Amazon EC2 Interview Questions and Answers

01. What is Amazon EC2 service?

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable (scalable) computing capacity in the cloud. You can use Amazon EC2 to launch as many virtual servers you need. In Amazon EC2 you can configure security and networking, and manage storage.

02. What are the features of Amazon EC2 service?

As Amazon EC2 service is a cloud service so it has all the cloud features. Amazon EC2 provides the following features:

* Virtual computing environment (known as instances)
* Pre-configured templates for your instances (known as Amazon Machine Images – AMIs)
* Amazon Machine Images (AMIs) is package that you need for your server (including the operating system and additional software)
* Amazon EC2 provides various configuration of CPU, memory, storage and networking capacity for your instances (known as instance type)
* 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)
* Amazon EC2 provides persistent storage volumes (using Amazon Elastic Block Store – EBS)
* 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 address)
* Amazon EC2 provides metadata (known as tags)
* Amazon EC2 provides virtual networks that are logically isolated from the rest of the AWS cloud, and that you can optionally connect to your own network (known as virtual private clouds – VPCs)

03. What is Amazon Machine Image and what is the relation between Instance and AMI?

Amazon Web Services provides several ways to access Amazon EC2, like web-based interface, AWS Command Line Interface (CLI) and Amazon Tools for Windows Powershell. First you need to signed up for an AWS account and you can access Amazon EC2.

Amazon EC2 provides a Query API. These requests are HTTP or HTTPS requests that use the HTTP verbs GET or POST and a Query parameter named Action.

04. What is Amazon Machine Image (AMI)?

An Amazon Machine Image (AMI) is a template that contains a software configuration (for example, an operating system, an application server, and applications). From an AMI, we launch an instance, which is a copy of the AMI running as a virtual server in the cloud. We can launch multiple instances of an AMI.

05. What is the relation between Instance and AMI?

We can launch different types of instances from a single AMI. An instance type essentially determines the hardware of the host computer used for your instance. Each instance type offers different compute and memory capabilities.

After we launch an instance, it looks like a traditional host, and we can interact with it as we would any computer. We have complete control of our instances; we can use sudo to run commands that require root privileges.

06. Explain storage for Amazon EC2 instance.

Amazon EC2 provides many data storage options for your instances. Each option has a unique combination of performance and durability. These storage can be used independently or in combination to suit your requirements.

There are mainly four types of storage provided by AWS.

**Amazon EBS:** Its durable, block-level storage volumes that you can attach to a running Amazon EC2 instance. The Amazon EBS volume persists independently from the running life of an Amazon EC2 instance. After an EBS volume is attached to an instance, you can use it like any other physical hard drive. Amazon EBS encryption feature supports encryption feature.  
**Amazon EC2 Instance Store:** Storage disk that is attached to the host computer is referred to as instance store. Instance storage provides temporary block-level storage for Amazon EC2 instances. The data on an instance store volume persists only during the life of the associated Amazon EC2 instance; if you stop or terminate an instance, any data on instance store volumes is lost.  
**Amazon S3:** Amazon S3 provides access to reliable and inexpensive data storage infrastructure. It is designed to make web-scale computing easier by enabling you to store and retrieve any amount of data, at any time, from within Amazon EC2 or anywhere on the web.  
**Adding Storage:** Every time you launch an instance from an AMI, a root storage device is created for that instance. The root storage device contains all the information necessary to boot the instance. You can specify storage volumes in addition to the root device volume when you create an AMI or launch an instance using block device mapping.

07. What are the Security Best Practices for Amazon EC2?

There are several best practices for secure Amazon EC2. Following are few of them.

* Use AWS Identity and Access Management (IAM) to control access to your AWS resources.
* Restrict access by only allowing trusted hosts or networks to access ports on your instance.
* Review the rules in your security groups regularly, and ensure that you apply the principle of least
* Privilege — only open up permissions that you require.
* Disable password-based logins for instances launched from your AMI. Passwords can be found or cracked, and are a security risk.

08. Explain Stopping, Starting, and Terminating an Amazon EC2 instance?

**Stopping and Starting an instance:** When an instance is stopped, the instance performs a normal shutdown and then transitions to a stopped state. All of its Amazon EBS volumes remain attached, and you can start the instance again at a later time. You are not charged for additional instance hours while the instance is in a stopped state.  
**Terminating an instance:** When an instance is terminated, the instance performs a normal shutdown, then the attached Amazon EBS volumes are deleted unless the volume’s deleteOnTermination attribute is set to false. The instance itself is also deleted, and you can’t start the instance again at a later time.

09. What are regions and availability zones in Amazon EC2? Explain in brief.

Amazon EC2 is hosted in multiple locations world-wide. These locations are composed of regions and Availability Zones. Each region is a separate geographic area. Each region has multiple, isolated locations known as Availability Zones.

Each region is completely independent. Each Availability Zone is isolated, but the Availability Zones in a region are connected through low-latency links. The following diagram illustrates the relationship between regions and Availability Zones.

10. Explain how to Launch EC2 instance in an Availability Zone?

Each region is completely independent and each Availability Zone is isolated. When you view your resources, you’ll only see the resources tied to the region you have specified.

To launch a EC2 instance, you must select an AMI that’s in the same region (if the AMI is in another region then you can copy the AMI to the region you are using). Now select an  
Availability Zone or let AWS choose for you. After creating the EC2 instance, it will show up in selected Availability Zone.

11. How to Migrate an Instance to another Availability Zone?

You can migrate your EC2 instance from one Availability Zone to another. Following are the steps to migrate an Instance to another Availability Zone.

1. Create an AMI from the running instance
2. Launch an instance from the AMI that you just created, specify the new Availability Zone
3. You can use the same instance type as the original instance, or select a new instance type
4. If the original instance has an associated Elastic IP address, then associate it with the new instance
5. If the original instance is a Reserved Instance, change the Availability Zone for your reservation

12. What is Amazon EC2 Root Device Volume?

When you launch an instance, the Root Device Volume contains the image used to boot the instance.  
You can launch an instance from one of two types of AMIs:

1. Instance store-backed AMI
2. EBS based storage

13. How to persist Root Device Volume in Amazon EC2 Instance?

By default, the root device volume for an AMI backed by Amazon EBS is deleted when the instance terminates. To change the default behavior, set the DeleteOnTermination attribute to false using a block device mapping.

**To change the root device volume of an instance to persist at launch using the console**

1. Open the Amazon EC2 console.
2. From the Amazon EC2 console dashboard, click Launch Instance.
3. On the Choose an Amazon Machine Image (AMI) page, choose the AMI to use and click Select.
4. Follow the wizard to complete the Choose an Instance Type and Configure Instance Details pages.
5. On the Add Storage page, deselect the Delete On Termination check box for the root volume.
6. Complete the remaining wizard pages, and then click Launch.

**Changing the Root Volume of an Instance to Persist Using the AWS CLI**  
Use the run-instances command to preserve the root volume by including a block device mapping that sets its DeleteOnTermination attribute for to false.

$ aws ec2 run-instances –image-id ami-1a2b3c4d –block-device-mappings ‘[{"DeviceName":"/dev/sda1","Ebs":{"DeleteOnTermination":false}}]‘

14. What is Key Pair?

AWS uses public-key cryptography to secure the login information for your instance. A Linux instance has no password; you use a key pair to log in to your instance securely.  
You specify the name of the key pair when you launch your instance, then provide the private key when you log in using SSH.

15. How to create Key Pair?

We can create one using the Amazon EC2 console. To launch instances in multiple regions, we’ll need to create a key pair in each region.  
**Following are the steps to create Key Pair:**

1. Sign in to Amaon Web Service.
2. From the AWS dashboard, choose EC2 to open the Amazon EC2 console.
3. From the navigation bar, select a region for the key pair.
4. In the left navigation pane, under **NETWORK & SECURITY**, click Key **Pairs**.
5. Click Create **Key Pair**.
6. 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**.
7. 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.

16. What is the use of Key Pair?

Key pair is used to log in to your instance securely. This is public-key cryptography to secure the login information for your instance.

17. What is Security Group in Amazon EC2?

Security groups act as a firewall for associated instances, controlling both inbound and outbound traffic at the instance level.

18. What are the features of Security Group in Amazon EC2?

**Following are the features of the Security Group in Amazon EC2:**

1. We can add rules to a security group that enable us to connect to our instance from our IP address using SSH.
2. We can also add rules that allow inbound and outbound HTTP and HTTPS access from anywhere.

19. How to create Security Group in Amazon EC2?

We can create Security Group in Amazon EC2 using the Amazon EC2 console. To launch instances in multiple regions, we’ll need to create a Security Group in each region.  
**Following are the steps to create Security Group in Amazon EC2:**

1. Open the Amazon EC2 console.
2. From the left navigation bar, select a region for the security group.
3. Click **Security Groups** in the navigation pane.
4. Click **Create Security Group**.
5. Enter a name for the new security group and a description.
6. In the **VPC** list, select your VPC.
7. On the **Inbound** tab, click **Add Rule** for each new rule, and then click **Create**.

20. How to launch an Amazon EC2 Instance?

We can launch Linux/Windows Amazon EC2 instance using AWS Management Console. Following are the steps to create Amazon EC2 instance.

1. Open the Amazon EC2 console.
2. From the console dashboard, choose Launch Instance.
3. Choose an Amazon Machine Image (AMI).
4. Choose an Instance Type.
5. Click on Review and Launch to let the wizard complete the other configuration setting.
6. On the Review Instance Launch page, under Security Groups select a Security Group.
7. Click on Launch on the Review Instance Launch.
8. Select an Existing ket pair when it prompte for key pair.
9. Click on View Instance to return on the console to see instance is launching.

21. How to connect to your Amazon EC2 Instance?

There are several ways to connect to a Linux instance. One of the commonly used method is to connect Linux instance from Windows local machine using PuTTY.

**Following are the steps to connect to a Linux instance.**

1. Install PuTTY on your local machine.
2. Get your instance ID.
3. Get the public DNS name of the instance.
4. Locate the private key.
5. Enable inbound SSH traffic from your IP address to your instance.
6. Converting Your Private Key Using PuTTYgen.
7. Starting a PuTTY Session.
8. Now you are connected to your EC2 instance.

22. How to add a EBS Volume to your Amazon EC2 Instance?

We can attach an EBS volume to one of our instances that is in the same Availability Zone as the Volume.  
**Following are the steps to attache an EBS volumn to an instance using console:**

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the left navigation pane, choose **Volumes**.
3. Select a volume and choose **Attach Volume**.
4. Select the instance to which you want to attach the volume.
5. Click on **Attach**.
6. Now connect to your instance and make the volume available.

23. How to clean up your Amazon EC2 Instance and Volume?

After we are finished with the instance we created, we can clean up by terminating the instance.  
**Following are the steps to terminate the EC2 instance:**

1. In the navigation pane, choose Instances. In the list of instances, select the instance.
2. Choose Actions, then Instance State, and then choose Terminate.
3. Choose Yes,Terminate when prompted for confirmation.

24. What are the best practices for Amazon EC2?

To get the maximum benefit from and satisfaction with Amazon EC2. There are mainly four best practices.

1. **Security and Network Best Practices**
2. **Storage**
3. **Resource Management**
4. **Backup and Recovery**

25. How to create your own Amazon Machine Image (AMI)?

You can customize a instance that is launched from a public AMI and then save that configuration as a custom AMI for your own use.  
Instances that you launch from your AMI use all the customizations that you’ve made.

26. Explain types of storage for the Root Device and difference between them?

There are 2 types of storage for the Root Device, as either **backed by Amazon EBS** or **backed by Instance store**. he former means that the root device for an instance launched from the AMI is an Amazon EBS volume created from an Amazon EBS snapshot.  
This section summarizes the important differences between the two types of AMIs. The following table provides a quick summary of these differences.

|  |  |  |
| --- | --- | --- |
| **Characteristic** | **Amazon EBS-Backed** | **Amazon Instance Store-Backed** |
| Boot time | Usually less than 1 minute | Usually less than 5 minutes |
| Size limit | 16 TiB | 10 GiB |
| Root device volume | Amazon EBS volume | Instance store volume |
| Data persistence | By default, the root volume is deleted when the instance terminates.\* Data on any other Amazon EBS volumes persists after instance termination by default. Data on any instance store volumes persists only during the life of the instance. | Data on any instance store volumes persists only during the life of the instance. Data on any Amazon EBS volumes persists after instance termination by default. |
| Upgrading | The instance type, kernel, RAM disk, and user data can be changed while the instance is stopped. | Instance attributes are fixed for the life of an instance. |
| Charges | You’re charged for instance usage, Amazon EBS volume usage, and storing your AMI as an Amazon EBS snapshot. | You’re charged for instance usage and storing your AMI in Amazon S3. |
| AMI creation/bundling | Uses a single command/call | Requires installation and use of AMI tools |
| Stopped state | Can be placed in stopped state where instance is not running, but the root volume is persisted in Amazon EBS | Cannot be in stopped state; instances are running or terminated |

27. How to determine the Root Device type of your AMI?

We can determine the Root Device type of AMI using following 2 methods.  
Method 1: Following are the steps to determine the Root Device type of an AMI using the console  
1. Open the Amazon EC2 console  
2. In the navigation pane, click **AMIs**, and select the AMI  
3. Check the value of **Root Device Type** in the Details tab as follows  
3.1 If the value is **ebs**, this is an Amazon EBS-backed AMI  
3.2 If the value is **instance store**, this is an instance store-backed AMI

Method 2: Following are the steps to determine the root device type of an AMI using the command line  
We can use one of the following commands.  
1. describe-images (AWS CLI)  
2. Get-EC2Image (AWS Tools for Windows PowerShell)

28. What is the size limit for Amazon EC2 instance store-backed AMIs and Amazon EBS-backed AMIs?

All AMIs are categorized as either backed by Amazon EBS or backed by instance store.

**Backed by Amazon EBS** – means that the root device for an instance launched from the AMI is an Amazon EBS volume created from an Amazon EBS snapshot.

**Backed by instance store** – means that the root device for an instance launched from the AMI is an instance store volume created from a template stored in Amazon S3.

**Root device size limit for** –  
Amazon EBS – Backed is 16 TiB  
Amazon Instance Store-Backed is 10 GiB

29. How you’re charged in Amazon EC2? Explain in detail.

Charges varies upon AMIs backed and storage volums.

AMIs backed by instance storage charged for: **AMI storage + Instance usage**  
AMIs backed by Amazon EBS storage charged for: **Volume storage + Usage in addition to the AMI + instance usage**

When an Amazon EBS-backed instance is stopped, you are not charged for instance usage, but you are **still charged for volume storage**.

AWS charges a full instance hour for every transition from a stopped state to a running state, even if we transition the instance multiple times within a single hour.  
For example: if hourly instance charge for your instance is $0.10 and if you were to run that instance for one hour without stopping it, you would be charged $0.10. If you stopped and restarted that instance twice during that hour, then you would be charged $0.30 for that hour of usage (the initial $0.10, plus 2 x $0.10 for each restart).

30. What is shared AMI?

A shared AMI is an AMI that a developer created and made available for other developers to use.  
One of the easiest ways to get started with Amazon EC2 is to use a shared AMI that has the components you need and then add custom content. You can also create your own AMIs and share them with others.

**Note**: Use a shared AMI at your own risk. Amazon can’t vouch for the integrity or security of AMIs shared by other Amazon EC2 users. AWS recommends that you get an AMI from a trusted source.

31. How to update AMI tools at Boot Time?

AWS recommends that your AMIs download and upgrade the Amazon  
EC2 AMI creation tools during startup. This ensures that new AMIs based on your shared AMIs have the latest AMI tools.

For Amazon Linux, add the following to /etc/rc.local:

# Update the Amazon EC2 AMI tools  
echo ” + Updating EC2 AMI tools”  
yum update -y aws-amitools-ec2  
echo ” + Updated EC2 AMI tools”

32. How to disable Password-Based Logins for Root in Amazon EC2 Instance?

Using a fixed root password for a public AMI is a security risk that can quickly become known. Even relying on users to change the password after the first login opens a small window of opportunity for potential abuse.

Following are the steps to disable password-based remote logins for the root user.

1.Open the /etc/ssh/sshd\_config file with a text editor and locate the following line:  
#PermitRootLogin yes

2. Change the line to:  
PermitRootLogin without-password

The location of this configuration file might differ for your distribution.

33. What is Public Key Credentials and how to install it?

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.

After configuring the AMI to prevent logging in using a password, you must make sure users can log in using another mechanism.

34. What is sshd DNS Checks and how to disable it?

A

35. What is paid AMI and how to use them?

A

35. How to sell your AMI?

A

36. How to create an Amazon EBS-Backed Linux AMI?

A

37. How to create an AMI from an Instance?

A

38. How to create an AMI from a Snapshot?

A

39. How to create an Instance Store-Backed Linux AMI?

A

40. How to convert your Instance Store-Backed AMI to an Amazon EBS-Backed AMI?

A

41. How to copy an Amazon EC2 AMI from one Region to another Region?

A

42. What is Amazon EBS-Optimized Instances?

A

43. How to resize your Amazon EC2 Instance?

A

44. What is Spot Instances and what are the advantages of them?

A