an Amazon S3 bucket and configure it as a website.
2. Add a bucket policy that make the bucket content public.

The content that you serve at the website endpoint must be publicly readable. You can grant the necessary permissions by adding a bucket policy or using Access Control List (ACL). Here we describe adding a bucket policy.

3. Upload an index document.
4. Test your website using the Amazon S3 bucket website endpoint.

To create a bucket and configure it as a website

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Create a bucket.
3. Open the bucket **Properties** panel, click **Static Website Hosting** and do the following:
 1. Select the **Enable website hosting**.
 2. In the **Index Document** box, add the name of your index document. This name is typically index.html.
 3. Click **Save** to save the website configuration.
 4. Note down the **Endpoint**.

This is the Amazon S3 provided website endpoint for your bucket. You will use this endpoint in the following steps to test your website.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



To upload an index document

1. Create a document. The file name must be same as the name that you provided for the index document earlier.
2. Using the console, upload the index document to your bucket.

Test your website.

- Enter the following URL in the browser, replacing `example-bucket` with the name of your bucket and `website-region` with the name of the region where you deployed your bucket.

```
http://example-bucket.s3-website-region.amazonaws.com
```

If your browser displays your `index.html` page, the website was successfully deployed.

Setting Up Notification of Bucket Events

The Amazon S3 notifications feature enables you to configure a bucket so that Amazon S3 publishes a message to an Amazon Simple Notification Service (Amazon SNS) topic when Amazon S3 detects a key event on a bucket. Subscribers to this topic can have messages for bucket events delivered to an endpoint such as a web server, e-mail address

Object Lifecycle Management

Lifecycle management defines how Amazon S3 manages objects during their lifetime.

Some objects that you store in an Amazon S3 bucket might have a well-defined lifecycle:

- If you are uploading periodic logs to your bucket, your application might need these logs for a week or a month after creation, and after that you might want to delete them.
- Some documents are frequently accessed for a limited period of time. After that, you might not need real-time access to these objects, but your organization might require you to archive them for a longer period and then optionally delete them later. Digital media archives, financial and healthcare records, raw genomics sequence data, long-term database backups, and data that must be retained for regulatory compliance are some kinds of data that you might upload to Amazon S3 primarily for archival purposes.

For such objects, you can define rules that identify the affected objects, a timeline, and specific actions you want Amazon S3 to perform on the objects.

Amazon S3 manages object lifetimes with a lifecycle configuration, which is assigned to a bucket and defines rules for individual objects. Each rule in a lifecycle configuration consists of the following:

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



[Course tutorial and much more for extra reading]

- A object key prefix that identifies one or more objects to which the rule applies.
- An action or actions that you want Amazon S3 to perform on the specified objects.
- A date or a time period, specified in days since object creation, when you want Amazon S3 to perform the specified action.

You can add these rules to your bucket using either the Amazon S3 console or programmatically.

Lifecycle Configuration Rules

A rule can apply to a single object or multiple objects whose key name begins with the prefix specified in the rule. For example, suppose you have the following objects:

logs/day1

logs/day2

logs/day3

ExampleObject.jpg

If you specify `ExampleObject.jpg` as the prefix, the rule applies to the specific object. If you specify `logs/` as the prefix, the rule applies to the three objects whose key name begins with the string "logs/".

A rule can specify the following actions:

- Transition— When a specified date or time period in the object's lifetime is reached, Amazon S3 sets the storage class to Glacier.

Expiration—When the specified time period is reached in the object's lifetime, Amazon S3 deletes it.

For example, you can set a rule with an expiration action so that Amazon S3 will delete objects with the key prefix "log2012-01-01" 30 days after creation.

Expiration applies to all Amazon S3 objects, including those that are archived in Amazon Glacier.

You can specify a date or a time period in days since object creation when the action will be taken on the specified object or objects.

- When you specify a number of days, Amazon S3 calculates the time by adding the number of days specified in the rule to the object creation time and rounding the resulting time to the next day midnight UTC. For example, if an object was created on 1/15/2012 10:30 a.m. UTC and you specify 3 days in a transition rule, then the transition date of the object would be calculated as 1/19/2012 00:00 UTC.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



[Course tutorial and much more for extra reading]

- When you specify a date in a rule, the specified action is executed on the specified date. That is, Amazon S3 transitions or expires the objects on the specified date.

Manage Object Lifecycle Using the AWS Management Console

In the console, the bucket **Properties** provides a **Lifecycle** tab as shown in the following example screen shot. It shows bucket with two rules and both rules are enabled. You can click **Modify** to view the rule details or click **Add rule** to add a new rule.



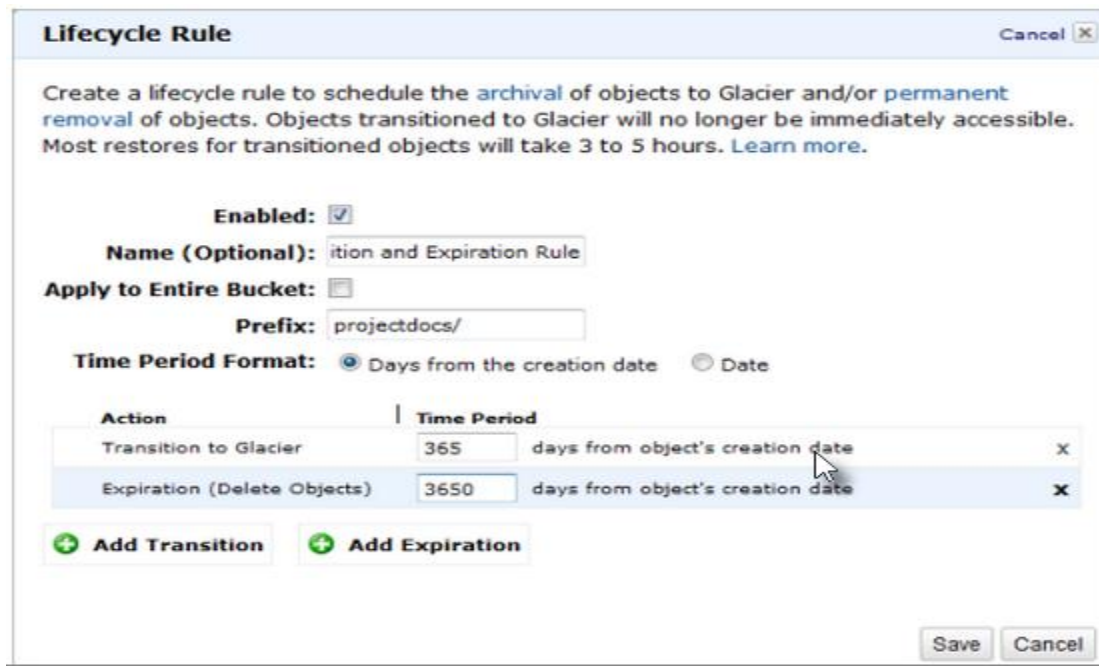
The **Lifecycle Rule** wizard shown in the following example shows a rule's details. It shows that the rule applies to objects with key prefix "projectdocs/". The rule defines two actions for Amazon S3; the **Transition** action instructs Amazon S3 to transition objects to the Glacier storage class a year after creation, and the **Expiration** action instructs Amazon S3 to delete the objects 10 years after creation.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India





The screenshot shows the 'Lifecycle Rule' configuration window in the AWS Management Console. The window has a title bar with 'Lifecycle Rule' and a 'Cancel' button. Below the title bar is a descriptive text: 'Create a lifecycle rule to schedule the archival of objects to Glacier and/or permanent removal of objects. Objects transitioned to Glacier will no longer be immediately accessible. Most restores for transitioned objects will take 3 to 5 hours. Learn more.' The configuration fields include: 'Enabled' (checked), 'Name (Optional):' (set to 'ition and Expiration Rule'), 'Apply to Entire Bucket:' (unchecked), 'Prefix:' (set to 'projectdocs/'), and 'Time Period Format:' (set to 'Days from the creation date'). Below these is a table with two columns: 'Action' and 'Time Period'. The table contains two rows: 'Transition to Glacier' with a time period of '365 days from object's creation date' and 'Expiration (Delete Objects)' with a time period of '3650 days from object's creation date'. At the bottom of the table are two buttons: 'Add Transition' and 'Add Expiration'. The bottom of the window has 'Save' and 'Cancel' buttons.

Action	Time Period
Transition to Glacier	365 days from object's creation date
Expiration (Delete Objects)	3650 days from object's creation date

Using Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. In one bucket, for example, you can have two objects with the same key, but different version IDs, such as `photo.gif (version 111111)` and `photo.gif (version 121212)`

You might enable versioning to prevent objects from being deleted or overwritten by mistake, or to archive objects so that you can retrieve previous versions of them.

Buckets can be in one of three states: unversioned (the default), versioning-enabled, or versioning-suspended. Once you version enable a bucket, it can never return to an unversioned state. You can, however, suspend versioning on that bucket.

Only the bucket owner can configure the versioning state of a bucket. The versioning state applies to all (never some) of the objects in that bucket. The first time you enable a bucket for versioning, objects in it are thereafter always versioned and given a unique version ID.

Enabling Versioning

Objects stored in your bucket before you set the versioning state have a version ID of `null`. When you enable versioning the objects in your bucket do not change. What changes is how Amazon S3 handles the objects in future requests in that bucket.

Suspending Versioning :

Once you suspend versioning on a bucket, Amazon S3 automatically adds a `null` version ID to every subsequent object stored thereafter in that bucket.

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India



[Course tutorial and much more for extra reading]

If a null version is already in the bucket and you add another object with the same key, the added object overwrites the original null version.

If there are versioned objects in the bucket, the version you `PUT` becomes the latest version of the object.

Restoring Previous Versions

One of the value propositions of versioning is the ability to retrieve previous versions of an object. There are two approaches to doing so:

- Copy a previous version of the object into the same bucket

The copied object becomes the latest version of that object and all object versions are preserved.

- Permanently delete the latest version of the object

When you delete the latest object version you, in effect, turn the previous version into the latest version of that object.

Because all object versions are preserved, you can make any earlier version the latest version by copying a specific version of the object into the same bucket.

S3 Storage Pricing: Refer: <http://aws.amazon.com/s3/pricing/>

By ANIL KUMAR

cloud.b.lab@zoho.com, www.cloud-b-lab.com, www.cloud-b-lab.co.in

Chennai and Trivandrum , India

