



Short Interview questions on AWS Key pairs

What are key pairs ?

Key pairs are a combination of **public and private SSH keys** used to securely connect to an EC2 instance:

- The **public key** is stored by AWS.
- The **private key** is downloaded by the user and used to SSH into the instance.

What is a key pair in AWS EC2 and why is it important?

A key pair (public/private) is used for secure SSH access to Linux EC2 instances.

Can you connect to an EC2 instance without a key pair? If yes, how?

Yes, by using Systems Manager Session Manager or setting a password-based login (not recommended for security).

What happens if you lose your private key? Can you still access your instance?

There are a few rescue options depending on your cloud provider:

1. Use an alternative user/connection (if configured)

- If you had set up another user account or another way of connecting (for example, a different key, or a bastion/jump server), use that.

2. Create a new key pair and replace the old key (common method)

- **Detach the disk (root volume)** of the instance.
- **Attach it** temporarily to another instance where you have access.
- **Mount the disk** and **manually update the** `authorized_keys` file (in `/home/username/.ssh/authorized_keys`) with a new public key corresponding to a new private key pair.
- **Reattach the disk back** to the original instance and reboot.
- Now you can SSH using your new private key.

3. Use provider-specific rescue features

- AWS: Use **EC2 Instance Connect** (browser-based SSH for Amazon Linux/Ubuntu if enabled).
- AWS Systems Manager: If SSM agent is installed and configured, you can use **Session Manager** to connect without SSH at all.

How would you add a new key pair to an existing EC2 instance?

Manually add the new public key to the `~/.ssh/authorized_keys` file on the instance.

Where is the public key stored when you create a key pair in AWS?

The **public key** is automatically stored on the EC2 instance in the `authorized_keys` file of the specified user account (usually the default user like `ec2-user` for Amazon Linux, `ubuntu` for Ubuntu, or `admin` for other distributions). This file is located in the home directory of the user, under the `.ssh` folder:

- **Path:** `/home/username/.ssh/authorized_keys`

When the key pair is created, AWS adds the **public key** to this file during instance creation. This allows the corresponding **private key** (that you download at the time of creation) to be used for authentication when you SSH into the instance.

What are the security best practices for storing and using key pairs?

Store the private key securely (e.g., in a password-protected vault or secrets manager).

- Set strict file permissions (e.g., `chmod 400` for `.pem` files).
- Never share the private key.
- Rotate keys periodically if needed.
- Avoid hardcoding or uploading the key to public repositories.

Can the same key pair be used across multiple EC2 instances?

Yes, it's common to use the same key pair for managing multiple instances.

How do key pairs relate to SSH access on Linux vs RDP access on Windows EC2?

Linux uses key pairs for SSH, Windows uses passwords which are encrypted using the key pair.

Can you change the key pair associated with a running instance? How?

Not directly. You must manually replace the public key on the instance or create a new AMI and launch a new instance with the new key.


Where is the private key stored after creating a key pair?

- A. In AWS S3
- B. In EC2 metadata
- C. Downloaded by the user
- D. Stored in CloudTrail

 **Answer:** C. Downloaded by the user


What happens if you lose your private key for an EC2 instance?

- A. AWS can regenerate it
- B. Access is lost; recovery requires attaching the volume to another instance
- C. You can reset it via EC2 dashboard
- D. Instance automatically creates a new key

 **Answer:** B. Access is lost; recovery requires attaching the volume to another instance

What file permission should you set for a .pem file to use it with SSH?

- A. chmod 777
- B. chmod 644
- C. chmod 400
- D. Chmod 600

 **Answer:** C. chmod 400

Which statement is false about AWS key pairs?

- A. A public key is stored in AWS
- B. A private key is stored securely by AWS
- C. You must download the private key at creation time
- D. Key pairs are used for authentication

 **Answer:** B. A private key is stored securely by AWS