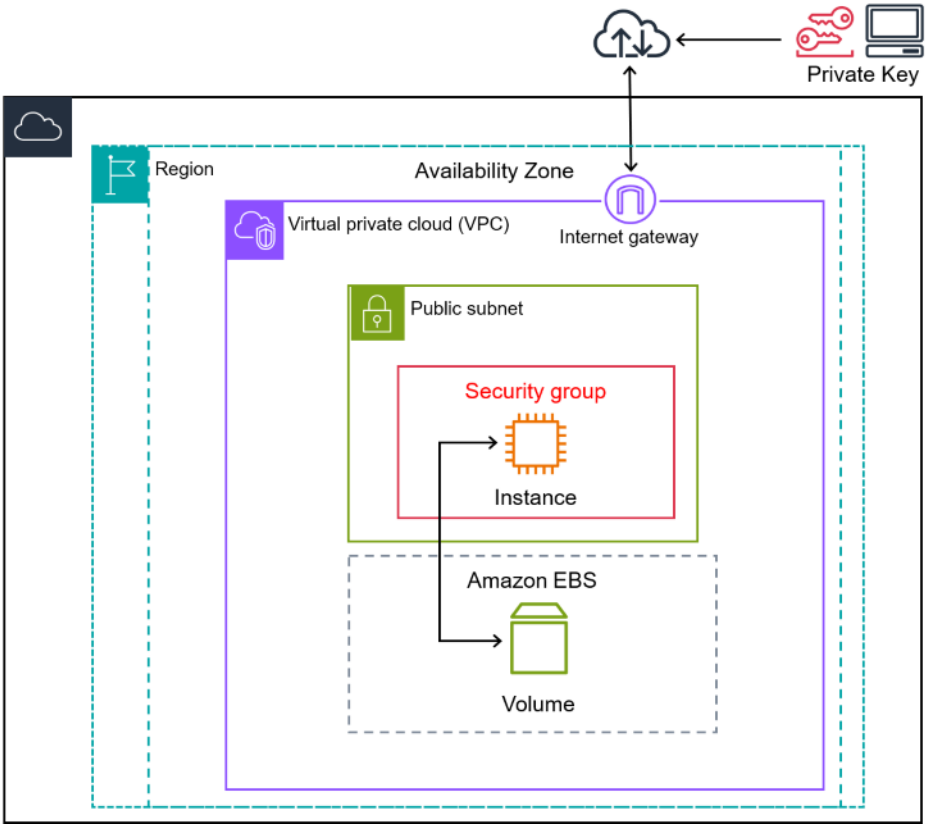
Case study on Amazon EC2 and learn about Amazon EC2 web services.

What is Amazon EC2?

Amazon Elastic Compute Cloud (Amazon EC2) provides on-demand, scalable computing capacity in the Amazon Web Services (AWS) Cloud. Using Amazon EC2 reduces hardware costs 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. You can add capacity (scale up) to handle compute-heavy tasks, such as monthly or yearly processes, or spikes in website traffic. When usage decreases, you can reduce capacity (scale down) again.

Basic Architecture of Amazon EC2

The following diagram shows a basic architecture of an Amazon EC2 instance deployed within an Amazon Virtual Private Cloud (VPC). In this example, the EC2 instance is within an Availability Zone in the Region. The EC2 instance is secured with a security group, which is a virtual firewall that controls incoming and outgoing traffic. A private key is stored on the local computer and a public key is stored on the instance. Both keys are specified as a key pair to prove the identity of the user. In this scenario, the instance is backed by an Amazon EBS volume. The VPC communicates with the internet using an internet gateway.



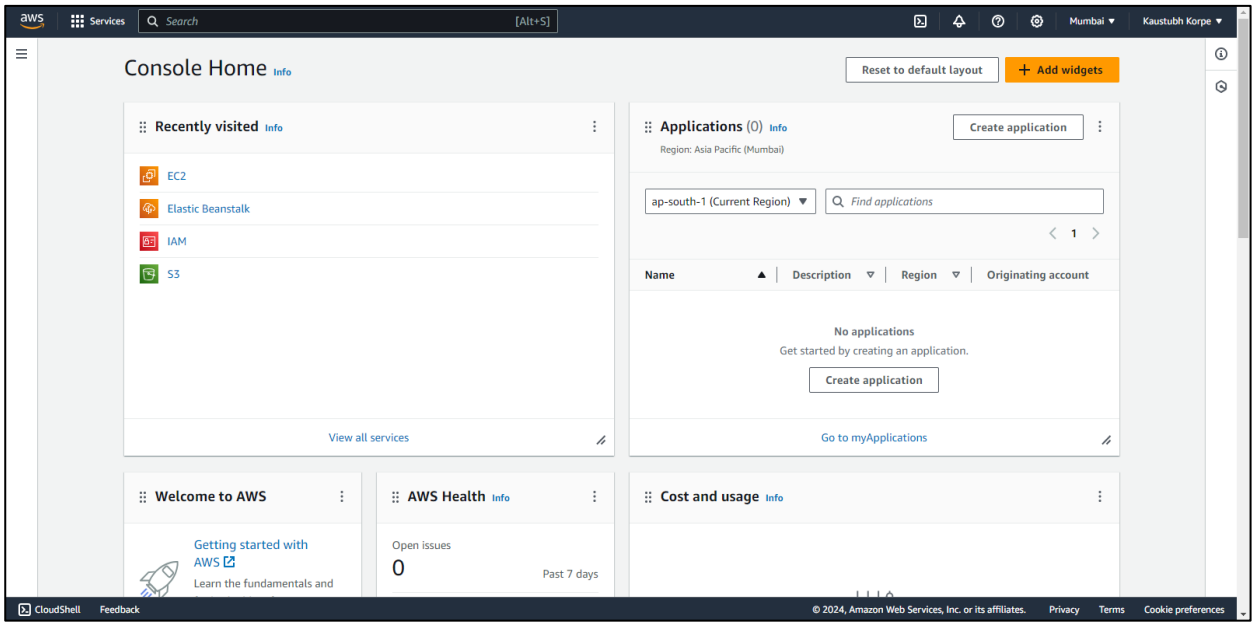
Features of Amazon EC2

Amazon EC2 provides the following high-level features:

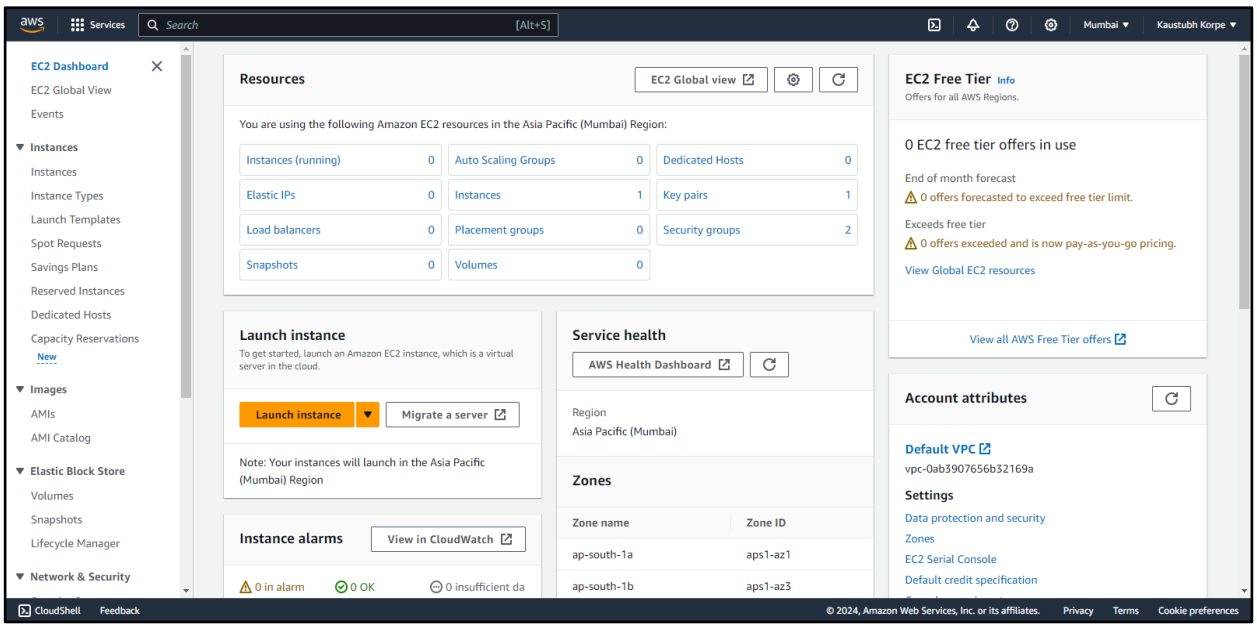
- **Instances:** Virtual servers.
- **Amazon Machine Images (AMIs):** Preconfigured templates for your instances that package the components you need for your server (including the operating system and additional software).
- **Instance types:** Various configurations of CPU, memory, storage, networking capacity, and graphics hardware for your instances.
- **Key pairs:** Secure login information for your instances. AWS stores the public key and you store the private key in a secure place.
- **Instance store volumes:** Storage volumes for temporary data that is deleted when you stop, hibernate, or terminate your instance.
- **Amazon EBS volumes:** Persistent storage volumes for your data using Amazon Elastic Block Store (Amazon EBS).
- **Regions, Availability Zones, Local Zones, AWS Outposts, and Wavelength Zones:** Multiple physical locations for your resources, such as instances and Amazon EBS volumes.
- **Security groups:** A virtual firewall that allows you to specify the protocols, ports, and source IP ranges that can reach your instances, and the destination IP ranges to which your instances can connect.
- **Elastic IP addresses:** Static IPv4 addresses for dynamic cloud computing.
- **Tags:** Metadata that you can create and assign to your Amazon EC2 resources.
- **Virtual private clouds (VPCs):** Virtual networks you can create that are logically isolated from the rest of the AWS Cloud. You can optionally connect these virtual networks to your own network.

Launching an Instance in Amazon EC2

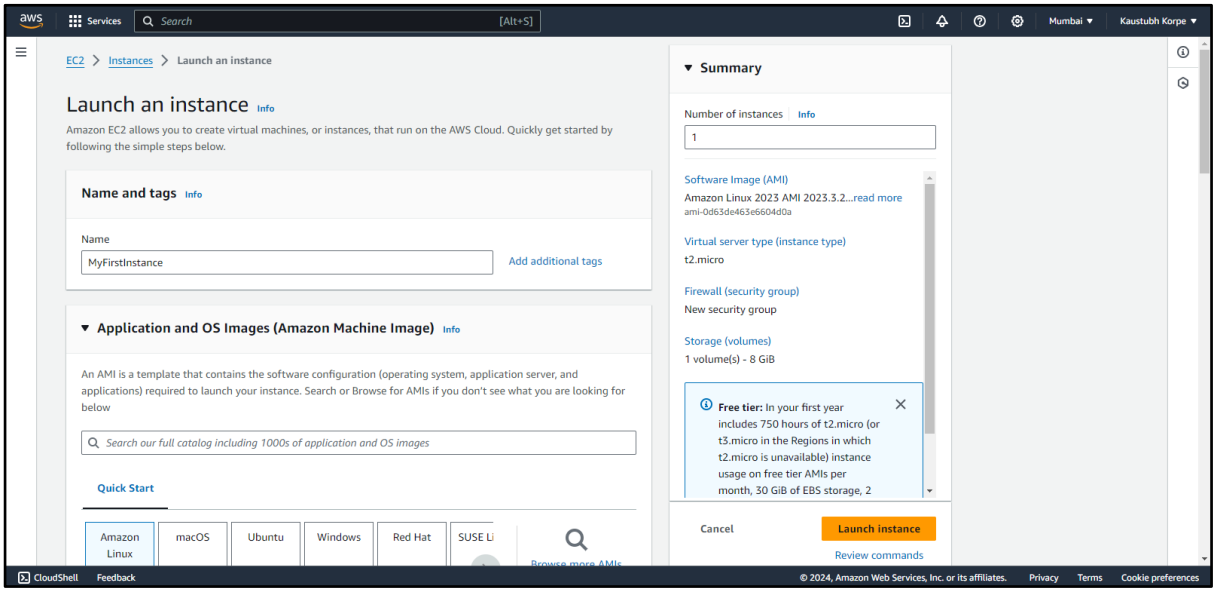
1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.



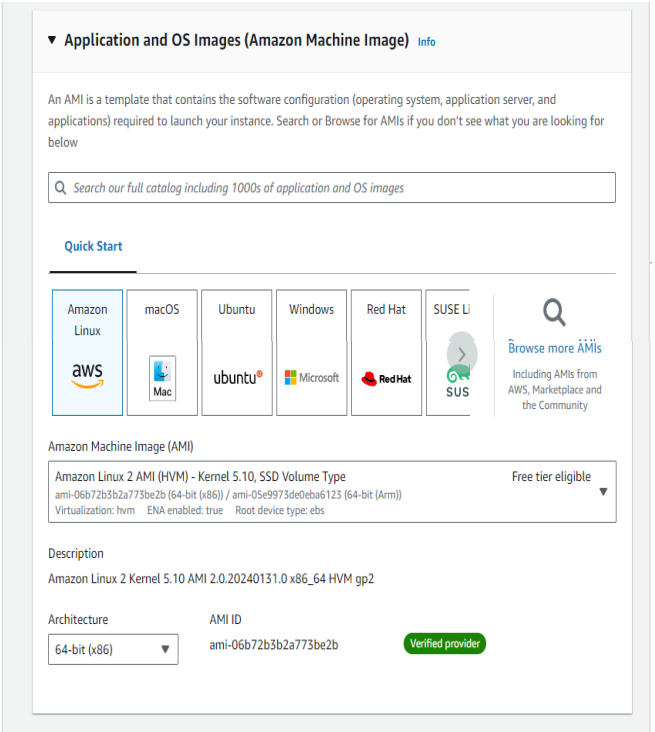
2. From the EC2 console dashboard, in the **Launch instance** box, choose **Launch instance**.



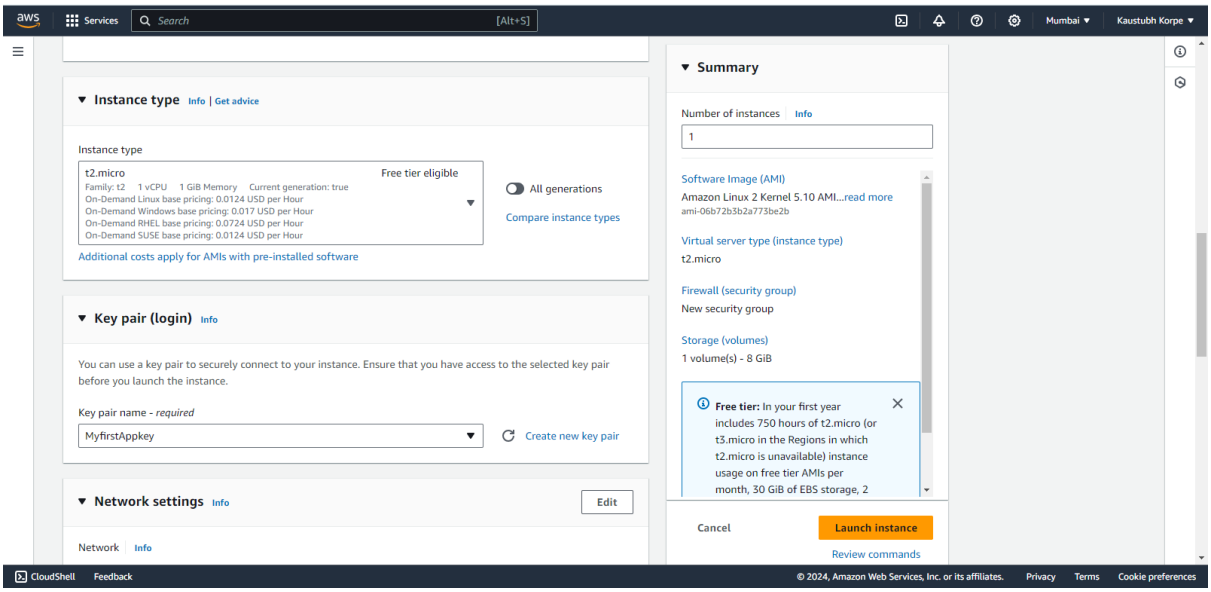
3. Under **Name and tags**, for **Name**, enter a descriptive name for your instance.



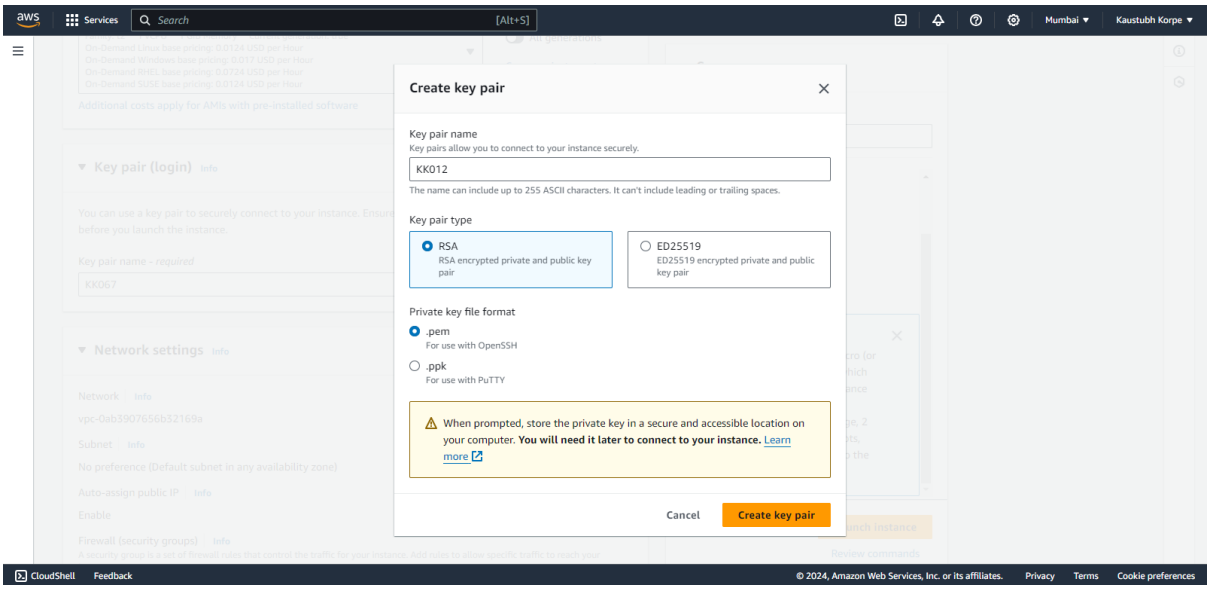
4. Under **Application and OS Images (Amazon Machine Image)**, do the following:
   a) Choose **Quick Start**, and then choose Amazon Linux. This is the operating system (OS) for your instance. From **Amazon Machine Image (AMI)**, select an HVM version of Amazon Linux 2.
   b) Notice that these AMIs are marked **Free Tier eligible**. An *Amazon Machine Image (AMI)* is a basic configuration that serves as a template for your instance.



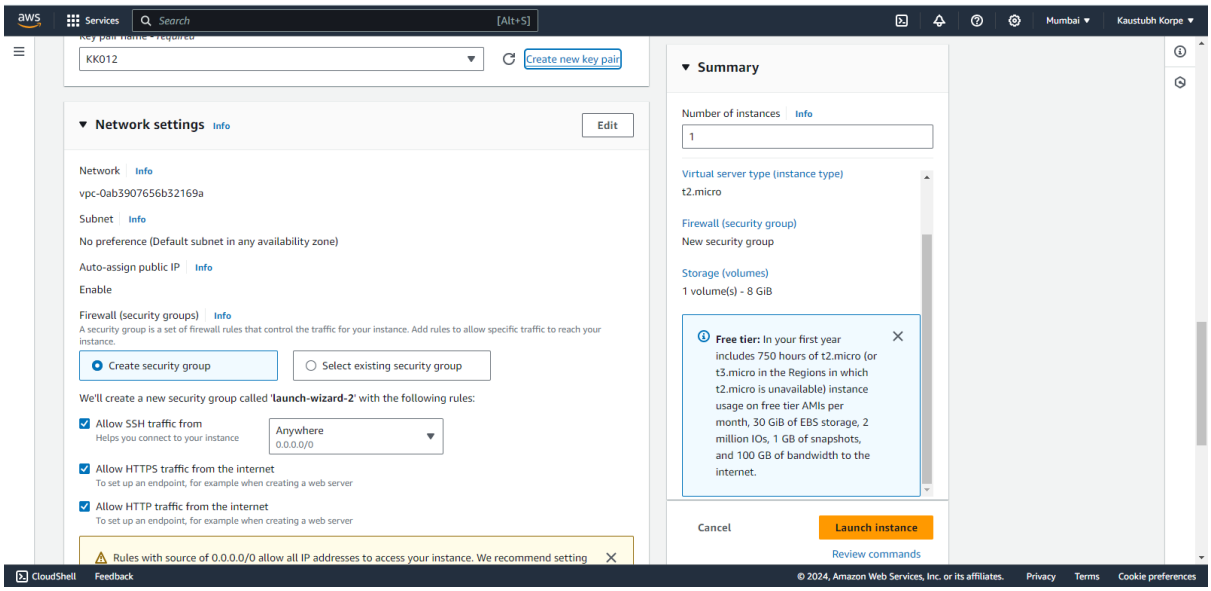
5. Under **Instance type**, from the **Instance type** list, you can select the hardware configuration for your instance. Choose the t2.micro instance type, which is selected by default. The t2.micro instance type is eligible for the Free Tier. In Regions where t2.micro is unavailable, you can use a t3.micro instance under the Free Tier.



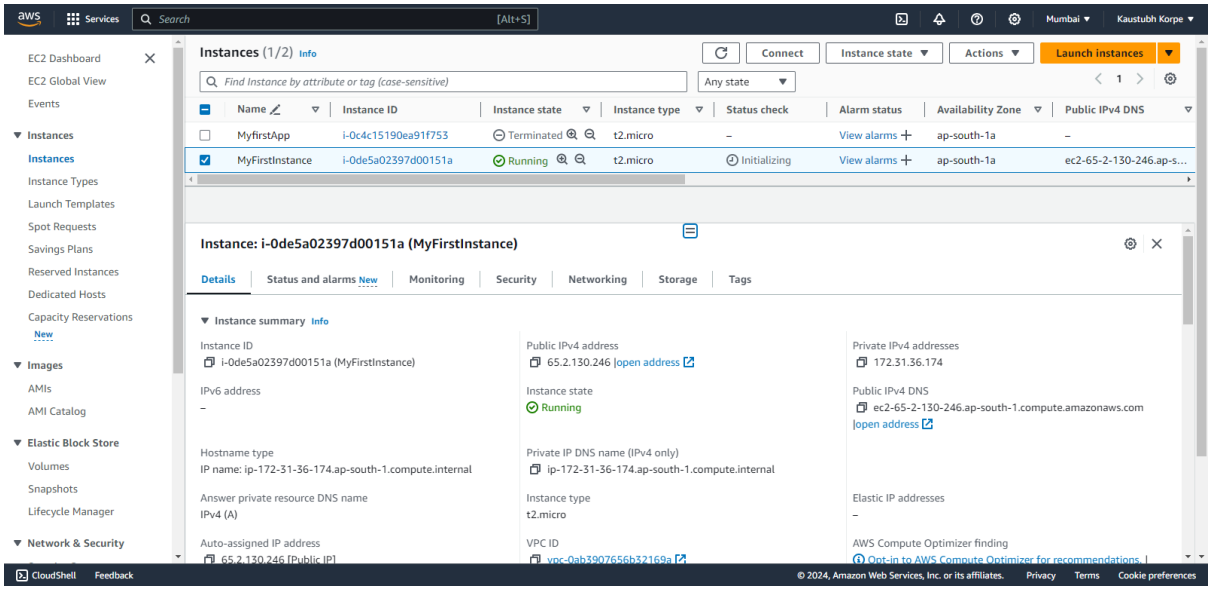
6. Under **Key pair (login)**, for **Key pair name**, choose the key pair that you created when getting set up.



7. Next to **Network settings**, choose **Edit**. For **Security group name**, you'll see that the wizard created and selected a security group for you. You can use this security group, or alternatively you can select the security group that you created when getting set up using the following steps:
    a. Choose **Select existing security group**.
    b. From **Common security groups**, choose your security group from the list of existing security groups.
8. Keep the default selections for the other configuration settings for your instance.
9. Review a summary of your instance configuration in the **Summary** panel, and when you're ready, choose **Launch instance**.



10. A confirmation page lets you know that your instance is launching. Choose **View all instances** to close the confirmation page and return to the console.
11. 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 IPv4 DNS** column is hidden, choose the settings icon (⚙) in the top-right corner, toggle on **Public IPv4 DNS**, and choose **Confirm**.
12. It can take a few minutes for the instance to be ready for you to connect to it. Check that your instance has passed its status checks; you can view this information in the **Status check** column.



Connecting to the Instance

There are many ways to connect to your Linux instance.

Once instance is created, select the connect button given on the console.