Q1:

▼ Key pair (login)  Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

ec2usecase1

Create new key pair

▼ Network settings  Info                                    Edit

Network  Info
vpc-0dbfb4d3298e3435a

Subnet  Info
No preference (Default subnet in any availability zone)

▼ Summary

Number of instances  Info

1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.0.2...read more
ami-02396cdd13e9a1257

Virtual server type (instance type)
t2.micro

Cancel          Launch instance

Review commands

CloudShell   Feedback   Language          © 2023, Amazon Web Services India Private Limited or its affiliates.   Privacy   Terms   Cookie preferences

ec2usecase1 (1).ppk        ec2usecase1.ppk        facebook.ppk        Show all

---



Enable

Firewall (security groups)  Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

◉ Create security group          ○ Select existing security group

We'll create a new security group called 'launch-wizard-2' with the following rules:

☑ Allow SSH traffic from          Anywhere
Helps you connect to your instance    0.0.0.0/0

☐ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☑ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

▼ Summary

Number of instances  Info

1

Software Image (AMI)
Amazon Linux 2 AMI (HVM) - Ker...read more
ami-03c7d01cf4dedc891

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Cancel          Launch instance

Review commands

CloudShell   Feedback   Language          © 2023, Amazon Web Services India Private Limited or its affiliates.   Privacy   Terms   Cookie preferences

Q2:

Q3:

**Object Ownership** Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

**ACLs disabled (recommended)**
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

**ACLs enabled**
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

⚠ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

Object Ownership

◉ Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

○ Object writer
The object writer remains the object owner.

---

**Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

**Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

**Block public access to buckets and objects granted through *any* access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.

**Block public access to buckets and objects granted through *new* public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

**Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

⚠ **Turning off block all public access might result in this bucket and the objects within becoming public**
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☑ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Hi this is Sanjay!!